

MyEye

Bullet
Dome

CE

IP Smart Bullet Camera

IP Smart Dome Camera

EN - Instructions and warnings for installation and use

1 - IMPORTANT SAFEGUARDS AND WARNINGS	5
1.1 - Privacy protection notice	5
1.2 - About the manual	5
1.3 - Transportation and storage requirements	5
1.4 - Installation requirements	5
1.5 - Operation requirements	5
2 - DEVICE DESCRIPTION	6
3 - CONFIGURATION FLOW	7
4 - DEVICE INITIALIZATION	8
5 - LOGIN	10
5.1 - Device login	10
5.2 - Resetting password	10
6 - HOME PAGE	11
7 - LOCAL	12
8 - CAMERA	13
8.1 - Image	13
8.1.1 - Page layout	13
8.1.2 - AI SSA	14
8.1.3 - Image	14
8.1.4 - WB	15
8.1.5 - Day/Night	16
8.1.6 - Illuminator	16
8.2 - Encode	17
8.3 - Overlay	18
8.3.1 - Privacy Masking	18
8.3.2 - Channel Title	18
8.3.3 - Time Title	19
8.3.4 - Location	19
8.3.5 - Font Properties	19
8.3.6 - Picture Overlay	20
8.3.7 - Custom Title	20
8.4 - Audio	21
8.4.1 - Audio parameters	21
8.4.2 - Alarm Tone	22
9 - NETWORK	23
9.1 - TCP/IP	23
9.2 - Port	24
9.3 - PPPoE	25
9.4 - DDNS	25
9.5 - Email	26
9.6 - UPnP	27
9.7 - SNMP	27
9.8 - Bonjour	29
9.9 - Multicast	29
9.10 - Auto Registration	29
9.11 - QoS	30
9.12 - Platform Access	30
9.12.1 - P2P	30
9.12.2 - ONVIF	30
9.12.3 - RTMP	31
9.13 - Basic Service	31
10 - EVENT	33
10.1 - Alarm Linkage	33
10.1.1 - Adding Schedule	33
10.1.2 - Record Linkage	34
10.1.3 - Snapshot Linkage	34
10.1.4 - Alarm Linkage	34
10.1.5 - Email Linkage	34
10.2 - Subscribing Alarm	34

10.3 - Setting Exception	35
10.3.1 - SD Card Exception	35
10.3.2 - Network Exception	35
10.3.3 - Voltage Exception	36
10.4 - Video Detection	36
10.4.1 - Motion Detection	36
10.4.2 - Video Tampering	37
10.4.3 - Scene Changing	38
10.5 - Audio Detection	39
10.6 - Disarming	39
11 - STORAGE	40
12 - SYSTEM	41
12.1 - Basic	41
12.2 - Date & Time	41
12.3 - Account	41
12.3.1 - User	42
12.3.2 - User Group	43
12.3.3 - ONVIF User	44
12.4 - Manager	45
12.4.1 - Maintenance	45
12.4.2 - Import/Export	45
12.4.3 - Default	46
12.5 - Upgrade	46
13 - SYSTEM INFO	46
14 - LOG	47
14.1 - Logging in system	47
14.2 - Remote Log	47
15 - LIVE	48
15.1 - Live Page	48
15.2 - Encode	48
15.3 - Live View function bar	49
15.4 - Image Adjustment bar	49
15.5 - Image Adjustment	49
16 - AI: IVS	50
17 - SECURITY	51
17.1 - Security Status	51
17.2 - System Service	51
17.2.1 - 802.1x	51
17.2.2 - HTTPS	52
17.3 - Attack Defense	53
17.3.1 - Firewall	53
17.3.2 - Account Lockout	53
17.3.3 - Anti-DoS Attack	54
17.4 - CA Certificate	54
17.4.1 - Creating Device Certificate	54
17.4.2 - Importing third-party CA Device Certificate	55
17.4.3 - Installing existing Device Certificate	55
17.4.4 - Installing Trusted CA Certificate	56
17.5 - A/V Encryption	56
17.6 - Security Warning	57
18 - RECORD	58
18.1 - Search Video	58
18.1.1 - Clipping video	59
18.1.2 - Downloading video	59
18.2 - Record Control	60
18.3 - Time Plan	60
18.4 - Storage	61
18.4.1 - Local Storage	61
18.4.2 - FTP	61
18.4.3 - NAS	62

19 - PICTURE	64
19.1 - Playing back picture	64
19.1.1 - Downloading snapshots	65
19.2 - Setting snapshot parameters	65
19.3 - Setting snapshot plan	66
19.4 - Storage	66
19.5 - Setting upload method	66
20 - CYBERSECURITY RECOMMENDATIONS	67
21 - REGULATIONS	68

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 same quality 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 otherwise specified, to avoid damage to the device.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- The device needs 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 an 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 breaking out.
- Don't block the ventilation opening of the device to avoid heat accumulation.
- Don't walk on or squeeze the line cord and wires, particularly at plugs, power sockets, 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 on the 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.

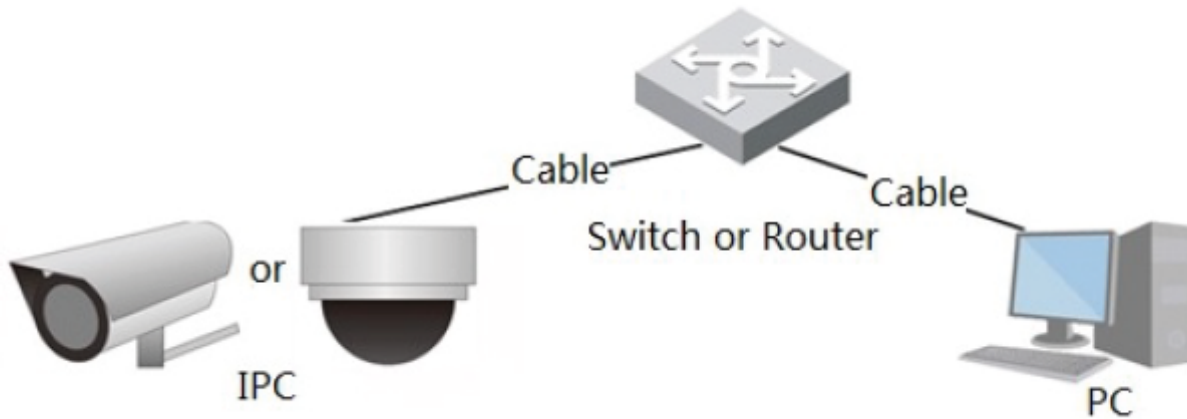


Figure 1: General IPC network

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, video tampering detection and scene changing detection.
When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, 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.
- **IVS**
When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.

3 CONFIGURATION FLOW

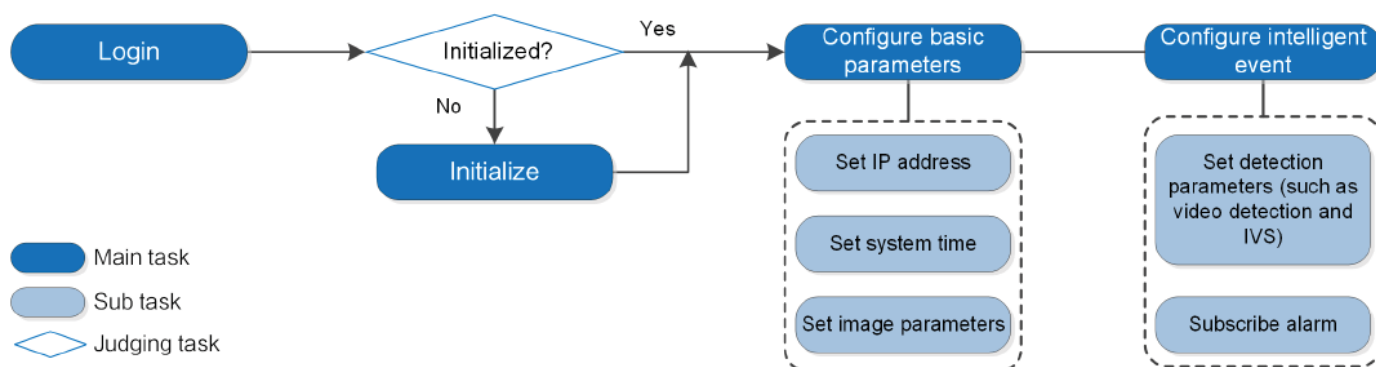


Figure 2: Configuration flow

Table 1 - MyEye Bullet and Dome - 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.	10.2 - Subscribing Alarm
AI	AI rules	Configure IVS.	16 - AI: IVS

4 DEVICE INITIALIZATION

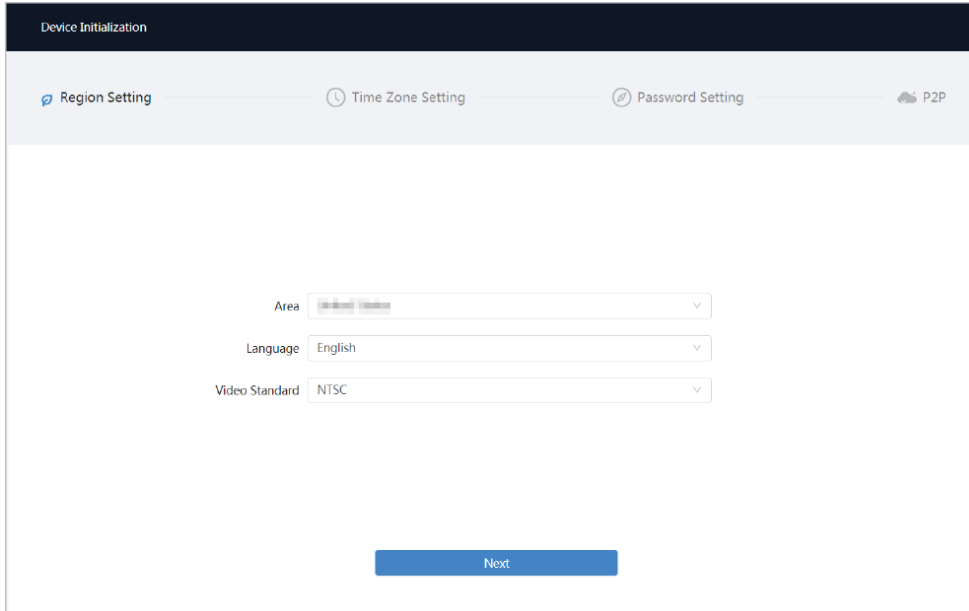
Device initialization is required for the first-time use. This manual is based on the operation on the web page. You can also initialize device using ConfigTool, recorder, or platform devices.

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:

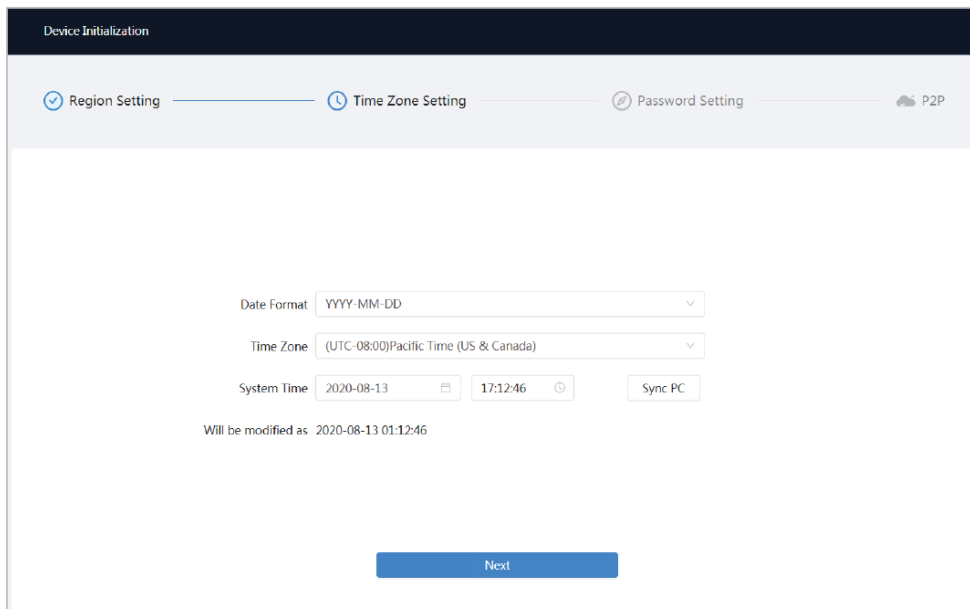
1. Enter the IP address of the device in the web browser and press the Enter key. The IP is **192.168.1.108** by default.
2. Select the area, language, and video standard and click **Next**.



The screenshot shows the 'Device Initialization' web interface. At the top, there's a dark blue header with the title 'Device Initialization'. Below it, a progress bar indicates four steps: 'Region Setting' (active, with a blue checkmark), 'Time Zone Setting', 'Password Setting', and 'P2P'. The main content area has three dropdown menus: 'Area' (set to 'United States'), 'Language' (set to 'English'), and 'Video Standard' (set to 'NTSC'). At the bottom, there is a blue 'Next' button.

Figure 3: Region setting

3. Tick the **I have read and agree to the terms of the Software License Agreement and Privacy Policy** checkbox, and click **Next**.
4. Configure the **Time zone setting**, and click **Next**.



The screenshot shows the 'Device Initialization' web interface at the 'Time Zone Setting' step. The progress bar now shows 'Region Setting' as completed (with a blue checkmark) and 'Time Zone Setting' as the active step. The main content area includes a 'Date Format' dropdown set to 'YYYY-MM-DD', a 'Time Zone' dropdown set to '(UTC-08:00)Pacific Time (US & Canada)', and a 'System Time' section showing '2020-08-13' and '17:12:46' with a 'Sync PC' button. Below this, it says 'Will be modified as 2020-08-13 01:12:46'. At the bottom, there is a blue 'Next' button.

Figure 4: Time zone setting

5. Set the password for admin account.

Device Initialization

✓ Region Setting

✓ Time Zone Setting

✗ Password Setting

P2P

Username admin

New Password

Confirm Password

☒ Reserved Email

For password reset. Recommended or improved in time.

Next

Figure 5: Password setting

Table 2 - MyEye Bullet and Dome - 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	
Reserved email	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.

6. Click **Next**. The P2P page is displayed.

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**.

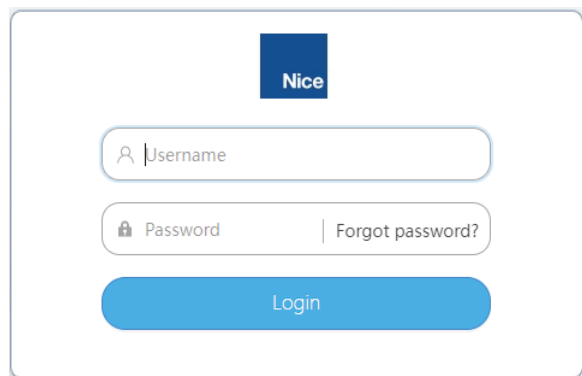
The image shows a login form with a blue header bar containing the word "Nice" in white. Below the header, there is a white input field for the username, preceded by a small person icon. Below the username field is a white input field for the password, preceded by a small lock icon. To the right of the password field is a link that says "Forgot password?". Below these fields is a large blue button with the word "Login" in white text.

Figure 6: Login

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. For more information, see Figure 7.

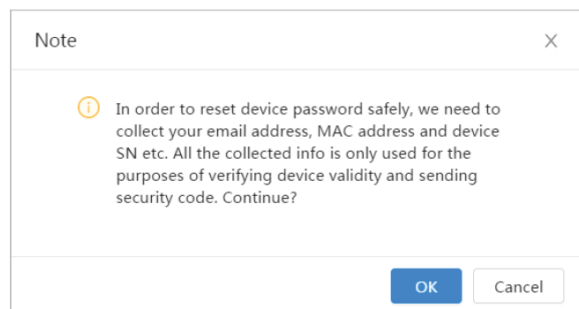
The image shows a "Note" dialog box with a close button (X) in the top right corner. The main text area contains an information icon (i) followed by the text: "In order to reset device password safely, we need to collect your email address, MAC address and device SN etc. All the collected info is only used for the purposes of verifying device validity and sending security code. Continue?". At the bottom of the dialog box, there are two buttons: "OK" and "Cancel".

Figure 7: Note

Click the  icon in the upper-left corner of the page to display the home page.

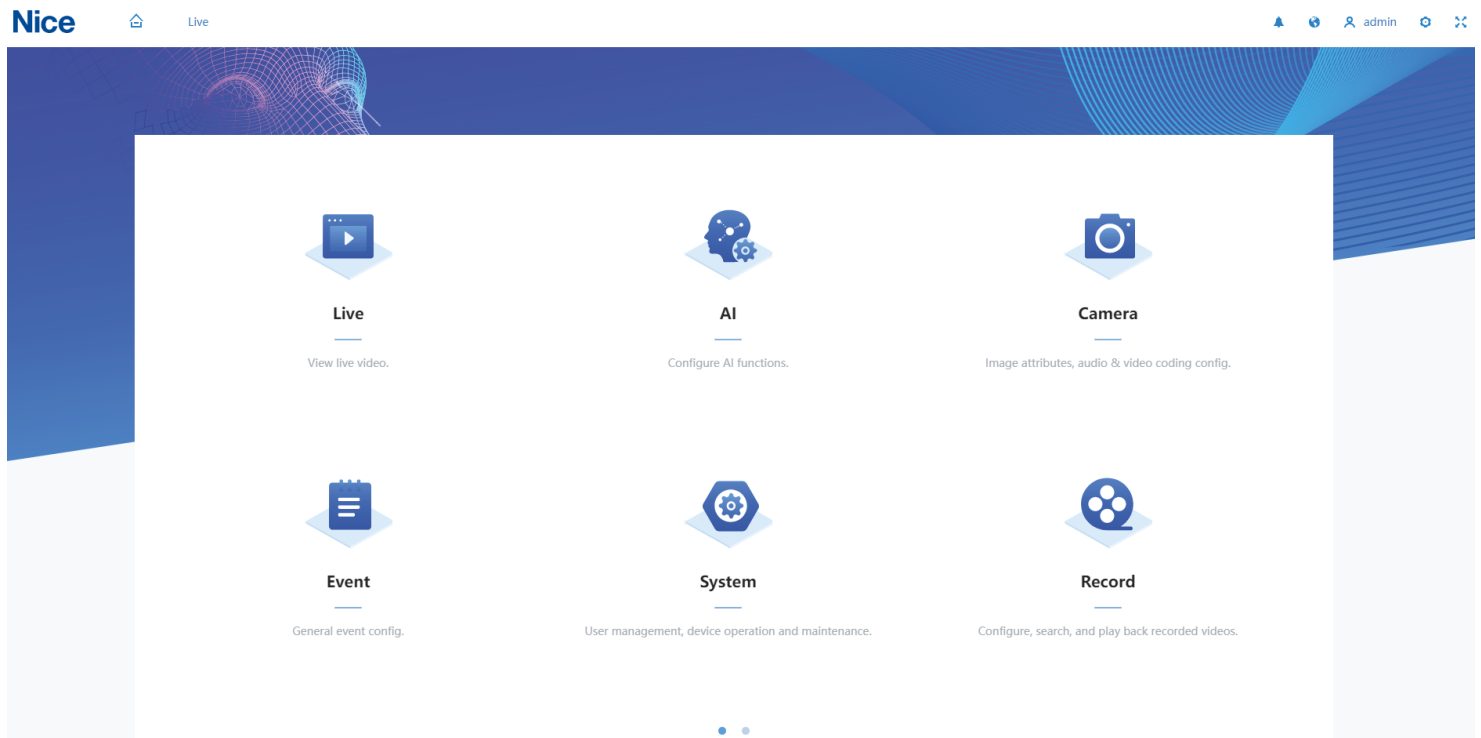


Figure 8: Home page

Home page contains the following sections:

- Live - enabling you to see the real-time monitoring image
- AI - enabling you to configure AI functions of the camera.
- Camera - enabling you to configure camera parameters, such as image parameters, encoder parameters or audio parameters
- Event - enabling you to configure functions such as alarm linkage exception, video detection, and audio detection
- System - enabling you to configure parameters such as date & time, account, safety, default, import/export, auto maintain or upgrade
- Record - enabling you to play back or download recorded video
- Picture - enabling you to play back or download recorded files
- Security - enabling you to check the device security status and set security functions

Right corner of the top bar contains the following icons:

-  Alarm - where you can subscribe alarm and configure other alarm settings
-  Language - where you can choose the language of the interface
-  admin - where you can logout or reboot the system
-  Setting - where you can configure the basic parameters divided into the following sections: Local, Camera, Network, Event, Storage, System, System Info, Log
-  Full screen - where you can enter full screen mode or exit full screen mode

7 LOCAL

In this section you can select protocol and configure the storage path for live snapshot, live record, playback snapshot, playback download, and video clips.

Procedure:

1. Go to  > **Local**.
2. Click **Browse** to select the storage path for live snapshot, live record, playback snapshot, playback download, and video clips.

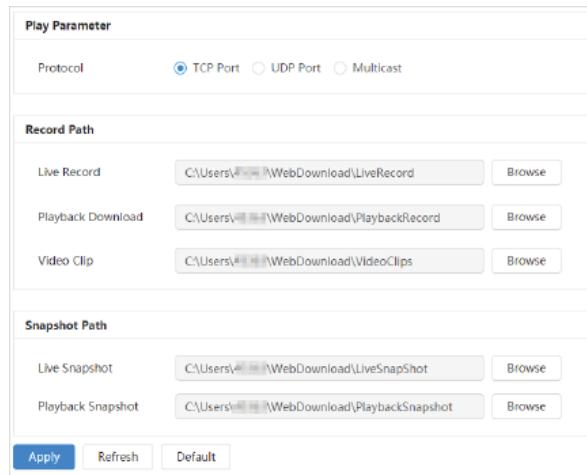


Figure 9: Local section

Table 3 - MyEye Bullet and Dome - Local parameters

Parameter	Description
Protocol	Select the network transmission protocol by ticking one of the options: • TCP • UDP • Multicast Before selecting Multicast , make sure that you have set the Multicast parameters.
Live Record	The recorded video of live page Default path: C:\Users\admin\WebDownload\LiveRecord
Playback Download	The downloaded video of playback page Default path: C:\Users\admin\WebDownload\PlaybackRecord
Video Clips	The recorded video of live page Default path: C:\Users\admin\WebDownload\VideoClips
Live Snapshot	The snapshot of live page Default path: C:\Users\admin\WebDownload\LiveSnapshot
Playback Snapshot	The snapshot of playback page Default path: C:\Users\admin\WebDownload\PlaybackSnapshot

Note

Admin in the paths in the table refers to the account being used

3. Click **Apply** to save the setting.

8.1 - Image

8.1.1 - Page layout

Go to **Camera > Image** to improve the scene clarity, and ensure that surveillance goes properly.

You can select one of the following **Working Modes**:

- **Self-adaptive** - The camera adjusts the image according to the environment.

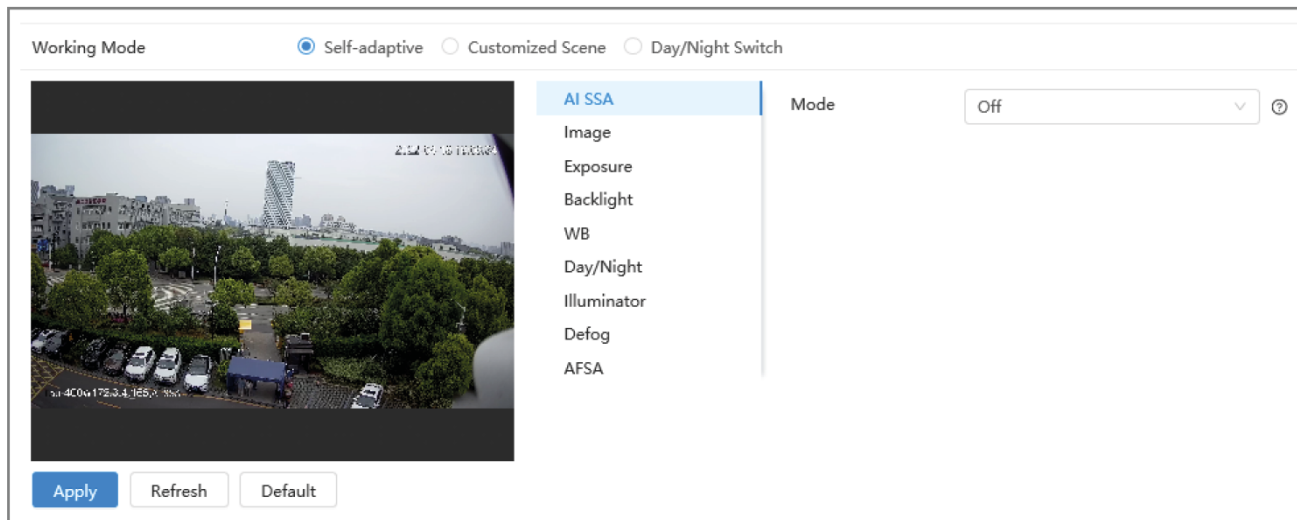


Figure 10: Self-adaptive page layout

- **Customized scene** - You can configure the profile in **Time PlanSetting** by dragging the slide block to set the time. For more information, see Figure 11.

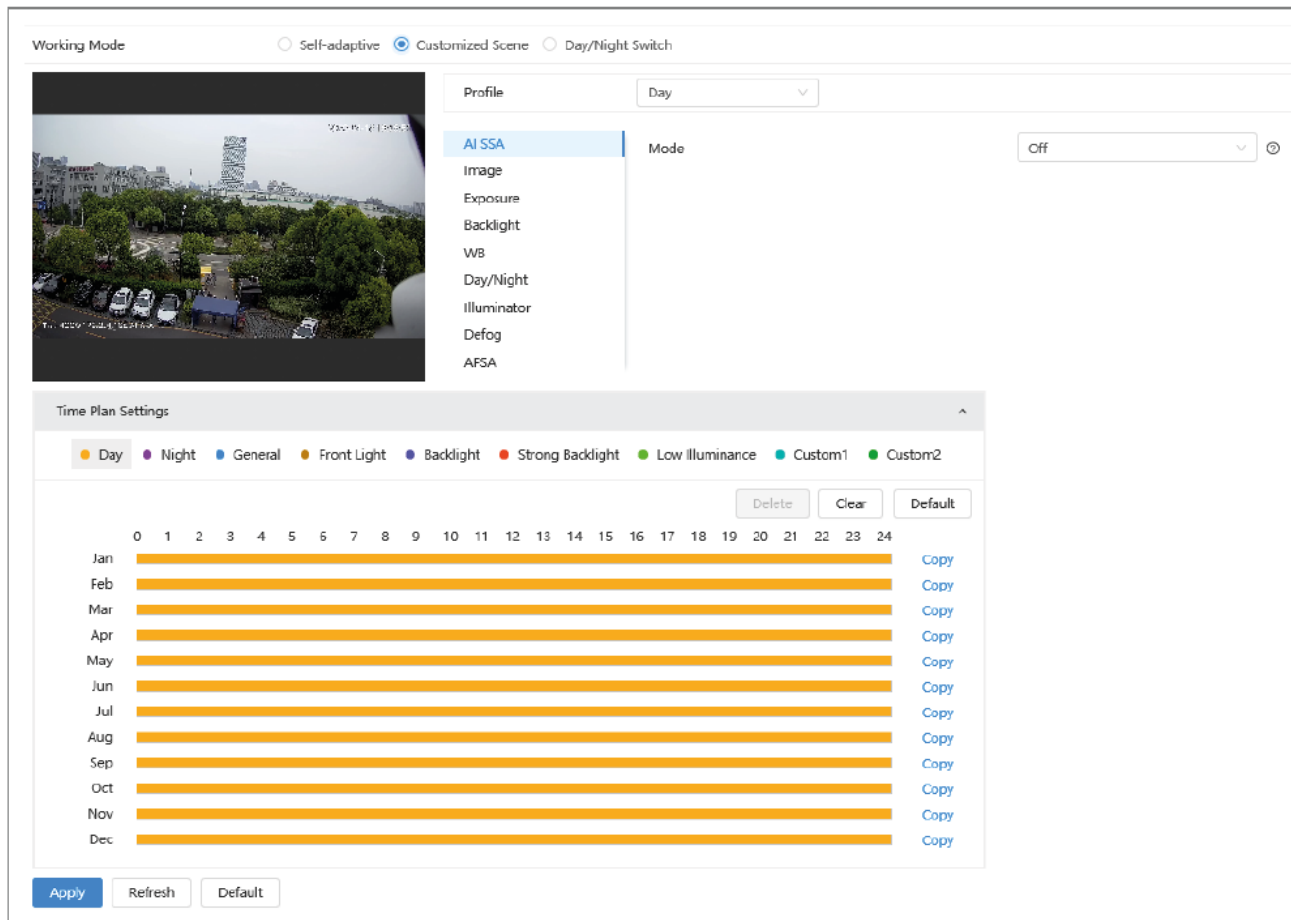


Figure 11: Customized scene page layout

- **Day/night Switch** - In this mode you can configure different settings for day and night.

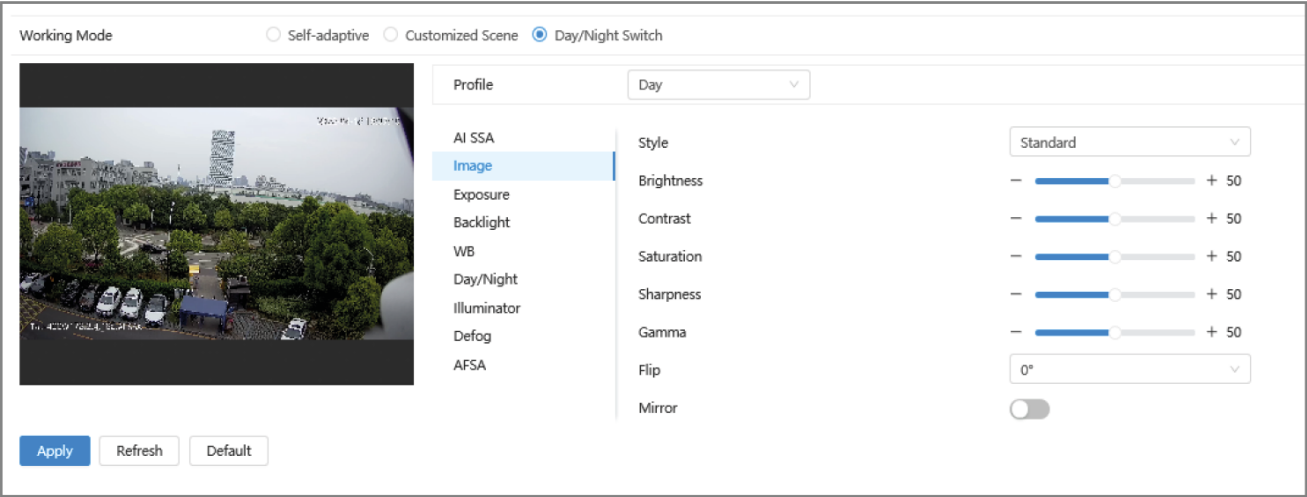


Figure 12: Day/Night Switch page layout

8.1.2 - AI SSA

With AI Scene Self-adaptation (AI SSA) enabled the camera can detect environmental conditions, such as rain, fog, backlight, low light or flicker. The camera adjust the parameters of the image to the conditions to ensure clear images.

Procedure:

1. Go to > **Camera > Image > AI SSA**.
2. Select **On** in the dropdown list.
3. Click **Apply**.

8.1.3 - Image

In this section you can configure picture parameters.

Procedure:

1. Go to > **Camera > Image > Image**.
2. Configure picture parameters listed in the table below.
3. Click **Apply** to save the settings.

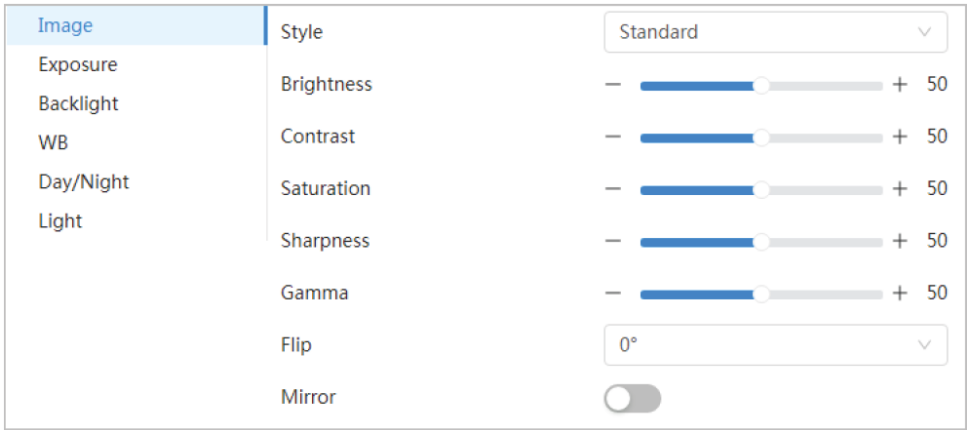


Figure 13: Image settings

8.1.4 - WB

Table 4 - MyEye Bullet and Dome - Image parameters	
Parameter	Description
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.
Flip	Changes the display direction of the picture. You can choose one of the options: • 0° - normal display • 90° - the picture rotates 90° clockwise • 180° - the picture rotates 90° counterclockwise • 270° - the picture flips upside down Note For some models set the resolution to 1080p or lower when using 90° and 180°. For more information, see 8.2 - Encode .
Mirror	Click the  icon for the picture to display with left and right side reversed.

WB function makes the image color display precisely as it is. In WB mode white objects are always displayed white in different environments.

Procedure:

1. Go to  > **Camera > Image > WB**.
2. Select one of the modes from a dro-down-list. Modes are listed in the table below.
3. Click **Apply** to save the settings.

Image	Mode	Auto
Exposure		
Backlight		
WB		
Day/Night		
Light		

Figure 14: WB settings

Table 5 - MyEye Bullet and Dome - WB modes	
WB mode	Description
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.
Custom Area	The system compensates WB only to the set area according to color temperature to ensure color precision.

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  > **Camera** > **Image** > **Day/Night**.

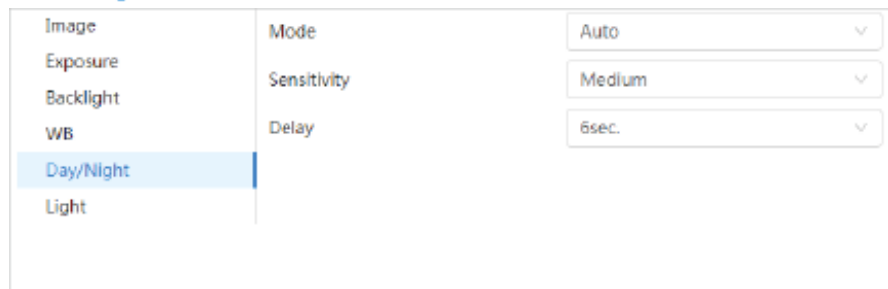


Figure 15: Day and night settings

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

Table 6 - MyEye Bullet and Dome - 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 **Apply** to save the settings.

8.1.6 - Illuminator

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

Procedure:

1. Go to  > **Camera** > **Image** > **Illuminator**.

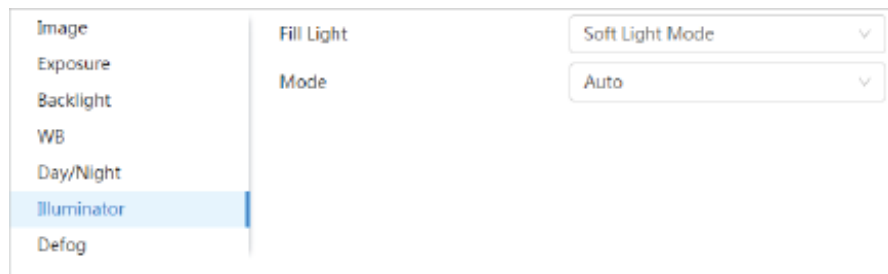


Figure 16: Illuminator settings

2. Configure illuminator parameters listed in the table below.

Table 7 - MyEye Bullet and Dome - Illuminator parameters	
Parameter	Description
Fill Light	Set Fill Light for sound and siren cameras. You can select one of the options: • IR Mode - enables the IR illuminator. The white light is disabled. When an alarm is triggered, the system links the white light. • White Light - enables the white light. The IR illuminator is disabled. • Soft Light Mode - enables IR illuminator and white light adjusting the brightness of the two illuminators to get clear images.
Mode	You can select one of the options: • Manual - Adjust the brightness of illuminator manually. The system supplies illuminator to the image accordingly. • Auto - The system adjusts the illuminator intensity according to the ambient lighting condition. • Zoom Priority - The system adjusts the illuminator intensity automatically according to the change of the ambient light. When the ambient light turns darker, the system turns on the low beam lights first. If the brightness still isn't enough, it turns on the high beam lights. When the ambient light gets brighter, the system dims high beam lights. When the ambient light turns darker the low beam lights. When the focus reaches certain wide angle, the system doesn't turn on high beam light to avoid over-exposure in short distance. If needed, you can configure light compensation manually to fine-tune IRlight intensity. • Off - Illuminator is off.

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

8.2 - Encode

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  > **Camera > Encode > Encode.**

EncodeOverlayROI

ChannelCAM 1

Main Stream

Sub Stream

CompressionH.264H

Smart Codec

Resolution2592*1944(2592x1944)

Frame Rate (FPS)25

Bit Rate TypeCBR

Reference Bit Rate3329-16093 (Kb/s)

Bit Rate6144 (Kb/s)

I Frame Interval50 (25-150)

SVC1(off)

Sub StreamSub Stream 1

CompressionH.264H

Resolution704*576(D1)

Frame Rate (FPS)25

Bit Rate TypeCBR

Reference Bit Rate256-2304 (Kb/s)

Bit Rate512 (Kb/s)

I Frame Interval50 (25-150)

SVC1(off)

Watermark

Watermark StringDigitalCCTV

ApplyRefreshDefault

Figure 17: Encode settings

2. Configure illuminator parameters listed in the table below.

Table 8 - MyEye Bullet and Dome - Encode parameters	
Parameter	Description
Sub Stream	It's enabled by default. If not, click the  button to enable. You can enable multiple sub streams simultaneously.
Compression	• 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. • MJPEG - With this mode, the image requires high bitrate value to ensure clarity. We recommend to set the Reference Bit Rate to the biggest value.
Smart Codec	Click the  button to enable. The function improves video compressibility and saves storage space. With Smart Codec enable, the camera stops supporting the third bit stream.
Output Mode	Select Single Stream or Flex Stream .
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, can only be set when Encode Mode is set to MJPEG • 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.
SVC	Scaled video coding encodes a high quality video bit stream that contains one or more subset bit streams. When sending stream, the system quits some data of related layers according to the network status to improve fluency. • 1 -The default value, which means that there is no layered coding. • 2, 3 and 4 - The layer number that the video stream contains.
Watermark	You can verify the watermark to check if the video has been tampered.
Watermark String	

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

8.3 - Overlay

You can configure overlay settings to be displayed on the Live page.

8.3.1 - Privacy Masking

You can enable this function to protect the privacy of some area of the video image.

You can select the following types of the masking:

- **Color Block** - You can draw triangles and convex quadrilaterals as blocks. You can draw no more than 8 blocks. Their color is black.
- **Mosaic** - You can draw rectangles as blocks with mosaic. You can draw no more than 4 blocks.
- **Color Block + Mosaic** - You can draw no more than 8 blocks

Procedure:

1. Go to **Camera > Encode > Overlay > Privacy Masking**.
2. Click the **Enable** button to **Enable**.
3. Click **Add** and drag the block to the area that you want to cover.
4. Click **Apply**.

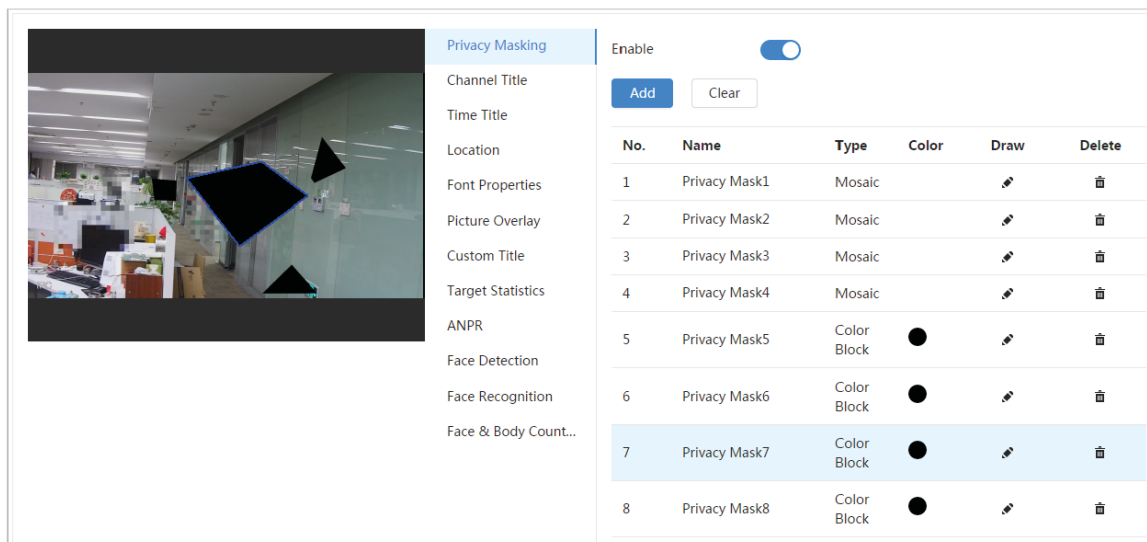


Figure 18: Privacy masking

Related operations

You can:

- View and **edit** the **block** by selecting the privacy masking rule to be edited in the list. The rule is highlighted, and the block frame is displayed in the image. You can edit the selected block as needed, including moving the position, and adjusting the size.
- **Edit the block name** by double-clicking the name in the **Name** column to edit the block name.
- **Delete the block** by clicking the to delete blocks one by one. Click **Clear** to delete all blocks.

8.3.2 - Channel Title

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

Procedure:

1. Go to **Camera > Encode > Overlay > Channel Title**.
2. Click the **Enable** button next to **Enable**.
3. Click the **+** icon to add a channel title no longer than one line.
4. Select **Text Alignment**.
5. Move the title box to the position that you want in the image.
6. Click **Apply**.

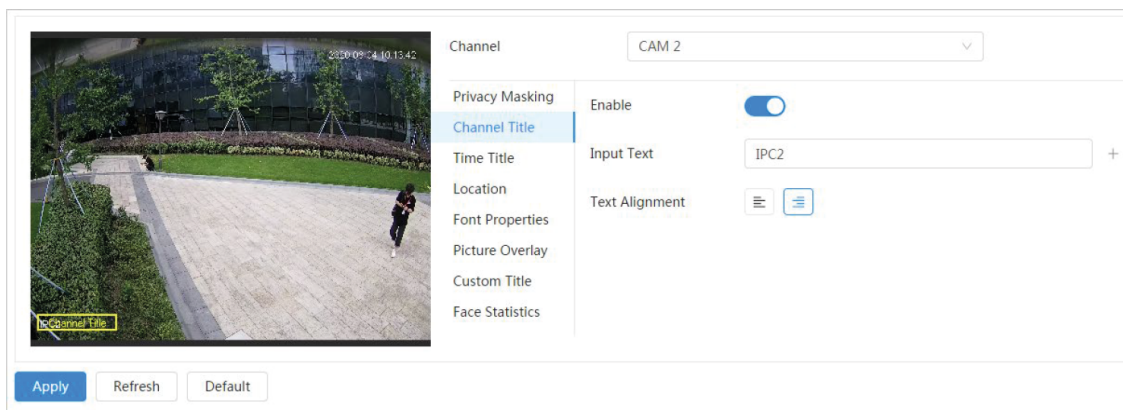


Figure 19: Channel title

8.3.3 - Time Title

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

Procedure:

1. Go to  > **Camera > Encode > Overlay > Time Title**.
2. Click the  button next to **Enable**.
3. Click the  button 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 **Apply**.

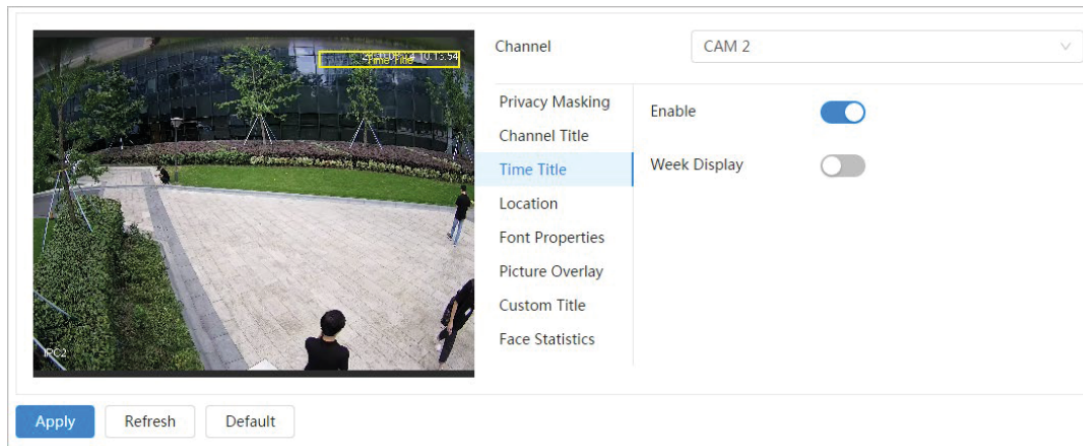


Figure 20: Time Title setting

8.3.4 - Location

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

Note

Text overlay and picture overlay can't work at the same time. IPC connected to a mobile recorder with private protocol displays GPS information as priority.

Procedure:

1. Go to  > **Camera > Encode > Overlay > Location**.
2. Click the  button next to **Enable**.
3. Click the  icon to add a text overlay no longer than 13 lines.
4. Select **Text Alignment**.
5. Move the title box to the position that you want in the image.
6. Click **Apply**.

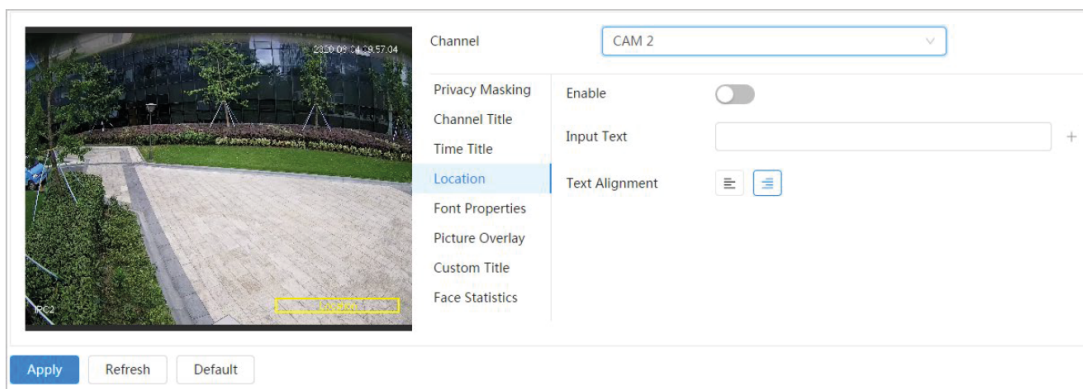


Figure 21: Location setting

8.3.5 - Font Properties

With this function enabled you can adjust the font size in the video image.

Procedure:

1. Go to  > **Camera > Encode > Overlay > Font Properties**.
2. Select the font color and size. You can set the RGB value to customize the font color.
3. Click **Apply**.

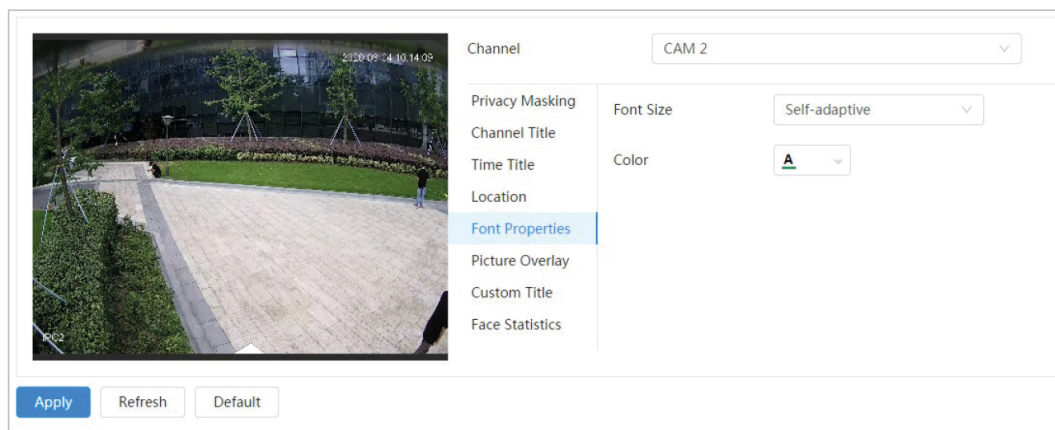


Figure 22: Font Properties

8.3.6 - Picture Overlay

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

Note

Text overlay and picture overlay can't work at the same time.

Procedure:

1. Go to > **Camera > Encode > Overlay > Picture Overlay**.
2. Click the button next to **Enable**.
3. Click **Upload** and select the picture to be overlaid.
4. Move the overlaid picture to the position that you want in the image.
5. Click **Apply**.

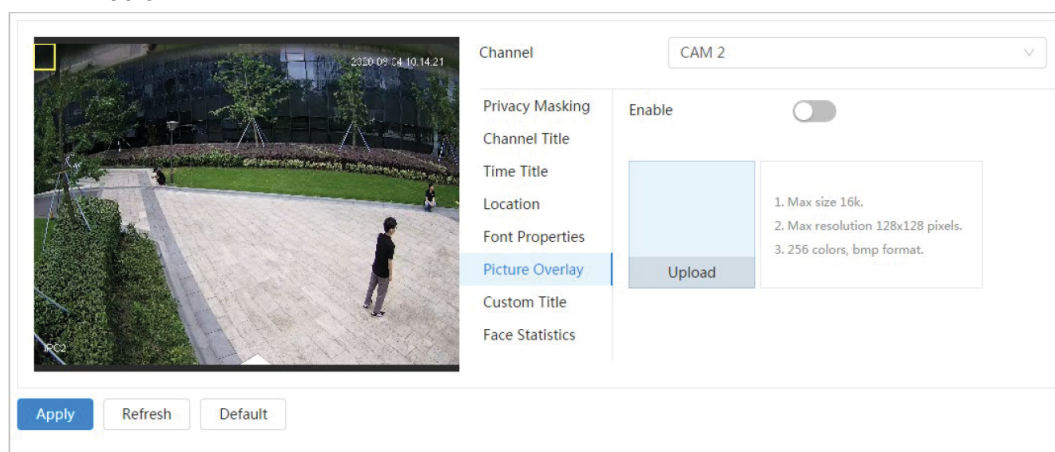


Figure 23: Picture Overlay

8.3.7 - Custom Title

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

Procedure:

1. Go to > **Camera > Encode > Overlay > Custom Title**.
2. Click the button next to **Enable**.
3. Click the to add a text overlay no longer than one line.
4. Select **Text Alignment**.
5. Move the custom box to the position that you want in the image.
6. Click **Apply**.

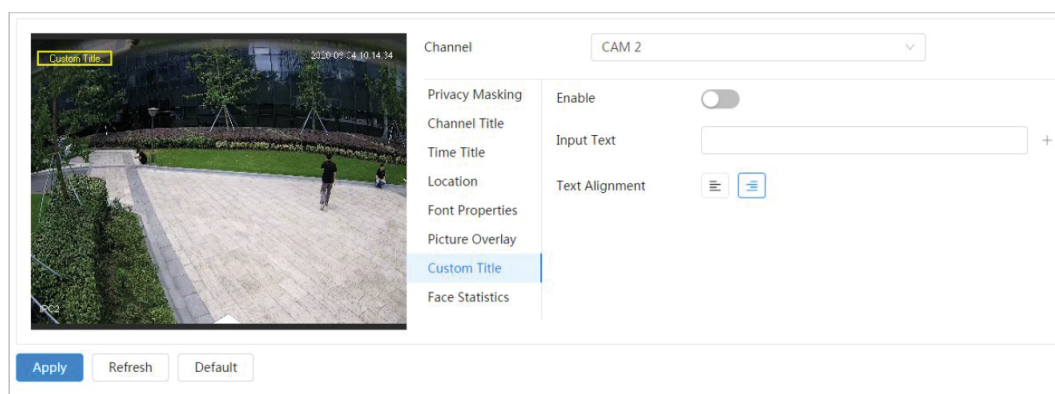


Figure 24: Custom Title

8.4 - Audio

8.4.1 - Audio parameters

Procedure:

- 1. Go to  > **Camera > Audio**.
- 2. Click the  button to **Enable** in **Main Stream** or **Sub Stream**.
For the camera with multiple channels, select the channel number.
Carefully activate the audio acquisition function according to the actual requirements.

Main Stream

Enable



Compression

G.711A

▼

Sampling Frequency

8000

▼

Sub Stream

Enable



Sub Stream

Sub Stream 1

▼

Compression

G.711A

▼

Sampling Frequency

8000

▼

Audio Input Type

LineIn

▼

Noise Filter



Microphone Volume

—

+

50

Speaker Volume

—

+

50

Apply

Refresh

Default

Figure 25: Audio parameters

- 3. Configure audio parameters listed in the table below.

Table 9 - MyEye Bullet and Dome - Audio parameters	
Parameter	Description
Compression	You can set audio Encode Mode selecting one of the following options: • PCM • G.711A • G.711Mu • G.726 • AAC • G.723 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, 32000, 48000, 64000 .
Audio Input Type	You can select one of the following options: • LineIn - requires external audio device. • 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 **Apply** to save the settings.

8.4.2 - Alarm Tone

You can record or upload an alarm audio file. The audio file is played when the alarm is triggered.

Procedure:

- 1. Go to  > **Camera > Audio Tone**.
- 2. Click **Add**.

Add

Record

Upload

File.pcm

Record

Figure 26: Adding alarm tone

- 3. To record an audio file select **Record**, enter the audio name in the input box, and click **Record**. The camera supports recording audio file only in .pcm format.
To record an audio file select **Upload**, click **Browse** to select the audio file, and click **Upload**. You can upload audio files in .pcm, .wav2, .mp3, or .aac format.
- 4. Select the file that you need.

Audio

Alarm Tone

Add

	Name	Play	Download	Edit	Delete
☐	Danger no climbing.wav				
☐	Danger zone keep away.wav				
☐	Deep water be cautious.wav				
☐	No parking here.wav				
☐	Private land no entry.wav				
☐	Sidewalk only no vehicles.wav				
☐	Valuables Don't touch.wav				

Figure 27: Audio tone

Related operations

You can:

- play an audio file by clicking the  icon.
- download an audio file by clicking the  icon.
- edit an audio file by clicking the  icon.
- delete an audio file by clicking the  icon.

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  > **Network** > **TCP/IP**.

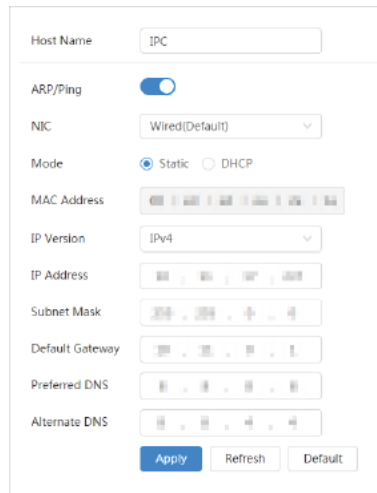


Figure 28: TCP/IP

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

Table 10 - MyEye Bullet and Dome - TCP/IP parameters			
Parameter	Description		
Host Name	Enter the host name no longer than 15 characters		
ARP/Ping	This function is enabled by default. If disabled, click the  button to enable ARP/Ping and set IP address service. Get the camera MAC address to configure the device IP address with ARP/ping command. During restart, you have up to 2 minutes to configure the device IP address by a ping packet of certain length. The server turns off after 2 minutes, or when the IP address is successfully configured. To configure IP address with ARP/Ping: 1. Keep the camera that needs to be configured and the PC in the same local network, and get a usable IP address. 2. Get the MAC address of the camera from device label. 3. Open command editor on the PC and enter the following command. <table border="1"> <tr> <td> Windows syntax <pre>arp -s <IP Address> <MAC> ^ ping -l 480 -t <IP Address> ^</pre> Windows example <pre>arp -s 192.168.0.125 11-40-8c-18-10-11^ ping -l 480 -t 192.168.0.125^</pre> </td><td> UNIX/Linux/Mac syntax <pre>arp -s <IP Address> <MAC> ^ ping -s 480 <IP Address> ^</pre> UNIX/Linux/Mac example <pre>arp -s 192.168.0.125 11-40-8c-18-10-11^ ping -s 480 192.168.0.125^</pre> </td></tr> </table> 4. Restart the camera. 5. Check the PC command line. Information such as Reply from 192.168.0.125...means the configuration has succeeded. 6. Enter http://(IP address) in the browser address bar to log in.	Windows syntax <pre>arp -s <IP Address> <MAC> ^ ping -l 480 -t <IP Address> ^</pre> Windows example <pre>arp -s 192.168.0.125 11-40-8c-18-10-11^ ping -l 480 -t 192.168.0.125^</pre>	UNIX/Linux/Mac syntax <pre>arp -s <IP Address> <MAC> ^ ping -s 480 <IP Address> ^</pre> UNIX/Linux/Mac example <pre>arp -s 192.168.0.125 11-40-8c-18-10-11^ ping -s 480 192.168.0.125^</pre>
Windows syntax <pre>arp -s <IP Address> <MAC> ^ ping -l 480 -t <IP Address> ^</pre> Windows example <pre>arp -s 192.168.0.125 11-40-8c-18-10-11^ ping -l 480 -t 192.168.0.125^</pre>	UNIX/Linux/Mac syntax <pre>arp -s <IP Address> <MAC> ^ ping -s 480 <IP Address> ^</pre> UNIX/Linux/Mac example <pre>arp -s 192.168.0.125 11-40-8c-18-10-11^ ping -s 480 192.168.0.125^</pre>		
NIC	Select the Ethernet 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 MAC address		
IP Version	Select IPv4 or IPv6		
IP Address	When you select Static in Mode , enter needed IP address and subnet mask.		
Subnet Mask	The default gateway needs to be in the same network segment as the IP address.		
Default Gateway	IPv6 doesn't have subnet mask.		
Preferred DNS	IP address of the preferred DNS		
Alternate DNS	IP address of the alternate DNS		

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

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  > **Network > Port.**

Max Connection

(1-20)

TCP Port

(1025-65534)

UDP Port

(1025-65534)

HTTP Port

RTSP Port

RTMP Port

(1025-65534)

HTTPS Port

Apply

Refresh

Default

Figure 29: Ports

2. Configure TCP/IP 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 11 - MyEye Bullet and Dome - 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 **Apply** to save the settings.

Note

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

9.3 - PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is one of the protocols that device uses to connect to the Internet. Get the PPPoE username and password from the Internet service provider to set up network connection through PPPoE. The camera acquires a WAN dynamic IP address.

Procedure:

1. Connect the camera to the network.
2. Go to  > **Network > PPPoE**.

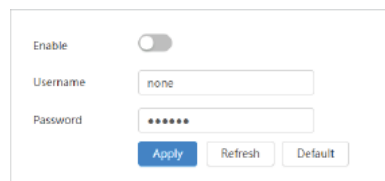


Figure 30: PPPoE

3. Click the  button next to **Enable** and enter a username and password.

Note

- Disable UPnP while using PPPoE to avoid possible influence.
- With the PPPoE connection enabled, the device IP address can't be modified through the web page.

4. Click **Apply**.

The success prompt box is displayed, and the real-time WAN IP address is displayed. You can access camera through the IP address.

9.4 - DDNS

Properly configure DDNS and the domain name on the DNS server matching your IP address enables you to visit the camera with the same domain name no matter how the IP address changes. The matching relation refreshes in real time.

Third party server might collect your device information after DDNS is enabled.

Register and log in to the DDNS website to view the information of all the connected devices in your account.

Procedure:

1. Connect the camera to the network.
2. Go to  > **Network > DDNS**.

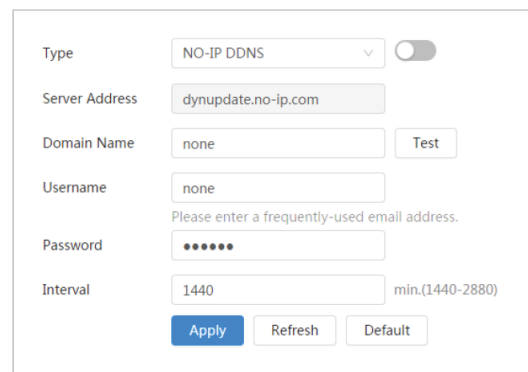


Figure 31: DDNS

3. Click the  button to enable the function.
4. Configure DDNS parameters listed in the table below.

Table 12 - MyEye Bullet and Dome - DDNS parameters	
Parameter	Description
Type	Before configuration, check the type of DNS server supported by the camera.
Server Address	The name and web address of the DDNS service provider, see the matching relationship below: • CN99 DDNS web address: www.3322.org • NO-IP DDNS web address: dynupdate.no-ip.com • Dyndns DDNS web address: members.dyndns.org
Domain Name	The domain name you registered on the DDNS website
Test	Only when selecting NO-IP DDNS type, you can click Test to check if the domain name registration is successful.
Username	Enter the username and password obtained from DDNS service provider. You need to register the username, password and other information on the website of DDNS service provider.
Password	
Interval	The update cycle of the connection between the device and the server. Ten minutes is the default time.

5. Click **Apply** to save the settings.
6. In the web browser enter domain name at the address bar and press **Enter**. The login page is displayed.

9.5 - Email

You can configure email parameter and enable email linkage. The system sends email to the defined address when the corresponding alarm is triggered.

Procedure:

1. Go to  > **Network > Email.**

Enable

☒

SMTP Server

smtp.gmail.com

Port

587

Anonymous

☐

Username

Password

.....

Sender

Encryption Type

TLS(Recommended)

Subject

IPC Message

☒ Attachment

Device Name

Event Type

Receiver

Add

Test

Health Mail

☐

Sending Interval

30

min (30-1440)

Apply

Refresh

Default

Figure 32: Email setting

2. Click the  button next to **Enable**.
3. Configure Email parameters listed in the table below.

Table 13 - MyEye Bullet and Dome - Email parameters	
Parameter	Description
SMTP Server	SMTP server address: smtp.gmail.com
Port	The port number of the SMTP server. • 465 for SSL • 587 for TLS
Username	The account of SMTP server
Password	The password of SMTP server
Anonymous	Click the  button for the sender's information not to be displayed in the email.
Sender	Enter the sender's email address
Subject	You can enter up to 64 characters using Chinese, English and Arabic numerals. Click the  icon to select title type, including Device Name , Device ID , and Event Type . You can set maximum 2 titles.
Attachment	Tick the check box to support attachment in the email.
Receiver	Receiver's email address; supports 3 addresses at most After entering the receiver's email address, the Test button is display. Click Test to check if the emails can be sent and received successfully.
Health Mail	The system sends test mail to check if the connection is configured successfully. Click the  button and configure Sending Interval for the system to send test mail according to the set intervals.

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

9.6 - UPnP

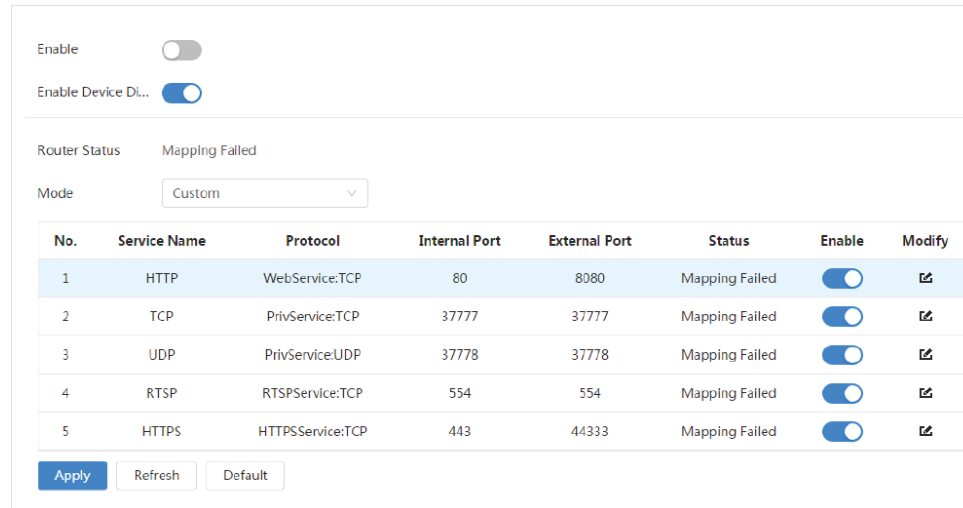
Universal Plug and Play (UPnP) is a protocol that establishes mapping relation between local area and wide area networks. This function enables you to access local area device through wide area IP address.

Before starting the procedure:

- Make sure the UPnP service is installed in the system.
- Log in the router, and configure WAN IP address to set up the Internet connection.
- Enable UPnP in the router.
- Connect your device to the LAN port of the router.
- Go to  > **TCP/IP, in IP Address** and enter the local area IP address of the router or select DHCP and acquires IP address automatically.

Procedure:

1. Go to  > **Network > UPnP**.



No.	Service Name	Protocol	Internal Port	External Port	Status	Enable	Modify
1	HTTP	WebService:TCP	80	8080	Mapping Failed	☒	
2	TCP	PrivService:TCP	37777	37777	Mapping Failed	☒	
3	UDP	PrivService:UDP	37778	37778	Mapping Failed	☒	
4	RTSP	RTSPService:TCP	554	554	Mapping Failed	☒	
5	HTTPS	HTTPSService:TCP	443	44333	Mapping Failed	☒	

Figure 33: UPnP

2. Click the  button next to **Enable**.
3. Select the mapping mode
 - **Custom** - Click the  icon to change external port as needed
 - **Default** - The system finishes mapping with unoccupied port automatically. You can't edit mapping relation.
4. Click **Apply** to save the settings.
5. In the web browser enter enter http:// wide area IP address: external port number, and press **Enter** to visit the local area device with corresponding port.

9.7 - SNMP

Simple Network Management Protocol (SNMP) can be used to enable software such as MIB Builder and MG-SOFT MIB Browser used for managing and monitoring the camera.

Before starting the procedure:

- Install an SNMP monitoring and managing tool such as MIB Builder and MG-SOFT MIB Browser.
- Get the MIB file of the matched version from technical support.

Procedure:

1. Go to  > **Network > UPnP**.
2. Select SNMP version to enable SNMP.
 - **V1** - The system can only process information of V1 version.
 - **V2** - The system can only process information of V2 version.
 - **V3** - V1 and V2 become unavailable. You can configure username, password and authentication type. It requires corresponding username, password and authentication type to visit your device from the server. **V3** is recommended, because V1 and V2 might cause data leakage.

The image shows a web-based configuration interface for SNMP. It is divided into two main sections. The top section is for general SNMP settings, and the bottom section is for user authentication and encryption. In the top section, 'Version' is set to 'V3(Recommended)', 'SNMP Port' is '161', 'Read Community' is 'public', 'Write Community' is empty, 'Trap Address' is empty, and 'Trap Port' is '162'. In the bottom section, 'Read-Only Userna...' is 'public', 'Authentication Type' is 'MD5', 'Authentication Pa...' is masked with dots, 'Encryption Type' is 'CFB-AES', and 'Encryption Passwo...' is masked with dots. At the bottom of the interface are three buttons: 'Apply', 'Refresh', and 'Default'.

Figure 34: SNMP

3. In **Trap Address** enter the IP address of the PC that has MIB Builder or MG-SOFT MIB Browser installed, and leave other parameters to the default.

Table 14 - MyEye Bullet and Dome - SNMP parameters	
Parameter	Description
Version	Tick the checkbox of SNMP version that you are using. The recommended version is V3 .
SNMP Port	The listening port of the software agent in the device
Read Community	The read and write community string that the software agent supports. You can enter number, letter, underline and dash to form the name.
Write Community	
Trap Address	The target address of the Trap information sent by the software agent in the device
Trap Port	The target port of the Trap information sent by the software agent in the device
Read-Only Username	Set the read-only username accessing device; it's public by default You can enter number, letter, and underline to form the name.
Read/Write Username	Set the read/write username access device; it's private by default You can enter number, letter, and underline to form the name.
Authentication Type	Select MD5 or SHA . The default type is MD5 .
Authentication Password	Enter the password for authentication. The password should be no less than eight characters.
Encryption Type	Select an encryption type. The default setting is CBC-DES .
Encryption Password	Enter the encryption password. The password should be no less than eight characters.

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

When the procedure is finished, you can:

- view device configuration through MIB Builder or MG-SOFT MIB Browser.
- compile the two MIB files with MIB Builder.
- load the generated modules with MG-SOFT MIB Browser.
- enter the IP address of the device you need to manage in the MG-SOFT MIB Browser and select version to search.
- unfold all the tree lists displayed in the MG-SOFT MIB Browser to view the configuration information, video channel amount, audio channel amount, and software version.
- disable SNMP Trap service using Windows operating system. The MG-SOFT MIB Browser displays prompt when alarm is triggered.

9.8 - Bonjour

Enable this function for OS and clients supporting Bonjour so that cameras can be found automatically. You can visit to cameras using Safari browser.

Procedure:

- 1. Go to  > **Network > Bonjour**.

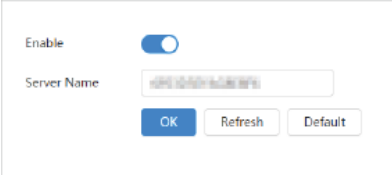


Figure 35: Bonjour

- 2. Bonjour should be enabled by default. If not, click the  button next to **Enable**.
- 3. Enter **Server Name**.
- 4. Click **OK**.
- 5. Click **Show All Bookmarks** in Safari browser.
- 6. Enable **Bonjour**. The OS or client detects automatically the network cameras with Bonjour enabled in the LAN.
- 7. Click the camera to visit the corresponding web page.

9.9 - 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  > **Network > Multicast**.

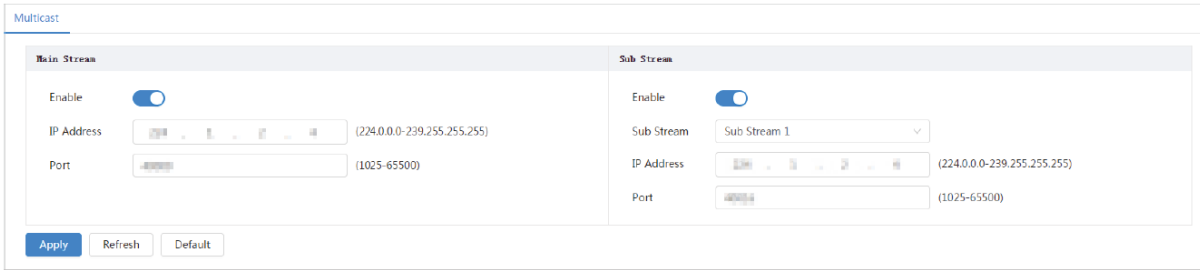


Figure 36: Multicast

- 2. Click the  button next to **Enable**.
- 3. Enter **IP 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**, for **Sub Stream1** - **40016**, and for **Sub Stream2** - **40032**. The range is 1025 – 65500.
- 5. Click **Apply**.
- 6. On the **Live** page, select **RTSP** in **Multicast** to view the video image with multicast protocol.

9.10 - Auto Registration

With this function enabled, when the camera is connected in the Internet, it reports the current location to the specified server which acts as the transit to make it easier for the client software to access the camera.

Procedure:

- 1. Go to  > **Network > Auto Registration**.



Figure 37: Auto Registration

- 2. Click the  button next to **Enable** and configure parameters listed in the table below.

Table 15 - MyEye Bullet and Dome - Auto Registration parameters	
Parameter	Description
Server Address	The IP address or domain name of the server to be registered
Port	The port for registration
Sub-Device ID	The custom ID for the camera

- 3. Click **Apply**.

9.11 - QoS

You can solve problems such as network delay and congestion with this function. It helps to assure bandwidth, reduce transmission delay, packet loss rate, and delay jitter to improve experience.
0-63 means 64 degrees of priority; 0 for the lowest and 63 the highest.

Procedure:

- 1. Go to  > **Network > QoS**.

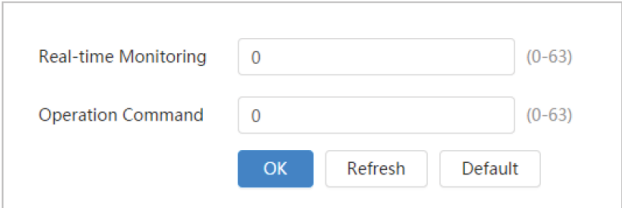


Figure 38: QoS

- 2. Enter the value from 0 to 63 in **Real-time Monitor** to configure the priority of the data packets used for network surveillance. 0 for the low-est and 63 the highest.
- 3. Enter the value from 0 to 63 in **Operation Command** to configure the priority of the data packets that used for configure or checking.
- 4. Click **OK**.

9.12 - Platform Access

9.12.1 - P2P

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  > **Network > Platform Access > 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.

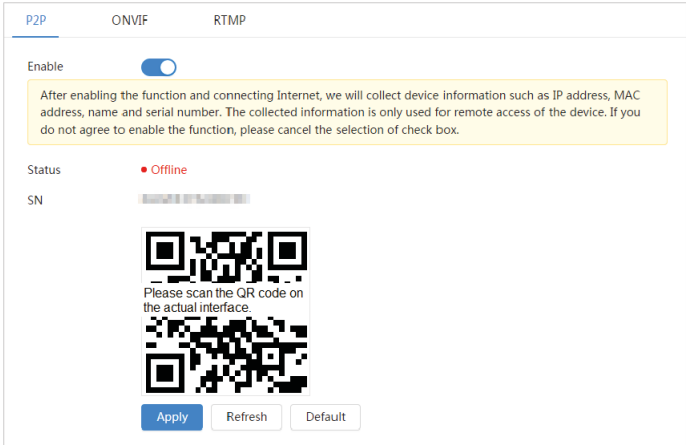


Figure 39: P2P

- 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.

9.12.2 - ONVIF

The ONVIF verification is **enabled by default**, which allows the network video products, such as video recording device, from other manufactur-ers to connect to your device.

Procedure:

- 1. Go to  > **Network > Platform Access > ONVIF**.
- 2. Click the  button next to **ONVIF Verification**.
- 3. Click **Apply**.

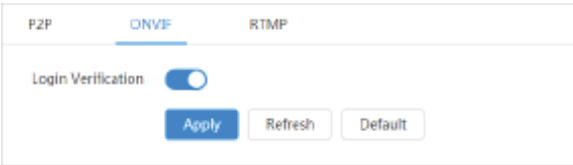


Figure 40: ONVIF

9.12.3 - 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  > **Network > Platform Access > RTMP**.
- 2. Click the  button next to **Enable**.

Note
Make sure that the IP address is trustable when enabling RTMP.

P2P

ONVIF

RTMP

Enable



Stream Type

☒ Main Stream

☐ Sub Stream 1

☐ Sub Stream 2

Address Type

☒ Non-custom

☐ Custom

IP Address

Port

(0-65535)

Custom Address

Apply

Refresh

Default

Figure 41: RTMP

- 3. Configure RTMP parameters listed in the table below.

Table 16 - MyEye Bullet and Dome - 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.
Port	• IP address - support IPv4 or domain name. • Port - keep the default value.
Custom Address	When selecting Custom , you need to enter the path allocated by the server.

- 4. Click **Apply**.

9.13 - Basic Service

To enhance network and data security configure the IP hosts (devices with IP address) that are allowed to visit the device. Only the hosts in the trusted sites list can log into the webpage.

Procedure:

- 1. Go to  > **Network > Basic Service**.

SSH



Multicast/Broadc...



CGI



ONVIF



Genetec



Mobile Push Noti...



Private Protocol A...

Security Mode (Recommen...

▼

Apply

Refresh

Default

Figure 42: Basic service

2. Enable the basic service listed in the table below according to the actual needs.

Table 17 - MyEye Bullet and Dome - Basic Service parameters	
Function	Description
SSH	Used to perform safety management
Multicast/Broadcast Search	With this function enabled multiple users viewing the device video image simultaneously through network can find your device with multicast/broadcast protocol.
CGI	With these functions enabled other devices can access the camera. These functions are enabled by default.
ONVIF	
Genetec	
Mobile Push Notification	With this function enabled the system sends the snapshot taken when alarm is triggered to your phone. This function is enabled by default.
Private Protocol Authentication Mode	Select the authentication mode from Security Mode and Compatible Mode . Security Mode is recommended.

3. Click **Apply**.

10.1 - Alarm Linkage

When an alarm is triggered by the device connected to the alarm-in port, the system performs the defined alarm linkage.

Procedure:

1. Go to  > **Event > Alarm**.
2. Click the  button next to **Enable**.

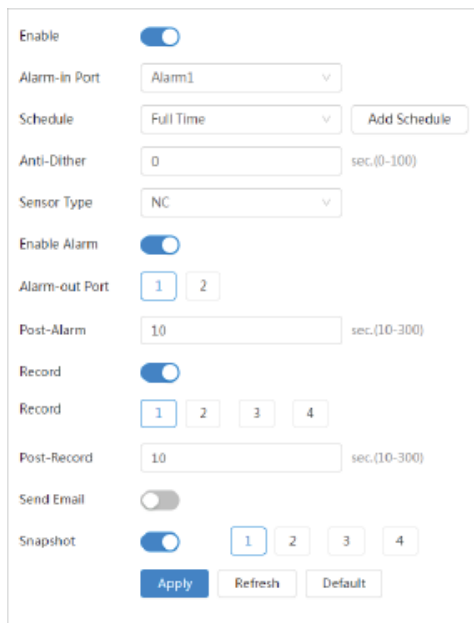


Figure 43: Alarm linkage

3. Select **Alarm-in Port**.
4. Select **Sensor Type** choosing NO or NC.
5. Set **Anti-Dither** period. Only one record alarm is possible during one the anti-dither period.
6. Select **Schedule**, Arming Periods and **Alarm Linkage Action**. If the schedules can't meet the scene requirement, you can click **Add Schedule** to add new schedule. For more information, see 10.1.1 - Adding Schedule.
7. Click **Apply**.

10.1.1 - Adding Schedule

Set arming periods. The system only performs corresponding linkage action in the configured period.

Procedure:

1. Go to  > **Event > Alarm**.
2. Click **Add Schedule** next to **Schedule**.

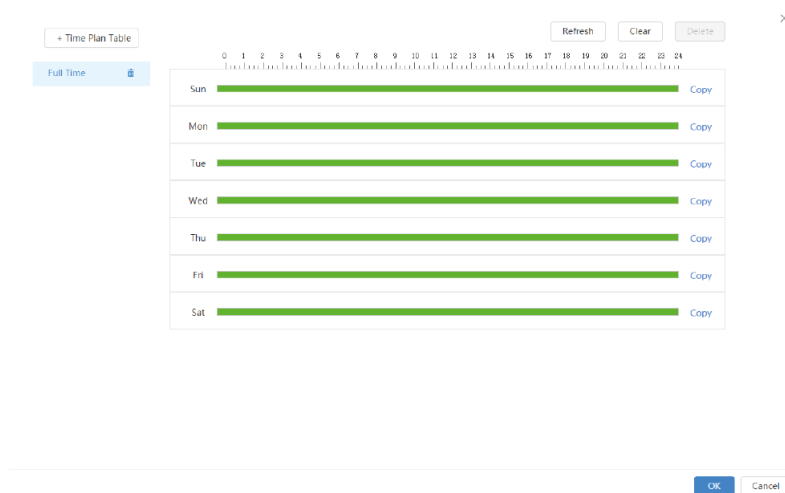


Figure 44: Schedule

3. Press and drag the left mouse button on the timeline to set arming periods. Alarms is triggered in the period in green on the timeline. Click **Copy** next to a day, and select the days that you want to copy configuration to. Tick the **Select All** check box to select all days to copy the configuration. You can set 6 periods per day.
4. Optional: click **+Time Plan Table** to add a new time plan table. Double-click the table name to edit it. Click the  icon to delete the table as needed.
5. Click **OK**.

10.1.2 - Record Linkage

The system can link record channel when an alarm event occurs. After an alarm stops the system keeps recording for an extended period set in the **Post-Record** parameter.

With the corresponding alarm type (**Normal**, **Motion**, or **Alarm**) is enabled, the record channel links recording. For more information, see [18.3 - Time Plan](#).

Enable auto record mode for the record linkage to take effect. For more information, see [18.2 - Record Control](#).

Procedure:

1. Go to  > **Event > Alarm**.
2. Click the  button next to **Record** to enable record linkage.
3. Set the **Post-Record** time.

10.1.3 - Snapshot Linkage

With snapshot linkage configured, the system takes snapshots automatically when an alarm is triggered.

With the corresponding alarm type (**Normal**, **Motion**, or **Alarm**) is enabled, the record channel links snapshots. For more information, see [18.3 - Time Plan](#).

Procedure:

1. Go to  > **Event > Alarm**.
2. Click the  button next to **Snapshot**.

10.1.4 - Alarm Linkage

When an alarm is triggered, the system can link automatically with alarm-out device.

Procedure:

1. Go to  > **Event > Alarm**.
2. Click the  button next to **Enable Alarm** to enable alarm-out linkage.
3. Select **Alarm-out Port**.
4. Set the **Post-Alarm** time for alarm to continue for an extended period after the event ends.

10.1.5 - Email Linkage

When an alarm is triggered, the system send automatically an email to users. Email linkage takes effect only when SMTP is configured. For more information, see [9.5 - Email](#).

Procedure:

1. Go to  > **Event > Alarm**.
2. Click the  button next to **Send Email**.

10.2 - Subscribing Alarm

Table 18 - MyEye Bullet and Dome - Description of alarm types		
Alarm Type	Description	Preparation
Motion Detection	The alarm is triggered when moving object is detected.	Motion detection is enabled. For more information, see 10.4.1 - Motion Detection .
Disk Full	The alarm is triggered when the free space of SD card is less than the configured value.	The SD card no space function is enabled. For more information, see 10.3.1 - SD Card Exception .
Disk Error	The alarm is triggered when there is failure or malfunction in the SD card.	SD card failure detection is enabled. For more information, see 10.3.1 - SD Card Exception .
Video Tampering	The alarm is triggered when the camera lens is covered or there is defocus in video images.	Video tampering is enabled. For details, see 10.4.2 - Video Tampering .
External Alarm	The alarm is triggered when there is external alarm input.	The device has alarm input port and external alarm function is enabled. For more information, see 10.1.4 - Alarm Linkage .
Security Exception	The alarm is triggered when the device detects malicious attack.	Security exception is enabled. For more information, see 17.1 - Security Status .
Audio Detection	The alarm is triggered when there is audio connection problem.	Abnormal audio detection is enabled. For more information, see 10.5 - Audio Detection .
AI Event	The alarm is triggered when intelligent rule is triggered	Enable IVS. For more information, see 16 - AI: IVS .
Scene Changing	The alarm is triggered when the device monitoring scene changes.	Scene changing detection is enabled. For more information, see 10.4.3 - Scene Changing .
Voltage Detection	The alarm is triggered when the device detects abnormal voltage input	Voltage detection is enabled. For more information, see 10.3.3 - Voltage Exception .

When a subscribed alarm event is triggered, the system records detailed alarm information at the right side of the page.

Alarm

Alarm Subs... ^

All Types

Motion ...

Disk Full

Disk Error

Video Ta...

External ...

Security ...

Audio D...

AI Event

Scene C...

Voltage ...

Play Alarm Tone

Browse

No.	Time	Alarm Type	Source IP Address	Alarm Channel
No Data				

Clear

Figure 45: Alarm subscription

- Procedure:
- Click the  icon at the right-upper corner of the main page.
 - Click the  button next to **Enable**.
 - Select alarm type according to the actual need.
The system prompts and records alarm information according to actual conditions. When the subscribed alarm event is triggered a, a number is displayed on the  icon. The alarm information is recorded automatically. Click to view the details in the alarm list. You can click **Clear** to clear the record.
 - Click the  button next to **Play Alarm Tone** and select the tone path for the system to play the selected audio file when the alarm is triggered.

10.3 - Setting Exception

10.3.1 - SD Card Exception

In case of SD card exception, the system performs alarm linkage. The event types include No SD Card, Low SD Card Space, and SD Card Error.

- Procedure:
- Go to  > **Event > Exception > SD Card Exception**.

SD Card Exception

Network Exception

Voltage Detection

No SD card.

Low SD Card Space

SD card error

Apply

Refresh

Default

Figure 46: SD card exception

- Click the  button next to chosen SD card detection functions.
When enabling **Low SD Card Space**, set **Capacity Limit** so that when the remaining space of SD card is less than the set value, the alarm is triggered.
- Set alarm linkage actions.For more information, see [10.1 - Alarm Linkage](#).
- Click **Apply**.

10.3.2 - Network Exception

In case of network abnormality, the system performs alarm linkage. The event types include **Offline** and **IP Conflict**.

- Procedure:
- Go to  > **Event > Exception > SD Card Exception**.

SD Card Exception
Network Exception
Voltage Detection

Offline
☒

Enable Alarm
☐

Alarm-out Port

Post-Alarm
sec.(10-300)

Record
☐

Record

Post-Record
sec.(10-300)

IP Conflict
☒

Enable Alarm
☐

Alarm-out Port

Post-Alarm
sec.(10-300)

Record
☐

Record

Post-Record
sec.(10-300)

Apply
Refresh
Default

Figure 47: Network Exception

- Click the ☐ button next to chosen network detection functions.
- Set alarm linkage actions. For more information, see [10.1 - Alarm Linkage](#).
- Click **Apply**.

10.3.3 - Voltage Exception

When the input voltage is higher or lower than the rated value of the device, the system performs alarm linkage.

Procedure:

- Go to **Event > Exception > Voltage Detection**.

SD Card Exception
Network Exception
Voltage Detection

Voltage Exception
☒

Overlay
☒

Enable Alarm
☒

Alarm-out Port

Post-Alarm
sec.(10-300)

Send Email
☐

Apply
Refresh
Default

Figure 48: Voltage Detection

- Click the ☐ button next to the **Voltage Exeption** function.
With **Overlay** enabled, the alarm icon is displayed by overlapping when the alarm is triggered.
- Set alarm linkage actions. For more information, see [10.1 - Alarm Linkage](#).
- Click **Apply**.

10.4 - Video Detection

10.4.1 - 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, PTZ operation 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  > **Event > Video Detection > Motion Detection.**

Motion Detection

Video Tampering

Scene Changing

Enable

☐

Schedule

Full Time

Add Schedule

Anti-Dither

5

sec. (0-100)

Area

Setting

Alarm-out Port

☒

Alarm Channel

1

2

Post-Alarm

10

sec. (10-300)

Record

☒

Post-Record

10

sec. (10-300)

Send Email

☐

Snapshot

☒

Apply

Refresh

Default

Figure 49: Motion Detection

2. Click the ☐ button next to the **Motion Detection** function.
3. Click **Setting** next to **Area** to set an area for motion detection.

Area

X



Area

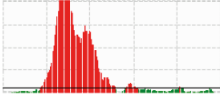
Area1

Sensitivity

+ 60

Threshold

+ 5



Clear

Delete

OK

Cancel

Figure 50: Area setting

4. Select a color and set the region name so that you can set different detection parameters for each region.
5. Set the **Sensitive** degree of outside changes. The higher the sensitivity the easier to trigger the alarm.
6. 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.
7. Click **OK**.
8. Set alarm linkage actions. For more information, see [10.1 - Alarm Linkage](#).
If the exiting schedules can't meet the scene requirement, you can click **Add Schedule** to add a new schedule. For more information, see [10.1.1 - Adding Schedule](#). With the **Anti-dither** time configured, the system only records one motion detection event in the period.
9. Click **Apply**.

10.4.2 - 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  > **Event > Video Detection > Video Tampering.**

Motion Detection

Video Tampering

Scene Changing

Event Type

Video Tampering

Enable

☐

Covered Area

100

% (1-100)

Duration

1

sec. (1-300)

Anti-Dither

1

sec. (0-100)

Schedule

Full Time

Add Schedule

Alarm-out Port

☒

Alarm Channel

1

2

Post-Alarm

10

sec. (10-300)

Record

☒

Post-Record

10

sec. (10-300)

Send Email

☐

Snapshot

☒

Apply

Refresh

Default

Figure 51: Video tampering

2. Configure the parameters listed in the table below.

Table 19 - MyEye Bullet and Dome - Description of video temper parameters	
Parameter	Description
Event Type	Video Tampering is the only available option. When the percentage of the tampered image and the duration exceed the configured values, an alarm is triggered.
Covered Area	When the percentage of the tampered image and the duration exceed the configured values, an alarm is triggered.
Duration	
Anti-Dither	Records only one alarm event during the anti-dither period

3. Set alarm linkage actions. For more information, see [10.1 - Alarm Linkage](#).
If the exiting schedules can't meet the scene requirement, you can click **Add Schedule** to add a new schedule. For more information, see [10.1.1 - Adding Schedule](#). With the **Anti-dither** time configured, the system only records one motion detection event in the period.
4. Click **Apply**.

10.4.3 - Scene Changing

The system performs alarm linkage when the image switches from the current scene to another one.

Procedure:

1. Go to  > **Event > Video Detection > Video Tampering**.

Motion Detection

Video Tampering

Scene Changing

Enable

☐

Schedule

Full Time

Add Schedule

Alarm-out Port

☒

Alarm Channel

1

2

Post-Alarm

10

sec. (10-300)

Record

☒

Post-Record

10

sec. (10-300)

Send Email

☐

Snapshot

☒

Apply

Refresh

Default

Figure 52: Scene Changing

2. Set alarm linkage actions. For more information, see [10.1 - Alarm Linkage](#).
If the exiting schedules can't meet the scene requirement, you can click **Add Schedule** to add a new schedule. For more information, see [10.1.1 - Adding Schedule](#). With the **Anti-dither** time configured, the system only records one motion detection event in the period.
3. Click **Apply**.

10.5 - Audio Detection

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

Procedure:

1. Go to  > **Event > Video Detection > Audio Detection.**

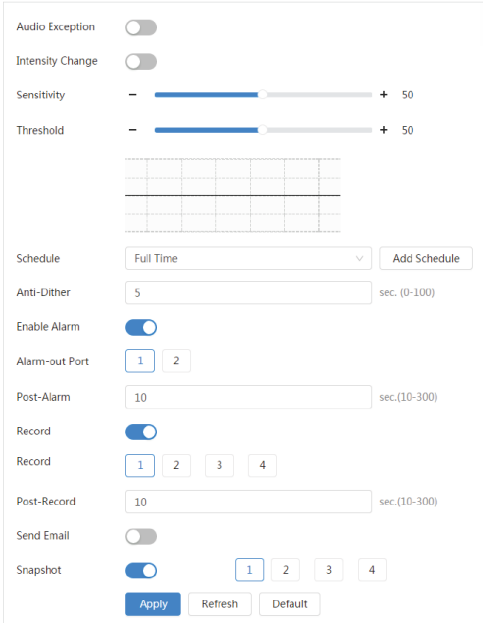


Figure 53: Audio detection

2. Configure the parameters listed in the table below.

Table 20 - MyEye Bullet and Dome - Description of Audio Detection parameters	
Parameter	Description
Audio Exeption	Click the  button next to Audio Exception for the alarm to be triggered when the system detects abnormal sound input.
Intensity Change	Click the  button next to Intensity Change and set Sensitivity and Threshold . The alarm is triggered when the system detects that the sound intensity exceeds the configured threshold.
Sensitivity	It's easier to trigger the alarm with higher sensitivity or smaller threshold. Set a high threshold for noisy environment. The red line in the waveform indicates audio detection is triggered, and the green one indicates no audio detection. Adjust sensitivity and threshold according to the waveform.
Threshold	

3. Set alarm linkage actions. For more information, see [10.1 - Alarm Linkage](#).
If the exiting schedules can't meet the scene requirement, you can click **Add Schedule** to add a new schedule. For more information, see [10.1.1 - Adding Schedule](#). With the **Anti-dither** time configured, the system only records one motion detection event in the period.
4. Click **Apply**.

10.6 - Disarming

The camera supports controlling disarm alarm linkage actions with one-click. With **Event Notification** enabled, the system only triggers the selected alarm linkage actions.

Procedure:

1. Go to  > **Event > Disarming.**

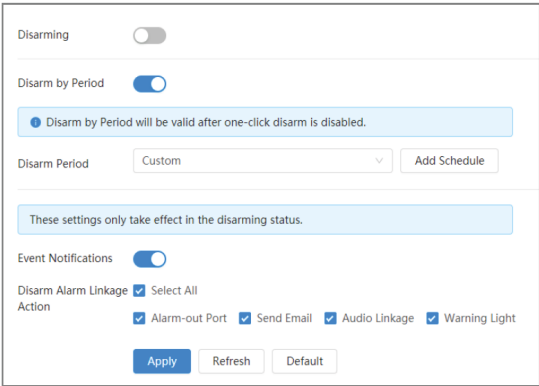


Figure 54: Disarming

2. Enable **Disarming** for the system to stop triggering alarm linkage actions all the time or **Disarm by Period** for the system to stop triggering alarm linkage actions in the period set by adding a schedule. For more information, see [10.1.1 - Adding Schedule](#).
3. Enable **Event Notification** and select the **Disarm Alarm Linkage Action** as needed.
4. Click **Apply**.

11 STORAGE

This section displays the information of the local SD card. Go to  > **Storage**.

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.
- **Format** - so that you can format the SD card.
- **Refresh** - the view is refreshed.

Format

Read-Only

Read/Write

Hot Swap

Refresh

☒	Name	Status	Properties	Used Space/Total Space	
☒	Local Disk1	Normal	Read/Write	25.88GB / 118.92GB	General Config

Figure 55: Storage section

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.

12.1 - Basic

Procedure:

1. Go to  > **System > General > Basic.**

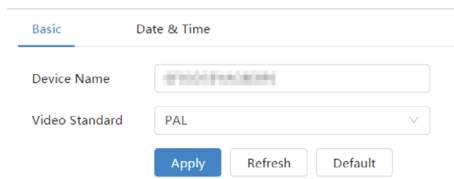


Figure 56: Basic section

2. Enter the **Device Name**.
3. Select **Video Standard** choosing **PAL** or **NTSC**.

12.2 - Date & Time

Procedure:

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

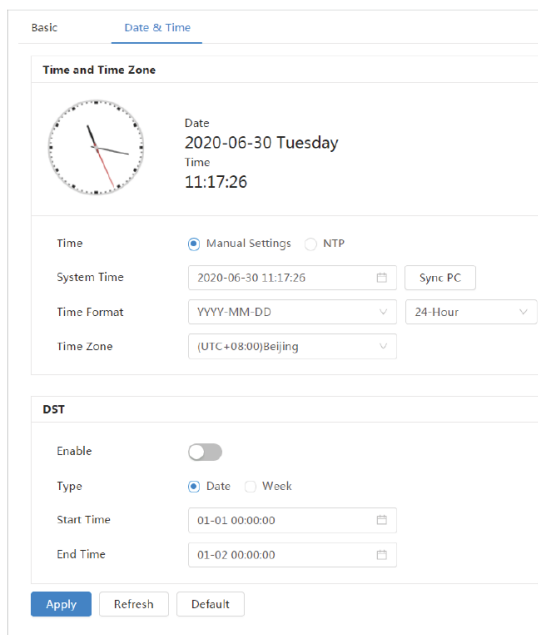


Figure 57: Date and time

2. Configure the parameters listed in the table below.

Table 21 - MyEye Bullet and Dome - Description of Date & Time parameters

Parameter	Description
Time	• Manually Setting - for manual parameters configuration • NTP - for the system to syncs time with the internet server in real time You can also enter the IP address, time zone, port, and interval of a PC with the installed NTP server to use NTP.
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	Click the  button next to DST to configure start time and end time of Daylight Saving Time (DST) with Date or Week .

3. Click **Apply**.

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.

Procedure of adding a new user:

1. Go to  > **System > Account > User.**

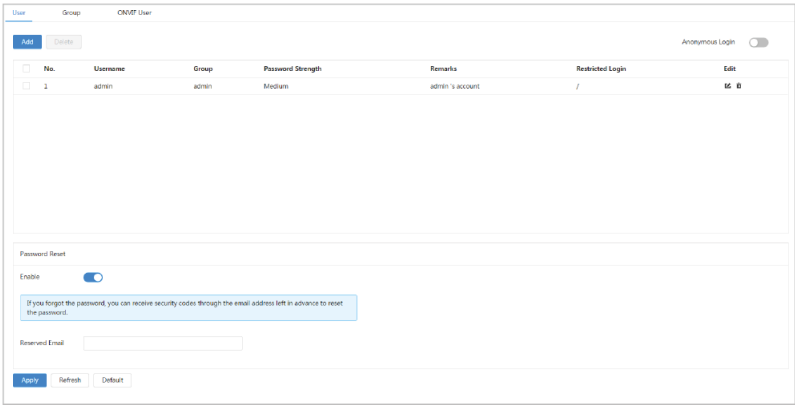


Figure 58: List of users

2. Click **Add.**

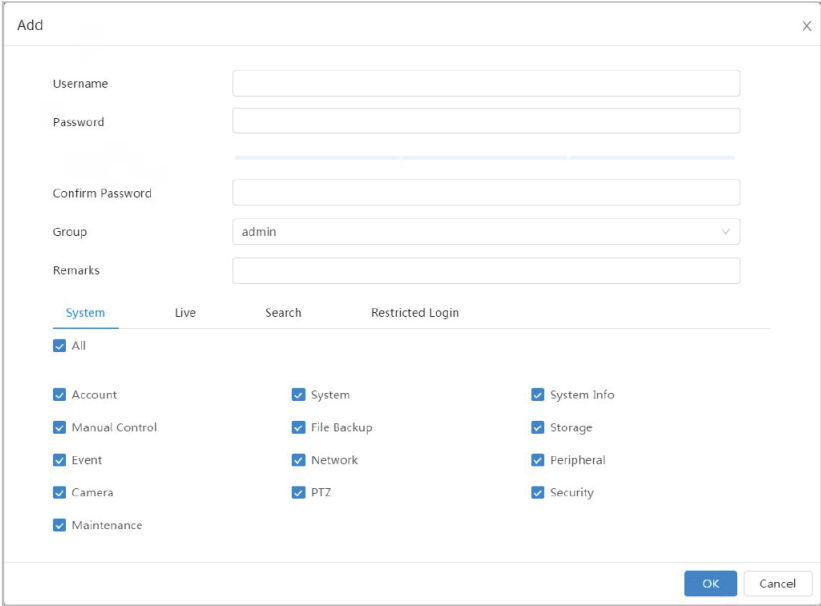


Figure 59: Adding users using the system

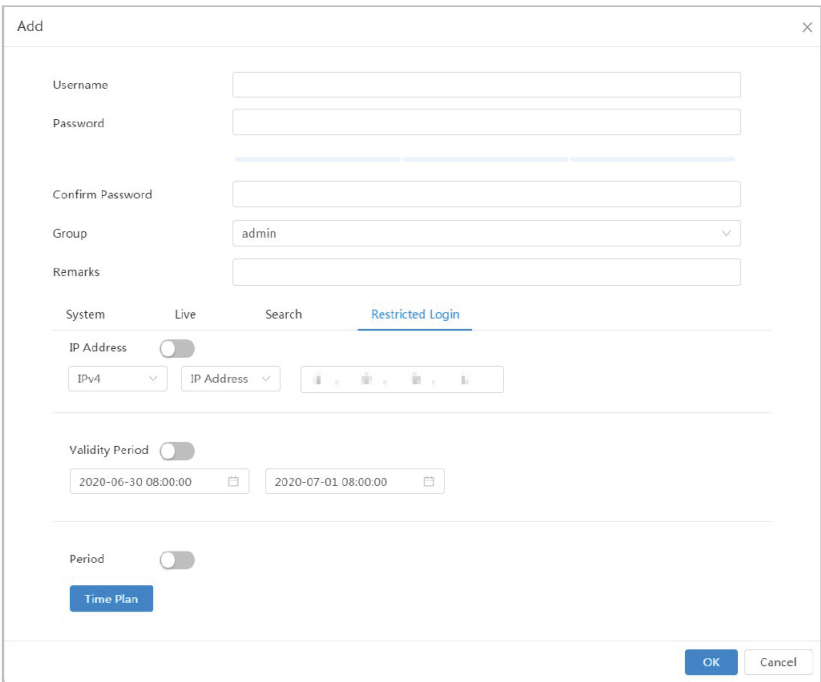


Figure 60: Adding users using the restricted login

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

Table 22 - MyEye Bullet and Dome - 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.
Remarks	Optional: enter a description of the account
System	Select permissions as needed. We recommend you give fewer permissions to normal users than premium users.
Live	Select the live view authority for the user to be added.
Search	Select the search authority for the user to be added.
Restricted Login	Set the PC address enabling the defined user to log in to the camera for the set period and time range. • IP address - You can log in the web through the PC with the set IP. • Validity period - You can log in the web in the set validity period. • Time range - You can log in the web in the set time range. Set as follows 1. IP address - Enter the IP address of the host to be added. 2. IP segment - Enter the start address and end address of the host to be added.

Related Operations

- Click the  icon to edit password, group, remarks or authorities. For admin account, you can only edit the password.
- Click the  icon to delete the added users. Admin user can't be deleted.

With the **Password Reset** function a user can reset password by clicking **Forget password?** on the login page. For more information, see [5.2 - Resetting password](#).

Procedure of resetting user's password:

1. Go to  > **System > Account > User**.
2. Click the  button next to Enable in the Password Reset section. For more information, see [Figure 58](#).
If the function is not enabled, you can only reset the password by resetting the camera.
3. Enter the reserved email address.
4. Click **Apply**.

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  > **System > Account > Group**.

User

Group

ONVIF User

Add

Delete

☐	No.	Group	Remarks	Operation
☐	1	admin	administrator group	 
☐	2	user	user group	 

Figure 61: List of groups

2. Click **Add**.
3. Enter the group name and remarks, and select group authorities.
You can't use existed group name. The max length of the group name is 31 characters including numbers, letters, underline, dash, dot and @.
4. Click **OK** to finish configuration. The newly added group displays in the group name list.

The 'Add' dialog box contains the following elements:

- Group** and **Remarks** text input fields.
- Tabs: **System** (selected), **Live**, and **Search**.
- A list of system components, each with a checked checkbox:
 - System**: All, System, File Backup, Network, PTZ.
 - System Info**: System Info, Storage, Peripheral, Security.
 - Manual Control**: Manual Control, Event, Camera, Maintenance.
- OK** and **Cancel** buttons at the bottom right.

Figure 62: Adding groups

Related Operations

- Click the icon to edit password, group, remarks or 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:

- Go to > **System > Account > ONVIF User**.

The 'ONVIF User' page includes:

- Add** and **Delete** buttons.

☐	No.	Username	Group	Password Strength	Edit
☐	1	admin	admin	Medium	

Figure 63: ONVIF User

- Click **Add**.

The 'Add' dialog box for an ONVIF user contains:

- Username**, **Password**, and **Confirm Password** text input fields.
- A **Group** dropdown menu with 'admin' selected.
- OK** and **Cancel** buttons at the bottom right.

Figure 64: Adding an ONVIF user

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

Table 23 - 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	Select a group for the account. The user rights must be within the group authorities.

- Click **OK** to finish configuration. The newly added group displays in the group name list.

Related Operations

- Click the icon to edit password, group, remarks or authorities. For admin account, you can only edit the password.
- Click the icon to delete the added users. Admin user can't be deleted.

12.4 - Manager

To make sure the system runs normally, maintain it as the following requirements:

- Check surveillance images regularly.
- Clear regularly user and user group information that aren't frequently used.
- Change the password every three months.
- View system logs and analyze them, and process the abnormality in time.
- Back up the system configuration regularly.
- Restart the device and delete the old files regularly.
- Upgrade firmware in time.

12.4.1 - Maintenance

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  > **System > Manager > Maintenance.**

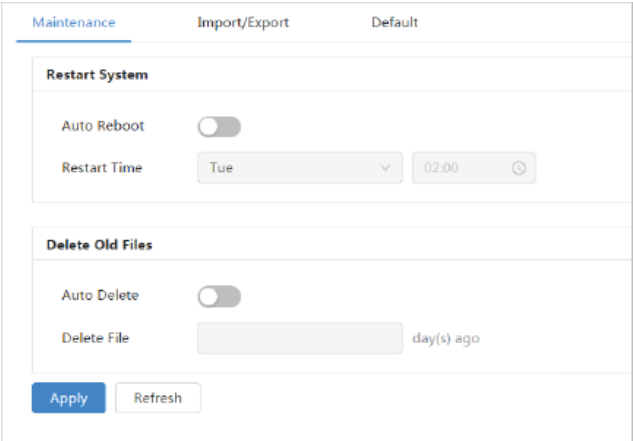


Figure 65: Maintenance

2. Optionally: click the  button next to **Auto Reboot** in the **Restart System** section and set the reboot time for the system to restart automatically at the set time every week.
3. Optionally: click the  button next to **Auto Delete** in the **Delete Old Files** section and set the time for the system to delete old files automatically at the set time. The time range is 1 to 31days.

Note

With the **Auto Delete** function enabled, the deleted files can't be restored. Operate it carefully.

4. Click **Apply**.

12.4.2 - Import/Export

- Export the system configuration file to back up the system configuration.
- Import system configuration file to make quick configuration or recover system configuration.

Procedure:

1. Go to  > **System > Manager > Import/Export.**

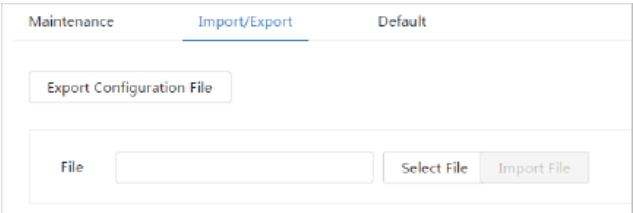


Figure 66: Import/Export

2. Import or export the file.
- Import - Select local configuration file, and click **Import File** to import the local system configuration file to the system.
 - Export - Click **Export Configuration File** to export the system configuration file to local storage.

12.4.3 - Default

To restore the device to default configuration or factory settings go to  > **System > Manager > Default.**

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

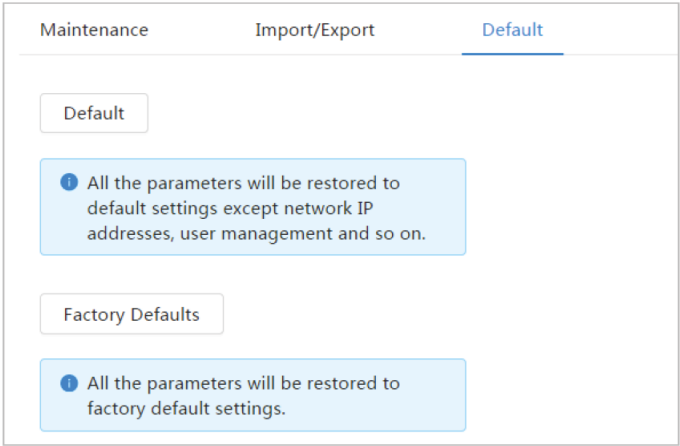


Figure 67: Default

12.5 - Upgrade

Upgrading to the latest system can refine camera functions and improve stability.
If wrong upgrade file has been used, restart the device; otherwise some functions might not work properly.

Procedure:

1. Go to  > **System > Upgrade.**
2. Click **Browse** and upload upgrade file. The upgrade file should be a .bin file.
3. Click **Update**.



Figure 68: Upgrade

13 SYSTEM INFO

- To view device information such as hardware, system version, and web version go to  > **System Info > Device Info.**
- To view all the online users logging in the web go to  > **System Info > Online User.**

14.1 - Logging in system

You can view and back up logs.

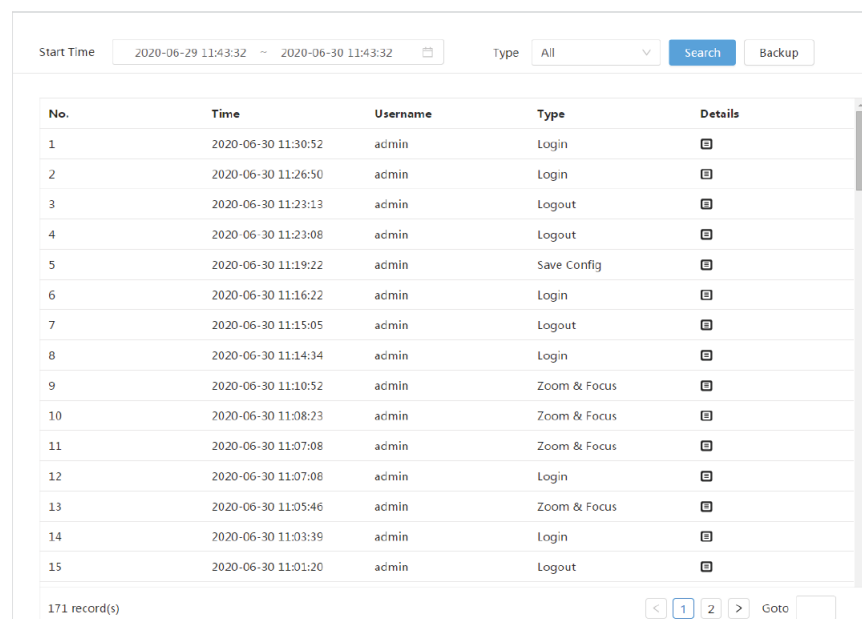
Procedure:

1. Go to  > **Log > Log**.
2. Configure **Start Time** and **End Time**.
The start time should be later than January 1st, 2000, and the end time should be earlier than December 31st, 2037.
3. Select a log type choosing one of options listed in the table below.

Table 24 - MyEye Bullet and Dome - Log types

Type	Description
System	Includes program start, abnormal close, close, program reboot, device close down, 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	Records events such as video detection, smart plan, alarm and abnormality; includes event start and event end
Record	Includes file access, file access error, and file search
Account	Includes login, logout, adding user, deleting user, editing user, adding group, deleting group, and editing group
Security	Includes password resetting and IP filter

4. Click **Search**.
5. Click the  icon or a certain log to view the detailed information in **Details** area.
6. Optionally: click **Backup** to back up all found logs to local PC.



No.	Time	Username	Type	Details
1	2020-06-30 11:30:52	admin	Login	
2	2020-06-30 11:26:50	admin	Login	
3	2020-06-30 11:23:13	admin	Logout	
4	2020-06-30 11:23:08	admin	Logout	
5	2020-06-30 11:19:22	admin	Save Config	
6	2020-06-30 11:16:22	admin	Login	
7	2020-06-30 11:15:05	admin	Logout	
8	2020-06-30 11:14:34	admin	Login	
9	2020-06-30 11:10:52	admin	Zoom & Focus	
10	2020-06-30 11:08:23	admin	Zoom & Focus	
11	2020-06-30 11:07:08	admin	Zoom & Focus	
12	2020-06-30 11:07:08	admin	Login	
13	2020-06-30 11:05:46	admin	Zoom & Focus	
14	2020-06-30 11:03:39	admin	Login	
15	2020-06-30 11:01:20	admin	Logout	

Figure 69: Log

14.2 - Remote Log

You can configure remote log to get the related log by accessing the set address.

Procedure:

1. Go to  > **Log > Remote Log**.
2. Click the  button to enable the remote log function.
3. Set address, port and device number.
4. Click **Apply**.

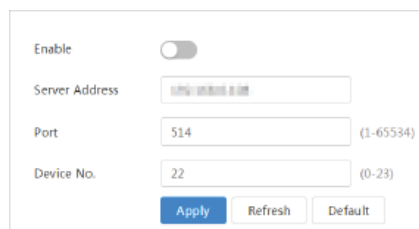


Figure 70: Remote Log

15.1 - Live Page

Log in and click the **Live** tab.

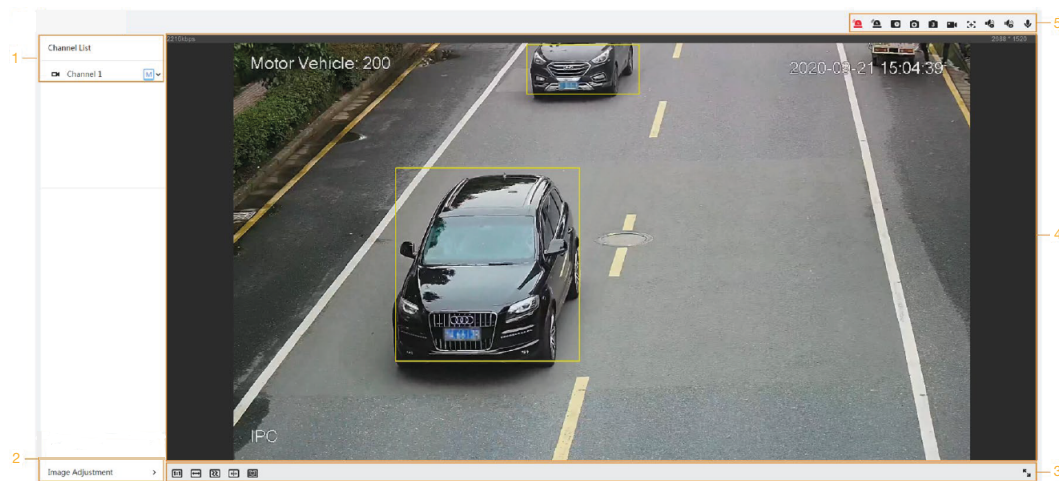


Figure 71: Live - single channel

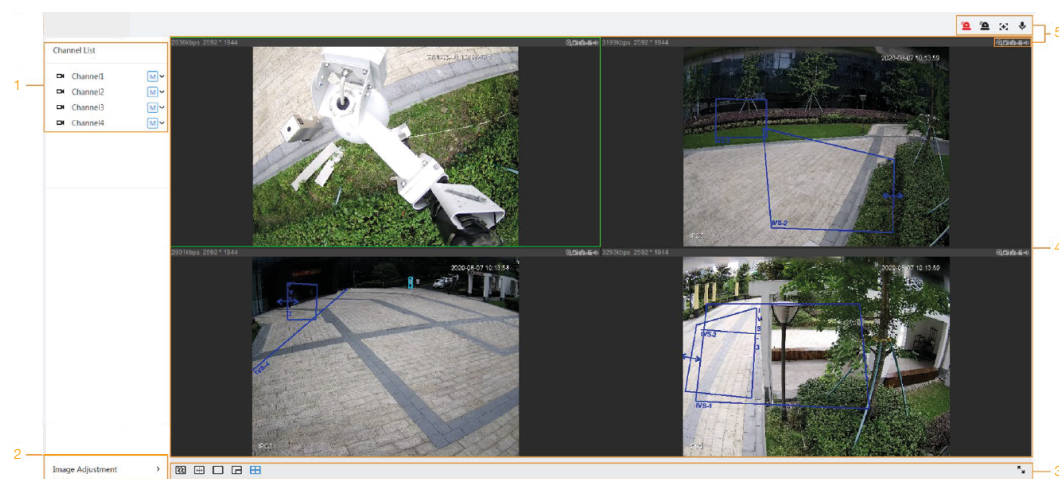


Figure 72: Live - multiple channels

Table 25 - MyEye Bullet and Dome - Description of function bar		
No.	Function	Description
1	Channel list	Displays all channels. You can select the channel as needed and set the stream type.
2, 3	Image adjustment	Operations adjustment in live viewing
4	Live view	Displays the real-time monitoring image
5	Live view function bar	Functions and operations in live viewing

15.2 - Encode

Click the  icon to select the stream as needed.

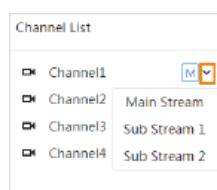


Figure 73: Encode bar

- **Main Stream** - It 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** - It has small bit stream value and smooth image, and requires less bandwidth. This option is normally used to replace main stream when bandwidth isn't enough.
- The  icon means the current stream is the main stream. The  icon means the current stream is sub stream 1. The  icon means the current stream is sub stream 2.

15.3 - Live View function bar

Table 26 - MyEye Bullet and Dome - Description of live view top function bar		
Icon	Function	Description
	Auxiliary Instalation	Click the icon to enable or disable IVS as AI rule
	Warning Light	Click the icon to enable or disable Warning Light
	Alarm	Displays the status of alarm
	Force Alarm1	Displays the status of alarm sound. Click the icon to enable or disable the alarm sound forcibly.
	Digital Zoom	You can zoom video image through two following operations: - Click the icon and select an area in the video image to zoom in; right-click on the image to resume the original size. In zoom state drag the image to check other area. - Click the icon, and scroll the mouse wheel in the video image to zoom in or out.
	Snapshot	Click the icon to capture one picture of the current image. It is saved to the configured storage path. For more information on viewing or configuring storage path, see 7 - LOCAL .
	Triple Snapshot	Click the icon to capture three pictures of the current image. They are saved to the configured storage path. For more information on viewing or configuring storage path, see 7 - LOCAL .
	Record	Click the icon to record video. It's saved to the configured storage path. For more information on viewing or configuring storage path, see 7 - LOCAL .
	Sound	Click the icon to enable or disable audio output.
	Talk	Click the icon to enable or disable the audio talk.

15.4 - Image Adjustment bar

Table 27 - MyEye Bullet and Dome - Description of Image Adjustment bar		
Icon	Function	Description
	Original Size	Click the icon for the video to display the original size.
	W:H	Click the icon to resume original ratio or change ratio.
	Smothness Adjustment	Click the icon to select one of the following options: Realtime - Guarantees the real time of the image. When the bandwidth isn't enough, the image might not be smooth. General - It is between the real time and Fluent. Fluent - Guarantees the fluency of the image. There might be delay between live view image and real-time image.
	AI Rule	Click the icon, and select Enable to display AI rules and detection box; select Disable to stop the display. It's enabled by default.
	Intelligence Area	Click the icon to adjust the view to previously configured AI rule.
	Window Layout	When viewing multi-channel image, you can select display layout.
	Full Screen	Click the icon to enter full screen mode; double-click or press Esc to exit.

15.5 - Image Adjustment

Click Image Adjustment at the lower-left corner of Live page, and click + or- button, or drag the slider to adjust image parameters. The adjustment is only available on the web page, and it doesn't adjust the camera parameters.

-  **Brightness** - Adjust the overall image brightness and change the value when the image is too bright or too dark.
-  **Contrast** - Change the value when the image brightness is proper but contrast isn't enough.
-  **Saturation** - Adjust the image saturation. This value doesn't change image brightness.
-  **Hue** - Make the color deeper or lighter. The default value is made by the light sensor, and it's recommended.
- Click **Reset** to restore focus to default value. You can restore the zoom if the image has poor clarity or has been zoomed too frequently.

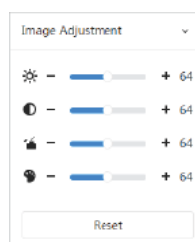


Figure 74: Image adjustment

Basic requirements on scene selection for intelligent video system (IVS) are as follows:

- The target should occupy no more than 10% of the whole image.
- The target size in the image should be at least 10×10 pixels. The target height and width should be no more than a third of the image height and width. The recommended target height is 10% of the image height.
- The brightness difference of the target and the background should be at least 10 gray levels. The target should be continuously present in the image for at least two seconds. The moving distance of the target should be larger than its width and at least 15 pixels (CIF image).
- Reduce the complexity of surveillance scene as much as you can. Intelligent analysis functions aren't recommended to be used in scene with dense targets and frequent illumination change.
- Avoid areas such as glass, reflective ground, water surface, and areas interfered by branch, shadow and mosquito. Avoid backlight scene and direct light.

Calibration purpose:

Determine corresponding relationship between 2D image captured by the camera and 3D actual object according to one horizontal ruler and three vertical rulers calibrated by the user and the corresponding actual distance.

Applicable scene:

- Medium or distant view with installation height of more than three meters. Scenes with parallel view or ceiling-mounted aren't supported.
- Calibrate horizontal plane, not vertical walls or sloping surfaces.
- Not applicable to scenes with distorted view, such as the distorted views captured by super wide-angle or fisheye camera.

Calibration:

- The drawn calibration area should be on one horizontal plane.
- The bottom of three vertical rulers should be on the same horizontal plane. Select three reference objects with fixed height in triangular distribution as vertical rulers, such as vehicle parked at roadside or road lamp poles. Arrange three people to draw at each of the three positions in the monitoring scene.
- Select reference object with known length on the ground, such as sign on the road, or use a tape to measure the actual length.

Procedure:

1. Go to **AI > Smart Plan**.
2. Click the ☐ button to **IVS** to enable IVS of the corresponding channel.
3. Click **Next**.

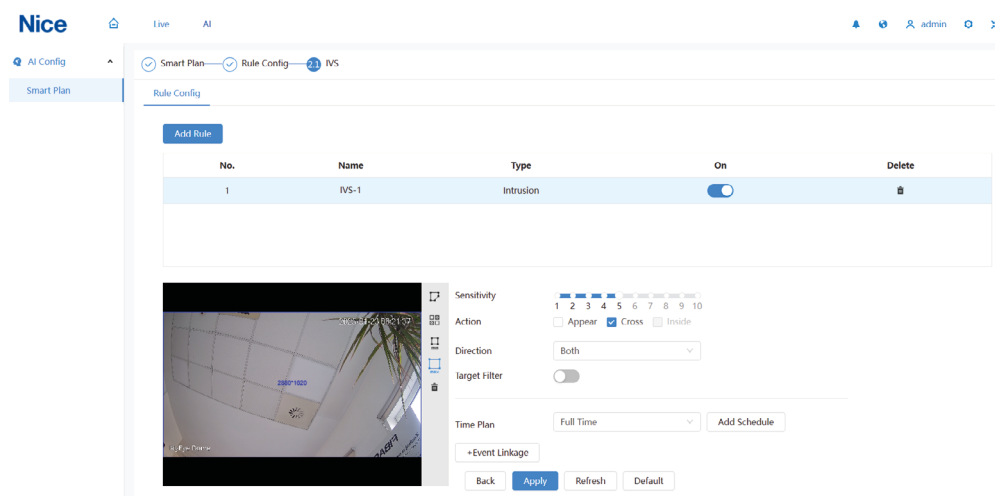


Figure 75: IVS configuration

4. Click **Add Rule**.
5. Select one of two options:
 - **Tripwire** - Click the icon to draw rule line in the image. Right-click to finish drawing. When the target crosses the tripwire from the defined motion direction, an alarm is triggered, and the system performs configured alarm linkages.
 - **Intrusion** - Draw a detection area. Tick a checkbox next to **Appear**, **Cross** or **Inside** to decide when an alarm should be triggered according to the object movement.
6. Configure calibration area by setting minimum and maximum size with the icons. You can also click the icon, and press and hold the left mouse button to draw a rectangle. Click the icon to delete the detection line if needed.
7. Set **Sensitivity**. The higher value, the easier to trigger an alarm when low-contrast object and small object are captured, and the false detection rate is higher. The pixel size is displayed.
8. Set the direction of rule **Detection**. Select **A->B**, **B->A**, or **Both** for **Tripwire**. Select **Enter**, **Exit**, or **Both** for **Intrusion**.
9. Click the ☐ button to **Target Filter** for the system to start an alarm when an object triggers the rule. With the **Tripwire** rule enabled you can select **Effective Target**. With the **Human** checkbox ticked an alarm is triggered when the system detects a person triggering the rule. With the **Motor Vehicle** checkbox ticked an alarm is triggered when the system detects a vehicle triggering the rule.
10. Click **Add Schedule** to set the time for the alarm to be triggered.
11. Click **+ Event Linkage** to set the linkage action.
12. Click **Apply**.

17.1 - Security Status

Scan the security modules to check the security status of the camera so that when abnormality appears you can process it timely.

- **User and service detection** - Detect login authentication, user status, and configuration security to check whether the current configuration conforms to recommendation.
- **Security modules scanning** - Scan the running status of security modules, such as audio/video transmission, trusted protection, security warning and attack defense. The function doesn't check if they are enabled.

Procedure:

1. Go to **Security > Security Status**.
2. Click **Rescan** to scan the security status of the camera.

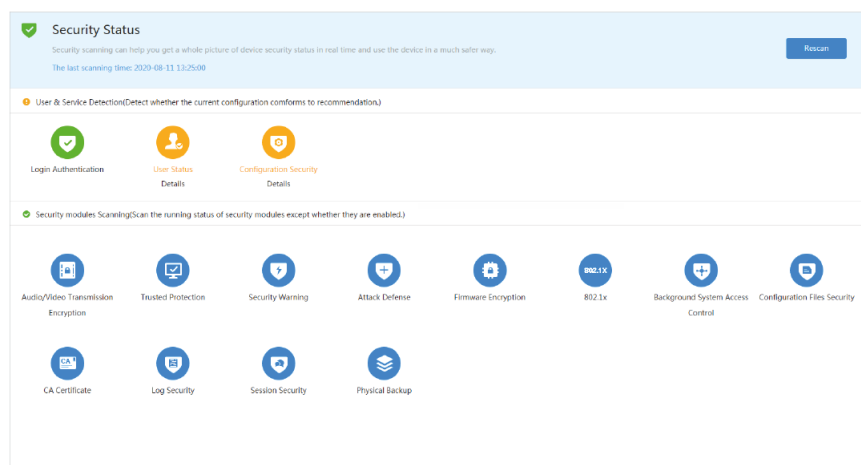


Figure 76: Security Status

After scanning, results are displayed with different colors. **Yellow** indicates that the security modules are **abnormal**, and **Green** indicates that the security modules are **normal**.

- Click **Details** to view the details of the scanning result.
- Click **Ignore** not to scan the exception in next scanning.
- Click **Joint Detection** for the exception to be scanned in next scanning.
- Click **Optimize** for the corresponding page to be displayed. You can edit the configuration to clear the exception.

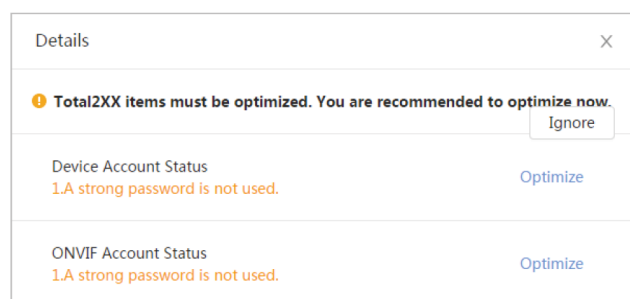


Figure 77: Details of security status

17.2 - System Service

17.2.1 - 802.1x

Cameras can connect to LAN after passing 802.1x authentication.

Procedure:

1. Go to **Security > System Service > 802.1x**.
2. Select the NIC name as needed, and click the ☐ button next to **Enable**.
3. Select the authentication mode choosing one of the options:
 - **PEAP** - Protected EAP protocol
Then, enter the username and password that has been authenticated on the server.
 - **TLS** - Transport Layer Security is applied in two communication application programs to guarantee the security and integrity of the data.
Then, enter the username
4. Click the ☐ button next to **CA certificate** and select the trusted CA certificate in list.
If there is no certificate in the list, click **Certificate Management** at the left navigation bar. For more information, see [17.4.4 - Installing Trusted CA Certificate](#).
5. Click **Apply**.

802.1x

HTTPS

802.1x is a network access control protocol which can effectively prevent access from unauthorized hosts.

NIC Name

NIC1

Enable

Authentication Mode

PEAP

Username

none

Password

••••

CA Certificate

Use a trusted CA certificate to verify the validity of peer authentication server (switch or Radius server).

Device Certificate

Trusted CA Certificates

Certificate List

Certificate Management

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
☐ 1		6F03D5EYAG9E43B	2059-05-23 11:05:14	Device Root CA	Device Root CA	
☐ 2		6F03D5EYAG9E43B	2049-05-30 13:58:24	Device IPC CA	Device Root CA	

Apply

Refresh

Default

Figure 78: 802.1x - PEAP

802.1x

HTTPS

802.1x is a network access control protocol which can effectively prevent access from unauthorized hosts.

NIC Name

NIC1

Enable

Authentication Mode

TLS

Username

none

CA Certificate

Use a trusted CA certificate to verify the validity of peer authentication server (switch or Radius server).

Device Certificate

Trusted CA Certificates

Certificate List

Certificate Management

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
☐ 1		6F03D5EYAG9E43B	2059-05-23 11:05:14	Device Root CA	Device Root CA	
☐ 2		6F03D5EYAG9E43B	2049-05-30 13:58:24	Device IPC CA	Device Root CA	

Apply

Refresh

Default

Figure 79: 802.1x - TLS

17.2.2 - HTTPS

HTTPS protects page authenticity on all types of websites, secure accounts, and keep user communications, identity, and web browsing private.

Procedure:

1. Go to **Security > System Service > HTTPS**.

2. Click the button next to **Enable**.

3. Select the certificate.
If there is no certificate in the list, click **Certificate Management** at the left navigation bar. For more information, see [17.4.4 - Installing Trusted CA Certificate](#).

4. Click **Apply**.

802.1x

HTTPS

Enable

HTTPS is a service entry based on Transport Layer Security (TLS). HTTPS provides web service, GINVI access service and RTSP access service.

Compatible with TLSv1.1 a...

There might be security risks if TLS of earlier versions are enabled. Please select carefully.

*Select a device certificate

Certificate Management

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
☒ 1		6F03D5EYAG9E43B	2050-07-15 15:37:32	6F03D5EYAG9E43B	Dohua Device IPC CA	HTTPS, RTSP over TLS

Apply

Refresh

Default

Download Root Certificate

Figure 80: HTTPS

17.3 - Attack Defense

17.3.1 - Firewall

Configure firewall to limit access to the camera.

Procedure:

- 1. Go to **Security > Attack Defense > Firewall**.

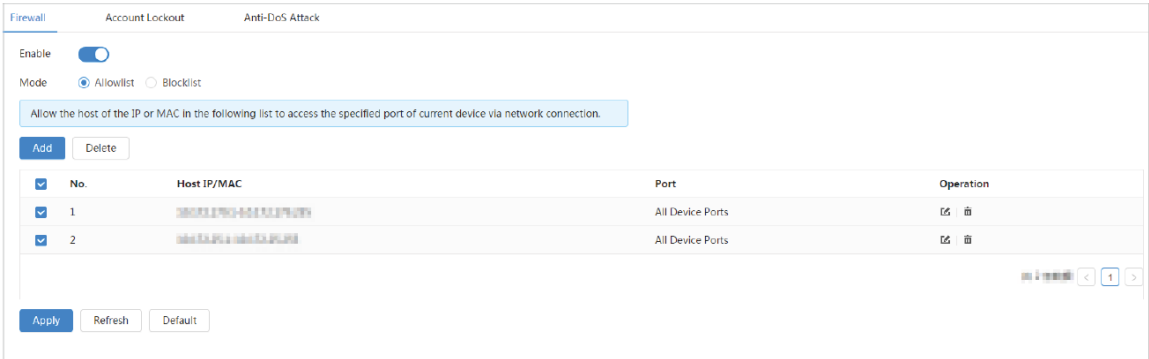


Figure 81: Firewall

- 2. Click the button next to **Enable**.
- 3. Select the mode choosing one of the options:
 - **Allowlist** - Only when the IP/MAC of your PC in the allow list, can you access the camera. Ports are the same.
 - **Blocklist** - When the IP/MAC of your PC is in the block list, you can't access the camera. Ports are the same.
- 4. Click **Add** to add the host IP/MAC address to **Allowlist** or **Blocklist**, and then click **OK**.
- 5. Click **Apply**.

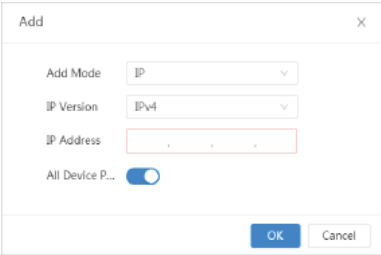


Figure 82: Adding to Allowlist/Blocklist

Related Operations

- Click the icon to edit the host information.
- Click the icon to delete the host information.

17.3.2 - Account Lockout

If you consecutively enter a wrong password more than the configured value, the account is locked.

Procedure:

- 1. Go to **Security > Attack Defense > Account Lockout**.
- 2. Configure **Login Attempt** and **Lock Time** for **Device Account** and **ONVIF User**.
 - **Login attempt** - upper limit of login attempts. If you consecutively enter a wrong password more than the configured value, the account is locked.
 - **Lock time** - the period during which you cannot login after the login attempts reaches upper limit.
- 3. Click **Apply**.

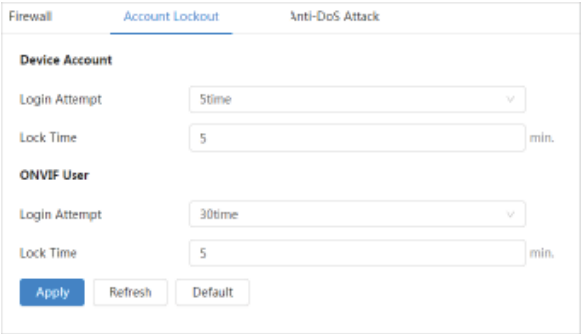


Figure 83: Setting account lockout

17.3.3 - Anti-DoS Attack

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the device against Dos attack.

Procedure:

- 1. Go to **Security > Attack Defense > Anti-DoS Attack**.
- 2. Select **SYN Flood Attack Defense** or **ICMP Flood Attack Defense**.

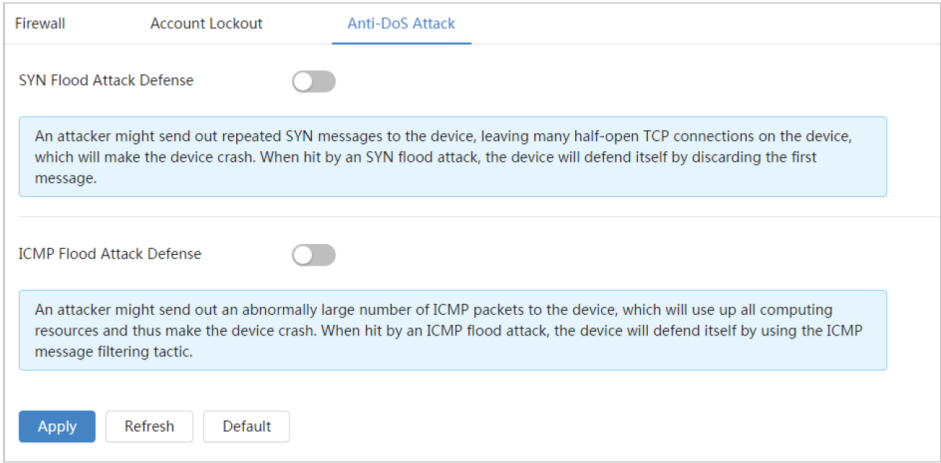


Figure 84: Setting Anti-DoS attack

17.4 - CA Certificate

17.4.1 - Creating Device Certificate

Create a certificate to log in through HTTPS on the camera using your PC.

Procedure:

- 1. Go to **Security > CA Certificate > Device Certificate**.
- 2. Select **Install Device Certificate**.
- 3. Select **Create Certificate** and **click Next**.
- 4. Enter the certificate information.

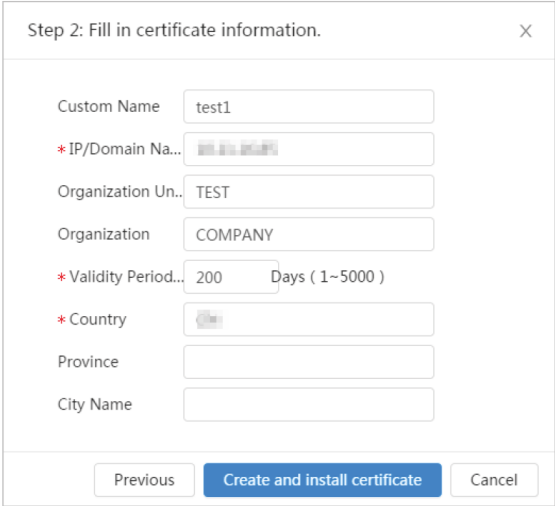


Figure 85: Certificate information

- 5. Click **Create and install certificate**.
After the certificate is created successfully, you can view this certificate on the **Device Certificate** page.

Related Operations

- Click **Enter Edit Mode** to edit the custom name of the certificate.
- Click the  icon to download the certificate.
- Click the  icon to delete the certificate.

17.4.2 - Importing third-party CA Device Certificate

Procedure:

- 1. Go to **Security > CA Certificate > Device Certificate**.
- 2. Select **Install Device Certificate**.
- 3. Select **Apply for CA Certificate and Import (Recommended)** and click **Next**.

Step 1: Select installation mode.

☐ Create Certificate

Fill in certificate information, and the device will create and issue the certificate.

☒ Apply for CA Certificate and Import (Recommended)

After you fill in certificate information, the device will generate a certificate request file. Please submit the file to a CA institute to apply for a signature and certificate, and then import them into the device.

☐ Install Existing Certificate

If you already have a certificate and private key file, please import the certificate and private key file in this way.

Next

Cancel

Figure 86: Selecting installation mode

- 4. Enter the certificate information.

Step 2: Fill in certificate information.

* IP/Domain Na...

Organization Un..

Organization

* Validity Period...

* Country

Province

City Name

Previous

Create and Download

Cancel

Figure 87: Certificate information

- 5. Click **Create and Download**. Save the request file to your PC.
- 6. Apply the CA certificate from the third-party certificate authority.
- 7. Import and save the CA certificate to the PC.
- 8. Repeat spteps 1 - 3 and click **Browse** to select the signed CE certificate.
- 9. Click **Install and Import**.
After the certificate is created successfully, you can view this certificate on the **Device Certificate** page.
Click **Recreate** to create the request file again.
Click **Import Later** to import the certificate next time.

Related Operations

- Click **Enter Edit Mode** to edit the custom name of the certificate.
- Click the  icon to download the certificate.
- Click the  icon to delete the certificate.

17.4.3 - Installing existing Device Certificate

Import the existing third-party certificate to the camera. When apply for the third-party certificate, you also need to apply for the private key file and private key password.

Procedure:

- 1. Go to **Security > CA Certificate > Device Certificate**.
- 2. Select **Install Device Certificate**.
- 3. Select **Install Existing Certificate** and click **Next**.

Figure 88: Certificate and private key

4. Click **Browse** to select the **Certificate Path** and **Private Key** file.
5. Enter the **Private Key Password**.
6. Click **Install and Import**.

After the certificate is created successfully, you can view this certificate on the **Device Certificate** page.

Related Operations

- Click **Enter Edit Mode** to edit the custom name of the certificate.
- Click the  icon to download the certificate.
- Click the  icon to delete the certificate.

17.4.4 - Installing Trusted CA Certificate

CA certificate is a digital certificate for the legal identity of the camera. When the camera accesses the LAN through 802.1x, the CA certificate is required.

Procedure:

1. Go to **Security > CA Certificate > Trusted CA Certificates**.
2. Select **Install Trusted Certificate**.
3. Click **Browse** to select the certificate.

Figure 89: Installing Trusted Certificate

4. Click **OK**.

After the certificate is created successfully, you can view this certificate on the **Device Certificate** page.

Related Operations

- Click **Enter Edit Mode** to edit the custom name of the certificate.
- Click the  icon to download the certificate.
- Click the  icon to delete the certificate.

17.5 - A/V Encryption

The device supports audio and video encryption during data transmission.

You are recommended to enable A/V Encryption function. There might be safety risk if this function is disabled.

Procedure:

1. Go to **Security > CA Certificate > A/V Encryption**.

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
1		61633137303235636234303531373336333830343037	2055-01-16 23:53:27	9F0AB24FAG69722	General Device IPC CA	HTTPS, RTSP over TLS

Figure 90: A/V encryption

2. Configure A/V encryption parameter listed in the table below.

Table 28 - MyEye Bullet and Dome - A/V encryption parameters		
Area	Parameter	Description
Private Protocol	Enable	Enables stream frame encryption by using private protocol. There might be safety risk if this service is disabled.
	Encryption Type	Use the default setting.
	Update Period of Secret Key	Secret key update period. Value range: 0 – 720 hours. 0 means never update the secret key. Default value: 12
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS. There might be safety risk if this service is disabled.
	Select a device certificate	Select a device certificate for RTSP over TLS.
	Certificate Management	For more information on certificate management, see 17.4 - CA Certificate .

17.6 - Security Warning

When security exception event is detected, the camera sends a warningfor you to process the issue timely.

Procedure:

- 1. Go to **Security > Security Warning**.
- 2. Click the  button next to **Enable** to enable security warning.
- 3. Select **Alarm-out Port** and set **Post-Alarm** period.
- 4. Click **+ Event Linkage** to set the linkage action.
- 5. Click **Apply**.

Enable 

Event Monitoring

Invalid executable programs attempting to run

Web Path Brute Force Attack

Session ID Brute Force Attack

Session connection number exceeds limit.

Security warning can detect device security status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks.

+Event Linkage

Enable Alarm Enabled

Alarm-out Port

1

2

Post-Alarm

10

sec.(10-300)

Apply

Refresh

Default

Figure 91: Security warning

57

18.1 - Search Video

This function enables video playback and is available on the camera with SD card.

Before playing back video, configure record time range, record storage method, record schedule and record control. For more information, see [18.2 - Record Control](#), [18.3 - Time Plan](#), and [11 - STORAGE](#).

Procedure:

1. Go to **Record > Search Video**.
2. Select a channel from **Channel List**.
3. Click **All** to select the record type from the drop-down list. You can select **All**, **General**, **Alarm**, or **Manual**.
4. Select the record time. The dates with blue dots indicate there are videos recorded on those days.
5. Click **Search**.

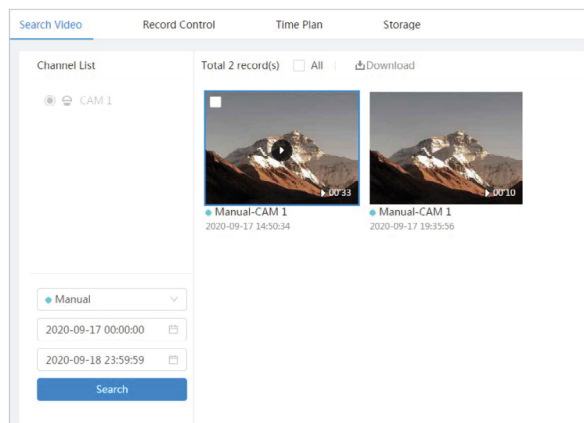


Figure 92: Search video

6. Point to the searched video, and then click the  icon in the picture to play back the selected video. The video playback page is displayed.

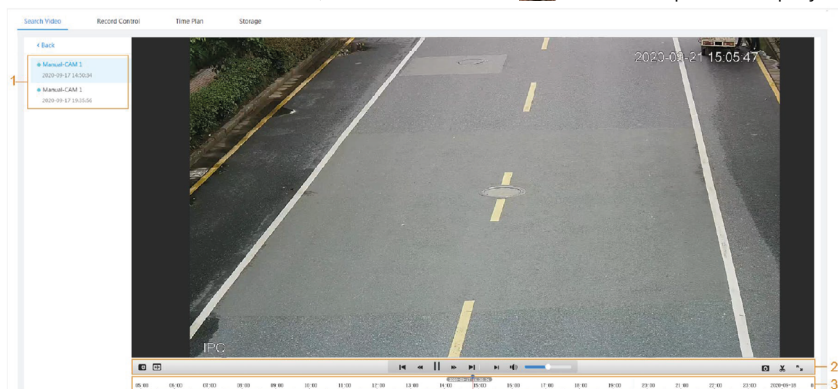


Figure 93: Video playback page

Table 29 - MyEye Bullet and Dome - Description of video playback page		
No.	Function	Description
1	Recorded video list	Displays all searched recorded video files. Click a choosen file to play back it. Click Back at the upper-left corner to go to the Search Video page.
2	Digital Zoom	You can zoom video image of the selected areain two following ways: • Click the icon and select an area in the video to zoom in; right-click on the image to resume the original size. In zoom state drag the image to check other areas. • Click the icon, and scroll the mouse wheel in the video image to zoom in or out.
	AI Rule	AI rules is valid if you enabled the rule during recording. Click the  icon and select Enable to display AI rules and detection box; select Disable to stop the display.
	Play control bar	 - play;  - stop;  - play the previous video on the list;  - play the next video;  - play the next frame;  - slow down the video;  - speed up the video
	Sound	 - Vocal state. You can adjust the sound.  - Mute mode
	Snapshot	Click  to capture a picture of the video. It's saved to the configured storage path. For more information, see 7 - LOCAL
	Video clip	Click  to save a chosen video. For more information, see 18.1.1 - Clipping video
3	Full Screen	Click  for the video to display in full-screen mode. Double-click the image or press Esc button to exit full-screen mode.
	Progress bar	Click any point in the colored area for the system to play back the recorded video from the selected moment. Each record type has its own color, and you can see their relations in Record Type bar.

18.1.1 - Clipping video

Procedure:

1. Click the  icon.
2. Drag the clipping box on the progress bar to select the start time and end time of the target video.

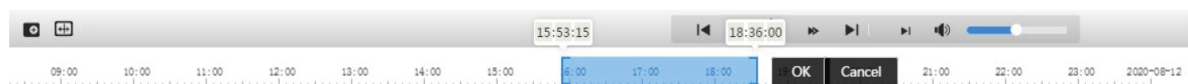


Figure 94: Clipping video

3. Click **OK** to download the video.
4. Select the download format and storage path.

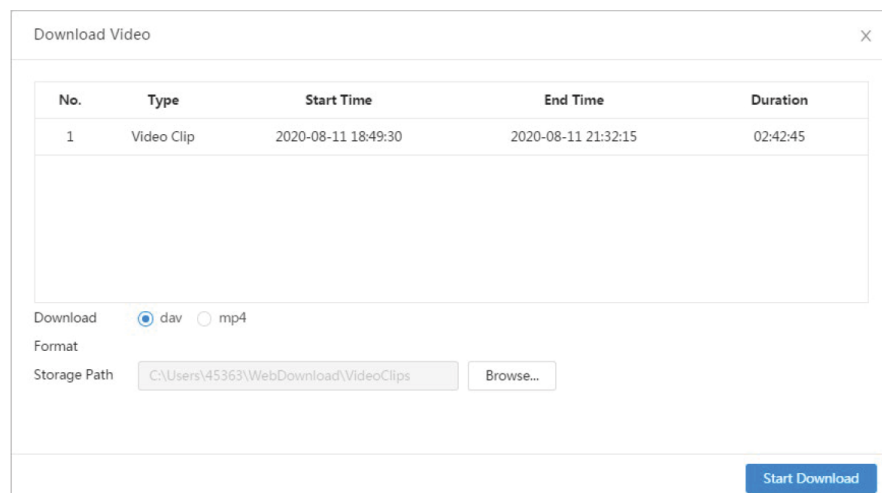


Figure 95: Downloading video

5. Click **Start Download**.

The playback stops and the clipped file is saved in the configured storage path. For more information on storage path, see [7 - LOCAL](#).

18.1.2 - Downloading video

Download videos to a defined path. You can download a single video, or download them in batches.

Playback and downloading at the same time isn't supported.

Operations might vary with different browsers.

Procedure:

1. Go to **Record > Search Video**.
2. Select the channel, the record type, and record time, and click **Search**.
3. Select the videos to be downloaded.
Tick the ☐ icon at the upper-right corner of each video file to select one or multiple videos.
Tick the ☐ icon next to **Select All** to select all searched videos.

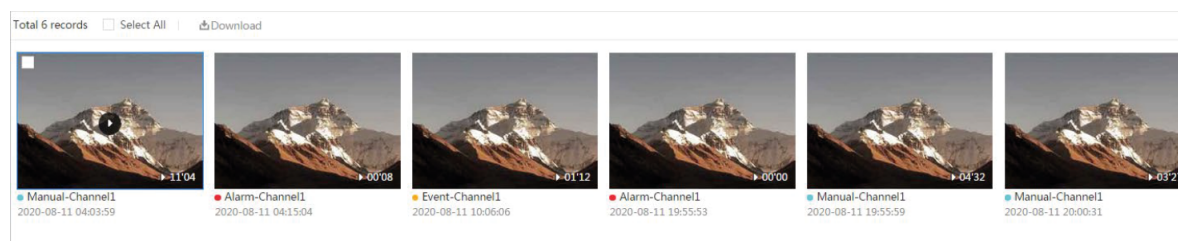


Figure 96: Selecting video file

4. Click **Download**.
5. Select the download format and storage path. For more information, see Figure 92.
6. Click **Start Download**.

The downloaded files are saved in the configured storage path. For more information on storage path, see [7 - LOCAL](#).

18.2 - Record Control

Procedure:

- 1. Click the Record section on the home page.
- 2. Click the **Record Control** tab.

Max Duration

min (1-120)

Pre-Record

sec (0-5)

Record Mode

☒ Auto ☐ Manual ☐ Off

Record Stream

Main Stream

Apply

Refresh

Default

Figure 97: Record Control

- 3. Set parameters listed in the table below.

Table 30 - MyEye Bullet and Dome - Description of record control parameters	
Parameter	Description
Max Duration	The time for packing each video file
Pre-Record	The time to record the video in advance of a triggered alarm event. When an alarm links recording and the recording isn't enabled, the system saves the video data within the pre-event record time to the video file.
Record Mode	When you select Manual , the system starts recording. When you select Auto , the system starts recording in the configured period of record plan.
Record Stream	Select Main Stream or Sub Stream .

- 4. Click **Apply**.

18.3 - Time Plan

After the corresponding alarm type (Normal, Motion, and Alarm) is enabled, the record channel links recording.
Set certain days as holiday, and when the **Record** is selected in the holiday schedule, the system records video as holiday schedule defined.

Procedure:

- 1. Click the Record section on the home page.
- 2. Click the **Time Plan** tab.

Channel

CAM 1

Holiday

Event Type: Scheduled Motion Alarm

Clear

Delete

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Sun

Copy

Mon

Copy

Tue

Copy

Wed

Copy

Thu

Copy

Fri

Copy

Sat

Copy

Apply

Refresh

Default

Figure 98: Time plan

- 3. Set record plan by selecting a record type, such as **Normal**, and directly pressing and dragging the left mouse button to set the period for normal record on the timeline.
 - **Green** represents normal record plan such as timing recording.
 - **Yellow** represents motion record plan such as recording triggered by intelligent events.
 - **Red** represents alarm record plan such as recording triggered by alarm-in.Click **Copy** next to a day, and select the days that you want to copy to in the prompt page. Tick the **Select All** checkbox to copy the configuration to all days. You can set 6 periods per day.
- 4. Click **Apply**.
- 5. Click **Holiday** to set holidays.

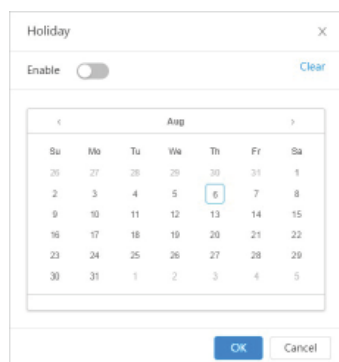


Figure 99: Setting holiday

6. Click the  icon to enable the holiday configuration, and select the days that you need to set as holiday.
When holiday schedule setting isn't the same as the general setting, holiday schedule setting is prior to the general setting.
Click **Clear** to cancel the selection.
7. Click **Apply**.

18.4 - Storage

In the **Storage** section you can configure the storage method for the recorded videos.

Procedure:

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

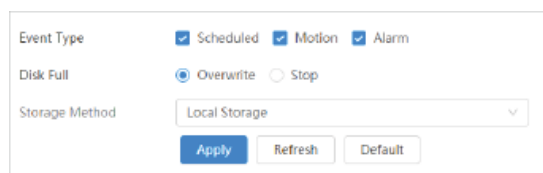


Figure 100: Setting storage

2. Set storage parameters listed in the table below.

Table 31 - MyEye Bullet and Dome - Description of storage parameters	
Parameter	Description
Event Type	Select from Scheduled , Motion Detection and Alarm .
Disk Full	Recording strategy when the disk is full. • Overwrite - cyclically overwrite the earliest video when the disk is full • Stop - stop recording when the disk is full
Storage Method	Select choosing one of the options: • Local storage - save the recorded videos in the internal SD card • Network storage - save the recorded videos in the FTP server or NAS

3. Click **Apply**.

18.4.1 - Local Storage

Procedure:

1. Go to **Record > Storage**.
2. Select the recording strategy in **Disk Full** choosing **Overwrite** or **Stop**. For more information see Table 31 and Figure 100.
3. Select **Local Storage** in **Storage Method** to save the recorded videos in the internal SD card.
4. Click **Apply**.

18.4.2 - FTP

With this function enabled you can save all the files in the FTP server.

Procedure:

1. Go to **Record > Storage**.
2. Select the recording strategy in **Disk Full** choosing **Overwrite** or **Stop**. For more information see Table 31 and Figure 100.
3. Select **Network Storage** in **Storage Method**.
4. Select **FTP** or **SFPT** from the drop-down list. **SFPT** is recommended to enhance the network security.
5. Click the  icon next to **Enable** to enable the **FTP** function.

Figure 101: FTP setting

6. Set FTP parameters listed in the table below.

Table 32 - MyEye Bullet and Dome - Description of FTP parameters	
Parameter	Description
Server IP	The IP address of the FTP server
Port	The port number of the FTP server
Username	The username to log in to the FTP server
Password	The password to log in to the FTP server
Storage Path	The destination path in the FTP server
Directory Structure	Set the directory structure selecting Use Level 1 Directory , Use Level 2 Directory , or Use Level 3 Directory
Level 1 Directory	Set the Level 1 Directory name selecting Device name , Device IP , or Custom . When you select Custom , enter the custom directory.
Level 2 Directory	Set the Level Directory name selecting File Type , Date , File Type_Channel Number , or Custom . When you select Custom , enter the custom directory.
Level 3 Directory	
Urgently store to local	Click the  icon for all the files to be saved to the internal SD card when the FTP server doesn't work.

7. Click **Save**.

8. Click **Test** to test whether FTP function works normally.

18.4.3 - NAS

With this function enabled you can save all the files in Network Attached Storage (NAS).

Procedure:

- Go to **Record > Storage**.
- Select the recording strategy in **Disk Full** choosing **Overwrite** or **Stop**. For more information see [Table 31](#) and Figure 100.
- Select **Network Storage** in **Storage Method** and then **NAS** to save the recorded videos in NAS server.
- Select NAS protocol type choosing one of the following options:
 - NFS** (Network File System) - A file system which enables computers in the same network to share files through TCP/IP.
 - SMB** (Server Message Block) - It provides shared access for clients and the server.

Event Type

☒ Scheduled ☒ Motion ☒ Alarm

Disk Full

☒ Overwrite ☐ Stop

Storage Method

Network Storage

NAS

Protocol Type

SMB

Enable

☐

Server IP

0.0.0.0

Storage Path

Username

anonymity

Password

Apply

Refresh

Default

Figure 102: NAS setting

5. Set NAS parameters listed in the table below.

Table 33 - MyEye Bullet and Dome - Description of NAS parameters	
Parameter	Description
Server IP	The IP address of the NAS server
Storage Path	The destination path in the NAS server
Username	When selecting SMB protocol, you are required to enter username and password.
Password	

6. Click **Apply**.

19.1 - Playing back picture

Before playing back picture, configure snapshot time range, snapshot storage method, snapshot plan. For more information, see [18.3 - Time Plan](#).

Procedure:

1. Go to **Picture > Picture Query**.
2. Select a channel from **Channel List**.
3. Click **All** to select the snapshot type from the drop-down list. You can select **All**, **General**, **Alarm**, or **Event**.
4. Select the record time. The dates with blue dots indicate there are snapshots taken on those days.
5. Click **Search**.

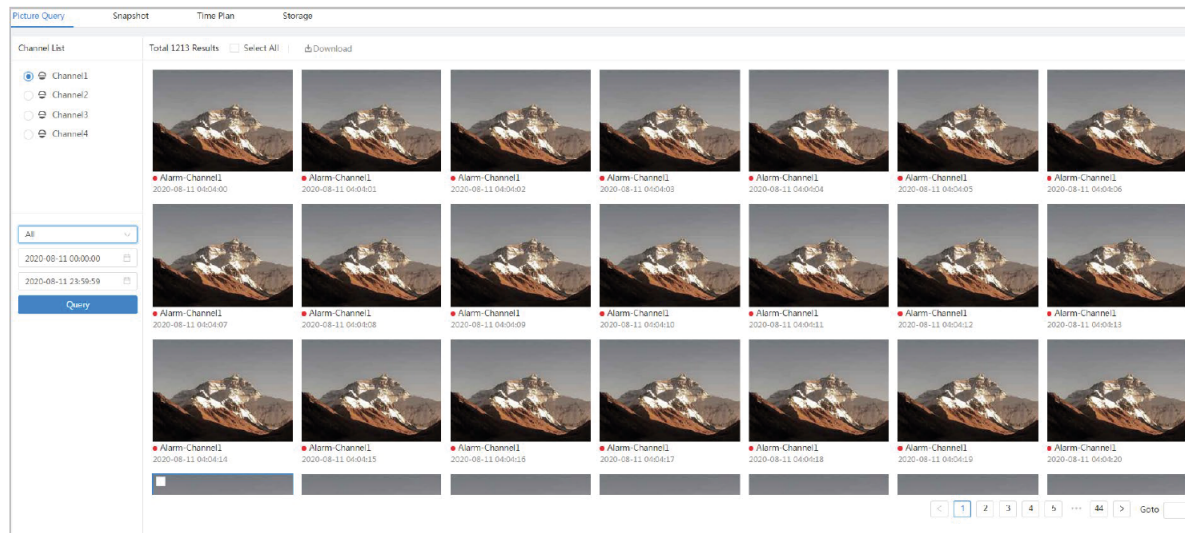


Figure 103: Picture query

6. Point to the searched picture, and then click the  icon in the picture to play back the selected video. The video playback page is displayed.

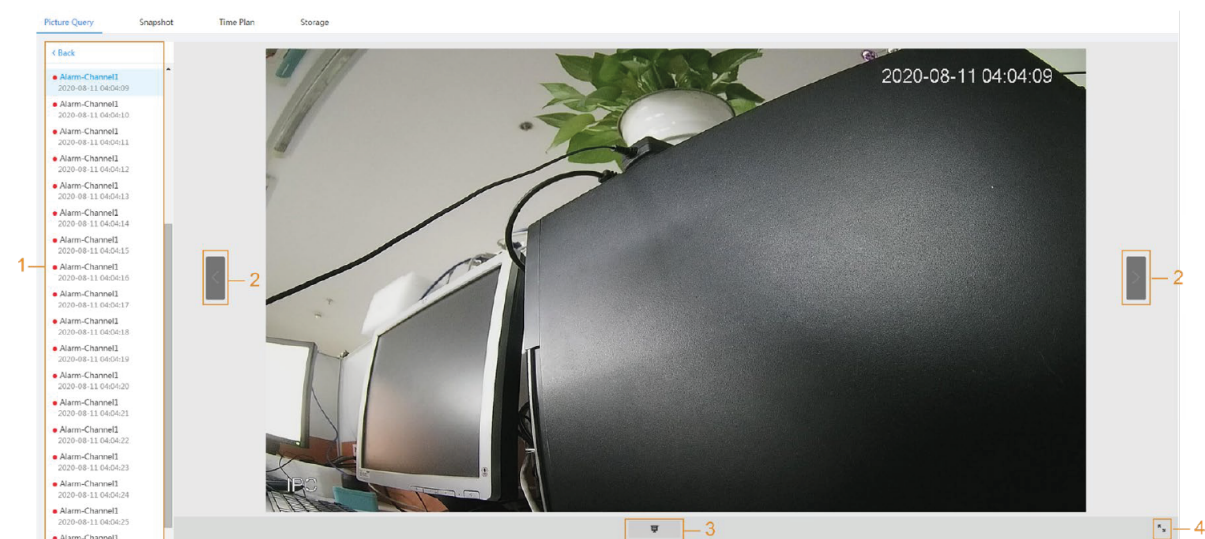


Figure 104: Picture playback

Table 34 - MyEye Bullet and Dome - Description of video playback page		
No.	Function	Description
1	Snapshot list	Displays all searched snapshots. Click any files to play it back. Click Back at the upper-left corner to go to the Picture Query page.
2	Manual display	- Click the  icon to display the previous snapshot in the snapshot list. - Click the  icon to display the next snapshot in the snapshot list.
3	Slide show	Click the  icon to display the snapshots list one by one in slide show mode.
4	Full screen	Click the  icon for the snapshot to be displayed in full-screen mode. Double-click the image or press Esc button to exit full-screen mode.

19.1.1 - Downloading snapshots

Download a snapshot to a defined path. You can download a single snapshot, or download them in batches. For more information on viewing or setting storage path, see [7 - LOCAL](#). Operations might vary with different browsers.

Procedure:

- 1. Go to **Record > Picture Query**.
- 2. Select the channel, the snapshot type, and record time, and click **Search**.
- 3. Select the snapshot to be downloaded.
Tick the ☐ icon at the upper-right corner of each video file to select one or multiple videos.
Tick the ☐ icon next to **Select All** to select all searched videos.

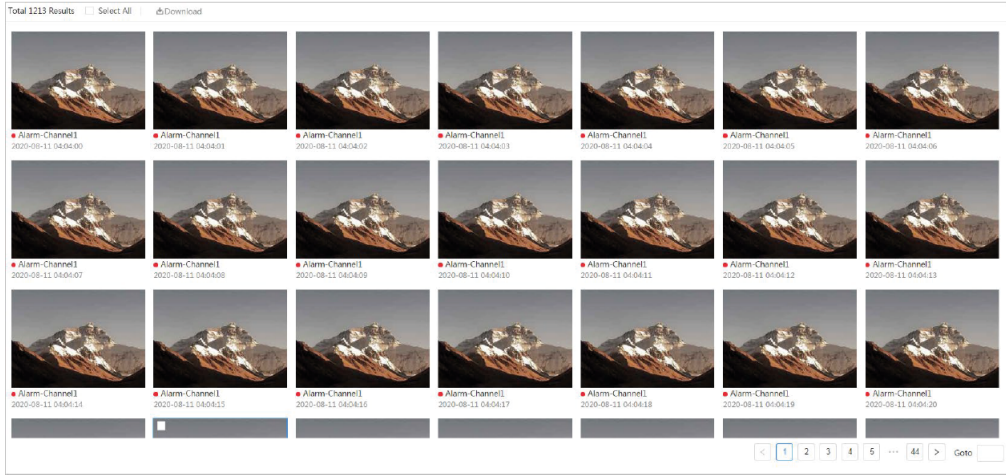


Figure 105: Selecting snapshot file

- 4. Click **Download**.
- 5. Select the **Download Format** and **Storage Path**.

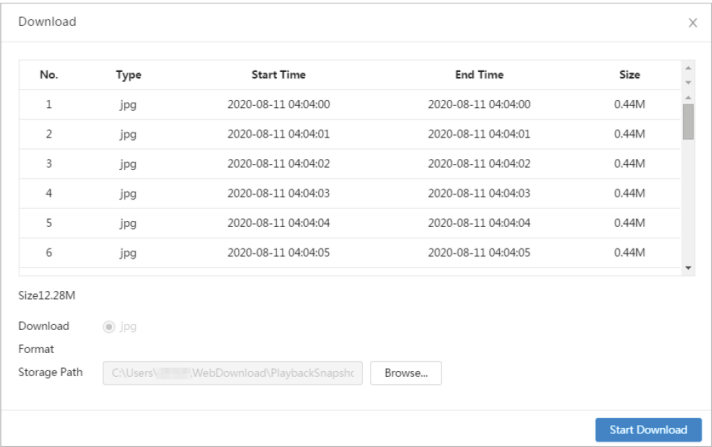


Figure 106: Downloading snapshots

- 6. Click **Start Download**.
The downloaded files are saved in the configured storage path. For more information on storage path, see [7 - LOCAL](#).

19.2 - Setting snapshot parameters

Procedure:

- 1. Go to **Record > Snapshot**.

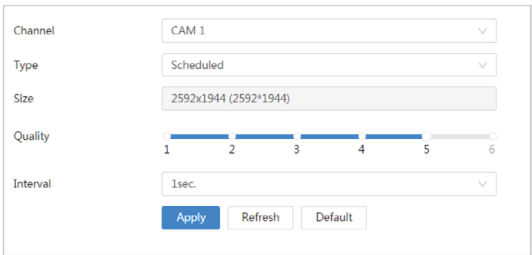


Figure 107: Snapshot setting

Table 35 - MyEye Bullet and Dome - Description of snapshot parameters	
Parameter	Description
Type	Select one of the following options: • Scheduled - capture images in configured period • Event - capture images when configured event is triggered
Size	It's same with the resolution of the main stream.
Quality	Set the quality of the snapshot. The higher the value, the better the quality.
Interval	Set the frequency of snapshot. You can select Custom to set the frequency as needed.

2. Select the channel and set the snapshot parameters.

3. Click **Apply**.

19.3 - Setting snapshot plan

According to the configured snapshot plan, the system enables or disables snapshot at the set time. For more information, see **18.3 - Time Plan**.

19.4 - Storage

Set the storage method for the snapshot. For more information, see **18.4 - Storage**.

19.5 - Setting upload method

When an alarm is triggered, images can be automatically uploaded to the defined server through HTTP protocol with no need to set upload period first.

Procedure:

1. Go to **Picture > Auto Upload**.

2. Click the  icon next to **Enable**.



No.	IP/Domain Name	Port	Path	Event Type	Test	Delete
1	Example : 172.16.1.1	Example : 80	Example : /example/	None	<button>Test</button>	
2	Example : 172.16.1.1	Example : 80	Example : /example/	None	<button>Test</button>	

Figure 108: Image Upload

Table 31 - MyEye Bullet and Dome - Description of HTTP mode parameters	
Parameter	Description
IP/Domain name	The IP address and port number of the server which the report is uploaded to.
Port	
Path	The storage path of the server for the report
Event type	Select the event type form the drop-down list. You can select more than one event type at the time. The event types are the same as in Picture Query .
Test	Test the network connection between the camera and the server.

3. Click **Add** to configure parameters of HTTP upload method. You can add two server information at most.

4. Click **Apply**.

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 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 protocol 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 a minimum 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.

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, ABNORMAL MECHANICAL 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 disposed with other household wastes. It shall be handed over to the applicable collection point for the recycling of waste electrical and electronic equipment.



Nice SpA
Oderzo TV Italia
info@niceforyou.com