MyEye

Bullet Lite
Dome Lite

IP Smart Bullet Camera
IP Smart Dome Camera

EN - Instructions and warnings for installation and use

v0.1

CONTENT

1 - IMPORTANT SAFEGUARDS AND WARNINGS **4**
1.1 - Privacy protection notice 4
1.2 - About the manual 4
1.3 - Transportation and storage requirements 4
1.4 - Installation requirements 4
1.5 - Operation requirements 4
2 - DEVICE DESCRIPTION **5**
3 - CONFIGURATION FLOW **6**
4 - DEVICE INITIALIZATION **7**
5 - LOGIN **8**
5.1 - Device login 8
5.2 - Resetting password 8
6 - LIVE **10**
7 - PLAYBACK **11**
7.1 - Playback interface 11
7.2 - Playing back and downloading video or snapshot 11
8 - CAMERA **12**
8.1 - Conditions 12
8.1.1 - Picture 12
8.1.2 - Exposure 13
8.1.3 - Backlight 13
8.1.4 - WB 14
8.1.5 - Day/Night 14
8.1.6 - Illuminator 15
8.1.7 - Profile Management 15
8.2 - Video setting 16
8.2.1 - Video 16
8.2.2 - Snapshot 17
8.2.3 - Privacy Masking 17
8.2.4 - Channel Title 18
8.2.5 - Time Title 18
8.2.6 - ROI 18
8.3 - Audio 19
9 - NETWORK **20**
9.1 - TCP/IP 20
9.2 - Port 20
9.3 - Multicast 21
9.4 - WiFi 22
9.5 - Platform Access 22
9.5.1 - P2P 22
9.5.2 - RTMP 23
10 - EVENT **24**
10.1 - Video Detection 24
10.1.1 - Motion Detection 24
10.1.2 - Video Tampering 25
10.2 - Smart Motion Detection 25
10.3 - Audio Detection 26
10.4 - Abnormality 26
10.4.1 - SD Card 26
10.4.2 - Network 27
10.4.3 - Illegal Access 27
10.4.4 - Security Exception 27
11 - STORAGE **28**
11.1 - Schedule 28
11.1.1 - Record 28
11.1.2 - Snapshot 28
11.1.3 - Holiday Schedule 28
11.2 - Destination 29
11.2.1 - Path 29
11.2.2 - Local 29

11.3 - Record Control 29
12 - SYSTEM **30**
12.1 - General 30
12.2 - Date & Time 30
12.3 - Account 31
12.3.1 - User 31
12.3.2 - User Group 32
12.3.3 - ONVIF User 33
13 - SAFETY **34**
13.1 - IP Filter 34
13.2 - System Service 34
13.3 - HTTPS 35
14 - DEFAULT **38**
15 - IMPORT/EXPORT **39**
15.1 - Import 39
15.2 - Export 39
16 - AUTO MAINTAIN **40**
17 - UPGRADE **41**
18 - INFORMATION **42**
18.1 - Version 42
18.2 - Log 42
18.3 - Remote Log 43
18.4 - Online User 43
18.5 - Legal Info 43
19 - ALARM **44**
20 - CYBERSECURITY RECOMMENDATIONS **45**
21 - REGULATIONS **46**

1 IMPORTANT SAFEGUARDS AND WARNINGS

1.1 - Privacy protection notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

1.2 - About the manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We aren't liable for any loss caused by the operations that don't comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description. If there is any doubt or dispute, please see our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

1.3 - Transportation and storage requirements

- Transport and store the device under allowed humidity and temperature conditions.
- Pack the device with packaging provided by its manufacturer or packaging of the samequality before transporting it.
- Don't expose to sunlight or near heat sources.
- Keep the device away from dampness, dust, soot, strong electromagnetic radiation, unstable illumination, extreme heat or cold.
- Install the device on a stable surface to prevent it from falling.
- Don't place heavy stress on the device, violently vibrate or immerse it in liquid.
- Operate the device within the rated range of power input and output.

1.4 - Installation requirements

- Use the accessories suggested by the manufacturer. Installation and maintenance needs to be performed by qualified professionals.
- Strictly comply with the local electric safety standards. Make sure the voltage is stable and meets the power supply requirements of the device.
- Don't connect the device to two or more kinds of power supplies, unless otherwisespecified, to avoid damage to the device.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and beno higher than PS2. Please note that the power supply requirements are subject to the device label.
- The device need to be installed in a location that only professionals can access to avoid the risk of non-professionals becoming injured from accessing the area while the device is working. Professionals need to have full knowledge of the safeguards and warnings of using the device.
- An emergency disconnect device needs to be available during installation and wiring at a accessible location for emergency power cut-off.
- We recommend you to use the device with a lightning protection device for stronger protection against lightning. For outdoor scenarios, strictly comply with the lightning protection regulations.
- Ground the function earthing portion of the device ⏚ to improve its reliability (certain models aren't equipped with earthing holes). The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- There might be a risk of electrostatic discharge on the dome cover. Power off the device when installing the cover after the camera finishes adjustment. Don't directly touch the cover and make sure the cover isn't exposed to other equipment or human bodies

1.5 - Operation requirements

- Don't open the cover while the device is powered on.
- Don't touch the heat dissipation component of the device to avoid the risk of getting burnt.
- Use the device under allowed humidity and temperature conditions.
- Don't aim the device at strong light sources, such as lamplight, and sunlight, when focusing it to avoid reducing the lifespan of the CMOS sensor, and causing overbrightness and flickering.
- When using a laser beam device, avoid exposing the device surface to laser beam radiation.
- Prevent liquid from flowing into the device to avoid damage to its internal components.
- Protect indoor devices from rain and dampness to avoid electric shocks and fires breakingout.
- Don't block the ventilation opening of the device to avoid heat accumulation.
- Don't walko on or squeeze the line cord and wires, particularly at plugs, powersockets, and the point where they exit from the device.
- The dome cover is an optical component. Don't directly touch or wipe the surface of the cover. When it's contaminated with dust, grease, or fingerprints, use degreasing cotton moistened with a little ether or a clean soft cloth dipped in water to gently wipe it clean.
- Don't touch the photosensitive CMOS. Use an air blower to clean the dust or dirt onthe lens.
- Clean the device body with a soft dry cloth. If there are any stubborn stains, clean them away with a soft cloth dipped in a neutral detergent, and then wipe the surface dry. Don't use volatile solvents such as ethyl alcohol, benzene, diluent, or abrasive detergents on the device to avoid damaging the coating and degrading the performance of the device.
- It's normal for a camera made of stainless steel to develop rust on its surface after being used in a strong corrosive environment, such as the seaside or chemical plants. Use an abrasive soft cloth moistened with a little acid solution (vinegar is recommended) to gently wipe it away. Afterwards, wipe it dry.

2 DEVICE DESCRIPTION

Internet Protocol camera (IPC) is a type of digital video camera that receives control data and sends image data through the Internet. They can be used for surveillance and require no local recording device, but only a local network connection. The device is a multi-channel camera where you can set the parameters for each channel.

In the general IPC network topology, IPC is connected to PC through network switch or router. Get IP address by searching on ConfigTool, to start accessing IPC through the network. Use Windows system to manage the camera, because it doesn't support macOS system.

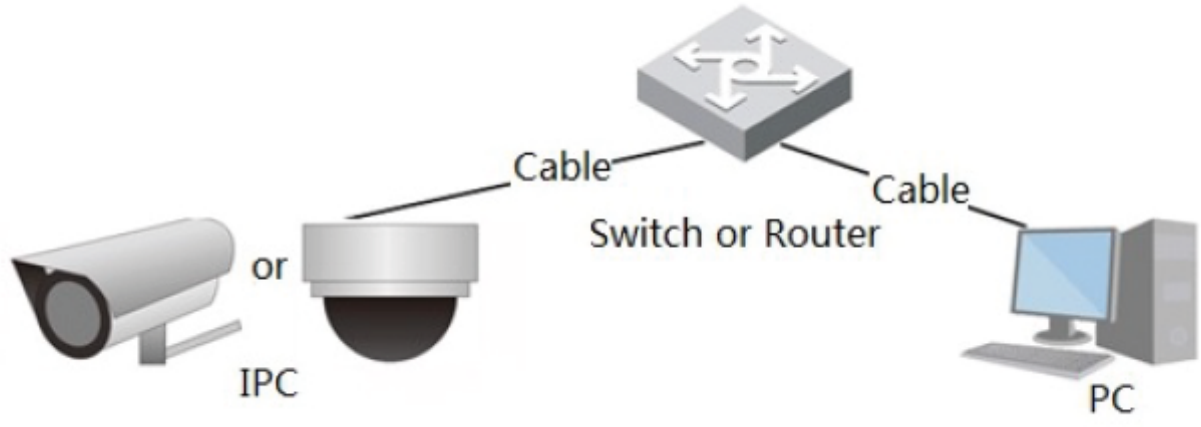

Figure 1: General IPC network

Main features of the device:

- Live view
  When live viewing the image, you can record, take a snapshot, enable audio, voice talk and connect monitoring center for quick processing on the abnormality.
- Alarm
  You can set alarm prompt mode and tone according to alarm type, and view alarm prompt messages.
- Exception
  When SD card error or illegal access is triggered, the system links alarm output and sends an email.
  When the network disconnection alarm is triggered, the system links the recording and alarm output.
  When the input voltage is more or less than the rated voltage, the alarm is triggered and the system links sending email.
- Video detection
  The function includes motion detection and video tampering detection.
  When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.
- Audio detection
  The function includes audio exception and intensity change detection.
  When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.
- Record
  You can record automatically as schedule, play back and download recorded video and picture.
- Account
  You can add, edit and delete the user group, and manage user authorities according to user group.
  You can add, edit and delete the user, and configure user authorities.

3 CONFIGURATION FLOW

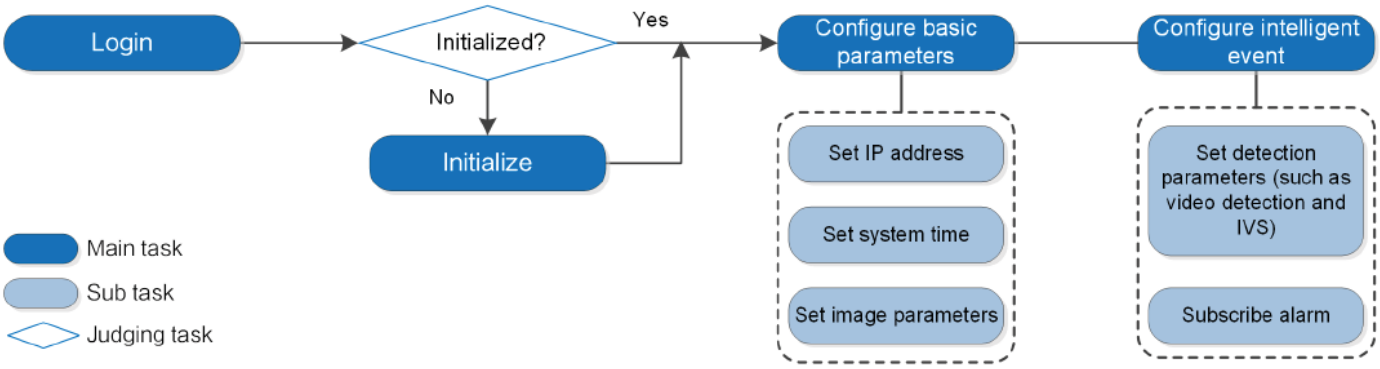

Figure 2: Configuration flow

Table 1 - MyEye Bullet and Dome Lite - Configuration flow

Configuration		Description	Reference
Login		Open a web browser and enter IP address to log into the device. The camera IP address is **192.168.1.108** by default.	5 - LOGIN
Initialization		Initialize the camera when you use it for the first time.	4 - DEVICE INITIALIZATION
Basic parameters	Camera parameters	Configure image parameters, encoder parameters, and audio parameters to ensure the image quality.	8 - CAMERA
	Date & time	Set date and time to ensure the recording time is correct.	12.2 - Date & Time
	IP address	Change IP address according to network planning for the first use or during network adjustment.	9.1 - TCP/IP
	Subscribe alarm	Subscribe alarm event. When the subscribed alarm is triggered, the system records the alarm on the alarm tab.	19 - ALARM

4 DEVICE INITIALIZATION

Device initialization is required for the first-time use. This manual is based on the operation on the web page. You can also initialize device using ConfigTool, recorder, or platform devices.

To ensure the device safety, keep the password properly after initialization and change the password regularly.

When initializing the device, keep the PC IP and device IP in the same network.

Procedure:

1. Enter the IP address of the device in the web browser and press the Enter key. The IP is **192.168.1.108** by default.
2. Set the password for admin account.

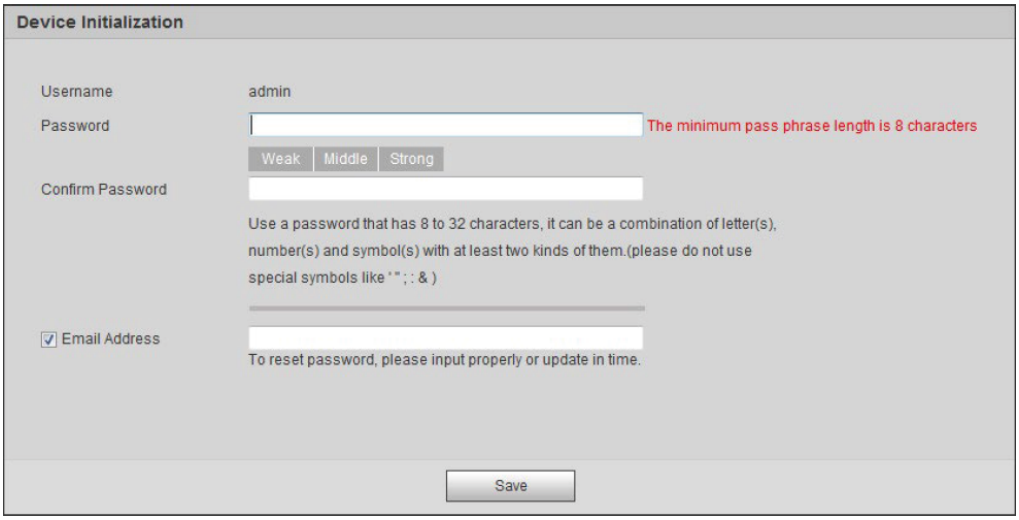

Figure 3: Password setting

Table 2 - MyEye Bullet and Dome Lite - Password parameters

Parameter	Description
Username	The default username is **admin**.
Password	The password needs to consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &). Set a high security level password according to the password security notice.
Confirm Password	
Email address	Enter an email address for password resetting. The checkbox of this option is ticked by default. When you need to reset the password of the admin account, a security code for password resetting is sent to the reserved email address.

3. Click **Save**.
4. Select the upgrading method as needed.
   If you tick **Auto-check for updates**, the system checks new version once a day automatically. There appears system notice on **Upgrade** interface and **Version** interface if any new version is available.
   To enable the auto-check function go to **Setting > System > Upgrade > Online Upgrade**.

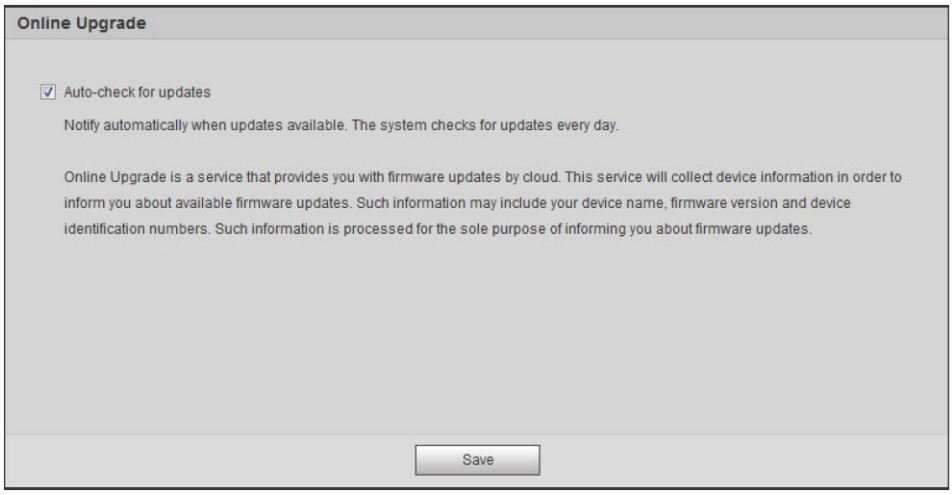

Figure 4: Online upgrade

5. Click **Save**.

5 LOGIN

5.1 - Device login

You need to initialize the camera before logging in the web page. For more information, see 4 - DEVICE INITIALIZATION.
When initializing the camera, keep the PC IP and camera IP in the same network.
Follow the instruction to download and install the plug-in for the first login.

Procedure:

1. Enter the IP address of the device in the web browser and press the Enter key. The IP is **192.168.1.108** by default.
2. Enter the username and password. The username is **admin** by default.
3. Click **Login**.

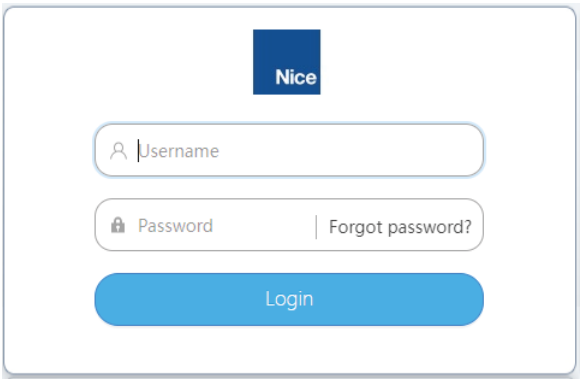

Figure 5: Login

Note
Click the **Logout** tab in the main interface to logs out of the system and move to **Login** inteface.

5.2 - Resetting password

When you need to reset the password for the admin account, a security code is sent to the entered email address necessary to reset the password.

Note
To reset the password you need to enable the password resetting service. For more information, see 12.3.1 - User.

Procedure:

1. Enter the IP address of the device in the web browser and press the Enter key. The IP is **192.168.1.108** by default.
2. Click **Forget password?** to reset the password using the email address set during the initialization.
3. Click **OK** to accept the note.
   Clicking **OK** means that you are informed that some of your personal data might be collected to help reset the password, such as phone

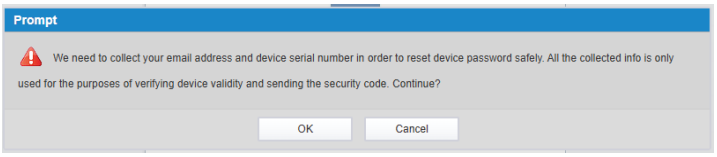

Figure 6: Note

number, MAC address, and device serial number. Read the prompt carefully to decide whether to authorize the collection activity.

4. Scan the QR code for a security code to be sent to the email address you entered. Enter the security code as instructed.
   Note
   - Use the security code within 24 hours after you receive it. Otherwise, it becomes invalid.
   - If you fail to use the security code for two times continuously, there appears a fail notice when you try to get a security code for the third

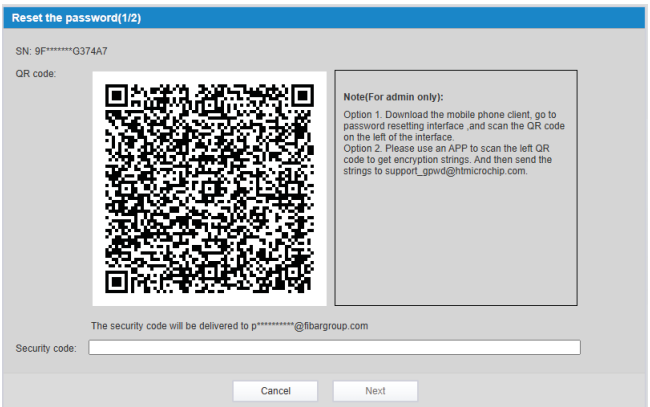

Figure 7: Resetting password 1

time. You have to reset the device to get a security code or wait 24 hours to get it again.

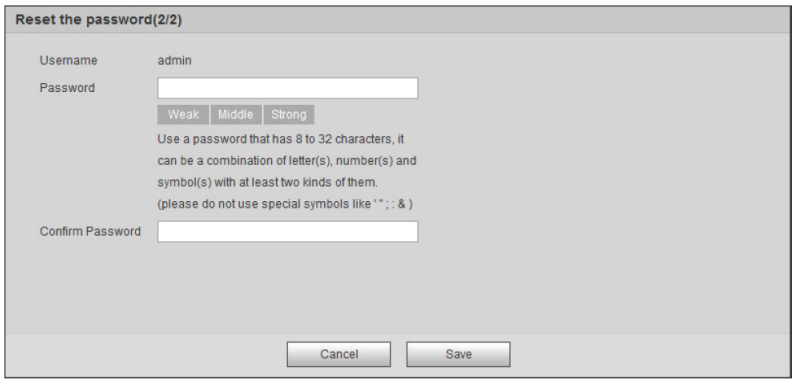

Figure 8: Resetting password 2

5. Enter **Security Code** and click **Next**.
6. Reset and confirm the password.
   The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
7. Click **Save**.

6 LIVE

In the **Live** section you can view the real-time monitoring image.

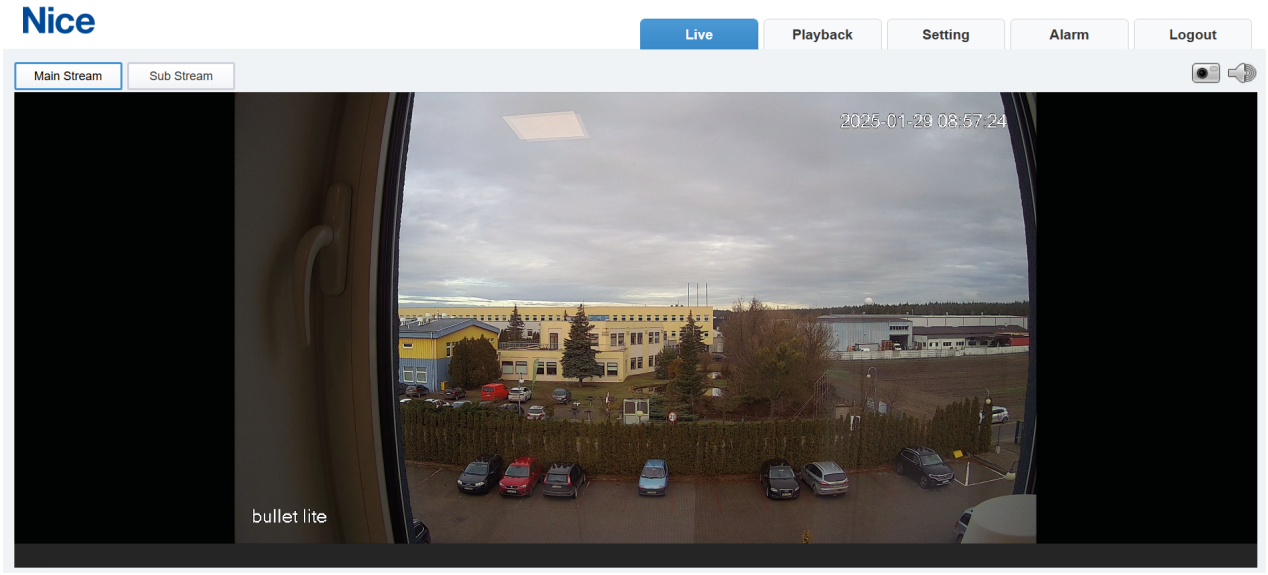

Figure 9: Live section

Table 3 - MyEye Bullet and Dome Lite - Elements of live section

Function	Description
Live	Displays the real-time monitoring image
Playback	Enables playing back or downloading recorded videos and image files
Setting	Enables configuration of camera functions
Alarm	Enables subscribing and viewing alarm information
Logout	Logs out of the system and moves to Login inteface. The system logs out automatically after idling for a period of time.
Main Stream	Has large bit stream value and image with high resolution, but requires large bandwidth. This option can be used for storage and monitoring.
Sub Stream	Has small bit stream value and smooth image, requires less bandwidth. This option is normally used to replace main stream when bandwidth isn't enough.
Snapshot	Captures one image of the current view by clicking the icon. The image is saved to the configured storage path. For more information on configuring a storage path, see 4.5.2.5. Path.
Audio	Enables or disables audio output

7 PLAYBACK

This section includes video and picture playback.

Before playing back video or a snapshot you need to configure record time range, record schedule and record control. For more information, see 11- STORAGE.

7.1 - Playback interface

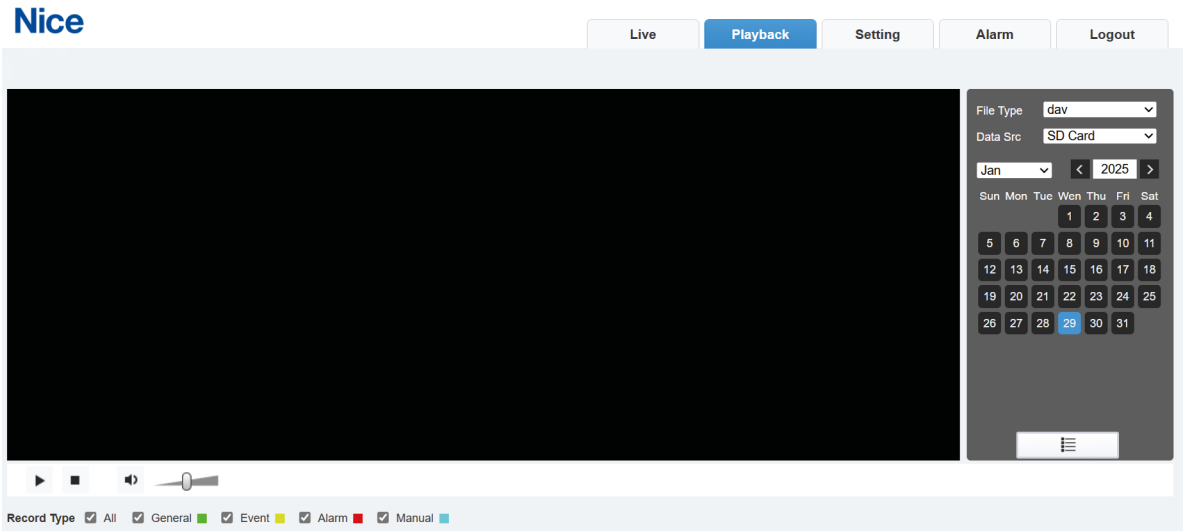

Figure 10: Playback interface

Table 4 - MyEye Bullet and Dome Lite - Playback interface

Function	Description
▶	Click the icon to play backrecorded videos
■	Click the icon to stop playing back recorded videos
🔊	Click the icon to mute or move the zip to adjust the sound
Record Type	Tick the checkbox next to a chosen type to search for such videos or snapshots

7.2 - Playing back and downloading video or snapshot

Procedure:

1. Go to **Playback.**
2. In **File Type** select **dav** to playback a video or **jpg** to playback a snapshot.
3. Select **Record Type**.
4. Select the month and year of the video that you want to play. The dates in blue color indicate there were videos recorded in those days.
5. Click the ▶ icon. The system plays the recorded video of the selected date in the order of time.

   You can also click the ☰ icon for the video files of the selected day to be listed. Enter the start time and end time, and click the 🔍 icon to search all files between the start time and end time. Double-click the file in the list for the system to play the video and displays file size, starting time, and ending time.

   Click the ⬇ icon next to the file to be download. The system downloads the file to the configured path. When downloading pictures, you don't need to select the download format.

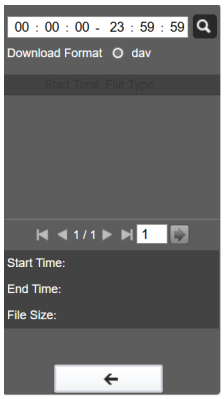

Figure 11: Record search

8.1 - Conditions

8.1.1 - Picture

To improve the scene clarity configure picture parameters.

Procedure:

1. Go to **Settings > Camera > Conditions > Conditions > Picture**.

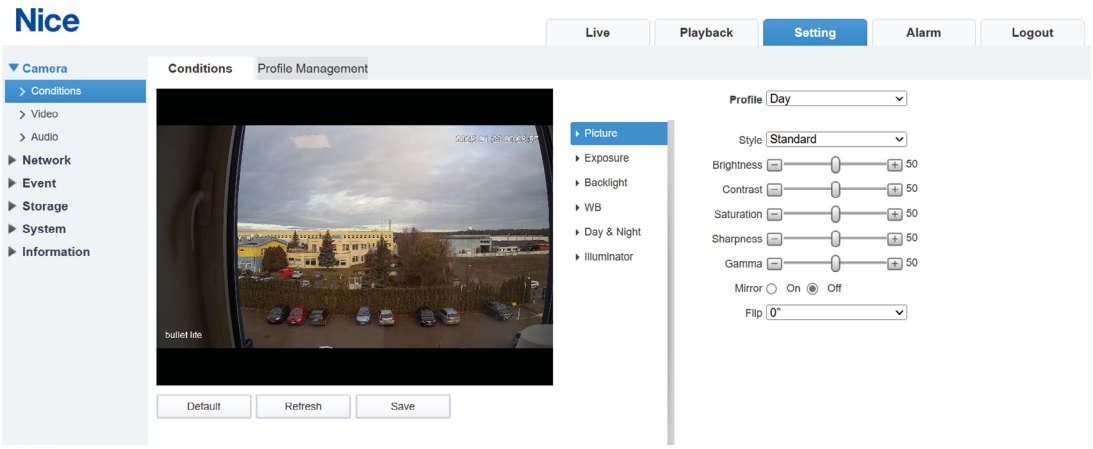

Figure 12: Conditions section

2. Configure picture parameters listed in the table below.

Table 5 - MyEye Bullet and Dome Lite - Picture parameters

Parameter	Description
Profile	Select one of the following options: • **General** • **Day** • **Night**
Style	Select one of the following options: • **Soft** - default image style displaying the actual color of the image • **Standard** - the hue of the image is weaker than the actual one and contrast is smaller • **Vivid** - the image is more vivid than the actual one
Brightness	Changes the value to adjust the picture brightness. The higher the value, the brighter the picture. The picture can be hazy if the value is configured too big.
Contrast	Changes the contrast of the picture. The higher the value, the bigger the contrast between bright and dark areas. If the value is set too big, the dark area would be too dark and bright area is easier to get overexposed. The picture can be hazy if the value is set too small.
Saturation	Makes the color deeper or lighter. The higher the value, the deeper the color. It doesn't change image brightness.
Sharpness	Changes the sharpness of picture edges. The higher the value, the clearer the picture edges. If the value is set too big, picture noises are more likely to appear.
Gamma	Changes the picture brightness and improves the picture dynamic range in a non-linear way. The higher the value, the brighter the picture.
Mirror	Tick the **On** checkbox for the picture to display with left and right side reversed.
Flip	Changes the display direction of the picture. You can choose one of the options: • **0°** - normal display • **180°** - the picture rotates 90° counterclockwise **Note** For some models set the resolution to 1080p or lower when using 180°. For more information, see "4.5.2.1 Video".

3. Click **Save**.

8.1.2 - Exposure

Configure iris and shutter to improve image clarity.

Note

Cameras with true WDR don't support long exposure when **WDR** is enabled in **Backlight**.

Procedure:

1. Go to **Settings > Camera > Conditions > Conditions > Exposure**.

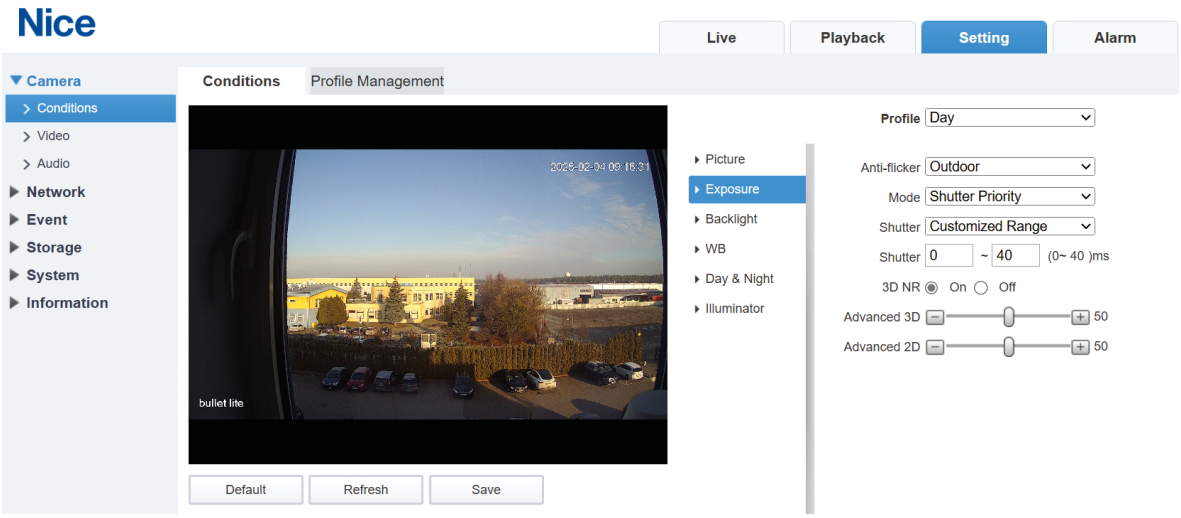

Figure 13: Exposure section

2. Configure picture parameters listed in the table below.

Table 6 - MyEye Bullet and Dome Lite - Exposure parameters

Parameter	Description
Anti-flicker	Select one of the following options: • **50 Hz** - When the electric supply is 50 Hz, the system adjusts the exposure according to ambient light automatically to ensure that there is no stripe appears. • **60 Hz**- When the electric supply is 60 Hz, the system adjusts the exposure according to ambient light automatically to ensure that there is no stripe appears. • **Outdoor** - You can select any exposure mode as needed.
Mode	Select one of the following options: • **Auto** - adjusts the image brightness automatically according to the actual condition • **Gain Priority** - when the exposure range is normal, the system prefers the configured gain range. If the image brightness isn't enough and the gain has reached an upper or lower limit, the system adjusts shutter value automatically to ensure the image at ideal brightness. • **Shutter priority** - when the exposure range is normal, the system prefers the configured shutter range. If the image brightness isn't enough and the shutter value has reached an upper or lower limit, the system adjusts gain value automatically to ensure the image at ideal brightness. • **Manual** - configure gain and shutter value manually to adjust image brightness
Shutter	When selecting **Shutter Priority** or **Manual** in **Mode**, and setting **Customized Range** in **Shutter**, you can set shutter range, measured in ms. The smaller the value, the shorter the exposure time.
Gain	When selecting **Gain Priority** or **Manual** in **Mode**, you can set shutter range. With minimum illumination, the camera increases **Gain** automatically to get clearer images.
3D NR	Works with multi-frame (no less than 2 frames) images and reduces noise by using the frame information between previous and latter frames.

3. Click **Save**.

8.1.3 - Backlight

Procedure:

1. Go to **Settings > Camera > Conditions > Conditions > Backlight**.
2. Select one of the following modes:
   - **Auto** - The system adjusts image brightness according to ambient lighting condition automatically to ensure image clarity.
   - **BLC** - The system gets clearer image of the dark areas on the target. Select the **Default** mode to ensure the clarity of the darkest area, or the **Customized** mode to ensure the image of the set area at ideal brightness.
   - **WDR** - The system dims bright areas and compensates dark areas to ensure the clarity of all the area. The higher the value, the brighter the dark, but the more the noise. There might be a few seconds of video loss when the device is switching to WDR mode from another mode.
   - **HLC** - The system dims strong light and reduces the size of Halo zone to lower the brightness of the whole image, so that the camera can capture human face or car plate detail clearly. The higher the value, the more obvious the HLC effect.
3. Click **Save**.

8.1.4 - WB

WB function makes the image colors display precisely. When in WB mode, white objects would always display white color in different environments.

Procedure:

1. Go to **Settings > Camera > Conditions > Conditions > WB**.
2. Select one of the modes from a drop-down-list. Modes are listed in the table below.

Table 7 - MyEye Bullet and Dome Lite - WB modes

WB mode	Description
Auto	The system compensates WB according to color temperature to ensure color precision.
Natural	The system auto compensates WB to environments without artificial light to ensure color precision.
Street Lamp	The system compensates WB to outdoor night scene to ensure color precision.
Outdoor	The system auto compensates WB to most outdoor environments with natural or artificial light to ensure color precision.
Manual	Configure red and blue gain manually. The system auto compensates WB according to color temperature.
Regionsl Custom	The system compensates WB only to the set area according to color temperature to ensure color precision.

3. Click **Save**.

8.1.5 - Day/Night

You can set the display mode of the image. The system switches between color and black-and-white mode according to the actual condition.

Procedure:

1. Go to **Settings > Camera > Conditions > Conditions > Day/Night.**

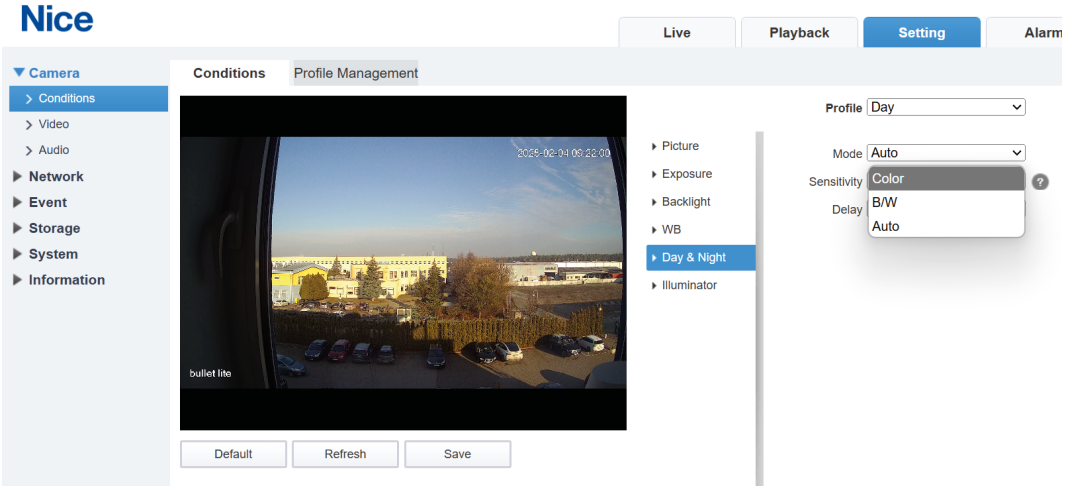

Figure 14: Day and night settings

2. Configure day and night parameters listed in the table below.

Table 8 - MyEye Bullet and Dome Lite - Day and night parameters

Parameter	Description
Mode	Day/Night configuration is independent from profile management configuration. You can select one of the options: • **Color** - The system displays color image. • **Auto** - The system switches between color and black-and-white display according to the actual condition. • **B/W** - The system displays black-and-white image.
Sensitivity	This configuration is available only when **Mode** is set to **Auto**. You can configure camera sensitivity when switching between color and black-and-white mode.
Delay	This configuration is available only when **Mode** is set to **Auto**. You can configure the delay for the camera to switch between color and black-and-white mode. The lower the value, the faster the camera switches between color and black-and-white mode.

3. Click **Save**.

8.1.6 - Illuminator

This configuration is available only when the device is equipped with illuminator.

Procedure:

1. Go to **Settings > Camera > Conditions > Conditions > Illuminator.**
2. Select one of the following modes:
   - **Manual** - You can adjust the brightness of illuminator manually for the system to supply illuminator to the image accordingly.
   - **Smart IR** - The system adjusts the illuminator intensity according to the ambient lighting condition.
   - **Off** - The function is off.
3. Click **Save**.

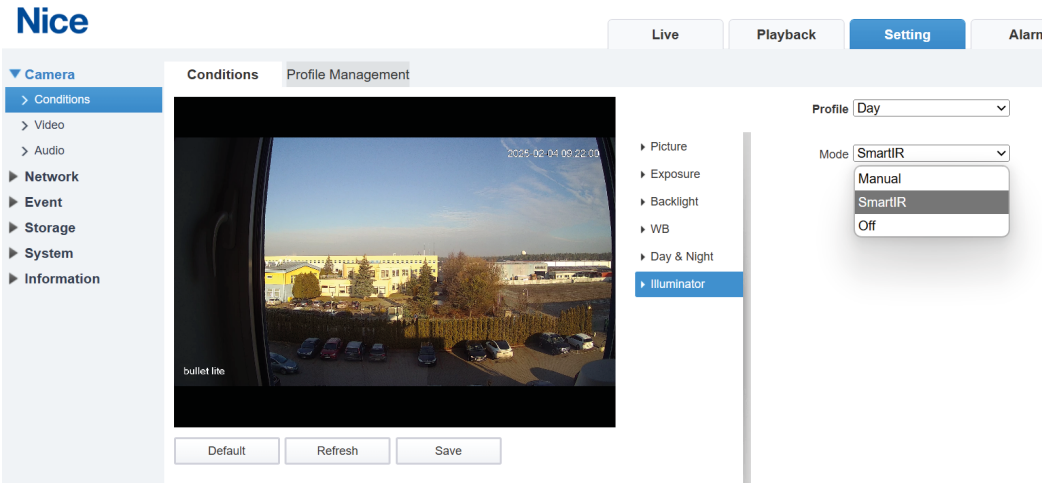

Figure 15: Illuminator settings

8.1.7 - Profile Management

Procedure:

1. Go to **Settings > Camera > Conditions > Profile Management.**
2. Select one of the following **Profile Management**:
   - **General** - The surveillance system works under general configuration.
   - **Full Time** - You can select **Day** or **Night** in the **Always Enable** dro-down-list. The surveillance system works under Always Enable configuration.
   - **Schedule** - You can drag the slide block to set certain time as Day or Night. For example, set 8:00–18:00 as day and 18:00–24:00 as night.
3. Click **Save**.

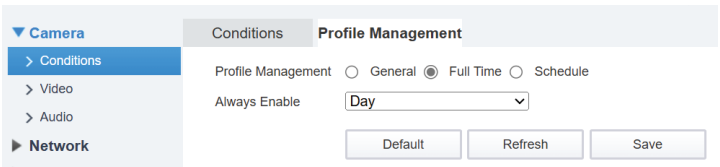

Figure 16: Profile Management - Full Time

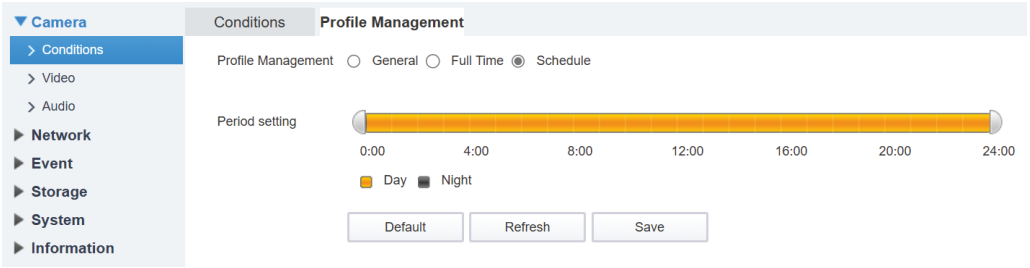

Figure 17: Profile Management - Schedule

8.2 - Video setting

8.2.1 - Video

In this section you can configure video stream parameters.

Click **Default** to restore device to default configuration. Click **Refresh** to view the latest configuration.

Procedure:

1. Go to **Settings > Camera > Video > Video.**

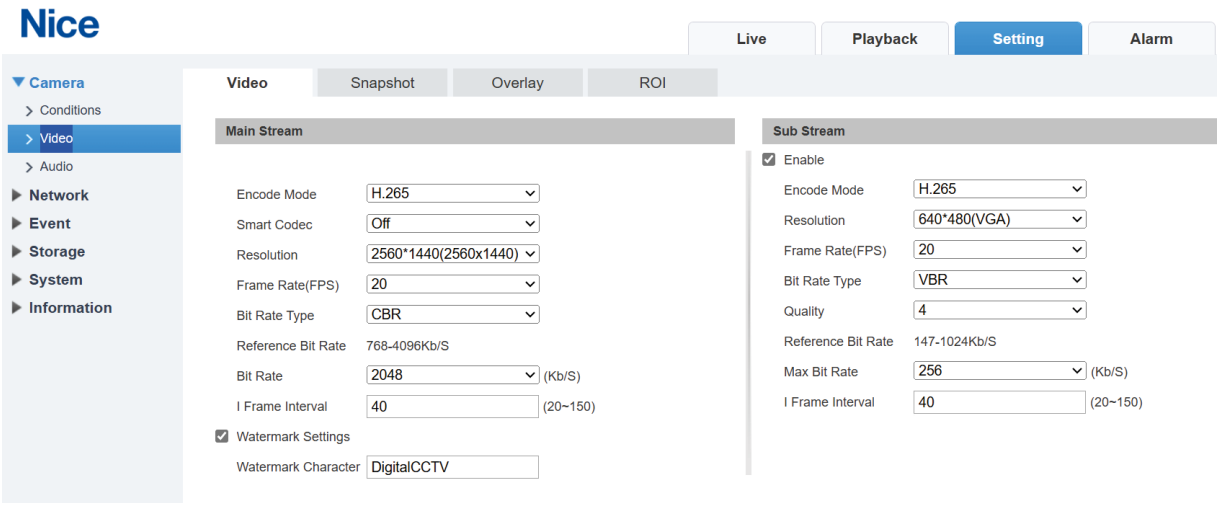

Figure 18: Video settings

2. Configure video parameters listed in the table below.

Table 9 - MyEye Bullet and Dome Lite - Video parameters

Parameter	Description
Enable	Tick the checkbox to enable **Sub Stream**. It's enabled by default.
Encode Mode	• **H.264** - main profile encode mode; requires smaller bandwidth than H.264B • **H.264H** - high profile encode mode; requires smaller bandwidth than H.264. • **H.264B** - baseline profile encode mode • **H.265** - main profile encode mode; it requires smaller bandwidth than H.264.
Smart Codec	Select On from a from a drop-down-list to enable. The function improves video compressibility and saves storage space. It's applicable to staticscenes.
Resolution	The higher the value, the clearer the image, but the bigger the required bandwidth.
Frame Rate (FPS)	The number of frame in one second of video. The higher the value, the clearer and smoother the video.
Bit Rate Type	The bit rate control type during video data transmission. You can select the following options: • **CBR** (Constant Bit Rate) - The bit rate changes a little keeping close to the defined bit rate value. • **VBR** (Variable Bit Rate) - The bit rate changes as monitoring scene changes.
Quality	Can be configured only when the **Bit Rate Type** is set to **VBR**. The better the quality, the bigger the required bandwidth.
Reference Bit Rate	The most suitable bit rate value range recommended to user according to the defined resolution and frame rate.
Max Bit Rate	Can be configured only when the **Bit Rate Type** is set to **VBR**. You can select the value of the **Max Bit Rate** according to the **Reference Bit Rate** value. When monitoring scene changes, the max bit rate keeps close to the defined value.
Bit Rate	Can be configured only when the **Bit Rate Type** is set to **CBR**. Select the bit rate value according to the actual condition.
I Frame Interval	The number of P frames between two I frames. the I Frame Interval range changes as FPS changes. We recommend to set I Frame Interval twice as big as FPS.
Watermark	You can verify the watermark to check if the video has been tampered.
Watermark Character	

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

8.2.2 - Snapshot

Click **Default** to restore device to default configuration. Click **Refresh** to view the latest configuration.

Procedure:

1. Go to **Settings > Camera > Video > Snapshot.**

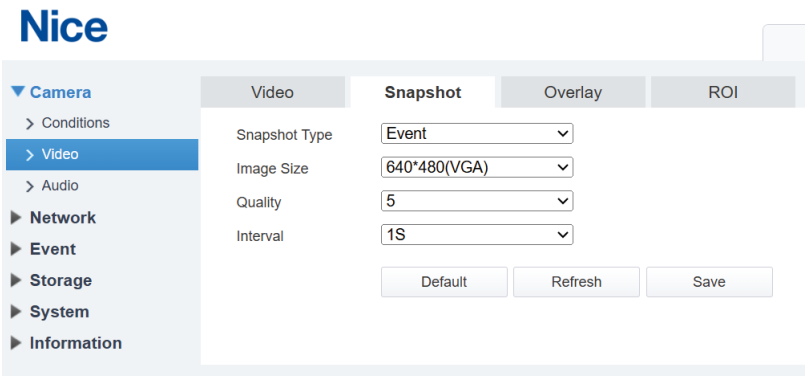

Figure 19: Snapshot settings

2. Configure snapshot parameters listed in the table below.

Table 10 - MyEye Bullet and Dome Lite - Snapshot parameters

Parameter	Description
Snapshot Type	**Event** - The system takes snapshot when the video detection, audio detection, event, or alarm is triggered. This function requires the corresponding snapshot being enabled.
Image Size	The same resolution with main stream
Quality	Six levels of Image quality, the sixth is the best
Interval	Configures the snapshot frequency. Select **Customized** to configure snapshot frequency manually.

3. Click **Save**

8.2.3 - Privacy Masking

You can enable this function when you need to protect privacy of some area on the video image.

Click **Default** to restore device to default configuration. Click **Refresh** to view the latest configuration.

Procedure:

1. Go to **Settings > Camera > Video > Overlay > Privacy Masking.**

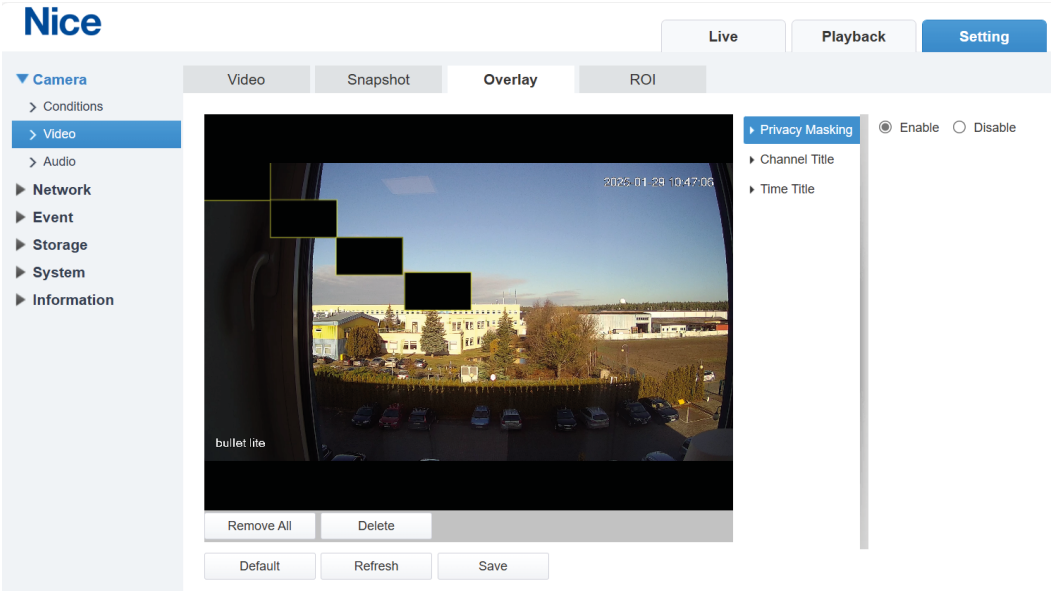

Figure 20: Privacy masking

2. Select **Enable.**
3. Drag the block to the area that you need to cover. You can drag 4 rectangles at most.
   You can click **Remove All** to delete all area boxes or select one box and click **Delete** or right-click to delete it.
4. Adjust the size of the rectangle to protect the privacy.
5. Click **Save**

8.2.4 - Channel Title

With this function enabled you can display channel title in the video image.

Procedure:

1. Go to ⚙ > **Setting > Camera > Video > Overlay > Channel Title.**
2. Tick the checkbox next to **Enable.**
3. Enter **Input Channel Title**.
4. Move the title box to the position that you want in the image.
5. Click **Save.**

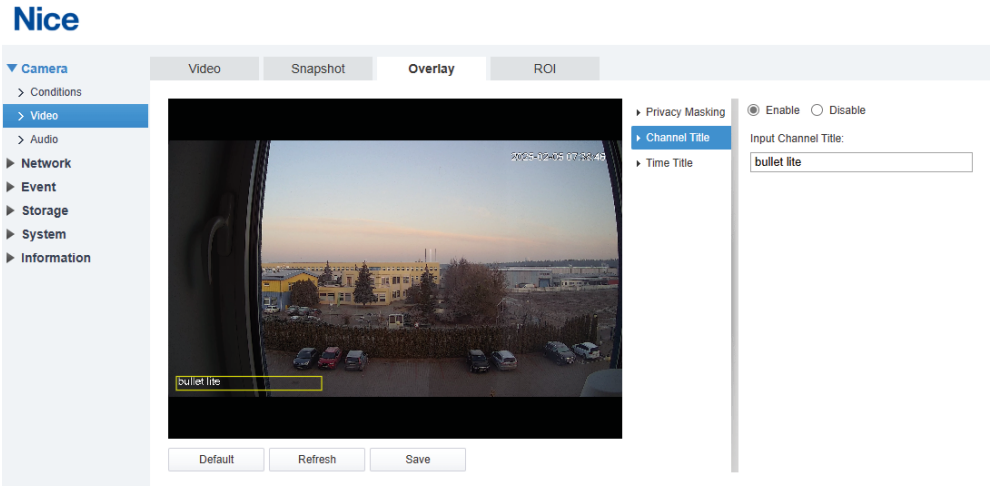

Figure 21: Channel Title setting

8.2.5 - Time Title

With this function enabled you can display time in the video image.

Procedure:

1. Go to **Setting > Camera > Video > Overlay > Time Title.**
2. Tick the checkbox next to **Enable.**
3. Tick the checkbox next to **Week Display** to display the day of week.
4. Move the title box to the position that you want in the image.
5. Click **Save.**

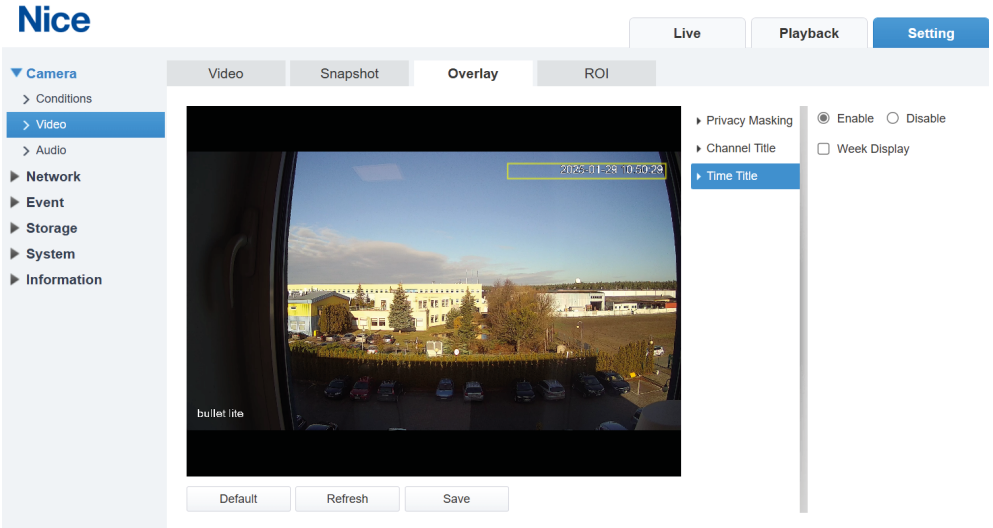

Figure 22: Time Title setting

8.2.6 - ROI

Region of interest (ROI) enables to configure a choosen area of the image to display it at defined quality.

Procedure:

1. Go to **Setting > Camera > Video > ROI**.
2. Tick the checkbox next to **Enable.**
3. Draw the area on the image. You can draw four area boxes at most.
   You can click **Remove All** to delete all the area boxes; select one box, and click **Delete** or right-click to delete it.
4. Configure the **Image Quality** of ROI. The higher the image quality value, the better the quality.
5. Click **Save.**

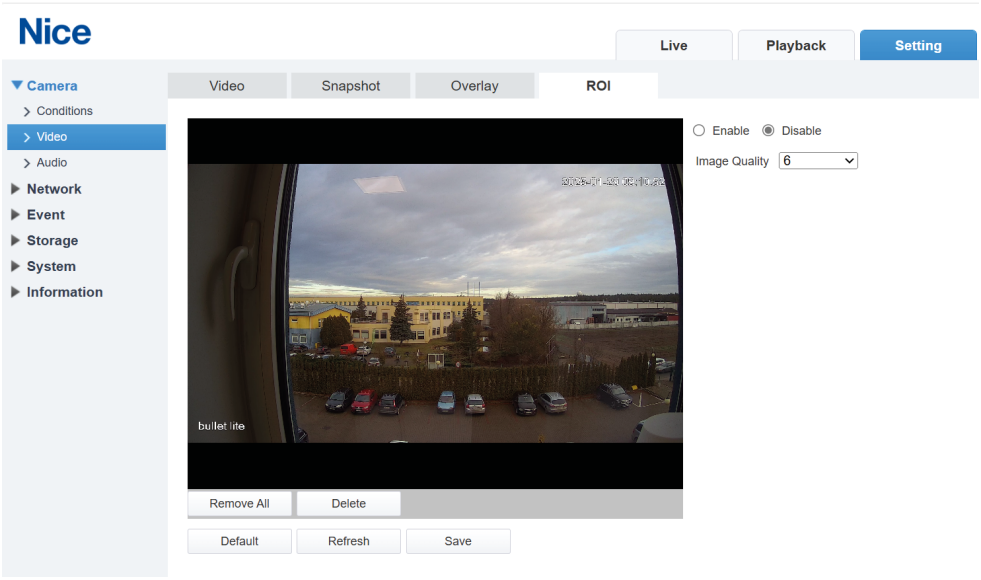

Figure 23: ROI

8.3 - Audio

Procedure:

1. Go to **Setting > Camera > Audio.**
2. Tick the checkbox next to **Enable** in **Main Stream** or **Sub Stream.**
   Carefully activate the audio acquisition function according to the actual requirements.

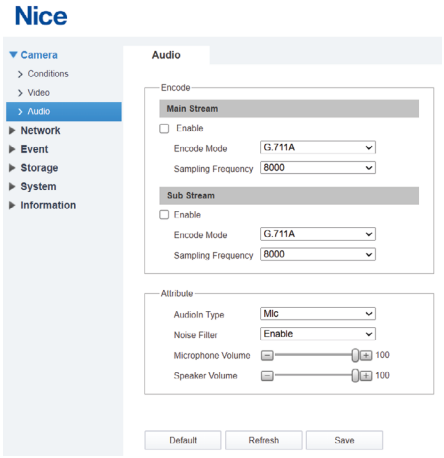

Figure 24: Audio parameters

3. Configure audio parameters listed in the table below.

Table 11 - MyEye Bullet and Dome Lite - Audio parameters

Parameter	Description
Encode Mode	Select one of the following options: • **PCM** • **G.711A** • **G.711Mu** • **G.726** • **AAC** The configured audio encode mode applies to both audio and intercom. The default value is recommended.
Sampling Frequency	Sampling number per second. The higher the sampling frequency, the more the sample in a second and the more accurate the restored signal. Available values of the audio Sampling Frequency: **8000, 16000.**
Audio Input Type	**Mic** - doesn't require external audio device.
Noise Filter	Enable for the system to auto filter ambient noise
Microphone Volume	Adjusts microphone volume
Speaker Volume	Adjusts speaker volume

4. Click **Save**.

9 NETWORK

9.1 - TCP/IP

You can configure IP address and Domain Name System (DNS) server according to network plan.

Procedure:

1. Connect the camera to the network.
2. Go to **Setting > Network > TCP/IP.**

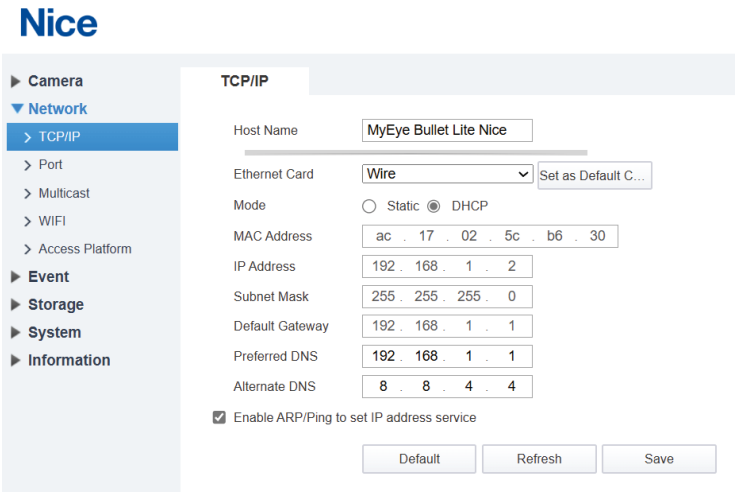

Figure 25: TCP/IP

3. Configure TCP/IP parameters listed in the table below.

Table 12 - MyEye Bullet and Dome - TCP/IP parameters

Parameter	Description
Host Name	Enter the host name no longer than 15 characters
Ethernet Card	Select **Wire** or **Wireless** card card that need to be configured. The default one is **Wire**.
Mode	The mode that the camera gets IP. You can select one of the following options: • **Static** - Configure **IP Address, Subnet Mask**, and **Default Gateway** manually, and click **Save**. The login page with the configured IP address is displayed. • **DHCP** - When there is DHCP server in the network, select DHCP for the camera to acquire IP address automatically.
MAC Address	Displays the host MAC address
IP Address	When you select **Static** in **Mode**, enter needed IP address and subnet mask. The default gateway needs to be in the same network segment as the IP address. IPv6 doesn't have subnet mask.
Subnet Mask	
Default Gateway	
Preferred DNS	IP address of the preferred DNS
Alternate DNS	IP address of the alternate DNS

4. Click **Save**.

9.2 - Port

You can configure the port numbers and the maximum number of users, including web, platform client, and mobile phone client, that can connect to the device simultaneously.

Procedure:

1. Go to **Setting > Network > Port**.

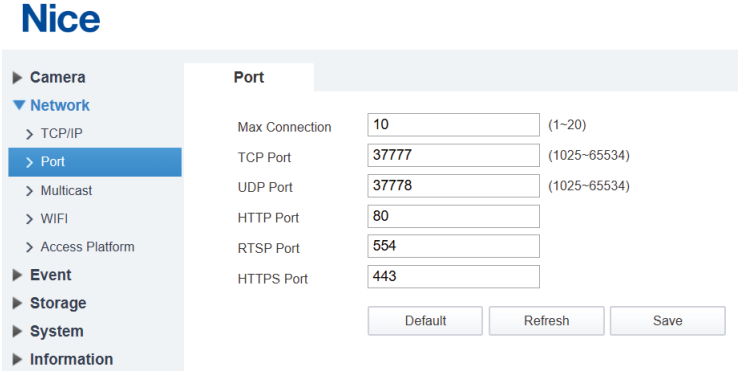

Figure 26: Port

2. Configure Port parameters listed in the table below.

Note

- 0–1024, 1900, 3800, 5000, 5050, 9999, 37776, 37780–37880, 39999, 42323 are reserved for specific uses.
- Don't use the same value for any other port during port configuration.

Table 13 - MyEye Bullet and Dome Lite - Port parameters

Parameter	Description
Max Connection	The maximum number of users, including web client, platform, and mobile client, accessing the recorder the device simultaneously. The default value is ten.
TCP Port	Transmission control protocol port - the default value is **37777**
UDP Port	User datagram protocol port - the default value is **37778**
HTTP Port	Hyper text transfer protocol port - the default value is **80**
RTSP Port	Real time streaming protocol port - the default value is **554** If you play live view with QuickTime, VLC or Blackberry smart phone, the following URL format is available. When the URL format requiring RTSP, you need to specify channel number and bit stream type in the URL as well as username and password if needed. When playing live view with Blackberry smart phone, you need to turn off the audio, and then set the codec mode to H.264B and resolution to CIF. URL format example: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0 where: • Username - the username, such as admin • Password - the password, such as admin • IP - the device IP, such as 192.168.1.112 • Port - leave it if the value is 554 by default • Channel -the channel number, which starts from 1. For example, if you are using channel 2, then the channel=2. • Subtype - the bit stream type; 0 means main stream (Subtype=0) and 1 means sub stream (Subtype=1) If you require the sub stream of channel 2 from a certain device, then the URL can be: rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=2&subtype=1 If username and password are not needed, then the URL can be: rtsp://ip:port/cam/realmonitor?channel=1&subtype=0
RTMP Port	Real Time Messaging Protocol. - the default value is **1935**
HTTPS Port	HTTPS communication port - the default value is **443**

3. Click **Save**.

Note

The configuration of **Max Connection** takes effect immediately. Configuration of other parameters take effect after reboot.

9.3 - Multicast

When multiple users are viewing the device video image simultaneously through network, it might fail due to limited bandwidth. You can solve this problem by setting up a multicast IP (224.0.1.0–238.255.255.255) for the camera and adopt the multicast protocol.

Procedure:

1. Go to **Setting > Network > Multicast.**
2. Tick the checkbox next to **Enable.**
3. Enter **Multicast Address** of **Main Stream/Sub Stream.** The default IP address is **224.1.2.4**. The range is 224.0.0.0 – 239.255.255.255.
4. Enter **Port** number. The default port for **Main Stream** is **40000** and for **Sub Stream - 40016**. The range is 1025 – 65500.
5. Click **Save**.
6. On the **Live** page, select **RTSP** in **Multicast** to view the video image with multicast protocol.

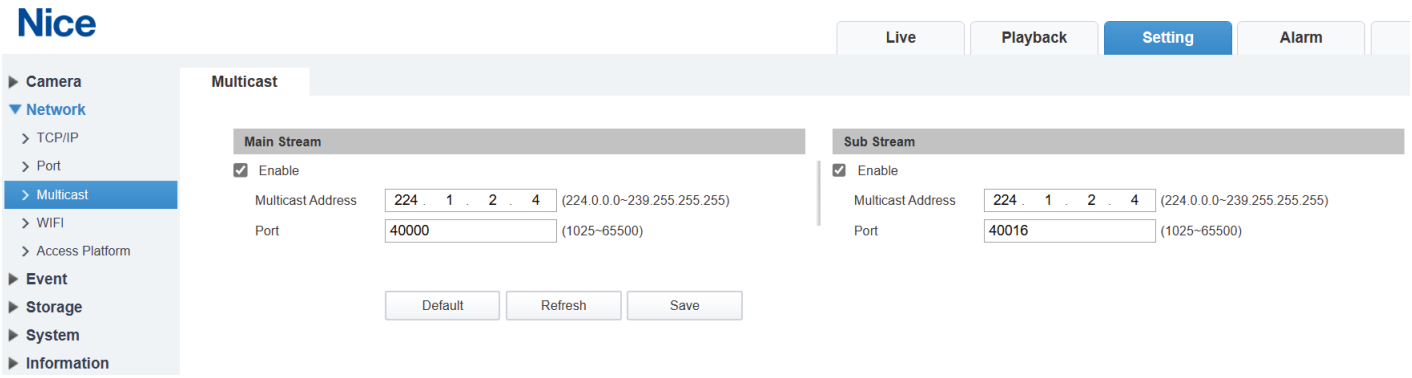

Figure 27: Multicast

9.4 - WiFi

Procedure:

1. Go to **Setting > Network > WiFi.**
2. Tick the checkbox next to **Enable.**
3. Tick the checkbox in the **ID List** column next to chosen Service Set Identifier (**SSID**) to connect to this network.
   You can also click **Add SSID** to add a WiFi network manually or click **Search SSID** for the device to find more WiFi networks.
4. Enter the password and click **Connection**.

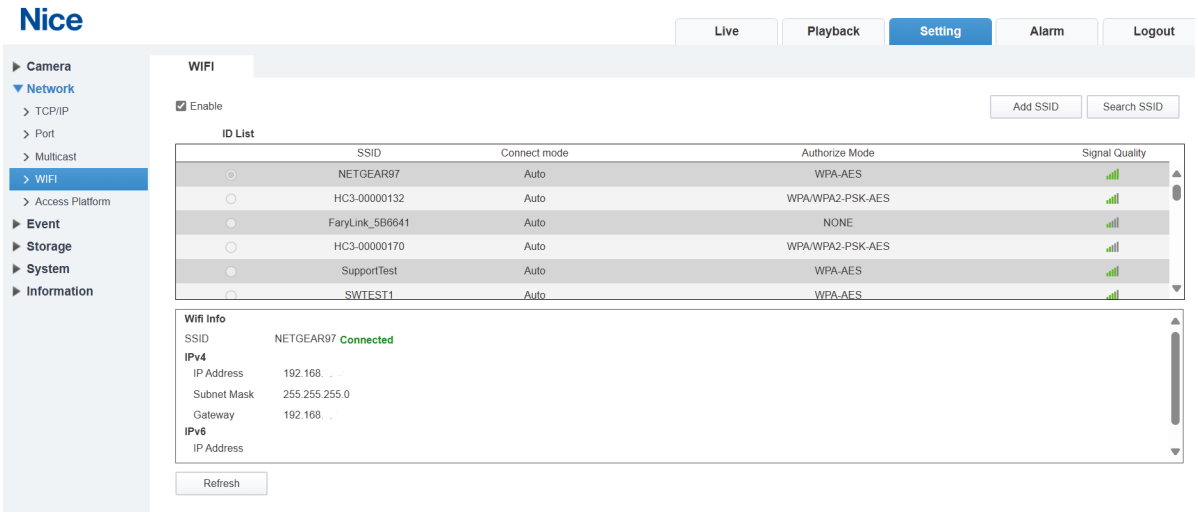

Figure 28: WiFi connection

9.5 - Platform Access

9.5.1 - P2P

Peer-to-peer (P2P) is a private network traversal technology which enables users to manage devices easily without requiring DDNS, port mapping or transit server.

Scan the QR code with your smartphone, and then you can add and manage more devices on the mobile phone client.

Procedure:

1. Go to **Setting > Network > Access Platform > P2P**.
   With P2P enabled:
   - remote management on device is supported.
   - the status is shown online when the device has an access to the network. The information on the IP address, MAC address, device name, and device SN is collected only for the remote access. You can click the **Enable** button to reject the collection.
2. Log in to mobile phone client and tap Device management.
3. Tap + at the upper-right corner.
4. Scan the QR code on the P2P page.
5. Follow the instructions to finish the settings.

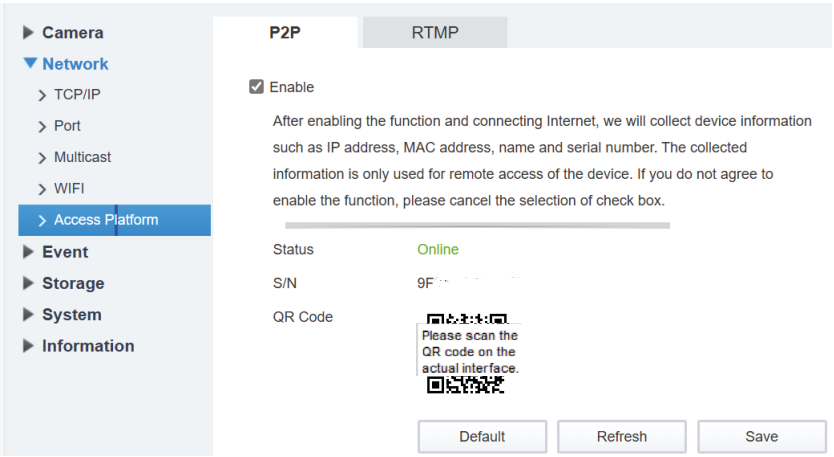

Figure 29: P2P

9.5.2 - RTMP

Through RTMP, you can access a third-party platform, such as YouTube, to realize video live view.
RTMP can be configured by admin only.
RTMP supports only the H.264, H.264 B and H.264H video formats, and the AAC audio format.

Procedure:

1. Go to **Setting > Network > Access Platform > RTMP.**
2. Tick the checkbox next to **Enable.**
   Note
   Make sure that the IP address is trustable when enabling RTMP.

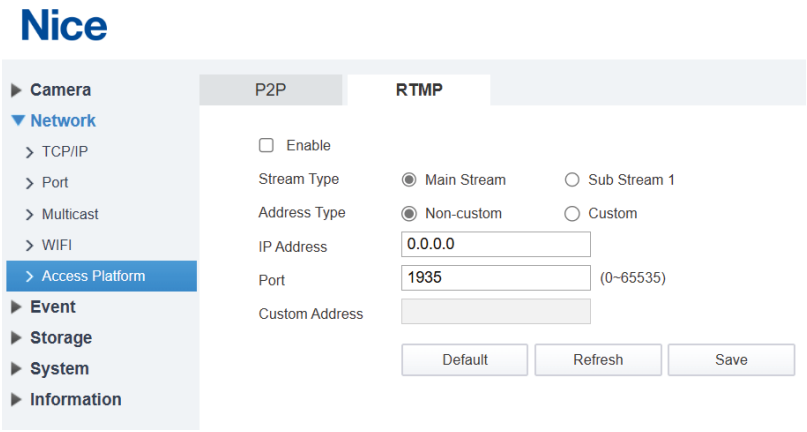

Figure 30: RTMP

3. Configure RTMP parameters listed in the table below.

Table 14 - MyEye Bullet and Dome Lite - RTMP parameters	
Parameter	**Description**
Stream Type	The stream for live view. Make sure that the video format is H.264, H.264 B and H.264H, and the audio format is AAC.
Address Type	• **Non-custom** - enter the server IP and domain name • **Custom** - enter the path allocated by the server
IP Address	When selecting **Non-custom**, you need to enter server IP address and port. • **IP address** - support IPv4 or domain name. • **Port** - keep the default value.
Port	
Custom Address	When selecting **Custom,** you need to enter the path allocated by the server.

4. Click **Save**.

10.1 - Video Detection

10.1.1 - Motion Detection

The system performs an alarm linkage when a moving object appears in the image and its moving speed reaches the configured sensitivity.

If you enable motion detection and smart motion detection simultaneously, and configure the linked activities, the linked activities take effect as follows:

- When motion detection is triggered, the camera records and takes snapshots, but other configured linkages such as sending emails don't take effect.
- When smart motion detection is triggered, all the configured linkages take effect.

If you only enable motion detection, all the configured linkages take effect when motion detection is triggered.

Procedure:

1. Go to **Setting > Event > Video Detection > Motion Detection**.

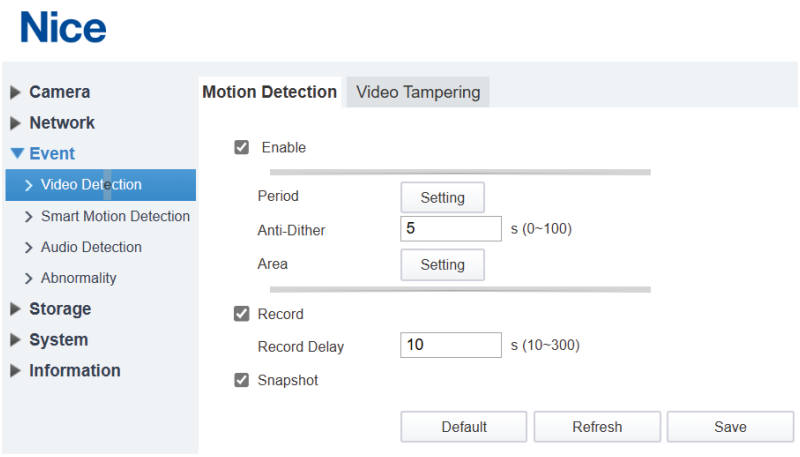

Figure 31: Motion Detection

2. Tick the checkbox next to **Enable.**
3. Click **Setting** next to **Period** to configure arming periods.

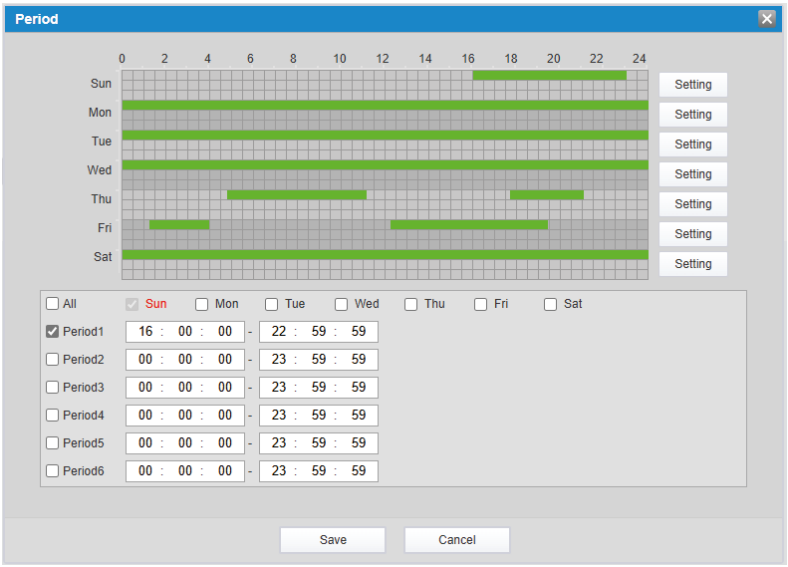

Figure 32: Setting arming periods

4. Select days, and press and drag the left mouse button to set time periods on the plan or enter the values next to Periods 1 to 6. You can set 6 time periods per day.
5. Click **Save**.
6. Set **Anti-Dither** period. Only one record alarm is possible during one the anti-dither period.
7. Click **Setting** next to **Area** to configure area for motion detection.
8. Select a color selecting one of the following  and enter **Name** to set different detection parameters for each region.
9. Set the **Sensitive** degree of outside changes. The higher the sensitivity the easier to trigger the alarm.
10. Set the **Threshold** for motion detection. The smaller the threshold, the easier to trigger the alarm.
    The whole video image is the effective area for motion detection by default.
    The red line in the waveform indicates that the motion detection is triggered, and the green one indicates that there is no motion detection.
    Adjust sensitivity and threshold according to the waveform.
11. Click **Save**.

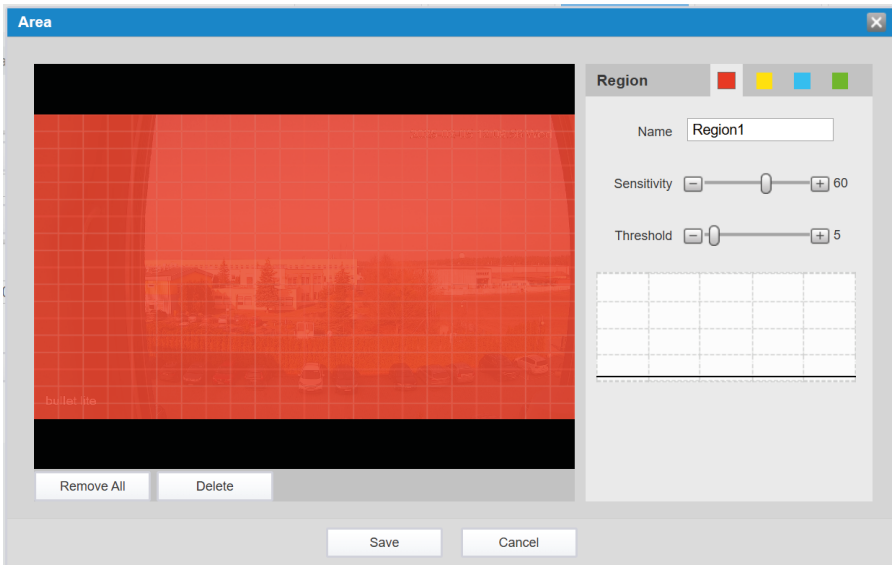

Figure 33: Setting area for motion detection

12. Tick the checkbox next to **Record** and set **Record Delay** for the system to start recording when the alarm is triggered.
13. Tick the checkbox next to **Snapshot** for the system to take a snapshot when the alarm is triggered.
14. Click **Save**.

10.1.2 - Video Tampering

The system performs alarm linkage when the lens is covered or video output is a mono-color screen for example, because of light.

Procedure:

1. Go to **Setting > Event > Video Detection > Video Tampering.**
2. Tick the checkbox next to **Enable.**
3. Click **Setting** next to **Period** to configure arming periods.
4. Select days, and press and drag the left mouse button to set time periods on the plan or enter the values next to Periods 1 to 6. You can set 6 time periods per day. For more information, see Figure 32.
5. Click **Save**.
6. Tick the checkbox next to **Record** and set **Record Delay** for the system to start recording when the alarm is triggered.
7. Tick the checkbox next to **Snapshot** for the system to take a snapshot when the alarm is triggered.
8. Click **Save**.

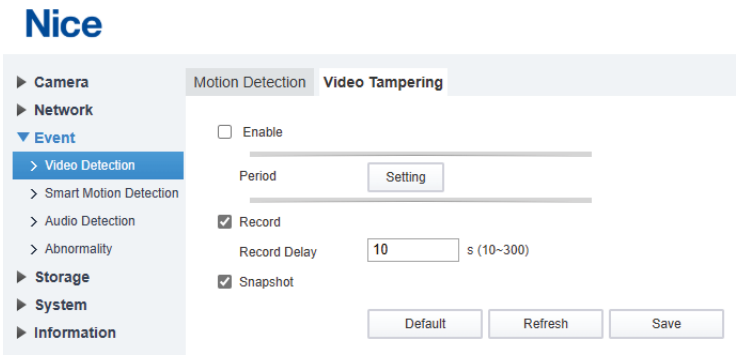

Figure 34: Video tampering

10.2 - Smart Motion Detection

The system performs alarm linkage when human or non-motorized vehicle appears in the detection area and its moving speed reaches the pre-set sensitivity. Enabling smart motion detection can avoid the alarms triggered by the environment changes. The function is enabled by default.

Procedure:

1. Go to **Setting > Event > Smart Motion Detection**.
2. Enable **Motion Detection.** For more information, see **10.1.1 - Motion Detection.**
3. Set **Period** and **Area** in **Motion Detection** making sure that the **Sensitivity** value is larger than 0, and the **Threshold** value is smaller than 100.
4. Go to **Setting > Event > Smart Motion Detection.**
5. Tick the checkbox next to **Enable** and **Human** for the camera to detect human and non-motorized vehicle.
6. Set **Sensitivity** selecting **Low, Middle,** or **High** from a drop-down list.
7. Click **Save**.

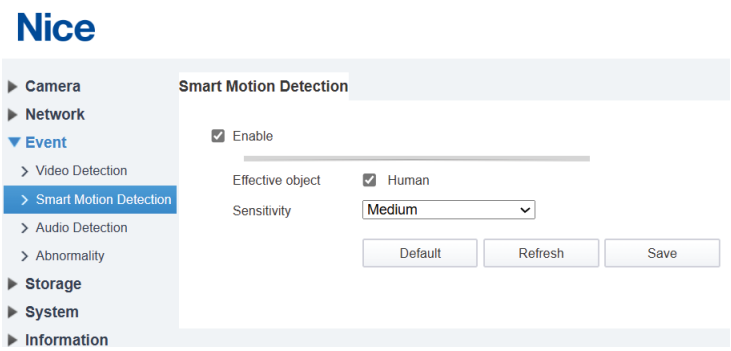

Figure 35: Motion Detection

10.3 - Audio Detection

The system performs alarm linkage when vague voice, tone change, or rapid change of sound intensity is detected.

Procedure:

1. Go to **Setting > Event > Audio Detection.**
2. Tick the checkboxes next to **Input Abnormal** and **Intensity Change**.
3. Set **Sensitivity** and **Threshold**. The alarm is triggered when the system detects that the sound intensity exceeds the configured threshold. It's easier to trigger the alarm with higher sensitivity or smaller threshold. Set a high threshold for noisy environment.
4. Click **Setting** next to **Period** to configure arming periods.
5. Select days, and press and drag the left mouse button to set time periods on the plan or enter the values next to Periods 1 to 6. You can set 6 time periods per day. For more information, see Figure 32.
6. Click **Save**.
7. Tick the checkbox next to **Record** and set **Record Delay** for the system to start recording when the alarm is triggered.
8. Tick the checkbox next to **Snapshot** for the system to take a snapshot when the alarm is triggered.
9. Click **Save.**

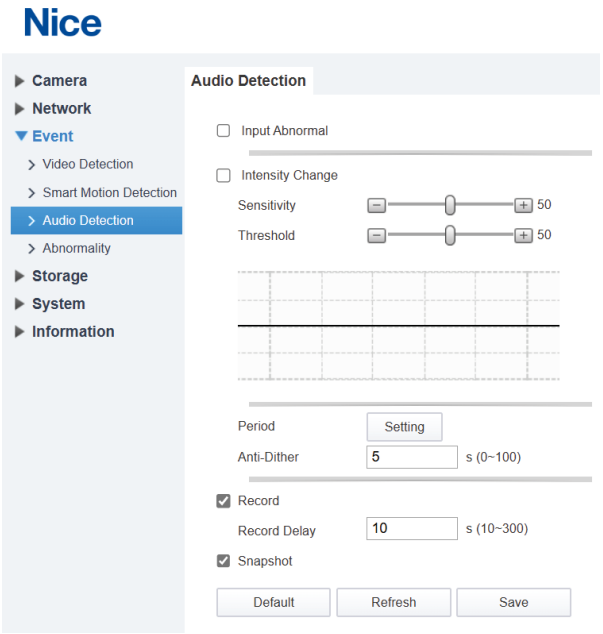

Figure 36: Audio detection

10.4 - Abnormality

10.4.1 - SD Card

In case of SD card abnormality, the system performs alarm linkage.

Procedure:

1. Go to **Setting > Event > SD Card.**
2. Select Event Type choosing **No SD Card, SD Card Error** or **Capacity Warning**.
3. Tick the checkbox next to **Enable.**
4. Click **Save**.

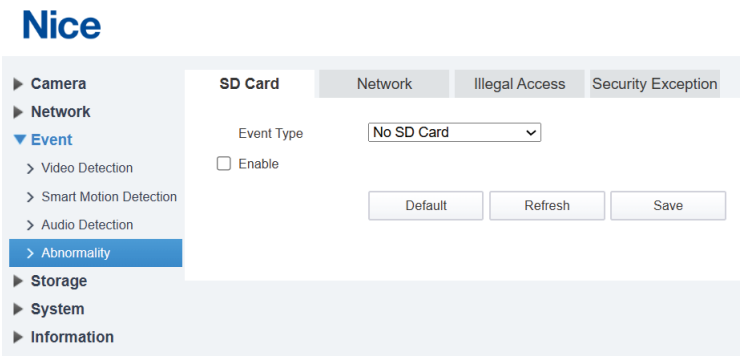

Figure 37: SD card abnormality

10.4.2 - Network

Procedure:

1. Go to **Setting > Event > Network.**
2. Select Event Type choosing **Disconnection** or **IP Conflict**.
3. Tick the checkbox next to **Enable.**
4. Tick the checkbox next to **Record** and set **Record Delay** for the system to start recording when the alarm is triggered.
5. Click **Save**.

Figure 38: Network abnormality

10.4.3 - Illegal Access

Procedure:

1. Go to **Setting > Event > Illegal Access.**
2. Tick the checkbox next to **Enable.**
3. Set number of **Login Error**s.
4. Click **Save**.

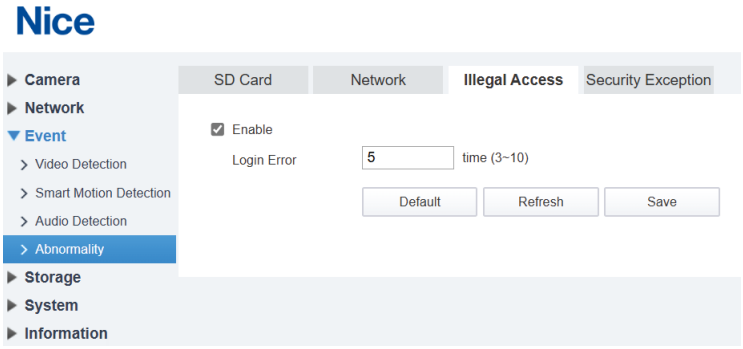

Figure 39: Illegal Access

10.4.4 - Security Exception

When a hostile attack is detected, the system performs alarm linkage.

Procedure:

1. Go to **Setting > Event > Security Exception.**
2. Tick the checkbox next to **Enable.**
3. Click **Save**.

11 STORAGE

In this section you can manage saved resources (such as recorded video) and storage space.

11.1 - Schedule

11.1.1 - Record

After the corresponding alarm type, **General, Event**, or **Alarm**, is enabled, the record channel links recording.

Procedure:

1. Go to **Setting > Storage > Schedule > Record.**

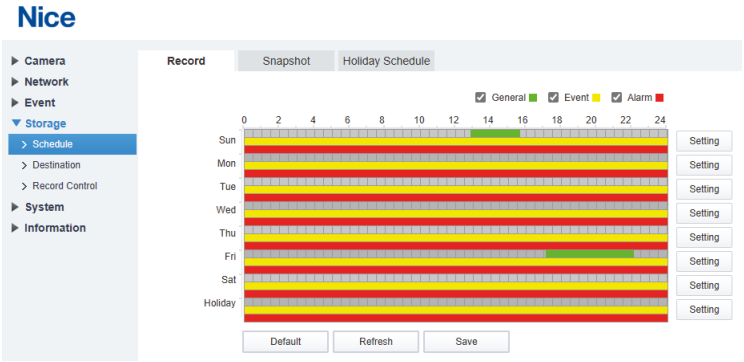

Figure 40: Record Schedule

2. Select record plan type ticking one or more following options:
   - **General** - green used for timing recording
   - **Event** - yellow used for recording triggered by an event
   - **Alarm** - red used for recording triggered by an alarm-in
3. Press and drag the left mouse button to set the time period for the chosen record type(s) on the timeline next to chosen day. You can also enter time periods by clicking **Setting** at the end of a chosen timeline. For more information, see Figure 39.

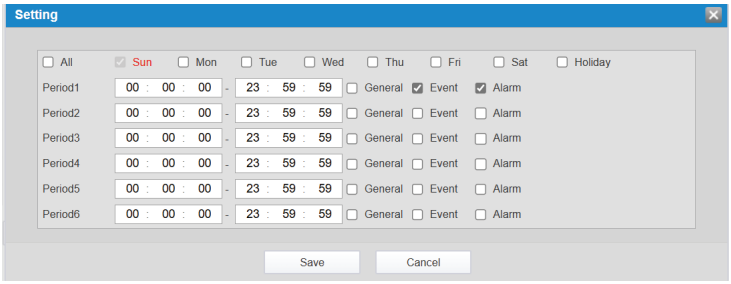

Figure 41: Record setting

4. Click **Save** to save the setting.
5. Click **Save** to save the record plan.

11.1.2 - Snapshot

After the corresponding alarm type, **Event**, or **Alarm**, is enabled, the record channel links a snapshot.

Procedure:

1. Go to **Setting > Storage > Schedule > Snapshot.**
2. Select record plan type ticking one or two following options:
   - **Event** - yellow used for recording triggered by an event
   - **Alarm** - red used for recording triggered by an alarm-in
3. Press and drag the left mouse button to set the time period for the chosen record type(s) on the timeline next to chosen day. You can also enter time periods by clicking **Setting** at the end of a chosen timeline. For more information, see Figure 39.
4. Click **Save** to save the setting.
5. Click **Save** to save the record plan.

11.1.3 - Holiday Schedule

After the corresponding alarm type, **Event**, or **Alarm**, is enabled, the record channel links a snapshot.

Procedure:

1. Go to **Setting > Storage > Schedule > Holiday Schedule.**
2. Tick the checkbox next to **Record** for the system to record.
3. Tick the checkbox next to **Snapshot** for the system to take a snapshot.
4. Select the days to set as holiday. Selected days are marked blue.
5. Click **Save**.

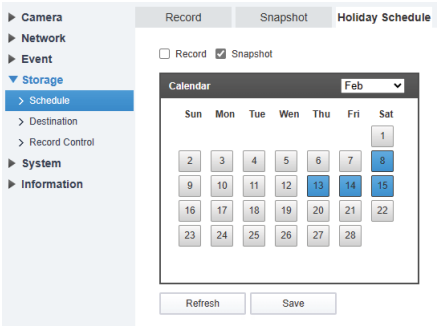

Figure 42: Holiday Schedule

Note
When **Holiday Schedule** setting isn't the same as the **General** setting, the **Holiday Schedule** setting is prior to the **General** setting.

11.2 - Destination

11.2.1 - Path

Go to **Setting > Storage > Destination > Path** to select **Event Type**(s) to be saved on the internal SD card. **Event Type**s include **Scheduled**, **Event** and **Alarm**.

11.2.2 - Local

Go to **Setting > Storage > Destination > Local** to display the information of the local SD card.

You can select one of the following options:

- **Read-Only** - the SD card is set to read only.
- **Read & Write** - the SD card is set to read & write.
- **Hot Swap** - so that you can pull out the SD card.
- **Refresh** - the view is refreshed.

If the SD card capacity is much less than the nominal capacity, you need to format the SD card. Then the data in SD card is cleared. The SD card is formatted to be private file system. The private file system can improve SD card multimedia file read/write performance. Download Disk-manager from Toolbox to read the SD card. For details, contact after-sales technicians.

11.3 - Record Control

After the corresponding alarm type, **Event**, or **Alarm**, is enabled, the record channel links a snapshot.

Procedure:

1. Go to **Setting > Storage > Record Control.**
2. Configure Record Control parameters listed in the table below.

Table 15 - MyEye Bullet and Dome Lite - Record Control parameters	
Parameter	**Description**
Pack Duration	The time for packing each video file
Pre-event Record	The time to record the video in advance of a triggered alarm event. When an alarm or motion detection links recording, and the recording isn't enabled, the system saves the video data within the pre-event record time to the video file.
Disk Full	Recording strategy when the disk is full. • **Stop** - stops recording when the disk is full • **Overwrite** - overwrites cyclically the earliest video when the disk is full
Record Mode	• **Manual** - the system starts recording • **Auto** - the system starts recording in the configured time period of record plan • **Off** - the recording is off
Record Stream	Select **Main Stream** or **Sub Stream**

3. Click **Save**.

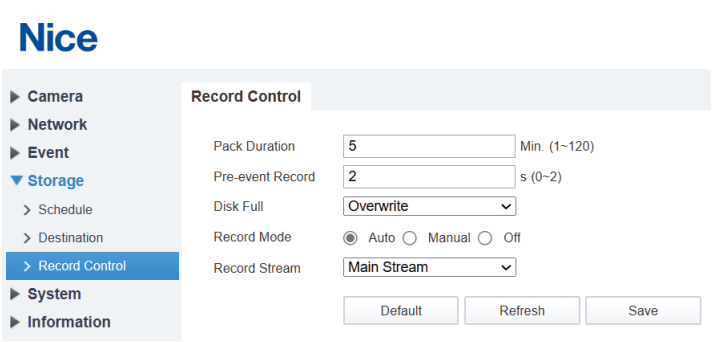

Figure 43: Record Control

12 SYSTEM

12.1 - General

Procedure:

1. Go to **Setting > System > General.**
2. Enter the device **Name.**
3. Select **Video Standard** choosing **PAL** or **NTSC.**
4. Click **Save**.

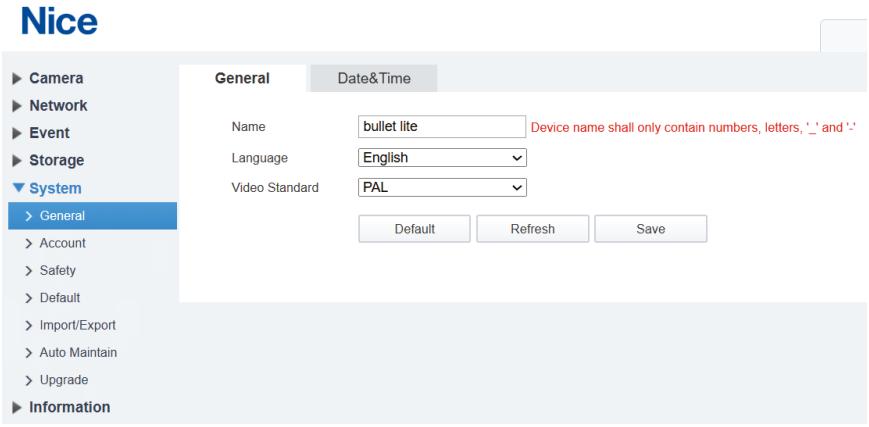

Figure 44: General section

12.2 - Date & Time

Procedure:

1. Go to **Setting > System > General > Date & Time.**

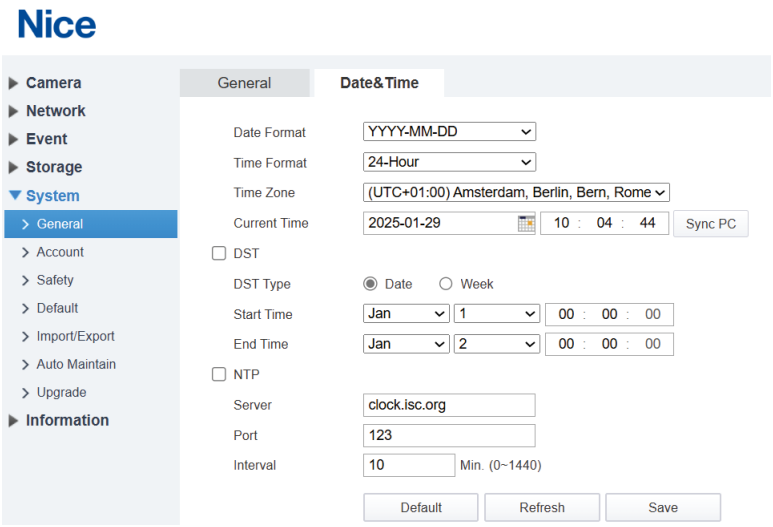

Figure 45: Date and time

2. Configure the parameters listed in the table below.

Table 16 - MyEye Bullet and Dome Lite - Description of Date & Time parameters

Parameter	Description
Date Format	Configure the date format
Time Format	You can select **12-Hour** or **24-Hour.**
Time Zone	Configure the time zone that the camera is at.
Current Time	Configure system time. Click **Sync PC** for the system time to change to the PC time.
DST	If needed tict the checkbox next to **DST** and configure **Start Time** and **End Time** of Daylight Saving Time (DST) with **Date** or **Week**.
NTP	Tict the checkbox next to network time protocol (**NTP**) for the system then syncs time with the internet server in real time.You can also enter **Port** of PC with installed NTP server and set **Interval** for the configured synchronisation.

3. Click **Save.**

12.3 - Account

You can manage users. Users include admin, added users and ONVIF users.

Managing users and groups are only available for administrator users.

You can manage users through single user or group. Duplicating usernames or group names isn't allowed. A user can only be in one group at a time, and the group users can own authorities within group authority range.

Online users can't edit their own authority.

Select **Anonymous Login** to log in with only IP address instead of username and password. Anonymous users only have preview authorities. During anonymous login, click **Logout** so that you can log in with other username.

12.3.1 - User

You are admin user by default. There is one admin by default who has the highest authority. You can add users, and configure different permissions. You can have 18 users at most.

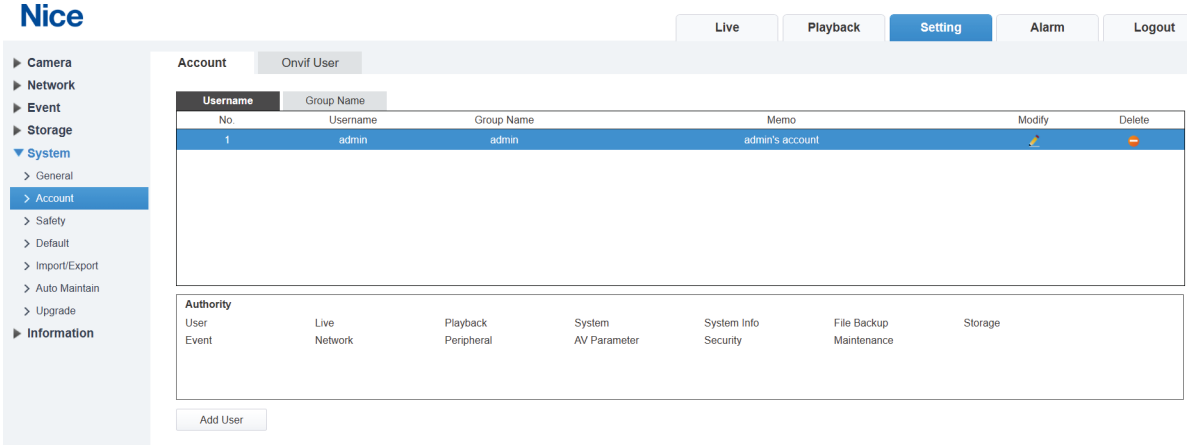

Figure 46: List of users

Procedure of adding a new user:

1. Go to **Setting** > **System > Account > Username.**
2. Click **Add User.**

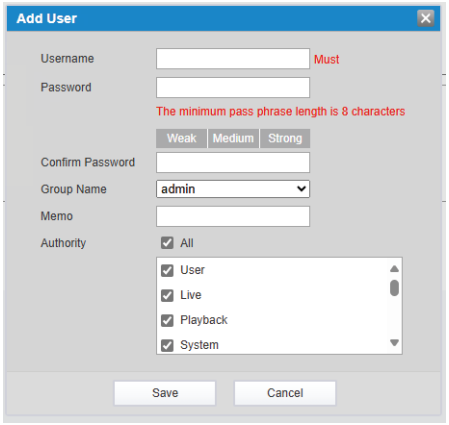

Figure 47: Adding user

3. Configure the user parameters listed in the table below.

Table 17 - MyEye Bullet and Dome Lite - User parameters	
Parameter	**Description**
Username	User's unique identification. You can't use existed username. The max length of the user name is 31 characters including numbers, letters, underline, dash, dot and @.
Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
Confirm Password	
Group	Select a group for the account. The user rights must be within the group authorities.
Memo	Optional: enter a description of the account
Authority	Select permissions as needed. We recommend you give fewer permissions to normal users than premium users.

4. Click **Save.**
   The newly added user is displayed in the user name list.

Related Operations

- Click the icon to edit password, group, remarks or authorities. For admin account, you can only edit the password. To change password tick the **Modify Password** checkbox, enter **Old Password** and **New Password**.
- Click the icon to delete the added users. Admin user can't be deleted.
- If the current account has the permission of user management, click the icon to view the login authorities of other accounts. If not, you can only view the login authorities of the current account.

12.3.2 - User Group

You have two groups named admin and user by default. You can add new groups, delete added groups or edit a group authority. You can have eight groups at most.

Procedure of adding a new user:

1. Go to **Setting > System > Account > Account > Group Name**.
2. Click **Add Group.**

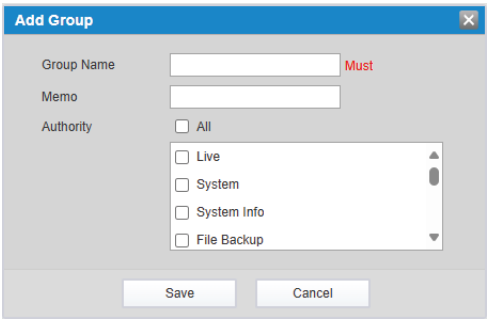

Figure 48: Adding group

3. Enter the **Group Name** and **Memo**.
   You can't use existing group name. The max length of the group name is 31 characters including numbers, letters, underline, dash, dot and @.
4. Select **Authority** ticking the checkboxes next to authorities listed in the table below.

Table 18 - MyEye Bullet and Dome Lite - Descrition of group authority

Group authority	Description	Availability for groups	
		Admin	User
Live	Real-time stream view	Yes	Yes
Playback	Playback view	Yes	Yes
System	Functions such as system time setting	Yes	N/A
System Info	Functions such as version information	Yes	N/A
File Backup	Creating backpups of files	Yes	N/A
Storage	Functions such as storage point configuration, snapshot recording time configuration, SFTP configuration	Yes	N/A
Event	Functions such as video and audio detection settings and alarm settings	Yes	N/A
Network	Functions such as IP, SMTP, SNMP and AP Hotspot settings	Yes	N/A
Peripheral	External light, wiper and serial port settings	Yes	N/A
AV Parameter	Functions such as camera property settings, audio and video settings	Yes	N/A
Security	Functions such as HTTPS settings and RTSP over TLS settings	Yes	N/A
Maintenance	Functions such as automatic maintenance settings	Yes	N/A

5. Click **Save** to finish configuration. The newly added group displays in the group name list.

Related Operations

- Click the icon to edit password, memo or authorities. Any user in the **Admin** group has User authorities to modify group authorities. TheUser group doesn't have this authorities.
- Click the icon to delete the added group. The admin group and user group can't be deleted.

12.3.3 - ONVIF User

Procedure of adding an ONVIF user:

1. Go to **Setting > System > Account > Onvif User**.
2. Click **Add User.**

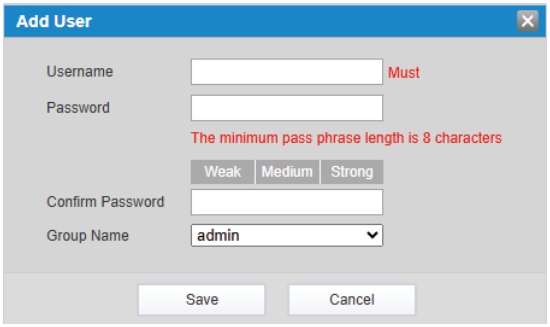

Figure 49: Adding ONVIF user

3. Configure the ONVIF user parameters listed in the table below.

Table 19 - MyEye Bullet and Dome - ONVIF user parameters

Parameter	Description
Username	User's unique identification. You can't use existed username. The max length of the user name is 31 characters including numbers, letters, underline, dash, dot and @.
Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
Confirm Password	
Group Name	Select a group for the account. The user rights must be within the group authorities.

4. Click **Save.**
   The newly added user is displayed in the user name list.

Related Operations

- Click the icon to edit password, group, remarks or authorities. For admin account, you can only edit the password. To change password tick the **Modify Password** checkbox, enter **Old Password** and **New Password**.
- Click the icon to delete the added users. Admin user can't be deleted.
- If the current account has the permission of user management, click the icon to view the login authorities of other accounts. If not, you can only view the login authorities of the current account.

13 SAFETY

13.1 - IP Filter

Configure the IP or MAC hosts, devices allowed to visit the camera. Only the hosts in the trusted sites list can log into the web interface.

Procedure:

1. Go to Go to **Setting > System > Safety > IP Filter**.
2. Click **Add IP/MAC** to add your device to **Allowlist** so that you can access the camera.

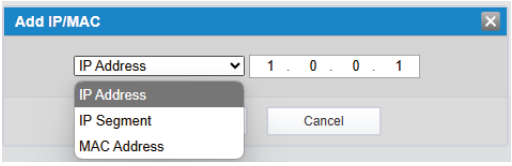

Figure 50: Adding PC to Allowlist

3. Select **IP Address, IP Segment** or **MAC Address** and enter selected data of your device.
4. Click **Save**. The newly added device is displayed in the list.
5. Click **Save**.

13.2 - System Service

Procedure:

1. Go to **Setting > System > Safety > System Service.**

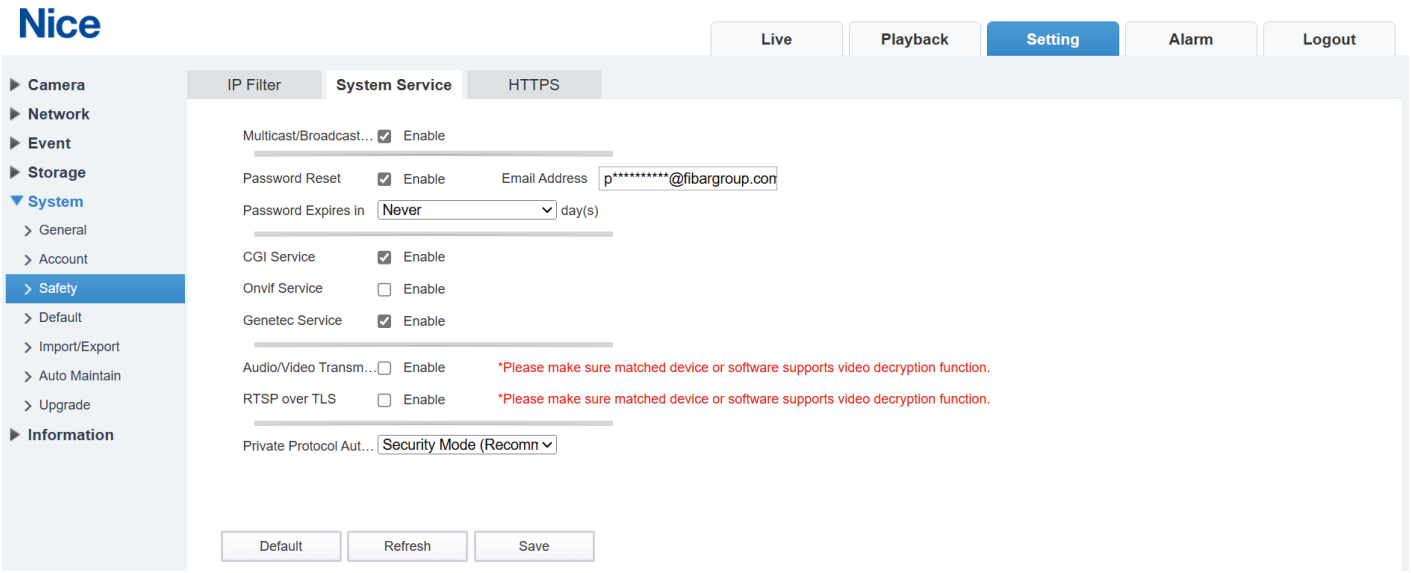

Figure 51: System Service

2. Enable the system services listed in the table below according to the actual needs.

Table 20 - MyEye Bullet and Dome Lite - Description of system services

Function	Description
Multicast/Broadcast Search	With this function enabled when multiple users are previewing the device video image simultaneously through network, they can find your device with multicast/broadcast protocol.
Password Reset	Enable password reset and enter the email address to be used for the reset
CGI Service	With this function enabled other devices can access the camera through this service.
Onvif Service	With this function enabled other devices can access the camera through this service.
Genetec Service	With this function enabled other devices can access the camera through this service.
Audio and Video Transmission Encryption	Make sure that the other devices and software that working together with the camera support video decryption.
RTSP over TLS	Real-Time Streaming Protocol (RTSP) over Transport Layer Security (TLS) enables controlling of multimedia content over a network.
Private Protocol Authentication Mode	This function provides an extra option for authentication.

3. Click **Save**.

13.3 - HTTPS

Create a certificate or upload an authenticated certificate so that you can log in the camera through HTTPS using your PC. The HTTPS can protect page authenticity on all types of websites, secure accounts, and keep user communications, identity, and web browsing private.

Procedure:

1. Go to **Setting > System > Safety > HTTPS**.

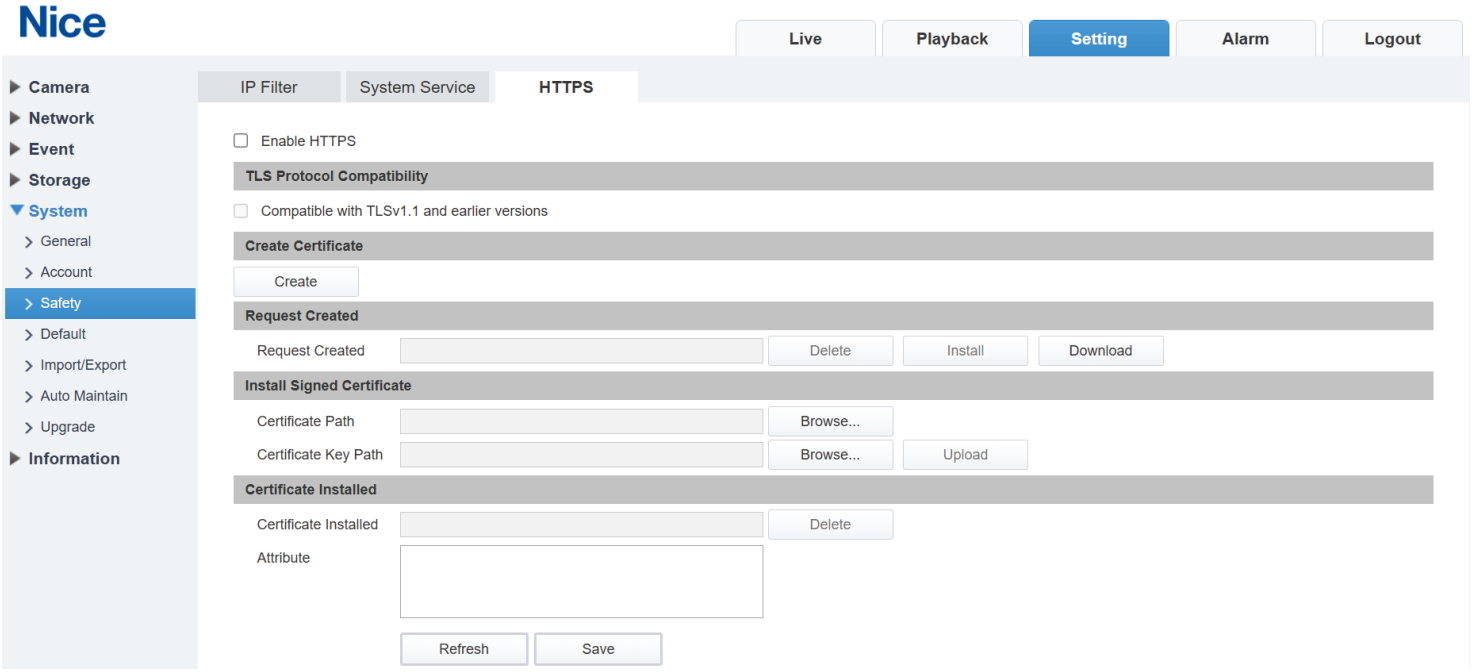

Figure 52: HTTPS configuration

2. Click **Create** to create a certificate or click **Browse** to select the certificate and certificate key, click **Upload** and skip to Step **5**.

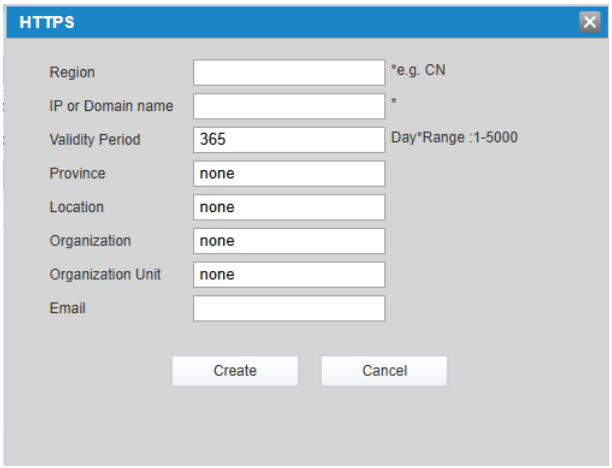

Figure 53: Creating certificate

3. Enter the required information and click **Create**.

   Note

   IP or Domain name needs to be the same as the IP or domain name of the device.

4. Click **Download** to download root certificate.
5. Open the certificate in the download section of your PC.

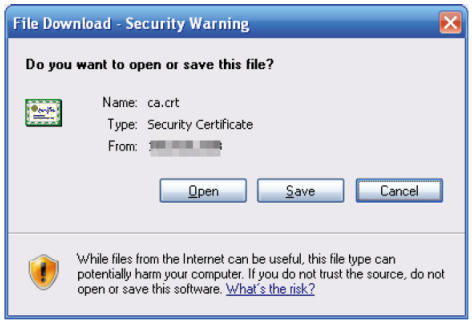

Figure 54: File downloading

6. Click **Open**.

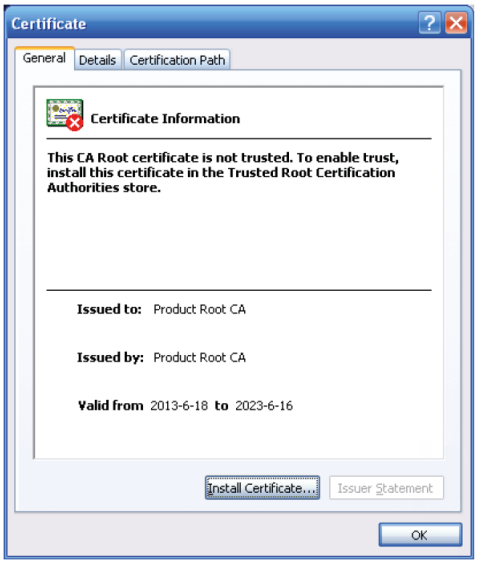

Figure 55: Certificate information

7. Click **Install Certificate**.

Figure 56: Certificate import wizard

8. Click **Next**.

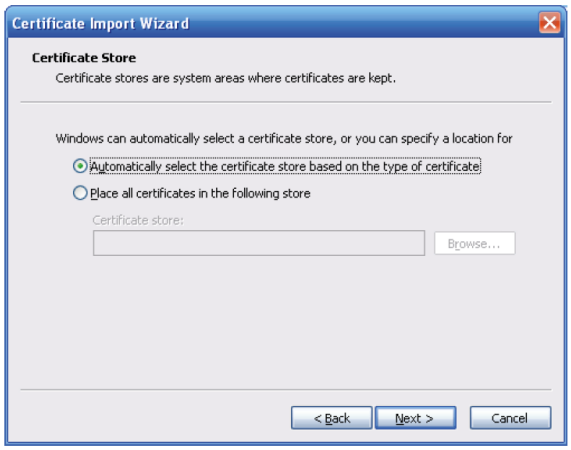

Figure 57: Storing certificate

9. Select the storage location and click **Next**.

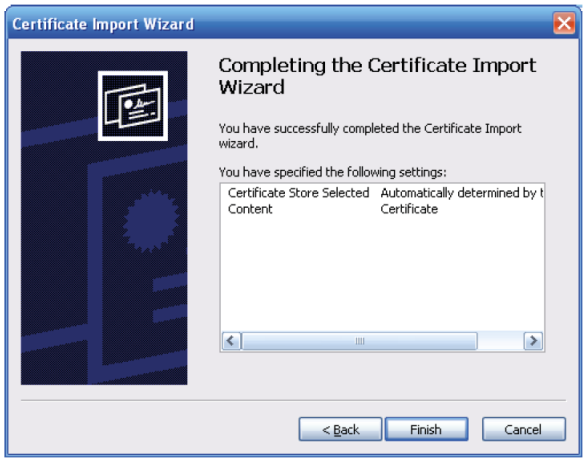

Figure 58: Completing certificate installation

10. Click **Finish** and a dialog box showing **The import was successful** pops up.

Figure 59: Import succeeds

14 DEFAULT

Go to **Setting > System > Default** to restore the device to default configuration or factory settings.

- Click **Default** to reset all the configurations except IP address and account to default.
- Click **Factory Default** to reset all the configurations to factory settings.

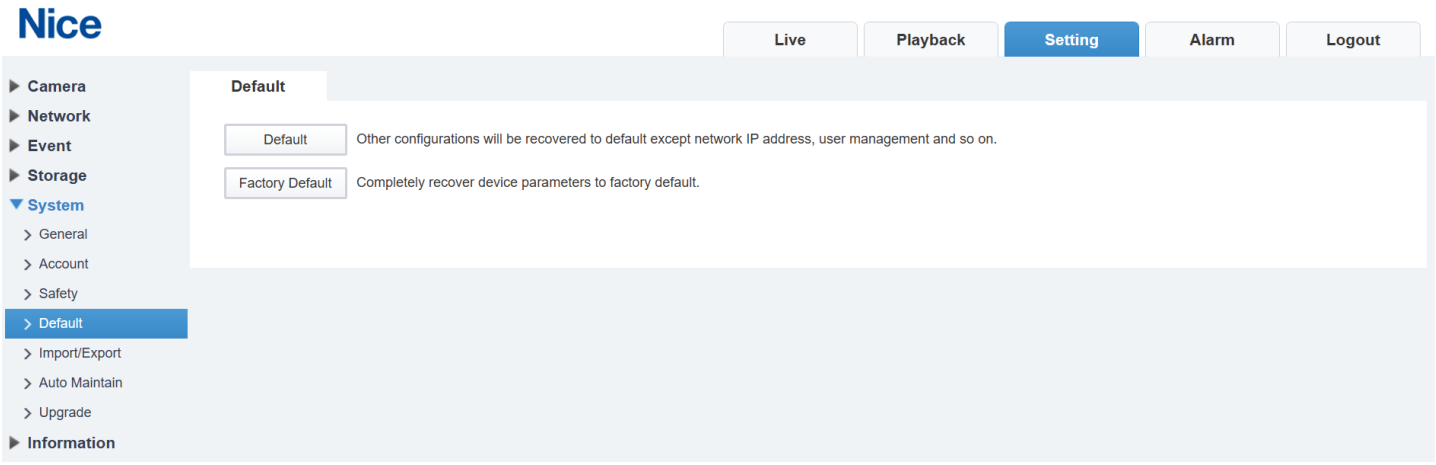

Figure 60: Default section

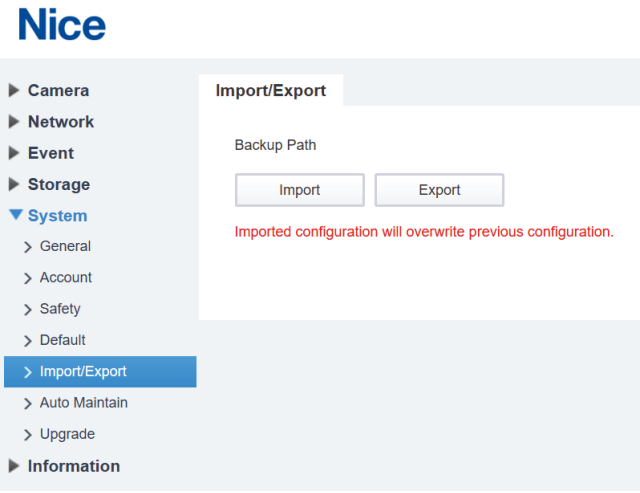

Figure 61: Import/Export section

15.1 - Import

Import system configuration file to make quick configuration or recover system configuration.

Procedure:

1. Go to **Setting > System > Import/Export.**
2. Click **Import**.
3. Select local configuration file, and click **Open** to import the local system configuration file to the system.
4. Click **Save** to finish configuration.

15.2 - Export

Export the system configuration file to back up the system configuration.

Procedure:

1. Go to **Setting > System > Import/Export.**
2. Click **Export**.
3. Select the storage path, and click **Save** to export the system configurationfile to local storage.
4. Click **Save** to finish configuration.

16 AUTO MAINTAIN

You can restart the system manually, and set the time of auto reboot and auto deleting old files. This function is disabled by default.

Procedure:

1. Go to **Setting > System > Auto Maintain.**

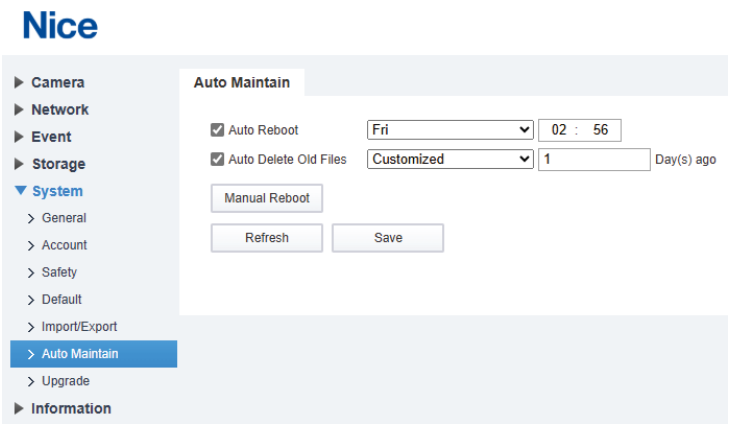

Figure 62: Auto Maintain section

2. Tick the **Auto Reboot** checkbox and set the reboot time. The system restarts automatically as the set time every week.
3. Tick the **Auto Delete Old Files** checkbox and set the time for the system to delete old files automatically. The time range is 1 to 31 days.
4. Click **Save.**

If needed click **Manual Reboot** and then click **OK** to confirm. The camera restarts.

17 UPGRADE

Upgrading to the latest system version can improve camera functions and stability.

Procedure:

1. Go to **Setting > System > Upgrade.**

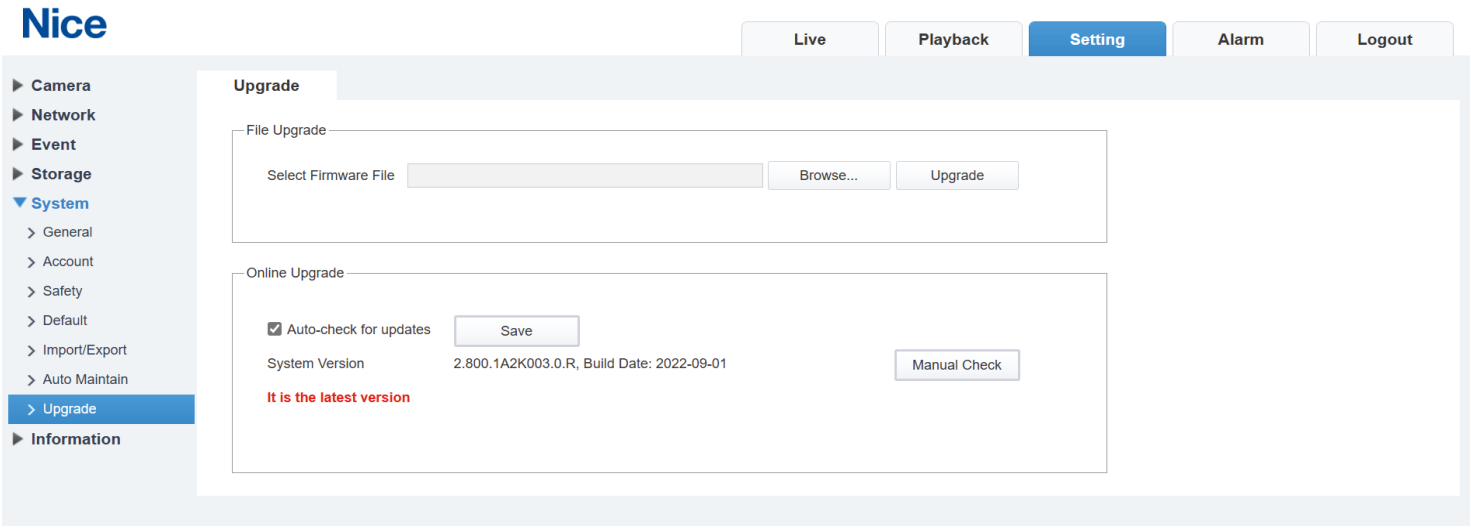

Figure 63: Upgrade section

2. Select upgrading method according to the actual needs:
   - **File Upgrade** - Click **Browse** to upload upgrade file, which should be a .bin file. Click **Upgrade** for the upgrade to start.
   - **Online Upgrade** - Tick the **Auto-check for updates** checkbox. The system checks for upgrade once a day automatically. There is a system notice if any upgrade is available. If there is any upgrade available, click **Upgrade** for the system to start upgrading.
     Click **Manual Check** to check for upgrade manually.

Note

- We need to collect the data such as device name, firmware version, and device serial number to proceed auto-check. The collected information is only used for verifying the legality of cameras and upgrade notice.
- If wrong upgrade file has been used, restart the device; otherwise some functions might not work properly.

18 INFORMATION

18.1 - Version

Go to **Setting > System > Version** to view the following information:

- Device Type
- System Version
- WEB Version
- ONVIF Version
- S/N
- Security Baseline Version

18.2 - Log

You can view and back up logs.

Procedure:

1. Go to **Setting > Information > Log.**

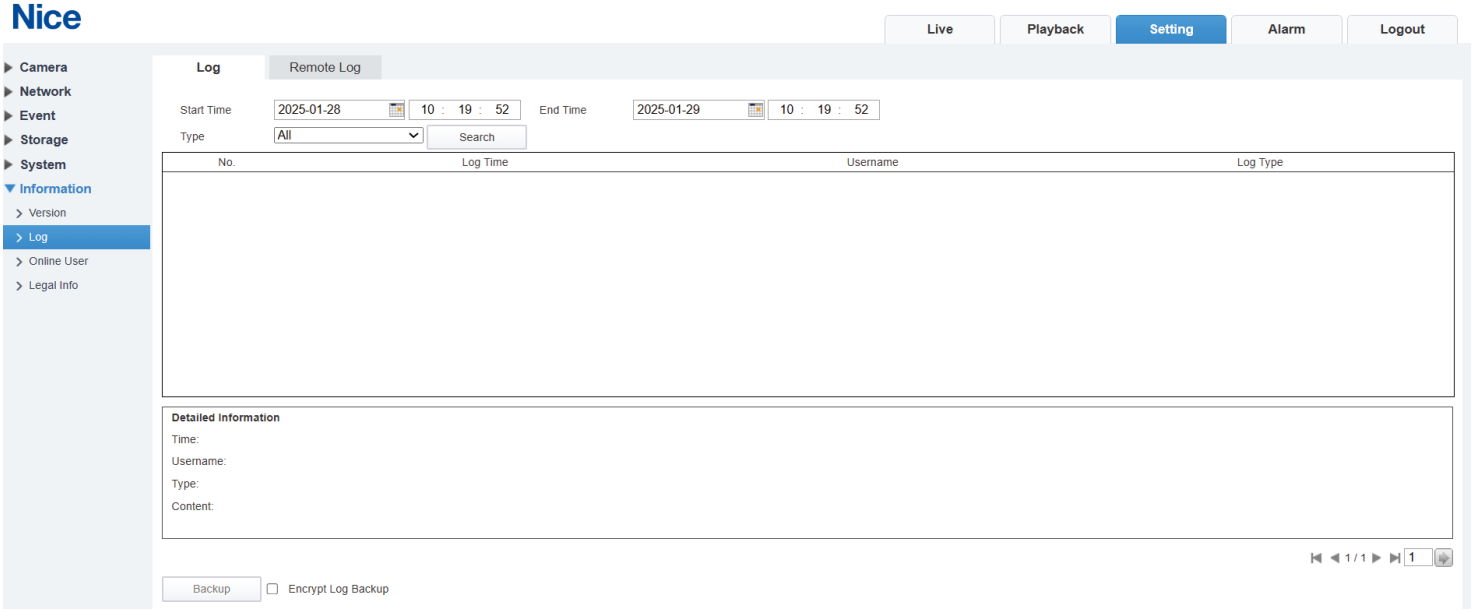

Figure 64: Log section

2. Configure **Start Time** and **End Time.**
3. Select the log type choosing one of the options listed in the table below:

Table 21 - MyEye Bullet and Dome Lite - Log types

Type	Description
All	Searches for all types of logs
System	Includes program start, abnormal close, close, program reboot, device closedown, device reboot, system reboot, and system upgrade
Setting	Includes saving configuration and deleting configuration file
Data	Includes configuring disk type, clearing data, hot swap, FTP state, and record mode
Event	Includes video detection, alarm and abnormality
Record	Includes file access, file access error, and file search
Account	Includes login, logout, adding user, deleting user, modifying user, addinggroup, deleting group, and modifying group
Safety	Includes password resetting and IP filter

4. Click **Search**.
5. Click a chosen log to view the detailed information in **Detailed Information** section.
6. Optionally: click **Backup** to back up all found logs to local PC.

18.3 - Remote Log

Configure remote log, and you can get the related log by accessing the set address.

Procedure:

1. Go to **Setting > Information > Log > Remote Log.**

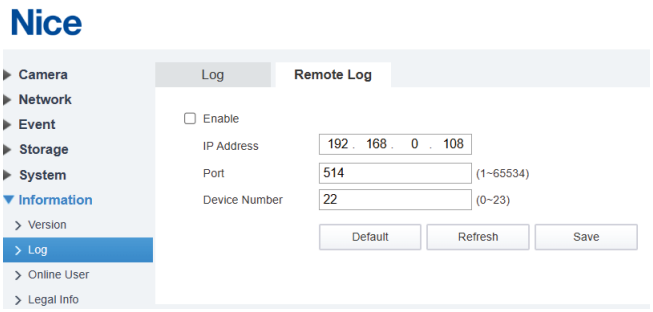

Figure 65: Remote log configuration

2. Tick the **Enable** checkbox to enable remote log function.
3. Set **IP Address, Port** and **Device Number.**
4. Click **Save.**

18.4 - Online User

Go to **Setting > Information > Online User** to view all the current users logging into the camera, their user group, IP address and time of logging in.

18.5 - Legal Info

Go to **Setting > Information > Legal Info** to read Open Source Software Notice.

19 ALARM

You can subscribe alarm event. When a subscribed alarm event is triggered, the system records detailed alarm information at the right side of the interface.

Procedure:

1. Click the **Alarm** tab.

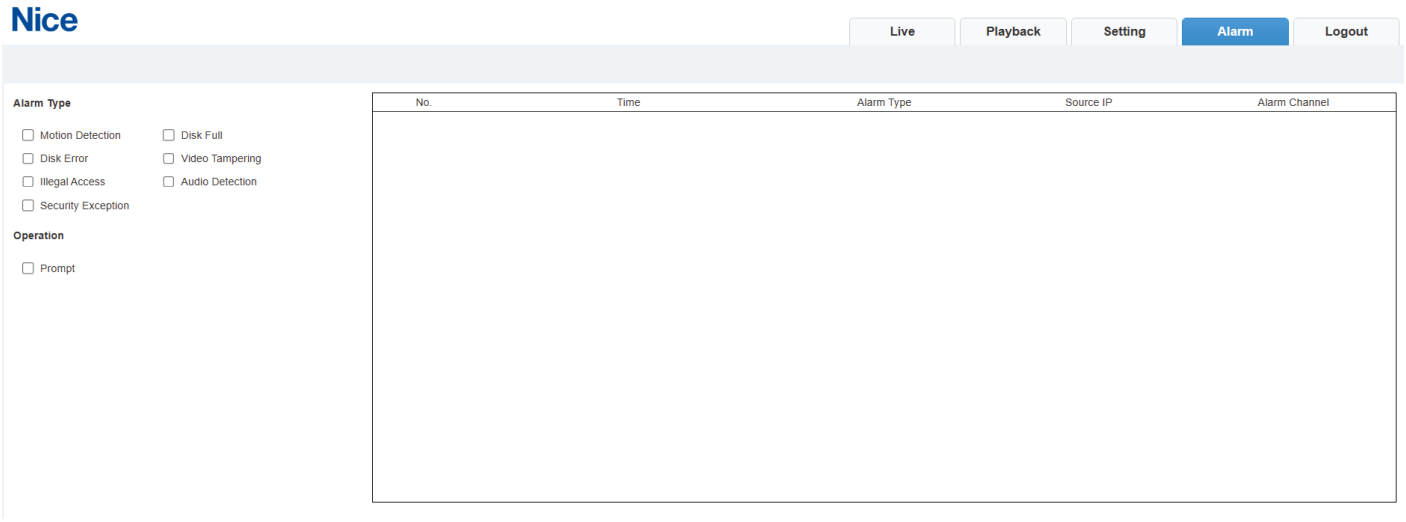

Figure 66: Alarm section

2. Select **Alarm Type**(s) ticking checkboxes next to chosen types from the list below:
   - Motion Detection
   - Disk Error
   - Illegal Access
   - Security Exception
   - Disk Full
   - Video Tampering
   - Audio Detection
3. Tick the **Prompt** checkbox for the system to prompt and record alarm information according to actual conditions.

- When the subscribed alarm event is triggered and the **Alarm** interface isn't displayed, the  icon is displayed on the **Alarm** tab and the alarm information is recorded automatically. Click the **Alarm** tab, and this icon disappears.
- When the subscribed alarm event is triggered and the **Alarm** interface is displayed, the corresponding alarm information is displayed in the alarm list at the right side of the **Alarm** interface.

20 CYBERSECURITY RECOMMENDATIONS

Mandatory actions to be taken towards cybersecurity:

1. Change passwords for strong ones.
   - Create a password longer than 8 characters.
   - Include at least two types of characters: upper and lower case letters, numbers and symbols.
   - Don't contain the account name or the account name in reverse order.
   - Don't use continuous characters, such as 123, abc, etc.
   - Don't use overlapped characters, such as 111, aaa, etc.
2. Update firmware
   As it's a standard procedure in the tech-industry, we recommend keeping the recorder and IP camera firmware up-to-date to ensure the system uses the latest security patches and fixes. When the recorder is connected to the public network, it's recommended to enable the **Auto-check for updates** function to obtain timely information of firmware updates released by the manufacturer. We recommend to download and use the latest version of client software.

“Nice to have” recommendations to improve your network security:

1. Use physical protection
   Place the recorder in a special computer room and cabinet, and implement access control permission and key management to prevent unauthorized people from actions such as damaging hardware or unauthorized connection of of removable device, including a USB flash disk or serial port.
2. Change passwords regularly
   This action reduce the risk of being guessed or cracked.
3. Set and update passwords reset information timely
   The recorder supports password reset function. Set up related information for password reset, including the end user’s mailbox and password protection questions. If the information changes, modify it in time. When setting password protection questions, use those that are difficult to guessed.
4. Enable account lock
   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address are locked.
5. Change default HTTP and other service ports
   We recommend to change default HTTP and other service ports into any set of numbers between 1024 – 65535 to make it more difficult to guess which port you use.
6. Enable HTTPS
   With the HTTPS protocole enabled you visit Web service using a secure communication channel.
7. Bind MAC address
   Binding the IP and MAC address of the hub to the recorder reduces the risk of ARP spoofing.
8. Assign accounts and privileges reasonably
   According to business and management requirements add users reasonably and assign aminimum set of permissions to them.
9. Disable unnecessary services and choose secure modes
   If not needed, turn off services such as SNMP, SMTP, UPnP.
   If necessary, it's highly recommended to use safe modes, including but not limited to the following services:
   - SNMP - Choose SNMP v3, and set up a strong encryption passwords and authentication passwords.
   - SMTP - Choose TLS to access mailbox server.
   - FTP - Choose SFTP, and set up strong passwords.
   - AP hotspot - Choose WPA2-PSK encryption mode, and set up strong passwords.
10. Audio and video encrypted transmission
    The function of encrypted transmission reduces the risk of audio and video data being stolen during transmission.
    Note: Encrypted transmission causes some loss in transmission efficiency.
11. Secure auditing
    - Check online users regularly to see if the recorder is logged in without authorization.
    - Check device log to know the IP addresses that were used to log in to your devices and their key operations.
12. Use network log
    Due to the limited storage capacity of the recorder, the stored log is limited. If you need to save the log for a long time enable the network log function to ensure that the critical logs are synchronized with the network log server for tracing.
13. Construct a safe network environment
    To better ensure the safety of the recorder and reduce potential cyber risks, we recommend:
    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - Partition and isolate the network according to the actual network needs. If there are no communication requirements between two sub networks, it's suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable the IP/MAC address filtering function to limit the range of hosts allowed to access the recorder.

21 REGULATIONS

Warranty

We warrant this product to be free from defects in material and workmanship under normal and proper use for two years from the purchase date of the original purchaser. We will, at its option, either repair or replace any part of the products that prove defective due to improper workmanship or materials. THIS LIMITED WARRANTY DOES NOT COVER ANY DAMAGE TO THIS PRODUCT THAT RESULTS FROM IMPROPER INSTALLATION, ACCIDENT, ABUSE, MISUSE, NATURAL DISASTER, INSUFFICIENT OR EXCESSIVE ELECTRICAL SUPPLY, ABNORMALMECHANICAL OR ENVIRONMENTAL CONDITIONS, OR ANY UNAUTHORIZED DISASSEMBLY, REPAIR OR MODIFICATION. This limited warranty shall not apply if: (i) the product was not used in accordance with any accompanying instructions, or (ii) the product was not used for its intended function. This limited warranty also does not apply to any product on which the original identification information has been altered, obliterated or removed, that has not been handled or packaged correctly, that has been sold as second-hand or that has been resold contrary to Country and other applicable export regulations.

Simplified EU declaration of conformity:

Hereby, Nice SpA Oderzo TV declares that the MyEye Bullet and MyEye Dome are in compliance with Directives 2014/53/EU, 2014/35/EU, 2011/65/EU and 2014/30/EU. The full text of the EU declaration of conformity is available at the following internet address: https://www.niceforyou.com/en/professional-area/download?v=18 under the **download** section.

WEEE Directive Compliance:

Device labelled with this symbol should not be dispo-sed with other household wastes. It shall be handed over to the applicable collection point for the recycling of waste electrical and electronic equipment.

IS0898A00EN_IS0897A00EN_17-02-2025

Nice SpA
Oderzo TV Italia
info@niceforyou.com