Network Speed Dome

User Manual

Initiatives on the Use of Video Products

Thank you for choosing Hikvision products.

Technology affects every aspect of our life. As a high-tech company, we are increasingly aware of the role technology plays in improving business efficiency and quality of life, but at the same time, the potential harm of its improper usage. For example, video products are capable of recording real, complete and clear images. This provides a high value in retrospect and preserving real-time facts. However, it may also result in the infringement of a third party's legitimate rights and interests if improper distribution, use and/or processing of video data takes place. With the philosophy of "Technology for the Good", Hikvision requests that every end user of video technology and video products shall comply with all the applicable laws and regulations, as well as ethical customs, aiming to jointly create a better community.

Please read the following initiatives carefully:

- Everyone has a reasonable expectation of privacy, and the installation of video products should not be in conflict with this reasonable expectation. Therefore, a warning notice shall be given in a reasonable and effective manner and clarify the monitoring range, when installing video products in public areas. For non-public areas, a third party's rights and interests shall be evaluated when installing video products, including but not limited to, installing video products only after obtaining the consent of the stakeholders, and not installing highly-invisible video products.
- The purpose of video products is to record real activities within a specific time and space and under specific conditions. Therefore, every user shall first reasonably define his/her own rights in such specific scope, in order to avoid infringing on a third party's portraits, privacy or other legitimate rights.
- During the use of video products, video image data derived from real scenes will continue to be generated, including a large amount of biological data (such as facial images), and the data could be further applied or reprocessed. Video products themselves could not distinguish good from bad regarding how to use the data based solely on the images captured by the video products. The result of data usage depends on the method and purpose of use of the data controllers. Therefore, data controllers shall not only comply with all the applicable laws and regulations and other normative requirements, but also respect international norms, social morality, good morals, common practices and other non-mandatory requirements, and respect individual privacy, portrait and other rights and interests.
- The rights, values and other demands of various stakeholders should always be considered when processing video data that is continuously generated by video products. In this regard, product security and data security are extremely crucial. Therefore, every end user and data controller, shall undertake all reasonable and necessary measures to ensure data security and avoid data leakage, improper disclosure and improper use, including but not limited to, setting up access

control, selecting a suitable network environment (the Internet or Intranet) where video products are connected, establishing and constantly optimizing network security.

- Video products have made great contributions to the improvement of social security around the world, and we believe that these products will also play an active role in more aspects of social life. Any abuse of video products in violation of human rights or leading to criminal activities are contrary to the original intent of technological innovation and product development. Therefore, each user shall establish an evaluation and tracking mechanism of their product application to ensure that every product is used in a proper and reasonable manner and with good faith.

Legal Information

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***).
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE

DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

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

Contents

Chapter 1 Overview

1.1 Product Introduction

The Network Speed Dome is an integration of the HD zoom camera and the PT module, ideal for remote monitoring and easy to install and operate.

The device has two channels: Camera 01 is the PTZ channel and Camera 02 is the panoramic channel. With two channels, the device is able to capture the overall image and details at the same time.

The device is ideal for use in classrooms, training rooms, lobbies, lecture halls, and factories. It performs attendance check alone or with the education sharing server or platform.

1.2 Key Function

The device is able to check attendance, detect standing students and other events, and perform PTZ functions.

Face Attendance

The device captures the faces in the detection area, uploads the pictures to server for attendance data analysis, or uses the face comparison function for attendance check and uploads the data to platform.

Student Stand Up

The device detects student behavior of standing up, sitting down, and walking around during the class. The device captures target pictures, shows the target in close-up, and sends alarms.

Event Function

The device detects basic events and smart events.

PTZ Function

The device supports PTZ functions, such as presets, scans, patrol, and power-off memory.

1.3 System Requirement

Your computer should meet the requirements for visiting and operating the product.

	Recommended Specifications
Operating System	Microsoft Windows 7/ Windows 8/ Windows 10

	Recommended Specifications
	Mac OS 10.13 or later
CPU	Intel® Pentium® IV 3.0 GHz or higher
RAM	1 GB or higher
Display	1024 × 768 resolution or higher
Web Browser	Internet Explorer 10 and above version, Apple Safari 12 and above version, Mozilla Firefox 52 and above version, Google Chrome 57 and above version.

Chapter 2 Device Activation and Accessing

To protect the security and privacy of the user account and data, you should set a login password to activate the device when access the device via network.

Note

Refer to the user manual of the software client for the detailed information about the client software activation.

2.1 Activate Device

The device needs to be activated by setting a strong password before use. This part introduces activation using different client tools.

2.1.1 Activate Device via Web Browser

Use web browser to activate the device. For the device with the DHCP enabled by default, use SADP software or PC client to activate the device.

Before You Start

Make sure your device and your PC connect to the same LAN.

Steps

1. Change the IP address of your PC to the same subnet as the device.

   The default IP address of the device is 192.168.1.64.
2. Open a web browser and input the default IP address.
3. Create and confirm the admin password.

   Caution

   STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
4. Click **OK** to complete activation and enter **Live View** page.
5. Modify IP address of the camera.

   1) Enter IP address modification page. **Configuration → Network → TCP/IP**

   2) Change IP address.

   3) Save the settings.

2.1.2 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website ***http://www.hikvision.com/*** , and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should belong to the same subnet.

The following steps show how to activate one device and modify its IP address. For batch activation and IP address modification, refer to *User Manual of SADP* for details.

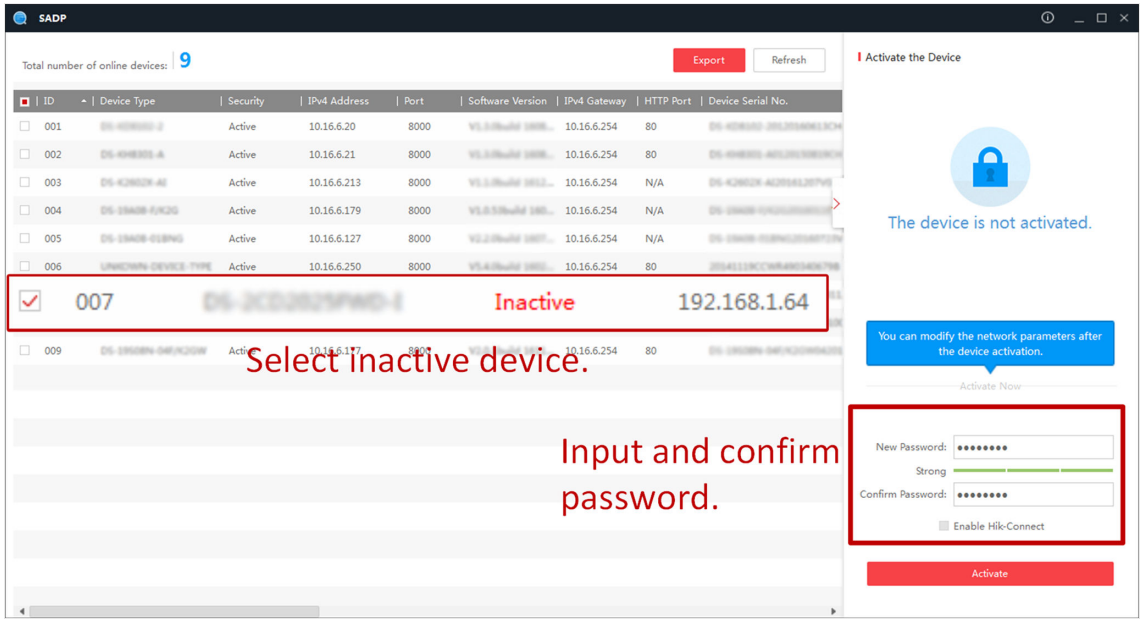
Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

Caution

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

4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.

1) Select the device.

2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
3) Input the admin password and click **Modify** to activate your IP address modification.

2.2 Access Device via Web Browser

Before You Start

Check the system requirement to confirm that the operating computer and web browser meets the requirements. See ***System Requirement*** .

Steps

1. Open the web browser.
2. Input IP address of the device to enter the login interface.
3. Input user name and password.

Note

Illegal login lock is activated by default. If admin user performs seven failed password attempts (five attempts for user/operator), the IP address is blocked for 30 minutes.
If illegal login lock is not needed, go to **Configuration → System → Security → Security Service** to turn it off.

4. Click **Login**.
5. Download and install appropriate plug-in for your web browser.

   For IE based web browser, webcomponents and QuickTime™ are optional. For non-IE based web browser, webcomponents, QuickTime™, VLC and MJEPG are optional.

2.2.1 Plug-in Installation

Certain operation systems and web browser may restrict the display and operation of the device function. You should install plug-in or complete certain settings to ensure normal display and operation. For detailed restricted function, refer to the actual device.

Operating System	Web Browser	Operation
Windows	Internet Explorer 10+	Follow pop-up prompts to complete plug-in installation.
Windows 7 and above version	Google Chrome 57+ Mozilla Firefox 52+	Click Download Plug-in to download and install plug-in.
Mac OS	Google Chrome 57+ Mozilla Firefox 52+ Mac Safari 12+	Plug-in installation is not required. Go to **Configuration → Network → Advanced Settings**

Operating System	Web Browser	Operation
		→ **Network Service** to enable WebSocket or Websockets for normal view. Display and operation of certain functions are restricted. For example, Playback and Picture are not available. For detailed restricted function, refer to the actual device.

Note

The device only supports Windows and Mac OS system and do not support Linux system.

2.2.2 Admin Password Recovery

If you forget the admin password, you can reset the password by clicking **Forget Password** on the login page after completing the account security settings.

You can reset the password by setting the security question or email.

Note

When you need to reset the password, make sure that the device and the PC are on the same network segment.

Security Question

You can set the account security during the activation. Or you can go to **Configuration → System → User Management** , click **Account Security Settings**, select the security question and input your answer.
You can click **Forget Password** and answer the security question to reset the admin password when access the device via browser.

Email

You can set the account security during the activation. Or you can go to **Configuration → System → User Management** , click **Account Security Settings**, input your email address to receive the verification code during the recovering operation process.

2.2.3 Illegal Login Lock

It helps to improve the security when accessing the device via Internet.

Go to **Configuration → System → Security → Security Service** , and enable **Enable Illegal Login Lock**. **Illegal Login Attempts** and **Locking Duration** are configurable.

Illegal Login Attempts

When your login attempts with the wrong password reach the set times, the device is locked.

Locking Duration

The device releases the lock after the setting duration.

Chapter 3 Smart Function

3.1 Allocate VCA Resource

VCA resource offers you options to enable certain VCA functions according to actual needs. It allocates resources to the desired functions.

Steps

1. Go to **VCA → VCA Resource** .
2. Select a VCA function.

   Attendance Check (Collaboration)

   Face Attendance and Student Stand Up are supported. The device can upload the data to the education sharing system or platform.

   Attendance Check (Standalone)

   Face Attendance and Face Comparison are supported. The device can upload the data to the education sharing system or platform.
3. Click **Save**.

3.2 Face Attendance

The device detects and captures faces with both panoramic and PTZ channels or with the PTZ channel only. The data are used for comparison in Attendance Check (Standalone) mode or sent to connected platforms for attendance check.

3.2.1 Attendance Check Settings

Set the detection rules and parameters for each channel to capture face pictures.

Set Attendance Check Manually for PTZ Channel

The PTZ channel can detect and capture faces in multiple scenes. In manual mode, you can define the scenes by yourself.

Steps

1. Go to **VCA → Face Attendance → Attendance Check Settings** .
2. Select **Channel No.** as **Camera 01 (PTZ)** and check **Enable**.
3. **Optional:** Check **Display PTZ Range and Target**.

   A frame that marks the PTZ view range shows in the panoramic channel.
4. Select **Attendance Check** as **Manual**.
5. Set a detection scene.

1) Select a **Detection Scene**.
2) Click on the PTZ camera view and adjust it to the area you want to detect by the PTZ control buttons.
3) Click to save the detection scene.

Note

- You can click and drag the mouse on the PTZ camera view to quickly select the area.
- Repeat the steps to set multiple detection scenes. Arming schedule and patrol path are generated automatically after you set the detection scenes.
- Click to delete the current setting of the scene.

6. Set detection rules.
   1) Click and click on the PTZ camera view to draw an area. It is recommended that the area covers 1/2 to 2/3 of the image.

      The device detects faces in the chosen area.
   2) Click and draw a frame on the image.

      Faces with smaller pupil distance than the frame are not detected.
   3) Enter the **Mounting Height** of the device.

      Accurate setting of mounting height improves the detection performance.
   4) Click **Save**.
7. Edit arming schedule and patrol path. See ***Set Arming Schedule*** and ***Edit Patrol Path*** for details.
8. Set linkage method. See ***Linkage Method Settings*** .
9. Click **Save**.

Set Attendance Check Automatically for PTZ Channel

The PTZ channel can detect and capture faces in multiple scenes. In auto mode, you can generate a patrol path within the area enclosed by 4 limits.

Steps

1. Go to **VCA → Face Attendance → Attendance Check Settings** .
2. Select **Channel No.** as **Camera 01 (PTZ)** and check **Enable**.
3. **Optional:** Check **Display PTZ Range and Target**.

   A frame that marks the PTZ view range shows in the panoramic channel.
4. Select **Attendance Check** as **Auto**.
5. Set a detection scene.
   1) Click **Quick Set Detection Scene**.
   2) Set the upper left, upper right, lower left, and lower right limits.

      Example

      Adjust the PTZ camera view to the upper left of the area you want to detect by the PTZ control buttons. Click to save the **Upper Left Limit**.
   3) Click **Generate**.

Arming schedule and patrol path are generated automatically.

Note

- You can click and drag the mouse on the PTZ camera view to quickly select the area.
- Click to view the limit position.

6. Set detection rules.
   1) Click and draw a frame on the image.

      Faces with smaller pupil distance than the frame are not detected.
   2) Enter the **Mounting Height** of the device.

      Accurate setting of mounting height improves the detection performance.
   3) Click **Save**.
7. Edit arming schedule and patrol path. See ***Set Arming Schedule*** and ***Edit Patrol Path*** for details.
8. Set linkage method. See ***Linkage Method Settings*** .
9. Click **Save**.

Set Attendance Check for Panoramic Channel

You can set the rules for the panoramic channel to detect and capture faces.

Steps

1. Go to **VCA → Face Attendance → Attendance Check Settings** .
2. Select **Channel No.** as **Camera 02 (Panoramic)** and check **Enable**.
3. **Optional:** Check **Display PTZ Range and Target**.

   A frame that marks the PTZ view range shows in the panoramic channel.
4. Set detection rules.
   1) Click and click on the panoramic camera view to draw an area.

      The device detects faces in the chosen area.
   2) Click and draw a frame on the image.

      Faces with smaller pupil distance than the frame are not detected.
   3) Enter the **Mounting Height** of the device.

      Accurate setting of mounting height improves the detection performance.
   4) Click **Save**.
5. Set the arming schedule. See ***Set Arming Schedule*** .
6. Set linkage method. See ***Linkage Method Settings*** .
7. Click **Save**.

Algorithm Parameters

The algorithm parameters can be adjusted to optimize face capture.

Face Recognition Version

It refers to the current algorithm version, which cannot be edited.

Restore Defaults

Click **Restore** to restore all the settings in advanced configuration to the factory default.

Capture Parameters

Best Shot

The device captures the target picture with the highest score.

Capture Times

It refers to the times a face will be captured during its stay in the detection area.

Capture Threshold

It refers for the quality of face to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.

Remove Duplicated Faces

This function can filter out repeated captures of a face.

Similarity Threshold for Duplicates Removing

It is the similarity between the newly captured face and the picture in the duplicates removing library. When the similarity is higher than the value you set, the captured picture is regarded as a duplicated face and will be dropped.

Duplicates Removing Library Grading Threshold

It is the face grading threshold that triggers duplicates checking. When the face grading is higher than the set value, the captured face is compared with the face pictures that are already in the duplicates removing library.

Duplicates Removing Library Update Time

Every face picture is kept in the duplicates removing library for the set update time.

Quick Shot

The device captures the target picture once the score of the captured face exceeds the **Quick Shot Threshold** during the **Max. Capture Interval**. Otherwise, the device selects and uploads the picture with the highest score during the **Max. Capture Interval**.

Quick Shot Threshold

It refers to the quality of face to trigger quick shot.

Max. Capture Interval

It describes the max. time occupation for one quick shot.

Target Picture Settings

You can set the face picture type by selecting **Custom**, **Head Shot**, **Half-Body Shot**, or **Full-Body Shot**. If you select **Custom**, you can define detailed picture width and height of a picture freely.

If the captured pictures should have the same picture height, check **Fixed Value** and input desired picture height.

Face Exposure

Enable the function, and the device automatically adjusts exposure level when human faces appear in the scene.

Reference Brightness

It refers to the reference brightness of a face in the face exposure mode. If a face in the actual scene is brighter than the set reference brightness, the device lower the exposure level. If a face in the actual scene is darker than the set reference, the device increases the exposure level.

Minimum Duration

The extra time the device keeps the face exposure level after the face disappears in the scene.

Face Filtering

Face Filtering Time

It means the time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.

3.2.2 Face Comparison

Face comparison serves the purpose of face recognition by comparing the captured faces with those in face picture library.

To realize the face comparison, you should set up:

- Attendance check for capturing face pictures. See ***Attendance Check Settings*** for configuration instructions.
- Face picture library, see ***Set Face Picture Library*** for configuration instructions.
- Face picture comparison rule, see ***Set Face Picture Comparison*** for configuration instructions.

Set Face Picture Library

Face picture library is used to store modeled human faces and information.

Steps

1. Go to **VCA → Comparison and Modeling → Face Picture Library** .
2. Create a face picture library.
   1) Click + to add a face picture library.
   2) Input library name, threshold and remarks.

Threshold

Face similarity higher than the set threshold triggers face picture comparison alarm uploading.

3) Click **OK**.
4) **Optional:** Modify a face picture library. Select the desired library and click and change related parameters.
5) **Optional:** Delete a library. Select the desired library and click .

3. Add face pictures to the library.

Note

The picture format should be JPEG, and the size no larger than 300 K per file.

Add one face picture	Click **Add** and upload the face picture with detailed face information.
Import face pictures in batch	Click **Import** and select picture path. **Note** When you import face pictures in batch, the picture name is saved as the face name. For other face information, you should modify one by one manually. The verification code for exporting and importing should be a combination of 8 to 16 digits, containing numerics, upper case and lower case letters.

4. Optional: Modify face information.
1) Select a face picture library.
2) Select the target face picture. You can use the search function to locate the picture by inputting search conditions, and click **Search**.
3) Click **Modify**.
4) Edit detailed information.

Note

Face picture is not allowed to change.

5) Click **OK**.

5. Create models for each face picture in library.

Modeling process builds up face model for each face picture. Face model is compulsory for face picture comparison to take effect.

Modeling	Select one or more face pictures, and click **Modeling**.
Batch Modeling	Select a face picture library, and click **Batch Modeling**.

6. Optional: Repeat to create more face libraries.

Set Face Picture Comparison

The function compares captured pictures with face pictures in the library and outputs comparison result. Comparison result can trigger certain actions when arming schedule and linkage method are set.

Before You Start

You should first create a face picture library and add face pictures. See ***Set Face Picture Library*** .

Steps

1. Go to **VCA → Comparison and Modeling → Face Comparison and Modeling** .
2. Select **Face Picture Comparison**.
3. Check **Enable Face Picture Comparison**.
4. Select a face picture library as the reference.
5. Select desired face information to upload.
6. Select a face comparison mode.

Best Comparison
The device captures and compares the target face continuously when the face target stays in the detection area, and upload the best scored face picture and related alarm information when the target face leaves the area.

Quick Comparison
The device capture and compares the target face when the face grading exceeds the set **Face Grading Threshold for Capture**.

Face Grading Threshold for Capture

The face grading threshold for the device to judge whether to capture and upload the face or not.

Max. Capture Interval

The max. interval between two captures when the target is in the detection area. The camera takes the capture when it reaches the max. interval even if the face grading does not reach the set threshold.

Quick Setup Mode

Custom, **Face Attendance**, and **Face Recognition** are selectable. Select according to actual using scenarios. In custom mode, you can set **Comparison Timeout** and **Comparison Times**.

7. Set arming schedule. See ***Set Arming Schedule*** .
8. Set linkage method. See ***Linkage Method Settings*** .

View Face Comparison Result

Steps

1. Go to **Application**.
2. Set search condition and click **Counting**.

Matched results are shown in **Face Picture Comparison Statistics** area.

3.3 Student Stand Up

The device detects student behavior of standing up, sitting down, and walking around during the class. The device captures target pictures, shows the target in close-up, and sends alarms.

3.3.1 Basic Configuration

Set the detection area, arming schedule, and linkage method for the device to detect standing students.

Steps

1. Go to **VCA → Student Stood Up Event → Student Stand Up → Basic Configuration** .
2. Check **Enable**.
3. Click ⬡ and click on the live view image to draw a detection area. Right-click to complete drawing.
4. Set arming schedule and linkage method. See ***Set Arming Schedule*** and ***Linkage Method Settings*** .
5. Click **Save**.

3.3.2 Advanced Parameters

You can adjust the parameters so that the detection is suitable for your using environment.

Display Installation Reference Line

Check and a blue line shows on the panoramic live view image. Make sure the student desks are above the blue line when installing the device.

Note

You also need to enable **Display Rules Information** in **Configuration → Local** for the blue line to show.

False Alarm Level

The higher the false alarm level, the easier to detect student resting on the desk, but the false alarms of standing up will also be high. Run some tests in your using environment and set the level accordingly.

Rising Detection Level

The higher the rising detection level, the easier to detect student standing up. Run some tests in your using environment and set the level accordingly.

Standing Duration Level

Standing duration level is the estimated longest time that a student will stand. Level 0 to 4 equal to 45 sec, 1 min, 2 min, 5 min, and 8 min respectively.

For example, when the **Standing Duration Level** is set to ***0***, the device considers a standing student to be seated if they stand for more than 45 sec. If the student sits down after that, the device does not trigger sitting-down alarm.

Alarm Linkage

Select the alarm action when one student stands up.

Note

The alarm linkage is triggered when only one person stands up. More than one person standing up, sitting down, or walking around does not trigger alarm linkage.

Close

No alarm action is taken.

Linked Capture Configuration

The PTZ channel is linked to capture the face picture of the target. You should calibrate the PTZ and panoramic channels first. See ***Panorama Tracking*** for details.

Post-Alarm

When the alarm is over, the PTZ channel stays to capture the face for the set post-alarm time before resuming to the previous status.

Duration

The lasting time of linked capture.

Capture Ratio Factor

The smaller the value is, the larger the ratio is, and the larger the target is to the size of the captured picture.

Target Cropping

The third stream live view of the panoramic channel shows the close-up of the standing student.

Post-Alarm

When the alarm is over, the third stream live view stays for the set post-alarm time before resuming to the normal view.

3.4 Head-Up Rate

The device calculates the ratio of students who are paying attention to the teacher.

Check **Upload Head-up Rate** to upload the data to the connected education sharing system.

3.5 Empty Seat Rate

The device detects people in the detection area and calculates the ratio of empty seats.

Steps

1. Go to **VCA → Face Attendance → Empty Seat Rate** .
2. Check **Enable**.
3. Click ⬡ and click on the live view image to draw a detection area. Right-click to complete drawing.
4. Enter the total **Number of Seats** in the detection area.
5. Click **Save**.

3.6 School Timetable

The device receives a timetable from the platform and performs detection, capture, comparison, and alarm actions according to the timetable. The timetable applies to VCA in both channels and overrides the arming schedules.

Before You Start

Set the school timetable on platform and the platform sends the timetable to the device every day.

Steps

1. Go to **Configuration → School Timetable** .
2. Check **Enable**.
3. Select a **Week**.
4. **Optional:** Adjust the timetable. See ***Set Arming Schedule*** .

   VCA takes effect in the selected periods.
5. Click **Save**.

Chapter 4 PTZ

PTZ is an abbreviation for pan, tilt, and zoom. It means the movement options of the camera.

4.1 PTZ Control

In live view interface, you can use the PTZ control buttons to control the device panning, tilting, and zooming.

PTZ Control Panel

	Click and hold the directional button to pan/tilt the device. **Note** • You can set **Keyboard Control Speed** in **Configuration → PTZ → Basic Settings** . The speed of pan/tilt movement in live view is based on this speed level. • You can set **Max. Tilt-angle** in **Configuration → PTZ → Basic Settings** to limit tilt movement range.
	Click the button, then the device keeps panning. **Note** You can set **Auto Scan Speed** in **Configuration → PTZ → Basic Settings** . The higher the value you set, the faster the device pans.
	Drag the slider to adjust the speed of pan/tilt movement.

Note

You can set **Manual Control Speed** in **Configuration → PTZ → Basic Settings** .

Compatible	The control speed is same as **Keyboard Control Speed**.
Pedestrian	Choose **Pedestrian** when you monitor the pedestrians.
Non-motor Vehicle	Choose **Non-motor Vehicle** when you monitor the non-motor vehicles.
Motor Vehicle	Choose **Motor Vehicle** when you monitor the motor vehicles.
Auto	You are recommended to set it as **Auto** when the application scene of the speed dome is complicated.

To avoid blurred image resulted from fast zoom, you can check **Enable Proportional Pan** in **Configuration → PTZ → Basic Settings** . If you enable this function, the pan/tilt speed change according to the amount of zoom. When there is a large amount of zoom, the pan/tilt speed will be slower for keeping the image from moving too fast on the live view image.

Zoom in/out

	Click the button, and the lens zooms in.
	Click the button, and the lens zooms out.

Note

- You can set **Zooming Speed** in **Configuration → PTZ → Basic Settings** . The higher the value is, the faster the zooming speed is.
- You can set **Zoom Limit** in **Configuration → Image → Display Settings → Other** to limit the maximum value of the total zoom (digital zoom and optical zoom).

Focus

	Click the button, then the lens focuses near and the object nearby gets clear.
	Click the button, then the lens focuses far and the object far away gets clear.

Iris

	When the image is too dark, click the button to enlarge the iris.
	When the image is too bright, click the button to stop down the iris.

4.2 Set Preset

A preset is a predefined image position. For the defined preset, you can call the preset No. to view the position.

Steps

1. Click to show the setting panel, and click .
2. Use the PTZ control buttons to move the lens to the desired position.
3. Select a preset number from the preset list, and click to finish the setting.

Note

Some presets are predefined with special command. You can only call them but not configure them.

4. Repeat the steps above to set multiple presets.

Click the button to call the preset.

Click the button to delete the preset.

Note

You can delete all presets in **Configuration → PTZ → Clear Config** . Click **Clear All Presets**, and click **Save**.

What to do next

Go to **Configuration → PTZ → Basic Settings** to set preset freezing and preset speed.
After enabling preset freezing, the live image switches directly from one preset to another, without showing the areas between these two scenes. It also guarantees the masked area will not be seen when the device is moving.

4.2.1 Special Presets

Special presets are predefined with commands and unable to configure. You can call the presets to perform certain functions.

Preset No.	Function	Preset No.	Function
34	Back to origin	94	Remote reboot
35	Call patrol 1	96	Stop a scan
36	Call patrol 2	97	Start random scan
37	Call patrol 3	98	Start frame scan
38	Call patrol 4	99	Start auto scan
41	Call pattern 1	100	Start tilt scan
42	Call pattern 2	101	Start panorama scan
43	Call pattern 3	102	Call patrol 5
44	Call pattern 4	103	Call patrol 6
45	One-touch patrol	104	Call patrol 7
92	Set manual limits	105	Call patrol 8
93	Save manual limits		

4.3 Set Patrol Scan

Patrol scan is a function to automatically move among multiple presets.

Before You Start

Make sure that you have defined more than one presets. See ***Set Preset*** for detailed configuration.

Steps

1. Click to show the setting panel, and click to enter patrol setting interface.
2. Select a patrol number from the list and click .
3. Click + to add presets.

Preset

Select predefined preset.

Speed

Set the speed of moving from one preset to another.

Time

It is the duration staying on one patrol point.

× Delete the presets in patrol.

Adjust the preset order.

Note

A patrol can be configured with 32 presets at most, and 2 presets at least.

4. Click **OK** to finish a patrol setting.
5. Repeat the steps above to configure multiple patrols.
6. Operate patrols.

   Call the patrol.

   Stop patroling.

   Delete the patrol.

   Set the patrol.

Note

You can delete all patrols in **Configuration → PTZ → Clear Config** . Click **Clear All Patrols**, and click **Save**.

4.3.1 Set One-Touch Patrol

The device automatically adds presets to one patrol path and starts patrol scan.

Steps

1. Set two or more presets except special presets. For setting presets, refer to ***Set Preset*** .

   The device will automatically add presets to patrol path No.8.
2. Choose one of the following methods to enable the function.
   - Click .
   - Call patrol path No.8.
   - Select and call preset No.45.

4.4 Set Pattern Scan

The device can move as the recorded pattern.

Steps

1. Click to show the PTZ control panel, and click .
2. Select one pattern scan path that needs to be set.
3. Click to start recording pattern scan.
4. Click PTZ control buttons as demands.

Note

Recording stops when the space for pattern scan is 0%.

5. Click to complete one pattern scan path settings.
6. Click to call pattern scan.

Stop pattern scan.

Reset pattern scan path.

Delete the selected pattern scan.

Note

If you need to delete all the pattern scans, go to **Configuration → PTZ → Clear Config** , and check **Clear All Patterns**, and click **Save**.

4.5 Set Limit

The device can only move within the limited range.

Steps

1. Go to **Configuration → PTZ → Limit** .
2. Select **Limit Type**.

   Manual Stops

   It refers to the movement range limit when you control the device manually.

   Scan Stops

   It refers to the movement range limit when the device scans automatically.

   Note

   Scan limit is only supported by the device that has scan function.
3. Click **Set** and set limits according to the prompt on the live image.
4. **Optional:** Click **Clear** to clear the limit settings of the selected mode.
5. Click **Save**.
6. Check **Enable Limit**.

   Note

   If you need to cancal all the set patrol paths, go to **Configuration → PTZ → Clear Config** , select **Clear All PTZ Limited**, and click **Save**.

Result

The device can only move within the set region after saving the settings.

4.6 Set Initial Position

Initial position refers to the relative initial position of the device azimuth. You can set the initial position if you need to select one point in the scene as the base point.

Steps

1. Go to **Configuration → PTZ → Initial Position** .
2. Move the device to the needed position by manually controlling the PTZ control buttons.
3. Click **Set** to save the information of initial position.

   Call The device moves to the set initial position.

   Clear Clear the set initial position.

4.7 Set Scheduled Tasks

You can set the device to perform a certain task during a certain period.

Steps

1. Go to **Configuration → PTZ → Scheduled Tasks** .
2. Check **Enable Scheduled Task**.
3. Select the task type and set the period. For setting the period, refer to ***Set Arming Schedule*** .
4. Repeat step 3 to set more than one scheduled tasks.
5. Set **Park Time**. During the set task period, if you operate the device manually, the scheduled task will be suspended. When the manual operation is over, the device will continue to perform the scheduled task after the set park time.
6. Click **Save**.

Note

If you want to clear all scheduled tasks, go to **Configuration → PTZ → Clear Config** , check **Clear All Scheduled Tasks**, and click **Save**.

4.8 Set Park Action

You can set the device to perform an action (for example, preset or patrol) or return to a position after a period of inactivity (park time).

Before You Start

Set the action type first. For example, if you want to select patrol as park action, you should set the patrol. See ***Set Patrol Scan*** for details.

Steps

1. Go to **Configuration → PTZ → Park Action** .
2. Check **Enable Park Action**.
3. Set **Park Time**: the inactive time before the device starts park action.
4. Select **Action Type** according to your needs.
5. Select an **Action Type ID**, if you select patrol or preset as action type.

   When the action type is patrol, action type ID stands for patrol No. When the action type is preset, action type ID stands for preset No.

6. Click **Save**.

4.8.1 Set One-Touch Park

This function is used to start park instantly.

Steps

1. Refer to ***Set Park Action*** to set a park action.
2. Click to start one-touch park.

4.9 Panorama Tracking

This function links panoramic channel with PTZ channel through calibration. The PTZ channel tracks moving objects in panoramic channel and automatically adjusts its PTZ positions to keep the target in the center of PTZ view for more details.

4.9.1 Set Panorama Tracking

The PTZ channel tracks detected target after panoramic channel and PTZ channel.

Steps

1. Go to **Configuration → PTZ → Panorama Tracking** .
2. Select calibration mode.

Auto Calibration	Select the **Calibration Mode** as **Auto**, and click **Start Calibration**. The device starts calibration automatically. After calibration finished, click **Stop Calibration** and exit the interface.
Manual Calibration	Select and add calibration positions manually. The detailed manual calibration configuration is as follows.

1) Select the **Calibration Mode** as **Manual**
2) Select a calibration point in **Calibration Parameter** list.

   A numbered green cross is displayed on the panoramic image. You can drag the green cross to adjust its position.
3) Click **Add** to save the cross position in the panoramic channel.
4) Adjust PTZ to place the green cross in the PTZ camera channel to the same position as the green cross in panoramic camera channel. 1× zoom ratio is recommended.

   Note

   To quickly locate the desired point in the PTZ channel, you can click and click the target position in the PTZ channel.
5) Click to save the PTZ position of this calibration point.
6) Repeat the steps above to set at least 4 calibration points.

7) Click **Start Calibration**.

3. Check **Track**.
4. Click **Save** to finish calibration.

4.10 Set Power Off Memory

This function can resume the previous PTZ status of device after it restarting from a power-off.

Steps

1. Go to **Configuration → PTZ → Basic Settings** .
2. Select **Resume Time Point**. When the device stays at one position for the set resume time point or more, the position is saved as a memory point. The device returns to the last memory point when it restarts.
3. Click **Save**.

Chapter 5 Live View

It introduces the live view parameters, function icons and transmission parameters settings.

5.1 Live View Parameters

The supported functions vary depending on the model.

Note

For multichannel devices, select the desired channel first before live view settings.

5.1.1 Window Division

You can choose a layout for live view window.

- displays one live image. You can click ← → to switch between channels.
- displays live images in 2 × 2 layout.
- displays live images in PIP (picture in picture) layout.
- displays live images in 1 × 2 layout.
- displays live images in 2 × 1 layout.

5.1.2 Start and Stop Live View

On **Live View** page, click to start all live view. Click to stop all live view.

You can also start the live view of the channels one by one through clicking a divided window first and double-clicking a channel from the channel list on left.

5.1.3 Live View Stream Type

Select the live view stream type according to your needs. For the detailed information about the stream type selection, refer to ***Stream Type*** .

5.1.4 Start Digital Zoom

It helps to see a detailed information of any region in the image.

Steps

1. Click to enable the digital zoom.
2. In live view image, drag the mouse to select the desired region.
3. Click in the live view image to back to the original image.

5.1.5 Conduct Regional Focus

You can enable the function to focus on certain area.

Steps

Note

This function varies with the device model.

1. Click to enable regional focus.
2. Drag the mouse on the live view to draw a rectangle as the desired focus area.
3. Click to disable this function.

5.1.6 Conduct Regional Exposure

When the brightness of live view is not balanced, you can enable this function to optimize the exposure of the selected image region.

Steps

1. Click to enable regional exposure.
2. Drag the mouse on the live view to draw a rectangle as the desired exposure area.
3. Click to disable this function.

5.1.7 Lens Initialization

The lens automatically adjusts the zoom and focus value to default settings.

You can initialize the lens in two ways:

- Click on PTZ control panel to reset the lens parameters once.
- Select **Lens Initialization** as **ON** in **Configuration → Image → Display Settings** to reset the lens parameters once.

5.1.8 Conduct 3D Positioning

3D positioning is to relocate the selected area to the image center.

Steps

1. Click to enable the function.
2. Select a target area in live image.
   - Left click on a point on live image: the point is relocated to the center of the live image. With no zooming in or out effect.
   - Hold and drag the mouse to a lower right position to frame an area on the live: the framed area is zoomed in and relocated to the center of the live image.

- Hold and drag the mouse to an upper left position to frame an area on the live: the framed area is zoomed out and relocated to the center of the live image.

3. Click the button again to turn off the function.

5.2 Set Transmission Parameters

The live view image may be displayed abnormally according to the network conditions. In different network environments, you can adjust the transmission parameters to solve the problem.

Steps

1. Go to **Configuration → Local** .
2. Set the transmission parameters as required.

Protocol

TCP

TCP ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected. It is suitable for the stable network environment.

UDP

UDP is suitable for the unstable network environment that does not demand high video fluency.

MULTICAST

MULTICAST is suitable for the situation that there are multiple clients. You should set the multicast address for them before selection.

Note

For detailed information about multicast, refer to ***Multicast*** .

HTTP

HTTP is suitable for the situation that the third-party needs to get the stream from the device.

Play Performance

Shortest Delay

The device takes the real-time video image as the priority over the video fluency.

Balanced

The device ensures both the real-time video image and the fluency.

Fluent

The device takes the video fluency as the priority over teal-time. In poor network environment, the device cannot ensures video fluency even the fluency is enabled.

Custom

You can set the frame rate manually. In poor network environment, you can reduce the frame rate to get a fluent live view. But the rule information may cannot display.

Auto Start Live View

- **Yes** means the live view is started automatically. It requires a high performance monitoring device and a stable network environment.
- **No** means the live view should be started manually.

3. Click **OK**.

Chapter 6 Video and Audio

This part introduces the configuration of video and audio related parameters.

6.1 Video Settings

This part introduces the settings of video parameters, such as, stream type, video encoding, and resolution.

Go to setting page: **Configuration → Video/Audio → Video** .

Note

For device with multiple camera channels, select a channel before other settings.

6.1.1 Stream Type

For device supports more than one stream, you can specify parameters for each stream type.

Main Stream

The stream stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually means larger storage space and higher bandwidth requirements in transmission.

Sub Stream

The stream usually offers comparatively low resolution options, which consumes less bandwidth and storage space.

Other Streams

Steams other than the main stream and sub stream may also be offered for customized usage.

6.1.2 Video Type

Select the content (video and audio) that should be contained in the stream.

Video

Only video content is contained in the stream.

Video & Audio

Video content and audio content are contained in the composite stream.

6.1.3 Resolution

Select video resolution according to actual needs. Higher resolution requires higher bandwidth and storage.

6.1.4 Bitrate Type and Max. Bitrate

Constant Bitrate

It means that the stream is compressed and transmitted at a comparatively fixed bitrate. The compression speed is fast, but mosaic may occur on the image.

Variable Bitrate

It means that the device automatically adjust the bitrate under the set **Max. Bitrate**. The compression speed is slower than that of the constant bitrate. But it guarantees the image quality of complex scenes.

6.1.5 Video Quality

When **Bitrate Type** is set as Variable, video quality is configurable. Select a video quality according to actual needs. Note that higher video quality requires higher bandwidth.

6.1.6 Frame Rate

The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps).

A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout. Note that higher frame rate requires higher bandwidth and larger storage space.

6.1.7 Video Encoding

It stands for the compression standard the device adopts for video encoding.

Note

Available compression standards vary according to device models.

H.264

H.264, also known as MPEG-4 Part 10, Advanced Video Coding, is a compression standard. Without compressing image quality, it increases compression ratio and reduces the size of video file than MJPEG or MPEG-4 Part 2.

H.264+

H.264+ is an improved compression coding technology based on H.264. By enabling H.264+, you can estimate the HDD consumption by its maximum average bitrate. Compared to H.264, H.264+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

When H.264+ is enabled, **Max. Average Bitrate** is configurable. The device gives a recommended max. average bitrate by default. You can adjust the parameter to a higher value if the video quality is less satisfactory. Max. average bitrate should not be higher than max. bitrate.

Note

When H.264+ is enabled, **Video Quality**, **I Frame Interval**, **Profile** and **SVC** are not configurable.

H.265

H.265, also known as High Efficiency Video Coding (HEVC) and MPEG-H Part 2, is a compression standard. In comparison to H.264, it offers better video compression at the same resolution, frame rate and image quality.

H.265+

H.265+ is an improved compression coding technology based on H.265. By enabling H.265+, you can estimate the HDD consumption by its maximum average bitrate. Compared to H.265, H.265+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

When H.265+ is enabled, **Max. Average Bitrate** is configurable. The device gives a recommended max. average bitrate by default. You can adjust the parameter to a higher value if the video quality is less satisfactory. Max. average bitrate should not be higher than max. bitrate.

Note

When H.265+ is enabled, **Video Quality**, **I Frame Interval**, **Profile** and **SVC** are not configurable.

MJPEG

Motion JPEG (M-JPEG or MJPEG) is a video compression format in which intraframe coding technology is used. Images in a MJPEG format is compressed as individual JPEG images.

6.1.8 Profile

This function means that under the same bitrate, the more complex the profile is, the higher the quality of the image is, and the requirement for network bandwidth is also higher.

6.1.9 SVC

Scalable Video Coding (SVC) is the name for the Annex G extension of the H.264 or H.265 video compression standard.

The objective of the SVC standardization has been to enable the encoding of a high-quality video bitstream that contains one or more subset bitstreams that can themselves be decoded with a complexity and reconstruction quality similar to that achieved using the existing H.264 or H.265 design with the same quantity of data as in the subset bitstream. The subset bitstream is derived by dropping packets from the larger bitstream.

SVC enables forward compatibility for older hardware: the same bitstream can be consumed by basic hardware which can only decode a low-resolution subset, while more advanced hardware will be able decode high quality video stream.

6.1.10 I-Frame Interval

I-frame interval defines the number of frames between 2 I-frames.

In H.264 and H.265, an I-frame, or intra frame, is a self-contained frame that can be independently decoded without any reference to other images. An I-frame consumes more bits than other frames. Thus, video with more I-frames, in other words, smaller I-frame interval, generates more steady and reliable data bits while requiring more storage space.

6.1.11 Smoothing

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

6.2 Audio Settings

It is a function to set audio parameters such as audio encoding, environment noise filtering.

Go to the audio settings page: **Configuration → Video/Audio → Audio** .

6.2.1 Audio Input

External audio pick-up device is available for audio input, and audio encoding and input volume are configurable.

Audio Encoding

The device offers several compression standard. Select according to your need.

Audio Input

LineIn is supported for external audio pick-up device.

Input volume

Adjust the volume of the audio input.

6.2.2 Audio Output

You can output audio through line out. You can adjust the output volume according to your needs.

Note

- Connect audio output device according to your needs.
- This function is only supported by certain models.

6.2.3 Environmental Noise Filter

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

6.3 Two-way Audio

It is used to realize the two-way audio function between the monitoring center and the target in the monitoring screen.

Before You Start

- Make sure the audio input device (pick-up or microphone) and audio output device (speaker) connected to the device is working properly. Refer to specifications of audio input and output devices for device connection.
- If the device has built-in microphone and speaker, two-way audio function can be enabled directly.

Steps

1. Click **Live View**.
2. Click on the toolbar to enable two-way audio function of the camera.
3. Click , disable the two-way audio function.

6.4 Display Settings

It offers the parameter settings to adjust image features.

Go to **Configuration → Image → Display Settings** .

For device that supports multiple channels, display settings of each channel is required. The settings for different channels may be different. This part introduces all possible parameters among the channels.

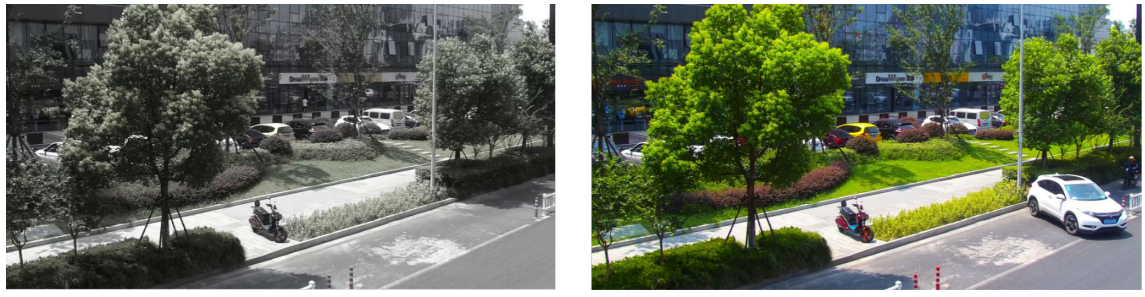
Click **Default** to restore settings.

6.4.1 Scene Mode

There are several sets of image parameters predefined for different installation environments. Select a scene according to the actual installation environment to speed up the display settings.

Image Adjustment

By adjusting the **Brightness**, **Saturation**, **Hue**, **Contrast** and **Sharpness**, the image can be best displayed.



Low Saturation High Saturation

Figure 6-1 Saturation

Exposure Settings

Exposure is controlled by the combination of iris, shutter, and gain. You can adjust image effect by setting exposure parameters.

Exposure Mode

Auto

The iris, shutter, and gain values are adjusted automatically.

You can limit the changing ranges of iris, shutter and gain by setting **Max. Iris Limit**, **Min. Iris Limit**, **Max. Shutter Limit**, **Min. Shutter Limit** and **Limit Gain** for better exposure effect.

Iris Priority

The value of iris needs to be adjusted manually. The shutter and gain values are adjusted automatically according to the brightness of the environment.

You can limit the changing ranges of the shutter and gain by setting **Max. Shutter Limit**, **Min. Shutter Limit** and **Limit Gain** for better exposure effect.

Shutter Priority

The value of shutter needs to be adjusted manually. The iris and gain values are adjusted automatically according to the brightness of the environment.

You can limit the changing ranges of the iris by setting **Max. Iris Limit**, **Min. Iris Limit** and **Limit Gain** for better exposure effect.

Manual

You need to set **Iris**, **Shutter**, and **Gain** manually.

Slow Shutter

The higher the slow shutter level is, the slower the shutter speed is. It ensures full exposure in underexposure condition.

Focus

It offers options to adjust the focus mode and the minimum focus distance.

Focus Mode

Auto

The device focuses automatically as the scene changes. If you cannot get a well-focused image under auto mode, reduce light sources in the image and avoid flashing lights.

Semi-auto

The device focuses once after the PTZ and lens zooming. If the image is clear, the focus does not change when the scene changes.

Manual

You can adjust the focus manually on the live view page.

Min. Focus Distance

When the distance between the scene and lens is shorter than the Min. Focus Distance, the lens does not focus.

Compatible

This mode is only recommended for indoor devices with a bubble when you cannot get a clear image with other options.

BLC

If the device focuses on an object against strong backlight, the object will be too dark to be seen clearly. BLC (backlight compensation) compensates light to the object in the front to make it clear. You can select the area that needs compensation lights.

HLC

When the bright area of the image is over-exposed and the dark area is under-exposed, the HLC (High Light Compression) function can be enabled to weaken the bright area and brighten the dark area, so as to achieve the light balance of the overall picture.

WDR

The WDR (Wide Dynamic Range) function helps the camera provide clear images in environment with strong illumination differences.

When there are both very bright and very dark areas simultaneously in the field of view, you can enable the WDR function and set the level. WDR automatically balances the brightness level of the whole image and provides clear images with more details.

Note

When WDR is enabled, some other functions may be not supported. Refer to the actual interface for details.

WDR Off WDR On

Figure 6-2 WDR

DNR

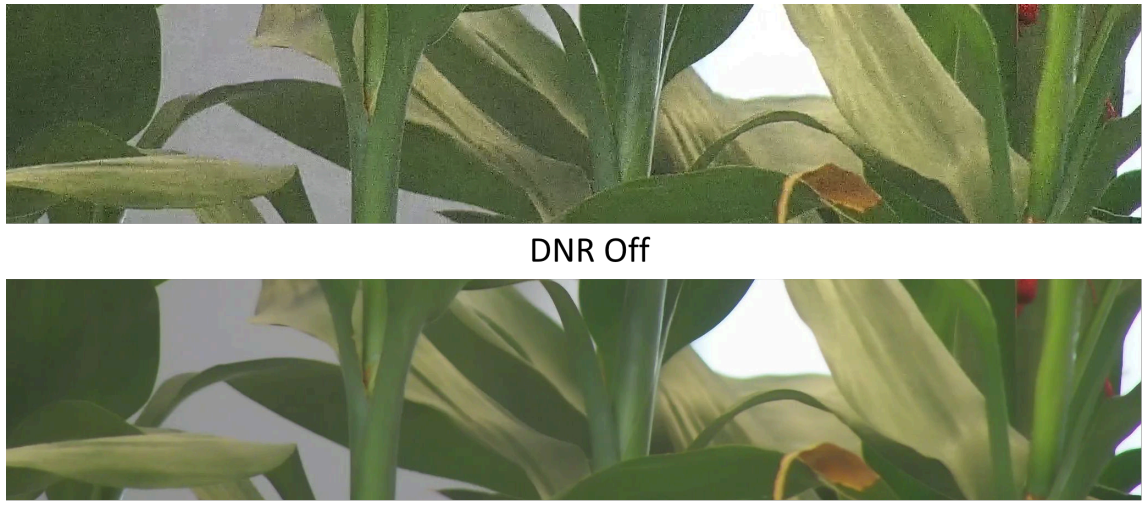
Digital Noise Reduction is used to reduce the image noise and improve the image quality. **Normal** and **Expert** modes are selectable.

Normal

Set the DNR level to control the noise reduction degree. The higher level means stronger reduction degree.

Expert

Set the DNR level for both space DNR and time DNR to control the noise reduction degree. The higher level means stronger reduction degree.



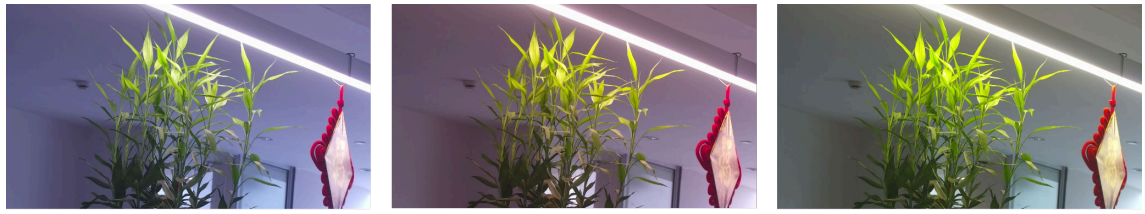
DNR Off

DNR On

Figure 6-3 DNR

White Balance

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



Cold Warm Auto White Balance

Figure 6-4 White Balance

6.4.2 Zoom Limit

You can set a certain value to limit the maximum value of zooming.

6.4.3 Lens Distortion Correction

For device equipped with motorized lens, image may appear distorted to some extent. Enable this function to correct the distortion.

Note

- This function is only supported by certain device equipped with motorized lens.
- The edge of image will be lost if this function is enabled.

6.4.4 Video Standard

Video standard is an ability of a video card or video display device that defines the amount of colors that are shown and the resolution. The two most common video standard used are NTSC and PAL. In NTSC, 30 frames are transmitted each second. Each frame is made up of 525 individual scan lines. In PAL, 25 frames are transmitted each second. Each frame is made up of 625 individual scan lines. Select video signal standard according to the video system in your country/region.

6.4.5 Image Parameters Switch

The device automatically switches image parameters in set time periods.

Go to image parameters switch setting page: **Configuration → Image → Image Parameters Switch** , and set parameters as needed.

Set Link to Preset

You can set a preset to switch the image to a linked scene.

Steps

1. Check **Link to Preset**.
2. Select a preset.
3. Check and set a time period and a linked scene mode.
4. Click **Save**.

Set Scheduled-switch

Switch the image to the linked scene mode automatically in certain time periods.

Steps

1. Check **Scheduled-switch**.
2. Select and configure the corresponding time period and linked scene mode.

   Note

   For Linked Scene configuration, refer to ***Scene Mode*** .
3. Click **Save**.

6.5 OSD

You can customize OSD (On-screen Display) information such as device name, time/date, font, color, and text overlay displayed on video stream.

Go to OSD setting page: **Configuration → Image → OSD Settings** .

Select a channel.

Set the corresponding parameters, and click **Save** to take effect.

Character Set

Select character set for displayed information. If Korean is required to displayed on screen, select **EUC-KR**. Otherwise, select **GBK**.

Displayed Information

Set camera name, date, week, and their related display format.

Text Overlay

Set customized overlay text on image.

OSD Parameters

Set OSD parameters, such as **Display Mode**, **OSD Size**, **Font Color**, and **Alignment**.

Chapter 7 Video Recording and Picture Capture

This part introduces the operations of capturing video clips and snapshots, playback, and downloading captured files.

7.1 Storage Settings

This part introduces the configuration of several common storage paths.

7.1.1 Memory Card

You can view the capacity, free space, status, type, and property of the memory card. Encryption of memory card is supported to ensure data security.

Set New or Unencrypted Memory Card

Before You Start

Insert a new or unencrypted memory card to the device. For detailed installation, refer to *Quick Start Guide* of the device.

Steps

1. Go to **Configuration → Storage → Storage Management → HDD Management** .
2. Select the memory card.

   Note

   If an **Unlock** button appears, you need to unlock the memory card first. See ***Detect Memory Card Status*** for details.
3. Click **Format** to initialize the memory card.

   When the **Status** of memory card turns from **Uninitialized** to **Normal**, the memory card is ready for use.
4. **Optional:** Encrypt the memory card.
   1) Click **Encrypted Format**.
   2) Set the encryption password.
   3) Click **OK**.

   When the **Encryption Status** turns to **Encrypted**, the memory card is ready for use.

   Note

   Keep your encryption password properly. Encryption password cannot be found if forgotten.
5. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.

6. Click **Save**.

Set Encrypted Memory Card

Before You Start

- Insert an encrypted memory card to the device. For detailed installation, refer to *Quick Start Guide* of the device.
- You need to know the correct encryption password of the memory card.

Steps

1. Go to **Configuration → Storage → Storage Management → HDD Management** .
2. Select the memory card.

   Note

   If an **Unlock** button appears, you need to unlock the memory card first. See ***Detect Memory Card Status*** for details.
3. Verify the encryption password.
   1) Click **Parity**.
   2) Enter the encryption password.
   3) Click **OK**.

   When the **Encryption Status** turns to **Encrypted**, the memory card is ready for use.

   Note

   If the encryption password is forgotten and you still want to use this memory card, see ***Set New or Unencrypted Memory Card*** to format and set the memory card. All existing contents will be removed.
4. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.
5. Click **Save**.

Detect Memory Card Status

The device detects the status of Hikvision memory card. You receive notifications when your memory card is detected abnormal.

Before You Start

The configuration page only appears when a Hikvision memory card is installed to the device.

Steps

1. Go to **Configuration → Storage → Storage Management → Memory Card Detection** .
2. Click **Status Detection** to check the **Remaining Lifespan** and **Health Status** of your memory card.

   Remaining Lifespan

It shows the percentage of the remaining lifespan. The lifespan of a memory card may be influenced by factors such as its capacity and the bitrate. You need to change the memory card if the remaining lifespan is not enough.

Health Status

It shows the condition of your memory card. There are three status descriptions: good, bad, and damaged. You will receive a notification if the health status is anything other than good when the **Arming Schedule** and **Linkage Method** are set.

Note

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

3. Click **R/W Lock** to set the permission of reading and writing to the memory card.
   - Add a Lock
     a. Select the **Lock Switch** as ON.
     b. Enter the password.
     c. Click **Save**
   - Unlock
     - If you use the memory card on the device that locks it, unlocking will be done automatically and no unlocking procedures are required on the part of users.
     - If you use the memory card (with a lock) on a different device, you can go to **HDD Management** to unlock the memory card manually. Select the memory card, and click **Unlock**. Enter the correct password to unlock it.
   - Remove the Lock
     a. Select the **Lock Switch** as OFF.
     b. Enter the password in **Password Settings**.
     c. Click **Save**.

Note

- Only admin user can set the **R/W Lock**.
- The memory card can only be read and written when it is unlocked.
- If the device, which adds a lock to a memory card, is restored to the factory settings, you can go to **HDD Management** to unlock the memory card.

4. Set **Arming Schedule** and **Linkage Method**. See ***Set Arming Schedule*** and ***Linkage Method Settings*** for details.
5. Click **Save**.

7.1.2 Set FTP

You can configure the FTP server to save images which are captured by events or a timed snapshot task.

Before You Start
Get the FTP server address first.

Steps

1. Go to **Configuration → Network → Advanced Settings → FTP** .
2. Configure FTP settings.

   FTP Protocol

   FTP and SFTP are selectable. The files uploading is encrypted by using SFTP protocol.

   Server Address and Port

   The FTP server address and corresponding port.

   User Name and Password

   The FTP user should have the permission to upload pictures.

   If the FTP server supports picture uploading by anonymous users, you can check **Anonymous** to hide your device information during uploading.

   Directory Structure

   The saving path of snapshots in the FTP server.

   Picture Filing Interval

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

   Picture Name

   Set the naming rule for captured pictures. You can choose **Default** in the drop-down list to use the default rule, that is, IP address_channel number_capture time_event type.jpg (e.g., 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg). Or you can customize it by adding a **Custom Prefix** to the default naming rule.
3. Check **Upload Picture** to enable uploading snapshots to the FTP server.
4. Click **Test** to verify the FTP server.
5. Click **Save**.

7.1.3 Set NAS

Take network server as network disk to store the record files, captured images, etc.

Before You Start

Get the IP address of the network disk first.

Steps

1. Go to NAS setting page: **Configuration → Storage → Storage Management → Net HDD** .
2. Click **HDD No.**. Enter the server address and file path for the disk.

   Server Address

   The IP address of the network disk.

   File Path

The saving path of network disk files.

Mounting Type

Select file system protocol according to the operation system.

Enter user name and password of the net HDD to guarantee the security if **SMB/CIFS** is selected.

3. Click **Test** to check whether the network disk is available.
4. Click **Save**.

7.1.4 Set Cloud Storage

It helps to upload the captured pictures and data to the cloud. The platform requests picture directly from the cloud for picture and analysis. The function is only supported by certain models.

Steps

Caution

If the cloud storage is enabled, the pictures are stored in the cloud video manager firstly.

1. Go to **Configuration → Storage → Storage Management → Cloud Storage** .
2. Check **Enable Cloud Storage**.
3. Set basic parameters.

Protocol Version	The protocol version of the cloud video manager.
Server IP	The IP address of the cloud video manager. It supports IPv4 address.
Serve Port	The port of the cloud video manager. You are recommended to use the default port.
AccessKey	The key to log in to the cloud video manager.
SecretKey	The key to encrypt the data stored in the cloud video manager.
User Name and Password	The user name and password of the cloud video manager.
Picture Storage Pool ID	The ID of the picture storage region in the cloud video manager. Make sure storage pool ID and the storage region ID are the same.

4. Click **Test** to test the configured settings.
5. Click **Save**.

7.1.5 eMMC Protection

It is to automatically stop the use of eMMC as a storage media when its health status is poor.

Note

The eMMC protection is only supported by certain device models with an eMMC hardware.

Go to **Configuration → System → Maintenance → System Service** for the settings.

eMMC, short for embedded multimedia card, is an embedded non-volatile memory system. It is able to store the captured images or videos of the device.

The device monitors the eMMC health status and turns off the eMMC when its status is poor. Otherwise, using a worn-out eMMC may lead to device boot failure.

7.2 Video Recording

This part introduces the operations of manual and scheduled recording, playback, and downloading recorded files.

7.2.1 Record Automatically

The device records video automatically during configured time periods.

Before You Start

Select **Trigger Recording** in event settings for each record type except **Continuous**. See ***Event and Alarm*** for details.

Steps

1. Go to **Configuration → Storage → Schedule Settings → Record Schedule** .
2. Select channel No.
3. Check **Enable**.
4. Select a record type.

   Note

   The record type is vary according to different models.

   Continuous

   The video will be recorded continuously according to the schedule.

   Target Capture

   When target capture is triggered, the device automatically records videos.

   Event

   The video is recorded when configured event is detected.
5. Set schedule for the selected record type. Refer to ***Set Arming Schedule*** for the setting operation.
6. Click **Advanced** to set the advanced settings.

   Overwrite

Enable **Overwrite** to overwrite the video records when the storage space is full. Otherwise the camera cannot record new videos.

Pre-record

The time period you set to record before the scheduled time.

Post-record

The time period you set to stop recording after the scheduled time.

Stream Type

Select the stream type for recording.

Note

When you select the stream type with higher bitrate, the actual time of the pre-record and post-record may be less than the set value.

Recording Expiration

The recordings are deleted when they exceed the expired time. The expired time is configurable. Note that once the recordings are deleted, they can not be recovered.

7. Click **Save**.

7.2.2 Record Manually

Steps

1. Go to **Configuration → Local** .
2. Set the **Record File Size** and saving path to for recorded files.
3. Click **Save**.
4. Click in the live view interface to start recording. Click to stop recording.

7.2.3 Playback and Download Video

You can search, playback and download the videos stored in the local storage or network storage.

Steps

1. Click **Playback**.
2. Select channel No.
3. Set search condition and click **Search**.

   The matched video files showed on the timing bar.
4. Click to play the video files.
   - Click to clip video files.
   - Click to play video files in full screen. Press **ESC** to exit full screen.

Note

Go to **Configuration → Local** , click **Save clips to** to change the saving path of clipped video files.

5. Click on the playback interface to download files.
   1) Set search condition and click **Search**.
   2) Select the video files and then click **Download**.

   Note

   Go to **Configuration → Local** , click **Save downloaded files to** to change the saving path of downloaded video files.

7.3 Capture Configuration

The device can capture the pictures manually or automatically and save them in configured saving path. You can view and download the snapshots.

7.3.1 Capture Automatically

This function can capture pictures automatically during configured time periods.

Before You Start

If event-triggered capture is required, you should configure related linkage methods in event settings. Refer to ***Event and Alarm*** for event settings.

Steps

1. Go to **Configuration → Storage → Schedule Settings → Capture → Capture Parameters** .
2. Set the capture type.

   Timing

   Capture a picture at the configured time interval.

   Event-Triggered

   Capture a picture when an event is triggered.
3. Set the **Format**, **Resolution**, **Quality**, **Interval**, and **Capture Number**.
4. Refer to ***Set Arming Schedule*** for configuring schedule time.
5. Click **Save**.

7.3.2 Capture Manually

Steps

1. Go to **Configuration → Local** .
2. Set the **Image Format** and saving path to for snapshots.

   JPEG

The picture size of this format is comparatively small, which is better for network transmission.

BMP

The picture is compressed with good quality.

3. Click **Save**.
4. Click near the live view or play back window to capture a picture manually.

7.3.3 View and Download Picture

You can search, view and download the pictures stored in the local storage or network storage.

Steps

1. Click **Picture**.
2. Select channel No.
3. Set search condition and click **Search**.

   The matched pictures showed in the file list.
4. Select the pictures then click **Download** to download them.

Note

Go to **Configuration → Local** , click **Save snapshots when playback** to change the saving path of pictures.

Chapter 8 Event and Alarm

This part introduces the configuration of events. The device takes certain response to triggered alarm.

8.1 Basic Event

8.1.1 Set Video Tampering Alarm

When the configured area is covered and cannot be monitored normally, the alarm is triggered and the device takes certain alarm response actions.

Steps

1. Go to **Configuration → Event → Basic Event → Video Tampering** .
2. Select the channel number.
3. Check **Enable**.
4. Set the **Sensitivity**. The higher the value is, the easier to detect the area covering.
5. Click **Draw Area** and drag the mouse in the live view to draw the area.

Stop Drawing	Finish drawing.
Clear All	Delete all the drawn areas.

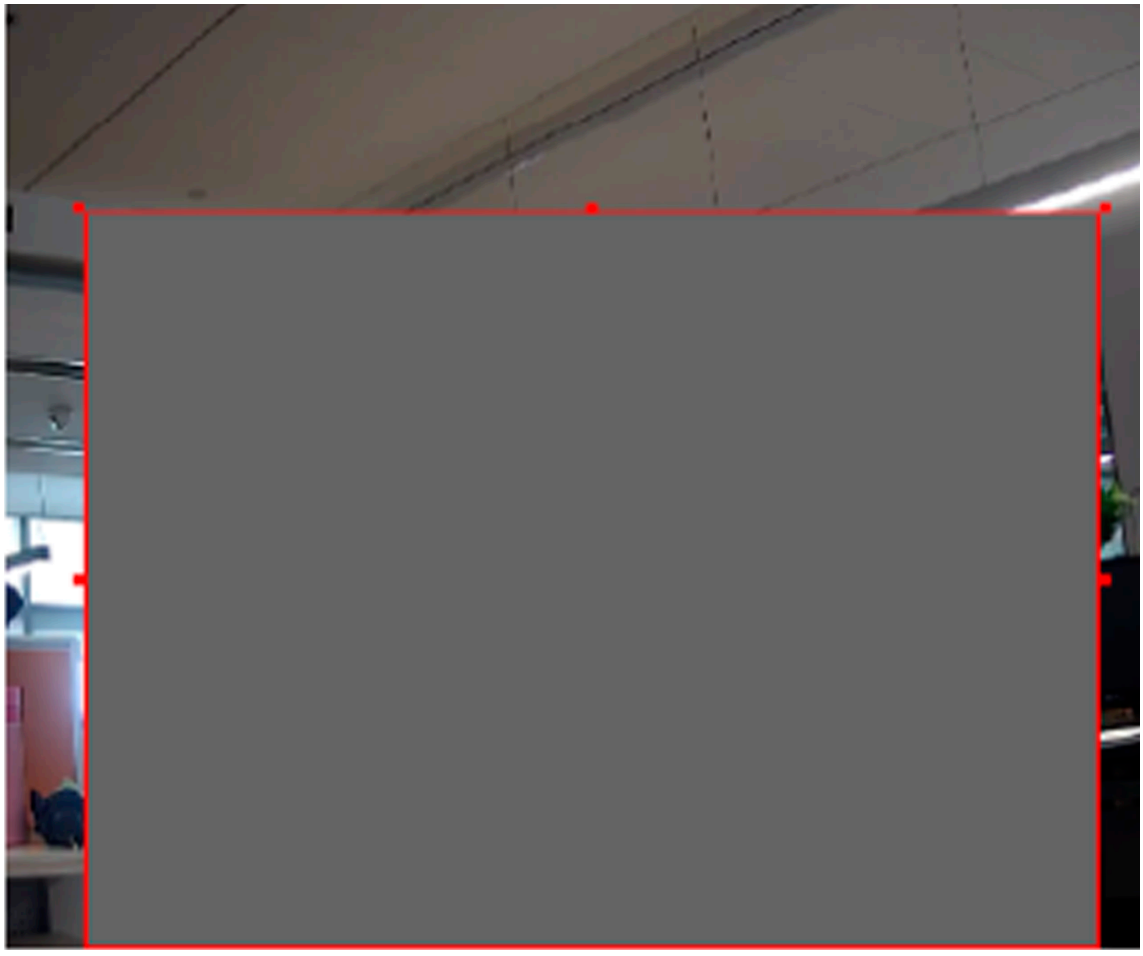


Figure 8-1 Set Video Tampering Area

6. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
7. Click **Save**.

8.1.2 Set Exception Alarm

Exceptions such as network disconnection can trigger the device to take corresponding action.

Steps

1. Go to **Configuration → Event → Basic Event → Exception** .
2. Select **Exception Type**.

HDD Full	The HDD storage is full.
HDD Error	Error occurs in HDD.
Illegal Login	Incorrect user name or password is entered.

3. Refer to ***Linkage Method Settings*** for setting linkage method.

4. Click **Save**.

8.2 Smart Event

Note

- For certain device models, you need to enable the smart event function on **VCA Resource** page first to show the function configuration page.
- The function varies according to different models.

8.2.1 Detect Audio Exception

Audio exception detection function detects the abnormal sound in the scene, such as the sudden increase/decrease of the sound intensity, and some certain actions can be taken as response.

Steps

1. Go to **Configuration → Event → Smart Event → Audio Exception Detection** .
2. Select one or several audio exception detection types.

   Audio Loss Detection

   Detect sudden loss of audio track.

   Sudden Increase of Sound Intensity Detection

   Detect sudden increase of sound intensity. **Sensitivity** and **Sound Intensity Threshold** are configurable.

   Note

   - The lower the sensitivity is, the more significant the change should be to trigger the detection.
   - The sound intensity threshold refers to the sound intensity reference for the detection. It is recommended to set as the average sound intensity in the environment. The louder the environment sound, the higher the value should be. You can adjust it according to the real environment.

   Sudden Decrease of Sound Intensity Detection

   Detect sudden decrease of sound intensity. **Sensitivity** is configurable.
3. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage methods.
4. Click **Save**.

Note

The function varies according to different models.

Chapter 9 Arming Schedule and Alarm Linkage

Arming schedule is a customized time period in which the device performs certain tasks. Alarm linkage is the response to the detected certain incident or target during the scheduled time.

9.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

1. Click **Arming Schedule**.
2. Drag the time bar to draw desired valid time.

   Note

   Up to 8 periods can be configured for one day.

3. Adjust the time period.
   - Click on the selected time period, and enter the desired value. Click **Save**.
   - Click on the selected time period. Drag the both ends to adjust the time period.
   - Click on the selected time period, and drag it on the time bar.
4. **Optional:** Click **Copy to...** to copy the same settings to other days.
5. Click **Save**.

9.1.1 Edit Patrol Path

The PTZ channel detects scenes in order. You can edit the order of scenes and the time that the camera stays in each scene.

Before You Start

Set multiple detection scenes.

Steps

1. Go to **VCA → Face Attendance → Attendance Check Settings → Arming Schedule** .
2. Click **Edit Patrol Path**.
3. Add scenes.

Quick Add	Generate a patrol path automatically.
Add	Add a detection scene to the patrol path.
	Adjust the order of the scenes.
×	Remove the detection scene from the path.

4. Set the **Dwell Time** for each scene.

   The camera stays at one scene for the set dwell time and then turns to the next scene.

5. Click **OK**.

9.2 Linkage Method Settings

You can enable the linkage functions when an event or alarm occurs.

9.2.1 FTP/NAS/Memory Card Uploading

If you have enabled and configured the FTP/NAS/memory card uploading, the device sends the alarm information to the FTP server, network attached storage and memory card when an alarm is triggered.

Refer to ***Set FTP*** to set the FTP server.

Refer to ***Set NAS*** for NAS configuration.

Refer to ***Set New or Unencrypted Memory Card*** for memory card storage configuration.

9.2.2 Send Email

Check **Send Email**, and the device sends an email to the designated addresses with alarm information when an alarm event is detected.

For email settings, refer to ***Set Email*** .

Set Email

When the email is configured and **Send Email** is enabled as a linkage method, the device sends an email notification to all designated receivers if an alarm event is detected.

Before You Start

Set the DNS server before using the Email function. Go to **Configuration → Network → Basic Settings → TCP/IP** for DNS settings.

Steps

1. Go to email settings page: **Configuration → Network → Advanced Settings → Email** .
2. Set email parameters.
   1) Input the sender's email information, including the **Sender's Address**, **SMTP Server**, and **SMTP Port**.
   2) **Optional:** If your email server requires authentication, check **Authentication** and input your user name and password to log in to the server.
   3) Set the **E-mail Encryption**.

- When you select **TLS**, and disable STARTTLS, emails are sent after encrypted by TLS. The SMTP port should be set as 465.
- When you select **TLS** and **Enable STARTTLS**, emails are sent after encrypted by STARTTLS, and the SMTP port should be set as 25.

Note

If you want to use STARTTLS, make sure that the protocol is supported by your email server. If you check the **Enable STARTTLS** while the protocol is not supported by your email sever, your email is sent with no encryption.

4) **Optional:** If you want to receive notification with alarm pictures, check **Attached Image**. The notification email has 3 attached alarm pictures about the event with configurable image capturing interval.
5) Input the receiver's information, including the receiver's name and address.
6) Click **Test** to see if the function is well configured.

3. Click **Save**.

9.2.3 Notify Surveillance Center

Check **Notify Surveillance Center**, the alarm information is uploaded to the surveillance center when an alarm event is detected.

9.2.4 Trigger Recording

Check **Trigger Recording**, and the device records the video about the detected alarm event.

For device with more than one camera channels, you can set one or more channels to take recordings if needed.

For recording settings, refer to ***Video Recording and Picture Capture*** .

Chapter 10 Network Settings

10.1 TCP/IP

TCP/IP settings must be properly configured before you operate the device over network. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.

Go to **Configuration → Network → Basic Settings → TCP/IP** for parameter settings.

NIC Type

Select a NIC (Network Interface Card) type according to your network condition.

IPv4

Two IPv4 modes are available.

DHCP

The device automatically gets the IPv4 parameters from the network if you check **DHCP**. The device IP address is changed after enabling the function. You can use SADP to get the device IP address.

Note

The network that the device is connected to should support DHCP (Dynamic Host Configuration Protocol).

Manual

You can set the device IPv4 parameters manually. Input **IPv4 Address**, **IPv4 Subnet Mask**, and **IPv4 Default Gateway**, and click **Test** to see if the IP address is available.

IPv6

Three IPv6 modes are available.

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.

Note

Route advertisement mode requires the support from the router that the device is connected to.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Input **IPv6 Address**, **IPv6 Subnet**, **IPv6 Default Gateway**. Consult the network administrator for required information.

MTU

It stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.

The valid value range of MTU is 1280 to 1500.

DNS

It stands for domain name server. It is required if you need to visit the device with domain name. And it is also required for some applications (e.g., sending email). Set **Preferred DNS Server** and **Alternate DNS server** properly if needed.

Dynamic Domain Name

Check **Enable Dynamic Domain Name** and input **Register Domain Name**. The device is registered under the register domain name for easier management within the local area network.

Note

DHCP should be enabled for the dynamic domain name to take effect.

10.1.1 Multicast

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneously.

Go to **Configuration → Network → Basic Settings → Multicast** for the multicast settings.

For a device with more than one channel, multicast can be set independently for each channel.

IP Address

It stands for the address of multicast host.

Stream Type

The stream type as the multicast source.

Video Port

The video port of the selected stream.

Audio Port

The audio port of the selected stream.

10.1.2 Multicast Discovery

Check the **Enable Multicast Discovery**, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.

10.2 Port

The device port can be modified when the device cannot access the network due to port conflicts.

Caution

Do not modify the default port parameters at will, otherwise the device may be inaccessible.

Go to **Configuration → Network → Basic Settings → Port** for port settings.

HTTP Port

It refers to the port through which the browser accesses the device. For example, when the **HTTP Port** is modified to 81, you need to enter ***http://192.168.1.64:81*** in the browser for login.

HTTPS Port

It refers to the port through which the browser accesses the device with certificate. Certificate verification is required to ensure the secure access.

RTSP Port

It refers to the port of real-time streaming protocol.

SRTP Port

It refers to the port of secure real-time transport protocol.

Server Port

It refers to the port through which the client adds the device.

Enhanced SDK Service Port

It refers to the port through which the client adds the device. Certificate verification is required to ensure the secure access.

WebSocket Port

TCP-based full-duplex communication protocol port for plug-in free preview.

WebSockets Port

TCP-based full-duplex communication protocol port for plug-in free preview. Certificate verification is required to ensure the secure access.

Note

- Enhanced SDK Service Port, WebSocket Port, and WebSockets Port are only supported by certain models.
- For device models that support that function, go to **Configuration → Network → Advanced Settings → Network Service** to enable it.

10.3 Port Mapping

By setting port mapping, you can access devices through the specified port.

Before You Start
When the ports in the device are the same as those of other devices in the network, refer to ***Port*** to modify the device ports.

Steps
1. Go to **Configuration → Network → Basic Settings → NAT** .
2. Select the port mapping mode.

Auto Port Mapping	Refer to ***Set Auto Port Mapping*** for detailed information.
Manual Port Mapping	Refer to ***Set Manual Port Mapping*** for detailed information.

3. Click **Save**.

10.3.1 Set Auto Port Mapping

Steps
1. Check **Enable UPnP™**, and choose a friendly name for the camera, or you can use the default name.
2. Select the port mapping mode to **Auto**.
3. Click **Save**.

Note
UPnP™ function on the router should be enabled at the same time.

10.3.2 Set Manual Port Mapping

Steps
1. Check **Enable UPnP™**, and choose a friendly name for the device, or you can use the default name.
2. Select the port mapping mode to **Manual**, and set the external port to be the same as the internal port.
3. Click **Save**.

What to do next
Go to the router port mapping settings interface and set the port number and IP address to be the same as those on the device. For more information, refer to the router user manual.

10.3.3 Set Port Mapping on Router

The following settings are for a certain router. The settings vary depending on different models of routers.

Steps

1. Select the **WAN Connection Type**.
2. Set the **IP Address**, **Subnet Mask** and other network parameters of the router.
3. Go to **Forwarding → Virtual Severs** , and input the **Port Number** and **IP Address**.
4. Click **Save**.

Example

When the cameras are connected to the same router, you can configure the ports of a camera as 80, 8000, and 554 with IP address 192.168.1.23, and the ports of another camera as 81, 8001, 555, 8201 with IP 192.168.1.24.

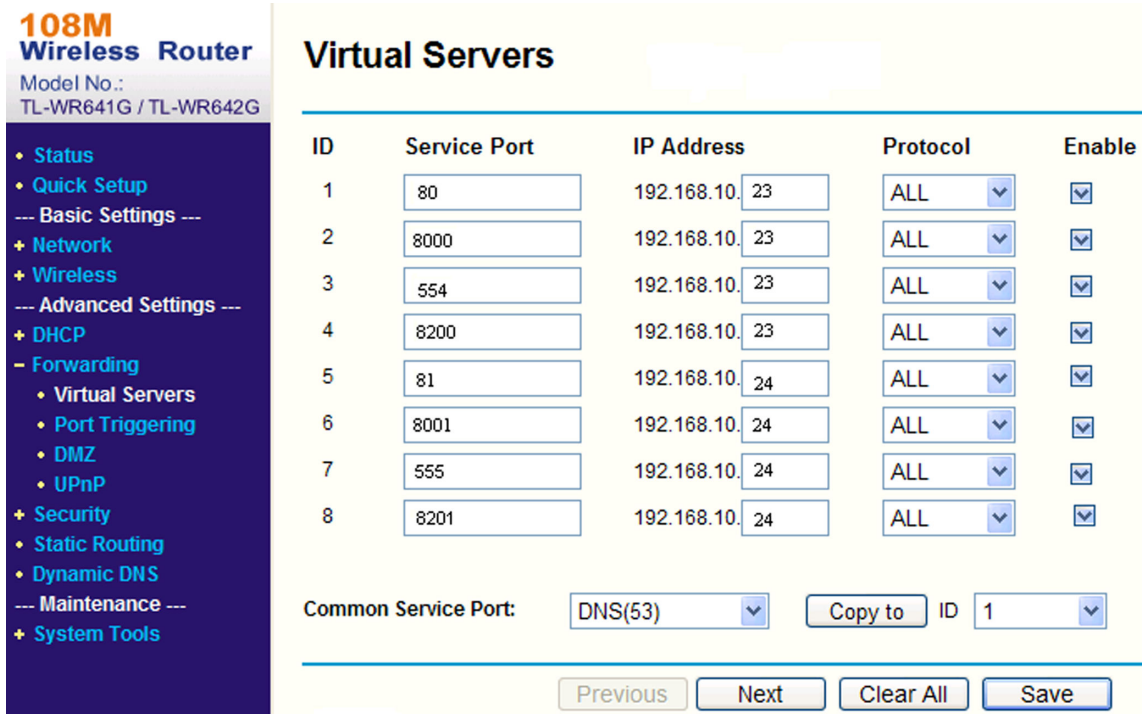


Figure 10-1 Port Mapping on Router

Note

The port of the network camera cannot conflict with other ports. For example, some web management port of the router is 80. Change the camera port if it is the same as the management port.

10.4 SNMP

You can set the SNMP network management protocol to get the alarm event and exception messages in network transmission.

Before You Start
Before setting the SNMP, you should download the SNMP software and manage to receive the device information via SNMP port.

Steps
1. Go to the settings page: **Configuration → Network → Advanced Settings → SNMP** .
2. Check **Enable SNMPv1**, **Enable SNMP v2c** or **Enable SNMPv3**.

Note
The SNMP version you select should be the same as that of the SNMP software.
And you also need to use the different version according to the security level required. SNMP v1 is not secure and SNMP v2 requires password for access. And SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.

3. Configure the SNMP settings.
4. Click **Save**.

10.5 Access to Device via Domain Name

You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

Before You Start
Registration on the DDNS server is required before configuring the DDNS settings of the device.

Steps
1. Refer to ***TCP/IP*** to set DNS parameters.
2. Go to the DDNS settings page: **Configuration → Network → Basic Settings → DDNS** .
3. Check **Enable DDNS** and select **DDNS type**.

   DynDNS

   Dynamic DNS server is used for domain name resolution.

   NO-IP

   NO-IP server is used for domain name resolution.
4. Input the domain name information, and click **Save**.
5. Check the device ports and complete port mapping. Refer to ***Port*** to check the device port , and refer to ***Port Mapping*** for port mapping settings.
6. Access the device.

By Browsers	Enter the domain name in the browser address bar to access the device.

By Client Software Add domain name to the client software. Refer to the client manual for specific adding methods.

10.6 Access to Device via PPPoE Dial Up Connection

This device supports the PPPoE auto dial-up function. The device gets a public IP address by ADSL dial-up after the device is connected to a modem. You need to configure the PPPoE parameters of the device.

Steps

1. Go to **Configuration → Network → Basic Settings → PPPoE** .
2. Check **Enable PPPoE**.
3. Set the PPPoE parameters.

   Dynamic IP

   After successful dial-up, the dynamic IP address of the WAN is displayed.

   User Name

   User name for dial-up network access.

   Password

   Password for dial-up network access.

   Confirm

   Input your dial-up password again.
4. Click **Save**.
5. Access the device.

   By Browsers Enter the WAN dynamic IP address in the browser address bar to access the device.

   By Client Software Add the WAN dynamic IP address to the client software. Refer to the client manual for details.

Note

The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (e.g. DynDns.com). Refer to ***Access to Device via Domain Name*** for detail information.

10.7 Set ISUP

When the device is registered on ISUP platform (formerly called Ehome), you can visit and manage the device, transmit data, and forward alarm information over public network.

Steps

1. Go to **Configuration → Network → Advanced Settings → Platform Access** .
2. Select **ISUP** as the platform access mode.
3. Select **Enable**.
4. Select a protocol version and input related parameters.
5. Click **Save**.

   Register status turns to **Online** when the function is correctly set.

10.8 Set Open Network Video Interface

If you need to access the device through Open Network Video Interface protocol, you can configure the user settings to enhance the network security.

Steps

1. Go to **Configuration → Network → Advanced Settings → Integration Protocol** .
2. Check **Enable Open Network Video Interface**.
3. Click **Add** to configure the Open Network Video Interface user.

   Delete Delete the selected Open Network Video Interface user.

   Modify Modify the selected Open Network Video Interface user.
4. Click **Save**.
5. **Optional:** Repeat the steps above to add more Open Network Video Interface users.

10.9 Set Network Service

You can control the ON/OFF status of certain protocol as desired.

Steps

Note

This function varies according to different models.

1. Go to **Configuration → Network → Advanced Settings → Network Service** .
2. Set network service.

   WebSocket & WebSockets

   WebSocket or WebSockets protocol should be enabled if you use Google Chrome 57 and its above version or Mozilla Firefox 52 and its above version to visit the device. Otherwise, live view, image capture, digital zoom, etc. cannot be used.

   If the device uses HTTP, enable WebSocket.

   If the device uses HTTPS, enable WebSockets.

   When you use WebSockets, select the **Server Certificate**.

Note

Complete certificate management before selecting server certificate. Refer to ***Certificate Management*** for detailed information.

SDK Service & Enhanced SDK Service

Check **Enable SDK Service** to add the device to the client software with SDK protocol.

Check **Enable Enhanced SDK Service** to add the device to the client software with SDK over TLS protocol.

When you use Enhanced SDK Service, select the **Server Certificate**.

Note

- Complete certificate management before selecting server certificate. Refer to ***Certificate Management*** for detailed information.
- When set up connection between the device and the client software, it is recommended to use Enhanced SDK Service and set the communication in Arming Mode to encrypt the data transmission. See the user manual of the client software for the arming mode settings.

TLS (Transport Layer Security)

The device offers TLS1.1, TLS1.2 and TLS1.3. Enable one or more protocol versions according to your need.

Bonjour

Uncheck to disable the protocol.

3. Click **Save**.

10.10 Set Alarm Server

The device can send alarms to destination IP address or host name through HTTP, HTTPS, or ISUP protocol. The destination IP address or host name should support HTTP, HTTP, or ISUP data transmission.

Steps

1. Go to **Configuration → Network → Advanced Settings → Alarm Server** .
2. Enter **Destination IP or Host Name**, **URL**, and **Port**.
3. Select **Protocol**.

Note

HTTP, HTTPS, and ISUP are selectable. It is recommended to use HTTPS, as it encrypts the data transmission during communication.

4. Click **Test** to check if the IP or host is available.
5. Click **Save**.

10.11 TCP Acceleration

TCP acceleration is used to improve latency and reduce packet loss caused by network congestion in poor network condition, and guarantee the fluency of live view.

10.12 Traffic Shaping

Traffic shaping is used to shape and smooth video data packet before transmission.

It helps to improve latency and reduce packet loss caused by network congestion and ensure the video quality as well. Shaping level is configurable.

10.13 Set SRTP

The Secure Real-time Transport Protocol (SRTP) is a Real-time Transport Protocol (RTP) internet protocol, intended to provide encryption, message authentication and integrity, and replay attack protection to the RTP data in both unicast and multicast applications.

Steps

1. Go to **Configuration → Network → Advanced Settings → SRTP** .
2. Select **Server Certificate**.
3. Select **Encrypted Algorithm**.
4. Click **Save**.

Note

- Only certain device models support this function.
- If the function is abnormal, check if the selected certificate is abnormal in certificate management.

Chapter 11 System and Security

It introduces system maintenance, system settings and security management, and explains how to configure relevant parameters.

11.1 View Device Information

You can view device information, such as Device No., Model, Serial No. and Firmware Version.

Enter **Configuration → System → System Settings → Basic Information** to view the device information.

11.2 Restore and Default

Restore and Default helps restore the device parameters to the default settings.

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance** .
2. Click **Restore** or **Default** according to your needs.

Restore Reset device parameters, except user information, IP parameters and video format to the default settings.

Default Reset all the parameters to the factory default.

Note

Be careful when using this function. After resetting to the factory default, all the parameters are reset to the default settings.

11.3 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

1. Go to **Configuration → System → Maintenance → Log** .
2. Set search conditions **Major Type**, **Minor Type**, **Start Time**, and **End Time**.
3. Click **Search**.

   The matched log files will be displayed on the log list.
4. **Optional:** Click **Export** to save the log files in your computer.

11.4 Import and Export Configuration File

It helps speed up batch configuration on other devices with the same parameters.

Steps

1. Export configuration file.
   1) Go to **Configuration → System → Maintenance → Upgrade & Maintenance** .
   2) Click **Device Parameters** and input the encryption password to export the current configuration file.
   3) Set the saving path to save the configuration file in local computer.
2. Import configuration file.
   1) Access the device that needs to be configured via web browser.
   2) Click **Browse** to select the saved configuration file.
   3) Input the encryption password you have set when exporting the configuration file.
   4) Click **Import**.

11.5 Export Diagnose Information

Diagnose information includes running log, system information, hardware information.

Go to **Configuration → System → Maintenance → Upgrade & Maintenance** . Check desired diagnose information and click **Diagnose Information** to export corresponding diagnose information of the device.

11.6 Reboot

You can reboot the device via browser.

Go to **Configuration → System → Maintenance → Upgrade & Maintenance** , and click **Reboot**.

11.7 Upgrade

Before You Start

You need to obtain the correct upgrade package.

Caution

DO NOT disconnect power during the process, and the device reboots automatically after upgrade.

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance** .
2. Choose one method to upgrade.

Firmware	Locate the exact path of the upgrade file.

Firmware Directory Locate the directory which the upgrade file belongs to.

3. Click **Browse** to select the upgrade file.
4. Click **Upgrade**.

11.8 View Open Source Software License

Go to **Configuration → System → System Settings → About** , and click **View Licenses**.

11.9 Set Live View Connection

It controls the remote live view connection amount.

Live view connection controls the maximun live view that can be streamed at the same time.

Enter **Configuration → System → Maintenance → System Service** to set the upper limit of the remote connection number.

11.10 Time and Date

You can configure time and date of the device by configuring time zone, time synchronization and Daylight Saving Time (DST).

11.10.1 Synchronize Time Manually

Steps

1. Go to **Configuration → System → System Settings → Time Settings** .
2. Select **Time Zone**.
3. Click **Manual Time Sync.**.
4. Choose one time synchronization method.
   - Select **Set Time**, and manually input or select date and time from the pop-up calendar.
   - Check **Sync. with computer time** to synchronize the time of the device with that of the local PC.
5. Click **Save**.

11.10.2 Set NTP Server

You can use NTP server when accurate and reliable time source is required.

Before You Start

Set up a NTP server or obtain NTP server information.

Steps

1. Go to **Configuration → System → System Settings → Time Settings** .
2. Select **Time Zone**.
3. Click **NTP**.
4. Set **Server Address**, **NTP Port** and **Interval**.

Note

Server Address is NTP server IP address.

5. Click **Test** to test server connection.
6. Click **Save**.

11.10.3 Set DST

If the region where the device is located adopts Daylight Saving Time (DST), you can set this function.

Steps

1. Go to **Configuration → System → System Settings → DST** .
2. Check **Enable DST**.
3. Select **Start Time**, **End Time** and **DST Bias**.
4. Click **Save**.

11.11 Security

You can improve system security by setting security parameters.

11.11.1 Authentication

You can improve network access security by setting RTSP and WEB authentication.

Go to **Configuration → System → Security → Authentication** to choose authentication protocol and method according to your needs.

RTSP Authentication

Digest and digest/basic are supported, which means authentication information is needed when RTSP request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

RTSP Digest Algorithm

MD5, SHA256 and MD5/SHA256 encrypted algorithm in RTSP authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to log in to the

device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

WEB Authentication

Digest and digest/basic are supported, which means authentication information is needed when WEB request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

WEB Digest Algorithm

MD5, SHA256 and MD5/SHA256 encrypted algorithm in WEB authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to log in to the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

Note

Refer to the specific content of protocol to view authentication requirements.

11.11.2 Set IP Address Filter

IP address filter is a tool for access control. You can enable the IP address filter to allow or forbid the visits from the certain IP addresses.

IP address refers to IPv4.

Steps

1. Go to **Configuration → System → Security → IP Address Filter** .
2. Check **Enable IP Address Filter**.
3. Select the type of IP address filter.

   Forbidden IP addresses in the list cannot access the device.

   Allowed Only IP addresses in the list can access the device.
4. Edit the IP address filter list.

   Add Add a new IP address or IP address range to the list.

   Modify Modify the selected IP address or IP address range in the list.

   Delete Delete the selected IP address or IP address range in the list.
5. Click **Save**.

11.11.3 Set MAC Address Filter

MAC address filter is a tool for access control. You can enable the MAC address filter to allow or forbid the visits from the certain MAC addresses.

Steps

1. Go to **Configuration → System → Security → MAC Address Filter** .
2. Check **Enable MAC Address Filter**.
3. Select the type of MAC address filter.

   Forbidden MAC addresses in the list cannot access the device.

   Allowed Only MAC addresses in the list can access the device.
4. Edit the MAC address filter list.

   Add Add a new MAC address to the list.

   Modify Modify the selected MAC address in the list.

   Delete Delete the selected MAC address in the list.
5. Click **Save**.

11.11.4 Set HTTPS

HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Configuration → Network → Advanced Settings → HTTPS** .
2. Check **Enable**.
3. **Optional:** Check **HTTPS Browsing** to access the device only via HTTPS protocol.
4. Select a server certificate.

   Note

   - Complete certificate management before selecting server certificate. Refer to ***Certificate Management*** for detailed information.
   - If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.
5. Click **Save**.

11.11.5 Set QoS

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

Note

QoS needs support from network device such as router and switch.

Steps

1. Go to **Configuration → Network → Advanced Configuration → QoS** .

2. Set **Video/Audio DSCP**, **Alarm DSCP** and **Management DSCP**.

Note

Network can identify the priority of data transmission. The bigger the DSCP value is, the higher the priority is. You need to set the same value in router while configuration.

3. Click **Save**.

11.11.6 Set IEEE 802.1X

You can authenticate user permission of the connected device by setting IEEE 802.1X.

Go to **Configuration → Network → Advanced Settings → 802.1X** , and enable the function.

Select protocol and version according to router information. User name and password of server are required.

Note

- If you set the **Protocol** to **EAP-TLS**, select the **Client Certificate** and **CA Certificate**.
- If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.

11.11.7 Security Audit Log

The security audit logs refer to the security operation logs. You can search and analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events.

Security audit logs can be saved on device internal storage. The log will be saved every half hour after device booting. Due to limited storage space, you can also save the logs on a log server.

Search Security Audit Logs

You can search and analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events.

Steps

Note

This function is only supported by certain camera models.

1. Go to **Configuration → System → Maintenance → Security Audit Log** .
2. Select log types, **Start Time**, and **End Time**.
3. Click **Search**.

   The log files that match the search conditions will be displayed on the Log List.
4. **Optional:** Click **Export** to save the log files to your computer.

Set Log Server

The log server should support syslog (RFC 3164) over TLS.

Before You Start

- Install client and CA certificates before configuration. Refer to ***Certificate Management*** for detailed information.
- Select certificates according to the requirement of the log server. If two-way authentication is required, select the CA certificate and the client certificate. If one-way authentication is required, select the CA certificate only.

Steps

1. Check **Enable Log Upload Server**.
2. **Optional:** Check **Enable Encrypted Transmission** if you want the log data to be encrypted.
3. Input **Log Server IP** and **Log Server Port**.
4. **Optional:** Select client certificate.
5. Select CA certificate to the device.
6. Click **Test** to test the settings.
7. Click **Save**.

11.11.8 Control Timeout Settings

If this function is enabled, you will be logged out when you make no operation (not including viewing live image) to the device via web browser within the set timeout period.

Go to **Configuration → System → Security → Advanced Security** to complete settings.

11.11.9 SSH

Secure Shell (SSH) is a cryptographic network protocol for operating network services over an unsecured network.

Go to **Configuration → System → Security → Security Service** , and check **Enable SSH**.

The SSH function is disabled by default.

Caution

Use the function with caution. The security risk of device internal information leakage exists when the function is enabled.

11.11.10 Certificate Management

It helps to manage the server/client certificates and CA certificate, and to send an alarm if the certificates are close to expiry date, or are expired/abnormal.

Note

The function is only supported by certain device models.

Server Certificate/Client Certificate

Note

The device has default self-signed server/client certificate installed. The certificate ID is ***default***.

Create and Install Self-signed Certificate

Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. Click **Create Self-signed Certificate**.
3. Input certificate information.

   Note

   The input certificate ID cannot be the same as the existing ones.
4. Click **OK** to save and install the certificate.

   The created certificate is displayed in the **Server/Client Certificate** list.

   If the certificate is used by certain functions, the function name is shown in the column **Functions**.
5. **Optional:** Click **Certificate Property** to see the certificate details.

Install Self-signed Request Certificate

You can send the self-signed certificate to a trusted third-party for the signature, and install the certificate to the device.

Before You Start

Create a self-signed certificate first. See ***Create and Install Self-signed Certificate*** for instructions.

Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. Select a self-signed certificate from the Server/Client Certificate list.
3. Click **Create Certificate Request**.

4. Input request information.
5. Click **OK**.

   The certificate request details are displayed in a pop-up window.
6. Copy the request content and save it as a request file.
7. Send the file to a trusted-third party for signature.
8. After receiving the certificated sent back from the third-party, install it to the device.
   1) Click **Import**.
   2) Input **Certificate ID**.

   Note

   The input certificate ID cannot be the same as the existed ones.

   3) Click **Browse** to select the certificate file.
   4) Select **Self-signed Request Certificate**.
   5) Click **OK**.

   The imported certificate is displayed in the **Server/Client Certificate** list.

   If the certificate is used by certain function, the function name is shown in the column **Functions**.
9. **Optional:** Click **Certificate Property** see the certificate details.

Install Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. Click **Import**.
3. Input **Certificate ID**.

   Note

   The input certificate ID cannot be the same as the existed ones.
4. Click **Browse** to select the certificate file.
5. Select **Certificate and Key** and select a **Key Type** according to your certificate.

Independent Key	If your certificate has a independent key, select this option. Browse to select the private key and input the private-key password.
PKCS#12	If your certificate has the key in the same certificate file, select this option and input the password.
6. Click **OK**.

   The imported certificate is displayed in the **Server/Client Certificate** list.

   If the certificate is used by certain function, the function name is shown in the column **Functions**.

Install CA Certificate

Before You Start
Prepare a CA certificate in advance.

Steps
1. Go to **Configuration → System → Security → Certificate Management** .
2. Input **Certificate ID**.

   Note

   The input certificate ID cannot be the same as the existing ones.
3. Click **Browse** to select the certificate file.
4. Click **OK**.

   The imported certificate is displayed in the **CA Certificate** list.

   If the certificate is used by certain functions, the function name is shown in the **Functions** column.

11.11.11 User and Account

Set User Account and Permission

The administrator can add, modify, or delete other accounts, and grant different permission to different user levels.

Caution

To increase security of using the device on the network, please change the password of your account regularly. Changing the password every 3 months is recommended. If the device is used in high-risk environment, it is recommended that the password should be changed every month or week.

Steps
1. Go to **Configuration → System → User Management → User Management** .
2. Click **Add**. Enter **User Name**, select **Level**, and enter **Password**. Assign remote permission to users based on needs.

   Administrator

   The administrator has the authority to all operations and can add users and operators and assign permission.

   User

   Users can be assigned permission of viewing live video, setting PTZ parameters, and changing their own passwords, but no permission for other operations.

Operator

Operators can be assigned all permission except for operations on the administrator and creating accounts.

Modify Select a user and click **Modify** to change the password and permission.

Delete Select a user and click **Delete**.

Note

The administrator can add up to 31 user accounts.

3. Click **OK**.

Simultaneous Login

The administrator can set the maximum number of users logging into the system through web browser simultaneously.

Go to **Configuration → System → User Management** , click **General** and set **Simultaneous Login**.

Online Users

The information of users logging into the device is shown.

Go to **Configuration → System → User Management → Online Users** to view the list of online users.

Appendix A. Device Command

Scan the following QR code to get device common serial port commands.

Note that the command list contains the commonly used serial port commands for all Hikvision network cameras.

Appendix B. Device Communication Matrix

Scan the following QR code to get device communication matrix.

Note that the matrix contains all communication ports of Hikvision network cameras.

Appendix C. FAQ

Scan the following QR code to find the frequently asked questions of the device.

Note that some frequently asked questions only apply to certain models.


See Far, Go Further