

Fire Detection Camera

Legal Statement

About this Document

- This Document 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 Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (*https://www.hikvision.com*). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- 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.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT 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 DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Introduction

The purpose of this section is to make sure the user can use the product correctly in this manual to avoid risky operation or property damage. Before using this product, please read the product manual carefully and keep it for future reference.

Pre-Use Description

- Go to our website (www.hikvision.com) to get manuals, application tools, and development materials.
- Please sync the device before use.
- Part of the web page configuration in the manual is applicable to the latest software version. Please contact technical support to update software.

Applicable Model

Product Name	Product Model
Thermal Imaging Thermal Fire Detector	HF-VH221

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
Note	Provides additional information to emphasize or supplement important points of the main text.
Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.

Safety Instruction

Danger

- It is a Class B product. In the living environment, the product may cause radio interference. In this case, the

user may be required to take practical steps to avoid interference.

- During product installation and use, the electrical safety regulations of the country and area of use should be strictly observed.
- Please use the power adapter provided by normal manufacturer. See product parameter table for the specific requirements of the power adapter.
- The plug or socket of the device is the device that disconnects the power supply. Do not block the plug or plug in or unplug.
- Do not connect more than one product to the same power adapter (it may cause excessive heat or fire if the adapter is overloaded).
- Make sure to disconnect the product power supply during wiring, disassembling, etc., and do not power on the device.
- Warning: Battery of incorrect model may cause explosion.
- Changing batteries with incorrect models (e.g., certain types of lithium batteries) may invalidate safety protection.
- Do not put the battery in the fire or in the heater. Do not crush, bend, or cut the battery, which may cause explosion.
- Do not place the battery in extremely high temperature environment. The battery may explode or leak flammable liquid or gas.
- Do not place the battery in extremely low air pressure environment. The battery may explode or leak flammable liquid or gas.
- Discarded batteries will pollute the environment. Please follow the instructions to dispose of the used batteries.
- When installing the product on a wall or ceiling, fix the product firmly.
- To avoid heat build-up, keep the device ventilated.
- If the product smokes, it may cause bad taste, or sound noise, please disable the power supply and unplug the power cable. Please contact the distributor or service center.
- If laser product is used, do not direct the laser of the laser smart dome to avoid possible harm to the human eye.
- The laser of laser product can expose flammable objects to fire hazards. Please keep a safe distance during installation.
- If the product is not working normally, please contact the store or nearest service center of the device. Do not disassemble or edit the product in any way. (The Company shall not be responsible for problems caused by unauthorized editing or repair).

Caution

- Product functions can only be carried out when the product is installed and maintained. This product is used to help you prevent disaster, but it cannot replace you for on-site inspection, or prevent the accident from happening or expanding. You should still be more vigilant, be safer, and pay careful attention to the safety of your person and property.
- Please follow the installation method in this guide to install the device.
- To prevent injury, the device must be secured to the wall or ceiling.
- The serial port of the device is for debugging only. The user is not allowed.
- Do not let the object fall on the product or vibrate the product so that the product is away from the point where magnetic field interference exists. Do not install the product in the area of surface vibration or shock risk (ignoring this item may damage the product).
- Do not use the product in high temperature, low temperature, or high humidity. Please refer to the product parameter table for temperature and humidity requirements.
- The device's enclosure position temperature may be too hot. It may take about half an hour after powering

off.

- For low-temperature products, preheat before starting. The pre-heating time should be determined according to different environment. Make sure the heat is enough before starting the product.
- Do not place exposed flame sources on the device, such as lighted candles.
- Do not target the product lens to strong light source. Otherwise, the camera or thermal imaging detector will be damaged.
- The product cannot be exposed to rain or humidity.
- Do not place the product in an environment with corrosive gas, which may cause damage to the device.
- Avoid placing the product in direct sunshine location, place with poor ventilation, or near heat sources such as heater or heater (ignoring this item may cause fire risk).
- When cleaning product lens or shield, please use a sufficiently soft dry cloth or other alternative to wipe the outer surface. Do not use basic cleaning agent to wash the lens or shield.
- When removing the transparent cover, please use randomly carried gloves to avoid direct contact with the transparent cover. The acid sweat of the finger film may corrode the surface coating of the transparent cover. The device may be fuzzy when scratching the transparent cover with hard objects, which may affect the image quality.
- The product may face network security problems. Please strengthen the protection of personal information and data security. Please contact us when you find that the device may have network security risks.
- Please understand that it is your responsibility to reasonably configure all password and other related product security settings, and to properly keep your user name and password.
- Please keep all the original packaging materials of the product properly, so that when the problem persists, the packaging material can be used to package the product and send to the agent or return to the manufacturer. The company shall not be liable for the accidental damage caused by the transportation of non-original packaging material.

Note

Quality Requirements for Installation and Maintenance Personnel:

- Qualification certificate or experience in video live view system installation, maintenance, and related tasks (such as high-altitude work). You must also have the following knowledge and operation skills.
- Basic knowledge and installation skills of live view system and component.
- Basic knowledge and operation skills of low-voltage wiring and low-voltage electronic wiring.
- It has basic network security knowledge and skills, and is able to read and understand the contents of this manual.

The requirements for lifting devices:

- Use a safe elevator device suitable for installation location and device installation mode.
- The lifting device has enough lifting and lifting level to reach the installation position.
- The lifting device has good safety performance.

CONTENTS

Chapter 1 Product Introduction . . . 1
1.1 Product Description . . . 1
1.2 Product Function . . . 1
1.3 Appearance Interface . . . 1
1.4 Indicator Status Description . . . 2
Chapter 2 Product Installation . . . 3
2.1 Pre-Installation Description . . . 3
2.2 Installation Method . . . 3
2.2.1 Top-up Installation . . . 3
2.3 Adjust Sphere Direction . . . 4
Chapter 3 Pre-Use Operation Information . . . 5
3.1 Network Connection . . . 5
3.2 Activate Device . . . 5
3.2.1 Activate Device via SADP Software . . . 5
3.2.2 Activate via Web Page . . . 6
3.3 Access Device . . . 7
3.3.1 Access Device via Web Client . . . 7
3.3.2 Access Device via EZVIZ Cloud . . . 7
3.3.3 Add Device to Hikvision Connected Mobile Client . . . 8
Chapter 4 Local Function Description . . . 10
4.1 Reset . . . 10
4.2 Restore Factory Settings . . . 10
Chapter 5 Web Client Configuration and Operation . . . 11
5.1 Live View . . . 11
5.2 Parameter Configuration . . . 12
5.2.1 Local Configuration . . . 12
5.2.2 System Parameters . . . 13
5.2.3 Network Parameters . . . 17
5.2.4 Video Audio Parameters . . . 19
5.2.5 Image Parameters . . . 21
5.2.6 Event and Alarm . . . 23

Chapter 1 Product Introduction

1.1 Product Description

The fire detection camera is a new fusion camera. Provide early fire alarm, alarm, and on-site alarm visualization and review management. It is widely used in key fire protection and control sites such as financial network (device room, ATM room), logistics network, warehouse, digital archive room, and laboratory. It meets both security and fire protection needs.

1.2 Product Function

This section provides information about the security and safety camera.

- Support High temperature alarm and Differential temperature alarm.
- High quality imaging with 2 MP resolution.
- Supplement Light Range 30m.
- Support alarm linkage alarm picture and alarm video.
- Support local alarm indicator.
- Supports mute remotely.
- Built-in microphone for real-time audio security.
- Water and dust resistant (IP66).

1.3 Appearance Interface

Note

The product picture in this manual is a picture. Please use the actual device.

Sphere Appearance

1. Indicator
2. Infrared LED
3. Microphone
4. Visible Light Camera
5. Temperature Detector

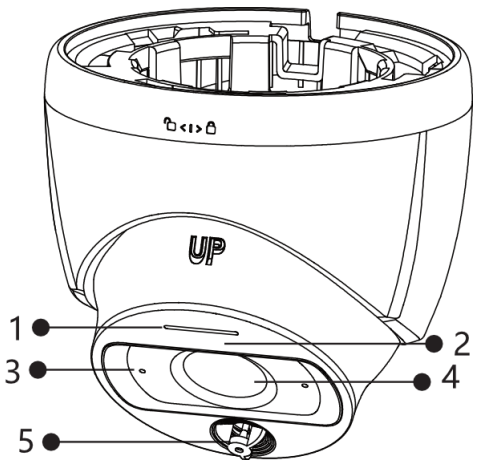


Figure 1-1 Sphere Appearance Figure

Device Appearance and Interface Description

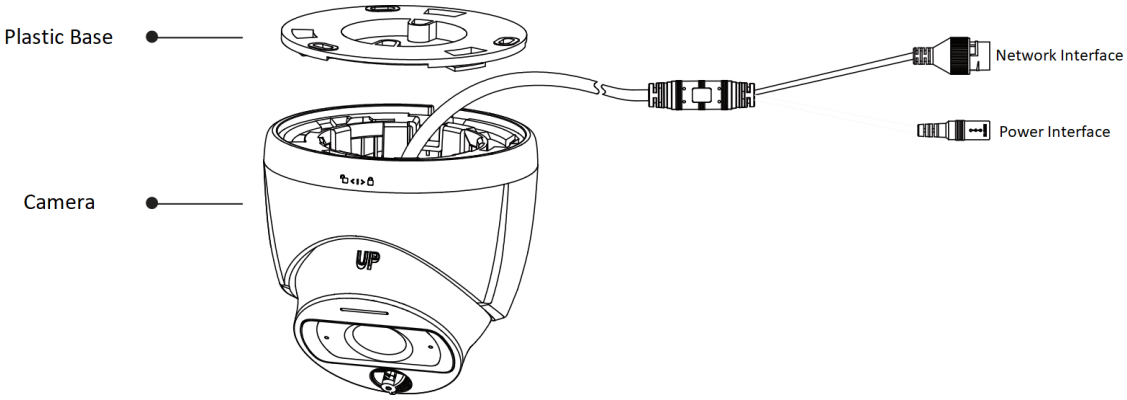


Figure 1 - 2 Device Appearance Interface

Network Interface

Network Signal Output

Power Supply Interface

DC 12 V input. Please connect to the positive and negative terminals.

1.4 Indicator Status Description

Table 1-1 Indicator and Buzzer Description

Indicator	Description
Red Light	Alarm
Green Light	Normal Operation
Yellow Light	Fault

Chapter 2 Product Installation

2.1 Pre-Installation Description

- Please make sure the device in the box is intact before installation. All components are complete.
- The wall should be of a certain thickness and be able to withstand at least 4 times the total weight of the device and installation accessories.
- If it is a cement ceiling wall, please install expansion screw (the mounting hole of expansion screw should be the same with the bracket), and then install the bracket.
- If it is a wood wall, the self-tapping screw can be used to directly install the bracket.
- The brackets in the manual are optional. Please select according to actual needs.

2.2 Installation Method

The device supports top-up installation or cable trap installation.

2.2.1 Top-up Installation

The device can be installed with top-mounted, wall-mounted, suspended, and tilt mount.

The device can be installed with top-mounted, wall-mounted, suspended, and tilt mount. DS-1272ZJ-110-TRS wall mounting bracket is recommended for wall mounting. DS-1271ZJ-110-TRS lifting bracket is recommended for lifting. DS-1281ZJ-S is recommended for tilting base installation.

Four installation methods are similar. For example, do the installation of top-end installation.

Steps

1. Remove the installation stickers included in the box, apply the installation stickers to the wall on which the camera needs to be installed, and drill holes according to the holes marked on the installation stickers.



Figure 2-1 Installing Sticker

2. Use 3 PA4 × 25 screws to secure the device base to the wall.

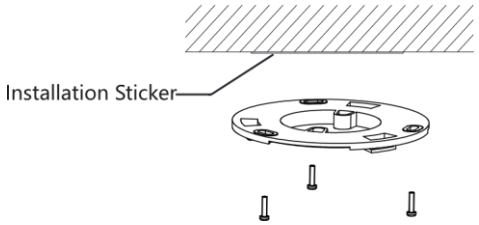


Figure 2-2 Fixed Base

3. Set up and connect the power cables and network cables of the camera, and keep the power cables insulated.
4. Align the camera body with the quick-loading turntable and rotate it in the direction indicated.

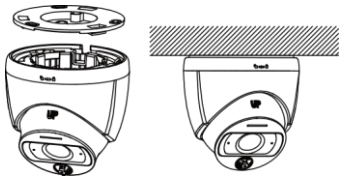


Figure 2 to 3 Installation Device

Note

After installation, the UP ID on the sphere should face up.

2.3 Adjust Sphere Direction

Adjust the cover and sphere to the scene.
Adjust camera angle by rotating the cover and sphere.

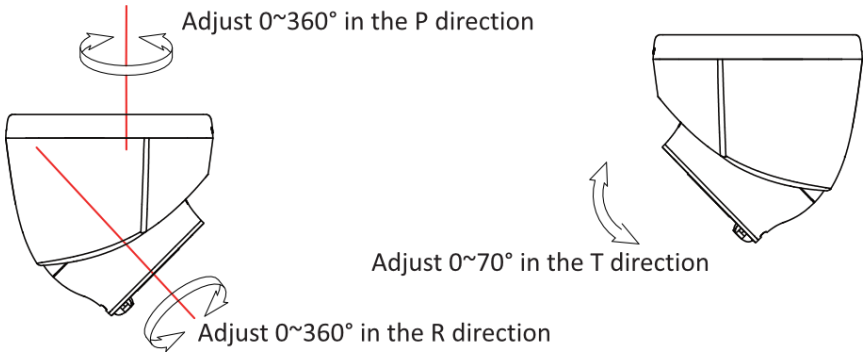


Figure 2 to 4 Adjust Sphere Direction

Chapter 3 Pre-Use Operation Information

3.1 Network Connection

Note

If you connect the product to the Internet, including but not limited to cyber attack, hacking, virus infection, etc., the company will not be responsible for the abnormal work and information disclosure of the product, but will provide technical support to you.

Use network cable to connect the device to Ethernet. After connecting to the network, you can enter the device web page via browser to configure device functions and parameters.

3.2 Activate Device

In network access, to protect the security and privacy of personal account, you can set a login password to activate the device, prevent others from logging in to the device, and get the information.

Note

Please refer to the latest client software manual for activation method through client software.

3.2.1 Activate Device via SADP Software

Download SADP software and run. The SADP software will search for inactive devices or all online devices in the same network segment. The list will display information such as device type, IP address, security status, and device serial No. You can activate the inactive device via SADP software.

Prerequisite

Power on the device and connect to the network.

Steps

1. Download SADP software from official website and run.
2. Download SADP software and run.
3. Select the device to activate. Information about the device will be displayed on the right side of the list.
4. Set the device password in the Activate Device field, and click *OK* to complete the activation.

Note

- To protect your privacy and corporate data, and avoid network security issues with device products, it is recommended to set strong password that meets security requirements.
- To improve the security of product network, the password should be between 6 and 16 characters, and it should contain at least 2 of the following types: digits, lowercase letters, and uppercase letters. Special characters are not allowed.

After the device is activated, the activation status in the list will be updated to **activated**.

5. Optional: Edit device IP address.
   1) Select the activated device in the device list.
   2) Enter IP address, subnet mask, gateway, etc. in **the modified network parameter** on the right.

> Note
>
> Edit IP address according to actual needs. For example, when you need to log in to device web page to configure device, set the IP address of the device and the IP address of the computer to log in to device web page in the same network segment.

   3) Enter the password to activate the device after editing, and click *Edit*.



Figure 3-1 Edit Device IP Address

The **parameter** settings such as IP address will take effect. The device will reboot after network parameters are edited.

3.2.2 Activate via Web Page

Access the device through the web page and activate the device.

Steps

1. Connect the device directly to the computer network cable.
2. Edit the IP address of the computer and the IP address of the device in the same network segment.

> Note
>
> Device IP address: 192.168.1.64.

3. Enter 192.168.1.64 in the browser, and press Enter to display the activation page.
4. Set device activation password.

> Note
>
> - To protect your privacy and corporate data, and avoid network security issues with device products, it is recommended to set strong password that meets security requirements.

- The password should contain 8 to 16 characters, including at least 2 of the following types: digits, lowercase letters, uppercase letters, and special characters.

5. Click *OK* to activate the device.
6. Enter activation password, log in to device, enter *configuration → network → basic configuration → TCP/IP address*, and change device IP address to make the device IP address in the same network segment.

Note

See *Set TCP/IP address* to edit device network parameters.

3.3 Access Device

Provide access method through web page and Hik-Connect.

3.3.1 Access Device via Web Client

Login System

Log in to the device's web page, and configure and operate the device through the web page.
Power on the device and connect to the network. Enter the device IP address in the browser address field to log in.

Note

After login, if you pop up the installation browser plug-in interface, please allow installation.

Get Help

Quick access to the device through online help.
Click to open the online help document and view the operating instructions.

Exit System

If the device is set or operated, you need to exit the device system safely.
Click to exit the device system.

3.3.2 Access Device via EZVIZ Cloud

Devices connected to Hik-Connect can receive abnormal information of the scene of interest and take security measures in time.

Note

The operation is only applicable to gateway and wireless repeater.

Enable Hik-Connect

Enable Hik-Connect via SADP or web page.

Enable Hik-Connect via SADP

Enable Hik-Connect via SADP software.

Prerequisite

Get SADP software via official website and install.
Get SADP software and install.

Steps

1. Open SADP software.
2. Select the device to enable Hik-Connect.
   - Select inactive device. Select *Hik-Connect to use* Hik-Connect to set the verification code to enable Hik-Connect.
   - Select the activated device, select *Use Hik-Connect*, set verification code, enter device password, and click *Edit* to enable Hik-Connect.

Enable Hik-Connect via web page.

You can enable and set Hik-Connect to access Hik-Connect.

Steps

1. On the device web page, go to *Configuration → Network → Advanced Configuration → Platform Access*.
2. **Platform access mode** is Hik-*Connect*.
3. Select *Enable*.
4. Set Hik-Connect access parameters.

   Access Server IP Address

   By **default**, the device will automatically assign a server address to the server in the nearest area. **Custom** means you can set domain name server address manually.

   Verification Code

   For device access security, please customize a verification code or edit the original verification code to add the device to Hik-Connect account.

   Note

   The verification code should contain 6 to 12 characters, including letters and digits, and it is case sensitive. For device security, it is recommended to set a combination of uppercase letters and digits with 8 or more characters.

5. Click *Save*.
   The registration status is **online**, meaning the device is registered to Hik-Connect platform.

3.3.3 Add Device to Hikvision Connected Mobile Client

Add to Hikvision Connected Mobile Client and access the device via mobile client.

Prerequisite

Connect the device to the network in one of the following ways, according to the communication mode

supported by the device.

- The device is connected to the router via wired network. Please make sure the router is connected to the WAN normally.
- The device is connected via 4G Cat1 Wi-Fi, and the wireless network signal is normal. The SIM card has enough traffic.

Steps

1. The cell phone will scan Hikvision connected mobile client and download, install, and register client software.

Note

Downloading will consume data. It is recommended to operate in Wi-Fi.



Figure 3-2 Hikvision Internet Download QR Code

Note

Hikvision connected QR code supports scanning and downloading by cell phone of Android system or iOS system.

2. Click Add Device → Scan/Add Device on Client Software Home Page to add.
   - Scan the QR code on the device body to add the device.
   - Enter the serial No. on the device label to add the device.

Note

Select the adding method according to client interface and actual situation.

3. Please enter device verification code.

Note

The verification code is on the device. If you have edited the verification code when enabling Hik-Connect via SADP software or web page, please enter the latest verification code.

Result Description

After the device is added to Hikvision Connected Mobile Client, you can view video, alarm information, and historical alarm.

Chapter 4 Local Function Description

4.1 Reset

Reset the device to standby status. When the temperature is lower than the response threshold, the alarm status will be removed and the device will automatically restore to standby status.

4.2 Restore Factory Settings

Press and hold [RESET] button, and power on the device. Press [RESET] button for 10 to 15 seconds to release.

Chapter 5 Web Client Configuration and Operation

5.1 Live View

Live View Screen Function

- In the live view page, you can control functions such as live view, recording, capture picture, and volume adjustment.
- The image size can be set as Original Size, 4:3; 16:9; or Self-Adaptive according to user requirements.
- The stream type can be set as “main stream” and “sub-stream”.
- The control is related to specific browser. The core browser supports Web-components and QuickTime. The non-core browser supports Web-components, QuickTime, VLC, and MJPEG.

Live View Screen Icon Function Description

Table 5-1 Icon Function Description

Icon	Function Description
	Select the picture size during live view. 4:3; 16:9; original size and adaptive display, respectively.
	Select stream type during live view. Main stream and sub-stream are respectively represented.
	Play plug-in switch selection.
	Live view is enabled and disabled.
	Capture picture during live view.
	Local recording is enabled and disabled during live view.
	Enlarge.
	Enable and disable audio during live view.
Reset	Reset button, reset alarm, and clear alarm status.

5.2 Parameter Configuration

5.2.1 Local Configuration

Go to *Configuration* → *Local*. You can configure the following parameters.

Playing Parameters

Protocol Type

Set according to actual situation.

Playing Performance

Set according to actual playing requirements.

Display Rule Information

You can select **Yes** or **No**. When the display rule information is enabled, the information box will be displayed on the live view page, including dynamic analysis box of mobile detection.

Capture File Format

Set the saving format of captured pictures.

Capture Rule Information

You can select **Yes** or **No**.

Video File

Video File Package Size

The size of a single video file stored locally.

Video File Saving Path

The video file is stored in the local path. Click *Browse* to change the path. Click *Open Folder* to open the folder in the archive path.

Download and Save Playback Path

The downloaded video file or picture will be stored in the local path. Click *Browse* to change the path. Click *Open Folder* to open the folder in the archive path.

Capture and Clip

Live View Capture Save Path

The captured picture will be stored locally during live view. Click *Browse* to change the path. Click *Open Folder* to open the folder in the archive path.

Playback Capture Save Path

The captured picture will be stored locally during playback. Click *Browse* to change the path, and Open *Folder* to open the folder under archive path.

Playback Clip Saving Path

When playing back, the edited video file will be stored locally. Click *Browse* to change the path, and Open *Folder* to open the folder under archive path.

5.2.2 System Parameters

System Settings

Note

The system settings are dependent on the actual device. The system settings that the device may support are described below.

View Basic Device Information

Device system information includes device model, serial No., version information, channel number, HDD number, and alarm input/output number.

Enter *Configuration* → *System* → *System Settings* → *Basic Information* to edit device name and device No.

Set Device Time

Set device time. Two time sync modes are supported: NTP time sync and manual time sync.

Go to *Configuration* → *System* → *System Settings* → *Time Configuration*.

Select the time zone and time sync mode.

NTP Time Sync

Configure NTP server address, server port, and time sync interval.

Note

Click *Test* to test if the NTP server is correct.

After setting, the device will sync from NTP server periodically according to time sync interval.

Manual Time Sync

You can set device time directly or sync *with computer time*.

About Device

Go to *Configuration* → *System* → *System Settings* → *About Device*, click *View* to display open source license

information.

System Maintenance

Upgrade and Maintenance

Restart device, restore device parameters, export information, import parameters, and upgrade device.

Go to *Configuration → System → System Maintenance → Upgrade Maintenance*.

Reboot Device

Click *Reboot* to restart the device.

Restore Default Value

Simple Restore

Simply restore device parameters, except IP address, subnet mask, gateway, user information, format, and security question.

Restored completely.

Restore device parameters to factory settings.

Export Information

Device Parameters

It is used to export device parameter file. It is used to configure device with the same parameter.

1. Click *Device Parameters* to pop up *the* file encryption configuration window.
2. Set encryption password to encrypt the exported device parameter file.
3. Click *OK* to select storage path to export.

Import Parameter

Device Parameters

Importing device parameter file will make it easy for the user to configure the device with the same parameters.

1. Click *Browse* to select the storage path of the device parameter file, and click *Open*.
2. Click *Import*. The prompt will be displayed.
3. Click *OK* to enter the encryption password, and import the device parameter file.

Upgrade

Upgrade File

When the device needs to be upgraded, you can copy the upgrade program to the local computer, click *Browse* to select the path of saving the upgrade file, and click *Upgrade* to start upgrading.

Note

The device will reboot automatically after upgrading. Do not power off during upgrading.

Search Security Audit Log

It is used to search and manage device security logs.

Steps

1. On the device web page, go to *Configuration → System → System Maintenance → Security Audit Log*.
2. Set log main type, minor type, start time, and end time.
3. Click *Search*.
   The log list shows all the logs that meet the search condition.
4. Optional: Click *Export* to save log to computer.

Security Management

Set Authentication Mode

Set RTSP authentication.

You can select the authentication mode as “digit” or “digit/basic”. The information to be carried by different modes of authentication is different. See detailed protocol for the information.

Note

Basic authentication information is relatively simple. If the requirements for network security are high, it is recommended to use bigest.

Set Security Service

Configure invalid login locking function and security mode.

Go to *Configuration → System → Security Management → Security Service* to enable or disable corresponding security service according to actual situation. The configuration will take effect after saving.

Enable Invalid Login Lock

Enable the function. Enter user name or password at login to the upper limit (seven times, and 5 times after SSH is enabled). The device will be prompted with lock information and automatically enter lock status.

Note

For the security of your account, and to prevent unauthorized user login to the device, you are recommended to enable this function. Please set according to the actual situation.

Enable Security Mode

Select *Enable Security Mode*, enter administrator password, and enable the function. After enabling the function, the device will use strong password to test. In this mode, some versions of older NVRs will be disabled.

User Management

User Management

When you log in to the system using device default user name (admin), you can edit admin user password, create other users, and create up to 31 users.

Account Security Settings

Click *Account Security Settings* and enter admin user password to set or edit security questions. After setting the security question, click Forgot Password in the login page to answer the security question and reset the password.

Note

- Please keep the device and computer in the same network segment on the LAN when resetting.
- The admin is the default user. The user name cannot be edited. Only its password can be edited.
- When adding, editing, and deleting admin user, you should enter the admin user password.

Note

- To ensure the security of the account information, the password should contain at least 8 to 16 characters, including digits, lowercase letters, uppercase letters, and special characters (! ''# $%&'()*+,-./:;<=>?@[\]^_`{|}~ space) and cannot contain user name.
- Password should contain no more than 8 characters. Password should contain only one type of character, the same as user name, or the reverse of user name. The above types of passwords are risky. To better protect your privacy and improve product security, it is recommended to change the risky password to high-intensity.

Add User/Edit User/Delete User

- Click *Add* to add new user. You can set user type, password, and permission. Set the complexity of the password as strong, medium, and weak.
- Select existing user. Click *Edit* to edit user information.
- Select existing user. Click *Delete* to delete the invalid user information.

View Online User

It is used to display the list of users logged into the device in the network.

Go to *Configuration → System → User Management → Online User* to view all user information logged in to the device, including user name, user type, IP address, and user operation time. Click *Refresh* to refresh current user information.

Note

- If the IP address and user name are the same, only one user login information will be shown.
- Up to 30 user logins can be displayed in the online user interface.

5.2.3 Network Parameters

Set TCP/IP address

TCP/IP is the most basic transmission control protocol of the Internet. TCP/IP configuration is required for network operation.

Go to *Settings* → *Network* → *Basic Settings* → *TCP/IP address*, set network parameters, and click *Save* to take effect.

Note

The TCP/IP parameters that the device may support are described below. The specific parameters that the device supports are subject to the actual device interface.

NIC Type

Select according to network environment.

IPv4 Address

- Select *Auto Get*. The device will automatically get network parameters according to the network environment.
- Uncheck *to get automatically*. Manually enter device IPv4 address, IPv4 subnet mask, IPv4 default gateway, and other LAN parameters.

Note

When manually entering IPv4 network parameters, click *Test* to check if the IP address is available, and click Save.

MTU

The max. transmission unit refers to the size of the max. data packet in TCP/UDP protocol network transmission.

DNS Server Configuration

You can parse the domain name when the device has set the correct available DNS server address.

Configure Port Parameters

You can edit the device port when network access is not available due to port conflict.

Note

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

Enter *configuration* → *Network* → *Basic configuration* → *Port*, set port parameters, and save to take effect.

HTTP Port

The port of the browser accessing device. For example, if **HTTP port** is changed to 81, you should enter to access it when you log in *http://192.168.1.64:81* via browser.

RTSP Port

The port of the real-time transmission protocol of the device.

Service Port

When using the client to log in to the camera, you need to enter the port No. in the login page to log in to the camera normally.

Set Platform Access Function

Platform access function is configured to access Hik-Connect platform. Hik-Connect access supports Hik-Connect access device to register to Hik-Connect platform and access via Hik-Connect.

Hik-Connect

Hik-Connect is the micro-video service platform of Hik-Connect. The Hik-Connect device can be accessed through Hik-Connect.

Steps

1. Enter *configuration → Network → Advanced configuration → Platform access*.
2. Select *Hik-Connect.*
3. Select *Enable*.
4. Select Custom or Default *to access server IP* address.
   - Custom: Set domain name server IP address manually.
   - Default: The device will automatically assign a server IP address of the nearby area.
5. Click *Save*.

Note

- Refresh the page or restart the device to check *the registration status*. Check if the device is registered.
- If you log in via administrator, you can view the device's Hik-Connect verification code. If you log in via non-admin user, you cannot view the code.

Configure Open Network Video Interface

Connect device via open network video interface protocol to enhance device network security.

Steps

1. Go to *Settings → Network → Advanced Settings → Integration Protocol*.
2. Select *Enable Open Network Video Interface*.
3. Click *Save*.

5.2.4 Video Audio Parameters

Note

The content in the audio parameter settings will be determined according to the actual device. The following description refers to the audio settings that the device may support.

Video Configuration

You can set video parameters according to the quality requirements of the live view image.

Go to *Settings* → *Audio* → *Video* and configure video parameters.

Note

The video parameters of the device are described below. The settings supported by the device are subject to the actual interface of the device.

Stream Type

Main Stream (Timed)

Main stream is used for HD storage and live view, resolution, bitrate, and image quality.

Sub-Stream

Sub-stream is used for standardizing storage and live view, resolution, bitrate, and image quality when network bandwidth is insufficient.

Video Type

Video Stream

Video stream only.

Composite Stream

Including video stream and audio stream.

Resolution

Select according to the customer's requirements for video clarity. The higher the resolution, the higher the bandwidth requirement.

Bitrate Type and Bitrate Upper Limit

Fixing Rate

It means that the bit rate is maintained at the average bit rate for transmission. The compression speed is fast, but video mosaic may be caused.

Change Bit Rate

It means adjusting the bit rate on the basis of the upper limit of the bit rate. The compression speed is relatively slow, but it can ensure the image definition of complex scene.

Image Quality

When the bit rate is variable bit rate, you can set the image quality. Select according to the customer's

requirements for image clarity. The higher the image quality, the higher the bandwidth requirement.

Video Frame Rate

It refers to the number of frames per second. The higher the video frame rate, the higher the bandwidth, and the higher the storage space.

Video Encoding

H.264

H.264 is a high-performance video encoding/decoding technology, with high compression, flexible handling, and ultra-low bit rate, saving network transmission bandwidth and storage space.

Note

When **the video encoding** parameter of sub-stream is set as *MJPEG*, H.264 encoding format is recommended to ensure smooth picture if the live view is stuttered.

H.265

H.265 is a high-performance video encoding/decoding technology with high compression ratio, flexible handling, and ultra-low bitrate. Compression performance is twice as high as H.264, saving bandwidth and storage space.

Encoding Complexity

The higher the encoding complexity under the same bit rate, the higher the image quality, but the higher the network bandwidth requirements.

I Frame Interval

The number of frames between the two key frames. The larger the I frame interval, the smaller the stream fluctuations, but the poorer the image quality, the larger the stream fluctuations, and the higher the image quality.

SVC

It is a scalable video encoding technology that can be used for encoding storage when bandwidth is insufficient. This function needs to be implemented with back-end storage device. The device encoding H.264/H.265 can be configured.

Stream Smoothing

Drag the progress bar or set stream smoothing value. The higher the value, the better smoothing degree, but the image will be relatively unclear. Otherwise, the smoothness of the image will be poor, and the image is relatively clear.

Audio Configuration

Go to *Settings* → *Audio* View → *Audio* → and configure audio parameters.

Audio Encoding

Set audio encoding type, including G.711ulaw and AAC.
When the encoding type is *AAC*, set the sampling rate and audio bit rate parameters. Select the sampling rate and audio bit rate parameters from the drop-down list.

Audio Input

The audio input mode. By default, *MicIn* is used, i.e., passive microphone.

Input Volume

The gain control value of the audio input source. The user can adjust the value from 1 to 100.

5.2.5 Image Parameters

Set Display Parameters

Enter *Configuration* → *Image* → *Display Settings* to set the image quality of the main live view.

Image Adjustment

Adjust the brightness, contrast, saturation, and sharpness of the live view by dragging the progress bar. You can also set the value after the progress bar.

Exposure

Optical Circle Type

By default, *this* option cannot be edited for cameras with circled cameras.

Exposure Time

The camera digital shutter time can set different exposure time according to different device scene. If manual circle camera mode is used, the time set here is the longest exposure time, and the device will automatically adjust the exposure time according to the brightness of the scene.

Gain

Adjust the zoom in of video signal. The larger the gain, the more obvious the image noise.

Day/Night Conversion

Day/Night Conversion

You can select *daytime*, *nighttime*, *auto*-switch, *and alarm input to trigger*. In daytime mode, it is color image. In nighttime mode, the device will automatically control day and night according to external environment brightness. In scheduled switch mode, the user will set start time and end time. In this time period, the device will automatically use night mode.

Note

The start time and end time can be set to the next day when you select *the scheduled switch*. Please set the start time and end time to the next day.

Backlight

Width Dynamic

Select to *disable*, *enable*, and *auto*.

Width Dynamic Level

0 to 100 adjustable.

White Balance

White balance: Manual white balance, automatic white balance 1, locked white balance, sunlight, incandescent light, hot light, and natural light can be selected.

Note

- Lock the white balance to lock the current color correction matrix. If the actual scene is of fixed light type, you can select sunlight, incandescent light, hot light, and natural light according to the actual situation.
- The sunlight is applicable to the color temperature environment of around 6500K; the incandescent light is applicable to the color temperature environment of around 3000K; the hotlight is applicable to the color temperature environment of around 4000K; the natural light is applicable to the color temperature environment of around 5500K.

Image Enhancement

Digital Noise Reduction

It refers to using advanced 3D image noise reduction technology to effectively reduce image noise and make the image softer. Digital noise reduction mode can be set to *normal mode*, *expert mode*, and *disabled*. You can drag progress bar or set noise reduction level value in normal noise reduction mode. You can adjust the two dimensions of air and time zone noise reduction when in expert noise reduction mode.

Video Adjustment

Mirror

You can adjust video by mirror image as needed. You can select *center*, *left*, right, *up*, down mirror image to adjust, or disable mirror image. When the image is inverted, you can flip the image through the menu.

Video Format

PAL50Hz can be selected. The max. frame rate is 25 frames/sec.

Set OSD Parameters

OSD refers to the information displayed on the video screen. The video screen can display device name, date, week, and superimposed characters.

Enter *configuration → image → OSD settings*, select display item, set channel name, set corresponding parameters, and save to take effect.

Basic OSD Information Settings

- Select the OSD information to display: Select *the display name*, *date*, *and week*, and the corresponding OSD information will be displayed on the live view.
- Enable temperature data overlay: When enabled, the function will overlay the real-time temperature wave chart.
- Edit OSD information display location: Drag the OSD red box on the live view to move to the location you want to display.
- Edited display format: In **the channel name/time format/date format**, you can edit the channel name displayed on the live view and the time and date format.

OSD Attribute Settings

Set OSD information attribute, font size, color, and alignment method displayed on live view.

Overlay Custom Characters

The device can overlay multiple characters to the video. Check and set the required characters. The characters in the screen will be red font. Drag the characters or set **the alignment mode** to adjust the displayed characters to the required position. Click *Save* to finish the settings.

Note

Some characters are default fire alarm characters, and cannot be edited.

Set Video Tampering

Video masking refers to covering sensitive areas in the video picture, and is not displayed in the image.

Steps

1. On the device web page, go to *Configuration* → *Image* → *Video Masking*.
2. Select *Enable Video Masking*.
3. Click the *drawing area*, click the left mouse button in the picture, drag the mouse, and release the left mouse button to draw an area.

   Note

   Up to 4 areas can be drawn in the picture.

4. When the area is drawn, click *Stop Drawing* to finish the area drawing.
5. Optional: Click *Clear All* to clear all areas drawn.
6. Click *Save*.

5.2.6 Event and Alarm

Describe the function configuration of each event supported by the device, and configure the corresponding event according to needs, and trigger the device to execute linkage actions.

Note

The event functions supported by the device are described below. Please use the function supported by the actual device.

Schedule and Linkage Configuration

The device receives alarm information during the scheduled time period. The device is linked to execute

corresponding actions.

Set Arming Time

Set the start time and end time of task execution.

Steps

1. Click *Arming Time*.
2. Select a point in the timeline as start point. Hold the left mouse button to drag in the timeline, and release the mouse when dragging to the end point to set the arming time.

Note

8 time periods are supported in one time axis.

3. Adjust arming time.
   - Click Arming Time Period to enter start time and end time manually to adjust arming time. Click *Save*.
   - Click arming time period, and two circles will be displayed on both ends of the time period. Move the mouse to both ends of the time period, and display the adjustment arrow in the left and right directions. Move the adjustment arrow to adjust the time period.
   - Drag the arming time period to any position on the axis to reset the time period.

Click to Delete Time Period	Delete current time period.
Click to *Delete*	Delete the selected time period.
Click to *Delete All*	Delete all time periods.
Click *to copy to...*	Copy the same schedule to other time.

4. Click *Save*.

Linkage Configuration

You can enable alarm linkage when there is an event or alarm.

The linkage mode that the device may support is described below. Please configure the linkage mode according to available options on the actual device interface.

Normal Linkage

Upload Center

Select *Upload Center* to upload alarm information and pictures to remote central platform when alarm occurs.

Please go to Settings → Network → Advanced Settings → Platform Access to configure the upload center.

Video Linkage

Select and configure recording schedule. When alarm is triggered, the channel can be linked for recording.

See for recording schedule configuration.

Configure Normal Event

Describe the basic event configuration of the device.

Note

The event types that the device may support are described below. The actual event types will be determined according to the actual interface.

Configure Motion Detection

The function is used to detect whether an area has moved objects during a certain time period. When there is a moving object, the device will be triggered to execute linkage actions.

Steps

1. Enter *configuration → event → normal event → mobile detection*.
2. Select *Enable Motion Detection*.
3. Optional: Set the moving object in the picture to green to highlight.
   1) Select *Enable Dynamic Analysis*.
   2) Go to *Configuration → Local* and select **Rule Information** to *enable*.
4. Select the **area**, click *Draw Area* to start drawing, click *Stop to* finish drawing, or click *Clear to clear all* drawn content.
5. Set arming time and linkage mode. See *Schedule and Linkage Configuration*.
6. Set *sensitivity*. 0 to 100 can be adjusted.
7. Click *Save*.

Configure Exception Alarm

When the device is abnormal (such as network disconnection), the configured linkage action can be triggered.

Steps

1. Enter *Configuration → Event → Normal Event → Exception*
2. Select exception alarm type.
3. Set linkage mode. See *Schedule and Linkage Configuration* for linkage mode settings.
4. Click *Save* to complete the exception alarm configuration.

Configure Temperature Detection

Temperature detection function is used to detect temperature. When the device detects the temperature exceeded threshold, the device will be triggered to execute linkage action.

Steps

1. Enter *configuration → event → normal event → temperature detection*.
2. Select *Enable*.
3. Set temperature alarm threshold. 0-120 can be adjusted.
   The device will be triggered to execute linkage actions when the detected temperature exceeds the set

threshold.

4. Set temperature alarm time threshold, which can be adjusted from 1 to 30.
5. Select differential temperature detection type.
6. Set the alarm threshold of temperature surge. 1-120 can be adjusted.
7. Set the alarm time threshold of temperature surge. 1 to 30 can be adjusted.
8. Set arming time and linkage mode. See *Schedule and Linkage Configuration*.
9. Click *Save*.


See Far, Go Further