



Thermographic Automation Camera

User Manual

Legal Information


©2022 Hangzhou Microimage Software Co., Ltd. All rights reserved.

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 HIKMICRO website (<http://www.hikmicrotech.com>).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

 **HIKMICRO** and other HIKMICRO's trademarks and logos are the properties of HIKMICRO 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". HIKMICRO 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 HIKMICRO 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 HIKMICRO 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 HIKMICRO 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, HIKMICRO 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




Thermographic Automation Camera User Manual

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.

Symbol Conventions

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

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

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

Laws and Regulations

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.

Transportation

- Keep the device in original or similar packaging while transporting it.
- Keep all wrappers after unpacking them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and the company shall not take any responsibilities.
- DO NOT drop the product or subject it to physical shock. Keep the device away from magnetic interference.

Power Supply

- Please purchase the charger by yourself. Input voltage should meet the Limited Power Source (12 VDC) according to the IEC62368 standard. Please refer to technical specifications for detailed information.
- Make sure the plug is properly connected to the power socket.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- DO NOT connect multiple devices to one power adapter, to avoid over-heating or fire hazards caused by overload.
- DO NOT touch the bare metal contacts of the inlets after the circuit breaker is turned off. Electricity still exists.
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current. - identifies the negative terminal(s) of equipment which is used with, or generates direct current.

Battery

- Risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions. Il y a risque d'explosion si la batterie est remplacée par une batterie de type incorrect. Mettre au rebut les batteries usagées conformément aux instructions.
- The built-in battery cannot be dismantled. Please contact the manufacture for repair if necessary.
- For long-term storage of the battery, make sure it is fully charged every half year to ensure the battery quality. Otherwise, damage may occur.
- This equipment is not suitable for use in locations where children are likely to be present.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for

example, in the case of some lithium battery types).

- DO NOT dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- DO NOT leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- DO NOT subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.

Installation

- Never place the equipment in an unstable location. The equipment may fall, causing serious personal injury or death.
- This equipment is for use only with corresponding brackets. Use with other (carts, stands, or carriers) may result in instability causing injury.

System Security

- You acknowledge that the nature of Internet provides for inherent security risks, and our company shall not take any responsibilities for abnormal operation, privacy leakage or other damages resulting from cyber attack, hacker attack, however, our company will provide timely technical support if required.
- Please enforce the protection for the personal information and the data security as the device may be confronted with the network security problems when it is connected to the Internet. Please contact us when the device might exist network security risks.
- Please understand that you have the responsibility to configure all the passwords and other security settings about the device, and keep your user name and password.


Maintenance

- If the product does not work properly, please contact your dealer or the nearest service center. We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.
- A few device components (e.g., electrolytic capacitor) require regular replacement. The average lifespan varies, so periodic checking is recommended. Contact your dealer for details.
- Wipe the device gently with a clean cloth and a small quantity of ethanol, if necessary.
- If the equipment is used in a manner not specified by the manufacturer, the protection provided by the device may be impaired.
- To reduce the risk of fire, replace only with the same type and rating of fuse.
- The serial port of the equipment is used for debugging only.

Using Environment

- Make sure the running environment meets the requirement of the device. The operating temperature shall be -20°C to 50°C (-4°F to 122°F), and the operating humidity shall be 95% or less, no condensing.
- DO NOT expose the device to high electromagnetic radiation or dusty environments.
- DO NOT aim the lens at the sun or any other bright light.
- The equipment shall not be exposed to dripping or splashing and that no objects filled with

liquids, such as vases, shall be placed on the equipment.

- No naked flame sources, such as lighted candles, should be placed on the equipment.
- Provide a surge suppressor at the inlet opening of the equipment under special conditions such as the mountain top, iron tower, and forest.
- Burned fingers when handling the parts with symbol . Wait one-half hour after switching off before handling the parts.

Emergency

- If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.

COMPLIANCE NOTICE: The thermal series products might be subject to export controls in various countries or regions, including without limitation, the United States, European Union, United Kingdom and/or other member countries of the Wassenaar Arrangement. Please consult your professional legal or compliance expert or local government authorities for any necessary export license requirements if you intend to transfer, export, re-export the thermal series products between different countries.

Contents

Chapter 1 Overview.....	1
1.1 Brief Description.....	1
1.2 Function	1
Chapter 2 Device Activation and Accessing	2
2.1 Activate the Device via HIKMICRO Studio.....	2
2.2 Activate the Device via Browser	3
2.3 Login.....	3
2.3.1 Plug-in Installation	3
2.3.2 Illegal Login Lock.....	4
Chapter 3 Temperature Measurement.....	6
3.1 Set Thermometry Parameters	6
3.2 Set Non-ROI Thermography	7
3.3 Set ROI Thermometry.....	8
3.3.1 Set Thermography Rule.....	9
3.3.2 Point Thermography	9
3.3.3 Line Thermography	9
3.3.4 Area Thermography	10
Chapter 4 Event and Alarm.....	11
4.1 Set Alarm Input.....	11
4.2 Set Exception Alarm	11
4.3 Set Burning-Prevention	12
Chapter 5 Arming Schedule and Alarm Linkage	13
5.1 Set Arming Schedule	13
5.2 Linkage Method Settings.....	13
5.2.1 Trigger Alarm Output	13
5.2.2 FTP Uploading.....	14
5.2.3 Send Email	15
5.2.4 Notify Surveillance Center	15
5.2.5 Trigger Recording	16

Chapter 6 Live View	17
6.1 Live View Parameters	17
6.1.1 Window Proportion	17
6.1.2 Live View Stream Type	17
6.1.3 Select the Third-Party Plug-in	17
6.1.4 Enable and Disable Live View	17
6.1.5 Start Digital Zoom	17
6.1.6 Quick Set Live View	18
6.1.7 Lens Parameters Adjustment.....	18
6.1.8 Light	18
6.1.9 Wiper	18
6.1.10 Lens Initialization	19
6.1.11 Auxiliary Focus.....	19
6.2 Set Transmission Parameters	19
Chapter 7 Video and Audio	21
7.1 Video Settings	21
7.1.1 Stream Type.....	21
7.1.2 Video Type	21
7.1.3 Resolution.....	21
7.1.4 Bitrate Type and Max. Bitrate	21
7.1.5 Video Quality	22
7.1.6 Frame Rate	22
7.1.7 Video Encoding.....	22
7.1.8 Smoothing.....	23
7.1.9 Display VCA Info	23
7.1.10 Set ROI	23
7.2 Display Settings	24
7.2.1 Image Adjustment	24
7.2.2 Image Adjustment (Thermal Channel)	24
7.2.3 DNR	24
7.2.4 Set Palette	25

7.2.5 Set Palette Range	25
7.2.6 DDE.....	25
7.2.7 Mirror.....	25
7.2.8 Video Standard	26
7.2.9 Local Video Output.....	26
7.3 OSD	26
7.4 Overlay Picture	26
7.5 Set Manual DPC (Defective Pixel Correction).....	27
Chapter 8 Video Recording and Picture Capture.....	28
8.1 Set FTP	28
8.2 Record Manually	28
8.3 Capture Configuration.....	29
8.3.1 Capture Automatically	29
8.3.2 Capture Manually.....	29
Chapter 9 Network Settings.....	30
9.1 TCP/IP	30
9.1.1 Multicast Discovery.....	31
9.2 Port.....	31
9.3 Port Mapping.....	32
9.3.1 Set Auto Port Mapping.....	33
9.3.2 Set Manual Port Mapping.....	33
9.3.3 Set Port Mapping on Router	33
9.4 SNMP	34
9.5 Access to Device via Domain Name.....	35
9.6 Set Open Network Video Interface.....	35
Chapter 10 System and Security	37
10.1 View Device Information	37
10.2 Import and Export Configuration File.....	37
10.3 Export Diagnose Information.....	37
10.4 Reboot	37
10.5 Restore and Default	38

10.6 Upgrade	38
10.7 View Open Source Software License	38
10.8 Time and Date	39
10.8.1 Synchronize Time Manually	39
10.8.2 Set NTP Server	39
10.8.3 Set DST	39
10.9 Set RS-232	40
10.10 Set RS-485	40
10.11 Set Same Unit	40
10.12 Security	41
10.12.1 Authentication	41
10.12.2 Security Audit Log	41
10.12.3 Set IP Address Filter	42
10.12.4 Set SSH	42
10.12.5 Set HTTPS	42
10.12.6 Set QoS	44
10.12.7 Set IEEE 802.1X	44
10.13 User and Account	44
10.13.1 Set User Account and Permission	44
Chapter 11 Appendix	46
11.1 Common Material Emissivity Reference	46
11.2 Device Command	46
11.3 Device Communication Matrix	47
11.4 FAQ	47

Chapter 1 Overview

1.1 Brief Description

The Thermographic Automation Network Camera is a camera with function of high accuracy temperature measurement.

With built-in high sensitivity sensor and passive infrared imaging, the camera is able to measure object's temperature from far distance at a high accuracy in bad weather. It can also detect image information under circumstances like no light, backlight.

With the advantage of small size, low power consumption and easy integration, it can independently be used, or be integrated into devices like intelligent robots for equipment maintenance, failure detection, industrial process control, etc.

1.2 Function

This section introduces main functions of the device.

Temperature Measurement

Device detects the real-time temperature all the day, and display it on live view.

Temperature Alarm

Device outputs alarm when the temperature is higher than the setting alarm threshold value.

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 the Device via HIKMICRO Studio

Search and activate the online devices via HIKMICRO Studio software.

Before You Start

Access www.hikmicrotech.com to get HIKMICRO Studio software to install.

Steps

1. Connect the device to network using the network cable.
2. Run the software, and create super user name and password to log in.
3. Go to **Device Management** → **Device** → **Online Device** to search the online devices.
4. Check **Security Level** from the device list, and select the device to be activated.
5. Create and input the new password in the password field, and confirm the password.

Caution

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.

6. Click **OK**.
Security Level changes into **Active**.
7. Optional: Change the network parameters of the device in **Modify Netinfo**.

Note

For detailed operation, please refer to the user manual of HIKMICRO Studio .

2.2 Activate the Device via Browser

You can access and activate the device via the browser.

Steps

1. Connect the device to the PC using the network cables.
2. Change the IP address of the PC and device to the same segment.

Note

The default IP address of the device is 192.168.1.64. You can set the IP address of the PC from 192.168.1.2 to 192.168.1.253 (except 192.168.1.64). For example, you can set the IP address of the PC to 192.168.1.100.

3. Input **192.168.1.64** in the browser.
4. Set device activation password.

Caution

We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: 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.

5. Click **OK**.
6. Input the activation password to log in to the device.
7. Optional: Go to **Configuration** → **Network** → **Basic** → **TCP/IP** to change the IP address of the device to the same segment of your network.


2.3 Login

Log in to the device via Web browser.

2.3.1 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.

Operating System	Web Browser	Operation
	<p>Google Chrome 57+</p> <p>Mozilla Firefox 52+</p>	<p>Click  Download Plug-in to download and install plug-in.</p> <p>Go to Configuration → Network → Advanced Settings → Network Service to enable WebSocket or WebSockets for normal view if plug-in installation is not required. 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.</p>
<p>Mac OS 10.13+</p>	<p>Mac Safari 12+</p>	<p>Plug-in installation is not required.</p> <p>Go to Configuration → Network → Advanced Settings → 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.</p>

 **Note**

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

2.3.2 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 Temperature Measurement

When you enable this function, the device measures the actual temperature of the scene. It alarms when temperature exceeds the temperature threshold value.

3.1 Set Thermometry Parameters

Configure the parameters of temperature measurement.

Steps

1. Go to **Configuration** → **Local**, enable **Display Temperature Info.** .

Display Temperature Info.

Select **Yes** to display temperature information on live view.

Enable **Rules** to display the rules information on live view.

2. Click **Save**.

3. Go to **Configuration** → **Temperature Measurement** → **Basic Settings** to configure parameters.

Enable Temperature Measurement

Check to enable temperature measurement function.

Enable Color-Temperature

Check to display Temperature-Color Ruler in live view.

Display Temperature Info. on Stream

Check to display temperature information on the stream.

Display Max./Min./Average Temperature

Check to display maximum/minimum/average temperature information on live view when the temperature measurement rule is line or area.

Position of Thermometry Info

Select the position of temperature information showed on the live view.

- Near Target: display the information beside the temperature measurement rule.
- Top Left: display the information on the top left of screen.

Unit

Display temperature with Degree Celsius (°C)/Degree Fahrenheit (°F)/Degree Kelvin (K).

Temperature Range

Select the temperature measurement range.

Distance Mode

Select the distance mode for temperature measurement. **Fixed Distance** and **Self-Adaption** are selectable.

- Fixed Distance: Fixed distance mode is suitable for fixed objects or objects move in a very small area.
- Self-Adaption: Self-adaption mode is suitable for moving objects. In this mode, device automatically adjusts parameters according to the distance to objects, so as to ensure temperature measurement accuracy.

Note

This function is only supported by certain models.

External Optics/Window Correction

Set the temperature of the external window or optical material (e.g.: germanium window) to correct the measured temperature.

Version

View the version of current algorithm.

Calibration File Version

View the version of calibration file.

Alarm Interval

Set the time interval of alarms.

Display Rule Info. on Alarm Picture

Select the rule information to be added on the alarm capture.

Emissivity

Set the emissivity of the target. Refer to [**Common Material Emissivity Reference**](#) to search for the target emissivity.

Distance

The straight-distance between the target and the device.

Reflective Temperature

If there is any object reflecting to the target, e.g. a mirror, enter the background temperature value/the reflecting object's temperature value.

4. Click **Save**.

3.2 Set Non-ROI Thermography

This function is used to measure the temperature of the whole scene and alarm.

Steps

1. Go to **Configuration** → **Temperature Measurement** → **Basic Settings**, and check **Enable Temperature Measurement**.
2. Refer to [**Set Thermometry Parameters**](#) to set the parameters.

3. Go to **Configuration** → **Temperature Measurement** → **Advanced Settings**.
4. Configure the parameters of Non-ROI mode.

Pre-Alarm Threshold

When the temperature of target exceeds the pre-alarm threshold, it triggers pre-alarm.

Alarm Threshold

When the temperature of target exceeds the alarm threshold, it triggers alarm.

Tolerance Temperature

The triggered alarm does not stop until the temperature/temperature difference is lower/higher than rule temperature by tolerance temperature. For example, set tolerance temperature as 3 °C, set alarm temperature as 55 °C. It alarms when its temperature reaches 55 °C and only when the temperature is below 52 °C will the alarm be canceled.

5. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.
6. Click **Save**.
The maximum and minimum temperature will be displayed on the live view.



Go to **Image** → **VCA Rules Display** to adjust the font size and the temperature color of normal, alarm and pre-alarm.

3.3 Set ROI Thermometry

This function is used to detect the temperature of certain rule and output alarm.

Steps

1. Go to **Configuration** → **Temperature Measurement** → **Basic Settings**, and check **Enable Temperature Measurement**.
2. Refer to **Set Thermometry Parameters** to set the parameters.
3. Go to **Configuration** → **Temperature Measurement** → **Advanced Settings**.
4. Refer to **Set Thermography Rule** to set the rule.
5. Click **Area's Temperature Comparison**, and set the rule.
6. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.
7. Click **Save**.
The maximum and minimum temperature will be displayed on the live view.



Go to **Image** → **VCA Rules Display** to adjust the font size and the temperature color of normal, alarm and pre-alarm.

3.3.1 Set Thermography Rule

Steps

1. Customize the rule name.
2. Select the rule **type** to Point, Line, or Area. Then draw a point, line, or area on the interface where the position to be measured.

Point Please refer to [Point Thermography](#) for detailed configuration.

Line Please refer to [Line Thermography](#) for detailed configuration.

Area Please refer to [Area Thermography](#) for detailed configuration.

3. Click  and set the **Alarm Rule**.

Alarm Temperature and Pre-Alarm Temperature

Set the alarm temperature and pre-alarm temperature. E.g., select Alarm Rule as Above (Average Temperature), set the Pre-Alarm Temperature to 50 °C, and set the Alarm Temperature to 55 °C. The device pre-alarms when its average temperature is higher than 50 °C and alarms when its average temperature is higher than 55 °C.

Tolerance Temperature

Set the tolerance temperature to prevent the constant temperature change to affect the alarm. E.g., set tolerance temperature as 3°C, set alarm temperature as 55°C, and set pre-alarm temperature as 50°C. The device sends pre-alarm when its temperature reaches 50°C and it alarms when its temperature reaches 55°C and only when the device temperature is lower than 52°C will the alarm be canceled.

4. Click **Save**.
Click **Live View**, and you can view the temperature and rules information on live view.

3.3.2 Point Thermography

Configure the temperature measurement rule and click any point in live view to monitor the temperature.

Steps

1. Click in the live view and a cross cursor showed on the interface.
2. Drag the cross cursor to desired position.
Go to **Live View** interface to view the temperature and rule of the point in thermal channel.

3.3.3 Line Thermography

Configure the temperature measurement rule and monitor the maximum temperature of the line.

Steps

1. Click and drag the mouse to draw a line in the live view interface.

2. Click and move the line to adjust the position.
3. Click and drag the ends of the line to adjust the length.

Go to **Live View** interface to view the maximum temperature and rule of the line in thermal channel.

3.3.4 Area Thermography

Configure the temperature measurement rule and monitor the maximum temperature of the area.

Steps

1. Click and drag the mouse in the live view to draw the area and right click to finish drawing.
2. Click and move the area to adjust the position.
3. Drag the corners of the area to adjust the size and shape.

Go to **Live View** interface to view the maximum temperature and rule of the area in thermal channel.

Chapter 4 Event and Alarm

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

4.1 Set Alarm Input

Alarm signal from the external device triggers the corresponding actions of the current device.

Before You Start

Make sure the external alarm device is connected. See *Quick Start Guide* for cables connection.

Steps

1. Go to **Configuration** → **Event** → **Basic Event** → **Alarm Input**.
2. Check **Enable Alarm Input Handling**.
3. Select **Alarm Input NO.** and **Alarm Type** from the dropdown list. Edit the **Alarm Name**.
4. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.
5. Click **Copy to...** to copy the settings to other alarm input channels.
6. Click **Save**.

4.2 Set Exception Alarm

Exception 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.
Network Disconnected	The device is offline.
IP Address Conflicted	The IP address of current device is same as that of other device in the network.
Illegal Login	Incorrect user name or password is entered.
Calibration File Exception	The calibration file is modified. The temperature accuracy may be affected.

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

4.3 Set Burning-Prevention

This function is used to close the shutter to prevent the lens from high temperature damage.

Steps

1. Go to **Configuration** → **Event** → **Basic Event** → **Burning-Prevention**.
2. Check **Enable**.
3. Select burning-prevention mode.

Auto

The shutter will be closed automatically when detecting high temperature target. You can set the protection duration. The shutter is closed in the duration.

Manual

You can set the shutter status to open or closed as desired.

4. Optional: Check **Burning Recovery** to recover the live view image when the lens is damaged by high temperature target.
5. Click **Save**.

Chapter 5 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.

5.1 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.



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**.

5.2 Linkage Method Settings

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

5.2.1 Trigger Alarm Output

If the device has been connected to an alarm output device, and the alarm output No. has been configured, the device sends alarm information to the connected alarm output device when an alarm is triggered.

Steps

1. Go to **Configuration** → **Event** → **Basic Event** → **Alarm Output**.
2. Set alarm output parameters.

Automatic Alarm For the information about the configuration, see [Automatic Alarm](#).

Manual Alarm For the information about the configuration, see [Manual Alarm](#).

3. Click **Save**.

Manual Alarm

You can trigger an alarm output manually.

Steps

1. Set the manual alarm parameters.

Alarm Output No.

Select the alarm output No. according to the alarm interface connected to the external alarm device.

Alarm Name

Custom a name for the alarm output.

Delay

Select **Manual**.

2. Click **Manual Alarm** to enable manual alarm output.
3. Optional: Click **Clear Alarm** to disable manual alarm output.

Automatic Alarm

Set the automatic alarm parameters, then the device triggers an alarm output automatically in the set arming schedule.

Steps

1. Set automatic alarm parameters.

Alarm Output No.

Select the alarm output No. according to the alarm interface connected to the external alarm device.

Alarm Name

Custom a name for the alarm output.

Delay

It refers to the time duration that the alarm output remains after an alarm occurs.

2. Set the alarming schedule. For the information about the settings, see **Set Arming Schedule**.
3. Click **Copy to...** to copy the parameters to other alarm output channels.
4. Click **Save**.

5.2.2 FTP Uploading

If you have enabled and configured the FTP uploading, the device sends the alarm information to the FTP server when an alarm is triggered.

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

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

5.2.4 Notify Surveillance Center

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

5.2.5 Trigger Recording

Check **Trigger Recording**, and the device records the video about the detected alarm event.
For recording settings, refer to ***Video Recording and Picture Capture***





Chapter 6 Live View

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

6.1 Live View Parameters

The supported functions vary depending on the model.

6.1.1 Window Proportion

-  refers to the window size is 16 : 9.
-  refers to the window size is 4 : 3.
-  refers to original window size.
-  refers to self-adaptive window size.


6.1.2 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 .

6.1.3 Select the Third-Party Plug-in



When the live view cannot display via certain browsers, you can change the plug-in for live view according to the browser.

Steps

1. Click **Live View**.
2. Click  to select the plug-in.

6.1.4 Enable and Disable Live View

This function is used to quickly enable or disable live view of the channel.

- Click  to start the live view.
- Click  to stop the live view.

6.1.5 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.

6.1.6 Quick Set Live View

It offers the quick access to the display settings, OSD, and video/audio on live view page.



Steps

1. Click  and click **General** to show quick setup page.
2. Set display settings, OSD, and video/audio.
 - For parameter explanation and instructions of display settings, see [Display Settings](#).
 - For parameter explanation and instructions of OSD settings, see [OSD](#).
 - For parameter explanation and instructions of audio and video settings, see [Video and Audio](#).



6.1.7 Lens Parameters Adjustment

It is used to adjust the lens focus, zoom and iris.

Zoom

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



Focus

- Click , then the lens focuses far and the distant object gets clear.
- Click , then the lens focuses near and the nearby object gets clear.


PTZ Speed

Slide  to adjust the speed of the pan/tilt movement.

Iris


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

6.1.8 Light

Click  to turn on or turn off the illuminator.


6.1.9 Wiper

For the device that has a wiper, you can control the wiper via web browser.


Click  on live view page. The wiper wipes the window one time.

6.1.10 Lens Initialization

Lens initialization is used on the device equipped with motorized lens. The function can reset lens when long time zoom or focus results in blurred image. This function varies according to different models.

Click  to operate lens initialization.

6.1.11 Auxiliary Focus

Click  to realize automatic focus. This function is subject to the actual device model.

6.2 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.

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.

3. Click **OK**.

Chapter 7 Video and Audio

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

7.1 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**.

7.1.1 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 mean larger storage space and higher bandwidth requirements in transmission.

7.1.2 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.

7.1.3 Resolution

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

7.1.4 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.

7.1.5 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.

7.1.6 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.

7.1.7 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.

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.

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.

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.

7.1.8 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.

7.1.9 Display VCA Info

VCA information can be displayed by Player and Video.

Player

Player means the VCA info can be displayed by the dedicated player provided by the manufacturer.

Video

Video means the VCA info can be displayed by any general video player.

7.1.10 Set ROI

ROI (Region of Interest) encoding helps to assigns more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

Before You Start

Please check the video coding type. ROI is supported when the video coding type is H.264 or H.265.

Steps

1. Go to **Configuration** → **Video/Audio** → **ROI**.
2. Check **Enable**.
3. Select **Stream Type**.
4. Select **Region No.** in **Fixed Region** to draw ROI region.
 - 1) Click **Drawing**.
 - 2) Click and drag the mouse on the view screen to draw the fixed region.
 - 3) Click **Stop Drawing**.

Note

Select the fixed region that needs to be adjusted and drag the mouse to adjust its position.

5. Input the **Region Name** and **ROI Level**.
6. Click **Save**.

 **Note**

The higher the ROI level is, the clearer the image of the detected region is.

7. Optional: Select other region No. and repeat the above steps if you need to draw multiple fixed regions.

7.2 Display Settings

It offers the parameter settings to adjust image features.

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

Click **Default** to restore settings.

7.2.1 Image Adjustment

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

7.2.2 Image Adjustment (Thermal Channel)

You can optimize the image display effect of thermal channel by setting background correction and manual correction.

Background Correction

Fully cover the lens with an object of uniform temperature in front of the lens, such as foam board or paperboard. When you click **Correct**, the device will take the uniform object as the standard and optimize the image once.

Manual Correction

Click **Correct** to optimize the image once.

 **Note**

It is a normal phenomenon that short video freezing might occur during the process of **Background Correction** and **Manual Correction**.

7.2.3 DNR

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

OFF

Disable this function.

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.

7.2.4 Set Palette

You can select the palette mode to display the thermal grayscale image to colored image.

Steps

1. Go to **Configuration** → **Image** → **Display Settings**.
2. Select a palette mode in **Image Enhancement** according to your need.

Result

The live view displays the image with palette.

7.2.5 Set Palette Range

The live view can display the palettes effect of the specified temperature range.

Select **Manual** or **Auto** from **By Temp. Range** drop down list.

Auto

The device detects the max. temperature and min. temperature of the scene automatically and display image of the whole scene with palettes.

Manual

In this mode, you can enter the temperature upper limit and lower limit manually. And the live view shows the palettes effect of the desired temperature section more detailed.

7.2.6 DDE

Digital Detail Enhancement is used to adjust the details of the image. **OFF** and **Normal** modes are selectable.

OFF

Disable this function.

Normal

Set the DDE level to control the details of the image. The higher the level is, the more details shows, but the higher the noise is.

7.2.7 Mirror

When the live view image is the reverse of the actual scene, this function helps to display the image normally.

Select the mirror mode as needed.

 **Note**

The video recording will be shortly interrupted when the function is enabled.

7.2.8 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. In PAL, 25 frames are transmitted each second. Each frame is made up of 625 individual scan lines.

7.2.9 Local Video Output

If the device is equipped with video output interfaces, such as BNC, CVBS, HDMI, and SDI, you can preview the live image directly by connecting the device to a monitor screen. Select the output mode as ON/OFF to control the output.

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

Character Set

Select character set for displayed information. If Korean is required to be 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**.

7.4 Overlay Picture

Overlay a customized picture on live view.

Before You Start

The picture to overlay has to be in BMP format with 24-bit, and the maximum picture size is 128 ×

128 pixel.



Steps

1. Go to picture overlay setting page: **Configuration** → **Image** → **Picture Overlay**.
2. Click **Browse** to select a picture, and click **Upload**.
The picture with a red rectangle will appear in live view after successfully uploading.
3. Check **Enable Picture Overlay**.
4. Drag the picture to adjust its position.
5. Click **Save**.



7.5 Set Manual DPC (Defective Pixel Correction)

If the amount of defective pixels in the image is comparatively small and accurate correction is needed, you can correct these pixels manually.

Steps

1. Go to **Configuration** → **Image** → **DPC**.
2. Select manual mode.
3. Click the defective pixel on the image, then a cursor shows on the live view.
4. Click **Up**, **Down**, **Left**, **Right** to adjust the cursor position to the defective pixel position.
5. Click , then click  to correct defective pixel.

Note

If multiple defective pixels need to be corrected, click  after locating a defective pixel. Then after locating other pixels, click  to correct them simultaneously.

6. Optional: Click  to cancel defective pixel correction.

Chapter 8 Video Recording and Picture Capture

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

8.1 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.

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.

3. Click **Upload Picture** to enable uploading snapshots to the FTP server.
4. Click **Test** to verify the FTP server.
5. Click **Save**.

8.2 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  to start recording. Click  to stop recording.

8.3 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.

8.3.1 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**.

8.3.2 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.

Chapter 9 Network Settings

9.1 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 HIKMICRO Studio 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.



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

9.1.1 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.

9.2 Port

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



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.

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.
-

9.3 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**.

9.3.1 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.

9.3.2 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.

9.3.3 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 Servers**, 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.

108M
Wireless Router
Model No.:
TL-WR641G / TL-WR642G

- Status
- Quick Setup
- Basic Settings ---
- + Network
- + Wireless
- Advanced Settings ---
- + DHCP
- Forwarding
 - Virtual Servers
 - Port Triggering
 - DMZ
 - UPnP
- + Security
 - Static Routing
 - Dynamic DNS
- Maintenance ---
- + System Tools

Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	<input type="text" value="80"/>	192.168.10. <input type="text" value="23"/>	ALL <input type="button" value="v"/>	<input checked="" type="checkbox"/>
2	<input type="text" value="8000"/>	192.168.10. <input type="text" value="23"/>	ALL <input type="button" value="v"/>	<input checked="" type="checkbox"/>
3	<input type="text" value="554"/>	192.168.10. <input type="text" value="23"/>	ALL <input type="button" value="v"/>	<input checked="" type="checkbox"/>
4	<input type="text" value="8200"/>	192.168.10. <input type="text" value="23"/>	ALL <input type="button" value="v"/>	<input checked="" type="checkbox"/>
5	<input type="text" value="81"/>	192.168.10. <input type="text" value="24"/>	ALL <input type="button" value="v"/>	<input checked="" type="checkbox"/>
6	<input type="text" value="8001"/>	192.168.10. <input type="text" value="24"/>	ALL <input type="button" value="v"/>	<input checked="" type="checkbox"/>
7	<input type="text" value="555"/>	192.168.10. <input type="text" value="24"/>	ALL <input type="button" value="v"/>	<input checked="" type="checkbox"/>
8	<input type="text" value="8201"/>	192.168.10. <input type="text" value="24"/>	ALL <input type="button" value="v"/>	<input checked="" type="checkbox"/>

Common Service Port: ID

Figure 9-1 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.

9.4 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**.

9.5 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.

9.6 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.

Chapter 10 System and Security

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

10.1 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.

10.2 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**.

10.3 Export Diagnose Information

Diagnose information includes running log, system information, hardware information. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance**, and click **Diagnose Information** to export diagnose information of the device.

10.4 Reboot

You can reboot the device via browser. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance**, and click **Reboot**.

10.5 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.

10.6 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**.

10.7 View Open Source Software License

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

10.8 Time and Date

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

10.8.1 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**.

10.8.2 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**.



Server Address is NTP server IP address.

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

10.8.3 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**.

10.9 Set RS-232

RS-232 can be used to debug device or access peripheral device. RS-232 can realize communication between the device and computer or terminal when the communication distance is short.

Before You Start

Connect the device to computer or terminal with RS-232 cable.

Steps

1. Go to **Configuration** → **System** → **System Settings** → **RS-232**.
2. Set RS-232 parameters to match the device with computer or terminal.
3. Click **Save**.

10.10 Set RS-485

RS-485 is used to connect the device to external device. You can use RS-485 to transmit the data between the device and the computer or terminal when the communication distance is too long.

Before You Start

Connect the device and computer or terminal with RS-485 cable.

Steps

1. Go to **Configuration** → **System** → **System Settings** → **RS-485**.
2. Set the RS-485 parameters.



Note

You should keep the parameters of the device and the computer or terminal all the same.

3. Click **Save**.

10.11 Set Same Unit

Set the same temperature unit and distance unit. When you enable this function, the unit cannot be configured separately in other setting pages

Steps

1. Go to **Configuration** → **System** → **System Settings** → **Unit Settings**.
2. Check **Use Same Unit**.
3. Set the temperature unit and distance unit.

4. Click **Save**.

10.12 Security

You can improve system security by setting security parameters.

10.12.1 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.

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.



Note

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

10.12.2 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.

10.12.3 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 to the list.

Modify Modify the selected IP address in the list.

Delete Delete the selected IP address in the list.

5. Click **Save**.

10.12.4 Set SSH

SSH is a protocol to ensure security of remote login. This setting is reserved for professional maintenance personnel only.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service**.
2. Check **Enable SSH**.
3. Click **Save**.

10.12.5 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. Click **Delete** to recreate and install certificate.

Create and install self-signed certificate Refer to [Create and Install Self-signed Certificate](#)

Create certificate request and install certificate Refer to [Install Authorized Certificate](#)

4. Click **Save**.

Create and Install Self-signed Certificate

Steps

1. Check **Create Self-signed Certificate**.
2. Click **Create**.
3. Follow the prompt to enter **Country/Region, Hostname/IP, Validity** and other parameters.
4. Click **OK**.

Result

The device will install the self-signed certificate by default.

Install Authorized Certificate

If the demand for external access security is high, you can create and install authorized certificate via HTTPS protocol to ensure the data transmission security.

Steps

1. Select **Create certificate request first and continue the installation**.
2. Click **Create**.
3. Follow the prompt to input **Country/Region, Hostname/IP, Validity** and other parameters.
4. Click **Download** to download the certificate request and submit it to the trusted authority for signature.
5. Import certificate to the device.
 - Select **Signed certificate is available, start the installation directly**. Click **Browse** and **Install** to import the certificate to the device.
 - Select **Create the certificate request first and continue the installation**. Click **Browse** and **Install** to import the certificate to the device.
6. Click **Save**.

10.12.6 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**.

10.12.7 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**.
-

10.13 User and Account

10.13.1 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**.

Chapter 11 Appendix

11.1 Common Material Emissivity Reference

Material	Emissivity
Human Skin	0.98
Printed Circuit Board	0.91
Concrete	0.95
Ceramic	0.92
Rubber	0.95
Paint	0.93
Wood	0.85
Pitch	0.96
Brick	0.95
Sand	0.90
Soil	0.92
Cloth	0.98
Hard Paperboard	0.90
White Paper	0.90
Water	0.96

11.2 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 HIKMICRO thermal cameras.



11.3 Device Communication Matrix

Scan the following QR code to get device communication matrix.

Note that the matrix contains all communication ports of HIKMICRO thermal cameras.



11.4 FAQ

Scan the following QR code to get device common FAQ.





HIKMICRO

See the World in a New Way