# Network Camera

# User Manual

Version 1.0 - March 20261

# 1. Overview

## 1.1 System Requirements

Your computer must meet the following minimum requirements to access and operate the product:

**Table 1-1 System Requirements**

| Item | Recommended Specifications |
|---|---|
| Operating System | Microsoft Windows 10 or later |
| CPU | 2.0 GHz or faster |
| RAM | 2 GB or higher recommended |
| Display | 1024 × 768 resolution or higher |
| Web Browser | - Google Chrome (latest version recommended)<br>- Microsoft Edge (latest version recommended)<br>- Mozilla Firefox (latest version recommended) |

**Note**
The instructions in this manual are based on **Microsoft Windows 10 and Microsoft Edge**. User interface and functionality may vary depending on your operating system and browser.

## 1.2 Network Connection

**Before You Start**

- Before accessing a network camera from a PC, ensure the camera is properly connected using a network cable. The connection can be made directly to the PC or through a switch or router.
- The network camera supports both **direct power supply** and **PoE (Power over Ethernet)**. Ensure the device is properly powered on before use.

The following diagrams illustrate the two connection methods between a network camera and a computer.

**Connection Methods**

**1. Direct Connection**

Connect the network camera directly to the PC using a network cable, as shown in the figure below.

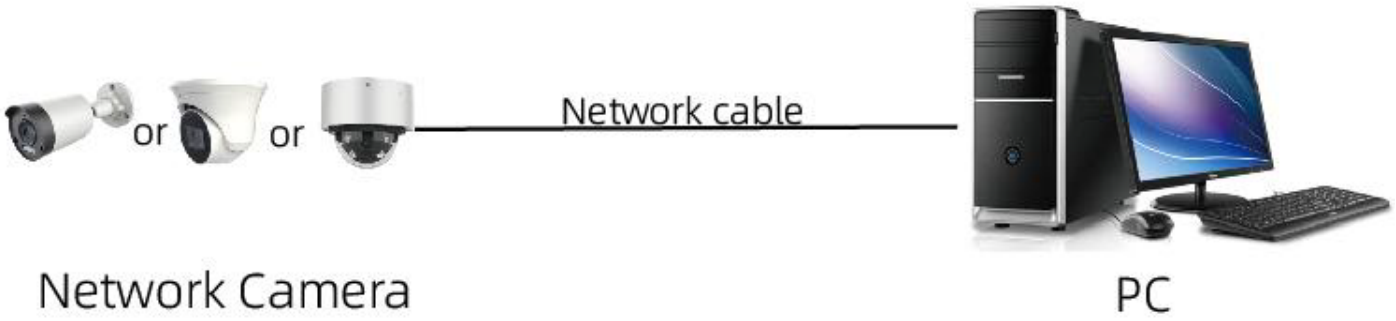



**Figure 1-1 Direct Connection**

**2. Connection via a Switch or Router**

Connect the network camera to a switch or router, then connect the switch or router to the PC using network cables, as shown in the figure below.


**Figure 1-2 Connection via a Switch or Router**

# 2. Login

## 2.1 Login

The following login procedure is illustrated using **Microsoft Edge**.

1. Enter the IP address of the camera in the browser address bar to access the login page.
2. Enter your username and click **Login**.
3. If the **Save Password** option is enabled, you will not need to re-enter your password on subsequent logins.
   For security reasons, the use of this feature is not recommended.
4. After logging in, the camera's live view will be displayed by default.

## 2.2 Install Plug-ins

If you are logging in for the first time, click **Plugin Download** to download the browser plug-in (**InaxsysLocalServerSetup.exe**).

1. Follow the prompts in your browser (e.g., **Download** → **Keep** → **Show more** → **Keep anyway**).
   The installer **InaxsysLocalServerSetup.exe** will be downloaded. Double-click the installer to begin the installation. Once the installation is complete, refresh your browser to finalize the setup.

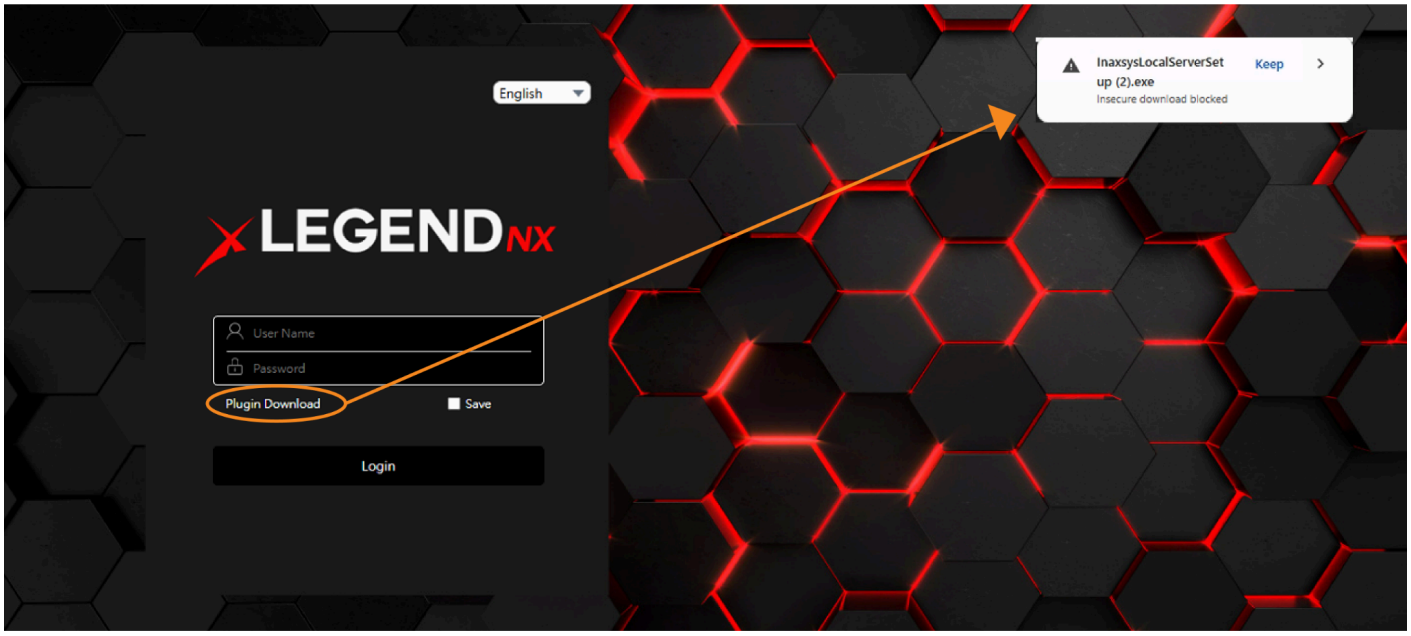



**Figure 2-1 Download**

**Note**
When installing **InaxsysLocalServerSetup.exe**, a security warning may appear on your PC. Click **More info**, then select **Run anyway** to proceed with the installation.

1. Install **InaxsysLocalServerSetup.exe**.

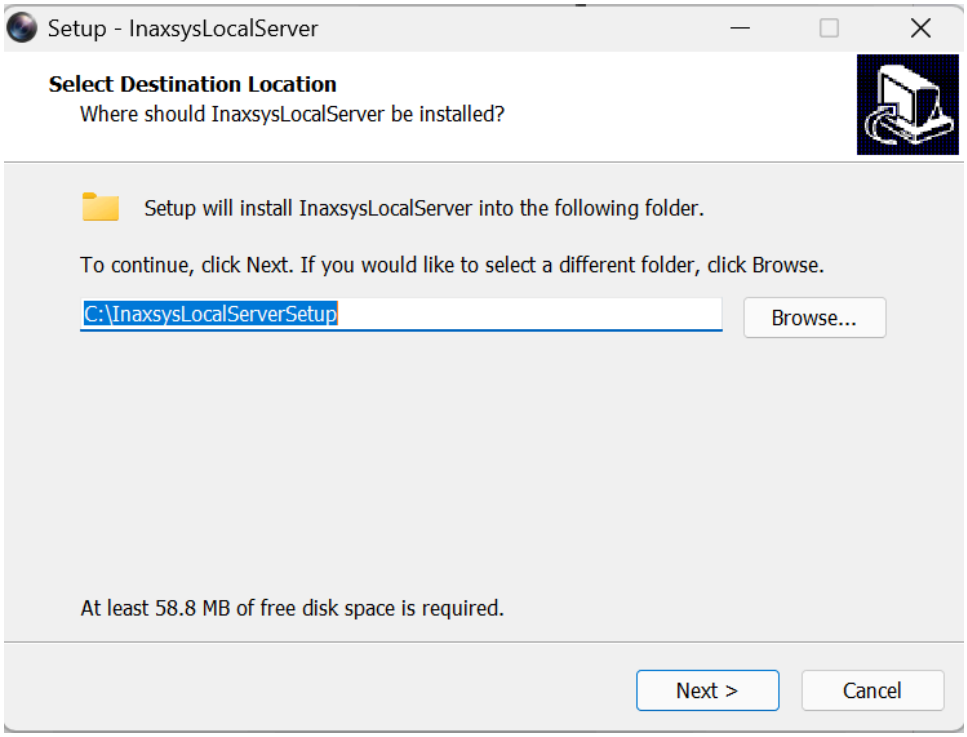



**Figure 2-2 Select Installation Folder**

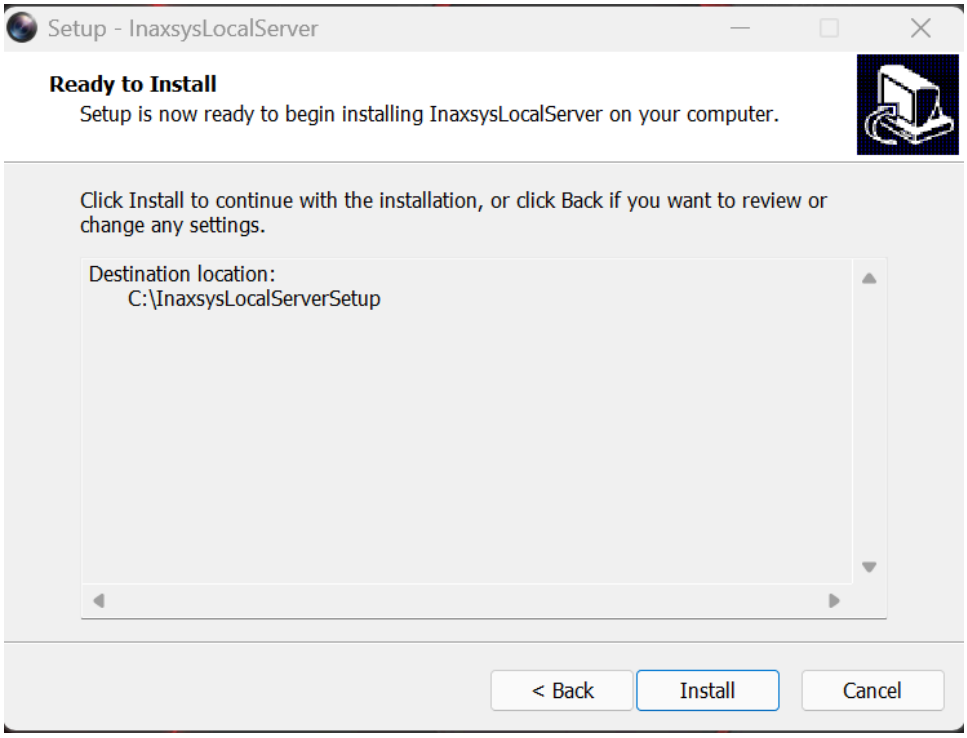



**Figure 2-3 Install**

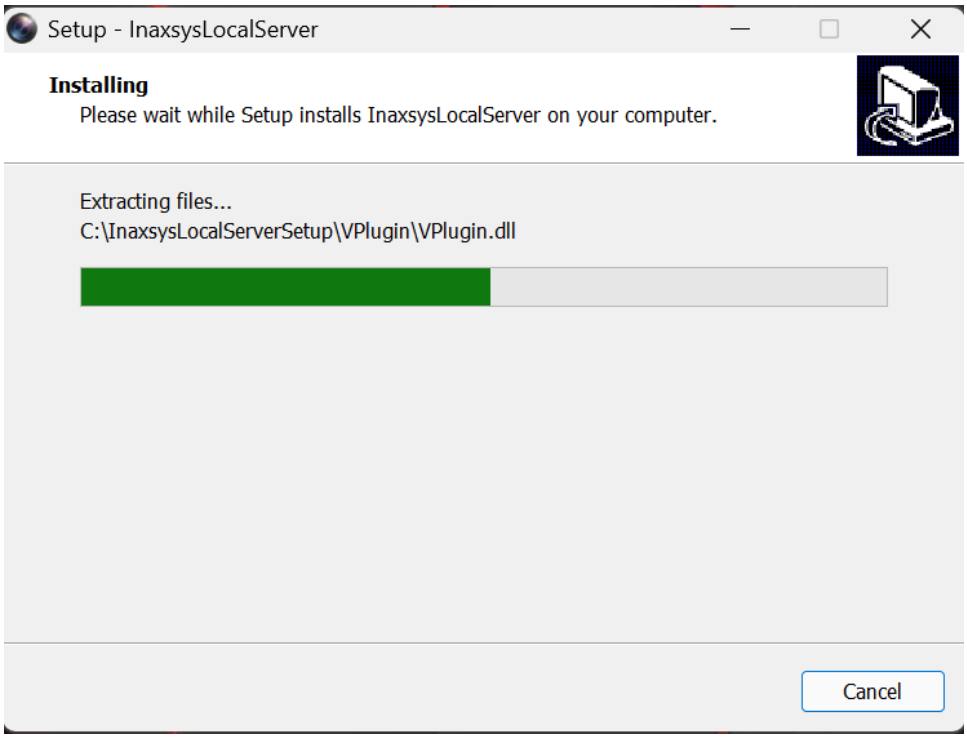



**Figure 2-4 Installing**

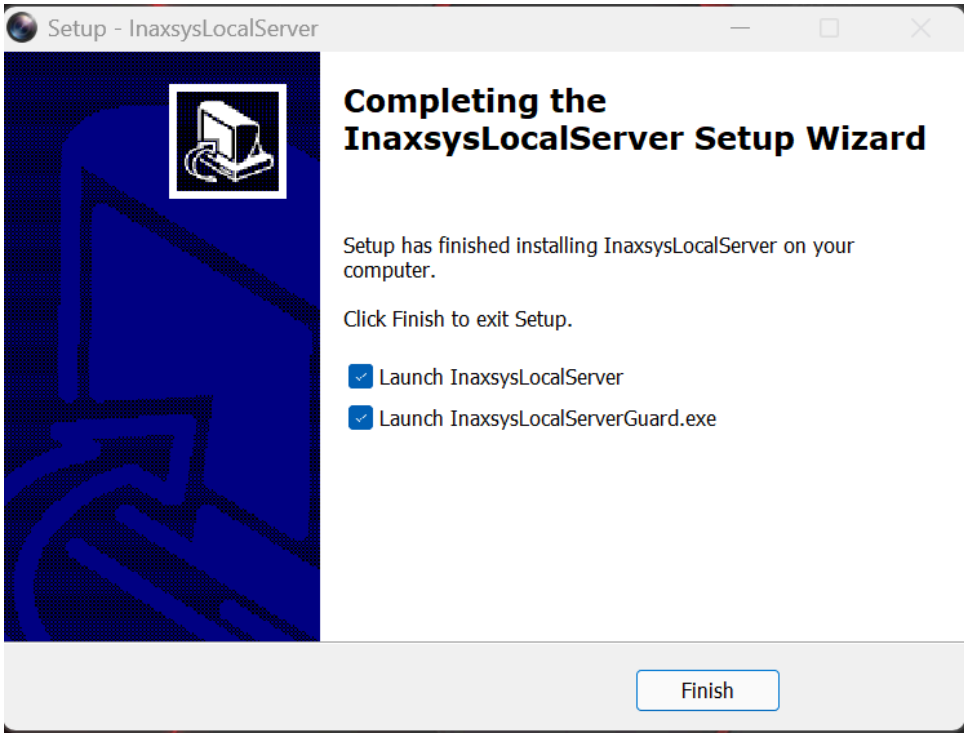



**Figure 2-5 Installation completed**

# 3. Live View

This chapter introduces the parameters of live view, the functions of each icon, and PTZ settings.

## 3.1 Introduction to Live View

By default, the live view window is displayed after logging in to the web interface, as shown in the figure below.

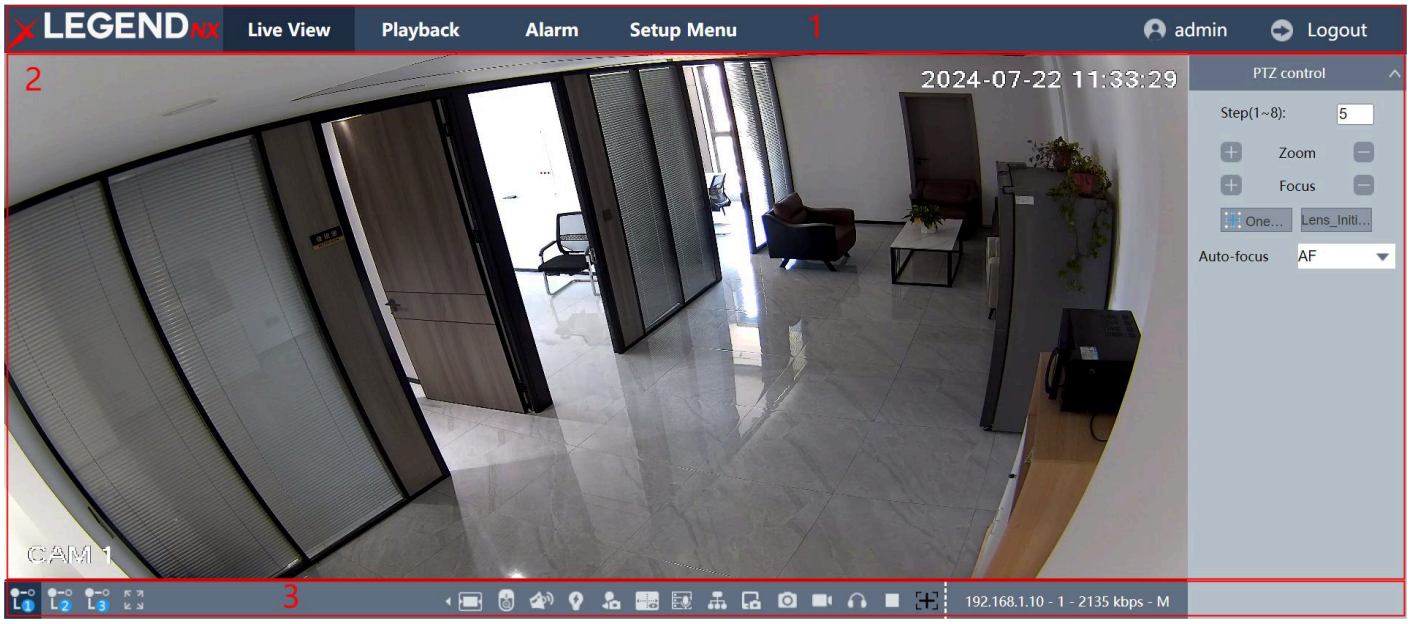
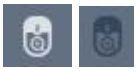


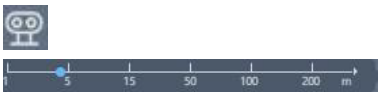

**Figure 3-1 Live View**

**Table 3-1 Live View**

| No. | Item | Description |
|---|---|---|
| 1 | Menu | You can navigate between Live View, Playback, Alarm, Setup Menu, and Account pages in this area. |
| 2 | Preview Window | The live video is displayed in this area. |
| 3 | Toolbar | You can adjust the size of the live view window and set the stream type. You can also perform operations such as start/stop live view, capture, record, audio on/off, etc. |

**Table 3-2 Live View Button Description**

| Button | Description |
|---|---|
|  | Live view (main stream) |
|  | Live view (sub stream) |
|  | Live view (third stream) |
|  | Full screen |
|  | Adaptive screen size |
|  | Set the aspect ratio to 4:3 |
|  | Set the aspect ratio to 16:9 |
|  | Set the aspect ratio according to the video source |
|  | Electronic zoom on/off |
|  | Siren on/off |
|  | Warning light on |
|  | Dynamic tracking on/off |
|  | Talk |
|  | Multicast (requires router support) |
|  | Device Snapshot |
|  | Local Record |
|  | Local snapshot |

| | |
|---|---|
|  | Audio |
|  | Star/stop live view |
|  | Image stitching: drag the scroll bar to adjust the stitching distance<br>Note: Only dual-lens camera support this function |
|   | Device IP address - Channel No. - Real bitrate - Stream Type |

**Note**
The available buttons may vary depending on the camera model.

## 3.2 Start and Stop Live View

Click **Live View**. Click ▸ to start live view. Click ■ to stop live view.

## 3.3 Full Screen Preview

This function is used to access full screen preview mode.

**Steps:**

1. Click **Live View**.
2. Click the full screen icon in the toolbar to enter full screen preview mode.
3. Press **Esc** to exit full screen preview mode.

## 3.4 Adjust Aspect Ratio

**Steps:**

1. Click **Live View**.
2. Click the aspect ratio icon to select the display mode.

- 4:3 refers to a 4:3 window size.
- 16:9 refers to a 16:9 window size.
- 1× refers to the original window size.
- The icon refers to adaptive window size.

## 3.5 Preview Stream Type

This function is used to select the preview stream type according to your needs.
For detailed information about stream types, refer to **Stream Type**.

**Steps:**

1. Click **Live View**.
2. Click the stream selection icon in the toolbar.

-  refers to the main stream.
-  refers to the sub stream.
-  refers to the third stream.

## 3.6 Manually Triggered Sound Alerts

**Steps:**

1. Click **Live View**.
2. Click  to manually activate the camera's siren once. The device supports switching alarm content. For red and blue light settings, refer to **6.3 Alarm Audio**.

## 3.7 Manually Triggered Light Alerts

**Steps:**

1. Click **Live View**.
2. Click  to manually activate the camera's warning light.
   For red and blue light settings, refer to **6.3 Alarm Audio**.

## 3.8 Dynamic Tracking Lines and Smart Rules

This function is used to display dynamic tracking lines and smart rules in preview.
For detailed information about smart rules, refer to **7.4 Smart Event**.

**Steps:**

Click   to enable or disable dynamic tracking lines and smart rules in preview.

## 3.9 Multicast View

This function is used to enable multicast view.
For detailed information about multicast, refer to **5.3.12 Multicast**.

**Steps:**

Click  to open multicast view.

## 3.10 Recording Videos and Capturing Pictures Manually

This function is used to capture pictures and record videos manually from Live View.

**Steps:**

1. Click  to take a snapshot and save the picture to the device memory.
2. Click  to take a snapshot and save the picture to the specified path on your PC.
3. Click  to start manual recording and click  again to stop the recording.

**Note**
The video will be saved to the specified path on your PC.  For path configuration, refer to 5.1 Local Storage.

## 3.11 Audio and Talk to the Device

**Steps:**

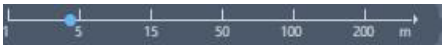
1. Click  to enable audio. You will hear sound from the camera's microphone.
2. Click  to talk to the device. The camera's speaker will play the sound from your microphone.

**Note**
This feature is only supported on cameras equipped with a microphone or speaker.

## 3.12 Image Stitching

This function is used to set the stitching distance for dual-lens cameras.

**Steps:**

1. Click **Live View**.
2. Click  .
3. Drag the slider  in the scroll bar 

to adjust the stitching distance.

# 4. Configuration

## 4.1 Local Storage

You can specify the path for saving recorded files and snapshot pictures on your PC by following the steps below.

Go to **Setup Menu** → **Local Set**.

● **Recorded video**
**Record Size:** Set the maximum file size for recorded videos. Available options are **256MB, 512MB, 1GB**.

**Record Path:** Specify the path for saving videos recorded manually from Live View. You can click **Browse** and select a folder as the storage path.

**Remote Path:** Specify the path for saving videos recorded manually or downloaded from Playback. You can click **Browse** and select a folder as the storage path.

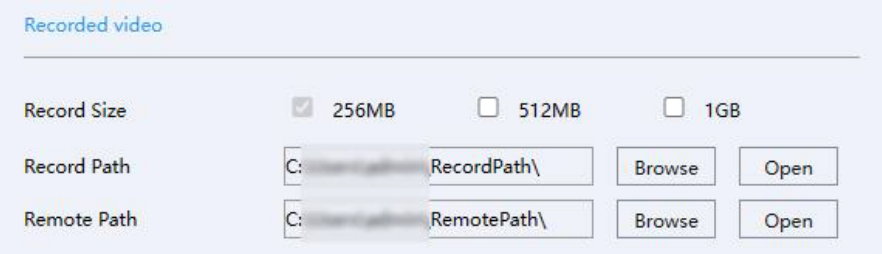



**Figure 4-1 Recorded Video**

● **Snapshot**
**Picture Path:** Specify the path for saving snapshots taken manually from Live View. You can click **Browse** and select a folder as the storage path.

**Picture Path:** Specify the path for saving snapshots taken manually from Playback. You can click **Browse** and select a folder as the storage path.


**Figure 4-2 Snapshot**

## 4.2 System Parameters

In this section, you can configure the device system parameters.

### 4.2.1 Check Device Information

On this page, you can view device information such as firmware version, MAC address, model, etc.

**Steps:**
Go to **Setup Menu** → **System** → **Setting** to view the device information.

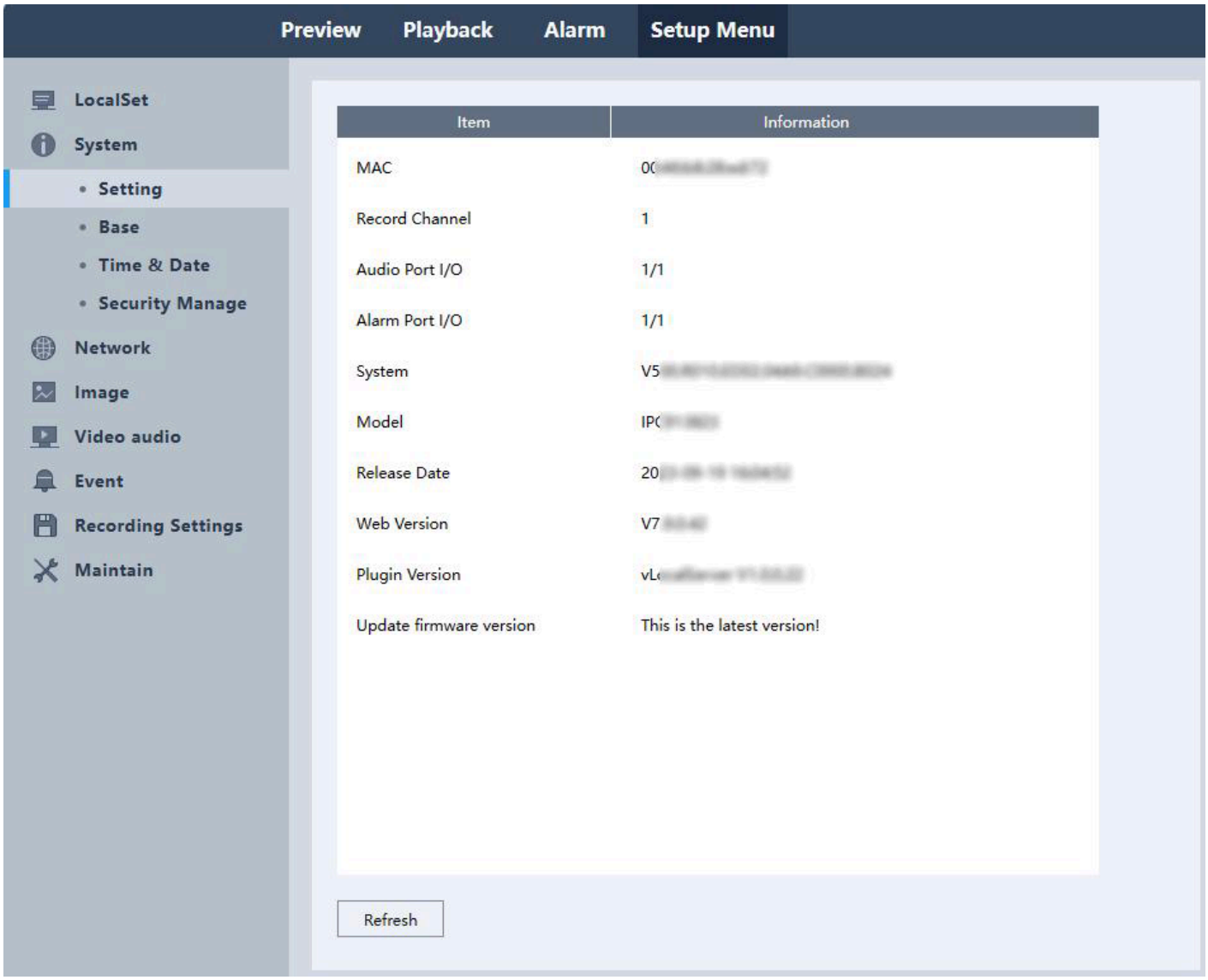



**Figure 4-3 System Settings**

**Note**
When you see “New version available!” on the interface, it is recommended to manually download and update the software.

### 4.2.2 Set Device Language, Video Format & Host Name

You can perform the following steps to set the device language, video format, and host name.

**Steps:**
Go to **Setup Menu** → **System** → **Base**.

● **Language:** Click ▼ and select the desired language. Click **Save** to apply the settings.

● **Video standard:** Click ▼ and select the video format (**PAL / NTSC**). Click **Save** to apply the settings.

● **Host name:** You can edit the host name as needed. Click **Save** to apply the settings.

**Note**
The host name will be displayed on the network and when using the email function. For details about the email function, please refer to 4.3.7 Email.

### 4.2.3 Time and Date

You can perform the following steps to set the device time, time format, DST, etc.

**● Set Manually or Sync with PC**

**Steps:**

1. Go to **Setup Menu** → **System** → **Time & Date**.


**Figure 4-4 Time**

2. Set the correct time zone and system time.
3. *(Optional)* Click **SyncPC** to synchronize the camera time with your PC.
4. Set the date and time format.
5. Click **Save**.

**● Set DST (Daylight Saving Time)**

Supports automatic adjustment of the device time.

**Steps:**

1. Go to **Setup Menu** → **System** → **Time & Date** → **DST**.


**Figure 4-5 DST**

2. Enable **DST**.
3. Choose the DST format: **Day of Week** or **Date**.
4. Set the start date and end date.
5. Click **Save**.

**● Set NTP**

The device time will be synchronized with the NTP server.

**Steps:**

1. Go to **Setup Menu → System → Time & Date**.


**Figure 4-6 NTP**

2. Enable **NTP**.
3. Set the Host IP (NTP server).
4. Set the **Port** number.
5. Set the **Update Time**. The device will synchronize the time with the NTP server at this interval.
6. Click **Save**.

### 4.2.4 User and Account Management

In this section, you can add/delete users, modify passwords, and block IP addresses.

**● Create Group and User Account**

**Steps:**

1. Go to **Setup Menu → System → Security Manage → Account**.

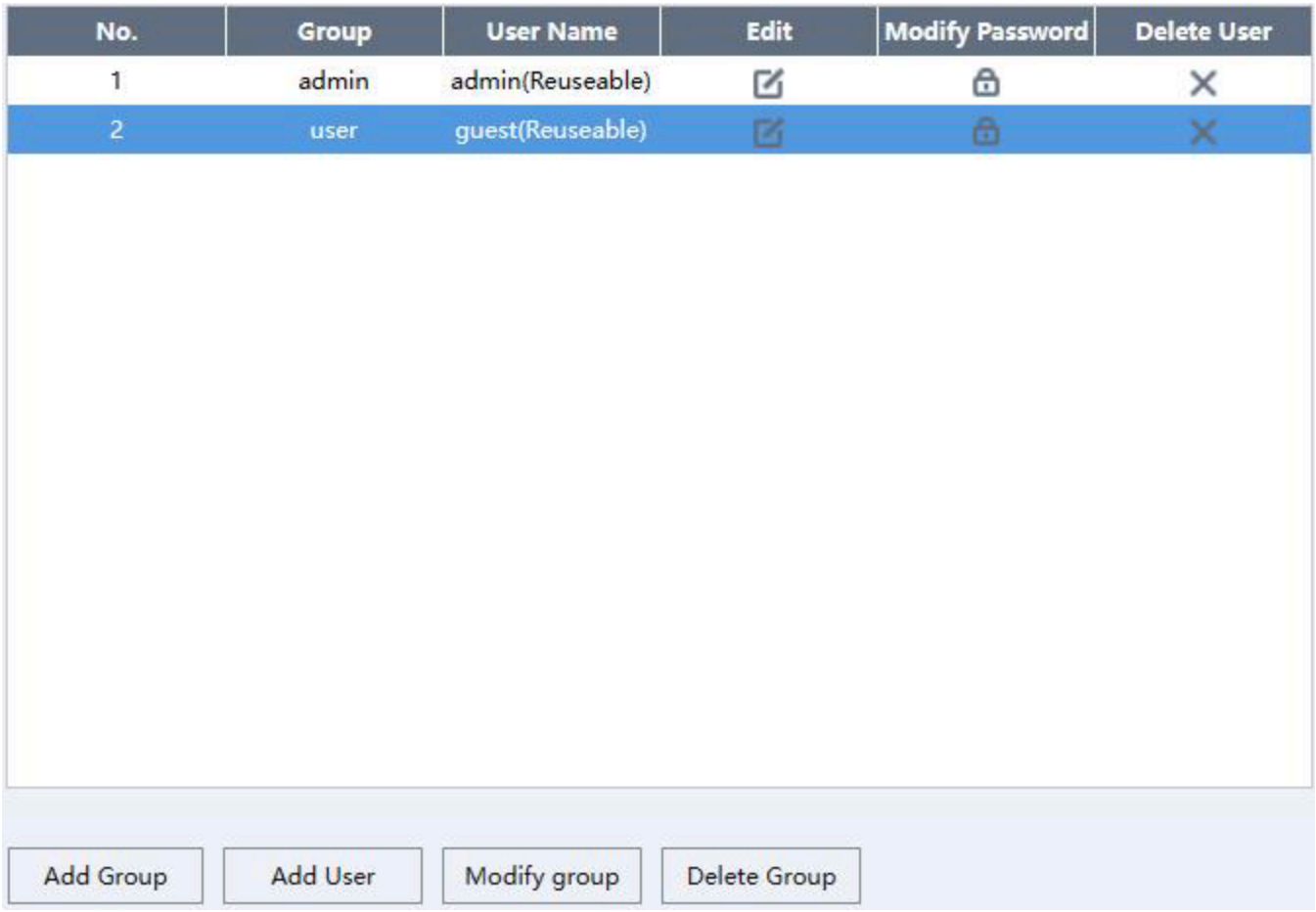



**Figure 4-7 Account**

2. Click **Add Group** to create a new group. Set the group name and permissions, then click **OK**.
3. Click **Add User** to create a new user. Set the username, password, group, and permissions, then click **OK**.

● **Modify User Password**

**Steps:**

1. Go to **Setup Menu** → **System** → **Security Manage** → **Account**.
2. Select the user whose password you want to modify.
3. Click **Modify Password** 🔒, then enter the **Old Password**, **New Password**, and **Confirm Password**.


**Figure 4-8 Modify Password**

4. Click **Save** to apply the changes.

**● Modify Username and Authority**

**Steps:**

1. Go to **Setup Menu** → **System** → **Security Manage** → **Account**.
2. Select the user whose information you want to modify.
3. Click . You can modify the username and user permissions as needed.
4. Click **OK**.

**● Delete User**

**Steps:**

1. Go to **Setup Menu** → **System** → **Security Manage** → **Account**.
2. Click the **Delete User** button (✖) next to the user you want to delete.
3. Enter the username in the pop-up dialog box to confirm.
4. Click **OK**.

**● IP Block**

You can add and delete IP addresses to and from the blacklist. Blocked IP addresses will not be permitted to access the device.

**Steps:**

1. Go to **Setup Menu** → **System** → **Security Manage** → **Access Control**.
2. Under **Restriction Type**, select **Blocked Sites**.
3. Enter the IP address you would like to block in the input box and click **Add IP**. This IP address will be added to the blacklist.

Optional: If you need to remove an IP address from the blacklist, select the IP address and click **Delete IP**.

4. Click **Save**.

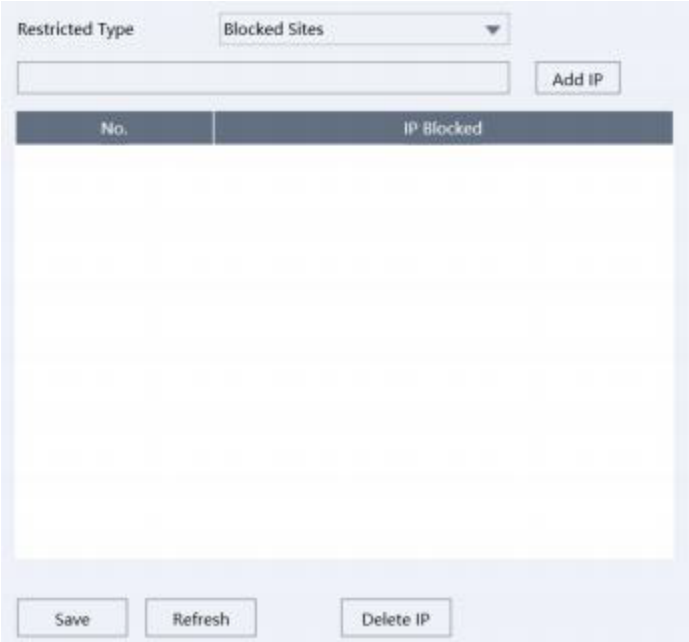



**Figure 4-9 Access Control - Blocked Sites**

**● IP Trust**

You can add IP addresses to the whitelist. IP addresses not included in the whitelist will not be permitted to access the device.

**Steps:**

1. Go to **Setup Menu → System → Security Manage → Account**.
2. Under **Restriction Type**, select **Trusted Sites**.
3. Enter the IP address you would like to add to the whitelist and click **Add IP**. This IP address will be added to the whitelist.

Optional: If you need to remove an IP address from the whitelist, select the IP address and click **Delete IP**.

4. Click **Save**.

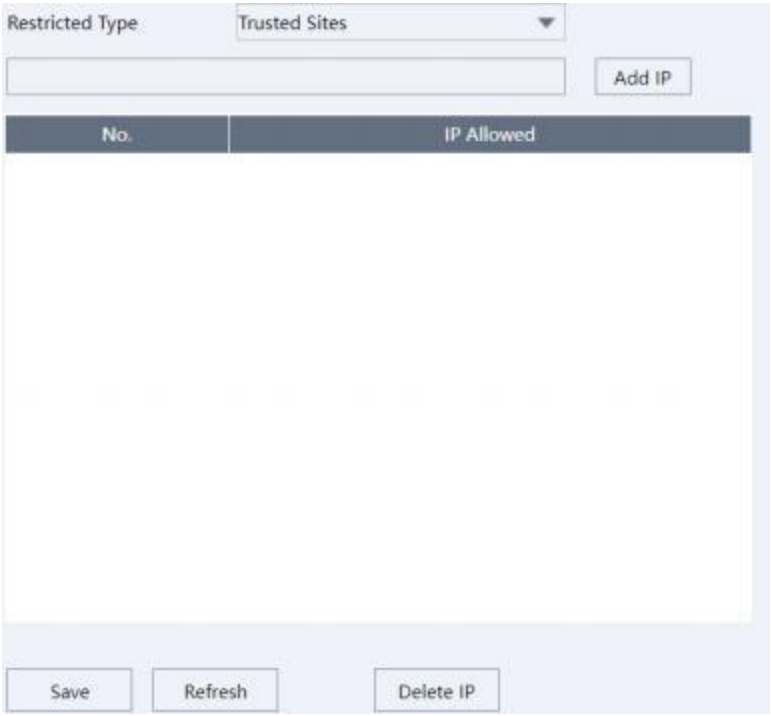



**Figure 4-10 Access Control - Trusted Sites**

**● View Online Users**

You can view the list of current online users in this section.

**Steps:**

1. Go to **Setup Menu → System → Security Manage → Online Users**.
   The information (Username, IP address, Login Way and Login Time) of the online users will be displayed as shown in the following picture.

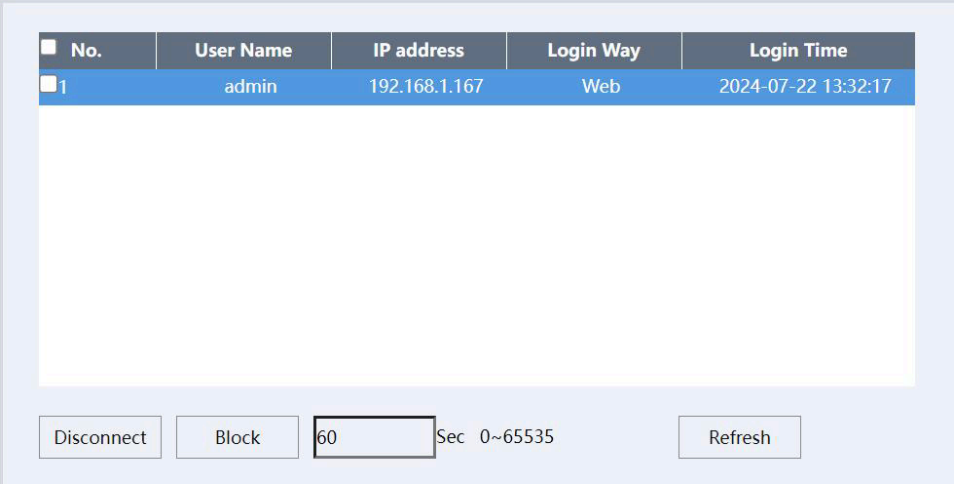



**Figure 4-11 Online Users**

Optional: If you need to disconnect a user from the device, you can select the user and click the **Disconnect** button. The selected user will be disconnected from the device instantly.

If you need to block an IP address of an online user from logging in, you can select the user from the online users list, enter a block duration, and click the **Block** button. IP addresses blocked by this method will not have access to the device for the set duration.

## 4.3. Network Configuration

**Note**
The Network Configuration page may vary depending on the model. Please refer to the actual web interface.

### 4.3.1. Configure Device TCP/IP Settings

TCP/IP settings must be configured properly before you operate the device over a network.

● **NIC Type**
Setting **Adaptive** as default is recommended.

● **DHCP**
By enabling DHCP, the device will automatically obtain an IP address and other network configurations (subnet mask, default gateway) from the DHCP server. Please note that the IP address of the device might change after enabling this feature.

**Steps:**

1. Go to **Setup Menu** → **Network** → **General** → **TCP/IP**.
2. Enable **DHCP**.
3. Click **Save.**

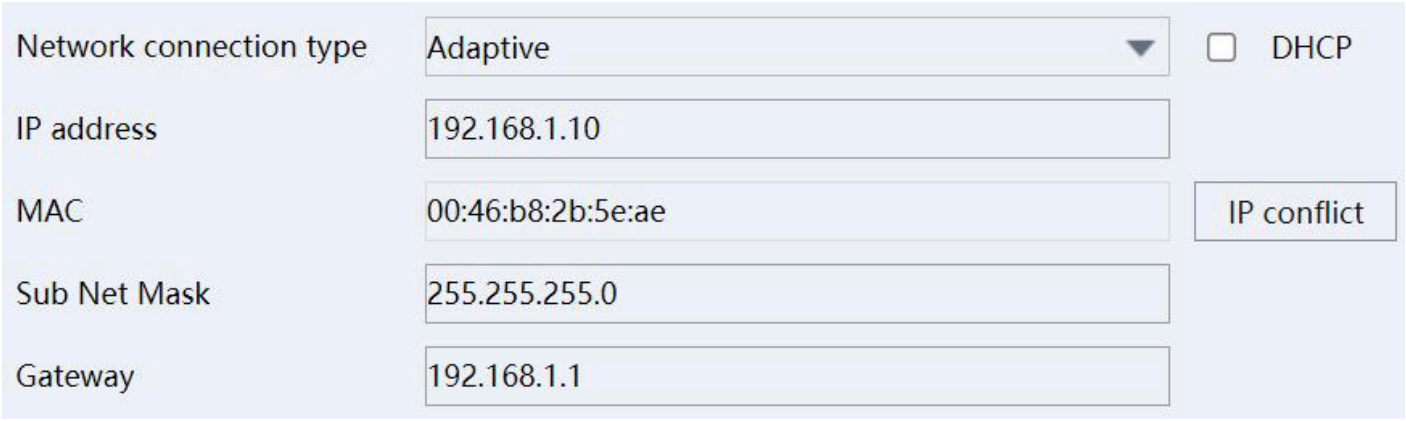



**Figure 4-12 TCP/IP**

● **Manual Configuration**
You can configure the network of the device manually. Enter the device IP Address, IP Subnet Mask, and Gateway, then click **IP conflict** to check if the IP address is available.

**Steps:**

1. Go to **Setup Menu** → **Network** → **General** → **TCP/IP**.
2. Confirm that **DHCP** is disabled.

3. Enter IP Address, Subnet Mask, and Gateway.
4. Click the **IP conflict** button to check if there is an IP conflict.
5. Click **Save**.

**● DNS Server**

DNS is the abbreviation of Domain Name Server. A DNS server is required if you want to access a site from the device through a domain name. It is also required for some features (e.g., sending emails, cloud storage). You need to configure **Preferred DNS Server** and **Alternate DNS Server** properly if you want to use these features.

**Steps:**

1. Go to **Setup Menu** → **Network** → **General** → **TCP/IP**.
2. Enter the **Preferred DNS Server** and **Alternate DNS Server**.
3. Click **Save**.

**● Transfer Mode**

You can set the Transfer Mode to self-adaptive, fluency preferred, or quality preferred.

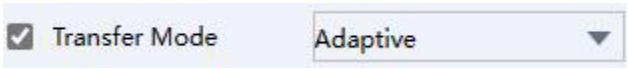



**Figure 4-13 Transfer Mode**

**● Max Users**

You can set the maximum number of IP addresses that can connect to the device simultaneously.

**● Ports**

You can configure the ports for HTTP, HTTPS, Media, RTSP, and RTMP in this section.


**Figure 4-14 Ports**

**● URL Templates**

This section provides templates for RTMP and RTSP URLs. You can use them after modifying them according to your specific situation.


**Figure 4-15 URL Templates**

### 4.3.2. Configure DDNS Settings

Supports the use of Dynamic DNS (DDNS) for network access.

DDNS is the abbreviation of Dynamic DNS. It maps the dynamically allocated IP address of the device to a static domain name that can be accessed from the external network.

**Steps:**

1. Go to **Setup Menu** → **Network** → **General** → **DDNS**.
2. Check the **Enable** checkbox.
3. Select your DDNS provider under **DDNS Type**, then enter your **Domain Name**, **Username**, and **Password**.
4. Click **Save**.

**Note**
Our devices support multiple DDNS providers, such as Oray DDNS, CN99 DDNS, DynDNS DDNS, and NO-IP DDNS. You need to register an account before use. The following table lists the websites of the supported DDNS providers for your reference.

**Table 4-1 DDNS Provider Websites**

| DDNS Type | Website |
|---|---|
| Oray | http://www.oray.com/ |
| DynDNS | http://dyn.com/dns/ |
| NO-IP | https://www.noip.com/ |
| CN99 | http://www.pubyun.com/ |

### 4.3.3. Configure NAT Settings

NAT is the abbreviation for Network Address Translation. It maps addresses and ports between your internal network and external network. You can configure the UPnP™ settings in this section.

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 simplifies the implementation of networks in home and corporate environments.

By enabling this feature, you will not need to configure port mapping for each port manually. The camera will be connected to the Wide Area Network via the router automatically.

**Steps:**

1. Go to **Setup Menu → Network → General → NAT.**
2. Click **Enable.**
3. Click **Save.**

**Note**
To ensure this feature functions properly, please make sure the UPnP feature on your router is enabled.

### 4.3.4. UPNP-TM

By enabling this feature, your network camera can be found as a network device on your network.

**Steps:**

1. Go to **Setup Menu → Network → General → UPNP-TM**.
2. Click **Enable** and enter the device name as you want.
3. Click **Save** to save changes.

**Note**
The default name of the device is its Cloud ID.

### 4.3.5. Cloud

After enabling the Cloud, users can access the device (image, alarm, etc.) via APP or IE Web.

**Steps:**

1. Go to **Setup Menu → Network → General → Cloud**.
2. Click **Enable**.
3. Click **Save**.

Click the **Refresh** button to reload the page. The device is connected to the Cloud when the **Status** changes to **Connected**.

**● Access the device via APP**
**Steps:**

1. Ensure the device **is connected to the Cloud**.
2. Scan the iPhone/Android QR code to download the APP.
3. Scan the Cloud ID QR code to bind the device and access the device.

**Note**
You can download our app LEGEND NX by scanning the QR code on the page corresponding to your platform. To bind your cameras for later access, scan the Cloud ID QR code on the right. Note that you will be required to register an account prior to using LEGEND NX.

● **Access the device via web**

**Steps:**

1. Ensure the device **is connected to the Cloud**.
2. Open your browser, enter the URL displayed by **IE Web** in the URL bar.


**Figure 4-16 IE Web**

3. Switch to **By device**, input **Cloud ID**, **Device username** and **Device password**.

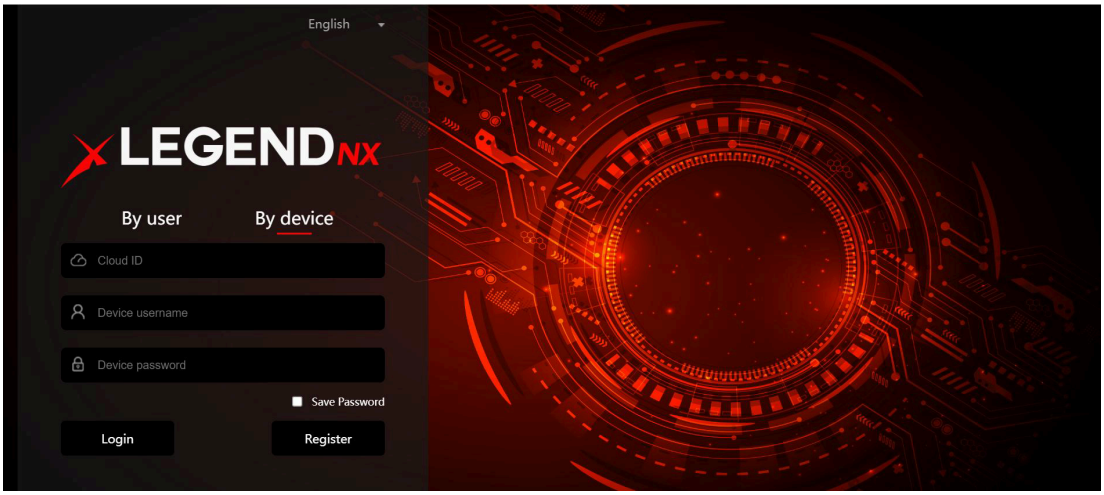



**Figure 4-17 By device**

4. Click **Login**.

## 4.3.6. FTP (File Transfer Protocol)

FTP is the abbreviation of File Transfer Protocol, which is designed for file transfer. In this section, you can configure FTP server settings to enable uploading captured pictures or recorded videos to the FTP server. The uploading process can be triggered by events or scheduled snapshot tasks.

**Steps:**

1. Go to **Setup Menu** → **Network** → **Advance Option** → **FTP**.
2. Select **Type**: Record FTP/Picture FTP.
3. Check the **Enable** checkbox.
4. Enter the IP address in the **Server** input box and the **Port** of your FTP server.
5. Configure the FTP settings: enter the username and password required to log in to the FTP server.
6. Specify the directory and file length for uploading.

**Directory:** The device will create a new folder on your FTP server if the specified directory does not exist.
**File length:** Recorded videos will be segmented into files with a size not larger than the specified file length (Max. 65535 MB).

7. Click **FTP Test** to test the connection to your FTP server.
8. Set the **FTP Schedule**.

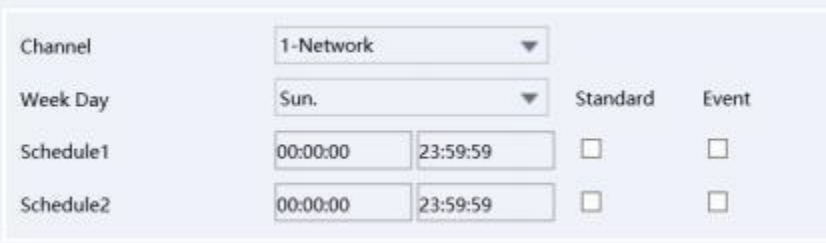



**Figure 4-18 FTP Schedule**

9. Click **Save** to save and apply the settings.

**Note**
To access the FTP server anonymously (without authentication), check the **Anonymous** checkbox. Note that this feature must be supported by the FTP server.

## 4.3.7. Email

The device can send email notifications to all designated receivers when an alarm event (e.g., motion detection, video loss, video tampering, etc.) is detected.

**Before you start:**
Please make sure the TCP/IP settings **have been configured** properly.

**Steps:**

1. Go to **Setup Menu** → **Network** → **Advance Option** → **Email**.
2. Configure the following settings:

**SMTP Server:** The IP address or domain name (e.g., smtp.263xmail.com) of the SMTP server.
**Email Encryption:** None or SSL. When SSL is selected, emails will be sent using SSL encryption.
**Port:** The SMTP port. The default SMTP port is 25 (not secure), and the default SSL SMTP port is 465.
**Snap Interval time:** The time interval between snapshots.
**Username:** The sender's email account.
**Password:** The password of the email account.
**Sender:** The name of the email sender.
**Subject:** The email subject.
**Receiver 1/2/3:** The email addresses of the recipients.

3. Click **Mail Test** to test whether the settings are configured properly.
4. Click **Save** to apply the settings.

**Note**
You can check with your email service provider for the SMTP settings.

### 4.3.8. SNMP

By enabling the SNMP feature, you can obtain the camera status, configurations, and alarm-related information. You can also manage the camera remotely when it is connected to the network.

**Before you start:**
Before configuring SNMP, please download the SNMP client and ensure that you can receive information from the camera via an SNMP port. Trap is an SNMP term for a message sent from one device to another to notify a specific event. By setting the **Trap Address** (the IP address of the trap receiver), the camera can send alarm events and exception messages to the surveillance center.

**Note**
The SNMP version you select should be the same as that of the SNMP client. Select the appropriate version based on the required security level: SNMP v1 provides no security; SNMP v2 requires authentication; SNMP v3 provides encryption. Before using SNMP v3, the HTTPS protocol must be enabled.

**Steps:**

1. Go to **Setup Menu → Network → Advance Option → SNMP**.
2. Check the checkbox for **Enable SNMPv1**, **Enable SNMP v2c**, or **Enable SNMPv3** as required.
3. Configure the **SNMP settings**.
4. Click **Save**.

**Note**
To reduce the risk of information leakage, SNMP v3 is highly recommended instead of SNMP v1 or v2.


**Figure 4-19 SNMP Settings**

## 4.3.9. HTTPS

HTTPS provides authentication of the website and its associated web server, protecting against man-in-the-middle attacks.

**Before you start:**
Make sure the HTTPS port is configured properly in **General** → **TCP/IP** before enabling the HTTPS feature on the device. For example, if the port number is set to 443 and the IP address is 192.168.1.10, you can access the device by entering https://192.168.1.10:443 in the address bar of a supported web browser.

**Steps:**

1. Go to **Setup Menu** → **Network** → **Advance Option** → **HTTPS**.
2. Check the **Enable** checkbox.

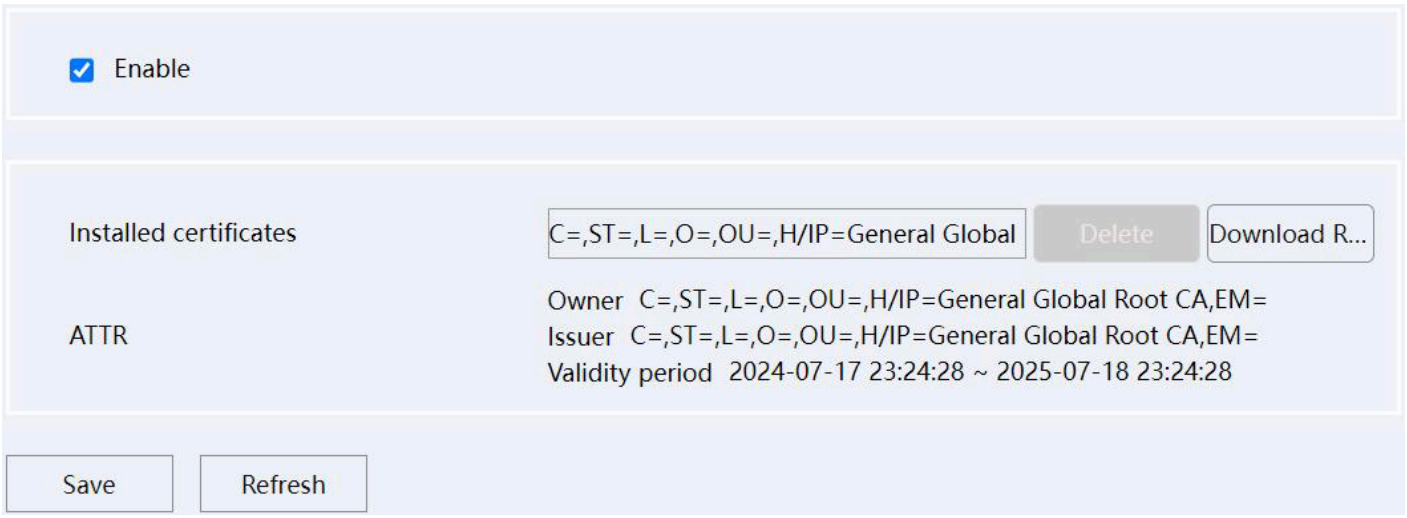



**Figure 4-20 HTTPS**

3. You need to **download** the certificate and install it on your PC before accessing the device via HTTPS.
4. Click **Save** to save changes.
5. The device will reboot to apply the settings.

**Note**
If the HTTPS feature is enabled but the certificate has not been installed on your PC, a notification such as “the certificate of this site has an issue” will be displayed when accessing the device web page.

## 4.3.10 Multicast

In computer networking, multicast (one-to-many or many-to-many distribution) is a group communication method where data transmission is addressed to a group of destination computers simultaneously.

When multiple servers request the same information, the source device only needs to send the data once. Therefore, the main benefit of multicast is saving transmission bandwidth when the device is accessed by multiple remote clients.

**Before you start:**

Please confirm that the router to which the device is connected supports the multicast feature.

**Steps:**

1. Go to **Setup Menu** → **Network** → **Advance Option** → **Multicast**.
2. Set the Multicast IP (224.0.0.0~239.255.255.255) and port (1025~65534).
3. Click **Save** to save changes.

# 5. Image Parameter Configuration

**Note**
The Image Configuration page may vary depending on the model. Please refer to the actual web interface.

## 5.1 Schedule Image Setting

You can select an image mode from three options: **Auto Switch**, **Scheduled Switch**, and **Universal Day and Night**.

● **Universal Day and Night**: The same image settings will be applied to both day and night modes.

● **Scheduled Switch**: You can configure image parameters for Daytime and Night modes individually. You need to set a schedule to switch between Daytime and Night modes if you select this option.

● **Auto Switch**: You can configure image parameters for Daytime and Night modes individually, and the device will automatically switch between them according to the day/night conditions.

**Steps:**

1. Go to **Setup Menu** → **Image** → **Image Configuration**.
2. Click the **Image Mode** drop-down box to select a mode.

## 5.2 Image Adjust

● **Brightness**: Specifies the brightness/luminance of the image. The parameter ranges from 0 to 100, with a default value of 50.

● **Contrast**: Specifies the difference between light and dark areas in the image. The parameter ranges from 0 to 100, with a default value of 50.

● **Saturation**: Specifies the color intensity of the image. The parameter ranges from 0 to 100, with a default value of 50.

● **Hue**: Defines the color tone based on its dominant wavelength. The parameter ranges from 0 to 100, with a default value of 50.

● **Sharpness**: Specifies the clarity of edges in the image. The parameter ranges from 0 to 100, with a default value of 50.

**Steps:**

1. Go to **Setup Menu** → **Image** → **Image Configuration**.
2. Click **Image Configuration** and adjust the parameters using the sliders for each setting.

## 5.3 Exposure

You can select the appropriate exposure mode to achieve the desired exposure effect.

● **Anti-Flicker**: Supports Outdoor / 50 Hz / 60 Hz anti-flicker modes. Select the appropriate option based on your environment.

**Note**: 50 Hz / 60 Hz reduces flickering (horizontal stripes) by adjusting the shutter frequency.

● **Exposure Mode**: Auto / Manual.

**Auto**: The camera automatically adjusts the exposure time according to the environment.

**Exposure Time**: Refers to the electronic shutter speed. Available options include 1/3, 1/4, 1/5, 1/6, 1/8, 1/10, 1/12, 1/15, 1/25, 1/30, 1/50, 1/60, 1/100, 1/120, 1/250, 1/500, 1/1000, 1/2000, 1/4000, and 1/10000. You can adjust it according to the lighting conditions.

**Note**: Exposure time controls the amount of light entering the lens. A fast shutter speed is suitable for fast-moving scenes, while a slow shutter speed is suitable for scenes with little movement.

● **Gain**: Adjusts the image signal to match lighting conditions. The default value is 50. Increasing the value makes the image brighter but also increases noise.

**Note**: The Gain parameter can only be configured when **Exposure Mode** is set to Auto.

**Steps:**

1. Go to **Setup Menu** → **Image** → **Image Configuration**.
2. Click **Exposure** and configure the parameters.

## 5.4 Back Light Compensation

**Note**
Only one of these features can be enabled at a time.

● **Light Inhibition**: This feature should be enabled when there is strong light in the scene.

You can adjust the **Highlight Compensation** parameter only when this function is enabled. The value ranges from 0 to 100. The higher the value, the stronger the effect.

● **Back Light Compensation (BLC)**: This function compensates for backlighting on a subject in the foreground to improve visibility. You can select from **Close**, **Default**, and **Custom**.

● **WDR/DWDR**: (Digital) Wide Dynamic Range can be enabled when there is a high contrast between bright and dark areas in the scene.

You can adjust the WDR/DWDR parameter (limit) only when the function is enabled. The higher the value, the wider the dynamic range.

**Steps:**

1. Go to **Setup Menu** → **Image** → **Image Configuration**.
2. Click **Back Light Comp** and configure the parameters.

## 5.5 White Balance

White balance controls how the camera renders white tones and is used to adjust color temperature according to the environment.

**Auto Mode**: The camera automatically adjusts the color temperature based on the environment.

**Manual Mode**: The user can manually adjust the R (red) gain and B (blue) gain.

**Steps:**

1. Go to **Setup Menu** → **Image** → **Image Configuration**.
2. Click **White Balance** and configure the parameters.

## 5.6 Day and Night Mode Switch

● **Day/Night Switch**: You can select the Day/Night mode based on different surveillance needs. Available options include **Daytime**, **Night**, and **Auto**.

**Daytime**: The camera remains in day (color) mode.

**Night**: The camera remains in night (black and white) mode.

**Auto**: The camera automatically switches between day and night modes based on lighting conditions to provide optimal image quality.

● **Filter Time**: Refers to the delay time for switching between day and night modes. The adjustable range is 5–120 seconds.

● **Fill Light Type**: Allows you to configure the **infrared (IR) lamp** mode. Available options are **Close**, **Auto**, and **Manual**.

**Close**: The infrared lamp is turned off.

**Auto**: When ambient light is low, the infrared lamp turns on automatically and adjusts its brightness to achieve the best image quality.

**Manual**: When ambient light is low, the infrared lamp turns on at maximum brightness.

**Steps:**

1. Go to **Setup Menu** → **Image** → **Image Configuration**.
2. Click **Day/Night Switch** and configure the parameters.

## 5.7 Illuminator

**Steps:**

1. Go to **Setup Menu** → **Image** → **Image Configuration**.

2. Click **Illuminator** and configure the parameters.

● **Smart IR**: Adjustable IR brightness feature that automatically adapts IR intensity based on image brightness.

When an object is very close to the camera, the IR illumination may be too strong, causing overexposure (white-out) and loss of detail. Smart IR automatically reduces IR intensity to prevent this issue and preserve image details.

There are three options: **Close**, **Manual**, and **Auto**.

**Close**: Turns off IR.

**Manual**: Adjusts IR brightness manually.

**Auto**: Adjusts IR brightness automatically.

● **Warm Light Setting**

**Fill Light Mode**: Three options are available: **Close**, **Manual**, and **Auto**.

- **Close**: Turns off the warm light.
- **Manual**: Adjusts the warm light brightness manually.
- **Auto**: Adjusts the warm light brightness automatically.

**Fill Light Position**: When the warning light is triggered, select whether the left or right light is activated.

**Brightness Upper Limit / Brightness**: The higher the value, the higher the brightness.

## 5.8 Enhancement

The device supports **Noise Reduction** and **Defog** features to improve image quality.

You can adjust the **NR Level** to control the intensity of noise reduction. Note that higher levels may result in a softer (slightly blurred) image.

You can enable the **Defog** feature to improve image clarity in foggy or hazy conditions.

● **NR Level**: Noise reduction level, ranging from 0 to 6. The higher the value, the lower the image noise.

● **Defog**: Enable this feature when the environment is foggy or the image appears hazy. It enhances fine details and improves overall image clarity.

**Steps:**

1. Go to **Setup Menu** → **Image** → **Image Configuration**.
2. Click **Enhancement** and configure the parameters.

## 5.9 Privacy Mask

In certain situations, you may need to define masked areas on the camera image to protect privacy (for example, an ATM keypad).

When a PTZ camera changes position or zooms, you may need to manually adjust the Privacy Mask to ensure the area remains covered.

**Steps:**

1. Go to **Setup Menu** → **Image** → **Privacy Mask**.
2. Check the **Enable** checkbox.
3. Left-click on the preview window and drag to draw a masked area (up to 4 areas).

**Optional:**

**Move a mask area**: Left-click on a masked area, then drag it to the desired position.

**Delete a mask area**: Left-click on a masked area, then click **Delete**. You can also click **Clear** to remove all masked areas.

4. Click **Save**.

# 6. Video and Audio Configuration

This section describes the configuration of video and audio parameters.

**Note**
Video and audio configuration options may vary depending on the model. Please refer to the actual web interface.

## 6.1 Video Settings

This section describes video parameters such as stream type, video encoding, and resolution.
To configure, go to **Setup Menu → Video audio → Video Settings**.

### 6.1.1 Stream Type

For devices that support multiple streams, you can specify the type for each stream.

- **Main Stream**
  This stream provides the highest quality supported by the device. It typically offers the best resolution and highest frame rate. However, higher resolution and frame rates require more storage space and bandwidth.

- **Sub Stream**
  This stream provides lower resolution video, consuming less bandwidth and storage space.

- **Mobile Stream**
  This stream is typically used for mobile app preview and consumes the least bandwidth and storage.

- **Event Stream**
  This stream is used for event recording. When an event is triggered, the NVR records video using the selected stream.

**Steps:**

1. Go to **Setup Menu → Video audio**.
2. Click **Video Settings → Stream Type**, then select the stream you want to configure.

### 6.1.2 Video Encoding

This refers to the compression standard used by the device for video encoding.

- **H.264**
  H.264, also known as MPEG-4 Part 10 or Advanced Video Coding (AVC), is a widely used compression standard. It provides a good balance between image quality and file size, significantly reducing storage requirements compared to MJPEG or MPEG-4 Part 2.

- **H.264+**
  H.264+ is an enhanced version of H.264. When enabled, it optimizes bitrate usage and reduces storage

consumption. Compared to H.264, it can reduce storage usage by up to 50% in most scenarios while maintaining similar image quality.

- **H.265**
  H.265, also known as High Efficiency Video Coding (HEVC) or MPEG-H Part 2, is a more advanced compression standard. Compared to H.264, it provides better compression efficiency at the same resolution, frame rate, and image quality.

- **H.265+**
  H.265+ is an enhanced version of H.265. When enabled, it further optimizes bitrate and storage usage. Compared to H.265, it can reduce storage consumption by up to 50% under similar conditions.

- **MJPEG**
  MJPEG (Motion JPEG) encodes video as a sequence of individual images. It is commonly used in scenarios requiring high image accuracy or frame-by-frame processing, but it consumes significantly more bandwidth and storage.

**Steps:**

1. Go to **Setup Menu** → **Video** → **Video Settings**.
2. Select **Compression** and choose **H.264** or **H.265**.
3. Check **Encode Enable** to activate **H.264+** or **H.265+**.
4. Click **Save**.

### 6.1.3 Complexity Level

You can select the encoding complexity level for the device: **Baseline**, **Main Profile**, or **High Profile**.
The higher the complexity level, the more efficient the compression and the smaller the video stream size.
(Available options may vary depending on the model.)

**Steps:**

1. Go to **Setup Menu** → **Video** → **Video Settings** → **Complexity Level**.
2. Select **Baseline**, **Main Profile**, or **High Profile**.
3. Click **Save**.

### 6.1.4 Video/Audio Enable

Configure whether video and audio are enabled for a specific stream.

**Steps:**

1. Go to **Setup Menu** → **Video** → **Video Settings**.
2. Enable or disable **Video/Audio** as needed.
3. Click **Save**.

**Note**
Disabling the Main Stream video is not supported.

### 6.1.5 Resolution

You can set the video resolution according to your needs for **Main Stream**, **Sub Stream**, or **Mobile Stream**. Higher resolutions require more bandwidth and storage space.

**Steps:**

1. Go to **Setup Menu** → **Video** → **Video Settings** → **Resolution**.
2. Select the desired **Resolution**.
3. Click **Save**.

### 6.1.6 Frame Rate (FPS)

Frame rate defines how many frames per second (FPS) are displayed in the video stream.
A higher frame rate provides smoother motion, especially in dynamic scenes, but requires more bandwidth and storage space.

**Steps:**

1. Go to **Setup Menu** → **Video** → **Video Settings** → **Frame Rate (FPS)**.
2. Select the desired **Frame Rate**.
3. Click **Save**.

### 6.1.7 Bit Rate Type

**CBR (Constant Bit Rate):**
The stream is encoded at a fixed bitrate. This ensures stable bandwidth usage and faster processing, but may result in lower image quality in complex scenes.

**VBR (Variable Bit Rate):**
The device dynamically adjusts the bitrate based on scene complexity. This provides better image quality in detailed scenes but uses variable bandwidth.

**Steps:**

1. Go to **Setup Menu** → **Video** → **Video Settings** → **Bit Rate Type**.
2. Select the desired **Bit Rate Type**.
3. Click **Save**.

### 6.1.8 Quality

When **Bit Rate Type** is set to **VBR**, you can configure the video quality level.
Higher quality improves image clarity but requires more bandwidth.

**Steps:**

1. Go to **Setup Menu** → **Video** → **Video Settings** → **Image Quality**.
2. Select the desired **Image Quality**.
3. Click **Save**.

### 6.1.9 Bit Rate (Kb/s)

The bit rate determines the amount of data used to encode the video stream.
Higher video quality requires a higher bit rate and more bandwidth. The available bit rate range depends on the selected resolution and image quality.

**Steps:**

1. Go to **Setup Menu** → **Video** → **Video Settings** → **Bit Rate (Kb/s)**.
2. Set the desired **Bit Rate**.
3. Click **Save**.

### 6.1.10 I-Frame Interval

The I-frame interval defines the number of frames between two I-frames.
In H.264 and H.265 encoding, an I-frame (intra-frame) is a full image that can be decoded independently without reference to other frames.

I-frames require more data than other frame types. A shorter interval (more I-frames) improves video stability and reliability but increases bandwidth and storage usage.

**Steps:**

1. Go to **Setup Menu** → **Video** → **Video Settings** → **I-Frame Interval**.
2. Enter the desired **I-Frame Interval** (typically from 10 to 100).
3. Click **Save**.

## 6.2 Audio Settings

You can configure audio parameters such as audio encoding and noise reduction in this section.

- **Audio Encoding Type:** Two encoding formats are supported: **G.711A** and **G.711U**.
- **Input Volume:** Adjustable from 0 to 100 (default value: 50).
- **Noise Reduction:** When enabled, background noise is reduced.

**Steps:**

1. Go to **Setup Menu** → **Video** → **Audio Settings**.
2. Configure the parameters as needed.
3. Click **Save**.

## 6.3 ROI (Region of Interest)

ROI encoding allows the device to allocate more encoding resources to specific areas of interest.
This improves image quality in selected regions while reducing detail in less important areas.

**Steps:**

1. Go to **Setup Menu** → **Video** → **ROI**.

2. Check the **Enable** checkbox.
3. Select a **Stream Type**.
4. Select a **Region No.** and draw the ROI area.
5. Set the **Level** and enter the **Region Name**.
6. Click **Save**.
7. **Optional:** Select an unused region number and repeat the steps above to create multiple ROI areas.

## 6.4 Snapshot Settings

You can configure snapshot settings in this section. Snapshots are captured when events are triggered.

**Steps:**

1. Go to **Setup Menu → Video → Snapshot Settings**.
2. Select the desired **Resolution** and **Quality**.
3. Click **Save**.

## 6.5 OSD Settings

In this section, you can configure OSD (On-Screen Display) information such as device name, date/time, font, color, and text overlays displayed on the video stream.

**Steps:**

1. Go to **Setup Menu → Video → OSD Settings**.
2. Enter the **Channel Name**.
3. Enable or disable **Channel Title** and **Time Title** to control their display on screen.
4. **Optional:** Drag the OSD elements on the live view to adjust their position.
5. Click **Save**.

## 6.6 Image Superposition

This function allows you to upload an image overlay to be displayed on the video.

**Note**
This feature is only supported on certain device models.

**Before you start:**
Prepare an image in **BMP format (24-bit)**. The image size must not exceed **128 × 128 pixels**.

**Steps:**

1. Go to **Setup Menu → Video → Image Superposition**.
2. Click **Browse** to select the image.
3. Click **Upload**.
4. Enable the image overlay.

**Optional:**

- **Set Transparency:** Enable transparency and enter the RGB color value (R/G/B) to be made transparent.
- **Set Position:** Click and drag the uploaded image to the desired position on the screen.

6. Click **Save**.

# 7. Event and Alarm Configuration

This section introduces event configuration and how the device responds to triggered alarms.

**Note**
Event and alarm configurations may vary depending on the model. Refer to the actual web interface.

## 7.1 Motion Detection

This feature detects motion within a defined area and triggers configured actions.

**Steps:**

1. Go to **Setup Menu → Event → Basic Event → Motion Detection**.
2. Check the **Enable** checkbox.
3. Set the **Sensitivity**. Higher sensitivity increases the likelihood of triggering.
4. Set the **Detection Area** by dragging the mouse over the preview (selected areas are highlighted in red).
5. Configure the **Arming Schedule** for motion detection.

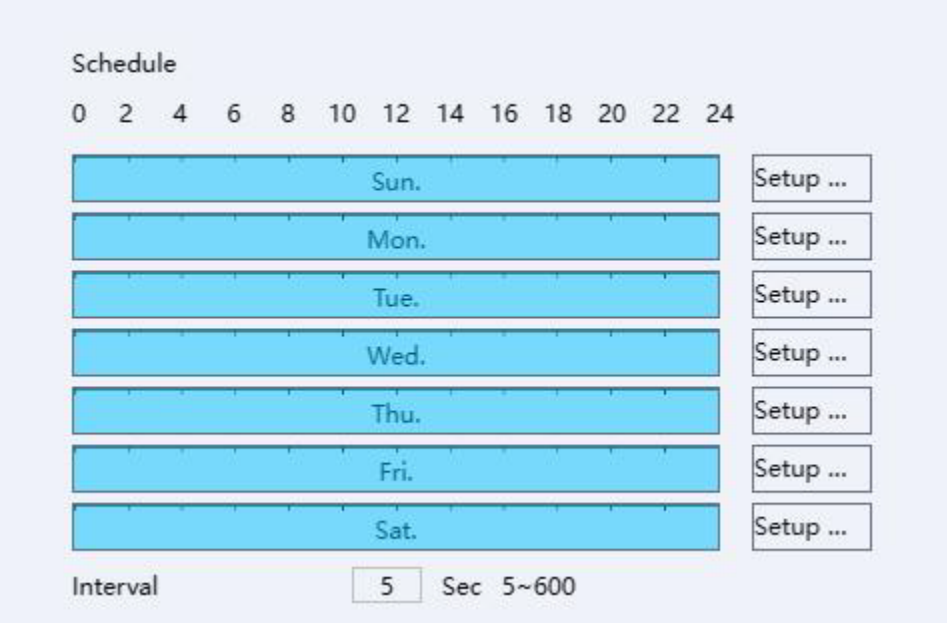



**Figure 7-1 Schedule**

A. Click **Setup** to define the detection schedule for each day.

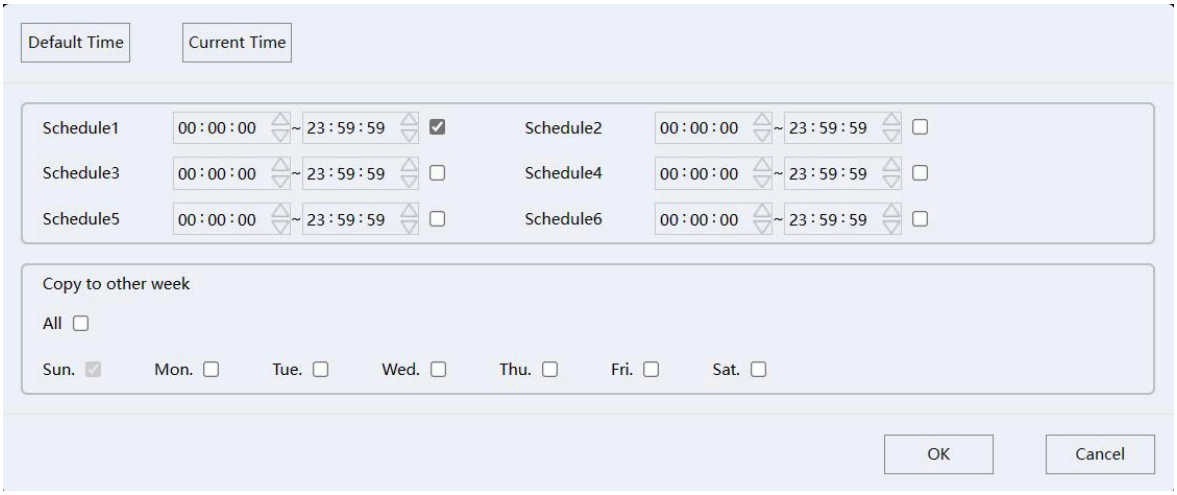



**Figure 7-2 Schedule Setup**

B. Set the **Interval time** (during this period, motion detection and alarms will be active).

6. To configure the actions triggered by an event, click **Actions**.

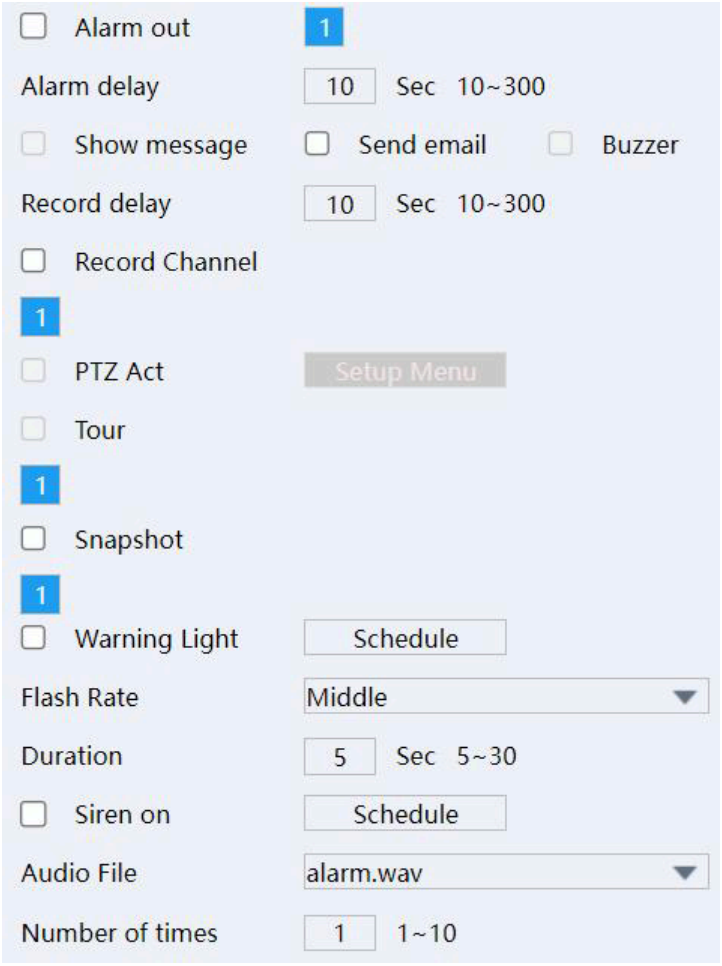



**Figure 7-3 Actions**

**Alarm Delay:** Duration of the alarm.

**Send Email:** When motion detection is triggered, the device sends emails to the configured recipients. For email settings, refer to **4.3.7 Email**.

**Record Channel:** When motion detection is triggered, the device starts recording on the selected channel.

**Record Delay:** The device continues recording for a set duration after the motion event ends.

**Snapshot:** When motion detection is triggered, the device captures snapshots of the video.

**Warning Light:** Supported only on active deterrence cameras. Used to configure red and blue flashing lights.

**Siren:** Supported only on active deterrence cameras. Used to configure alarm audio.

7. Click **Save**.

## 7.2 Video Tampering

When the configured area is covered or cannot be monitored normally, an alarm will be triggered and the device will perform the configured alarm actions.

**Steps:**

1. Go to **Setup Menu** → **Event** → **Basic Event** → **Video Tampering**.
2. Check the **Enable** checkbox.
3. Set the **Sensitivity**: A higher sensitivity increases the likelihood of triggering a tampering alarm.
4. Set the **Arming Schedule**. Click **Setup** to define the detection time for each day.
5. To configure the actions triggered after an event, click **Actions**:
    1. Configure **Alarm Output**, **Alarm Delay**, and **Send Email**.
       **Alarm Delay:** Duration of the alarm.
       **Send Email:** When tampering is detected, the device sends email notifications to configured recipients. Refer to **4.3.7 Email** for email settings.
       **Note:** The alarm output function is available only on devices that support alarm output.
    2. Configure **Record Delay** and **Record Channel**.
       **Record Channel:** When tampering is detected, the device starts recording on the selected channel.
       **Record Delay:** The device continues recording for a set duration after the tampering event ends.
    3. Configure **Snapshot**. When tampering is detected, the device captures snapshots of the video.
6. Click **Save**.

# 7.3 Alarm In/Out

## 7.3.1 Alarm Input

An alarm signal from an external device triggers the corresponding actions on this device.

**Before you start:**
Ensure that the external alarm device is properly connected and configured.

**Steps:**

1. Go to **Setup Menu** → **Event** → **Alarm** → **Alarm In**.
2. Check the **Enable** checkbox.
3. Set the **Type**: **Normally Closed** / **Normally Open**.
4. Set the **Arming Schedule**.
    2. Click **Setup** to define the detection time for each day.
    3. Set the **Interval Time** (during this period, the device will trigger alarms).
5. Configure the linkage actions. Click **Actions**:

    2. Configure **Alarm Output**, **Alarm Delay**, and **Send Email**.
       **Alarm Delay:** Duration of the alarm.
       **Send Email:** When an alarm input event is triggered, the device sends email notifications to configured recipients. Refer to **4.3.7 Email** for email settings.
6. **Buzzer:** Enables the buzzer when an alarm input is triggered.

    2. Configure **Record Delay** and **Record Channel**.
       **Record Channel:** When an alarm input event is triggered, the device starts recording on the selected channel.
       **Record Delay:** The device continues recording for a set duration after the alarm event ends.
    3. Configure **Snapshot**. When an alarm input event is triggered, the device captures snapshots of the video.
7. Click **Save**.

## 7.3.2 Alarm Output

If the device is connected to an alarm output device and the alarm output number is configured correctly, the device will send alarm signals to the connected output device when an alarm is triggered.

**Steps:**

1. Go to **Setup Menu** → **Event** → **Alarm** → **Alarm Output**.
2. Set the **Type**: **Schedule**, **Manual**, or **Stop**.
    1. **Schedule:** The alarm output is activated when an alarm is triggered during the configured schedule.
    2. **Manual:** The alarm output remains continuously active.
    3. **Stop:** The alarm output remains off.

**Note:** You can check the alarm output status via the status indicator.
When it is white, the alarm output is off; when it is red, the alarm output is active.

3. Click **Save**.

### 7.3.3 Notification Activation

1. **Arming:** When the system is armed, alarm linkage actions on the camera are enabled.
2. **Disarming:** When the system is disarmed, alarm linkage actions on the camera are disabled.
3. **Custom Disarming:** When custom disarming is selected, alarm linkage actions can be disabled once or according to a defined schedule.

## 7.4 Intelligent

### 7.4.1 Line Crossing Detection

This feature detects objects crossing a predefined virtual line. When triggered, the device can perform configured linkage actions.

**Steps:**

1. Go to **Setup Menu → Intelligent → AI Config → Line Crossing**.
2. Check the **Enable** checkbox.
   **Optional:** You can enable the **Human/Vehicle filter**, so that only human or vehicle targets trigger line crossing events.
3. Select the **warning area** to configure.
4. Click **Plot Area**. A virtual line will appear on the live image.
5. Click and drag the line to position it as needed on the live image.
6. Click the line. Two red squares will appear at each end. Drag either square to adjust the length and shape of the line.
7. Select the **Detection Direction**. Available options:
   - **A↔B:** Objects crossing the line in both directions will be detected and trigger alarms.
   - **A→B:** Only objects crossing from side A to side B will be detected.
   - **B→A:** Only objects crossing from side B to side A will be detected.

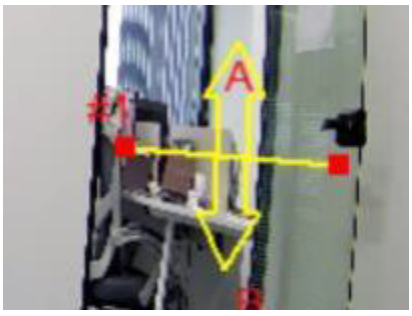



**Figure 7-4 Line Crossing**

8. Set the **Sensitivity**: Higher values increase detection sensitivity.
9. Configure the **Arming Schedule** and **Actions**. Refer to **7.1 Motion Detection** for details.
10. **Optional:** Enable **Dynamic Tracking** to activate dynamic tracking lines and smart rules.

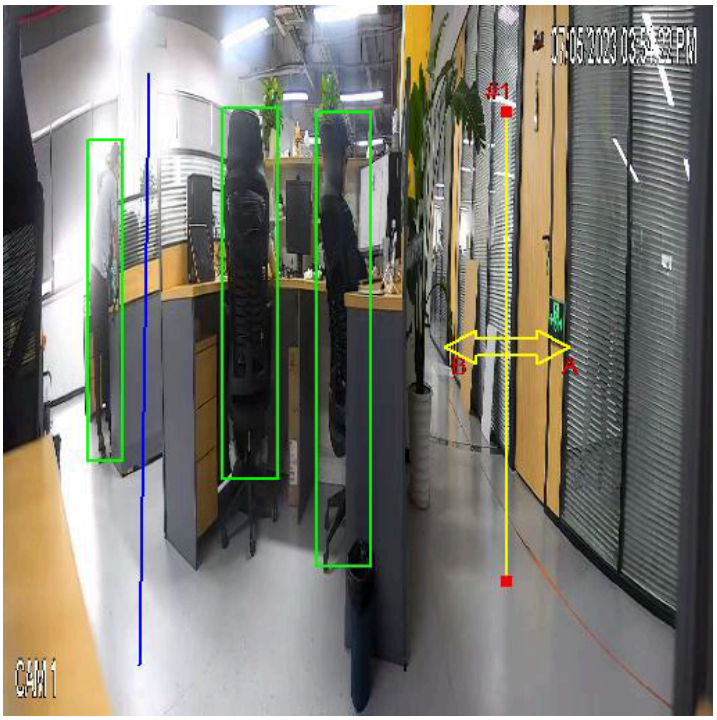



Figure 7-5 Enable Dynamic Tracking

11. Click **Save** to save and apply the settings.

### 7.4.2 Area Intrusion Detection

This feature detects objects entering or loitering within a predefined virtual area. When triggered, the device can perform configured linkage actions.

**Steps:**

1. Go to **Setup Menu → Intelligent → AI Config → Area Intrusion**.
2. Check the **Enable** checkbox.
   **Optional:** You can enable the **Human/Vehicle filter**, so that only human or vehicle targets trigger intrusion events.
3. Select the **warning area** to configure.
4. Draw the detection area:
    1. Click **Plot Area**. A virtual polygon will appear on the live image.
    2. Click and drag the shape to position it as needed.
    3. Click the shape. Red control points will appear at each corner. Drag them to adjust the shape and size of the area.

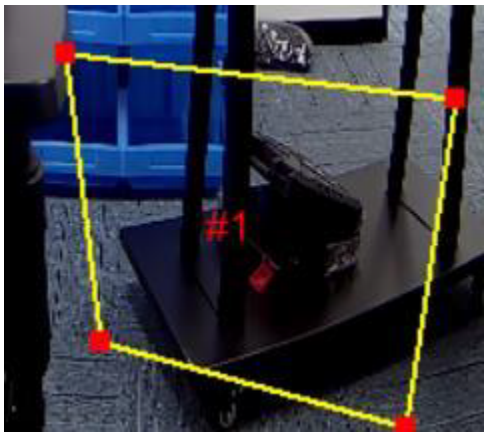



**Figure 7-6 Area Intrusion**

5. Set the **Time Threshold**.
   This defines how long an object must remain in the area before an alarm is triggered.
   For example, if set to 0, the alarm is triggered immediately when the object enters the area.
   The maximum value is 10 seconds.
6. Set the **Sensitivity**.
   Sensitivity determines how easily an object is detected as a target.
   Higher sensitivity detects smaller objects, while lower sensitivity focuses on larger objects.
7. Set the **Percent**.
   This defines how much of the defined area must be occupied by the target before triggering an alarm.
8. Configure the **Arming Schedule** and **Actions**. Refer to **7.1 Motion Detection** for details.
9. **Optional:** Enable **Dynamic Tracking** to activate dynamic tracking lines and smart rules.
10. Click **Save** to save and apply the settings.

### 7.4.3 Region Entrance Detection

This feature detects objects entering a predefined virtual area from outside. When triggered, the device can perform configured linkage actions.

**Steps:**

1. Go to **Setup Menu → Intelligent → AI Config → Region Entrance**.
2. Check the **Enable** checkbox.
   **Optional:** You can enable the **Human/Vehicle filter**, so that only human or vehicle targets trigger entrance events.
3. Select the **warning area** to configure.
4. Draw the detection area:
   1. Click **Plot Area**. A virtual polygon will appear on the live image.
   2. Click and drag the shape to position it as needed.
   3. Click the shape. Red control points will appear at each corner. Drag them to adjust the shape and size of the area.

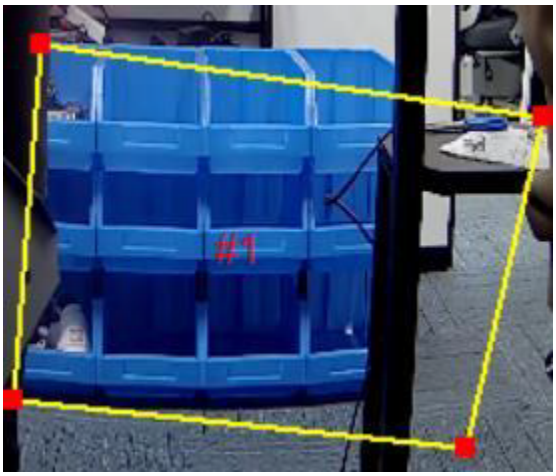



**Figure 7-7 Region Entrance**

5. Set the **Sensitivity**.
   Sensitivity determines how easily an object is detected as a target.
   Higher sensitivity detects smaller objects, while lower sensitivity focuses on larger objects.
6. Configure the **Arming Schedule** and **Actions**. Refer to **7.1 Motion Detection** for details.
7. **Optional:** Enable **Dynamic Tracking** to activate dynamic tracking lines and smart rules.
8. Click **Save** to save and apply the settings.

### 7.4.4 Region Exiting Detection

It is used to detect objects exiting from a pre-defined virtual region. When it occurs, the device can take linkage actions.

**Steps:**

1. Go to **Setup Menu** → **Intelligent** → **AI Config** → **Region Exiting**.
2. Check the checkbox of **Enable** to enable the function.

   **Optional:** You can select the Human/Car filter; the Area Intrusion will be triggered only by Human/Vehicle.

3. Select **Warning surfaces** you want to set.
4. Draw Area:
   1. Click the **Plot Area** button, and a virtual rectangle is displayed on the live image.
   2. Click-and-drag the rectangle, and you can locate it on the live image as desired.
   3. Click on the line, four 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.

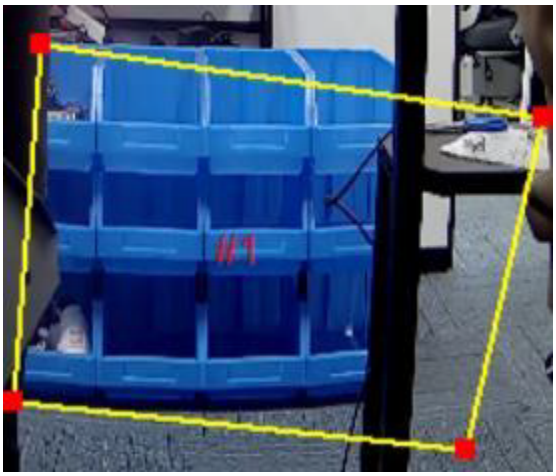


**Figure 7-8 Region Exiting**

5. Set the **Sensitivity**.
   It is used to set and control the size of the target object. The higher the sensitivity setting, the smaller the object exiting the area will be judged as the target object. The lower the sensitivity setting, the larger the object exiting the area will be judged as the target object.
6. Set the **Arming schedule** and **Actions**.
   Details refer to **7.1 Motion detection setting**.
7. Optional: Check the checkbox of **Dynamic Tracking** to enable the dynamic tracking lines and smart rules.
8. Click **Save** to save and finish the settings.

### 7.4.5 Blurred Detection

The blurred image caused by lens defocus can be detected. If it occurs, the device can take linkage actions.

**Steps:**

1. Go to **Setup Menu** → **Intelligent** → **AI Config** → **Blurred Detection**.
2. Check the checkbox of **Enable** to enable the function.
3. Select **Warning surfaces** you want to set.
4. Set the **Sensitivity**.
   Blurred Detection is easier to trigger with a higher sensitivity value.
5. Set the **Percent**.
   It indicates how much of the affected area is required to trigger the alarm; the percentage value is used as the input.
6. Set the **Arming schedule** and **Actions**.
   Please refer to **7.1 Motion detection setting** for details.
7. Click **Save** to save and finish the settings.

### 7.4.6 Scene Change Detection

Scene change detection detects changes in the surveillance scene. When it occurs, the device can take linkage actions.

**Steps:**

1. Go to **Setup Menu → Intelligent → AI Config → Scene Change**.
2. Check the checkbox of **Enable** to enable the function.
3. Set the **Sensitivity**.
   Scene Change Detection is easier to trigger with higher sensitivity.
4. Set the **Arming schedule** and **Actions**.
   Please refer to **7.1 Motion detection setting** for details.
5. Click **Save** to save and finish the settings.

### 7.4.7 Fast Moving Detection

This function is used to detect objects moving quickly within a defined area. When triggered, the device can take linkage actions.

**Steps:**

1. Go to **Setup Menu → Intelligent → AI Config → Fast Moving**.
2. Check the checkbox of **Enable** to enable the function.
3. Select **Warning surfaces** you want to set.
4. Draw Area:
   1. Click the **Plot Area** button, and a virtual rectangle is displayed on the live image.
   2. Click-and-drag the rectangle, and you can locate it on the live image as desired.
   3. Click on the line, four red squares are displayed on each end, and you can click-and-drag one of the red squares to define the shape and size of the area.
5. Set the **Sensitivity**.
   It is used to define the speed threshold of the moving object. A higher sensitivity means slower movements can trigger the alarm, while a lower sensitivity requires faster movement to trigger the alarm.
6. Set the **Arming schedule** and **Actions**.
   Please refer to **7.1 Motion detection setting** for details.
7. Click **Save** to save and finish the settings.

### 7.4.8 Loitering Detection

This function is used to detect objects lingering or wandering within a defined area. When triggered, the device can take linkage actions.

**Steps:**

1. Go to **Setup Menu → Intelligent → AI Config → Loitering Detection**.
2. Check the checkbox of **Enable** to enable the function.
3. Select **Warning surfaces** you want to set.
4. Draw Area:
   - Click the **Plot Area** button, and a virtual rectangle is displayed on the live image.
   - Click-and-drag the rectangle, and you can locate it on the live image as desired.
   - Click on the area, four red squares are displayed on each corner, and you can click-and-drag them to adjust the shape and size.
5. Configure the parameters:

- **Sensitivity:**
  Defines the size of the target object. A higher sensitivity detects smaller objects, while a lower sensitivity detects larger objects.
- **Time Threshold:**
  Defines how long an object must remain in the area before triggering the alarm. For example, if set to 0s, the alarm is triggered immediately when loitering behavior is detected.
- **Offset:**
  Determines loitering based on the displacement of the object. If the movement distance exceeds a defined threshold (based on the difference between the first and current frame), loitering is detected.
- **Weight:**
  Determines loitering based on the number of direction changes (turns) of the object within the area. The default threshold is 3 turns.
- **Journey:**
  Determines loitering based on the total distance traveled by the object within the area. The threshold is based on the longest diagonal length of the defined region.

6. Set the **Arming schedule** and **Actions**.
   Please refer to **7.1 Motion detection setting** for details.
7. Click **Save** to save and finish the settings.

### 7.4.9 People Gathering Detection

This function is used to detect whether people are gathering within a defined area. When triggered, the device can take linkage actions.

**Steps:**

1. Go to **Setup Menu → Intelligent → AI Config → People Gathering**.
2. Check the checkbox of **Enable** to enable the function.
3. Select **Warning surfaces** you want to set.
4. Draw Area:
   - Click the **Plot Area** button, and a virtual rectangle is displayed on the live image.
   - Click-and-drag the rectangle, and you can locate it on the live image as desired.
   - Click on the area, four red squares are displayed on each corner, and you can click-and-drag them to adjust the shape and size.
5. Configure the parameters:
   - **Sensitivity:**
     Defines the detection sensitivity for crowd gathering. Higher sensitivity makes it easier to detect gatherings.
   - **Percent:**
     Defines the density threshold of objects (people) in the area. A higher value requires a higher density of detected objects to trigger the alarm, while a lower value triggers the alarm with fewer detected objects.
6. Set the **Arming schedule** and **Actions**.
   Please refer to **7.1 Motion detection setting** for details.
7. Click **Save** to save and finish the settings.

## 7.4.10 Unattended Object Detection

This function is used to detect objects left unattended within a pre-defined region. When an object remains in the area for a specified period, the device can trigger linkage actions.

**Steps:**

1. Go to **Setup Menu → Intelligent → AI Config → Unattended Object**.
2. Check the checkbox of **Enable** to enable the function.
3. Draw Area:
    - Click the **Plot Area** button, and a virtual rectangle is displayed on the live image.
    - Click-and-drag the rectangle, and you can locate it on the live image as desired.
    - Click on the area, four red squares are displayed on each corner, and you can click-and-drag them to adjust the shape and size.
4. Configure the parameters:
    - **Sensitivity:**
      Defines the detection sensitivity for unattended objects. Higher sensitivity detects smaller changes, while lower sensitivity detects larger changes.
    - **Time Threshold:**
      Defines how long an object must remain in the area before triggering the alarm. For example, if set to 5 seconds, the alarm is triggered after the object remains for 5 seconds.
      **Note:** It may take up to 10 seconds to determine whether an object is unattended.
5. Set the **Arming schedule** and **Actions**.
   Please refer to **7.1 Motion detection setting** for details.
6. Click **Save** to save and finish the settings.

## 7.4.11 Object Missing Detection

This function is used to detect whether objects are removed from a pre-defined detection region (e.g., items on display). When triggered, the device can take linkage actions to help prevent property loss.

**Steps:**

1. Go to **Setup Menu → Intelligent → AI Config → Object Missing**.
2. Check the checkbox of **Enable** to enable the function.
3. Draw Area:
    - Click the **Plot Area** button, and a virtual rectangle is displayed on the live image.
    - Click-and-drag the rectangle, and you can locate it on the live image as desired.
    - Click on the area, four red squares are displayed on each corner, and you can click-and-drag them to adjust the shape and size.
4. Configure the parameters:
    - **Sensitivity:**
      Defines how sensitive the system is to detecting missing objects. Higher sensitivity detects smaller changes in the scene, while lower sensitivity requires more significant changes to trigger detection.
    - **Time Threshold:**
      Defines how long an object must be missing before triggering the alarm. For example, if set to 5 seconds, the alarm is triggered after the object is absent for 5 seconds.
      **Note:** It may take up to 10 seconds to confirm that an object is missing.

5. Set the **Arming schedule** and **Actions**.
   Please refer to **7.1 Motion detection setting** for details.
6. Click **Save** to save and finish the settings.

### 7.4.12 Parking Detection

This function is used to detect whether a vehicle is parked within a pre-defined area. When triggered, the device can take linkage actions.

**Steps:**

1. Go to **Setup Menu → Intelligent → AI Config → Parking Detection**.
2. Check the checkbox of **Enable** to enable the function.
3. Draw Area:
   - Click the **Plot Area** button, and a virtual rectangle is displayed on the live image.
   - Click-and-drag the rectangle, and you can position it on the live image as desired.
   - Click on the area, four red squares are displayed on each corner, and you can click-and-drag them to adjust the shape and size.
4. Configure the parameters:
   - **Sensitivity:**
     Defines the detection sensitivity for parked vehicles. A higher sensitivity detects smaller or slight changes, while a lower sensitivity requires more significant presence to trigger detection.
   - **Time Threshold:**
     Defines how long a vehicle must remain in the area before triggering the alarm. For example, if set to 5 seconds, the alarm is triggered after the vehicle stays in the area for 5 seconds.
5. Set the **Arming schedule** and **Actions**.
   Please refer to **7.1 Motion detection setting** for details.
6. Click **Save** to save and finish the settings.

### 7.4.13 Audio Exception Detection

This function detects abnormal audio events in the device's environment, such as sudden loud sounds or sharp drops in sound intensity. When triggered, the device can take linkage actions.

**Steps:**

1. Go to **Setup Menu → Intelligent → AI Config → Audio Exception Detection**.
2. Enable the desired detection types:
   - **Abnormal audio input**
   - **Strong sound intensity**
   - **Sound intensity dropped sharply**
3. Set the **Sensitivity**:
   A higher sensitivity increases the likelihood of detecting abnormal audio events.
4. Monitor the **real-time volume level** on the interface:


**Figure 7-9 Real-time Volume**

5. Set the **Arming schedule** and **Actions**.
   Please refer to **7.1 Motion detection setting** for details.
6. Click **Save** to save and finish the settings.

### 7.4.14 Face Detection

This function detects human faces within a defined detection area and triggers linkage actions when a face is identified.

**Note:**
Only certain device models support this function.

**Configure Face Detection**

**Steps:**

1. Go to **Setup Menu → Event → Face Detection → Base**.
2. Check the checkbox of **Enable** to activate the function.
3. Draw Area:
   1. Click the **Plot Area** button, and a virtual rectangle is displayed on the live image.
   2. Click-and-drag the rectangle to position it as desired.
   3. Click on the area; four red squares will appear at the corners, allowing you to adjust the shape and size.
4. Set the **Sensitivity**:
   A higher sensitivity increases the likelihood of detecting faces, including smaller or less distinct ones.
5. Set the **Arming schedule** and **Actions**.
   Please refer to **7.1 Motion detection setting** for details.
6. Click **Save** to save and finish the settings.

**Overlay and Capture Settings**

**Steps:**

1. Go to **Setup Menu → Event → Face Detection → Overlay and Capture**.
2. Configure the following parameters:
   - **Capture configuration:**
     Define the naming format for captured face images. You can use the default name or apply a custom prefix (1–15 characters).

- **Monitoring point parameters:**
  Set the device ID and monitoring point information.
- **OSD statistics:**
  Enable or disable on-screen display statistics (**Open/Stop**).

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

# 8. Recording to Local Storage / NAS

This chapter introduces the configuration and management of recording functions.

**Note:**
Only device models that support Local Storage (Micro-SD card) or NAS features can use these functions.

## 8.1 Record and Snapshot

You can configure recording and snapshot behaviors in this section.

### 8.1.1 Record Setting

**Steps:**

1. Go to **Setup Menu → Recording Settings → Record and Snap → Record → Record Schedule**.
2. Enable recording and select the stream type:
   - **Main stream**
   - **Sub stream**
3. Configure recording parameters:
   - **Pack Duration:**
     Defines the length of each recorded video file segment.
   - **Pre-Record:**
     Defines how long recording starts before an event occurs (0–30 seconds).
4. Set the **Record Control mode**:
   - **Schedule:** Recording follows the configured Record Plan.
   - **Manual:** Continuous recording (24/7).
   - **Stop:** Recording is disabled.
5. Configure the **Record Plan**:

   - Select the recording type:
     - **Normal** (continuous recording)
     - **MD** (motion detection)
     - **Alarm**
   - Click **Set** to configure the recording schedule for each day, then click **OK**.

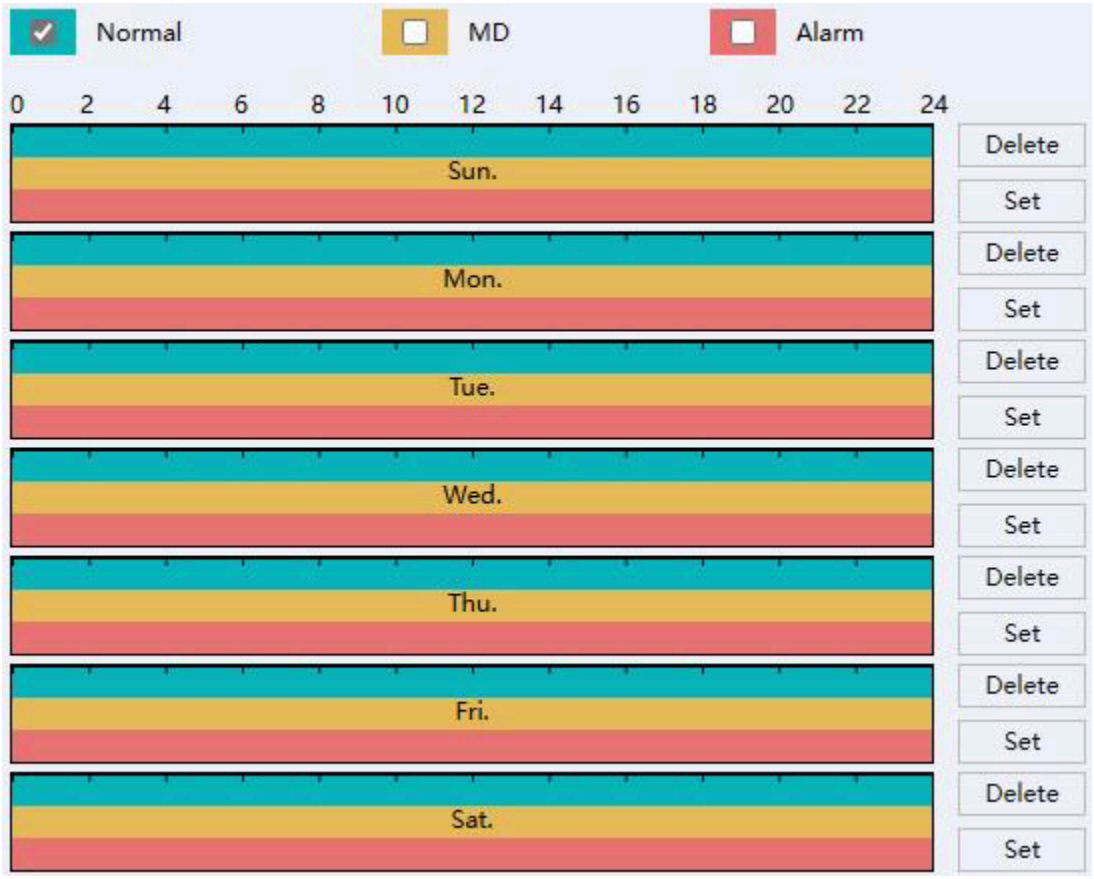



**Figure 8-1 Set Record Plan**

6. Set the **Record Control mode** (if needed):
    - **Schedule:** Camera follows the Record Plan to record.
    - **Manual:** Camera records continuously.
    - **Stop:** Camera stops recording.

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

## 8.1.2 Snapshot Setting

This section allows you to configure snapshot features.

**Interval Snapshot**

The camera captures snapshots at a defined time interval.

**Steps:**

1. Go to **Setup Menu → Recording Settings → Record and Snap → Snapshot Setting → Time Picture**.
2. Check the checkbox of **Enable** to activate interval snapshots.
3. Set the **Interval** time.
4. Set the **Schedule**.
5. Click **Save** to save and finish the settings.

**Alarm Snapshot**

The camera captures snapshots when an alarm signal is triggered.

**Steps:**

1. Go to **Setup Menu** → **Recording Settings** → **Record and Snap** → **Snapshot Setting** → **Alarm Snapshot**.
2. Check the checkbox of **Enable** to activate alarm-triggered snapshots.
3. Set the **Interval** time.
4. Set the **Snap Count** (number of snapshots per event).
5. Click **Save** to save and finish the settings.

**Event-Triggered Snapshot**

The camera captures snapshots when an event is triggered.

**Steps:**

1. Go to **Setup Menu** → **Recording Settings** → **Record and Snap** → **Snapshot Setting** → **Event-Triggered Snapshot**.
2. Check the checkbox of **Enable** to activate event-triggered snapshots.
3. Set the **Interval** time.
4. Set the **Snap Count** (number of snapshots per event).
5. Click **Save** to save and finish the settings.

# 8.2 Storage Manager

## 8.2.1 Local Storage Management (Micro-SD Card)

After inserting the Micro-SD card correctly, you can access and manage it as a local storage device.

Go to **Setup Menu** → **Recording Settings** → **Storage Manager**.

**Format / Delete Micro-SD Card**

This function allows you to format or delete data from the Micro-SD card.

**Steps:**

1. Select the storage device you want to manage.
2. Click **Format** or **Delete**.

**Storage Rule When Full**

Configure how the device behaves when the storage is full.

**Steps:**

1. Select the **HDD Full** option from the drop-down menu:
    - **Overwrite:** When storage is full, the camera overwrites the oldest files.
    - **Stop:** When storage is full, the camera stops recording.
2. Click **Save** to save and finish the settings.

**Quota Storage for Recording and Snapshot**

This function allows you to allocate storage capacity between video recordings and snapshots.

**Steps:**

1. Set the storage allocation:

    - **Record Quota (%)**
    - **Picture Quota (%)**

The device will allocate storage capacity according to these values.

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

## 8.2.2 Connect to NAS

This function allows the device to store recordings and snapshot files on a NAS (Network Attached Storage).

**Before you start:**
Ensure that the NAS service is available and accessible within the same network.

**Steps:**

1. Go to Setup Menu → Recording Settings → Storage Manager → NAS.

| Disk No. | Type | Server address | File path | Space(GB) |
|---|---|---|---|---|
| 1 | NAS | | | 2 |
| 2 | NAS | | | 2 |
| 3 | NAS | | | 2 |
| 4 | NAS | | | 2 |

**Figure 8-2 NAS**

2. Double-click a NAS entry to open its **Config** settings.
3. Configure the NAS parameters:
    - **Server Address**
    - **File Path**
    - **Mount Type** (e.g., NFS)
    - **Space (GB)**

- *(Optional)* Username and Password if required

4. Click **Test** to verify the connection:

   - If successful, click **OK**.
   - If failed, check the configuration parameters and try again.

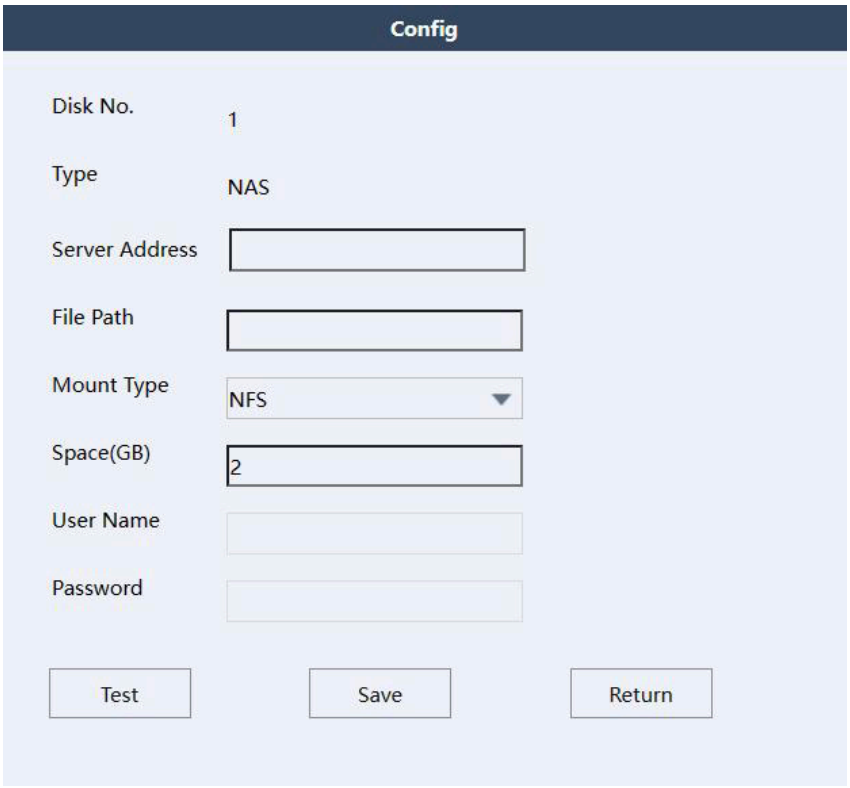



Figure 8-3 Config

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

# 9. Maintenance

## 9.1 Reboot Device

You can reboot the device via the web interface. The device also supports automatic reboot based on a configured schedule.

**Manual Reboot via Web Interface**

**Steps:**

1. Go to **Setup Menu** → **Maintain** → **Auto Reboot**.
2. Click **Reboot**, then click **OK** to confirm.
3. The device will restart, and you will be redirected to the login page.

**Scheduled (Auto) Reboot**

**Steps:**

1. Go to **Setup Menu** → **Maintain** → **Auto Reboot**.
2. Set the desired reboot time.
3. Click **Save** to apply the settings.

## 9.2 Restore and Default Settings

Restore and Default allows the device parameters to be reset to their default values.

### Restore Default Settings

**Steps:**

1. Go to **Setup Menu** → **Maintenance** → **Default Settings**.
2. Select the type of settings you want to restore.
3. Click **Execute** to apply the changes.

**Restore Factory Settings (via Interface)**

**Steps:**

1. Go to **Setup Menu** → **Maintenance** → **Default Settings**.
2. Click **Restore Factory**, then click **Execute** to reset all settings to default.

**Note**
Use this function with caution. All parameters will be reset to factory default settings.

**Restore Factory Settings via RESET Button**

This function allows restoring factory settings using the physical reset button on the camera.

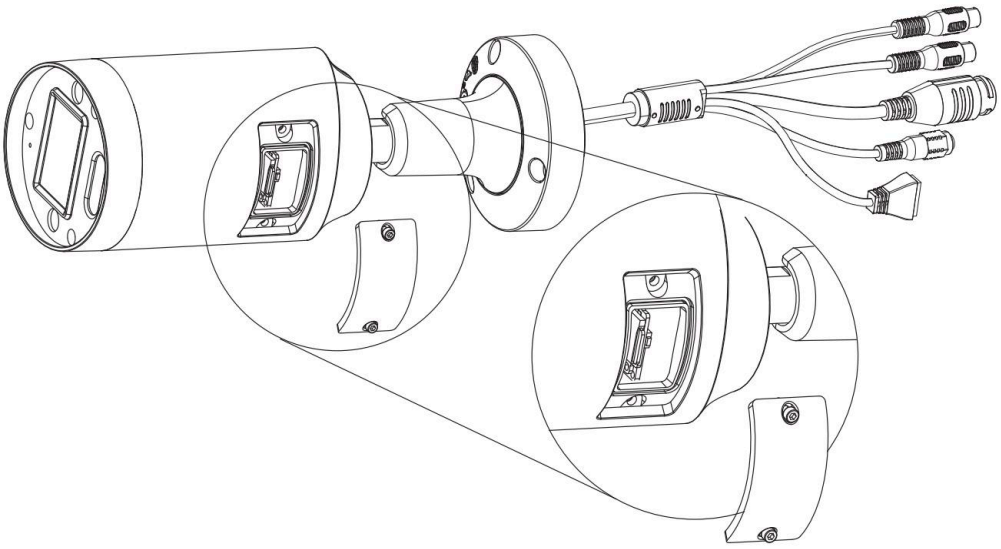
**Steps:**

1. Remove the cover to locate the reset button (refer to the illustrations below).
2. Power on the device, then press and hold the **RESET** button for about **10 seconds**.
3. The device will reboot and restore all settings to factory default.

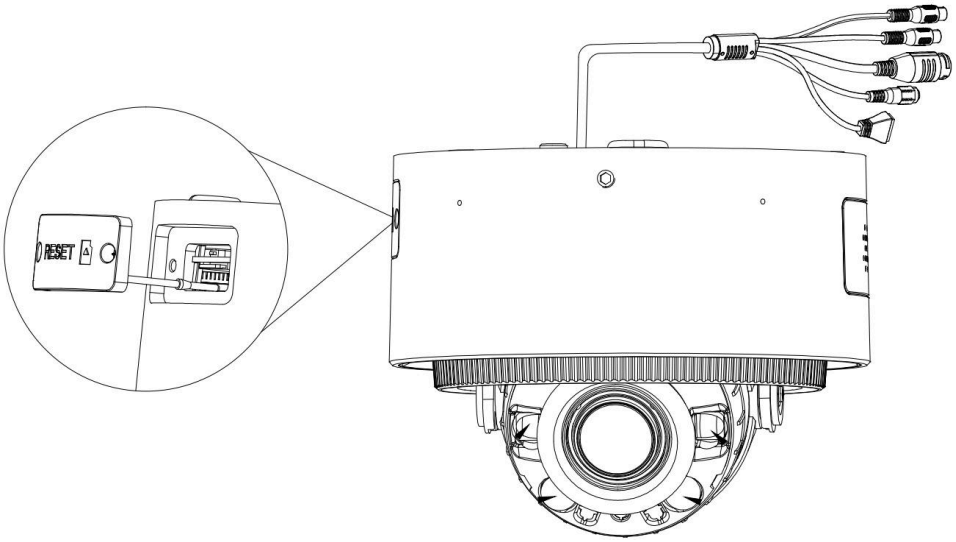
---

**Reset Button Location (Examples)**

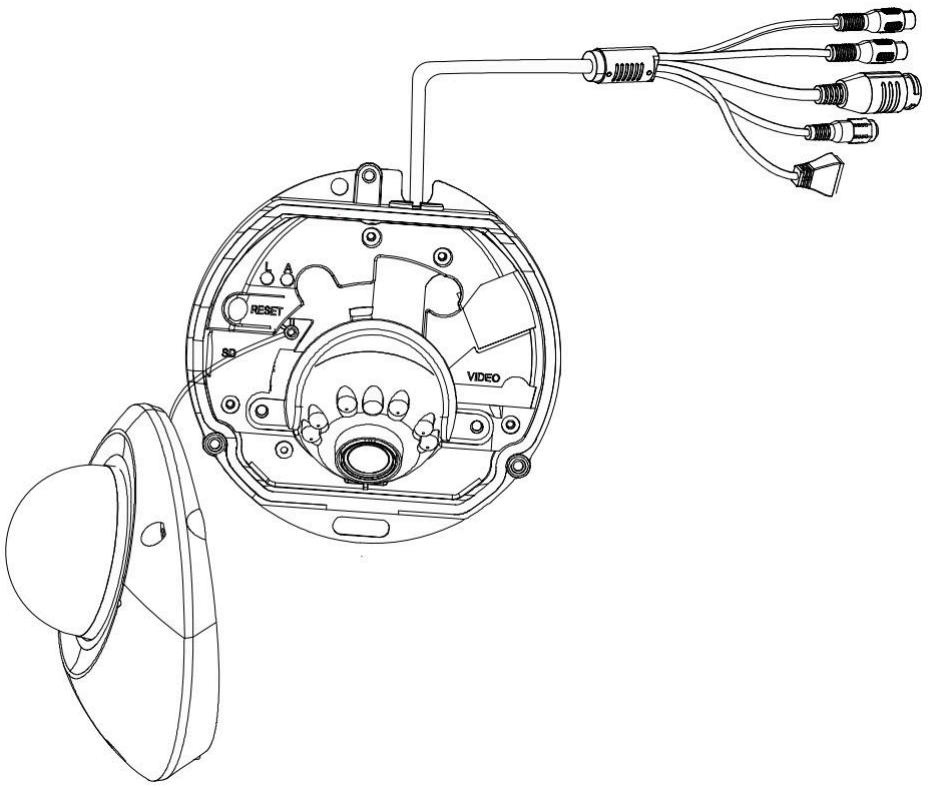
- Bullet Camera



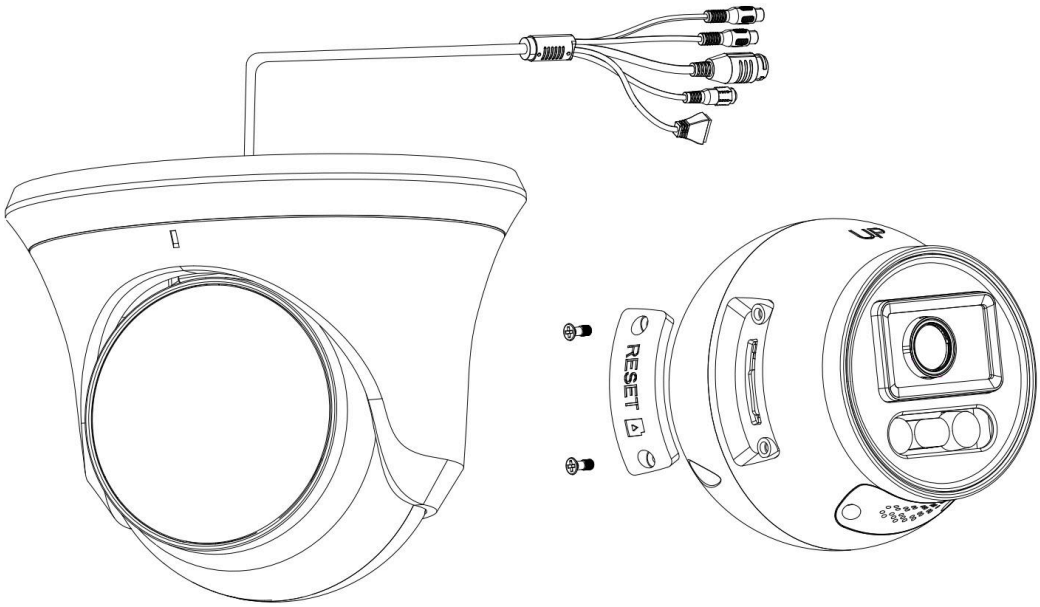
- Dome Camera



- Mini Dome Camera




- Turret Camera




**Additional Notes:**

Images are for reference only. Actual products may vary. Default credentials:

**Username:** admin - **Password:** 123456

## 9.3 Configuration Export / Import

This feature allows you to quickly apply the same configuration to multiple devices.

**Steps:**

1. Go to **Setup Menu** → **Maintenance** → **Export / Import**.
2. Click **Export Config**, then click **Execute**, and choose the folder where you want to save the configuration file.
3. Click **Import Config**, then click **Execute**, and select the configuration file you want to import.

## 9.4 Device Upgrade

**Before You Start**

Make sure you have the correct upgrade package for your device.

**Caution:**
Do **NOT** disconnect the power during the upgrade process. The device will reboot automatically after the upgrade is completed.

**Steps:**

1. Go to **Setup Menu** → **Maintenance** → **Upgrade**.
2. Click **Select Upgrade File** and choose the upgrade package.
3. Click **Upgrade** to start the process.

## 9.5 Log Search and Management

The log records device operations and helps identify and troubleshoot issues.

**Steps:**

1. Go to **Setup Menu** → **Maintenance** → **Log**.
2. Set the **Type**, **Start Time**, and **End Time**.
3. Click **Search**.
   → The matching logs will be displayed in the list.
4. (Optional) Click **Backup** to save the log files to your computer.

# 10. Playback and Video Download

This chapter explains how to use playback functions and download videos from local storage.

**Before You Start**

Make sure:

- A **Micro-SD card is inserted**
- A valid **recording schedule is configured**

## 10.1 Playback Recorded Video

**Steps:**

1. Go to **Playback**.
2. Select the date you want to search for recordings.
   → Dates highlighted in black indicate available recordings.
   → The device will search for video files on the selected date.
3. Select the type of recording you want to play:
   - **All Record**
   - **Standard**
   - **Event**

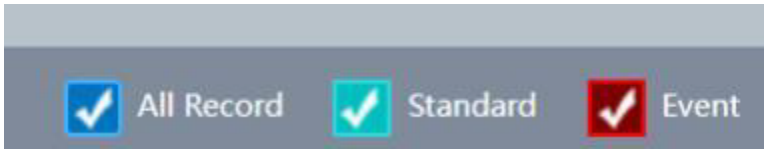



**Figure 10-1: Select recording type**

4. Click ▸ **(Play)** to start playback, or click directly on the timeline.
5. Click the switch icon  to open the video list page and access additional controls.

| | |
|---|---|
|  Stop playback |  Slow playback (×1/2, ×1/4, ×1/8) |
|  Pause playback |  Fast playback (×2, ×4, ×8, ×16) |
|  Play frame by frame |  Capture current frame |
|  Enable/Disable audio |  Open video file list |
|  Navigate or adjust timeline |  Click to access the record file download list |

# 10.2 Download Video Files

**Steps:**

1. Go to **Playback**.
2. Click ⬇ **(Download)** to open the download page.
3. Select the **Type** (**Record / Picture**) you want to download.
4. Set the **Start Time** and **End Time**, then click **Search**.
   → The list of available video/picture files will be displayed.
5. Select the file(s) you want to download.
6. Choose the file format (**DAV** or **AVI**).
7. Click **Download** to start the process.

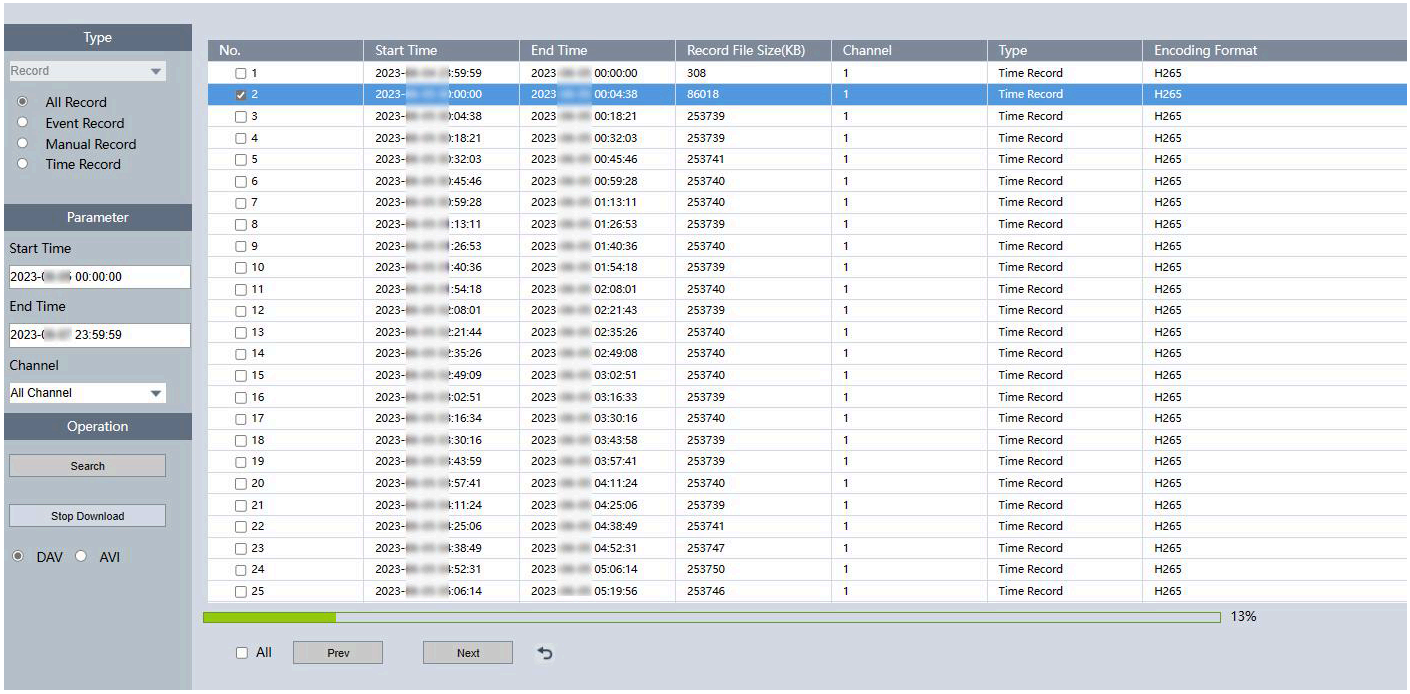



**Figure 10-2: Download interface**

**Note:**

- The selected file(s) will be downloaded and saved to your computer.
- To locate the files, check the configured save path (see **4.1 Local Storage**).

# Legal Information



## About This Manual

This manual provides instructions for the installation, configuration, operation, and maintenance of the product.

All images, diagrams, and illustrations in this manual are provided for reference purposes only and may differ from the actual product. The information contained herein is subject to change without prior notice due to firmware updates or product improvements. For the latest version of this manual, please visit the official Inaxsys website.

This manual is intended for use by qualified professionals. Installation and servicing should be performed by trained personnel only.

## Trademarks

Legend NX and all related trademarks, logos, and brand names are the property of **Inaxsys Security Systems Inc.** and may be registered in applicable jurisdictions.

## Disclaimer

To the maximum extent permitted by applicable law, this manual and the product described herein, including all hardware, software, and firmware, are provided **“as is”** and **“with all faults.”**

Inaxsys makes no warranties, express or implied, including but not limited to warranties of merchantability, fitness for a particular purpose, or satisfactory quality. Use of the product is at your own risk.

In no event shall Inaxsys be liable for any indirect, incidental, special, or consequential damages, including but not limited to:

- loss of business profits
- business interruption
- loss or corruption of data
- system failure
- loss of documentation

whether arising from breach of contract, tort (including negligence), product liability, or otherwise, even if Inaxsys has been advised of the possibility of such damages.

You acknowledge that internet-based products and systems may be subject to inherent security risks. Inaxsys shall not be held responsible for abnormal operation, privacy breaches, or damages resulting from cyber-attacks, hacking, viruses, or other network-related threats. However, Inaxsys will provide reasonable technical support where applicable.

You agree to use this product in compliance with all applicable laws and regulations. You are solely responsible for ensuring that your use does not infringe upon the rights of third parties, including but not limited to intellectual property rights, privacy rights, and data protection regulations.

This product must not be used for any prohibited purposes, including but not limited to:

- development or production of weapons of mass destruction
- chemical or biological weapons activities
- unsafe nuclear activities or nuclear fuel cycle misuse
- activities that violate human rights

In the event of any conflict between this manual and applicable law, the applicable law shall prevail.

# FCC Information

Please note that any changes or modifications not expressly approved by the party responsible for compliance may void the user's authority to operate this equipment.

# FCC Compliance

This equipment has been tested and found to comply with the limits for a **Class A digital device**, pursuant to **Part 15 of the FCC Rules**. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

# FCC Conditions

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

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

## Safety Instructions

- Proper configuration of all passwords and security settings is the responsibility of the installer and/or end user.
- In the use of this product, you must comply with all applicable electrical safety regulations for your country and region.
- Firmly connect the power plug to the outlet. Do not connect multiple devices to a single power adapter.
  Always power off the device before connecting or disconnecting accessories and peripherals.
- **Danger:** Shock hazard. Disconnect all power sources before performing maintenance.
- The equipment must be connected to a properly grounded (earthed) mains outlet.
- The socket outlet should be installed near the equipment and remain easily accessible.
- ⚡ Indicates hazardous live voltage. External wiring connected to terminals must be installed by a qualified person.
- **Warning:** Do not install the equipment in an unstable location. The device may fall, causing serious injury or death.
- The input voltage must comply with **SELV (Safety Extra Low Voltage)** and **LPS (Limited Power Source)** requirements in accordance with **IEC 62368**.
- High leakage current. Ensure proper grounding before connecting to the power supply.
- If smoke, unusual odor, or abnormal noise is detected, immediately power off the device, unplug it, and contact technical support.
- For optimal performance, use the device with a UPS (Uninterruptible Power Supply) and manufacturer-recommended hard drives.
- This product contains a coin/button cell battery. If swallowed, it can cause severe internal burns within two hours and may result in death.
- This equipment is not suitable for use in locations where children are likely to be present.
- Risk of explosion if the battery is replaced with an incorrect type.
- Improper battery replacement may disable safety protections (especially for certain lithium battery types).
- Do not dispose of the battery in a fire or a hot oven. Do not crush, puncture, or cut the battery, as this may result in explosion.
- Do not expose the battery to extremely high temperatures, which may result in explosion or leakage of flammable substances.
- Do not expose the battery to extremely low air pressure, which may result in explosion or leakage of flammable substances.
- Dispose of used batteries in accordance with local regulations.
- Keep body parts away from moving components such as fan blades and motors. Disconnect the power source before servicing.

## Preventive and Safety Guidelines

Before installing and operating this device, please review the following guidelines:

- This device is designed for **indoor use only**. Install it in a well-ventilated, dust-free environment away from liquids.
- Ensure the recorder is securely mounted on a rack or stable surface. Dropping or subjecting the unit to strong impacts may damage internal components.

- Do not expose the equipment to dripping or splashing liquids. Do not place objects filled with liquids (such as vases) on top of the device.
- Do not place open flame sources (such as lit candles) on or near the equipment.
- Do not obstruct ventilation openings. Avoid covering the device with materials such as newspapers, cloths, or curtains.
  Do not place the device on soft surfaces such as beds, sofas, or rugs that may block airflow.
- Maintain a minimum clearance of **200 mm (7.87 inches)** around the device to ensure proper ventilation.
- For applicable models, ensure correct wiring of terminals when connecting to an AC mains power supply.
- Certain models may be designed or configured for connection to an IT power distribution system. Verify compatibility before installation.
- The battery symbol indicates the battery holder and the correct polarity/positioning of the cell(s).
- The “+” and “–” symbols indicate the positive and negative terminals for direct current (DC) connections.
- Use only power supplies specified in this manual or provided by Inaxsys.
- The USB port is intended for connecting a mouse, keyboard, USB flash drive, or Wi-Fi dongle only.
- Avoid contact with sharp edges or corners of the equipment.