



**(IP) Network Camera
User Manual**

Copyright © 2018–2019 Hikvision USA Inc. and Hikvision Canada Inc.

Hikvision USA Inc., 18639 Railroad St., City of Industry, CA 91748, USA
Hikvision Canada, 4848 rue Levy, Saint Laurent, Quebec, Canada, H4R 2P1
Telephone: +1-909-895-0400 • Toll Free in USA: +1-866-200-6690
E-Mail: sales.usa@hikvision.com • www.hikvision.com

ALL RIGHTS RESERVED.

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be "Hikvision"). This user manual (hereinafter referred to be "the Manual") cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

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 in the company Website (<http://overseas.hikvision.com/en/>).

Please use this user manual under the guidance of professionals.

Manual Illustrations and Features: Graphics (screen shots, product pictures, etc.) in this document are for illustrative purposes only. Your actual product may differ in appearance. Your product might not support all features discussed in this document.

Trademarks Acknowledgement: **HIKVISION** and other Hikvision trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS," WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS 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 OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED FOR ILLEGITIMATE PURPOSES.

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

Regulatory Information

FCC Information: Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC Compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions: This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement



This product and, if applicable, the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.



2012/19/EU (WEEE Directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info



2006/66/EC (Battery Directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info

Industry Canada ICES-003 Compliance: This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Hikvision North America Privacy Policy

Last Updated: December 2018

Hikvision USA Inc. and Hikvision Canada Inc. and its affiliates (collectively "HIKVISION") provide the following services for use in conjunction with various HIKVISION Internet-connected products ("Products"): a HIKVISION user Website and user accounts that may be accessed at

us.hikvision.com,

ca.hikvision.com,

<https://distributors-us.hikvision.com/>,

<https://distributors-us.hikvision.com/guestLogin.htm>,

<https://ezviz-rma.hikvision.com/>,

<https://order-na.hikvision.com>,

and all associated sites connected with us.hikvision.com (the "Website"); and any services available on the Website, Web Apps, and Mobile Apps ("Available

Services”). The term “HIKVISION Services” means the Website and Available Services.

This Privacy Policy explains how HIKVISION handles the collection, storage, and disclosure of information, including personal information, regarding our HIKVISION Services. It also applies to any information we collect from the operation and use of Products we sell while connected to the HIKVISION Services (the “Products”), and any other HIKVISION Service that links to this Privacy Policy.

We may modify this Privacy Policy at any time, provided certain provisions of this Privacy Policy prove to be incomplete or outdated and further provided that these changes are reasonable for you, taking into account your interests. If we make material changes to this Privacy Policy, we will notify you by the e-mail address specified in your account or by means of notice on our Websites.

You can determine when this Privacy Policy was last revised by referring to the date it was “Last Updated” above.

What Information We Collect

In order to provide HIKVISION services to you, we will ask you to provide personal information that is necessary to provide those services to you. If you do not provide your personal information, we may not be able to provide you with our products or services.

“Personal information” shall have the same meaning as “personal data” and shall include any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity. Examples of personal information include your name, telephone number, e-mail address, and physical address.

Personal information also includes information that alone cannot directly identify you, but with other information we have access to can identify you such as product serial numbers, log data that automatically records information about your visit such as your browser type, domains, page views, the URL of the page that referred you, the URL of the page you next visit, your IP address, and page navigation, unique device ID collected from Products and your mobile devices, data from cookies, pixel tags, and Web beacons, video content files that do not contain personal visual identity information, the country and time zone of the connected Product, geo-location, mobile phone carrier identification, and device software platform and firmware information.

How We Collect and Use Your Information

Here are some examples of the personal information we may collect and how we may use it:

- When you create your account to use HIKVISION Services (“Account”), we will collect information including your name, phone number, and e-mail and physical address. In addition, when you install and activate Products, we will collect certain basic information via our HIKVISION Services such as your product name, the product’s verification code, and serial number, which are unique to the Product connected to the HIKVISION Services and associated with your Account.
- When you respond to our e-mails, contact our customer service, or use other customer support tools, we collect your information to provide you with support, verify your identity with your Account profile information, and confirm your Product.

We may also use the information we collect for the following purpose:

- send you reminders, technical notices, updates, alerts, support and administrative messages, service bulletins, and requested information; and
- pursuant to our legitimate business interests:
 - operate, maintain, improve, and develop our HIKVISION Services and Products;
 - personalize your experience with our HIKVISION Services and Products;
 - increase the safety of our HIKVISION Services and Products – for example, for user authentication, security protection, fraud detection, filing, and backups;
 - perform analytics and conduct customer research;
 - communicate and provide to existing customers additional information that may be of interest to you about our products and services;
 - manage our everyday business needs such as auditing, administration of our HIKVISION Services, forum management, fulfillment, analytics, fraud prevention, and enforcement of our corporate reporting obligations and Terms of Service;
 - enhance other information we have about you to help us better understand you and determine your interests; and
 - in the context of a corporate transaction (e.g., corporate restructuring, sale or assignment of assets, merger) and to protect our rights or property, to enforce our Terms of Service and legal notices and for the establishment, exercise, and defense of legal claims;

with your express consent to

- send you electronic communications in order to inform you about new products and services, unless you choose to unsubscribe;
- use certain non-essential cookies to better understand user behavior, in order to optimize user experience, perfect function design, and offers for products and services from us or to provide better services;
- meet a legal obligation, a court order or other binding decision(s); and accomplish a purpose unrelated to those described in this Privacy Policy by first notifying you and, where required, offering you a choice as to whether or not we may use your Personal Information in this different manner.

Cookies and Other Technologies

We also use cookies, Web beacons, pixel tags, and other technologies to keep records, store your preferences, improve our advertising, and collect information such as log data and device data. This allows us to better understand how you use our HIKVISION Services and Products, diagnose and troubleshoot any problems you have, and otherwise administer and improve our HIKVISION Services and Products. For more information about cookies, please refer to our **User of Cookies** (<https://order-na.hikvision.com/helpCenter/useOfCookies>).

How We Share Your Information

HIKVISION may disclose personal information to cloud service provider, network service provider, and other service providers on the basis of non-disclosure agreements.

The following are the limited situations where we may share personal information:

- We share your personal information with HIKVISION affiliates, who are required to use that information in accordance with the purposes described in this Privacy Policy.
- We use service providers, vendors, technicians, and other third-parties to help us process, store, and protect some of your data and otherwise help us administer our Products and HIKVISION Services effectively, provide a better user experience, process your purchases, and increase the quality of our Products and HIKVISION Services. These third-parties are forbidden from using your personal information for non-HIKVISION purposes and are required to protect your

information in accordance with this Privacy Policy and applicable laws.

- We may provide information to third-parties if we believe in good faith that we are required by mandatory law to do so. For example, to comply with legal orders and government requests; response to a subpoena, or similar legal process, including to law enforcement agencies, regulators, and courts; to protect the interests of our customers and users of the HIKVISION Service; to respond to claims that any content posted or displayed using the HIKVISION Service violates the rights of third parties; in an emergency protect the health and safety of users of the HIKVISION Service or the general public; or to enforce compliance with our Terms of Service.
- If HIKVISION and/or all or part of our assets are ever sold or transferred, your personal information may be among the items sold or transferred. Under such circumstance, we will notify you by the e-mail address specified in your account or by means of notice on us.hikvision.com and associated Websites of (i) the identity and contact information of the purchaser or transferee, (ii) your right to revoke your consent to the provision of personal information, and (iii) the means by which you may revoke such consent.
- We share information to protect our own legitimate business interests when we believe in good faith that we are required or permitted by law to do so. For example, we may share your personal information as needed to support auditing, compliance, and corporate governance functions; to combat fraud or criminal activity; to protect our rights or those of our affiliates and users; or as part of legal proceedings affecting HIKVISION.

We may also disclose non-personal information (for example, aggregated or anonymized data) publicly or with third-parties, provided those data have been rendered anonymous in such a way that the data subject is no longer identifiable. For example, we may share non-personal information:

- for the same reasons we might share Personal information;
- to better understand how our customers interact with our HIKVISION Services and Products, in order to optimize your experience, improve our products, or provide better services;
- for our own research and data analytics; or
- to our vendors for their own analysis and research.

Securing Your Personal Information

HIKVISION has implemented commercially reasonable administrative, technical, and physical security controls that are designed to safeguard personal information. We also conduct periodic reviews and assessments of the effectiveness of our security controls.

Notwithstanding the above, no method of transmission over the Internet, or method of electronic storage, is 100% secure. Therefore, HIKVISION cannot guarantee that your personal information is under absolute security with the existing security technology. If you have any questions about the security of our HIKVISION Services, you can contact us at the contact information below in **Contact Us**.

Accessing, Correcting, and Retention of Your Personal Information

HIKVISION generally stores your personal information on HIKVISION's servers, which is established upon Amazon Servers, until you delete or edit it, or for as long as you remain a HIKVISION customer in order to provide you with the most relevant offers.

Keeping your personal information current helps ensure that we provide you with the most relevant offers. You can access, update, or delete your personal information via your Account profile. We are ready to assist you in managing your subscriptions, deactivating your account, and removing your active profile and data. Your personal information might not be immediately deleted, as we are required to retain records relating to previous purchases through our HIKVISION Services for financial reporting and compliance reasons pursuant to applicable laws. In addition, because of the way we maintain certain services, after you delete certain information, we may temporarily retain backup copies of such information before it is permanently deleted.

We will retain your personal information for the period necessary to fulfill the purpose outlined in this Privacy Policy unless a longer retention period is required or permitted by applicable law.

If you are located in the European Union, subject to limitations in applicable law, you have certain rights in respect to your personal information such as a right of access, rectification, restriction, opposition, and portability. In order to exercise your rights please contact us at the contact information below in **Contact Us**. You also have the right to withdraw your consent at all times, free of charge. You can do this by opting out from direct marketing and by rejecting the use of cookies through your browser settings. If you have concerns about how we handle your personal information, you have the right to lodge a complaint with the data protection authority in your country of residence.

Social Community Features and Social Networks

Social Community Features

Our HIKVISION Services may allow you to publicly post or share information, communicate with others, or otherwise make information accessible to others. Prior to doing so, please read our Terms of Service carefully. All the information you post, share, or communicate may be accessible to anyone with Internet access, and any personal information you include may be read, collected, and used by others.

Social Networks

You have the option to link social networks such as Facebook to your Account. You will be able to post HIKVISION activity to your social network. By proceeding through any of the above steps, you grant HIKVISION permission to access elements of your social network profile information that you have made available to be shared and to use it in accordance with the social network's terms of use and this Privacy Policy.

Links to Other Websites

We may permit others to link to the HIKVISION services or to post a link to their Website. We do not endorse these Websites and are not responsible for other Websites or their privacy practices. Please read their privacy policies before submitting information.

Your Choices

We think that you benefit from a more personalized experience when we know more about you and your preferences. However, you can limit the information you provide to HIKVISION as well as the communications you receive from HIKVISION through your Account preferences.

Commercial E-mails

You will receive commercial e-mails from us only if you have granted prior express consent or if sending those e-mails is otherwise permitted, in accordance with applicable laws.

You may choose not to receive commercial e-mails from us by following the instructions contained in any of the commercial e-mails we send or by logging into your Account and adjusting your e-mail preferences. Please note that even if you unsubscribe from commercial e-mail messages, we may still e-mail you non-commercial e-mails related to your Account on the HIKVISION Services.

Device Data

You may manage how your mobile device and mobile browser share certain device data with HIKVISION by adjusting the privacy and security settings on your mobile device. Please refer to instructions provided by your mobile service provider or the manufacturer of your device to learn how to adjust your settings.

Children's Privacy

HIKVISION does not intend that any portion of its HIKVISION Services will be accessed or used by children under the age of 18, or equivalent minimum age in the relevant jurisdiction and such use is prohibited. Our HIKVISION Services are designed and intended for adults. By using the HIKVISION Services, you represent that you are at least 18 years old, or above the equivalent minimum age in the relevant jurisdiction and understand that you must be at least 18 years old, or above the equivalent minimum age in the relevant jurisdiction in order to create an account and purchase the goods or services advertised through our HIKVISION Services. If we obtain actual knowledge that an account is associated with a registered user who is under the age of 18 years old, or equivalent minimum age in the relevant jurisdiction, we will promptly delete information associated with that account. If you are a parent or guardian of a child under the age of 18, or equivalent minimum age in the relevant jurisdiction and believe he or she has disclosed personal information to us please contact us at the contact information below in **Contact Us**. A parent or guardian of a child under the age of 18, or equivalent minimum age in the relevant jurisdiction may review and request deletion of such child's personal information as well as prohibit the use thereof.

Global Operations

We transfer and process your information globally both in our own facilities and with service providers, or partners, regardless of where you use our Services. The laws, regulations, and standards of the country in which your information is stored or processed may be different from those of your own country.

California Privacy Rights: Pursuant to Section 1798.83 of the California Civil Code, residents of California can obtain certain information about the types of personal information that companies with whom they have an established business relationship have shared with third parties for direct marketing purposes during the preceding calendar year. In particular, the law provides that companies must inform consumers about the categories of personal information that have been shared with third parties, the names and addresses of those third parties, and examples of the types of services or products marketed by those third parties. To request a copy of the information disclosure provided by HIKVISION pursuant to Section 1798.83 of the California Civil Code, please contact us at the contact information below in **Contact Us**. Please allow 30 days for a response.

Contact Us

Please contact us if you have any questions or comments about our privacy practices or this Privacy Policy. You can always reach us through the below contact information:

- A&E Program: aepartners.usa@hikvision.com
- Cybersecurity: security.usa@hikvision.com
- Dealer Partner Program: partners.usa@hikvision.com
- Marketing: marketing.usa@hikvision.com
- OEM/ODM: oem.usa@hikvision.com
- Sales: inside.usa@hikvision.com
- Technical Support: techsupport.usa@hikvision.com
- Canadian Technical Support: techsupport.ca@hikvision.com
- Need Help with This Product/Product Detail feature: inside.usa@hikvision.com
- A&E partner inquiries (user registration, new project support, etc.): aepartners.usa@hikvision.com
- HDP partner inquiries (user registration, new partner registration, etc.): partners.usa@hikvision.com
- US Hikcentral Trial Version Request: sales.usa@hikvision.com
- Canada Hikcentral Trial Version Request: sales.canada@hikvision.com
- Hikvision Robotics Division: robotics.USA@hikvision.com
- Hikvision OEM/ODM Division: OEMODM.usa@hikvision.com
- A&E partner registrations: sarkis.timourian@hikvision.com
- RMA: rma.usa@hikvision.com
- Customer Service: csr.usa@hikvision.com
- Careers: hr.usa@hikvision.com
- Hikvision B2B Portal: b2b.usa@hikvision.com



Please provide: (i) your name (or nickname), your country or region of residence and your preferred method of contact; and (ii) the details of your request or comment along with any corresponding Website links.

Mandatory Electrical Requirements

Hikvision requires the following conditions and equipment for all of its electronic equipment:

- **Grounding:** Ensure good conductivity for all ground paths; examine ground path contact surfaces for defects, dirt, corrosion, or non-conductive coatings that may impede conductivity. Repair or clean contact surfaces as necessary to assure good metal-to-metal contact. Ensure fasteners are properly installed and tightened.
- **Electrical Wiring:** Ensure your outlets are properly wired. They can be checked with an electrical outlet tester.
- **Surge Suppressor (Required):** Hikvision is not responsible for any damage to equipment caused by power spikes in the electrical power grid. Use of a surge suppressor meeting the following specifications is mandatory for all Hikvision electronic equipment:
 - Specifications
 - > Listed by Underwriter’s Laboratories, meeting the UL 1449 Voltage Protection Rating (VPR)
 - > Minimum protection of 1,000 joules or higher
 - > Clamping voltage of 400 V or less
 - > Response time of 1 nanosecond or less
 - Usage
 - > Surge suppressors must not be daisy chained with power strips or other surge suppressors
 - Maintenance
 - > Replace after a serious electrical event (e.g., lighting blew out a transformer down the street)
 - > Replace yearly in storm-prone areas
 - > Replace every two years as routine maintenance

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

Symbol	Description
 WARNING	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury

Safety Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100–240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause overheating or a fire hazard.
- Please make sure that the plug is firmly connected into the power socket.
- If smoke, odor, or noise rise from the device, turn off the power at once, unplug the power cable, and then contact the service center.

Preventive and Cautionary Tips: Before connecting and operating your device, please be advised of the following tips:

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Power down the unit before connecting and disconnecting accessories and peripherals.

The precaution measure is divided into “Warnings” and “Cautions”:

- **Warnings:** Serious injury or death may be caused if any of these warnings are neglected.
- **Cautions:** Injury or equipment damage may be caused if any of these cautions are neglected.

	
Warnings	Cautions
Follow these safeguards to prevent serious injury or death.	Follow these precautions to prevent potential injury or material damage.

 **Warnings:**

- Use a power adapter that can meet the safety extra low voltage (SELV) standard, and source with 12 VDC or 24 VAC (depending on models) according to the IEC60950-1 and Limited Power Source standard.
- This installation should be made by a qualified service person and should conform to all the local codes.
- Please install blackout equipment into the power supply circuit to avoid interruption.

- Please make sure that the ceiling can support more than 50(N) Newton gravities if the camera is fixed to the ceiling.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)



Cautions:

- Make sure the power supply voltage is correct before using the camera.
- Do not drop the camera or subject it to physical shock.
- Do not touch sensor modules with fingers. If cleaning is necessary, use a clean cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period of time, put on the lens cap to protect the sensor from dirt.
- Do not aim the camera lens at a strong light such as the sun or an incandescent lamp. Strong light can cause fatal damage to the camera.
- The sensor may be burned out by a laser beam, so when any laser equipment is being used, make sure that the surface of the sensor not be exposed to the laser beam.
- Do not place the camera in extremely hot, cold temperatures (refer to product specification for working temperature), dusty or damp environment, and do not expose it to high electromagnetic radiation.
- To avoid heat accumulation, ensure there is good ventilation to the device.
- Keep the camera away from water and any liquids.
- While shipping, pack the camera in its original, or equivalent, packing materials. Or packing the same texture.
- Improper use or replacement of the battery may result in hazard of explosion. Please use the manufacturer recommended battery type.

NOTES: For cameras that support IR, you are required to pay attention to the following precautions to prevent IR reflection:

- Dust or grease on the dome cover will cause IR reflection. Please do not remove the dome cover film until the installation is finished. If there is dust or grease on the dome cover, clean the dome cover with clean soft cloth and isopropyl alcohol.
- Make certain the installation location does not have reflective surfaces of objects too close to the camera. The IR light from the camera may reflect back into the lens causing reflection.
- The foam ring around the lens must be seated flush against the inner surface of the bubble to isolate the lens from the IR LEDs. Fasten the dome cover to camera body so that the foam ring and the dome cover are attached seamlessly.

NOTE: If camera fails to synchronize local time with that of the network, you need to set up camera time manually. Visit the camera and enter system setting interface for time setting.

Table of Contents

Chapter 1.	System Requirements	13
Chapter 2.	Network Connection	14
2.1.	Setting the Network Camera over the LAN	14
2.1.1.	Wiring over the LAN	14
2.1.2.	Activating the Camera	15
2.1.2.1.	Activation via Web Browser	15
2.1.2.2.	Activation via SADP Software	16
2.1.2.3.	Activation via Client Software	18
2.1.3.	(Optional) Setting Security Question	21
2.2.	Setting the Network Camera over the WAN	21
2.2.1.	Static IP Connection	21
2.2.2.	Dynamic IP Address Connection	22
2.2.2.1.	Connecting Network Camera via a Router	22
2.2.2.2.	Connecting Network Camera via a Modem	23
Chapter 3.	Access to the Network Camera	24
3.1.	Accessing by Web Browsers	24
3.2.	Accessing by Client Software	25
Chapter 4.	Wi-Fi Settings	26
4.1.	Configuring Wi-Fi Connection in Manage and Ad-Hoc Modes.....	26
4.1.1.	Wireless Connection in Manage Mode.....	26
4.1.2.	Wireless Connection in Ad-Hoc Mode	27
4.1.3.	Security Mode Description:.....	28
4.2.	Easy Wi-Fi Connection with WPS Function	30
4.3.	IP Property Settings for Wireless Network Connection	32
Chapter 5.	Live View	33
5.1.	Live View Page.....	33
5.1.	Live View Page Descriptions	33
5.2.	Starting Live View.....	34
5.3.	Recording and Capturing Pictures Manually	34
5.4.	Operating PTZ Control	34
5.4.1.	PTZ Control Panel	34
5.4.2.	Setting/Calling a Preset	35
5.4.3.	Setting/Calling a Patrol	36
Chapter 6.	Network Camera Configuration	38
6.1.	Configuring Local Parameters.....	38
6.2.	Configure System Settings.....	39
6.2.1.	Configuring Basic Information.....	39
6.2.2.	Configuring Time Settings.....	40
6.2.3.	Configuring RS-232 Settings.....	41

6.2.4.	Configuring RS-485 Settings.....	42
6.2.5.	Configuring DST Settings.....	43
6.2.6.	Configuring External Devices	43
6.2.7.	Configuring VCA Resource.....	44
6.2.8.	Open Source Software License.....	44
6.3.	Maintenance.....	45
6.3.1.	Upgrade & Maintenance	45
6.3.2.	Log	46
6.3.3.	System Service.....	46
6.4.	Security Settings.....	47
6.4.1.	Authentication	47
6.4.2.	IP Address Filter	47
6.4.3.	Security Service	49
6.5.	User Management Interface	49
6.5.1.	User Management	49
6.5.2.	Security Question.....	50
6.5.2.1.	Set Security Question	51
6.5.2.2.	Reset Admin Password	51
6.5.3.	Online Users.....	51
Chapter 7.	Network Settings	52
7.1.	Configuring Basic Settings.....	52
7.1.	Configuring TCP/IP Settings	52
7.1.1.	Configuring DDNS Settings	53
7.1.2.	Configuring PPPoE Settings.....	54
7.1.3.	Configuring Port Settings	55
7.1.4.	Configure NAT (Network Address Translation) Settings	56
7.2.	Configure Advanced Settings	57
7.2.1.	Configuring SNMP Settings.....	57
7.2.2.	Configuring FTP Settings	59
7.2.3.	Configuring E-Mail Settings.....	60
7.2.4.	Platform Access	62
7.2.5.	Wireless Dial.....	63
7.2.6.	HTTPS Settings	64
7.2.7.	Configuring QoS Settings.....	66
7.2.8.	Configuring 802.1x Settings	67
7.2.9.	Integration Protocol.....	68
7.2.9.1.	CGI	68
7.2.9.2.	ONVIF	68
7.2.10.	Bandwidth Adaptation.....	68
7.2.11.	Network Service	68
7.2.11.1.	WebSocket and WebSockets.....	69

7.2.11.2.	SDK Service and Enhanced SDK Service	69
7.2.12.	Smooth Streaming	69
Chapter 8.	Video/Audio Settings	71
8.1.	Configuring Video Settings.....	71
8.1.1.	Video Settings.....	71
8.1.1.1.	H.264+ and H.265+ Video Compression.....	72
8.1.2.	Custom Video	73
8.1.3.	Configuring Audio Settings.....	74
8.1.4.	Configuring ROI Encoding	75
8.1.5.	Display Info. on Stream	77
8.1.6.	Configuring Target Cropping	77
Chapter 9.	Image Settings.....	79
9.1.	Configuring Display Settings.....	79
9.1.1.	Day/Night Auto-Switch.....	79
9.1.1.1.	Image Adjustment	79
9.1.1.2.	Exposure Settings.....	80
9.1.1.3.	Focus	80
9.1.1.4.	Day/Night Switch	80
9.1.1.5.	Backlight Settings	81
9.1.1.6.	White Balance	81
9.1.1.7.	Image Enhancement.....	82
9.1.1.8.	Video Adjustment	82
9.1.2.	Day/Night Scheduled-Switch	82
9.1.3.	Configuring OSD Settings.....	83
9.1.4.	Configuring Privacy Mask.....	85
9.1.5.	Configuring Picture Overlay	85
Chapter 10.	Event Settings	87
10.1.	Basic Events.....	87
10.1.1.	Configuring Motion Detection	87
10.1.2.	Configuring Video Tampering Alarm	92
10.1.3.	Configuring Alarm Input	93
10.1.4.	Configuring Alarm Output.....	94
10.1.5.	Handling Exception	94
10.1.6.	Configuring Other Alarms	95
10.1.6.1.	Wireless Alarm.....	95
10.1.6.2.	PIR Alarm	96
10.1.6.3.	Emergency Alarm	97
10.2.	Smart Events	97
10.2.1.	Configuring Audio Exception Detection.....	98
10.2.2.	Configuring Defocus Detection.....	99
10.2.3.	Configuring Scene Change Detection.....	99

10.2.4.	Configuring Face Detection.....	100
10.2.5.	Configuring Intrusion Detection.....	101
10.2.6.	Configuring Line Crossing Detection	103
10.2.7.	Configuring Region Entrance Detection	105
10.2.8.	Configuring Region Exiting Detection	107
10.2.9.	Configuring Unattended Baggage Detection	109
10.2.10.	Configuring Object Removal Detection	111
10.3.	VCA Configuration	113
10.3.1.	Behavior Analysis	113
10.3.2.	Face Capture	119
10.3.3.	People Counting	122
10.3.4.	Counting	125
10.3.5.	Heat Map	127
10.3.6.	Road Traffic	128
10.3.7.	Queue Management	129
Chapter 11.	Storage Settings	133
11.1.	Configuring Record Schedule.....	133
11.2.	Configure Capture Schedule	135
11.2.1.	Configuring Net HDD	136
11.3.	Memory Card Detection.....	138
11.4.	Configuring Lite Storage.....	140
Chapter 12.	Playback	141
Chapter 13.	Picture	143
Chapter 14.	Application.....	144
14.1.	Face Capture Statistics	144
14.2.	People Counting Statistics.....	144
14.3.	Heat Map Statistics.....	145
14.4.	Counting Statistics	146
14.5.	Queue Management Statistics.....	146
14.5.1.	Commonly Used Data Analysis	147
14.5.2.	Queuing-Up Time Analysis.....	147
14.5.3.	Queue Status Analysis.....	148
14.5.4.	Raw Data.....	148
Chapter 15.	Appendices	149
15.1.	Appendix 1 SADP Software Introduction	149
15.1.1.	Search Active Devices Online	149
15.1.2.	Modify Network Parameters	149
15.2.	Appendix 2 Port Mapping	151

Chapter 1. System Requirements

- **Operating System:** Microsoft Windows XP SP1 and above version
- **CPU:** 2.0 GHz or higher
- **RAM:** 1 GB or higher
- **Display:** 1024×768 resolution or higher
- **Web Browser**
 - **Cameras that Support Plug-In Free Live View:** Internet Explorer 8–11, Mozilla Firefox 30.0 and above, and Google Chrome 41.0 and above

NOTES: For Google Chrome 45 and above version or Mozilla Firefox 52 and above version, which are plug-in free, **Picture** and **Playback** functions are hidden. To use mentioned functions via a Web browser, change to a lower version or to Internet Explorer 8.0 and above version.

- **Cameras that Do NOT Support Plug-In Free Live View:** Internet Explorer 8–11, Mozilla Firefox 30.0–51, and Google Chrome 41.0–44.

Chapter 2. Network Connection

You shall acknowledge that the use of the product with Internet access might be under network security risks. For avoidance of any network attacks and information leakage, please strengthen your own protection. If the product does not work properly, contact your dealer or the nearest service center.

To ensure the network security of the network camera, we recommend that you have the network camera assessed and maintained periodically. Contact us if you need such service.

Before You Start

- If you want to set the network camera via a LAN (Local Area Network), refer to *Section 2.1, Setting the Network Camera over the LAN*.
- If you want to set the network camera via a WAN (Wide Area Network), refer to *Section 2.2, Setting the Network Camera over the WAN*.

2.1. Setting the Network Camera over the LAN

Purpose

To view and configure the camera via a LAN, you need to connect the network camera to the same subnet as your computer and install SADP or iVMS-4200 software to search and change the camera's IP address.

NOTE: For detailed introduction to SADP, refer to *Appendix 1 SADP Software Introduction*.

2.1.1. Wiring over the LAN

The following figures show the two ways for a cable connection between a network camera and a computer.

Purpose

- To test the network camera, you can directly connect the network camera to the computer with a network cable as shown.
- Refer to figure to set a network camera over the LAN via a switch or a router.

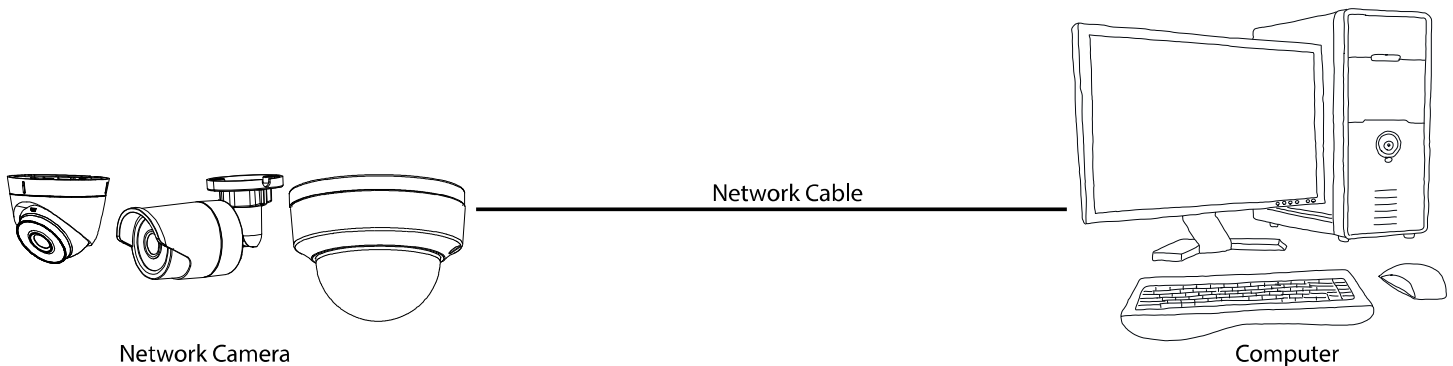


Figure 1, Connecting Directly

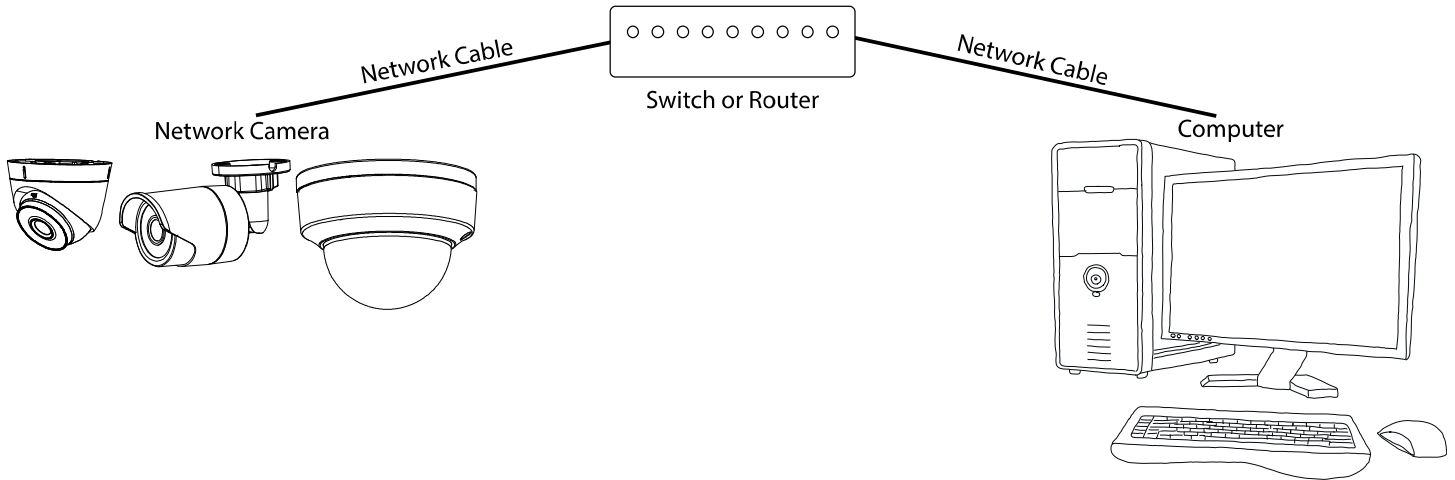


Figure 2, Connecting via a Switch or a Router

2.1.2. Activating the Camera

You are required to activate the camera first by setting a strong password for it before first use.

Activation via Web browser, activation via Hikvision's SADP (Search Active Device Protocol) software, and activation via client software are all supported.

2.1.2.1. Activation via Web Browser

1. Power on the camera and connect the camera to the network.
2. Input the IP address into the Web browser address bar, and click **Enter** to enter the activation interface.

NOTES: The default IP address of the camera is 192.168.1.64.

The computer and the camera should belong to the same subnet.

For cameras that enable DHCP by default, you must use the SADP software to search for the IP address.

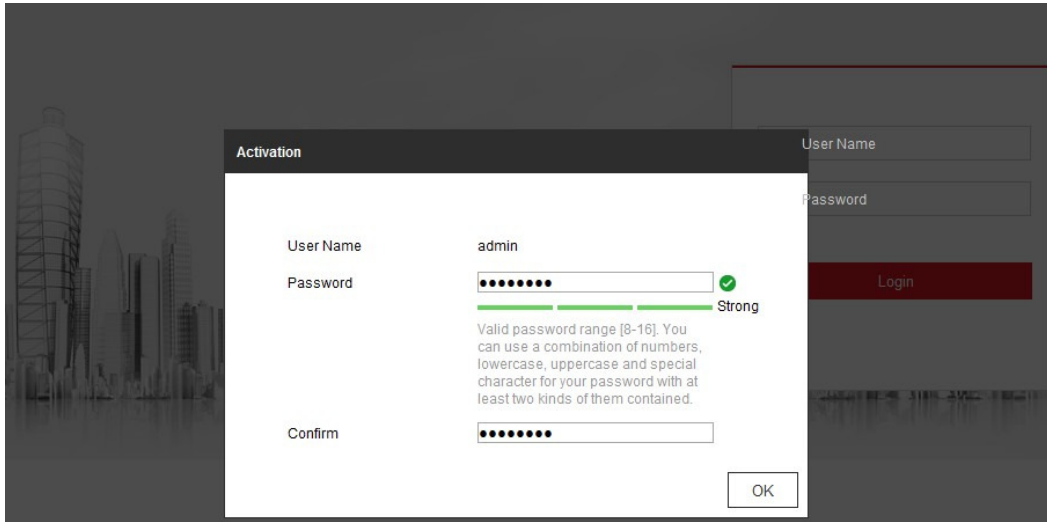


Figure 3, Activation via Web Browser

3. Create and input a password into the password field. A password containing the user name is not allowed.



STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

4. Confirm the password.
5. Click **OK** to save the password and enter the live view interface.

2.1.2.2. Activation via SADP Software

SADP software is used to detect the online device, activate the camera, and reset the password.

Get the SADP software from the supplied disk or the official Website, and install the SADP according to the prompts. Follow these steps to activate the camera:

1. Run the SADP software to search for online devices.
1. Check the device status from the device list, and select the inactive device.

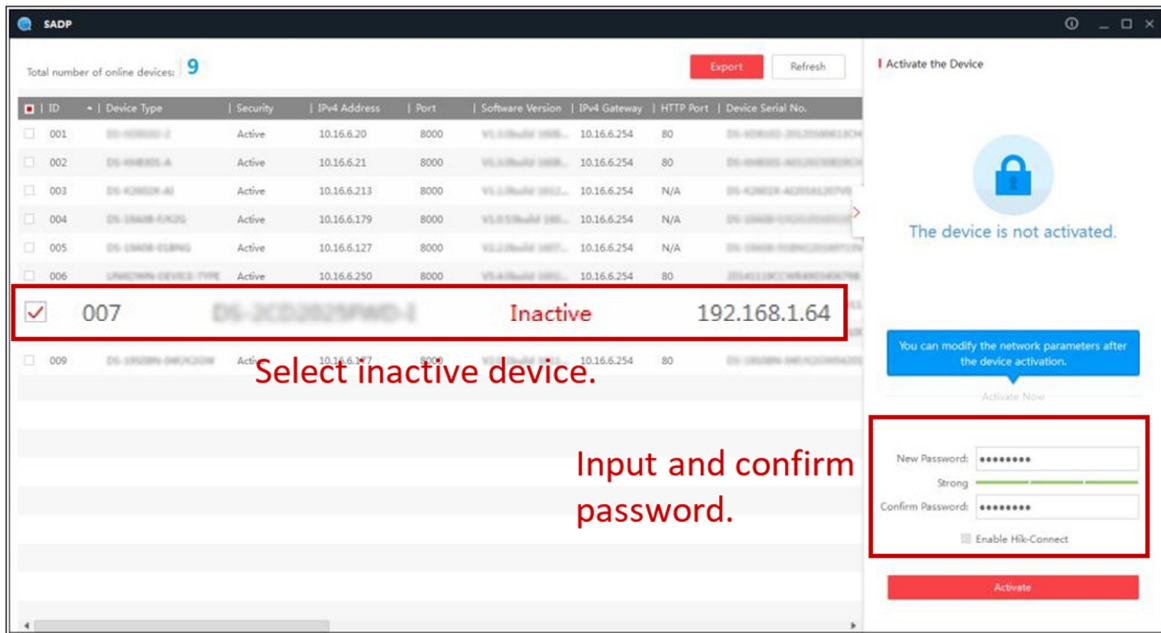


Figure 4, SADP Interface

NOTE: The SADP software supports activating the camera in batch. Refer to the SADP software user manual for details.

2. Create and input the password in the password field, and confirm the password. A password containing the user name is not allowed.



STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

NOTE: You can enable the Hik-Connect service for the device during activation.

3. Click Activate to start activation.

NOTE: You can check whether the activation is completed on the pop-up window. If activation failed, please make sure that the password meets the requirement and try again.

4. Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking the **Enable DHCP** checkbox.

Modify Network Parameters

Enable DHCP
 Enable Hik-Connect

Device Serial No.: XX-XXXXXXXX-XXXXXXXXXXXXXXXXXX

IP Address: 192.168.1.64

Port: 8000

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Security Verification

Admin Password: _____

Modify

[Forgot Password](#)

Figure 5, Modify the IP Address

5. Input the admin password and click **Modify** to activate your IP address modification.

NOTE: Batch IP address modification is supported by SADP. Refer to the SADP user manual for details.

2.1.2.3. Activation via Client Software

The client software is versatile video management software for multiple kinds of devices.

Get the client software from the supplied disk or the official Website, and install the software according to the prompts. Follow the steps to activate the camera.

1. Run the client software, and the software control panel pops up, as shown below.

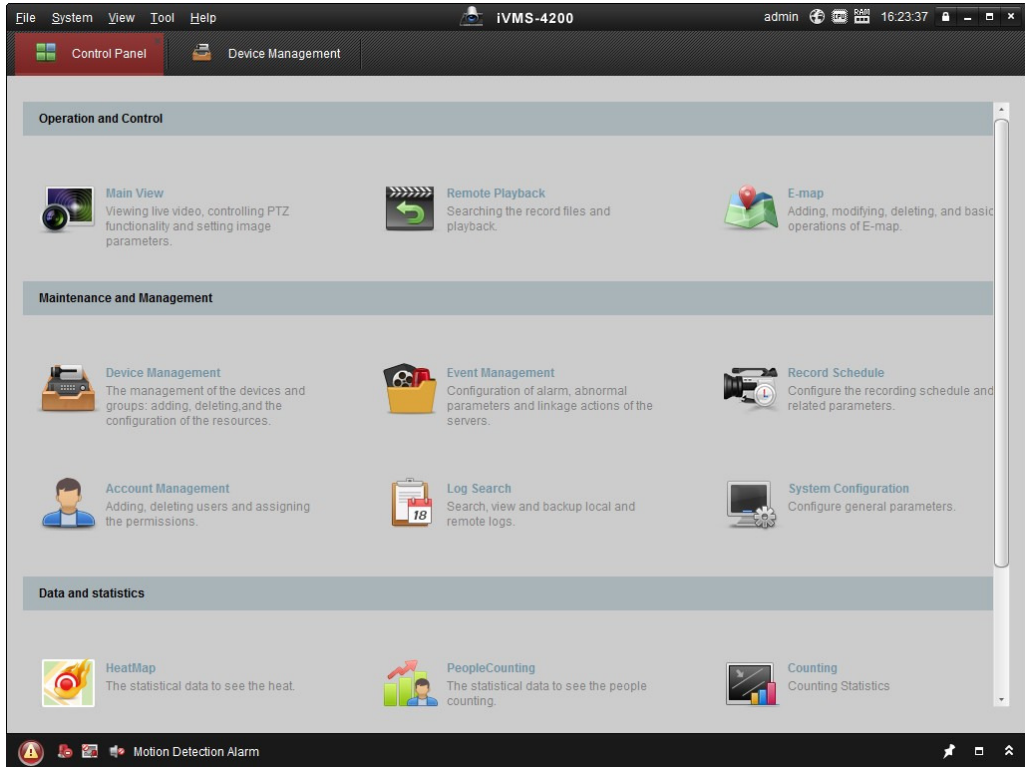


Figure 6, Control Panel

2. Click the **Device Management** icon to enter the **Device Management** interface, as shown below.

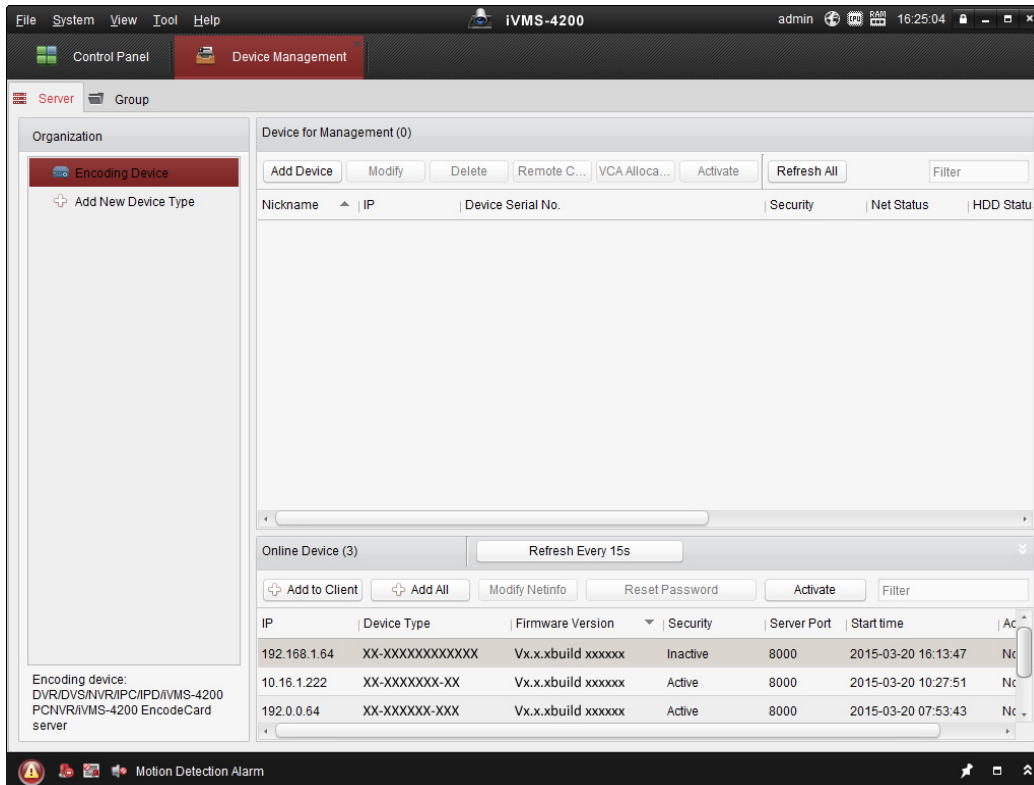


Figure 7, Device Management Interface

3. Check the device status from the device list, and select an inactive device.

4. Click the **Activate** button to pop up the **Activation** interface.

5. Create a password, input the password in the password field, and confirm the password.

NOTE: A password containing the user name is not allowed.



STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

The screenshot shows a dialog box titled "Activation". It has a dark header bar with the title and a close button. The main area is light gray and contains the following elements:

- User Name:** A text field containing "admin".
- Password:** A text field with masked characters (dots). Below it is a green progress bar that is nearly full, with the word "Strong" to its right.
- Instructions:** Text below the progress bar: "Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained."
- Confirm New Password:** A text field with masked characters (dots).
- Buttons:** "Ok" and "Cancel" buttons at the bottom right.

Figure 8, Activation Interface (Client Software)

6. Click the **OK** button to start activation.
7. Click the **Modify Netinfo** button to pop up the **Network Parameter Modification** interface, as shown in the figure below.

Figure 9, Modifying the Network Parameters

8. Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking the **Enable DHCP** checkbox.
9. Input the password to activate your IP address modification.

2.1.3. (Optional) Setting Security Question

Security question is used to reset the admin password when the admin user forgets the password.

Admin user can follow the pop-up window to complete the security question settings during camera activation, or the admin user can go to the **User Management** interface to set up the function.

2.2. Setting the Network Camera over the WAN

Purpose

This section explains how to connect the network camera to the WAN with a static IP or a dynamic IP.

2.2.1. Static IP Connection

Before You Start

Apply a static IP from an ISP (Internet Service Provider). With a static IP address, you can connect the network camera via a router or connect it to the WAN directly.

- **Connecting the Network Camera via a Router**

- Connect the network camera to the router.
- Assign a LAN IP address, the subnet mask, and the gateway.
- Save the static IP in the router.

- Set port mapping, e.g., 80, 8000, and 554 ports. The steps for port mapping vary by router. Please call the router manufacturer for assistance with port mapping.

NOTE: Refer to *Appendix 2* for detailed information about port mapping.

- Visit the network camera through a Web browser or the client software over the internet.

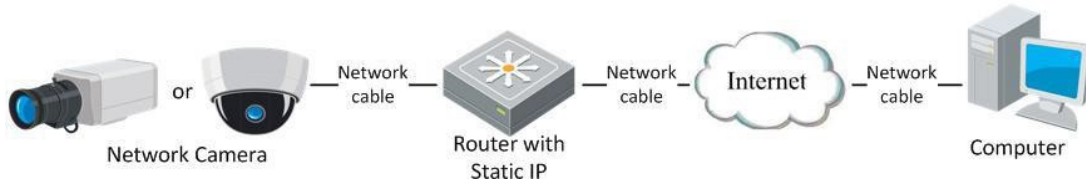


Figure 10, Accessing the Camera through a Router with a Static IP Address

• Connecting Network Camera with Static IP Address Directly

You can also save the static IP address in the camera and directly connect it to the internet without using a router. Refer to *Section 2.1.2* for detailed IP address configuration of the network camera.

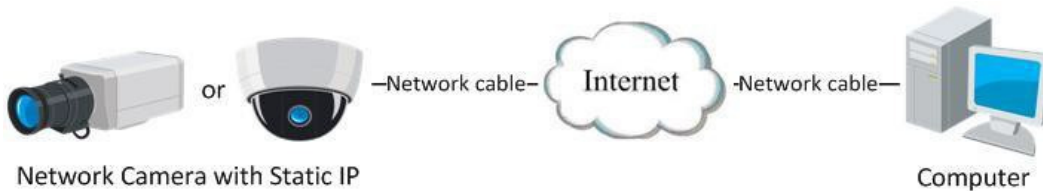


Figure 11, Accessing a Camera with a Static IP Address Directly

2.2.2. Dynamic IP Address Connection

Before You Start

Apply a dynamic IP address from an ISP. With a dynamic IP address, you can connect the network camera to a modem or a router.

2.2.2.1. Connecting Network Camera via a Router

1. Connect the network camera to the router.
2. In the camera, assign a LAN IP address, the subnet mask, and the gateway. Refer to *Section 2.1.2* for detailed IP address configuration of the network camera.
3. In the router, set the PPPoE user name, password, and confirm the password.
4. Set port mapping. E.g. 80, 8000, and 554 ports. The steps for port mapping vary by router. Contact your router manufacturer for assistance with port mapping.

NOTE: Refer to *Appendix 2* for detailed information about port mapping.

5. Apply a domain name from a domain name provider.
6. Configure the **DDNS** settings in the setting interface of the router.
7. Visit the camera via the applied domain name.

2.2.2.2. Connecting Network Camera via a Modem

Purpose

This camera supports the PPPoE auto dial-up function. The camera gets a public IP address by ADSL dial-up after the camera is connected to a modem. You need to configure the PPPoE parameters of the network camera. Refer to *Section 7.1.3 Configuring PPPoE Settings* for detailed configuration.

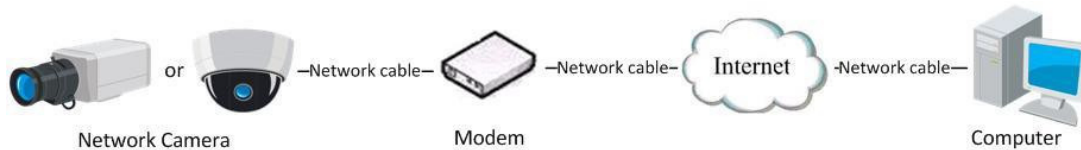


Figure 12, Accessing a Camera with a Dynamic IP Address

NOTE: The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of a dynamic IP, you need to get a domain name from the DDNS provider (E.g. DynDns.com). Please follow the steps below for normal domain name resolution and private domain name resolution to solve the problem.

- **Normal Domain Name Resolution**

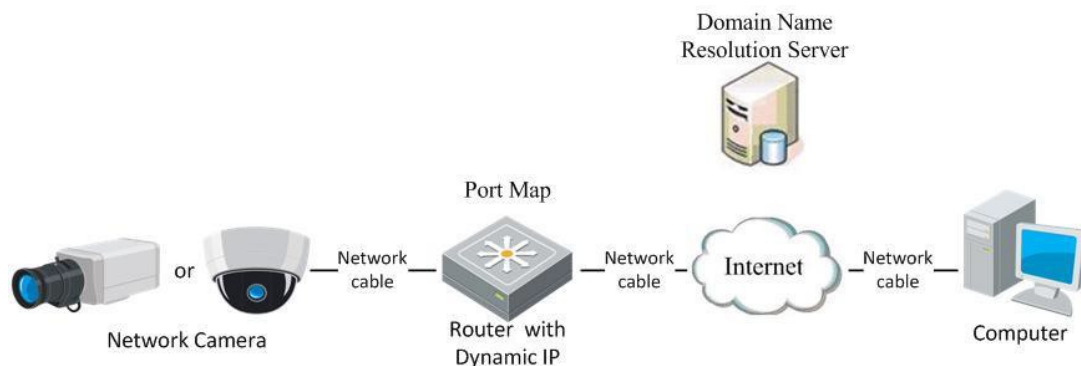


Figure 13, Normal Domain Name Resolution

- Apply a domain name from a domain name provider.
- Configure the DDNS settings in the **DDNS Settings** interface of the network camera. Refer to *Section 7.1.1, Configuring DDNS Settings* for details.
- Visit the camera via the applied domain name.

Chapter 3. Access to the Network Camera

3.1. Accessing by Web Browsers

NOTE: For certain camera models, HTTPS is enabled by default and the camera creates an unsigned certificate automatically. When you access to the camera the first time, the Web browser prompts a notification about the certificate issue.

To cancel the notification, install a signed-certificate to the camera. For detailed operation, see *Section 7.2.6 HTTPS Settings*.

1. Open the Web browser.
2. In the browser address bar, input the network camera's IP address, and press the **Enter** key to enter the login interface.

NOTE: The default IP address is 192.168.1.64. It is recommended that you change the IP address to the same subnet as your computer.

3. Input the user name and password and click **Login**.

The admin user should configure the device accounts and user/operator permissions properly. Delete unnecessary accounts and user/operator permissions.

NOTE: The IP address locks if the admin user performs seven failed password attempts (five attempts by a user/operator).



Figure 14, Login Interface

4. Click **Login**.
5. (Optional) Install the plug-in before viewing the live video and operating the camera. Follow the installation prompts to install the plug-in.

NOTE: For cameras that support plug-in free live view, if you are using Google Chrome 45 and above or Mozilla Firefox 52 and above, plug-in installation is not required. But **Picture** and **Playback** functions are hidden. To use these functions via a Web browser, change to their lower version, or change to Internet Explorer 8.0 and above version.

3.2. Accessing by Client Software

With iVMS-4200 client software (available on the Hikvision Website), you can view the live video and manage the camera with the software.

Follow the installation prompts to install the software. The iVMS-4200 client software live view interface and control panel are shown below.

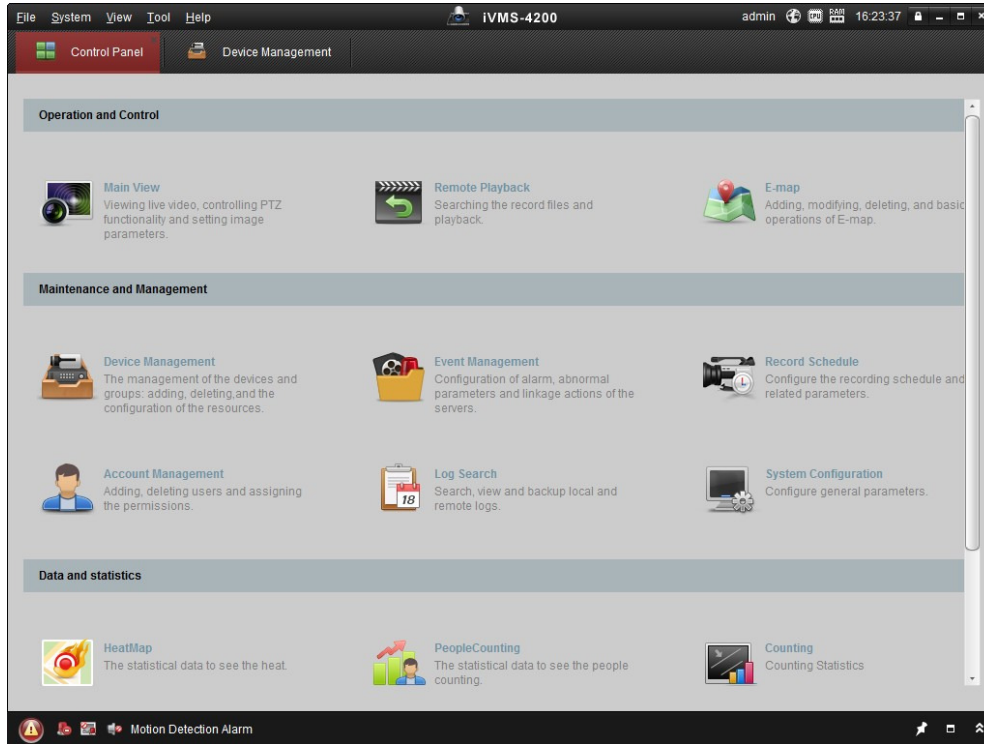


Figure 15, iVMS-4200 Control Panel

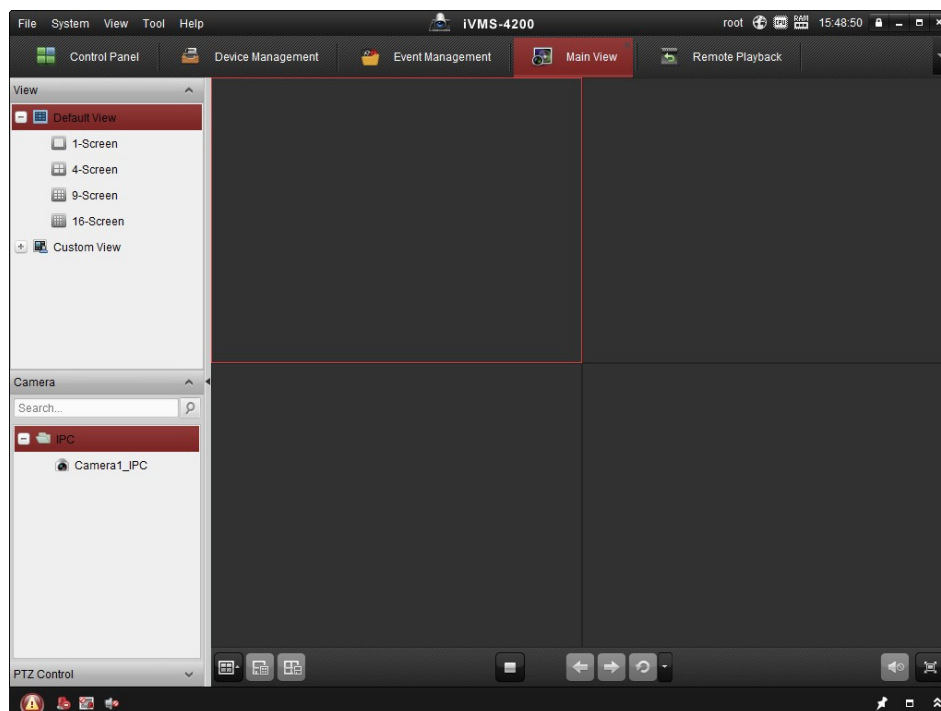


Figure 16, iVMS-4200 Main View

Chapter 4. Wi-Fi Settings

By connecting to the wireless network, you don't need to use cables for the network connection, which is very convenient for the actual surveillance application.

NOTE: This chapter is applicable only for cameras with a built-in Wi-Fi module.

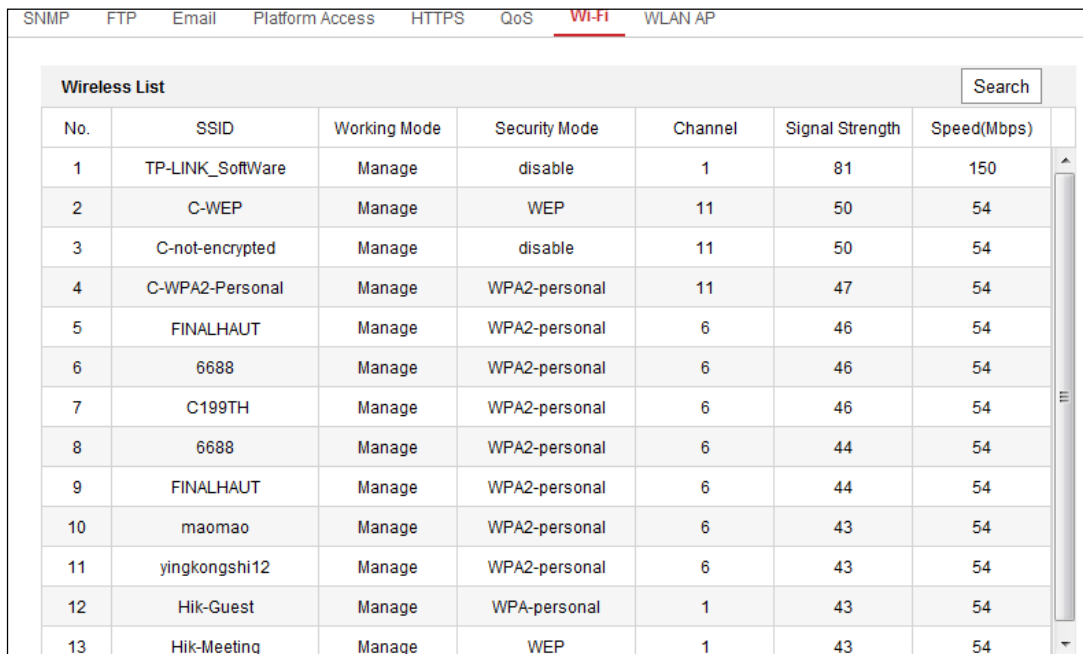
4.1. Configuring Wi-Fi Connection in Manage and Ad-Hoc Modes

Purpose

Two connection modes are supported. Choose a mode as desired and perform the steps to configure the Wi-Fi.

4.1.1. Wireless Connection in Manage Mode

1. Enter the Wi-Fi configuration interface, **Configuration > Network > Advanced Settings > Wi-Fi**.



The screenshot shows the 'Wi-Fi' configuration page with a 'Wireless List' table. The table has columns for No., SSID, Working Mode, Security Mode, Channel, Signal Strength, and Speed(Mbps). The 'Wi-Fi' menu item is highlighted in red in the top navigation bar.

No.	SSID	Working Mode	Security Mode	Channel	Signal Strength	Speed(Mbps)
1	TP-LINK_SoftWare	Manage	disable	1	81	150
2	C-WEP	Manage	WEP	11	50	54
3	C-not-encrypted	Manage	disable	11	50	54
4	C-WPA2-Personal	Manage	WPA2-personal	11	47	54
5	FINALHAUT	Manage	WPA2-personal	6	46	54
6	6688	Manage	WPA2-personal	6	46	54
7	C199TH	Manage	WPA2-personal	6	46	54
8	6688	Manage	WPA2-personal	6	44	54
9	FINALHAUT	Manage	WPA2-personal	6	44	54
10	maomao	Manage	WPA2-personal	6	43	54
11	yingkongshi12	Manage	WPA2-personal	6	43	54
12	Hik-Guest	Manage	WPA-personal	1	43	54
13	Hik-Meeting	Manage	WEP	1	43	54

Figure 17, Wi-Fi List

2. Click **Search** to search the online wireless connections.
3. Click to choose a wireless connection on the list.

Wi-Fi	
SSID	C-WPA2-Personal
Network Mode	<input checked="" type="radio"/> Manage <input type="radio"/> Ad-Hoc
Security Mode	WPA2-personal
Encryption Type	TKIP
Key 1	<input type="text"/>

Figure 18, Wi-Fi Setting – Manage Mode

4. Check the radio button to set the **Network Mode** to **Manage**, and the network **Security Mode** is automatically shown when you select the wireless network (don't change it manually).

NOTE: These parameters are identical to those of the router.

5. Enter the key to connect the wireless network. The key should be that of the wireless network connection you set on the router.

4.1.2. Wireless Connection in Ad-Hoc Mode

If you choose **Ad-Hoc Mode**, you don't need to connect the wireless camera via a router. The scenario is the same as connecting the camera and PC directly with a network cable.

Wi-Fi	
SSID	C-WPA2-Personal
Network Mode	<input type="radio"/> Manage <input checked="" type="radio"/> Ad-Hoc
Security Mode	WPA2-personal
Encryption Type	TKIP
Key 1	<input type="text"/>

Figure 19, Wi-Fi Setting – Ad-Hoc

1. Choose **Ad-Hoc Network Mode**.
2. Customize an **SSID (Service Set Identifier)** to identify the camera access point (maximum 32 characters).
3. Choose the wireless connection Security Mode.
4. Enable Wi-Fi wireless network function on your PC.
5. On the PC, search the networks for the camera SSID.



Figure 20, Ad-Hoc Connection Point

6. Choose the camera’s SSID and connect.

4.1.3. Security Mode Description:

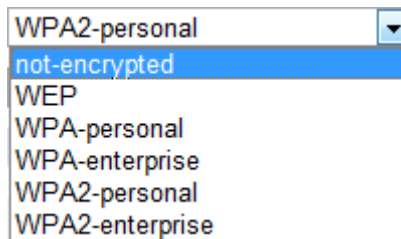


Figure 21, Security Mode

You can choose the Security Mode as not-encrypted, WEP, WPA-personal, WPA-enterprise, WPA2-personal, and WPA2-enterprise.

- **WEP Mode**

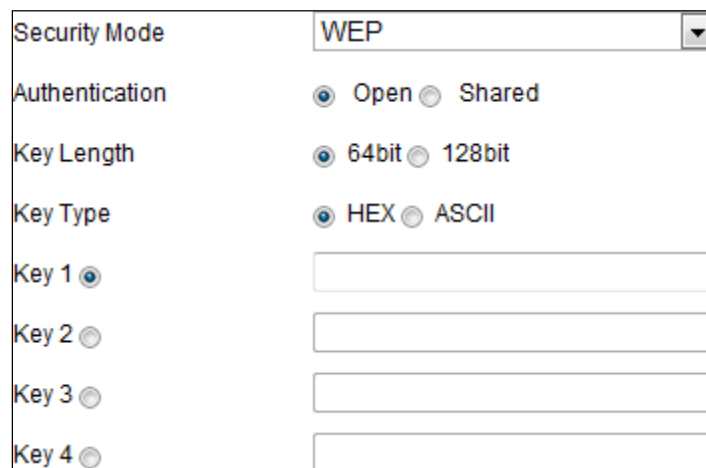


Figure 22, WEP Mode

- **Authentication** – Select **Open** or **Shared** Key System Authentication, depending on the method used by your access point. Not all access points have this option, in which case they probably use **Open** System, which is sometimes known as **SSID Authentication**.
- **Key Length** - This sets the length of the key used for the wireless encryption, 64 or 128 bits. The encryption key length can sometimes be shown as 40/64 and 104/128.

- **Key Type** - The key types available depend on the access point being used. The following options are available:
 - > **HEX:** Allows you to manually enter the hex key.
 - > **ASCII:** In this method the string must be exactly five characters for 64-bit WEP and 13 characters for 128-bit WEP.
 - > **WPA-personal and WPA2-personal Mode:** Enter the required Pre-Shared Key for the access point, which can be a hexadecimal number or a passphrase.

Security Mode	WPA-personal
Encryption Type	TKIP
Key 1 <input checked="" type="radio"/>	

Figure 23, Security Mode – WPA-Personal

- > **WPA- enterprise and WPA2-enterprise Mode:** Choose the type of client/server authentication being used by the access point, **EAP-TLS** or **EAP-PEAP**.

- **EAP-TLS**

Security Mode	WPA-enterprise
Authentication	EAP-TTLS
User Name	<input type="text"/>
Password	<input type="password"/>
Inner authentication	PAP
Anonymous identity	<input type="text"/>
EAPOL version	1
CA certificate	<input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Upload"/>

Figure 24, EAP-TLS

- *Identity* – Enter the user ID to present to the network.
- *Private Key Password* – Enter the password for your user ID.
- *EAPOL Version* – Select the version used (1 or 2) in your access point.
- *CA Certificates* – Upload a CA certificate to present to the access point for authentication.

- **EAP-PEAP**

- *User Name* – Enter the user name to present to the network.
- *Password* – Enter the network password.
- *PEAP Version* – Select the PEAP version used at the access point.

- *Label*– Select the label used by the access point.
- *EAPOL Version*– Select version (1 or 2) depending on the version used at the access point.
- *CA Certificates*– Upload a CA certificate to present to the access point for authentication.



STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

4.2. Easy Wi-Fi Connection with WPS Function

Purpose

Setting a wireless network connection is never easy. To avoid the complexity of setting up the wireless connection, you can enable the **WPS** function.

WPS (Wi-Fi Protected Setup) refers to an easy procedure to configure an encrypted connection between a device and a wireless router. WPS makes it easy to add new devices to an existing network without entering long passphrases. There are two modes of WPS connection, **PBC** mode and **PIN** mode.

NOTE: If you enable the **WPS** function, you do not need to configure parameters such as encryption type, and you don't need to know the wireless connection key.

The screenshot shows the WPS configuration page. At the top, there is a header 'WPS'. Below it, the 'Enable WPS' checkbox is checked. The 'PIN Code' field is set to '12345678' and has a 'Generate' button to its right. There are two radio button options: 'PBC connection' (which is selected) and 'Use router PIN code'. Each has a 'Connect' button next to it. The 'SSID' field is set to 'C-WPA2-Personal'. The 'Router PIN code' field is empty. At the bottom of the form is a red 'Save' button.

Figure 25, Wi-Fi Settings - WPS

PBC Mode

PBC stands for **Push-Button-Configuration**, in which the user simply has to push a button, either an actual or virtual one (as the **Connect** button on the Internet Explorer browser configuration interface), on both the Access Point (and a registrar of the network) and the new wireless client device.

1. Check the **Enable WPS** checkbox to enable **WPS**.

- Set the connection mode to **PBC**.

NOTE: Both the Access Point and connecting device must support this mode.

- Check the Wi-Fi router to see if there is a WPS button. If yes, press the button and you will see the indicator near the button start flashing, which means the WPS function of the router is enabled. For detailed operation, please see the router's user guide.
- Press the WPS button to enable the function on the camera.

NOTE: If there is no WPS button on the camera, you can also click the virtual button on the Web interface to enable the PBC function.

- Click the **Connect** button. If **PBC Mode** is enabled both in the router and on the camera, the camera and the wireless network will connect automatically.

PIN Mode

PIN mode requires a Personal Identification Number (PIN) to be read from either a sticker or the display on the new wireless device. This PIN must then be entered to connect to the network Access Point.

- Choose a wireless connection on the list and the **SSID** is loaded automatically.
- Choose **Use route PIN code**.

Figure 26, Use PIN Code

NOTE: If the PIN code is generated from the router, enter the PIN code you get from the router in the **Router PIN code** field.

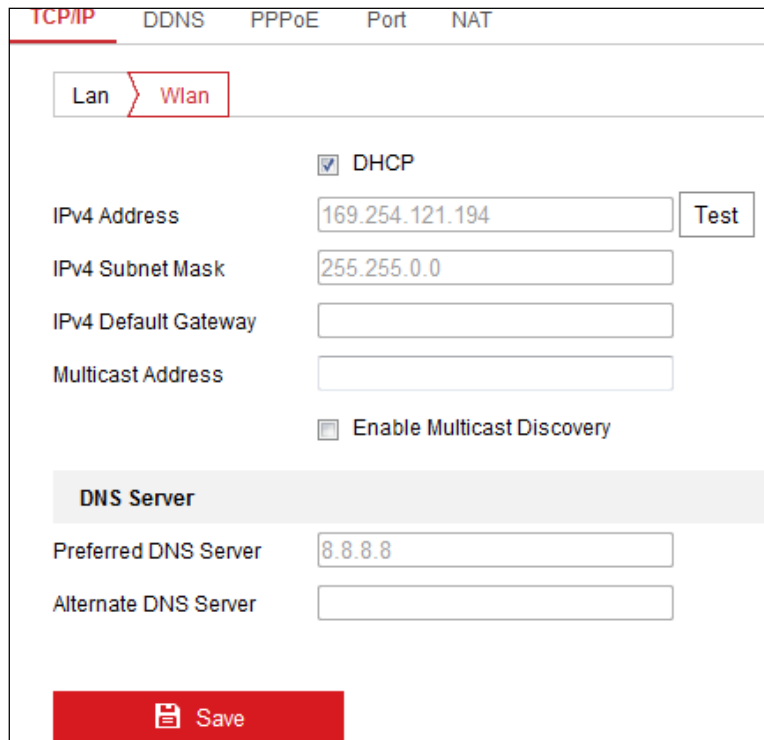
- Click **Connect**, or generate the PIN code on the camera. The PIN code expiration time is 120 seconds.
- Click **Generate**.

- Enter the code to the router.

4.3. IP Property Settings for Wireless Network Connection

The default IP address of the wireless network interface controller is 192.168.1.64. Once you connect to the wireless network, you can change the IP address.

1. Enter the TCP/IP configuration interface, **Configuration > Network > Basic Settings > TCP/IP**.
2. Select the **Wlan** tab.



The screenshot shows the TCP/IP configuration interface for a wireless network connection. The interface has a top navigation bar with tabs for TCP/IP, DDNS, PPPoE, Port, and NAT. Below the navigation bar, there are two tabs: Lan and Wlan, with Wlan selected. The main configuration area includes a DHCP checkbox (checked), an IPv4 Address field (169.254.121.194) with a Test button, an IPv4 Subnet Mask field (255.255.0.0), an IPv4 Default Gateway field, a Multicast Address field, and an Enable Multicast Discovery checkbox (unchecked). Below these fields is a DNS Server section with Preferred DNS Server (8.8.8.8) and Alternate DNS Server fields. A red Save button is located at the bottom of the configuration area.

Figure 27, Setting WLAN Parameters

3. Customize the **IPv4 Address**, the **IPv4 Subnet Mask**, and the **Default Gateway**. The setting procedure is the same as that for a LAN.

NOTE: If you want to be assigned the IP address automatically, check the DHCP checkbox.

Chapter 5. Live View Live View Page

Purpose

The live view page lets you view real-time video, capture images, control PTZ cameras, set/call presets, and configure video parameters.

Log in the network camera to enter the live view page, or click **Live View** on the menu bar of the main page.

5.1. Live View Page Descriptions

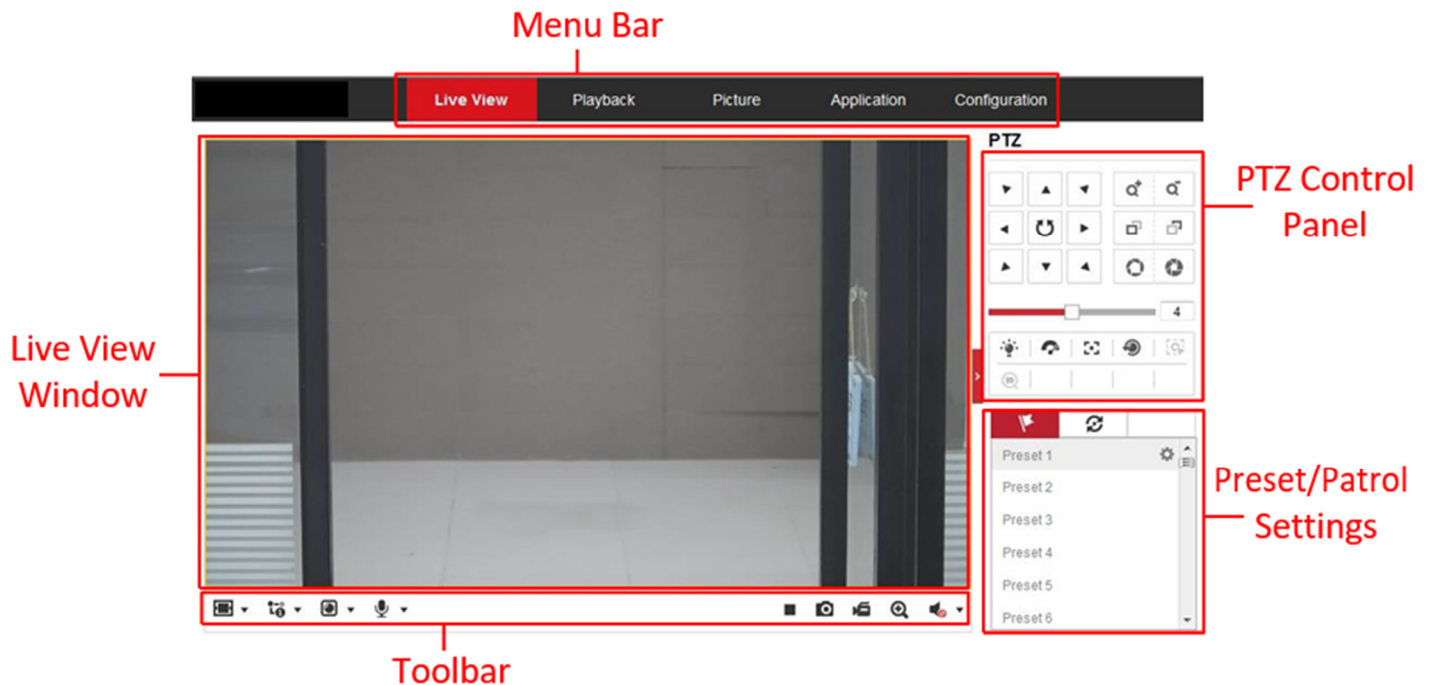


Figure 28, Live View Page

- **Menu Bar:** Click the relevant tab to enter Live View, Playback, Picture, Application, and Configuration page respectively.
- **Live View Window:** Display live video.
- **Toolbar:** Toolbar allows you to adjust the live view window size, the stream type, and the plug-ins. It also allows you to process the operations on the live view page (e.g., start/stop live view, capture, record, audio on/off, two-way audio, start/stop digital zoom, etc.).

For IE (Internet Explorer) users, plug-ins such as Web Components and Quicktime are selectable. For non-IE users, Web Components, Quicktime, VLC, or MJPEG are selectable if they are supported by the Web browser.

NOTE: For cameras that support plug-in free live view, if Google Chrome 45 and above version or Mozilla Firefox 52 and above version is used, plug-in installation is not required. But **Picture** and **Playback** functions are hidden. To use these functions via a Web browser, change to their lower versions, or use Internet Explorer 8.0 and above version.

- **PTZ Control:** Perform camera panning, tilting, and zooming actions. Control the light and the wiper (only available for cameras supporting PTZ function).
- **Preset/Patrol Settings:** Set/call/delete PTZ camera presets or patrols.

5.2. Starting Live View














In the live view window, click  on the toolbar to start the camera's live view.





Figure 29, Live View Toolbar

Table 5-1 Toolbar Descriptions

Icon	Description
/	Start/stop live view
	The window size is 4:3
	The window size is 16:9
	The original window size
	Self-adaptive window size
 , ,  , etc.	Live view with the different video streams (supported video streams vary by camera model)
	Click to select third-party plug-in
	Manually capture the picture
	Manually start/stop recording
	Audio on and adjust volume/Mute
	Turn on/off microphone
	Start/stop digital zoom function

NOTE: The icons vary by camera.

5.3. Recording and Capturing Pictures Manually

In the live view interface, click  on the toolbar to capture live pictures or click  to record the live view. The saving paths of the captured pictures and clips can be set on the **Configuration > Local** page.

NOTE: The captured image will be saved as a JPEG file or BMP file on your computer.

5.4. Operating PTZ Control

Purpose

In the live view interface, you can use the PTZ control buttons for pan/tilt/zoom control of the camera.

NOTE: For PTZ control, the camera connected to the network must support the PTZ function or have a pan/tilt unit installed. Properly set the PTZ parameters on the RS-485 settings page (refer to *Section 6.2.4, Configuring RS-485 Settings*).

5.4.1. PTZ Control Panel











1. On the live view page, click  next to the right side of the live view window to show the PTZ control panel (click  to hide it).
2. Click the direction buttons to control the pan/tilt movements.














Figure 30, PTZ Control Panel

3. Click the zoom/focus/iris buttons for lens control.

NOTES: There are eight direction arrows , , , , , , ,  in the control panel. Click the arrows to adjust the relative positions.

For cameras that support lens movements only, the direction buttons are invalid.

Table 5-2 Descriptions of PTZ Control Panel

Icon	Description
	Zoom in/out
	Focus near/far
	Iris +/-
	PTZ speed adjustment
	Light on/off
	Wiper on/off
	Auxiliary focus
	Initialize lens
	Adjust speed of pan/tilt movements
	Start Manual Tracking
	Start 3D Zoom

5.4.2. Setting/Calling a Preset

- **Setting a Preset**

1. In the PTZ control panel, select a preset number from the preset list.

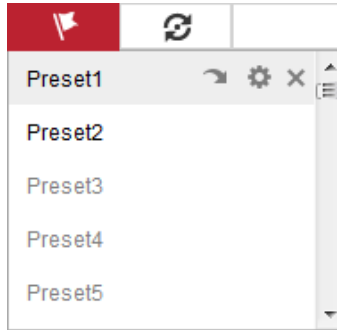


Figure 31, Setting a Preset

2. Use the PTZ control buttons to move the lens to the desired position.

- Pan the camera to the right or left
- Tilt the camera up or down
- Zoom in or out
- Refocus the lens


3. Click  to finish setting the current preset.

4. You can click  to delete the preset.

• Calling a Preset

This feature enables the camera to point to a predetermined preset scene manually or when an event takes place.

You can call a defined preset at any time.

In the PTZ control panel, select a defined preset from the list and click  to call it, or you can place the mouse on the presets interface and call the preset by typing the preset no.

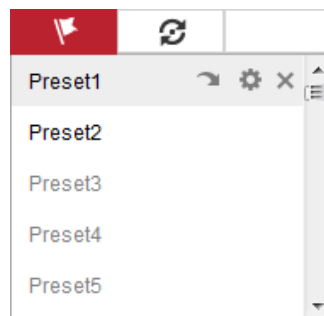



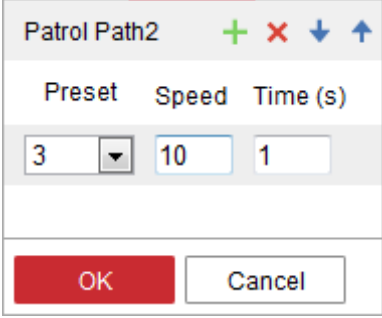
Figure 32, Calling a Preset

5.4.3. Setting/Calling a Patrol

NOTE: No less than two presets have to be configured before you can set a patrol.

1. Click  to enter the patrol configuration interface.




2. Select a path no., and click  to add the configured preset.
3. Select the preset, and input the patrol duration and patrol speed.
4. Click **OK** to save the first preset.
5. Follow the steps above to add other presets.



Preset	Speed	Time (s)
3	10	1

OK Cancel

Figure 33, Add Patrol Path

6. Click **OK** to save the patrol.
7. Click  to start the patrol, and click  to stop it.
8. (Optional) Click  to delete the patrol.

Chapter 6. Network Camera Configuration

6.1. Configuring Local Parameters

Purpose

Local configuration refers to live view, record file, and captured picture parameters. The record files and captured pictures are the ones you record and capture using a Web browser and thus their saving paths are on the PC running the browser.

1. Enter the Local Configuration interface: **Configuration > Local**.
 2. Configure the following settings:
 - **Live View Parameters:** Set the protocol type and live view performance.
 - **Protocol Type:** TCP, UDP, MULTICAST, and HTTP are selectable
 - TCP:** Ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected
 - UDP:** Provides real-time audio and video streams
 - HTTP:** Allows the same quality as TCP without setting specific ports for streaming under some network environments
 - MULTICAST:** It's recommended to select MCAST type when using the Multicast function. For detailed information about Multicast, refer to *Section 7.1, Configuring TCP/IP Settings*.
 - **Play Performance:** Set the live view performance to Shortest Delay, Balanced, Fluent, or Custom. For Custom, you can set the live view frame rate.
 - **Rules:** It refers to the rules on your local browser. Select enable or disable to display or not display colored marks when motion detection, face detection, or intrusion detection is triggered (e.g., enabled as the rules are, and the face detection is enabled as well, when a face is detected, it will be marked with a green rectangle on live view).
 - **Display POS Information:** If enabled, the detected target's feature information is dynamically displayed near the target in the live image. The feature information for different functions vary. For example, ID and waiting time for Queue Management, height for People Counting, etc.
- NOTE:** **Display POS Information** is available only for certain camera models.
- **Image Format:** Choose the image format for picture capture.

Live View Parameters				
Protocol	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP	<input type="radio"/> MULTICAST	<input type="radio"/> HTTP
Play Performance	<input type="radio"/> Shortest Delay	<input type="radio"/> Balanced	<input type="radio"/> Fluent	<input checked="" type="radio"/> Custom <input type="text" value="20"/> frame
Rules	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
Display POS Information	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
Image Format	<input checked="" type="radio"/> JPEG	<input type="radio"/> BMP		

Figure 34, Live View Parameters

- **Record File Settings:** Set the saving path of the recorded video files. Valid for the record files you recorded with the Web browser.
 - **Record File Size:** Select the packed size of the manually recorded and downloaded video files to 256 MB, 512 MB, or 1 GB. After selection, the maximum record file size is the selected value.
- **Save record files to:** Set the saving path for the manually recorded video files.
 - **Save downloaded files to:** Set the saving path for the downloaded video files in playback mode.
- **Picture and Clip Settings:** Set the saving paths of the captured pictures and clipped video files. Valid for the pictures you capture with the Web browser.
 - **Save snapshots in live view to:** Set the saving path of the manually captured pictures in live view mode.
 - **Save snapshots when playback to:** Set the saving path of the captured pictures in playback mode.
 - **Save clips to:** Set the saving path of the clipped video files in playback mode.

NOTE: You can click **Browse** to change the directory for saving the clips and pictures, and click **Open** to open the set folder of clips and picture saving.

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

6.2. Configure System Settings

Purpose

Follow the instructions below to configure the system settings, include System Settings, Maintenance, Security, User Management, etc.

6.2.1. Configuring Basic Information

Enter the Device Information interface: **Configuration > System > System Settings > Basic Information**.

In the **Basic Information** interface, you can edit the Device Name and Device No. Other information of the network camera, such as Model, Serial No., Firmware Version, Encoding Version, Number of Channels, Number of HDDs, Number of Alarm Input, and Number of Alarm Output are displayed. The information cannot be changed in this menu. It is the reference for future maintenance or modification.

6.2.2. Configuring Time Settings

Purpose

You can follow the instructions in this section to configure the time synchronization and DST settings.

1. Enter the Time Settings interface, **Configuration > System > System Settings > Time Settings**.

Figure 35, Time Settings

2. Select the Time Zone of your location from the drop-down menu.
3. Configure the NTP settings.
 - 1) Click to enable the **NTP** function.
 - 2) Configure the following settings:
 - **Server Address:** IP address of NTP server
 - **NTP Port:** Port of NTP server
 - **Interval:** The time interval between the two synchronizing actions with NTP server
 - 3) (Optional) Click the **Test** button to test the time synchronization function via NTP server.

Figure 36, Time Sync by NTP Server

NOTE: If the camera is connected to a public network, use an NTP server that has a time synchronization function such as the server at the National Time Center (IP Address: 210.72.145.44). If the camera is in a customized network, NTP software can be used to establish an NTP server for time synchronization.

4. Configure the manual time synchronization.


- 1) Check **Manual Time Sync.** to enable the manual time synchronization function.
- 2) Click the  icon to select the date and time on the pop-up calendar.
- 3) (Optional) Check **Sync. with computer time** to synchronize the device time with the local PC.



Figure 37, Time Sync Manually

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

6.2.3. Configuring RS-232 Settings

The RS-232 port can be used in two ways:

- **Parameters Configuration:** Connect a computer to the camera through the serial port. Device parameters can be configured by using software such as HyperTerminal. The serial port parameters must be the same as the serial port parameters of the camera.
- **Transparent Channel:** Connect a serial device directly to the camera. The serial device will be controlled remotely by the computer through the network.

1. Enter RS-232 Port Setting interface: **Configuration** > **System** > **System Settings** > **RS232**.
2. Configure the Baud Rate, Data Bit, Stop Bit, Parity, Flow Control, and Usage.

Basic Information	Time Settings	RS232	RS485	DST
Baud Rate		115200		
Data Bit		8		
Stop Bit		1		
Parity		None		
Flow Ctrl		None		
Usage		Console		

Save

Figure 38, RS-232 Settings

NOTE: To connect the camera by the RS-232 port, the RS-232 parameters should be exactly the same as the parameters you configured here.

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

6.2.4. Configuring RS-485 Settings

Purpose

The RS-485 serial port is used to control the PTZ of the camera. Configure the PTZ parameters before you control the PTZ unit.

1. Enter RS-485 Port Setting interface: **Configuration** > **System** > **System Settings** > **RS485**.

Basic Information	Time Settings	RS232	RS485	DST
RS485				
Baud Rate			9600	
Data Bit			8	
Stop Bit			1	
Parity			None	
Flow Ctrl			None	
PTZ Protocol			PELCO-D	
PTZ Address			0	

Save

Figure 39, RS-485 Settings

2. Set the RS-485 parameters and click **Save** to save the settings.
3. By default, the **Baud Rate** is set to 9600 bps, the **Data Bit** is 8, the **Stop Bit** is 1, and the **Parity and Flow Control** is None.

NOTE: The baud rate, PTZ protocol, and PTZ address parameters should be exactly the same as the PTZ camera parameters.

6.2.5. Configuring DST Settings

Purpose

Daylight Saving Time (DST) is a way of making better use of the natural daylight by setting your clock forward one hour during the summer months, and back again in the fall.

Configure DST according to your actual demand.

1. Enter the DST configuration interface, **Configuration > System > System Settings > DST**.

Basic Information	Time Settings	RS232	RS485	DST
<input type="checkbox"/> Enable DST				
Start Time		Jan	First	Sun 00
End Time		Jan	First	Sun 00
DST Bias		30min		

Figure 40, DST Settings

2. Select the start time and the end time.
3. Select **DST Bias**.
4. Click **Save** to activate the settings.

6.2.6. Configuring External Devices

Purpose

For devices that support external devices, including a housing wiper or LED light, you can control them via the Web browser. External devices vary by camera model.

1. Enter the External Device configuration interface, **Configuration > System > System Settings > External Device**.

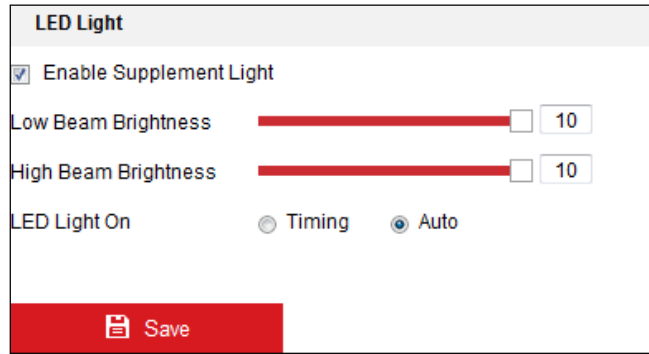


Figure 41, External Device Settings

2. Check the **Enable Supplement Light** checkbox to enable the LED light.
3. Move the slider to adjust the low beam brightness and high beam brightness.
4. Select the LED light mode. **Timing** and **Auto** are selectable.
 - **Timing:** The LED will turn on by the schedule set. Set the Start Time and End Time.

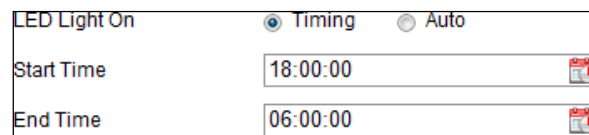


Figure 42, Set Schedule

- **Auto:** The LED will turn on according to the environment illumination.
5. Click **Save** to save the settings.

6.2.7. Configuring VCA Resource

Purpose

VCA Resource offers you options to enable certain VCA functions according to actual need when several VCA functions are available. It helps allocate more resources to the desired functions.

NOTE: **DS-2CD2xx6G1 Series Cameras Only:** Some Smart VCA functions (line crossing detection, intrusion detection, region entrance/exit detection) are not functional when using third video stream, H.265+ video compression, or motion detection.

1. Enter the VCA Resource interface, **Configuration > System > System Settings > VCA Resource**.
2. Select a desired VCA combination. Available VCA combinations vary by camera model.
3. Click **Save** to save the settings. A reboot is required after setting the VCA Resource.

NOTES: VCA combinations are mutually exclusive. When you activate one, the others are hidden.

The function may not be supported by some camera models.

6.2.8. Open Source Software License

Information about the open source software that applies to the IP camera can be checked if required. Go to **Configuration > System Settings > About**.

6.3. Maintenance

6.3.1. Upgrade & Maintenance

Purpose

The Upgrade & Maintenance interface allows you to process operations, including reboot, partly restore, restore to default, export/import the configuration files, and upgrade the device.

1. Enter the Maintenance interface: **Configuration > System > Maintenance > Upgrade & Maintenance**.

- **Reboot:** Restart the device.
- **Restore:** Reset all parameters, except IP parameters and user information, to the default settings.
- **Default:** Restore all the parameters to the factory default.

NOTE: After restoring the default settings, the IP address is also restored to the default IP address, please be careful with this action.

For cameras that support Wi-Fi, wireless dial, or the wlan function, the **Restore** action does not restore the related settings of mentioned functions to default.

- **Information Export**
- **Device Parameters:** Click to export the camera's current configuration file. This operation requires admin password to proceed.

For the exported file, you also have to create an encryption password. The encryption password is required when you import the file to other cameras.

- **Diagnose Information:** Click to download log and system information.
- **Import Config. File:** Configuration file is used for batch configuration of the cameras.

- 1) Click **Browse** to select the saved configuration file.
- 2) Click **Import** and input the encryption password that you set during export.

NOTE: You need to reboot the camera after importing the configuration file.

- **Upgrade:** Upgrade the device to a particular version.
 - 1) Select the firmware or the firmware directory to locate the upgrade file.

Firmware: Locate the exact path of the upgrade file.

Firmware Directory: Only the directory the upgrade file belongs to is required.

- 2) Click **Browse** to select the local upgrade file, and then click **Upgrade** to start remote upgrade.

NOTE: The upgrading process will take 1 to 10 minutes. Don't disconnect camera power during the process. The camera will reboot automatically after the upgrade.

6.3.2. Log

Purpose

The camera's operation, alarm, exception, and information can be stored in log files. You can also export the log files on demand.

Before You Start

Configure network storage for the camera or insert an SD card in the camera.

1. Enter the log searching interface: **Configuration** > **System** > **Maintenance** > **Log**.

No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP

Figure 43, Log Searching Interface

2. Specify the log search conditions, including the Major Type, Minor Type, Start Time and End Time.
3. Click **Search** to search log files. The matched log files will be displayed on the log list interface.

No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP
1	2015-05-25 19:12:34	Operation	Remote: Get Working Sta...		admin	10.16.1.107
2	2015-05-25 19:12:12	Operation	Remote: Get Working Sta...		admin	10.16.1.107
3	2015-05-25 19:12:12	Operation	Remote: Get Working Sta...		admin	10.16.1.107
4	2015-05-25 19:12:12	Operation	Remote: Get Working Sta...		admin	10.16.1.107
5	2015-05-25 19:12:11	Operation	Remote: Get Working Sta...		admin	10.16.1.107
6	2015-05-25 19:12:11	Operation	Remote: Get Working Sta...		admin	10.16.1.107
7	2015-05-25 19:12:11	Operation	Remote: Get Working Sta...		admin	10.16.1.107
8	2015-05-25 19:12:10	Operation	Remote: Get Working Sta...		admin	10.16.1.107
9	2015-05-25 19:09:28	Operation	Remote: Get Parameters		admin	10.16.1.107
10	2015-05-25 19:09:25	Operation	Remote: Get Parameters		admin	10.16.1.107
11	2015-05-25 19:09:25	Operation	Remote: Get Parameters		admin	10.16.1.107
12	2015-05-25 19:09:24	Operation	Remote: Get Parameters		admin	10.16.1.107

Total 614 Items


Figure 44, Log Searching

4. To export the log files, click **Export** to save the log files.

6.3.3. System Service

Purpose

System service settings refer to the hardware service the camera supports. Supported functions vary by camera. For cameras that support IR Light, ABF (Auto Back Focus), Auto Defog, or Status LED, you can select to enable or disable the corresponding service according to your actual demand.

- **ABF:** When the ABF function is enabled, you can click  on the PTZ control panel for auxiliary focus.
- **Third Stream:** For some models, third stream is not enabled by default. Check **Enable Third Stream** checkbox to enable the function.

6.4. Security Settings

Configure the parameters, including Authentication, IP Address Filter, and Security Service on the security interface.

6.4.1. Authentication

Purpose

You can specifically secure the live view stream data.

1. Enter the Authentication interface, **Configuration > System > Security > Authentication**.

Authentication	IP Address Filter	Security Service
RTSP Authentication	digest	▼
WEB Authentication	digest	▼

Figure 45, Authentication

2. Set up authentication method for RTSP authentication and WEB authentication.

CAUTION: **Digest** is the recommended authentication method for better data security. You must be aware of the risk if you adopt **Basic** as the authentication method.

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

6.4.2. IP Address Filter

Purpose

This function makes access control possible.

1. Enter the IP Address Filter interface: **Configuration > System > Security > IP Address Filter**.

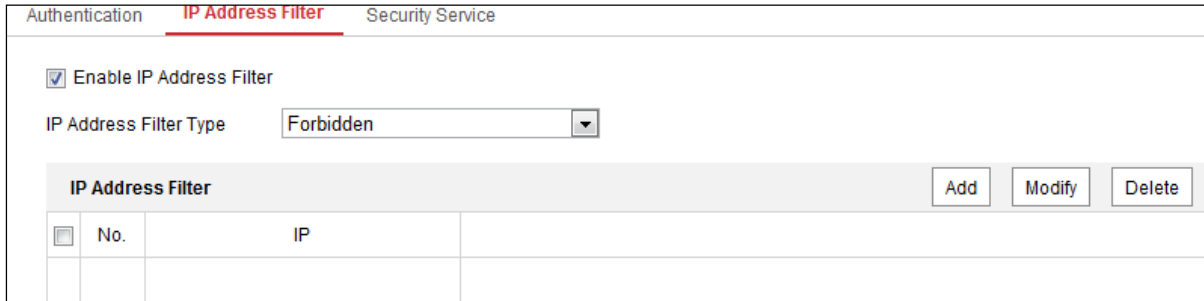


Figure 46, IP Address Filter Interface

2. Check the **Enable IP Address Filter** checkbox.
3. Select the type of IP Address Filter in the drop-down list, **Forbidden** and **Allowed** are selectable.
4. Set the IP Address Filter list.
 - **Add an IP Address**
 - 1) Click **Add** to add an IP address.
 - 2) Input the IP Address.



Figure 47, Add an IP

- 3) Click **OK** to finish adding.
- **Modify an IP Address**
 - 1) Left-click an IP address from filter list and click **Modify**.
 - 2) Modify the IP address in the text field.



Figure 48, Modify an IP

- 3) Click the **OK** to finish modifying.

- Delete one or more IP addresses

- 1) Select the IP address(es) and click **Delete**.
- 2) Click **Save** to save the settings.

6.4.3. Security Service

To enable remote login and improve data communication security, the camera provides security service for better user experience.

1. Enter the security service configuration interface: **Configuration > System > Security > Security Service**.

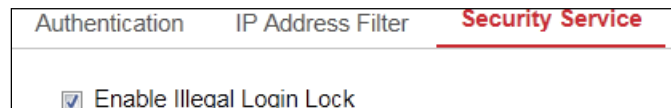


Figure 49, Security Service

2. Check the **Enable Illegal Login Lock** checkbox.

NOTE: **Illegal Login Lock** limits user login attempts. Login attempt from the IP address is rejected if the admin user performs seven failed user name/password attempts (five times for operator/user).

If the IP address is rejected, you can again try to log in to the device after 30 minutes.

6.5. User Management Interface

6.5.1. User Management

- **As Administrator:** The admin user can add, delete, or modify user accounts and grant permissions. We recommend that you manage the user accounts and permissions carefully.

Enter the User Management interface, **Configuration > System > User Management**.

NOTE: Admin password is required for adding and modifying a user account.

User List		Security Question	Add	Modify	Delete
No.	User Name	Level			
1	admin	Administrator			
2	test 01	Operator			

Figure 50, User Management Interface

- **Adding a User:** The **admin** user has all permissions by default and can create/modify/delete other accounts. The **admin** user cannot be deleted, and you can change only the *admin* password.

1. Click **Add** to add a user.

2. Input the **Admin Password**, **User Name**, select **Level**, and input **Password**.

NOTES: Up to 31 user accounts can be created.

Users of different levels have different default permissions. Operator and user are selectable.



STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

3. You can check or uncheck the permissions for the new user.
4. Click **OK** to finish adding the user.

- **Modifying a User**

1. Left-click to select the user from the list, and click **Modify**.
2. Modify the **User Name**, **Level**, and **Password**.



STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

3. Check or uncheck the permissions.
4. Click **OK** to finish the user modification.

- **Deleting a User**

1. Click to select the user you want to delete, and click **Delete**.
2. Click **OK** on the pop-up dialogue box to confirm the deletion.

- **As Operator or User:** Operator or user can modify passwords. Old password is required for this action.

6.5.2. Security Question

Purpose

Security question is used to reset the admin password when the admin user forgets the password.

6.5.2.1. Set Security Question

You can set the security questions during camera activation, or you can set the function in the **User Management** interface.

Security question setting is not cleared when you restore the camera (not to default).

1. Enter setting interface, **Configuration > System > User Management > User Management**.
2. Click **Security Question**.
3. Input correct admin password.
4. Select questions and input answers.
5. Click **OK** to save the settings.

6.5.2.2. Reset Admin Password

Before You Start

The PC used to reset the password and the camera should be in the same IP address segment and LAN.

- Enter login interface via a Web browser.
- Click **Forget Password**.
- Answer security question.
- Create new password.

NOTE: User IP address locks for 30 minutes after seven failed attempts to answer the security questions.

6.5.3. Online Users

Purpose

You can see the current users who are visiting the device through this interface. User information such as user name, level, IP address, and operation time, is displayed in the User List.

1. Click **Refresh** to refresh the list.

User Management		Online Users		
User List				Refresh
No.	User Name	Level	IP Address	User Operation Time
1	admin	Administrator	10.16.2.101	2015-11-16 10:57:55

Figure 51, View the Online Users

Follow the instructions in this chapter to configure the basic settings and advanced settings.

Chapter 7. Network Settings Configuring Basic Settings

Purpose

You can configure network parameters, including TCP/IP, DDNS, PPPoE, Port, and NAT, etc., by following the instructions in this section.

7.1. Configuring TCP/IP Settings

Purpose

TCP/IP settings must be properly configured before operating the camera over a network. The camera supports both IPv4 and IPv6. Both versions can be configured simultaneously without conflicting with each other, and at least one IP version must be configured.

1. Enter the TCP/IP Settings interface, **Configuration > Network > Basic Settings > TCP/IP**.

The screenshot shows the TCP/IP configuration page. At the top, there are tabs for 'TCP/IP', 'DDNS', 'PPPoE', 'Port', and 'NAT'. The 'TCP/IP' tab is selected. The main area contains several configuration items:

- NIC Type:** A dropdown menu set to 'Auto'.
- DHCP:** An unchecked checkbox.
- IPv4 Address:** A text input field containing '10.11.37.120' with a 'Test' button to its right.
- IPv4 Subnet Mask:** A text input field containing '255.255.255.0'.
- IPv4 Default Gateway:** A text input field containing '10.11.37.254'.
- IPv6 Mode:** A dropdown menu set to 'Route Advertisement' with a 'View Route Advertisement' button to its right.
- IPv6 Address:** A text input field containing '::'.
- IPv6 Subnet Mask:** A text input field containing '0'.
- IPv6 Default Gateway:** A text input field containing '::'.
- Mac Address:** A text input field containing 'c0:56:e3:60:27:5d'.
- MTU:** A text input field containing '1500'.
- Multicast Address:** An empty text input field.
- Enable Multicast Discovery:** A checked checkbox.

Below these fields is a grey-shaded section titled 'DNS Server' containing:

- Preferred DNS Server:** A text input field containing '8.8.8.8'.
- Alternate DNS Server:** An empty text input field.

At the bottom of the page is a red button with a floppy disk icon and the text 'Save'.

Figure 52, TCP/IP Settings

2. Configure the basic network settings, including NIC Type, IPv4 or IPv6 Address, IPv4 or IPv6 Subnet Mask, IPv4 or IPv6 Default Gateway, MTU settings, and Multicast Address.
3. (Optional) Check the **Enable Multicast Discovery** checkbox, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.
4. Configure the DNS server. Input the preferred DNS server and alternate DNS server.

5. Click **Save** to save the above settings.

NOTES: The valid MTU value range is 1280 to 1500.

The Multicast sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Before using this function, enable the Multicast function of your router.

A reboot is required for the settings to take effect.

7.1.1. Configuring DDNS Settings

Purpose

If your camera is set to use PPPoE as its default network connection, you can use Dynamic DNS (DDNS) for network access.

Before You Start

Registration on the DDNS server is required before configuring the camera's DDNS settings.

1. Enter the DDNS Settings interface, **Configuration > Network > Basic Settings > DDNS**.
2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Two DDNS types are selectable: DynDNS and NO-IP.
 - **DynDNS**
 - (1) Enter DynDNS **Server Address** (e.g. members.dyndns.org).
 - (2) In the **Domain** text field, enter the domain name obtained from the DynDNS Website.
 - (3) Enter the **User Name** and **Password** registered on the DynDNS Website.
 - (4) Click **Save** to save the settings.

The screenshot shows the DDNS configuration page with the following fields and values:

Field	Value	Status
Enable DDNS	<input checked="" type="checkbox"/>	
DDNS Type	DynDNS	
Server Address	members.dyndns.org	✓
Domain	123.dyndns.com	✓
User Name	test	✓
Port	0	
Password	••••••••	✓
Confirm	••••••••	✓

A red **Save** button is located at the bottom of the form.

Figure 53, DynDNS Settings

- **NO-IP**

(1) Choose the DDNS Type as **NO-IP**.

The screenshot shows the DDNS configuration page with the following fields and values:

Field	Value
Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	NO-IP
Server Address	www.noip.com
Domain	
User Name	
Port	0
Password	
Confirm	

A red 'Save' button is located at the bottom of the form.

Figure 54, NO-IP DNS Settings

(2) Enter the Server Address as www.noip.com

(3) Enter the Domain name you registered.

(4) Enter the User Name and Password.

(5) Click **Save**, and then you can view the camera by using the domain name.

NOTE: Reboot the device to have the settings take effect.

7.1.2. Configuring PPPoE Settings

1. Enter the PPPoE Settings interface, **Configuration > Network > Basic Settings > PPPoE**.

The screenshot shows the PPPoE configuration page with the following fields and values:

Field	Value
Enable PPPoE	<input checked="" type="checkbox"/>
Dynamic IP	0.0.0.0
User Name	
Password	
Confirm	

A red 'Save' button is located at the bottom of the form.

Figure 55, PPPoE Settings

2. Check the **Enable PPPoE** checkbox to enable this feature.

3. Enter **User Name**, **Password**, and **Confirm** password for PPPoE access.

NOTE: The User Name and Password should be assigned by your ISP.



STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

4. Click **Save** to save and exit the interface.

NOTE: A reboot is required for the settings to take effect.

7.1.3. Configuring Port Settings

Purpose

You can set the port no. of the camera, e.g., HTTP port, RTSP port, and HTTPS port.

1. Enter the Port Settings interface, **Configuration > Network > Basic Settings > Port**.

TCP/IP	DDNS	PPPoE	Port	NAT
			HTTP Port	<input type="text" value="80"/>
			RTSP Port	<input type="text" value="554"/>
			HTTPS Port	<input type="text" value="443"/>
			Server Port	<input type="text" value="8000"/>
			WebSocket Port	<input type="text" value="7681"/>
			WebSockets Port	<input type="text" value="7682"/>

Figure 56, Port Settings

2. Set the camera ports.

- **HTTP Port:** The default port number is 80, and it can be changed to any unoccupied port no.
- **RTSP Port:** The default port number is 554, and it can be changed to any port no. from 1 to 65535.
- **HTTPS Port:** The default port number is 443, and it can be changed to any unoccupied port no.
- **Server Port:** The default server port number is 8000, and it can be changed to any port no. from 2000 to 65535.

NOTE: If you use client software to visit the camera and you changed the server port number, you have to input the correct server port number in the login interface to access the camera.

- **WebSocket Port:** The default port no. is 7681. It can be changed to any port no. from 1 to 65535.

- **WebSockets Port:** The default server port no. is 7682. It can be changed to any port no. from 1 to 65535.

NOTE: WebSocket and WebSockets protocol are used for plug-in free live view. For detailed information, see *Section 7.2.11.1 WebSocket and WebSockets*.

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

NOTE: A reboot is required for the settings to take effect.

7.1.4. Configure NAT (Network Address Translation) Settings

Purpose

The NAT interface allows you to configure the UPnP™ parameters.

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software, and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

With the function enabled, you don't need to configure port mapping for each port, and the camera is connected to the Wide Area Network via the router.

Enable UPnP™				
Friendly Name	TestCam <input type="checkbox"/>			
Port Mapping Mode	Auto <input type="button" value="v"/>			
Port Type	External Port	External IP Address	Internal Port	Status
HTTP	80	0.0.0.0	80	Not Valid
RTSP	554	0.0.0.0	554	Not Valid
Server Port	8000	0.0.0.0	8000	Not Valid
WEBSOCKET	7681	0.0.0.0	7681	Not Valid
WEBSOCKETS	7682	0.0.0.0	7682	Not Valid

Figure 57, UPnP Settings

1. Enter the NAT settings interface, **Configuration > Network > Basic Settings > NAT**.

2. Check the checkbox to enable the UPnP™ function.

NOTE: Only when the UPnP™ function is enabled are the camera ports active.

3. Choose a friendly name for the camera, or you can use the default name.

4. Select the port mapping mode. **Manual** and **Auto** are selectable.

NOTE: If you select **Auto**, you enable the UPnP™ function on the router.

If you select **Manual**, you can customize the value of the external port and complete port mapping settings on the router manually.

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

7.2. Configure Advanced Settings

Purpose

You can configure the parameters, including SNMP, FTP, Email, HTTPS, QoS, 802.1x, etc., by following the instructions in this section.

7.2.1. Configuring SNMP Settings

Purpose

You can set the SNMP function to get camera status, parameters, and alarm related information, and manage the camera remotely when it is connected to the network.

Before You Start

Before setting the SNMP, download the SNMP software and manage to receive the camera information via the SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance center.

NOTE: The SNMP version you select should be the same as that of the SNMP software. You also need to use a version according to the security level you require. SNMP v1 provides no security and SNMP v2 requires a password for access. SNMP v3 provides encryption, and if you use the third version, HTTPS protocol must be enabled.



STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

1. Enter the SNMP Settings interface, **Configuration > Network > Advanced Settings > SNMP**.


SNMP	FTP	Email	HTTPS	QoS	802.1x
SNMP v1/v2					
<input type="checkbox"/>	Enable SNMPv1				
<input type="checkbox"/>	Enable SNMP v2c				
Read SNMP Community	<input type="text" value="public"/>				
Write SNMP Community	<input type="text" value="private"/>				
Trap Address	<input type="text"/>				
Trap Port	<input type="text" value="162"/>				
Trap Community	<input type="text" value="public"/>				
SNMP v3					
<input checked="" type="checkbox"/>	Enable SNMPv3				
Read UserName	<input type="text"/>				
Security Level	no auth, no priv ▼				
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA				
Authentication Password	<input type="text" value="....."/>				
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES				
Private-key password	<input type="text" value="....."/>				
Write UserName	<input type="text"/>				
Security Level	no auth, no priv ▼				
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA				
Authentication Password	<input type="text" value="....."/>				
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES				
Private-key password	<input type="text" value="....."/>				
SNMP Other Settings					
SNMP Port	<input type="text" value="161"/>				
					

Figure 58, SNMP Settings

2. Check the **Enable SNMPv1**, **Enable SNMP v2c**, **Enable SNMPv3** checkbox to enable the feature correspondingly.
3. Configure the SNMP settings.

NOTE: The settings of the SNMP software should be the same as the settings you configure here.

4. Click **Save** to save and finish the settings.

NOTES: A reboot is required for the settings to take effect.

To lower the risk of information leakage, enable SNMP v3 instead of SNMP v1 or v2.

7.2.2. Configuring FTP Settings

Purpose

You can configure the FTP server related information to enable the uploading of the captured pictures to the FTP server. The captured pictures can be triggered by events or a timing snapshot task.

1. Enter the FTP Settings interface, **Configuration > Network > Advanced Settings > FTP**.

The screenshot shows the 'FTP' configuration page with the following fields and values:

- Server Address: 0.0.0.0
- Port: 21
- User Name: (empty)
- Password: (empty)
- Confirm: (empty)
- Directory Structure: Save in the root directory
- Picture Filing Interval: 7 Day(s)
- Picture Name: Default
- Upload Picture
- Test button
- Save button (red)

Figure 59, FTP Settings

2. Input the FTP address and port.
3. Configure the FTP settings; and the user name and password are required for the FTP server login.



STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

4. Set the directory structure and picture filing interval.
 - **Directory:** In the **Directory Structure** field, you can select the root directory, parent directory, and child directory. If the parent directory is selected, you have the option to use the **Device Name**,

Device Number, or **Device IP** for the name of the directory, and if the child directory is selected, you can use the Camera Name or Camera No. as the name of the directory.

- **Picture Filing Interval:** For better picture management, you can set the picture filing interval from 1 day to 30 days. Pictures captured in the same time interval will be saved in one folder named after the beginning date and ending date of the time interval.
- **Picture Name:** Set the naming rule for captured picture files. You can choose **Default** in the drop-down list to use the default rule, that is, *IP address_channel number_capture time_event type.jpg* (e.g., *10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg*), or you can customize it by adding a **Custom Prefix** to the default naming rule.

5. Check the **Upload Picture** checkbox to enable the function.

- **Upload Picture:** To upload captured pictures to the FTP server.
- **Anonymous Access to the FTP Server** (in which case user name and password won't be required): Check the Anonymous checkbox to enable anonymous access to the FTP server.

NOTE: The anonymous access function must be supported by the FTP server.

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

7.2.3. Configuring E-Mail Settings

Purpose

The system can be configured to send an e-mail notification to all designated receivers if an alarm event is detected, e.g., motion detection event, video loss, video tampering, etc.

Before You Start

Configure the DNS Server settings under **Configuration > Network > Basic Settings > TCP/IP** before using the e-mail function.

1. Enter the TCP/IP Settings, **Configuration > Network > Basic Settings > TCP/IP**, to set the **IPv4 Address**, **IPv4 Subnet Mask**, **IPv4 Default Gateway**, and the **Preferred DNS Server**.

NOTE: Refer to *Section 7.1, Configuring TCP/IP Settings* for detailed information.

2. Enter the **Email Settings** interface, **Configuration > Network > Advanced Settings > Email**.

3. Configure the following settings:

- **Sender:** The name of the e-mail sender.
- **Sender's Address:** The e-mail address of the sender.
- **SMTP Server:** IP address or host name (e.g., smtp.263xmail.com) of the SMTP Server.
- **SMTP Port:** The SMTP port. The default TCP/IP port for SMTP is 25 (not secured), and the SSL SMTP port is 465.

- **Email Encryption: None, SSL, and TLS** are selectable. If you select **SSL** or **TLS** and disable **STARTTLS**, e-mails will be sent after being encrypted by **SSL** or **TLS**.

The SMTP port should be set to 465 for this encryption method. When you select **SSL** or **TLS** and enable **STARTTLS**, e-mails will be sent after being encrypted by **STARTTLS**, and the **SMTP port** should be set to 25.

NOTE: To use **STARTTLS**, make sure that the protocol is supported by your e-mail server. If you check the **Enable STARTTLS** checkbox when the protocol is not supported by your e-mail sever, your e-mail will not be encrypted.

- **Attached Image:** Check the **Attached Image** checkbox if you want to send e-mails with attached alarm images.
- **Interval:** The interval refers to the time between two actions of sending attached pictures.
- **Authentication (Optional):** If your e-mail server requires authentication, check this checkbox to use authentication to log in to this server and input the login user name and password.



STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

- **Receiver Table:** Select the receiver to which the e-mail is sent. Up to three receivers can be configured.
 - **Receiver:** The name of the user to be notified.
 - **Receiver's Address:** The e-mail address of user to be notified.

SNMP FTP **Email** HTTPS QoS 802.1x

Sender: test ✓

Sender's Address: test@gmail.com ✓

SMTP Server: []

SMTP Port: 25

E-mail Encryption: None

Attached Image

Interval: 2 s

Authentication

User Name: []

Password: []

Confirm: []

Receiver			
No.	Receiver	Receiver's Address	Test
1			Test
2			
3			

Save

Figure 60, E-Mail Settings

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

7.2.4. Platform Access

Purpose

Platform access provides you with an option to manage the devices via platform.

1. Enter the **Platform Access** settings interface, **Configuration > Network > Advanced Settings > Platform Access**.
2. Check the **Enable** checkbox to enable the device's platform access function.
3. Select the **Platform Access Mode**.

NOTE: Hik-Connect is an application for mobile devices. With the app, you can view live image of the camera, receive alarm notification, etc.

To set **Platform Access Mode** to **Hik-Connect**:

- 1) Click and read "Terms of Service" and "Privacy Policy" in the pop-up window.
- 2) Create a verification code or change the verification code for the camera.

NOTE: The verification code is required when you add the camera to the Hik-Connect app.

For more information about the Hik-Connect app, see Hik-Connect Mobile Client User Manual.

4. You can use the default server address, or you can check the **Custom** checkbox on the right, and input a desired server address.
5. Click **Save** to save the settings.

7.2.5. Wireless Dial

Purpose

Data stream of audio, video, and image can be transferred via a 3G/4G wireless network.

NOTES: The wireless dial function may not be supported by some camera models.

Cameras that support wireless dial do not support PPPoE.

1. Click the **Wireless Dial** tab to enter the **Wireless Dial Configuration** interface, **Configuration > Network > Advanced Settings > Wireless Dial**.
2. Check the checkbox to enable the wireless dial settings.
3. Configure the dial parameters.
 - 1) Select the dial mode from the drop-down list. **Auto** and **Manual** are selectable. If **Auto** is selected, you can set the arming schedule for dialing; If **Manual** is selected, you can set the offline time and manual dialing parameters.
 - 2) Set the **access number, user name, password, APN, MTU, and verification protocol**. You can also leave these parameters blank, and the device will use the default settings for dialing after other parameters are configured.
 - 3) Select the network mode from the drop-down list. **Auto, 3G, and 4G** are selectable. If **Auto** is selected, the network selection priority comes as: **4G > 3G > Wired Network**.
 - 4) Input the offline time if **Manual** is selected as the dial mode.
 - 5) Input the **UIM Number** (Mobile Phone Number).
 - 6) Click the **Edit** button to set the arming schedule if **Auto** is selected as the dial mode.
 - 7) Click **Save** to save the settings.
4. View the dial status.
 - 1) Click the **Refresh** button to view the dial status including **real-time mode, UIM status, signal strength**, etc.
 - 2) If **Manual** is selected as the dial mode, you can also manually connect/disconnect the wireless network.
5. Set the white list. A mobile phone number on the white list can receive an alarm message from the device and reboot the device via SMS.
 - Check the **Enable SMS Alarm** checkbox.

- Select the item on the white list, and click the **Edit** button.
- Input the mobile phone number for the white list, check the **Reboot via SMS** checkbox, select the alarm for SMS push, and click **OK**.

NOTE: To reboot the device via SMS, send the message "reboot" to the device, and the device will reply with the message, "reboot success" after rebooting succeeds.

- (Optional) Click **Send Test SMS** to send a message to the mobile phone as a test.
- Click **Save** to save the settings.

7.2.6. HTTPS Settings

Purpose

HTTPS authenticates a Web site and its Web server, which protects against Man-in-the-Middle attacks.

NOTE: For cameras that support plug-in free live view, if you use HTTPS to visit the camera, enable **Websockets** for live view. Go to **Configuration > Network > Advanced Settings > Network Service**.

If HTTPS is enabled by default, the camera creates an unsigned certificate automatically. When you visit the camera via HTTPS, the Web browser will send a notification about the certificate issue. Install a signed-certificate to the camera to cancel the notification.

1. Enter the HTTPS settings interface, **Configuration > Network > Advanced Settings > HTTPS**.
2. Check **Enable** to access the camera via HTTP or HTTPS protocol.
3. Check **Enable HTTPS Browsing** to access the camera only via HTTPS protocol.



Figure 61, HTTPS Configuration Interface

4. Create the self-signed certificate or authorized certificate.

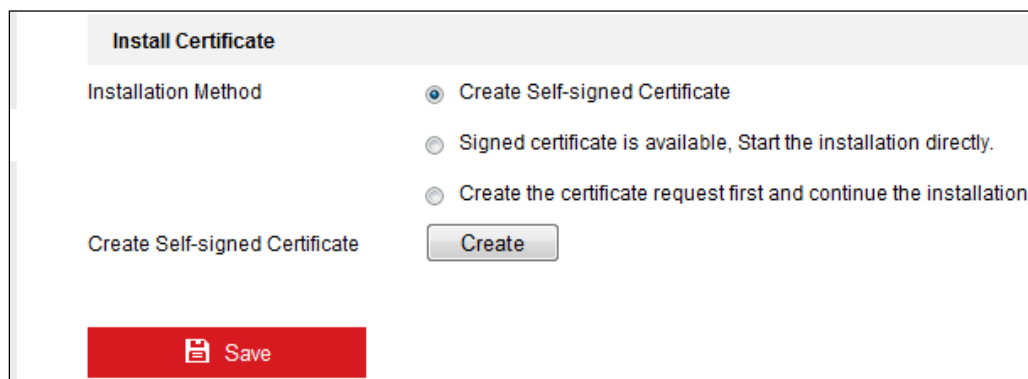
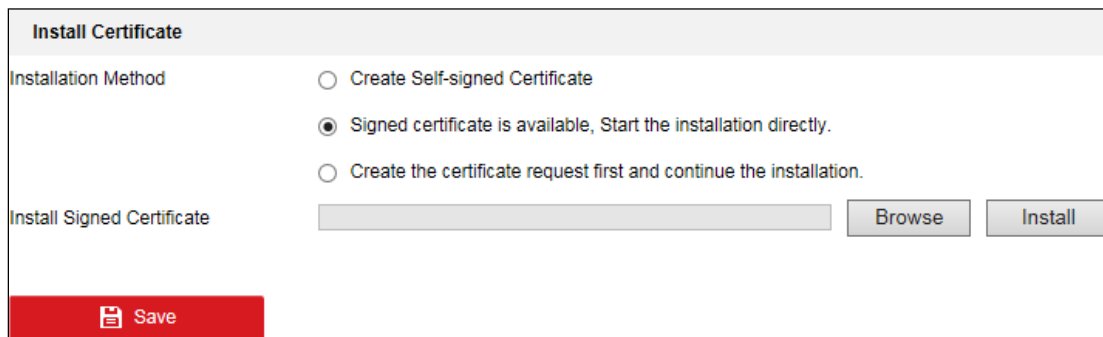


Figure 62, Create Self-Signed Certificate

- Create the self-signed certificate.
 1. Select **Create Self-signed Certificate** as the **Installation Method**.
 2. Click the **Create** button to enter the creation interface.
 3. Enter the country, host name/IP, validity, and other information.
 4. Click **OK** to save the settings.

NOTE: If you already had a certificate installed, the Create Self-signed Certificate is grayed out.

- Create the request and import the authorized certificate.
 1. Select **Create the certificate request first and continue the installation** as the **Installation Method**.
 2. Click the **Create** button to create the certificate request. Fill in the required information in the pop-up window.
 3. Click **Download** to download the certificate request, and submit it to the trusted certificate authority for signature.
 4. After receiving the signed valid certificate, you can import the certificate in two ways:
 - a. Select **Signed certificate is available, Start the installation directly**. Click **Browse** and **Install** to import the certificate to the device.



The screenshot shows a dialog box titled "Install Certificate". Under "Installation Method", the second option, "Signed certificate is available, Start the installation directly.", is selected with a radio button. Below this, there is a text input field labeled "Install Signed Certificate" followed by "Browse" and "Install" buttons. At the bottom left, there is a red "Save" button with a floppy disk icon.

Figure 63, Import the Certificate (1)

- b. Select **Create the certificate request first and continue the installation**. Click **Browse** and **Install** to import the certificate to the device.

Figure 64, Import the Certificate (2)

- There will be the certificate information after successfully creating and installing the certificate.

Figure 65, Installed Certificate

- Export and save the certificate for verification when adding the device to client software.

NOTE: The exported certificate should be saved in the certificate folder of your client software before adding the device to your PC client.

- Click the **Save** button to save the settings.

7.2.7. Configuring QoS Settings

Purpose

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

- Enter the QoS Settings interface, **Configuration > Network > Advanced Settings > QoS**.

Figure 66, QoS Settings

2. **Configure** the QoS settings, including **Video/Audio DSCP**, **Event/Alarm DSCP**, and **Management DSCP**.

The valid value range of the DSCP is 0 to 63. The bigger the DSCP value is, the higher the priority is.

NOTE: DSCP refers to the Differentiated Service Code Point; and the DSCP value is used in the IP header to indicate the priority of the data.

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

NOTE: A reboot is required for the settings to take effect.

7.2.8. Configuring 802.1x Settings

Purpose

The IEEE 802.1x standard is supported by the network cameras, and when the feature is enabled, the camera data is secured and user authentication is needed when connecting the camera to the network protected by IEEE 802.1x.

Before You Start

The authentication server must be configured. Please apply and register a user name and password for 802.1x in the server.



STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

1. Enter the **802.1X Settings** interface, **Configuration > Network > Advanced Settings > 802.1x**.

Figure 67, 802.1x Settings

2. Check the **Enable IEEE 802.1X** checkbox to enable the feature.

3. Configure the 802.1x settings, including **Protocol**, **EAPOL version**, **User Name**, **Password**, and **Confirm**.

NOTE: The **EAPOL version** must be identical with that of the router or the switch.

4. Enter the user name and password to access the server.
5. Click **Save** to finish the settings.

NOTE: A reboot is required for the settings to take effect.

7.2.9. Integration Protocol

Purpose

If you need to access the camera through a third party platform, you can enable the **CGI** function. And if you need to access to the device through **ONVIF protocol**, you can configure the ONVIF user in this interface. Refer to ONVIF standard for detailed configuration rules.

7.2.9.1. CGI

Check the **Enable Hikvision_CGI** checkbox, then select the authentication method from the drop-down list.

NOTE: Digest is the recommended authentication method.

7.2.9.2. ONVIF

1. Check the **Enable ONVIF** checkbox to enable the function.
2. Add ONVIF users. Up to 32 users are allowed.

Set the user name and password, and confirm the password. You can set the user as **media user**, **operator**, and **administrator**.

NOTE: The ONVIF user account is different from the camera user account. You have to set the ONVIF user account independently.

3. Save the settings.

NOTE: ONVIF user settings are cleared when you restore the camera.

7.2.10. Bandwidth Adaptation

When you enable the function, live view fluency is taken as the priority of camera performance. The camera adjusts video-related parameters automatically, and the pre-set video-related configuration is invalid. A reboot is required for the function to take effect.

NOTE: Bandwidth adaptation is available only for certain camera models.

7.2.11. Network Service

You can control the ON/OFF status of certain protocols that the camera supports.

NOTE: Keep unused functions OFF for security concerns.

Supported functions vary by camera model.

7.2.11.1. WebSocket and WebSockets

WebSocket or **WebSockets** protocol should be enabled if you use Google Chrome 45 and above version or Mozilla Firefox 52 and above version to visit your camera. Otherwise, live view, image capture, and digital zoom function cannot be used.

- If the camera uses HTTP, enable **WebSocket**
- If the camera uses HTTPS, enable **WebSockets**

7.2.11.2. SDK Service and Enhanced SDK Service

To add the device to the client software, enable SDK Service or Enhanced SDK Service.

- **SDK Service:** SDK protocol is used.
- **Enhanced SDK Service:** SDK over TLS protocol is used. Communication between the device and the client software is secured by using TLS (Transport Layer Security) protocol.
- **TLS (Transport Layer Security):** The device offers TLS 1.1 and TLS 1.2. Enable one or more protocol versions according to your need.

7.2.12. Smooth Streaming

Purpose

If the network is unstable or high quality of video is required, you can enable the Smooth Streaming function to view the live view smoothly via the client software or a Web Browser.

Before You Start

Add the device to your client software and select **NPQ** protocol in the client software before configuring the smooth streaming function.

1. Enter the **Smooth Streaming** interface, **Configuration > Network > Advanced Settings > Smooth Streaming**.

Figure 68, Smooth Streaming Settings

2. Select the **Stream Type**.
3. Check **Enable Smooth Streaming**.

NOTE: Be sure the **Bitrate Type** is selected as **Constant** and the **SVC** is set to **OFF** before enabling this function. Go to **Configuration > Video/Audio > Video** page to set the parameters.

4. Select the smooth streaming mode. There are three modes selectable: **Auto**, **Resolution Priority**, and **Error Correction**.

- **Auto:** The resolution and bitrate will be adjusted automatically and resolution will take priority. The upper limits of these two parameters will not exceed the values you set on the Video page. Go to the **Configuration > Video/Audio > Video** page, set the **Resolution** and **Max. Bitrate** before you enable the smooth streaming function. In this mode, the framerate will be adjusted to **Max.** value automatically.
- **Resolution Priority:** The resolution stays the same as the set value in the **Video** page, and the bitrate will be adjusted automatically. Go to the **Configuration > Video/Audio > Video** page, set the **Max. Bitrate** before you enable the smooth streaming function. In this mode, the framerate will be adjusted to **Max.** value automatically.
- **Error Correction:** The resolution and bitrate stay the same as the set values in the **Video** page. When the bandwidth is sufficient, there is packet loss or bit error during transmission and these situations will lead to video data error or loss. This mode is used to correct the data error during transmission to ensure image quality. You can configure the error correction proportion from 0–100. If the proportion is 0, the data error will be corrected by data retransmission. If the proportion is higher than 0, the error data will be corrected via redundant data that is added to the stream and data retransmission. The higher the value, the more redundant data will be generated, the more the data error will be corrected, and the larger the bandwidth is required. When the proportion is 100, the redundant data will be as large as the original data, and twice the bandwidth is required.

NOTE: Be sure the bandwidth is sufficient in **Error Correction** mode.

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

Chapter 8. Video/Audio Settings

Purpose

Follow the instructions to configure the **video setting**, **audio settings**, **ROI**, **Display info. on Stream**, etc.

8.1. Configuring Video Settings

For certain camera models, you can configure parameters for available video streams. For example, the main stream, the sub-stream, etc. You can also customize additional video streams for further needs.

- On the **Video** page, set-up available video streams.
- On the **Custom Video** page, add extra video streams

8.1.1. Video Settings

1. Enter the **Video Settings** interface, **Configuration > Video/Audio > Video**.

Video	Custom Video	Audio	ROI	Display Info. on Stream	Target Cro
Stream Type	Main Stream(Normal) ▼				
Video Type	Video Stream ▼				
Resolution	3840*2160 ▼				
Bitrate Type	Variable ▼				
Video Quality	Medium ▼				
Frame Rate	25 ▼ fps				
Max. Bitrate	16384 Kbps ✓				
Video Encoding	H.264 ▼				
H.264+	OFF ▼				
Profile	Basic Profile ▼				
I Frame Interval	25 ✓				
SVC	OFF ▼				
Smoothing	<input type="range" value="50"/> 50 [Clear<->Smooth]				

Figure 69, Video Settings

2. Select the **Stream Type**. Supported stream types are listed in the drop-down list.

NOTE: **DS-2CD2xx6G1 Series Cameras Only:** Some Smart VCA functions (line crossing detection, intrusion detection, region entrance/exit detection) are not functional when using third video stream, H.265+ video compression, or motion detection.

NOTES: For some models, the **Third Stream** is not enabled by default. Going to **System > Maintenance > System Service > Software** to enable the function is required.

The main stream is usually for recording and live view with good bandwidth, and the sub-

stream can be used for live view when the bandwidth is limited.

3. You can customize the following parameters for the selected stream type.

- **Video Type:** Set the stream type to **Video** stream, or **Video & Audio** composite stream. The audio signal will be recorded only when the **Video Type** is **Video & Audio**.
- **Resolution:** Select the resolution of the video output.
- **Bitrate Type:** Select the bitrate type to **constant** or **variable**.
- **Video Quality:** When bitrate type is set to **Variable**, six levels of video quality are selectable.
- **Frame Rate:** Set the frame rate. The frame rate describes the frequency at which the video stream is updated and 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.
- **Max. Bitrate:** Set the max. bitrate from 32 to 16384 Kbps. The higher value corresponds to higher video quality, but better bandwidth is required.

NOTE: The maximum limit of the max. bitrate value varies by camera platform. For certain cameras, the maximum limit is 8192 Kbps or 12288 Kbps.

- **Video Encoding:** The camera supports multiple video encodings types such as **H.264**, **H.265**, **MJPEG**, and **MPEG4**. Supported encoding type for different stream types may differ. **H.265** is a new encoding technology. Compared with **H.264**, it reduces the transmission bitrate under the same resolution, frame rate and image quality.

NOTE: Selectable video encoding types may vary according to different camera modes.

8.1.1.1. H.264+ and H.265+ Video Compression

NOTE: **DS-2CD2xx6G1 Series Cameras Only:** Some Smart VCA functions (line crossing detection, intrusion detection, region entrance/exit detection) are not functional when using third video stream, H.265+ video compression, or motion detection.

- **H.264+:** If you set the main stream as the stream type, and H.264 as the video encoding, you will see H.264+ available. H.264+ is an improved compression coding technology based on H.264. By enabling H.264+, users can estimate the HDD consumption by its maximum average bitrate. Compared to H.264, H.264+ reduces storage by up to 50% with the same maximum bitrate in most scenes.
- **H.265+:** If you set the main stream as the stream type, and H.265 as the video encoding, you will see H.265+ available. H.265+ is an improved compression coding technology based on H.265. By enabling H.265+, users can estimate the HDD consumption by its maximum average bitrate. Compared to H.265, H.265+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

NOTE: You need to reboot the camera if you want to turn on or turn off H.264+/H.265+. If you switch from H.264+ to H.265+ directly, and vice versa, a reboot is not required by the system.

Upgrade your video player to the latest version if live view or playback does not work properly

due to compatibility.

With H.264+/H.265+ enabled, the parameters such as profile, I frame interval, video quality, and SVC are greyed out.

With H.264+/H.265+ enabled, some functions are not supported. For those functions, corresponding interfaces will be hidden.

H.264+/H.265+ can spontaneously adjust the bitrate distribution according to the requirements of the actual scene in order to realize the set maximum average bitrate in the long term. The camera needs at least 24 hours to adapt to a fixed monitoring scene.

- **Max. Average Bitrate:** When you set a maximum bitrate, its corresponding recommended maximum average bitrate will be shown in the **Max. Average Bitrate** box. You can also set the maximum average bitrate manually from 32 Kbps to the value of the set maximum bitrate.
 - **Profile:** When you select H.264 or H.265 as video encoding, you can set the profile. Selectable profiles vary by camera model.
 - **I Frame Interval:** Set I Frame Interval from 1 to 400.
 - **SVC:** Scalable Video Coding is an extension of the H.264/AVC and H.265 standard. Select OFF/ON to disable/enable the SVC function. Select **Auto** and the device will automatically extract frames from the original video when the network bandwidth is insufficient.
 - **Smoothing:** It refers to the smoothness of the stream. The higher value the smoothing is, the better fluency the stream will be, although the video quality may not be so satisfactory. The lower value the smoothing is, the higher quality the stream will be, although it might not appear fluent.
4. Click **Save** to save the settings.

NOTE: The video parameters vary by camera model. Refer to the actual display page for camera functions.

8.1.2. Custom Video

You can set up additional video streams if required. For custom video streams, you can live view them, but cannot record or play them back.

NOTES: Custom video function requires the support of the camera.

After a camera restore action (not restore to default setting), quantity of custom video streams and their names are kept, but the related parameters are restored.

Figure 70, Custom Video Settings

1. Click **+** to add a stream.

2. Change the stream name if needed.

NOTE: Up to 32 letters and symbols (except &, <, >, ', or ") are allowed for the stream name.

3. Customize the stream parameters (resolution, frame rate, max. bitrate, video encoding). For parameter introduction, see *Section 8.1.1*.

4. (Optional) Add stream description if needed.

5. (Optional) If a custom stream is not needed, click **-** to delete it.

6. Save the settings.

8.1.3. Configuring Audio Settings

1. Enter the Audio Settings interface: **Configuration > Video/Audio > Audio**.

The screenshot shows the 'Audio' configuration panel. At the top, there are four tabs: 'Video', 'Audio' (which is highlighted with a red underline), 'ROI', and 'Display Info. on Stream'. Below the tabs, the following settings are visible:

- Channel No.:** A dropdown menu showing 'Analog Camera1'.
- Audio Encoding:** A dropdown menu showing 'G.711alaw'.
- Audio Input:** A dropdown menu showing 'MicIn'.
- Input Volume:** A horizontal slider bar with a white knob positioned at the 50 mark.
- Environmental Noise Filter:** A dropdown menu showing 'OFF'.

At the bottom of the panel is a prominent red button with a white floppy disk icon and the text 'Save'.

Figure 71, Audio Settings

2. Configure the following settings.

NOTE: Audio settings vary by camera model.

- **Audio Encoding:** G.722.1, G.711 ulaw, G.711 alaw, G.726, MP2L2, and PCM are selectable. For MP2L2, the Sampling Rate and Audio Stream Bitrate are configurable. For PCM, the Sampling Rate can be set.
- **Audio Input:** MicIn and LinIn are selectable for the connected microphone and pickup respectively.
- **Input Volume:** 0–100 adjustable.
- **Environmental Noise Filter:** Set it to OFF or ON. When the function is enabled, the noise in the environment can be filtered to some extent.

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

8.1.4. Configuring ROI Encoding

Purpose

ROI (Region of Interest) encoding helps to discriminate between the ROI and background information in video compression, which means the technology assigns more encoding resource to the region of interest, thus increasing the quality of the ROI whereas the background information is less focused.

NOTE: The ROI function varies by camera model.

Video Audio **ROI** Display Info. on Stream Target Cropping

Draw Area Clear

Stream Type

Stream Type Main Stream(Normal) ▾

Fixed Region

Enable

Region No. 1 ▾

ROI Level 3 ▾

Region Name

Dynamic Region

Enable Face Tracking

ROI Level 3 ▾

Figure 72, Region of Interest Settings

- Enter the ROI settings interface: **Configuration > Video/Audio > ROI**.
- Set the Stream Type for ROI encoding.
- Check the **Enable** checkbox under **Fixed Region** item.
- Set **Fixed Region** for ROI.
- Select the Region No. from the drop-down list.
- Check the **Enable** checkbox to enable ROI for the chosen region.

- Click **Drawing**. Click and drag the mouse on the view screen to draw a red rectangle as the ROI region. You can click **Clear** to cancel former drawing. Click **Stop Drawing** when you finish.
- Select the ROI level.
- Enter a region name for the chosen region.
- Click **Save** to save the ROI settings for the chosen fixed region.
- Repeat steps (1) to (6) to setup other fixed regions.
- Set **Dynamic Region** for ROI.
- Check the checkbox to enable **Face Tracking**.

NOTE: To enable the face tracking function, the face detection function should be supported and enabled.

- Select the ROI level.
- Click **Save** to save the settings.

NOTE: ROI level sets the image quality. The larger the value, the better the image quality.

8.1.5. Display Info. on Stream

Check the **Enable Dual-VCA** checkbox, and the object information (e.g., human, vehicle, etc.) will be marked in the video stream. Then, you can set rules on the connected rear-end device to detect events, including line crossing, intrusion, etc.



Figure 73, Display Info. on Stream

8.1.6. Configuring Target Cropping

Purpose

You can specify a target area on the live video, and the specified video area can be displayed via the third stream in certain resolution, providing more details of the target area if needed.

NOTE: The target cropping function varies by camera model.

1. Enter the **Target Cropping** settings interface.
2. Check the **Enable Target Cropping** checkbox to enable the function.

3. Set **Third Stream** as the stream type.
4. Select the cropping resolution for the target area video display. A red rectangle is displayed on the live video to mark the target area, and you can click-and-drag the rectangle to locate the target area as desired.
5. Click **Save** to save the settings.

Chapter 9. Image Settings

Follow the instructions in this chapter to configure the image parameters, including display settings, OSD settings, privacy mask, and picture overlay.

9.1. Configuring Display Settings

Purpose

Configure the image adjustment, exposure settings, day/night switch, backlight settings, white balance, image enhancement, video adjustment, and other parameters in display settings.

NOTE: The display parameters vary by camera model. Please refer to the actual interface for details.

9.1.1. Day/Night Auto-Switch

1. Enter the Display Settings interface, **Configuration > Image > Display Settings**.



Figure 74, Display Settings of Day/Night Auto-Switch

2. Set the camera image parameters.

NOTE: In order to guarantee the image quality in different illumination, there are two sets of parameters for users to configure.

9.1.1.1. Image Adjustment

- **Brightness** describes brightness of the image, which ranges from 1 to 100.
- **Contrast** describes the contrast of the image, which ranges from 1 to 100.
- **Saturation** describes the colorfulness of the image color, which ranges from 1 to 100.
- **Sharpness** describes the edge contrast of the image, which ranges from 1 to 100.

9.1.1.2. Exposure Settings

If the camera is equipped with a fixed lens, only **Manual** is selectable and the iris mode is not configurable.

If **Auto** is selected, you can set the auto iris level from 0 to 100.

Exposure Time refers to the electronic shutter speed, which ranges from 1 to 1/100,000s. Adjust it according to the actual luminance condition.

Gain can also be manually configured from 0 to 100. The bigger the value, the brighter the image, and the noise would also be amplified to a larger extent.

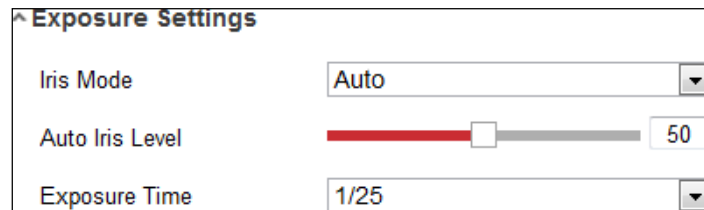


Figure 75, Exposure Settings

9.1.1.3. Focus

For cameras with a motor-driven lens, you can set the focus mode as **Auto**, **Manual**, or **Semi-auto**.

- **Auto:** Camera focus is adjusted automatically according to the actual monitoring scenario.
- **Manual:** You can control the lens by adjusting the zoom, focus, lens initialization, and auxiliary focus manually.
- **Semi-Auto:** Camera will focus automatically when you adjust the zoom parameters.

9.1.1.4. Day/Night Switch

Select the Day/Night Switch mode according to different surveillance demand. Day, Night, Auto, Scheduled-Switch, and Triggered by alarm input are selectable for day/night switch.

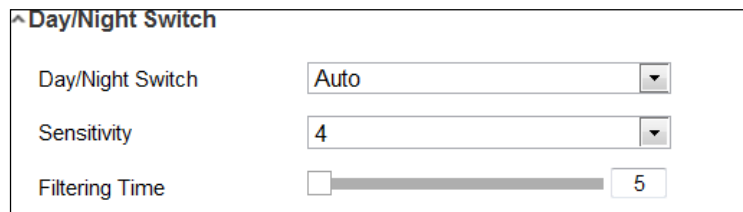


Figure 76, Day/Night Switch

- **Day:** Camera stays in day mode
- **Night:** Camera stays in night mode
- **Auto:** Camera switches between day mode and night mode according to the illumination automatically. The sensitivity ranges from 0 to 7. The higher the value, the easier the mode switches.

- **Filtering Time:** The interval time between the day/night switch. You can set it from 5s to 120s.
- **Scheduled-Switch:** Set the start time and the end time to define the duration for day/night mode.
- **Triggered by alarm input:** The switch is triggered by alarm input. You can set the triggered mode to day or night.
- **Smart Supplement Light:** Set the supplement light to ON, and **Auto** and **Manual** are selectable.
 - **Auto** – Supplement light changes according to the actual luminance. E.g., if the current scene is bright enough, then the supplement light adjusts itself to a lower power, and if the scene is not bright enough, the light adjusts itself to a higher power.
 - **Manual** – You can adjust the supplement by adjusting the distance. E.g., if the object is near the camera, the device **adjusts** the supplement light to lower power, and the light is in higher power if the object is far away.

9.1.1.5. Backlight Settings

- **BLC Area:** If you focus on an object against a strong backlight, the object will be too dark to be seen clearly. BLC compensates light to the object in the front to make it clear. **OFF, Up, Down, Left, Right, Center, Auto,** and **Custom** are selectable.

NOTE: If **BLC** mode is set as **Custom**, you can draw a red rectangle on the live view image as the **BLC** area.

- **WDR:** Wide Dynamic Range can be used when there is a high contrast between the scene's bright area and dark area.
- **HLC:** High Light Compression function can be used when there are strong lights in the scene affecting the image quality.

9.1.1.6. White Balance

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



Figure 77, White Balance

9.1.1.7. Image Enhancement

- **Digital Noise Reduction:** DNR reduces the noise in the video stream. **OFF**, **Normal**, and **Expert** are selectable. Set the **DNR** level from 0 to 100 in **Normal Mode**. Set the **DNR** level from both space **DNR** level [0–100] and time **DNR** level [0-100] in **Expert Mode**.
- **Defog Mode:** You can enable the defog function when the environment is foggy and the image is misty. It enhances subtle details so that the image appears clearer.
- **EIS (Electrical Image Stabilizer):** EIS reduces the effects of vibration in a video.
- **Grey Scale:** You can choose the range of the grey scale as [0–255] or [16–235].

9.1.1.8. Video Adjustment

- **Mirror:** It mirrors the image so you can see it inversed. Left/Right, Up/Down, Center, and OFF are selectable.
- **Rotate:** To make a complete use of the 16:9 aspect ratio, you can enable the rotate function when you use the camera in a narrow view scene.

When installing, turn the camera 90 degrees or rotate the 3-axis lens to 90 degrees, and set the rotate mode as on, you will get a normal view of the scene with 9:16 aspect ratio to ignore needless information such as the wall, and get more meaningful information of the scene.

- **Scene Mode:** Choose the scene as indoor or outdoor according to the real environment.
- **Video Standard:** 50 Hz and 60 Hz are selectable. Choose according to the different video standards, normally 50 Hz for PAL standard and 60 Hz for NTSC standard.
- **Lens Distortion Correction:** For cameras equipped with a motor-driven lens, image may appear distorted to some extent. Turn on this function to correct the distortion.
- **Others:** Some camera models support CVBS, SDI, or HDMI output. Set the local output ON or OFF according to the actual device.

9.1.2. Day/Night Scheduled-Switch

The **Day/Night scheduled-switch configuration** interface allows you to set the camera parameters for day and night separately, guaranteeing the image quality in different illumination.



Figure 78, Day/Night Scheduled-Switch Configuration Interface

1. Click the calendar icon to select the start time and the end time of the switch.

NOTES: The start time and end time refer to the valid time for day mode.

The time period can start and end on two days in a row. For example, if you set start time as 10:00 and end time as 1:00, the day mode will be activated at 10 o'clock in the morning and stopped at 1 o'clock early in the next morning.

2. Click the **Common** tab to configure the common parameters applicable to day mode and night mode.

NOTE: For the detailed information of each parameter, refer to *Section 9.1.1 Day/Night Auto-Switch*.

3. Click the **Day** tab to configure the parameters applicable for day mode.

4. Click the **Night** tab to configure the parameters applicable for night mode.

NOTE: The settings are saved automatically if any parameter is changed.

9.1.3. Configuring OSD Settings

Purpose

You can customize the camera name, time/date format, display mode, and OSD size displayed on the live view.



Figure 79, OSD Settings

1. Enter the OSD Settings interface: **Configuration > Image > OSD Settings**.
 2. Check the corresponding checkbox to select the display of **camera name**, **date**, or **week** if required.
 3. Edit the camera name in the **Camera Name** text field.
 4. Select from the drop-down list to set the time format and date format.
 5. Select from the drop-down list to set the time format, date format, display mode, OSD size, and OSD color.
 6. Configure the text overlay settings.
 - 1) Check the checkbox in front of the textbox to enable the on-screen display.
 - 2) Input the characters in the textbox.
- NOTE:** Up to eight text overlays are configurable.
7. Adjust the position and alignment of text frames.
 - Left align, right align, and custom are selectable. If you select custom, you can use the mouse to click and drag text frames in the live view window to adjust their positions.
- NOTE:** The alignment adjustment is applicable only to **Text Overlay** items.
8. Click **Save** to save the settings.

9.1.4. Configuring Privacy Mask

Purpose

Privacy mask enables you to cover certain areas on the live video to prevent certain spots in the surveillance area from being live viewed and recorded.

1. Enter the **Privacy Mask Settings** interface: **Configuration** > **Image** > **Privacy Mask**.
2. Check the **Enable Privacy Mask** checkbox to enable this function.
3. Click **Draw Area**.

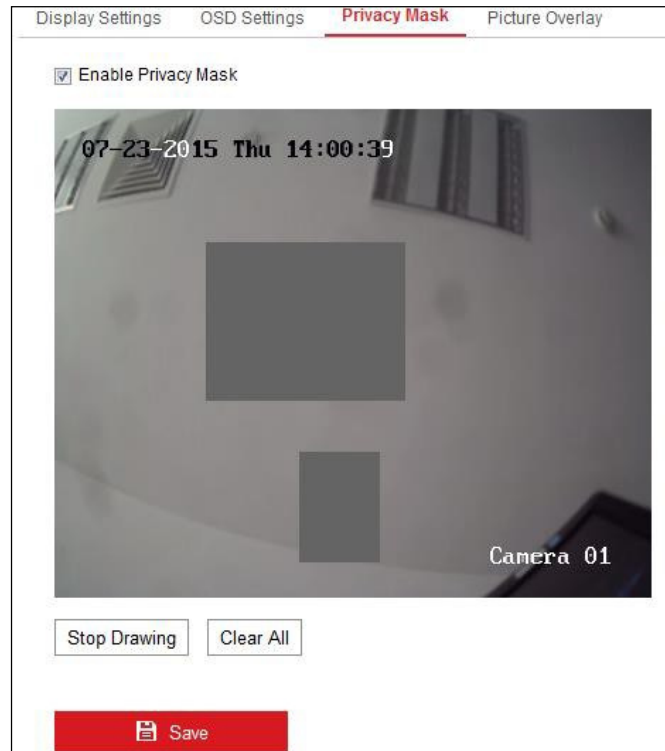


Figure 80, Privacy Mask Settings

4. Click and drag the mouse in the live video window to draw the mask area.

NOTE: You are allowed to draw up to four areas on the same image.

5. Click **Stop Drawing** to finish drawing or click **Clear All** to clear all areas you set without saving them.
6. Click **Save** to save the settings.

9.1.5. Configuring Picture Overlay

Purpose

Picture overlay allows you to overlay a picture on the image. This function enables a certain enterprise or users to overlay their logo on the image.

1. Enter the **Picture Overlay Settings** interface, **Configuration** > **Image** > **Picture Overlay**.

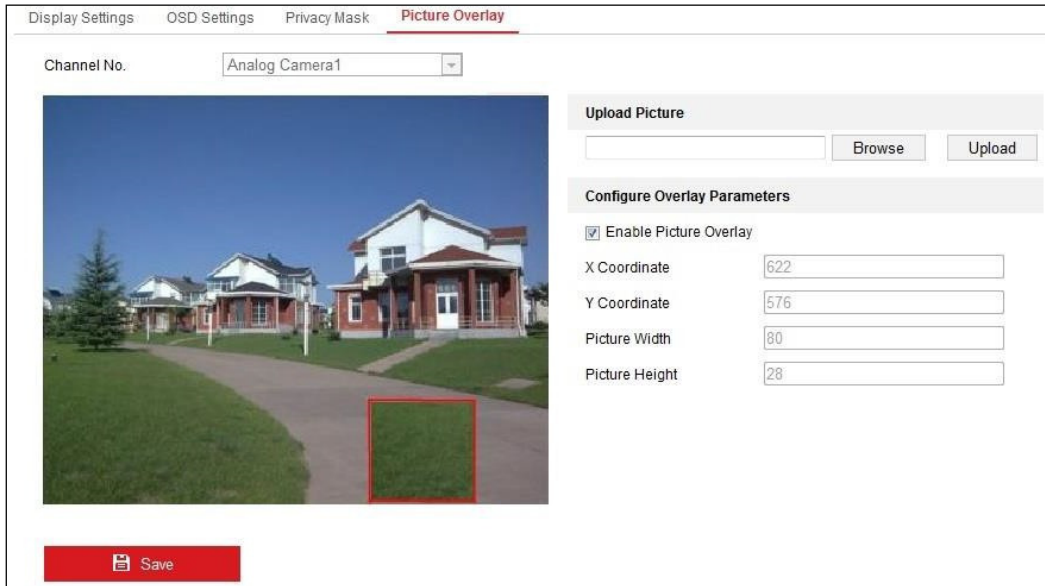


Figure 81, Picture Overlay

2. Click **Browse** to select a picture.
3. Click **Upload** to upload it.
4. Check the **Enable Picture Overlay** checkbox to enable the function.
5. Set **X Coordinate** and **Y Coordinate** values to adjust the picture position on the image. Adjust Picture Width and Picture Height to the desired size.
6. Click **Save** to save settings.

NOTE: The picture must be in RGB24 bmp format and the maximum picture size is 128*128.

Chapter 10. Event Settings

This section explains how to configure the network camera to respond to alarm events, including basic events and smart events.

10.1. Basic Events

You can configure events by following the instructions in this section, including motion detection, video tampering, alarm input, alarm output, exception, etc. These events can trigger linkage methods such as Notify Surveillance Center, Send Email, Trigger Alarm Output, etc.

NOTE: Check the **Notify Surveillance Center** checkbox if you want the alarm information to be pushed to a PC or mobile client software as soon as the alarm is triggered.

10.1.1. Configuring Motion Detection

Purpose

Motion detection detects moving objects in the configured surveillance area, and a series of actions can be taken when the alarm is triggered.

In order to detect the moving objects accurately and reduce the false alarm rate, normal configuration and expert configuration are selectable for different motion detection environments.

- **Normal Configuration**

Normal configuration adopts the same set of motion detection parameters in the day and at night.

- **Task 1: Set the Motion Detection Area Steps**

1. Enter the motion detection settings interface: **Configuration > Event > Basic Event > Motion Detection**.
2. Check the **Enable Motion Detection** checkbox.
3. Check the **Enable Dynamic Analysis for Motion** checkbox to show detected objects with green rectangles.

NOTE: Select **Disable for Rules** if you don't want the detected objects displayed with green rectangles. Select disable rules from **Configuration > Local Configuration > Live View Parameters-rules**.

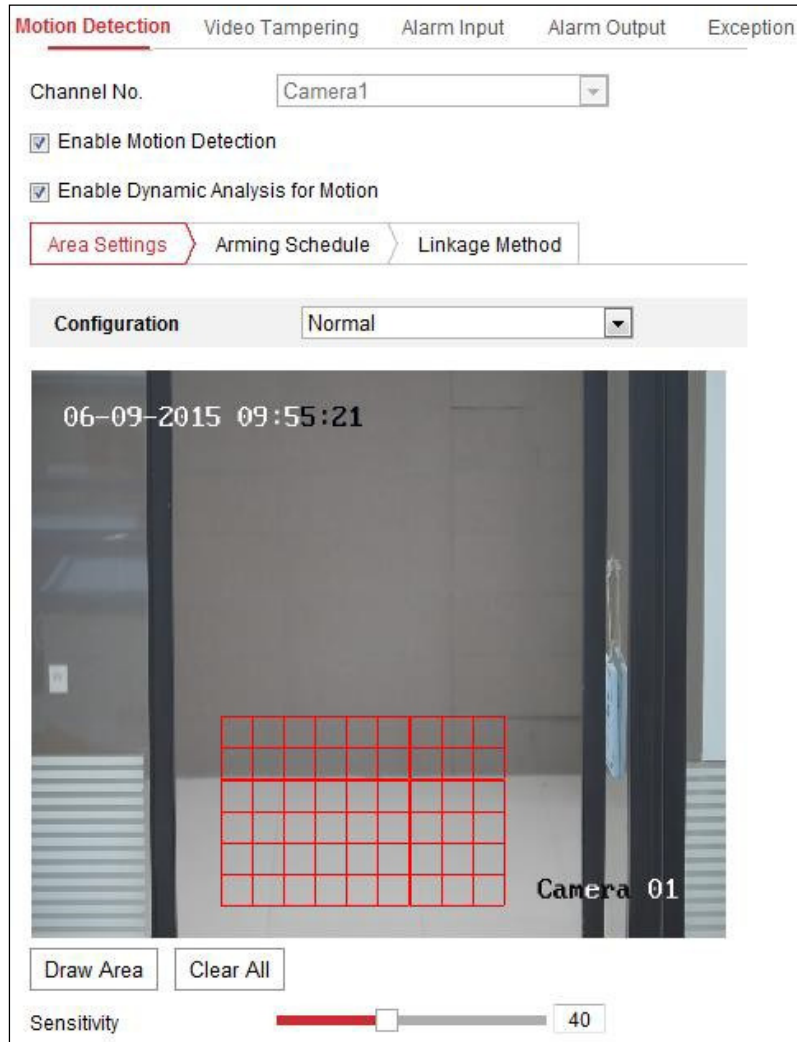


Figure 82, Enable Motion Detection

4. Click **Draw Area**. Click and drag the mouse on the live video to draw a motion detection area. Click **Stop Drawing** to finish drawing one area.
 5. (Optional) Click **Clear All** to clear all of the areas.
 6. (Optional) Move the slider to set the sensitivity of the detection.
- **Task 2: Set the Arming Schedule for Motion Detection**



Figure 83, Arming Schedule

1. Click **Arming Schedule** to edit the arming schedule.
2. Click on the time bar and drag the mouse to select the time period.

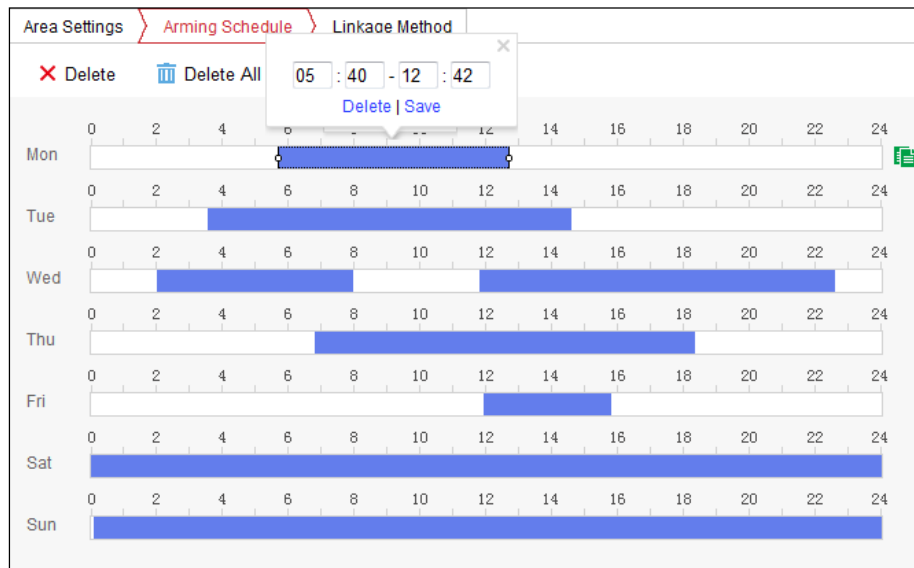


Figure 84, Arming Schedule

NOTE: Click on the selected time period, and you can adjust the time period to the desired time by either moving the time bar or inputting the exact time period.

3. (Optional) Click **Delete** to delete the current arming schedule, or click **Save** to save the settings.
4. Move the mouse to the end of each day, a copy dialogue box pops up, and you can copy the current settings to other days.

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

NOTE: The time of each period can't overlap. Up to eight periods can be configured for each day.

- **Task 3: Set the Linkage Method for Motion Detection**

Check the checkbox to select the linkage method. **Audible Warning**, **Send Email**, **Notify Surveillance Center**, **Upload to FTP/Memory Card/NAS**, **Trigger Channel**, and **Trigger Alarm Output** are selectable. You can specify the linkage method when an event occurs.

Normal Linkage	Trigger Alarm Output	Trigger Channel
<input type="checkbox"/> Audible Warning	<input type="checkbox"/> A->1	<input type="checkbox"/> A1
<input type="checkbox"/> Send Email		
<input type="checkbox"/> Notify Surveillance Center		
<input type="checkbox"/> Full Screen Monitoring		
<input type="checkbox"/> Upload to FTP		

Figure 85, Linkage Method

NOTE: The linkage methods vary by camera model.

- **Audible Warning:** Trigger the audible warning locally. Supported only by devices that have audio output.
- **Notify Surveillance Center:** Send an exception or alarm signal to remote management software when an event occurs.
- **Send Email:** Send an e-mail with alarm information to a user or users when an event occurs.

NOTE: To send the e-mail when an event occurs, refer to *Section 7.2.3, Configuring E-Mail Settings* to complete e-mail setup in advance.

- **Upload to FTP/Memory Card/NAS:** Capture the image when an alarm is triggered and upload the picture to a FTP server.

NOTES: Set the FTP address and the remote FTP server first. Refer to *Section 7.2.2, Configuring FTP Settings* for detailed information.

Go to **Configuration > Storage > Schedule Settings > Capture > Capture Parameters**, enable the event-triggered snapshot, and set the capture interval and capture number.

The captured image can also be uploaded to an available SD card or network disk.

- **Trigger Channel:** The video will be recorded when motion is detected. You must set the recording schedule to realize this function. Refer to *Section 11.1* for detailed information.
- **Trigger Alarm Output:** Trigger one or more external alarm outputs when an event occurs.

NOTE: To trigger an alarm output when an event occurs, refer to *Section 10.1.4, Configuring Alarm Output* to set the related parameters.

- **Expert Configuration:** Expert mode is used mainly to configure the sensitivity and proportion of object on each area for different day/night switch.

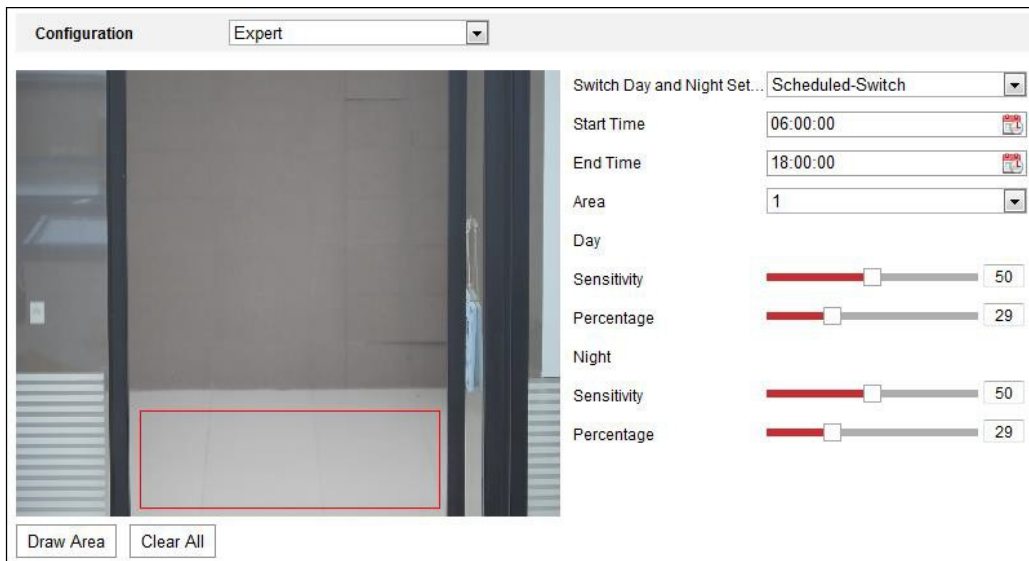


Figure 86, Expert Mode of Motion Detection

- Day/Night Switch OFF

1. Draw the detection area as in the normal configuration mode. Up to eight areas are supported.
2. Select **OFF** for **Switch Day and Night Settings**.
3. Select the area by clicking the area no.
4. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area.
5. Set the arming schedule and linkage method as in the normal configuration mode.
6. Click **Save** to save the settings.

- Day/Night Auto-Switch

1. Draw the detection area as in the normal configuration mode. Up to eight areas are supported.
2. Select **Auto-Switch** for **Switch Day and Night Settings**.
3. Select the area by clicking the area no.
4. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area in the daytime.
5. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area at night.

6. Set the arming schedule and linkage method as in the normal configuration mode.
7. Click **Save** to save the settings.

- Day/Night Scheduled-Switch

1. Draw the detection area as in the normal configuration mode. Up to eight areas are supported.
2. Select **Scheduled-Switch** for **Switch Day and Night Settings**.



Switch Day and Night Set...	Scheduled-Switch
Start Time	06:00:00
End Time	18:00:00

Figure 87, Day/Night Scheduled-Switch

3. Select the start time and the end time for the switch timing.
4. Select the area by clicking the area no.
5. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area in the daytime.
6. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area at night.
7. Set the arming schedule and linkage method as in the normal configuration mode.
8. Click **Save** to save the settings.

10.1.2. Configuring Video Tampering Alarm

Purpose

You can configure the camera to trigger an alarm when the lens is covered and take certain alarm response actions.

Detection area for this alarm is the whole screen.

1. Enter the **Video Tampering Settings** interface, **Configuration > Event > Basic Event > Video Tampering**.
2. Check the **Enable Video Tampering** checkbox to enable video tampering detection.
3. Click **Edit** to edit the video tampering arming schedule. The arming schedule configuration is the same as setting the motion detection arming schedule. Refer to *Task 2: Set the Arming Schedule for Motion Detection* in *Section 10.1.1*.
4. Check the checkbox to select the linkage method taken for the video tampering. Refer to *Task 3: Set the Linkage Method for Motion Detection* in *Section 10.1.1*.
5. Click **Save** to save the settings.

10.1.3. Configuring Alarm Input

1. Enter the **Alarm Input Settings** interface: **Configuration > Event > Basic Event > Alarm Input**.
2. Choose the alarm input no. and the **Alarm Type**. The alarm type can be NO (Normally Open) and NC (Normally Closed). Edit the name to set a name for the alarm input (optional).

The screenshot displays the 'Alarm Input' configuration page. At the top, there are navigation tabs: 'Motion Detection', 'Video Tampering', 'Alarm Input' (highlighted), 'Alarm Output', and 'Exception'. Below the tabs, the configuration fields are as follows:

- Alarm Input No.:** A dropdown menu showing 'A<-1'.
- IP Address:** A text input field containing 'Local'.
- Alarm Type:** A dropdown menu showing 'NO'.
- Alarm Name:** A text input field with '(cannot copy)' next to it.
- Enable Alarm Input Handling:** A checked checkbox.

Below the fields are two tabs: 'Arming Schedule' (highlighted) and 'Linkage Method'. Under 'Arming Schedule', there are two buttons: 'Delete' (with a red X icon) and 'Delete All' (with a trash can icon). The main area shows a weekly schedule grid with days of the week (Mon-Sun) on the y-axis and time slots (0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24) on the x-axis. Blue bars indicate the arming schedule for each day.

Figure 88, Alarm Input Settings

3. Click **Arming Schedule** to set the arming schedule for the alarm input. Refer to *Task 2: Set the Arming Schedule for Motion Detection* in *Section 10.1.1*.
4. Click **Linkage Method** and check the checkbox to select the linkage method taken for the alarm input. Refer to *Task 3: Set the Linkage Method for Motion Detection* in *Section 10.1.1*.
5. You can copy your settings to other alarm inputs.
6. Click **Save** to save the settings.

10.1.4. Configuring Alarm Output

Figure 89, Alarm Output Settings

1. Enter the **Alarm Output Settings** interface: **Configuration** > **Event** > **Basic Event** > **Alarm Output**.
2. Select one alarm output channel in the **Alarm Output** drop-down list. You can also set a name for the alarm output (optional).
3. The **Delay** time can be set to 5 sec, 10 sec, 30 sec, 1 min, 2 min, 5 min, 10 min, or Manual. The delay time refers to the time duration that the alarm output remains in effect after alarm occurs.
4. Click **Arming Schedule** to enter the **Edit Schedule Time** interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection. Refer to *Task 2: Set the Arming Schedule for Motion Detection* in *Section 10.1.1*.
5. You can copy the settings to other alarm outputs.
6. Click **Save** to save the settings.

10.1.5. Handling Exception

The exception type can be HDD full, HDD error, network disconnected, IP address conflicted, and illegal login to the cameras.

1. Enter the **Exception Settings** interface: **Configuration** > **Event** > **Basic Event** > **Exception**.
2. Check the checkbox to set the actions taken for the Exception alarm. Refer to *Task 3: Set the Linkage Method for Motion Detection* in *Section 10.1.1*.

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

10.1.6. Configuring Other Alarms

NOTE: Certain cameras support wireless alarms, PIR (passive infrared sensor) alarms, or emergency alarms.

10.1.6.1. Wireless Alarm

Purpose

When a wireless alarm signal is sent to the camera from a detector such as a wireless door contact, the wireless alarm is triggered and a series of response actions can be taken.

- Enter the **Wireless Alarm Settings** interface, **Configuration > Advanced Configuration > Basic Event > Wireless Alarm**.

<input type="checkbox"/> Normal Linkage	<input checked="" type="checkbox"/> Trigger Alarm Output	<input checked="" type="checkbox"/> Trigger Channel
<input checked="" type="checkbox"/> Audible Warning		<input checked="" type="checkbox"/> A1
<input checked="" type="checkbox"/> Send Email		
<input checked="" type="checkbox"/> Notify Surveillance Center		
<input checked="" type="checkbox"/> Upload to FTP		
<input type="checkbox"/> Wireless audible and visual...		

Figure 90, Setting Wireless Alarm

- Select the wireless alarm number. Up to eight channels of external wireless alarm input are supported.
- Check the **Enable Wireless Alarm** checkbox to activate the wireless alarm.
- Input the alarm name in the text field as desired.
- Check the checkbox to select the linkage methods taken for the wireless alarm.
- Click **Save** to save the settings.
- Locate the external wireless device beside the camera, and go to **Configuration > System > System Settings > Remote Control** to arm the camera and study the wireless alarm.

The screenshot shows the 'Remote Control' tab in a settings interface. It has two sections: 'Study' and 'Arm / Disarm'. In the 'Study' section, there is a 'Wireless Alarm' dropdown menu set to '1', a numeric input field containing '1', and a 'Study' button. In the 'Arm / Disarm' section, there is an 'Arm' dropdown menu, a numeric input field containing '0s', and a 'Set' button.

Figure 91, Configuring Wireless Alarm Settings

10.1.6.2. PIR Alarm

Purpose

A PIR (Passive Infrared) alarm is triggered when an intruder moves within the detector's field of view. The heat energy dissipated by a person, or any other warm blooded creature such as dogs, cats, etc., can be detected.

1. Enter the PIR Alarm Settings interface, **Configuration > Advanced Configuration > Basic Event > PIR Alarm**.

The screenshot shows the 'PIR Alarm' settings page. At the top, there are tabs for 'Motion Detection', 'Video Tampering', 'Exception', 'PIR Alarm' (selected), 'Wireless Alarm', and 'Emergency Alarm'. Below the tabs, there is an 'Enable' checkbox which is checked. An 'Alarm Name' text field is present. There are two tabs: 'Arming Schedule' (selected) and 'Linkage Method'. Below these are 'Delete' and 'Delete All' buttons. The main area is a calendar grid showing the arming schedule for each day of the week (Mon through Sun). Each day has a horizontal bar representing the 24-hour period, with tick marks every 2 hours. All bars are currently filled with blue, indicating the alarm is armed for the entire duration of each day.

Figure 92, Setting PIR Alarm

2. Check the **Enable** checkbox to activate the PIR alarm function.
3. Input the alarm name in the text field as desired.
4. Check the checkbox to select the linkage methods for the PIR alarm.
5. Click the **Edit** button to set the arming schedule.

- Click **Save** to save the settings.
- Go to **Configuration > Advanced Configuration > System > Remote Control** to arm the camera.

Figure 93, Arming PIR Alarm

10.1.6.3. Emergency Alarm

Purpose

You can press the **Emergency** button on the remote control to trigger the **Emergency Alarm** in case of an emergency.

NOTE: The remote control is required for the **Emergency Alarm**. Go to **Configuration > System > System Settings > Remote Control** to study the remote control first.

- Enter the **Emergency Alarm Settings** interface, **Configuration > Event > Basic Event > Emergency Alarm**.

Figure 94, Setting Emergency Alarm

- Check the checkbox to select the linkage methods for the Emergency alarm.
- Click **Save** to save the settings.

10.2. Smart Events

You can configure the smart events by following the instructions in this section, including audio exception detection, defocus detection, scene change detection, intrusion detection, line crossing detection, etc. These events can trigger linkage methods such as Notify Surveillance Center, Send Email, Trigger Alarm Output, etc.

NOTE: **DS-2CD2xx6G1 Series Cameras Only:** Some Smart VCA functions (line crossing detection, intrusion detection, region entrance/exit detection) are not functional when using third video stream, H.265+ video compression, or motion detection.

10.2.1. Configuring Audio Exception Detection

Purpose

The Audio Exception detection function detects abnormal sounds in the surveillance scene such as sudden increase/decrease in sound intensity, and certain actions can be taken when the alarm is triggered.

NOTE: The Audio Exception detection function varies by camera model.

1. Enter the **Audio Exception Detection** settings interface, **Configuration > Event > Smart Event > Audio Exception Detection**.

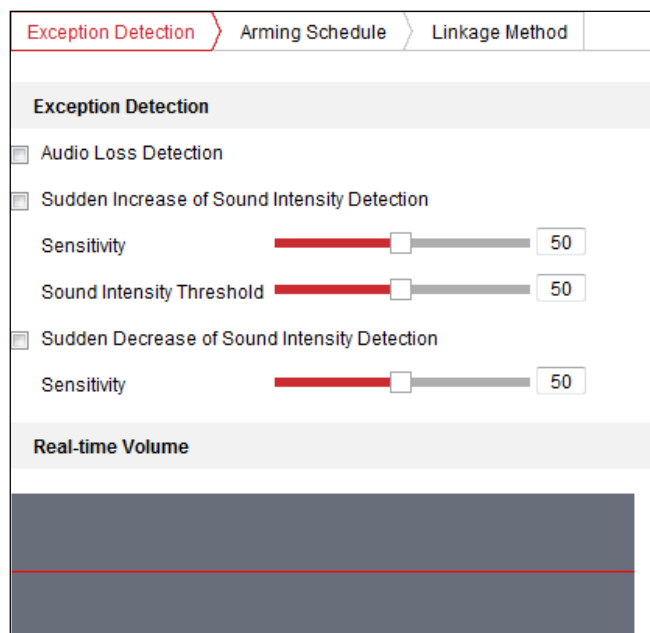


Figure 95, Audio Exception Detection

2. Check the **Audio Loss Exception** checkbox to enable the **Audio Loss** detection function.
3. Check the **Sudden Increase of Sound Intensity Detection** checkbox to detect a steep rise in the surveillance scene's sound. You can set the detection sensitivity and threshold.
4. Check the **Sudden Decrease of Sound Intensity Detection** checkbox to detect a steep drop in the surveillance scene's sound. You can set the detection sensitivity and threshold.

NOTES: **Sensitivity:** Range [1–100], the smaller the value, the more severe the change must be to trigger the detection.

Sound Intensity Threshold: Range [1–100], can filter environment sound, the louder the environment sound, the higher the value must be. Adjust it according to the real environment.

You can view the real-time sound volume on the interface.

- Click **Arming Schedule** to set the arming schedule. Refer to *Task 2 Set the Arming Schedule for Motion Detection* in *Section 10.1.1* for detailed steps.
- Click **Linkage Method** and select the linkage methods for audio exception, including Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel for recording, and Trigger Alarm Output.
- Click **Save** to save the settings.

10.2.2. Configuring Defocus Detection

Purpose

The image blur caused by lens defocus can be detected, and certain actions can be taken when the alarm is triggered.

NOTE: The Defocus Detection function varies by camera model.

- Enter the **Defocus Detection** settings interface, **Configuration > Event > Smart Event > Defocus Detection**.

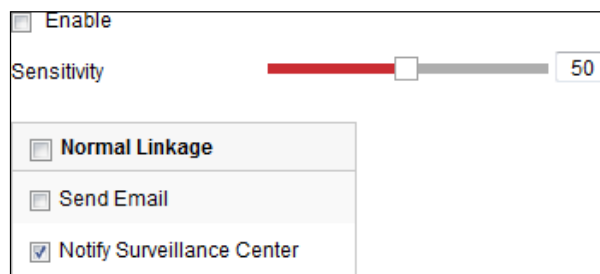


Figure 96, Configuring Defocus Detection

- Check the **Enable** checkbox to enable the function.
- Click-and-drag the slider to set the detection sensitivity. The sensitivity value ranges from 1 to 100, and the higher the value, the more easily the defocus image will trigger the alarm.
- Select the linkage method for defocus, including Notify Surveillance Center, Send Email, and Trigger Alarm Output.
- Click **Save** to save the settings.

10.2.3. Configuring Scene Change Detection

Purpose

Scene Change Detection detects the change of the surveillance environment affected by external factors such as intentional rotation of the camera. Certain actions can be taken when the alarm is triggered.

NOTE: The **Scene Change Detection** function varies by camera model.

- Enter the **Scene Change Detection** settings interface, **Configuration > Event > Smart Event > Scene Change Detection**.

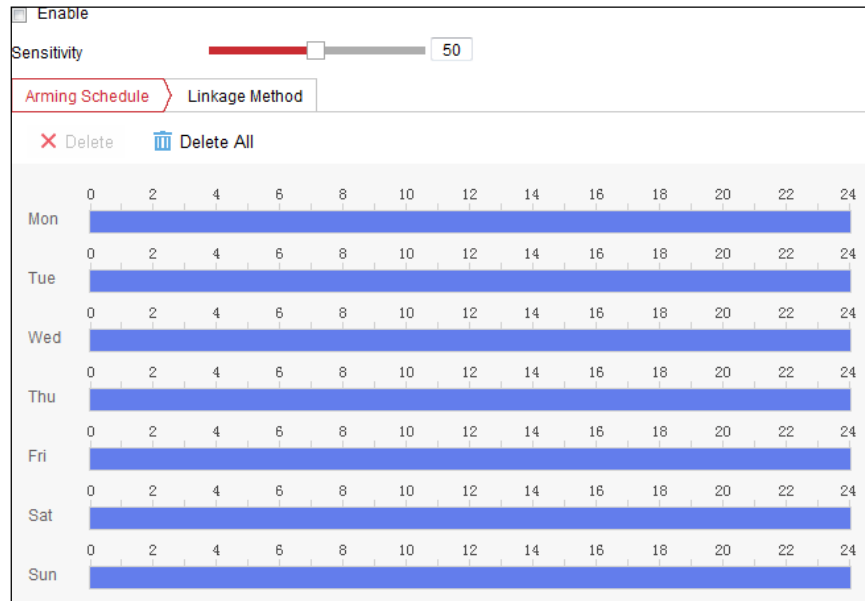


Figure 97, Scene Change Detection

2. Check the **Enable** checkbox to enable the function.
3. Click-and-drag the slider to set the detection sensitivity. The sensitivity value ranges from 1 to 100, and the higher the value, the more easily the change of scene will trigger the alarm.
4. Click **Arming Schedule** to set the arming schedule. Refer to *Task 2: Set the Arming Schedule for Motion Detection* in *Section 10.1.1* for detailed steps.
5. Click **Linkage Method** to select the linkage method for scene change, including Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel, and Trigger Alarm Output.
6. Click **Save** to save the settings.

10.2.4. Configuring Face Detection

Purpose

The **Face Detection** function detects faces that appear in the surveillance scene, and certain actions can be taken when the alarm is triggered.

1. Enter the **Face Detection** settings interface, **Configuration > Event > Smart Event > Face Detection**.
2. Check the **Enable Face Detection** checkbox to enable the function.
3. Check the **Enable Dynamic Analysis** checkbox for Face Detection, and then a detected face will be marked with a green rectangle on the live video.

NOTE: To mark the detected face on the live video, go to **Configuration > Local** to enable the **Rules**.

4. Click-and-drag the slider to set the detection sensitivity. The Sensitivity ranges from 1 to 5. The higher the value, the more easily the face will be detected.
5. Click **Arming Schedule** to set the arming schedule. Refer to *Task 2: Set the Arming Schedule for Motion Detection* in *Section 10.1.1* for detailed steps.

- Click **Linkage Method** to select the linkage method for face detection. Refer to *Task 3: Set the Linkage Method Taken for Motion Detection* in *Section 10.1.1*.

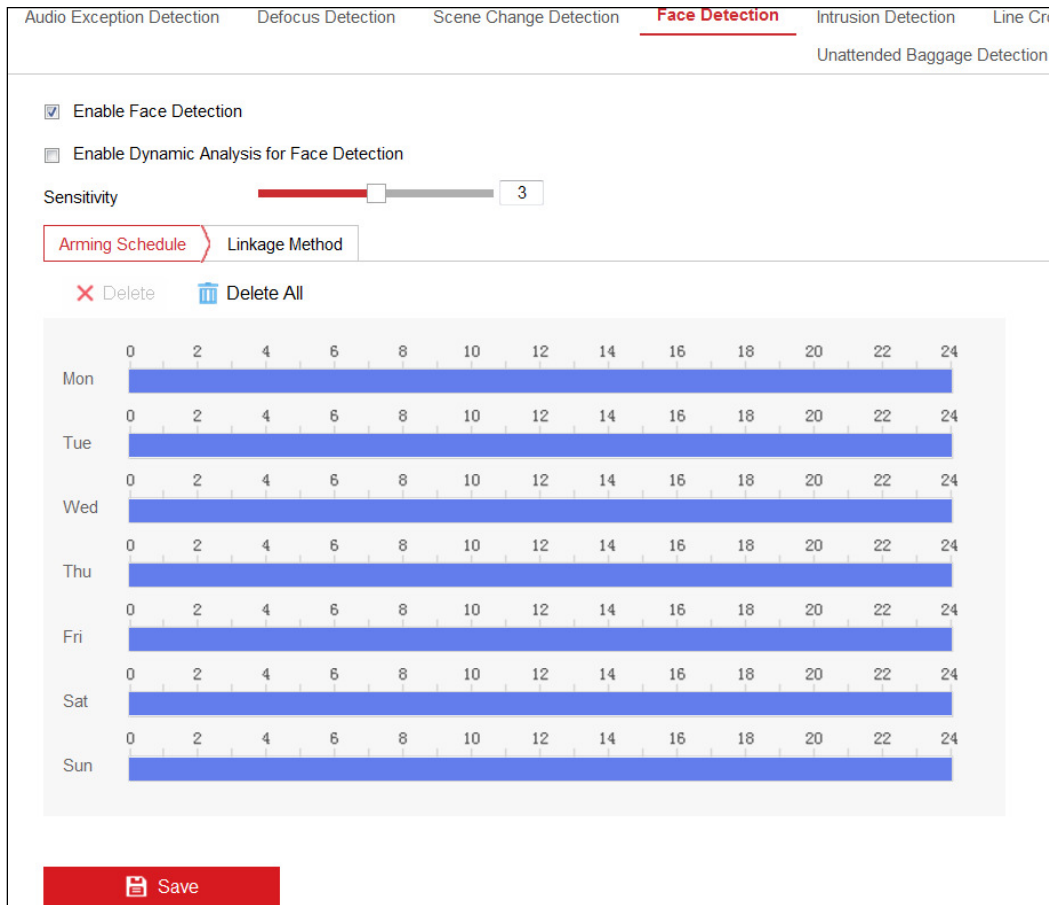


Figure 98, Face Detection

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

10.2.5. Configuring Intrusion Detection

Purpose

The **Intrusion Detection** function detects people, vehicles, or other objects that enter and loiter in a pre-defined virtual region, and certain actions can be taken when the alarm is triggered.

NOTE: The **Intrusion Detection** function varies by camera model.

- Enter the **Intrusion Detection** settings interface, **Configuration** > **Event** > **Smart Event** > **Intrusion Detection**.

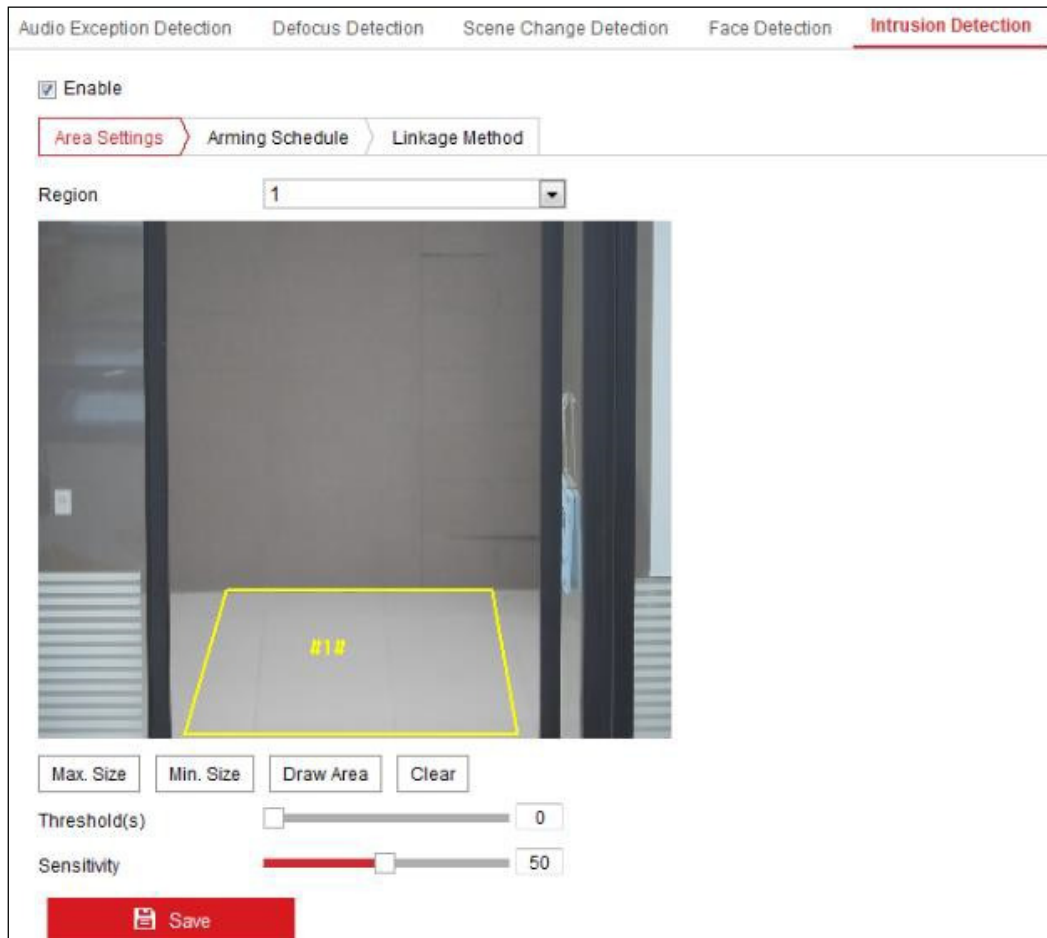


Figure 99, Intrusion Detection

2. Check the **Enable** checkbox to enable the function.
3. Select a region number from the **Region** drop-down list.
 - **Region:** A pre-defined vertices area on the live view image. Targets such as, people, vehicles, or other objects that enter and loiter in the region will be detected and trigger the set alarm.
4. Click **Area Settings** tab and click **Draw Area** button to start the region drawing.
5. Click on the live video to specify the four vertices of the detection region, and right click to complete drawing.
6. Set the **Max. Size** and **Min. Size** for valid targets. Targets smaller or larger than the valid target sizes are not able to trigger detection.
 - **Max. Size:** The maximum size of a valid target. Targets with larger sizes will not trigger detection.
 - **Min. Size:** The minimum size of a valid target. Targets with smaller sizes will not trigger detection.
7. Click **Stop Drawing** when finish drawing.
8. Set the time threshold for intrusion detection.
 - **Threshold:** Range [0s–10s], the threshold for the time of the object loitering in the region. If you

set the value to 0, alarm is triggered immediately once the object enters the region.

9. Drag the slider to set the sensitivity value.

- **Sensitivity:** Range [1–100]. Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region.

$$\text{Sensitivity} = 100 - S1/ST*100$$

S1 stands for the target body part that goes across the pre-defined region. ST stands for the complete target body.

Example: if you set the value as 60, the action will be counted as an intrusion only when 40 percent body part enters the region.

NOTE: The **Sensitivity** of the detection is supported by certain models. Refer to actual display for details.

10. Repeat the above steps to configure other regions. Up to four regions can be set. You can click the **Clear** button to clear all pre-defined regions.

11. Click **Arming Schedule** to set the arming schedule.

12. Click **Linkage Method** to select the linkage methods for intrusion detection, including Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel, and Trigger Alarm Output.

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

10.2.6. Configuring Line Crossing Detection

Purpose

The Line Crossing detection function detects people, vehicles, or other objects that cross a pre-defined virtual line, and certain actions can be taken when the alarm is triggered.

NOTE: The Line Crossing detection function varies by camera model.

1. Enter the **Line Crossing Detection settings** interface, **Configuration > Event > Smart Event > Line Crossing Detection**.



Figure 100, Line Crossing Detection

2. Check the **Enable** checkbox to enable the function.
3. Select the line from the drop-down list.
4. Click the **Area Settings** tab and click the **Draw Area** button, and a virtual line is displayed on the live video.
5. Drag the line, and you can locate it on the live video as desired. Click on the line, two red squares are displayed on each end, and you can click-and-drag one of the red squares to define the shape and length of the line.
6. Set the **Max. Size** and **Min. Size** for valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.
 - **Max. Size:** The maximum size of a valid target. Targets with larger sizes will not trigger detection.

- **Min. Size:** The minimum size of a valid target. Targets with smaller sizes will not trigger detection.
7. Set the direction for line crossing detection. You can set the direction as **A<->B**, **A->B**, and **B->A**.
 - **A<->B:** An object going across the plane in either direction is detected and alarm is triggered.
 - **A->B:** Only an object crossing the configured line from the A side to the B side can be detected.
 - **B->A:** Only an object crossing the configured line from the B side to the A side can be detected.
 8. Click **Stop Drawing** when finish drawing.
 9. Drag the slider to set the sensitivity value.
 - **Sensitivity:** Range [1–100]. It stands for the percentage of the body part of an acceptable target that goes across the pre-defined line.

$$\text{Sensitivity} = 100 - S1/ST*100$$

S1 stands for the target body part that goes across the pre-defined line. ST stands for the complete target body.

Example: If you set the value as 60, the action can be counted as a line crossing action only when 40 percent or more body part goes across the line.

NOTE: The detection **Sensitivity** is supported by certain models. Refer to actual display for details.

10. Repeat the above steps to configure other lines. Up to four lines can be set. You can click the **Clear** button to clear all pre-defined lines.
11. Click the **Arming Schedule** to set the arming schedule.
12. Select the linkage methods for line crossing detection, including Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel, and Trigger Alarm Output.
13. Click **Save** to save the settings.

10.2.7. Configuring Region Entrance Detection

Purpose

The **Region Entrance** detection function detects people, vehicles, or other objects that enter a pre-defined virtual region, and certain actions can be taken when the alarm is triggered.

1. Enter the **Region Entrance Detection** settings interface, **Configuration > Event > Smart Event > Region Entrance Detection**.

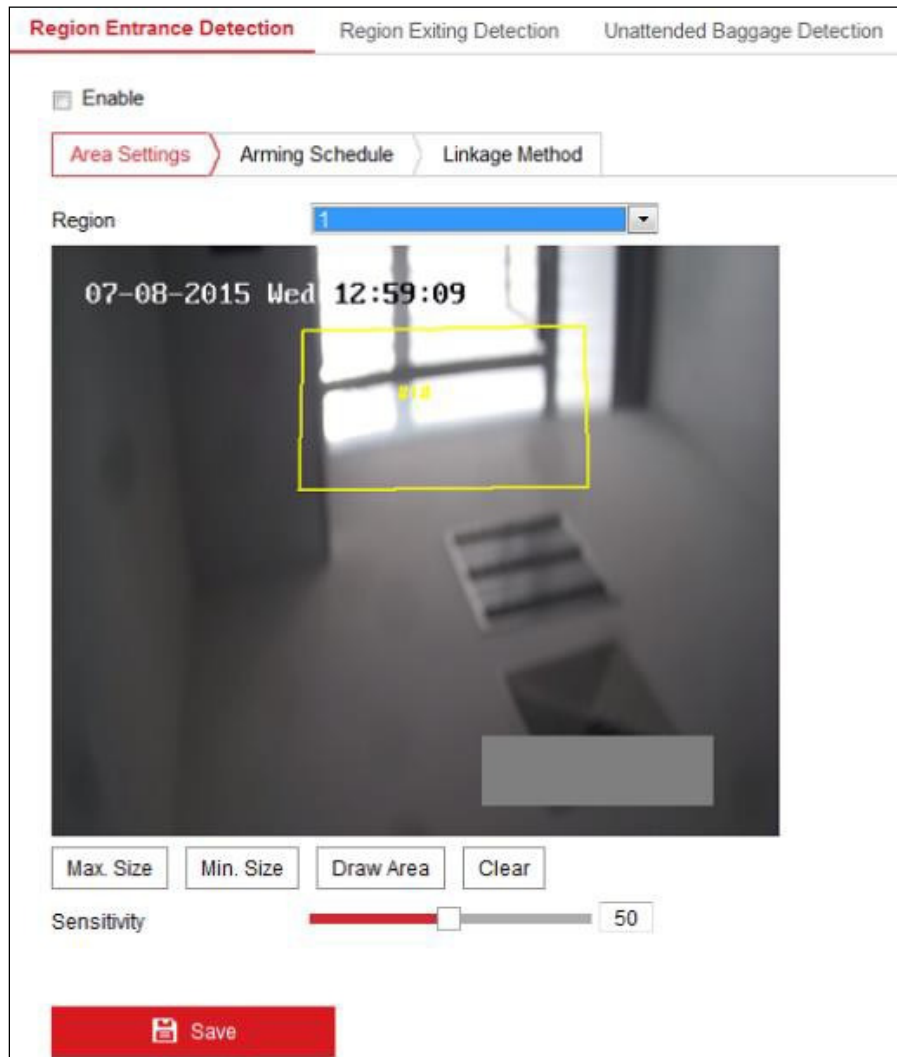


Figure 101, Region Entrance Detection

2. Check the **Enable** checkbox to enable the function.
3. Select the **Region** from the drop-down list for detection settings.
4. Click **Area Settings** and click **Draw Area** button to start the area drawing.
5. Click on the live video to specify the four vertices of the detection region, and right click to complete drawing.
6. Set the **Max. Size** and **Min. Size** for valid targets. Targets smaller or larger than the valid target size will not trigger detection.
 - **Max. Size:** The maximum size of a valid target. Targets with larger sizes will not trigger detection.
 - **Min. Size:** The minimum size of a valid target. Targets with smaller sizes will not trigger detection.
7. Click **Stop Drawing** when finished drawing.
8. Drag the slider to set the sensitivity value.

- **Sensitivity:** Range [1–100]. Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region.

$$\text{Sensitivity} = 100 - S1/ST*100$$

S1 stands for the target body part that enters the pre-defined region ST stands for the complete target body.

Example: If you set the value as 60, the action can be counted as an region entrance action only when 40 percent body part enters the region.

NOTE: The **Sensitivity** of the detection is supported by certain models. Refer to actual display for details.

9. Repeat the above steps to configure other regions. Up to four regions can be set. You can click the **Clear** button to clear all pre-defined regions.
10. Click **Arming Schedule** to set the arming schedule.
11. Click **Linkage Method** to select the linkage methods.
12. Click **Save** to save the settings.

10.2.8. Configuring Region Exiting Detection

Purpose

Region exiting detection function detects people, vehicles, or other objects that exit from a pre-defined virtual region, and certain actions can be taken when the alarm is triggered.

1. Enter the **Region Exiting Detection** settings interface, **Configuration > Event > Smart Event > Region Exiting Detection**.

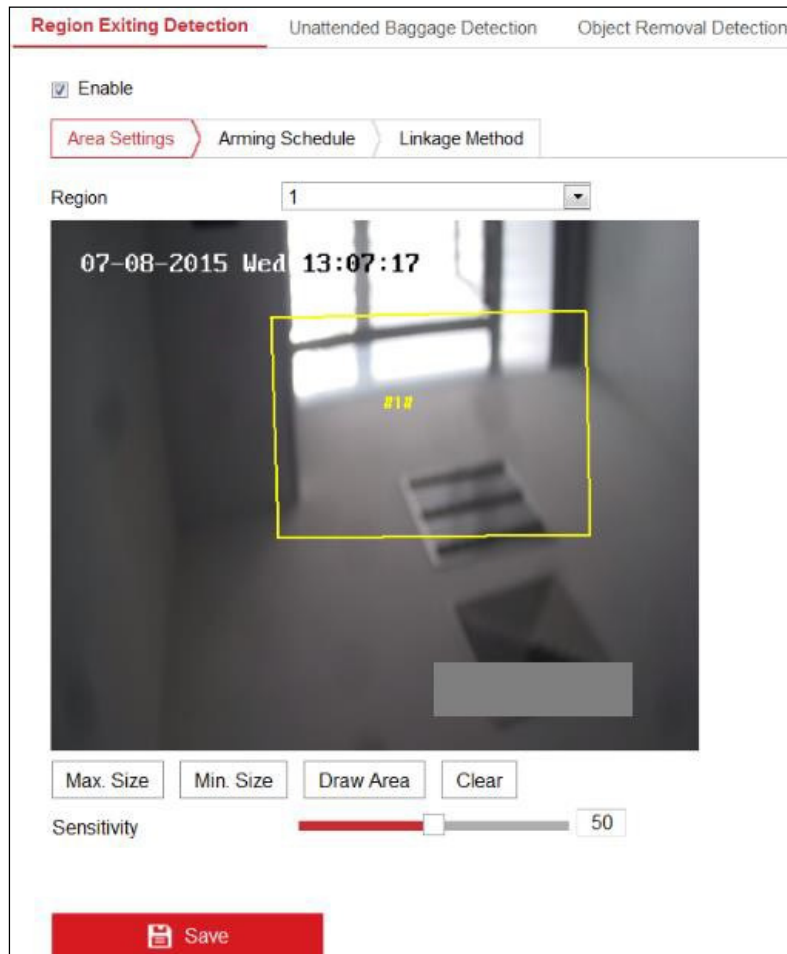


Figure 102, Region Exiting Detection

2. Check the **Enable** checkbox to enable the function.
3. Select the **Region** from the drop-down list for detection settings.
4. Click **Area Settings** and click **Draw Area** button to start the area drawing.
5. Click on the live video to specify the four vertices of the detection region, and right click to complete drawing.
6. Set the **Max. Size** and **Min. Size** for valid targets. Targets smaller or larger than the valid target size will not trigger detection.
 - **Max. Size:** The maximum size of a valid target. Targets with larger sizes will not trigger detection.
 - **Min. Size:** The minimum size of a valid target. Targets with smaller sizes will not trigger detection.
7. Click **Stop Drawing** when finish drawing.
8. Drag the slider to set the sensitivity value.
 - **Sensitivity:** Range [1–100]. Sensitivity stands for the percentage of the body part of an acceptable target that exits the pre-defined region.

$$\text{Sensitivity} = 100 - S1/ST*100$$

S1 stands for the target body part that exits the pre-defined region. ST stands for the complete target body.

Example: If you set the value as 60, the action can be counted as an region exiting action only when 40 percent body part exits the region.

NOTE: The **Sensitivity** of the detection is supported by certain models. Refer to actual display for details.

9. Repeat the above steps to configure other regions. Up to four regions can be set. You can click the **Clear** button to clear all pre-defined regions.
10. Click **Arming Schedule** to set the arming schedule.
11. Click **Linkage Method** to select the linkage methods.
12. Click **Save** to save the settings.

10.2.9. Configuring Unattended Baggage Detection

Purpose

The **Unattended Baggage** detection function detects objects left in a pre-defined region such as a baggage, purse, dangerous materials, etc. A series of actions can be taken when the alarm is triggered.

1. Enter the **Unattended Baggage Detection** settings interface, **Configuration > Event > Smart Event > Unattended Baggage Detection**.

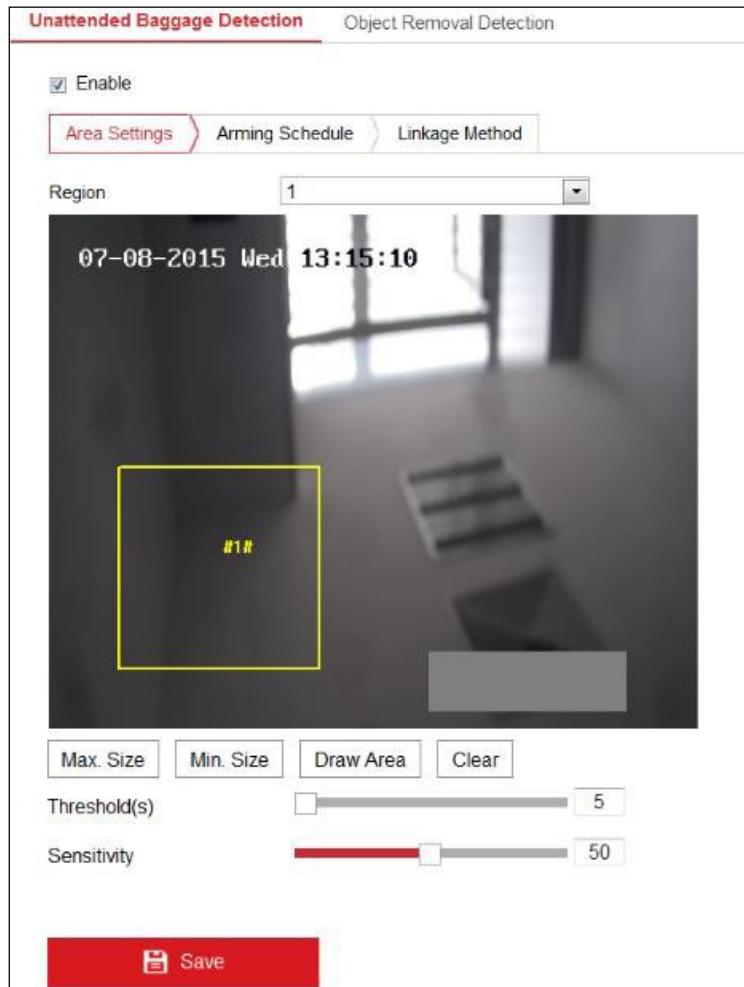


Figure 103, Unattended Baggage Detection

2. Check the **Enable** checkbox to enable the function.
3. Select the **Region** from the drop-down list for detection settings.
4. Click **Area Settings** and click **Draw Area** to start the area drawing.
5. Click on the live video to specify the four vertices of the detection region, and right click to complete drawing.
6. Set the **Max. Size** and **Min. Size** for valid targets. Targets smaller or larger than the valid target size will not trigger detection.
 - **Max. Size:** The maximum size of a valid target. Targets with larger sizes will not trigger detection.
 - **Min. Size:** The minimum size of a valid target. Targets with smaller sizes will not trigger detection.
7. Click **Stop Drawing** when finished drawing.
8. Set the time threshold and detection sensitivity for unattended baggage detection.

- **Threshold:** Range [5–100s], the threshold for the time of the objects left in the region. If you set the value as 10, an alarm is triggered if the object is left and stays in the region for 10s.

9. Drag the slider to set the sensitivity value.

- **Sensitivity:** Range [1–100]. Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region.

$$\text{Sensitivity} = 100 - S1/ST*100$$

S1 stands for target body part that enters the pre-defined region. ST stands for the complete target body.

Example: If you set the value as 60, a target is possible to be counted as an unattended baggage only when 40 percent body part of the target enters the region.

NOTE: The **Sensitivity** of the detection is supported by certain models. Refer to actual display for details.

10. Repeat the above steps to configure other regions. Up to four regions can be set. You can click the **Clear** button to clear all pre-defined regions.

11. Click **Arming Schedule** to set the arming schedule.

12. Click **Linkage Method** to select the linkage methods.

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

10.2.10. Configuring Object Removal Detection

Purpose

The **Object Removal** detection function detects objects removed from a pre-defined region such as exhibits on display, and a series of actions can be taken when the alarm is triggered.

1. Enter the **Object Removal Detection** settings interface, **Configuration > Event > Smart Event > Object Removal Detection**.

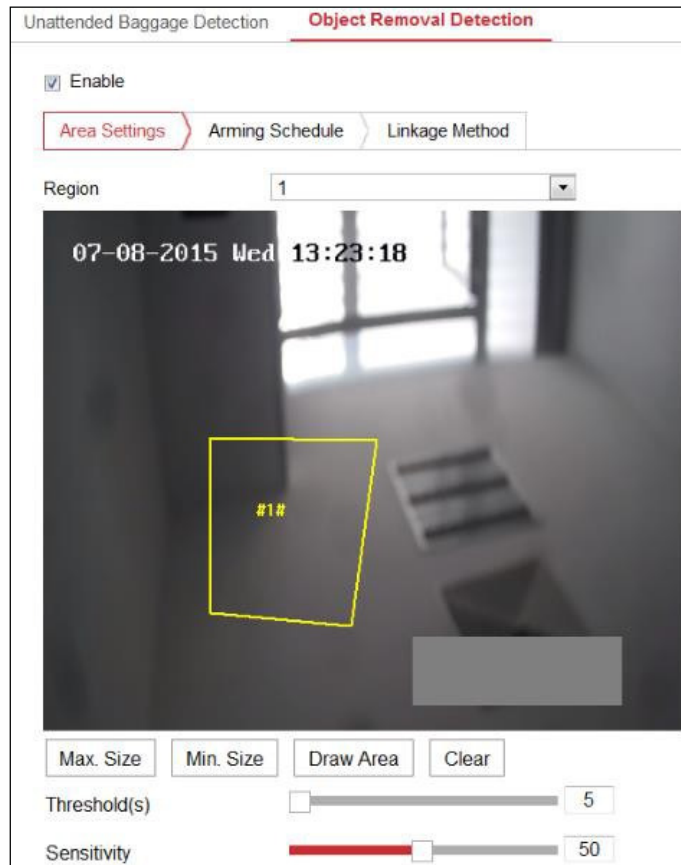


Figure 104, Object Removal Detection

2. Check the **Enable** checkbox to enable the function.
3. Select the **Region** from the drop-down list for detection settings.
4. Click **Area Settings** and click the **Draw Area** button to start the area drawing.
5. Click on the live video to specify the four vertices of the detection region, and right click to complete drawing.
6. Set the **Max. Size** and **Min. Size** for valid targets. Targets smaller or larger than the valid target size will not trigger detection.
 - **Max. Size:** The maximum size of a valid target. Targets with larger sizes will not trigger detection.
 - **Min. Size:** The minimum size of a valid target. Targets with smaller sizes will not trigger detection.
7. Click **Stop Drawing** when finish drawing.
8. Set the time threshold for object removal detection.
 - **Threshold:** Range [5–100s], the threshold for the time of the objects removed from the region. If you set the value as 10, alarm is triggered after the object disappears from the region for 10s.
9. Drag the slider to set the sensitivity value.

- **Sensitivity:** Range [1–100]. The percentage of an acceptable target that leaves the pre-defined region that will trigger an alarm.

$$\text{Sensitivity} = 100 - S1/ST*100$$

S1 stands for the target body part that leaves the pre-defined region. ST stands for the complete target body.

Example: If you set the value as 60, a target is possible to be counted as a removed object only when 40 percent body part of the target leaves the region.

NOTE: Detection **Sensitivity** is supported by certain models. Refer to actual display for details.

10. Repeat the above steps to configure other regions. Up to four regions can be set. You can click the **Clear** button to clear all pre-defined regions.
11. Click **Arming Schedule** to set the arming schedule.
12. Click **Linkage Method** to select the linkage methods.
13. Click **Save** to save the settings.

10.3. VCA Configuration

10.3.1. Behavior Analysis

Behavior Analysis detects a series of suspicious behaviors, and certain linkage methods will be enabled if the alarm is triggered.

Figure 105, Behavior Analysis

- **Overlay and Capture: Display information includes the display on picture and display on stream.**
 - **Display VCA info. on Stream:** Green frames will be displayed on the target if in live view or playback.

- **Display Target info. on Alarm Picture:** There will be a frame on the target on the uploaded alarm picture if the checkbox is checked.
- **Display Rule info. on Alarm Picture:** The captured target and the configured area will be framed on the alarm picture.




NOTE: Make sure the rules are enabled in your local settings. Go to **Configuration > Local Configuration > Rules** to enable it.

- **Snapshot Setting: You can set the quality and resolution for the captured picture.**

- **Upload JPEG Image to Center:** Check this checkbox to upload the captured image to the surveillance center when a VCA alarm occurs.
- **Picture Quality:** High, Medium, and Low are selectable.
- **Picture Resolution:** CIF, 4CIF, 720P, and 1080P are selectable.

- **Camera Calibration**

Perform the following steps to three-dimensionally measure and quantize the image from the camera, and then calculate the size of every target. The VCA detection will be more accurate if the camera calibration is configured.

1. Check the **Camera Calibration** checkbox to enable this function.
2. Set the calibration mode as **Input Basic Data** or **Draw on Live View Video**.
 - **Input Basic Data:** Input the mounting height, viewing angle, and horizon ratio of the camera manually.
 - **Draw on Live View Video:** Click **Draw Verification Line (Horizontal)/(Vertical)** to draw a horizontal/vertical line in live view, and input the actual length in the **Real Length** field. With the drawn reference lines and their real length, the camera can compare other objects that appear in the live view.
3. Click the **Horizontal Verify**  / **Vertical Verify**  button to draw a horizontal/vertical line on the live video, and click the **Start Verifying**  button to calculate the line length. Compare the calculated line length to the actual length to verify the calibration information you set.

NOTE: If live view is stopped, the camera calibration is invalid.

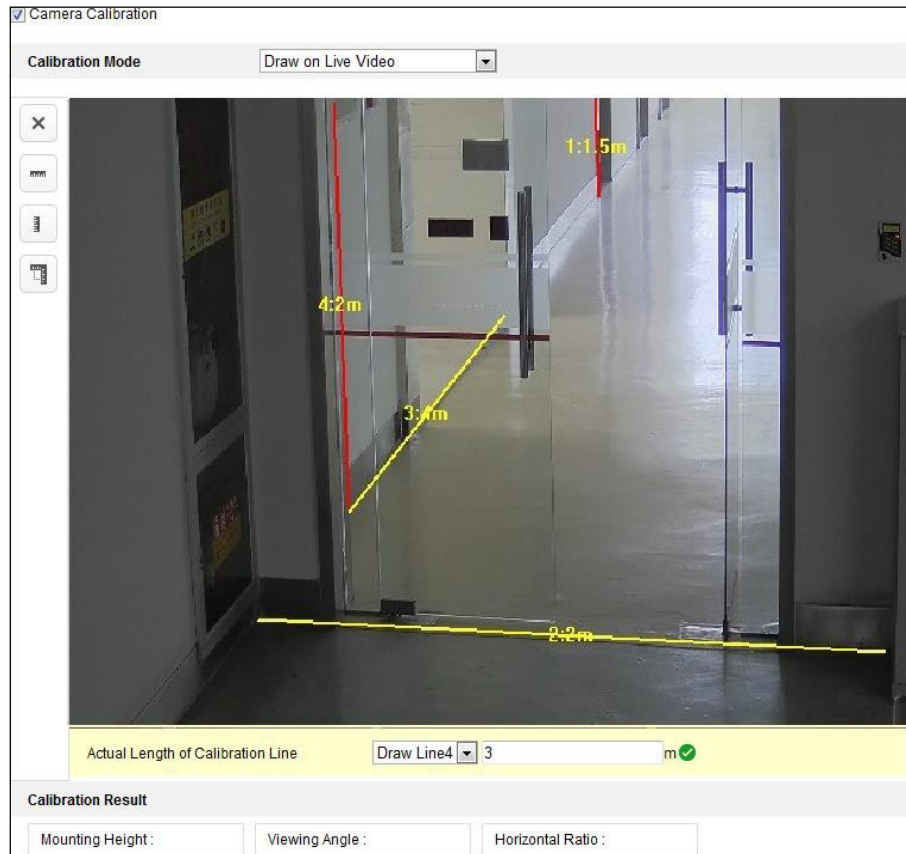




Figure 106, Draw on Live View Window

4. You can click  to delete the drawn lines.
5. Click **Save** to save the settings.

- **Shield Region**

The shield region allows you to set the specific region in which the behavior analysis will not function. Up to four shield regions are supported.

1. Click the **Shield Region** tab to enter the shield region configuration interface.
2. Click the hexagons sign  to draw shield area by left click end-points in the live view window, and right click to finish the area drawing.

NOTES: Polygon area with up to 10 sides is supported.

Click  to delete the drawn areas.

If live view is stopped, there is no way to draw the shield regions.

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

- **Rule**

Behavior Analysis supports a series of behaviors, including line crossing detection, intrusion, region entrance, and region exiting, etc.

NOTE: Please refer to each chapter for detailed information of each behavior.

1. Click the **Rule** tab to enter the rule configuration interface.
2. Check the checkbox of the single rule to enable the rule for behavior analysis.
3. Select the rule type, set the filter type, and then draw the line/area on the live video for the single rule.

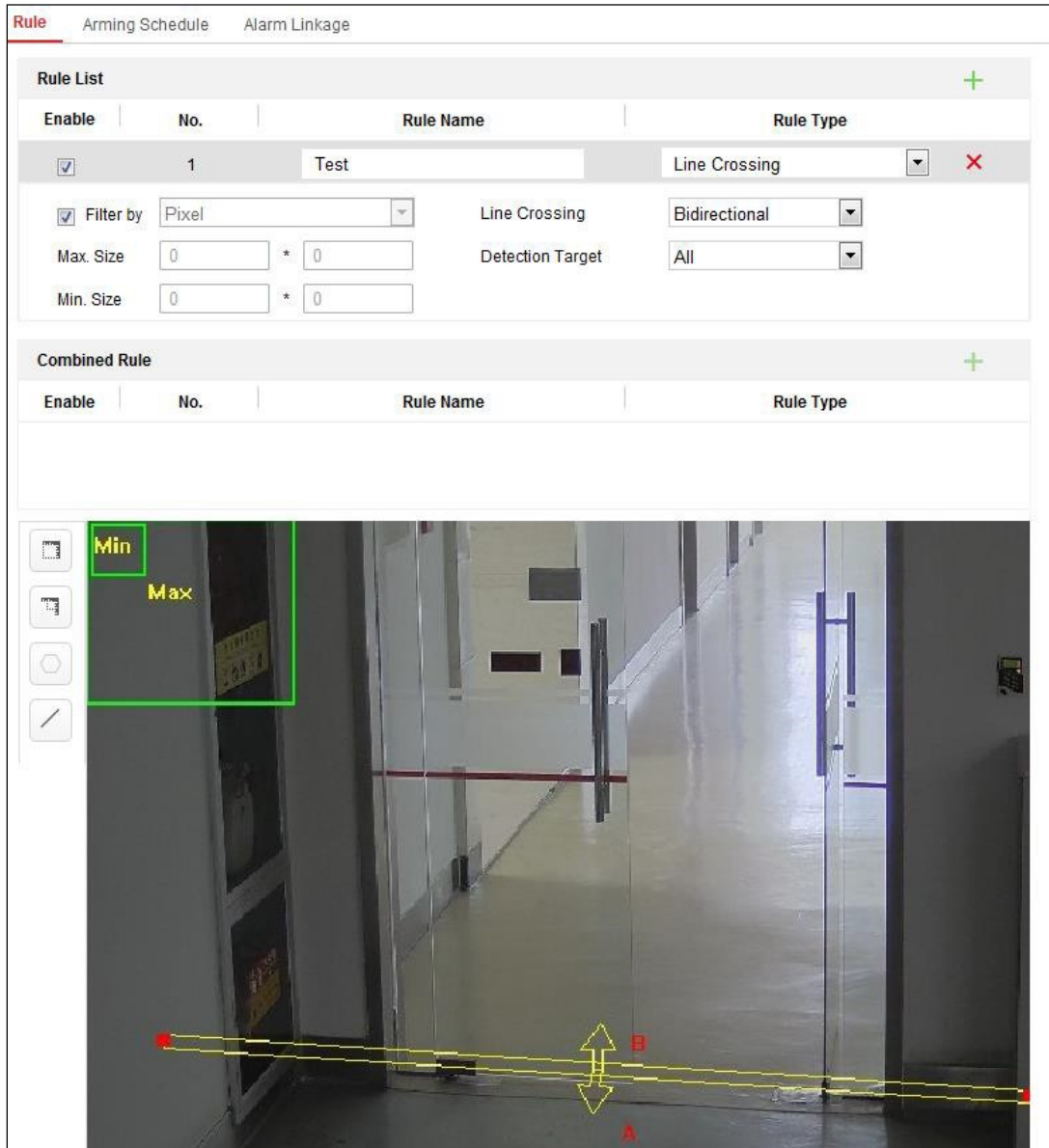


Figure 107, Configure the Rule

- **Filter type: Pixels and Actual Size** are selectable. If **Pixels** is selected, draw the area of maximum size and minimum size on the live video for each rule. If **Actual Size** is selected, input the length and width of the maximum size and minimum size. Only a target whose size is between the minimum value and maximum value will trigger the alarm.

NOTE: Make sure the camera calibration is configured if **Actual Size** is selected. **Detection Target:** Select **Human** or **Vehicle** as the detection target. You can also select **All** to detect all objects.

- **Draw line/area:** For line crossing detection, you have to draw a line and select the crossing direction, which is **bidirectional**, **A-to-B**, or **B-to-A**. For other events such as intrusion, region entrance, region exiting, etc., you have to left click on the live video to set the end points of the area and right click to finish the area drawing.

NOTE: If live view is stopped, the detection area/line cannot be drawn and the rules cannot be set.

4. Check the checkbox of the combined rule to enable the rule for behavior analysis.
5. Select two configured single rules as the **Rule A** and **Rule B** of the combined rule, set the minimum and maximum time interval for the two single rules, and then select the trigger order of the single rules for alarm filtering.

NOTES: If you select the rule type as **None**, the rule option is invalid and no behavior analysis can be configured.

Up to eight single rules and two combined rules are configurable. Line crossing, intrusion, region exiting, and region entrance are supported for the combined rules.

6. Click **Save** to save the settings.
7. Click the **Arming Schedule** tab to set the schedule time for each rule, and click **Save** to save the settings.
8. Click the **Linkage Method** tab, check the checkbox of the corresponding linkage method for each rule, and click **Save** to save the settings.

- **Advanced Configuration**

Behavior Analysis Version: Lists the algorithms library version.

- **Parameters**

Configure the following parameters to detail the configuration.

Figure 108, Advanced Configuration

- > **Detection Sensitivity** [0–4]: The sensitivity of the camera to detect a target. The higher the value, the easier a target will be recognized and the higher the possible misinformation. The default value of 3 is recommended.
- > **Background Update Rate** [0–4]: The speed of the new scene replacing the previous scene. The default value of 3 is recommended.
- > **Single Alarm**: If **Single Alarm** is checked, the target in the configured area will trigger the alarm once only. If it is not checked, the same target will cause continuous alarms in the same configured area.
- > **Leave Interference Suppression**: Check this checkbox to stop interference caused by leaves in the configured area.
- > **Output Type**: Select the position of the frame. Target center, bottom center, and top centers are selectable. E.g.: The target will be in the center of the frame if target center is selected.
- > **Restore Default**: Click to restore the configured parameters to the default.
- > **Restart VCA**: Restart the behavior analysis algorithms library.

- Global Size Filter

NOTE: Compared with the size filter under rule, which is aimed at each rule, the global size filter is aimed at all rules.

1. Check the **Global Size Filter** checkbox to enable the function.
2. Set the **Filter Type** as **Actual Size** or **Pixel**.
 - > **Actual Size**: Input the length and width of both the maximum size and the minimum size. Only targets whose size is between the minimum value and maximum value will trigger the alarm.

NOTES: Camera calibration has to be configured if you select the filter by **Actual Size**.

The maximum size length must be longer than the minimum size length. The maximum size width must be longer than the minimum size width.

- > **Pixel**: Click **Minimum Size** to draw a rectangle of the minimum size on the live view display. Click **Maximum Size** to draw a rectangle of the maximum size on the live view display. Targets smaller than the minimum size or larger than the maximum size will be filtered out.

NOTES: The drawn area will be converted to the pixel by the background algorithm.

The global size filter cannot be configured if live view is stopped.

The maximum size length must be longer than the minimum size length. The maximum size width must be longer than the minimum size width.

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

10.3.2. Face Capture

The camera can capture a face that appears in the configured area, and the face characteristic information such as age and gender will be uploaded with the captured picture as well.


- **Overlay and Capture**

Display information includes the display on picture and display on stream.

- **Display VCA info. on Stream:** Green frames will be displayed on the target if in live view or playback.
- **Display Target info. on Alarm Picture:** There will be a frame on the target on the uploaded alarm picture if the checkbox is checked.
- **Snapshot Setting:** Select the picture quality for the captured picture. **Good**, **Better**, and **Best** are selectable.
- **Background Upload:** Check the **Background Upload** checkbox to upload the background picture as well.
- **Camera Information:** You can set the **Device No.** and **Camera Info.** for the camera, which can be overlaid on the captured picture.
- **Picture Overlay Information:** You can check desired items and adjust their order to display on captured pictures.

- **Shield Region**

The shield region allows you to set specific regions where face capture are blocked. Up to four shield regions are supported.

1. Click the hexagons sign  to draw shield area by left clicking end-points in the live view window, and right click to finish the area drawing.

NOTES: Polygon area (4 to 10 sides are supported).

Click  to delete the drawn areas.

If live view is stopped, there is no way to draw the shield regions.

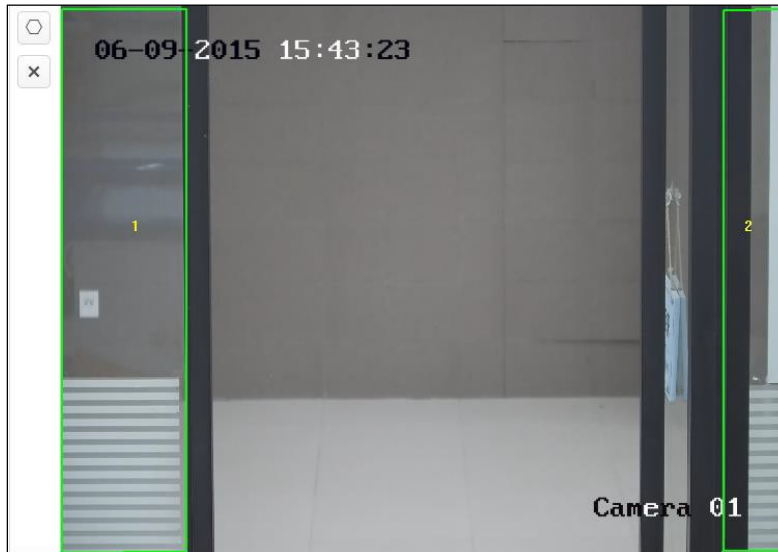


Figure 109, Draw Shield Area

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

- **Rule**

1. Check the **Rule** checkbox to enable face capture rules.
2. Click the rectangle sign to draw the minimum pupil distance. The distance of the drawn pupil will be displayed on the box below the live view. The minimize pupil distance refers to the minimum square size composed by the area between two pupils, and it is the basic standard for a camera to identify a target.
3. Click the hexagon sign to draw the detection area in which you want the face capture to take effect. Draw area by left click end-points in the live view window, and right click to finish the area drawing.

NOTES: Polygon area (4~10 sides are supported).

If live view is stopped, there is no way to draw the configured area.

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

- **Advanced Configuration**

Face Capture Version: Lists the algorithms library version. Configure the following parameters according to your actual environment.

Parameters

Face Capture Version

Detection Parameters

Generation Speed 3

Capture Times 1

Sensitivity 5

Capture Interval 2

Capture Sensitivity 10

Face Exposure

Reference Brightness 50

Min. Duration 1

Enable Face ROI

Setting the stream type as H.264 is required to make sure the ROI functioning.

Restore Parameters

Restore Defaults

Figure 110, Face Capture – Advanced Configuration

- Detection Parameters

- > **Generation Speed** [1–5]: The speed to identify a target. The higher the value, the quicker the target will be recognized. Setting the value low, if there is a face in the configured area from the start, this face will not be captured. It can reduce face misinformation in wall paintings or posters. The default value of 3 is recommended.
- > **Capture Times** [1–10]: Refers to the capture times a face will be captured during its stay in the configured area. The default value is 1.
- > **Sensitivity** [1–5]: The sensitivity to identify a target. The higher the value, the easier a face will be recognized, and the higher the possible misinformation. The default value of 3 is recommended.
- > **Capture Interval** [1–255 Frame]: The frame interval to capture a picture. If you set the value as 1, which is the default value, it means the camera captures the face in every frame.
- > **Capture Sensitivity** [0–20]: The threshold the camera treats the target as a face. Only when the face score generated by the algorithm is equal or higher than the value, will the camera treat the target as a face. The default value of 2 is recommended.
- > **Face Capture Advanced Parameters**
 - * **Face Exposure:** Check the checkbox to enable face exposure.
 - * **Reference Brightness** [0–100]: The reference brightness of a face in face exposure mode. If a face is detected, the camera adjusts the face brightness according to the value you set. The higher the value, the brighter the face.

- * **Minimum Duration** [1–60 min]: The minimum duration of the camera exposures the face. The default value is 1 minute.

NOTE: If face exposure is enabled, make sure the WDR function is disabled, and manual iris is selected.

- * **Enable Face ROI:** If the camera captures a face, the face area will be treated as the region of interest, and the image quality of this area will be improved.
- * **Restore Default:** Click **Restore** to restore all the settings in advanced configuration to the factory defaults.

10.3.3. People Counting

Purpose

People function is used to calculate the number of object entering or exiting a certain configured area, and it is applied to entrances and exits.

NOTES: It is recommended to install the camera directly above the entrance/exit. To improve the counting accuracy, make sure your camera is installed horizontally.

1. Enter the **Counting Configuration** interface: **Configuration** > **People Counting**.

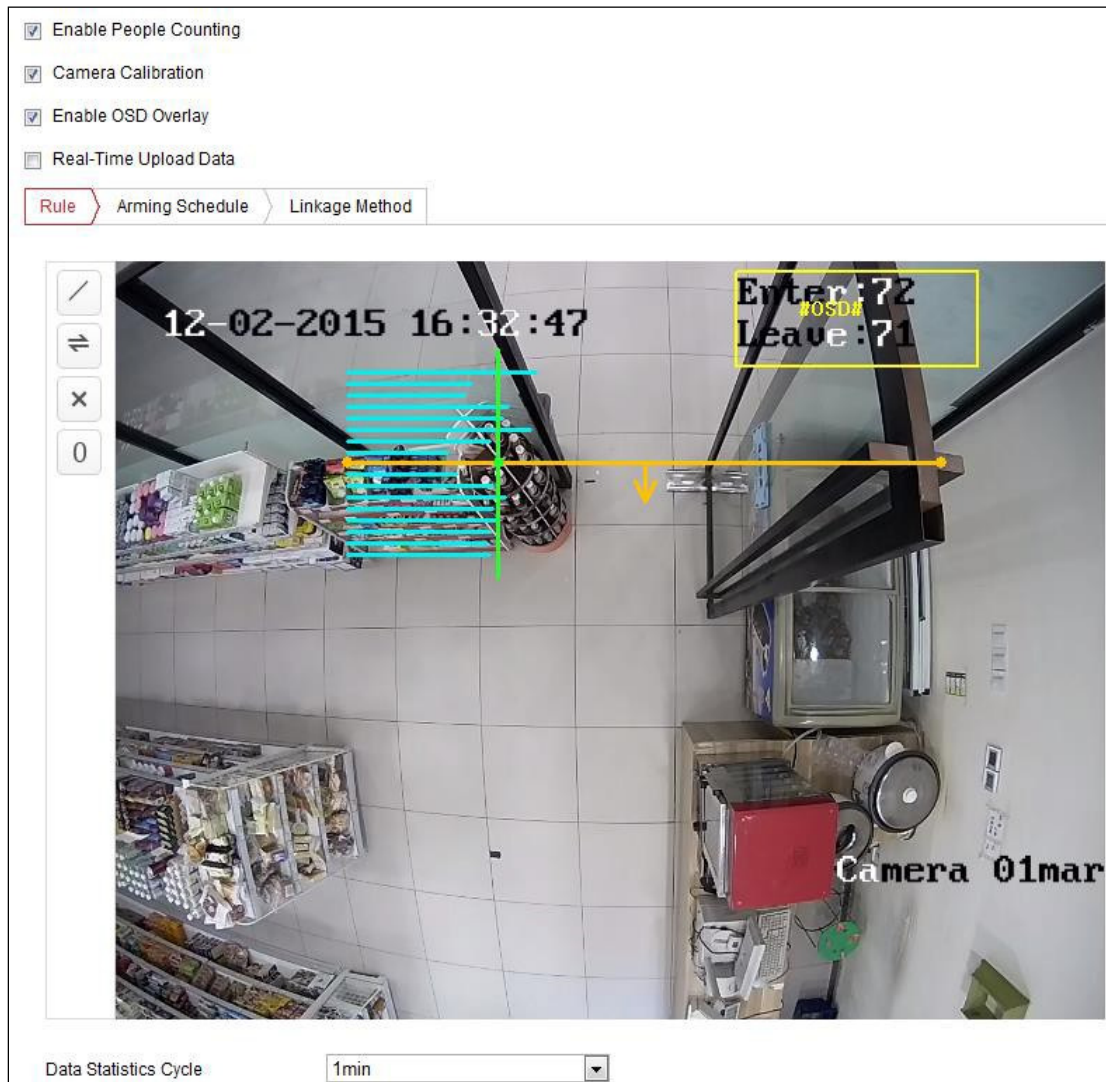



Figure 111, People Counting Configuration

2. Check the **Enable People Counting** checkbox to enable the function.
3. Set the detection line.


NOTE: An orange line, known as a detection line, can be set on the live video, and objects entering or exiting through the line will be detected and counted.


- 1) Click the  button on the left of the live view image. An orange line will appear on the image.
- 2) Drag the detection line to adjust its position.
- 3) Drag the yellow end points of the detection line to adjust its length.

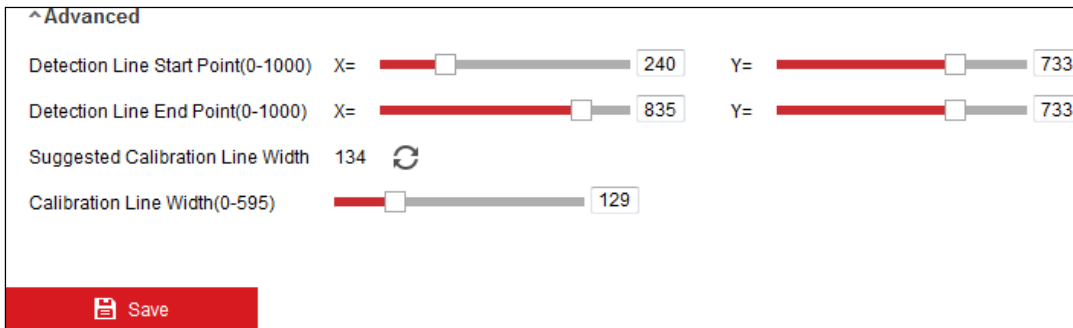
NOTE: The detection line should be drawn at the position right below the camera, and it should cover the entire entrance/exit.

Don't draw the line at a location where people may linger.

You can click  to delete the detection line.

You can click  to change the direction. The yellow arrow indicates the entering direction.

4. Check the **Camera Calibration** checkbox to enable camera calibration. A calibration line (the green vertical line) and several blue horizontal lines appear in the live view image.
 - **Camera Calibration:** You set the width (usually the shoulder breadth) of a person for counting. Well-set calibration parameters will help increase the counting accuracy.
 - **Blue Horizontal Lines:** One blue line indicates the detected width (usually the shoulder breadth) of a passing person. Up to eight blue lines can be shown on each side of the detection line. These lines are reference for calibration setting.
 - **Calibration Line (Green Vertical Line):** The distance from the left endpoint to the calibration line (calibration line width) indicates the set width of a person. You can drag the calibration line to adjust the distance according to the blue line distribution.
 - **Advanced:** You can precisely adjust the position and the size of detection line and calibration line.
 - 1) Drag the cursors or input values in the text fields to set the **Detection Line Start Point** and the **Detection Line End Point**.
 - 2) Click  to refresh the suggested calibration line width calculated by the system automatically.
 - 3) Drag the cursor or input a value to set the calibration. You can set the value as suggested, or set it according to your actual need.



The screenshot shows the 'Advanced' configuration panel for people counting. It contains four rows of settings, each with a slider and a numerical input field:

- Detection Line Start Point(0-1000):** X= 240, Y= 733
- Detection Line End Point(0-1000):** X= 835, Y= 733
- Suggested Calibration Line Width:** 134 (with a refresh icon)
- Calibration Line Width(0-595):** 129

A red 'Save' button is located at the bottom left of the panel.

Figure 112, People Counting Configuration – Advanced

5. Counting data setting and display.
 - 1) Check the **Enable OSD Overlay** checkbox, and the real-time number of people entering and exiting is displayed on the live video.
 - 2) You can drag the OSD text frame to adjust its position according to actual needs.
 - 3) If you need to upload the real-time counting data, check the **Real-Time Upload Data** checkbox.
 - 4) If you want to set the counting cycle manually, select the desired time period from the **Data Statistics Cycle** drop-down list.

- 5) To reset the counter, click the **0** button on the left of the live view image.
6. Click **Arming Schedule** to set the arming schedule. Refer to *Task 2: Set the Arming Schedule for Motion Detection* in *Section 10.1.1*.
7. Check the **Linkage Method** tab to select the linkage method. Refer to *Task 3: Set the Linkage Method for Motion Detection* in *Section 10.1.1*.
8. Click **Save** to save the settings.

NOTE: The people counting statistics will be calculated under the **Application** tab. Go to **Application** to check the people counting statistics.

10.3.4. Counting

The **Counting** function helps to calculate the number of people entering or exiting a configured area and is widely applied to entrances and exits.

As opposed to the **People Counting** function supported by an iDS camera, the **Counting** function needs no camera calibration.

NOTES: It is recommended to install the camera as directly above the entrance/exit as possible, and make sure it is horizontal to improve the counting accuracy.

1. Enter the **Counting Configuration** interface: **Configuration > Counting**.

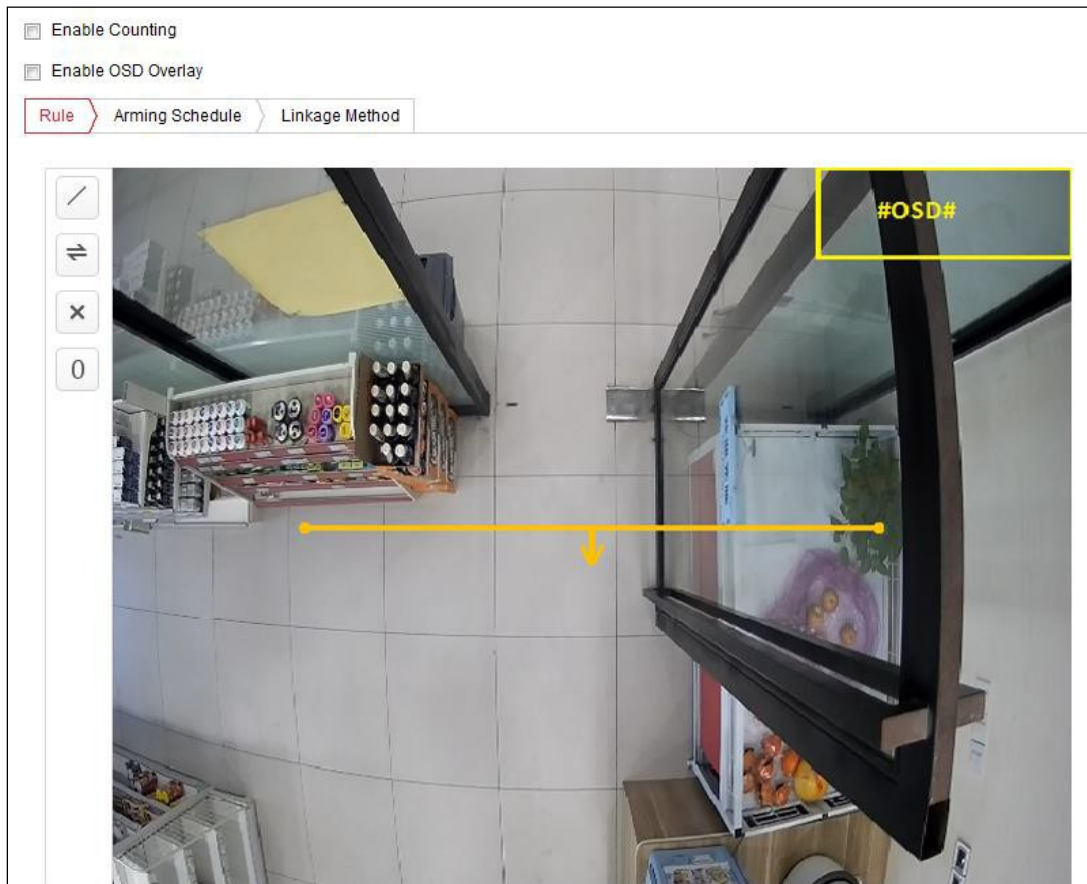





Figure 113, Counting Configuration

2. Check the **Enable Counting** checkbox to enable the function.
3. Check the **Enable OSD Overlay** checkbox, and the real-time number of people entering and exiting is displayed on the live video.
4. Set the detection line.

NOTE: An orange line, known as a detection line, can be set on the live video, and objects entering or exiting through the line will be detected and counted.

- 1) Click  to draw a detection line, and an orange detection line will appear on the image. Draw the detection line directly below the camera, and it should cover the entire entrance/exit. Draw the detection line in an area that doesn't have many people lingering.
- 2) Click-and-drag the detection line to adjust its position.
- 3) Click-and-drag the two end points of the detection line to adjust its length.
- 4) Click  delete the detection line.
- 5) Click  to change the direction.

5. Click the **0** button, and the number of people entering and exiting will be cleared to zero.

6. Click **Arming Schedule** to enter the arming schedule interface, and click-and-drag the mouse on the time bar to set the time.
7. Check **Linkage Method** tab to select the linkage method.
8. Click **Save** to save the settings.

NOTE: The counting statistics will be calculated under the **Application** tab. Go to **Application** to check the counting statistics.

10.3.5. Heat Map

Heat Map is a graphical representation of data represented by colors. The camera's **Heat Map** function is usually used to analyze the visit times and dwell times of customers in a configured area.

1. Enter the **Heat Map** configuration interface: **Configuration > Heat Map**.



Figure 114, Heat Map Configuration

2. Check the **Enable Heat Map** checkbox to enable the function.
3. Go to **Area Settings** to draw the detection area. Draw the area by left clicking the end-points in the live

view window, and right clicking to finish the area drawing. Up to eight areas are configurable.

NOTE: You can click **Select All** to select the whole live view window as the configured area, or click **Delete** to delete the current drawn area.

4. Configure the parameters for the drawn area.

- **Detection Sensitivity** [0–100]: The sensitivity of the camera to identify a target. Overly-high sensitivity may cause misinformation. It is recommended that you set the sensitivity at the default value of 50.
- **Background Update Rate** [0–100]: The speed a new scene replaces the previous scene. E.g., in front of a cabinet, people beside the cabinet will be double counted if the goods moved from the cabinet and the camera treats the cabinet (from which the good were removed) as a new scene. The default value of 50 is recommended.
- **Scene Change Level** [0–100]: The level of the camera response to the dynamic environment, e.g., a swaying curtain. The camera may treat the swaying curtain as a target. Setting the level properly will avoid misinformation. The default level is 50.
- **Minimum Target Size** [0–100]: The smallest size the camera identifies as a target. Set the target size according to the actual environment. The default size is 50.
- **Target Track:** Select **ON** or **OFF** to enable or disable tracking of the target.

5. Go to the **Arming Schedule** tab, and click-and-drag the mouse on the time bar to set the arming schedule.

6. Go to the **Linkage Method** tab, and select the linkage method by checking the **Notify the Surveillance Center** checkbox.

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

NOTE: The **Heat Map** statistics will be calculated under the **Application** tab. Go to **Application** to check the heat map statistics.

10.3.6. Road Traffic

Purpose

Vehicle Detection and **Mixed-Traffic Detection** are available for road traffic monitoring. In **Vehicle Detection**, a passing vehicle can be detected and a picture of its license plate can be captured; also, the vehicle color, vehicle logo, and other information can be recognized automatically. In **Mixed-Traffic Detection**, a pedestrian, motor vehicle, and non-motor vehicle can be detected, and the picture of the object (pedestrian/non-motor vehicle/motor vehicle without license plate) or license plate (motor vehicle with license plate) can be captured. You can send an alarm signal to notify the surveillance center and upload the captured picture to an FTP server.

NOTE: The **Road Traffic** function varies by camera model.

- **Detection Configuration**

1. Select the detection type from the list. **Vehicle Detection** and **Mixed-Traffic Detection** are selectable.

NOTE: Reboot the device to activate the new settings when switching the road traffic detection type.

2. Check the **Enable** checkbox to enable the selected detection function.
3. Select the lane number in the corresponding drop-down list. Up to four lanes are selectable.
4. Click-and-drag the lane line to set its position, or click-and-drag the line end to adjust the length and angle of the line.
5. Adjust the zoom ratio of the camera so that the size of the vehicle in the image is close to that of the red frame. Only the position of red frame is adjustable.

NOTE: Only one license plate can be captured at a time for each lane.

6. Select a **Province/State Abbreviation** in the drop-down list when the license plate attribution cannot be recognized.
7. Set the **Arming Schedule**.
 - 1) Click **Arming Schedule** to enter the arming schedule interface.
 - 2) Click on the time bar and drag the mouse to select the time period. Click **Delete** or **Delete All** to delete the configured schedule.
 - 3) Move the mouse to the end of each day, and a copy dialogue box pops up. You can copy the current settings to other days.
 - 4) Click **Save** to save the settings.

NOTE: The time of each period cannot overlap. Up to eight periods can be configured for each day.

8. Set the linkage method. **Notify Surveillance Center** and **Upload to FTP/Memory Card/NAS** are selectable.
 - **Notify Surveillance Center:** Send an exception or alarm signal to remote management software when an event occurs.
 - **Upload to FTP/Memory Card/NAS:** Capture the image when an alarm is triggered, upload the picture to an FTP server, and save the picture on the local SD card or connected NAS.
9. Click the **Save** button to activate the settings.

10.3.7. Queue Management

Queue Management detects the number of people queuing-up and the waiting time of each person.

The camera also generates reports to compare the efficiency of different queuing-ups and display the

changing status of one queue.

To use the function, set up detection rules first. To see the statistics of queue management, go to **Application**.

NOTE: **Queue Management** is supported only by certain camera models.

Rule Settings

The camera supports **Regional People Queuing-Up** and **Waiting Time Detection**. Check the appropriate checkbox to enable the desired function.

- **Regional People Queuing-Up:** Detects and calculates the number of people queuing-up in defined regions, and triggers alarms when the people number exceeds the set thresholds.
- **Waiting Time Detection:** Detects and calculates the waiting time of each person that enters the detection area, and trigger alarms when the waiting time exceeds the set thresholds.

1. Area Settings.

- **Add a region.** A region is the defined area in which the detections are active. When drawing the regions, note that a valid region-entering action of a target is that his/her head and shoulder enter the region.

(1) Click **Add Region**.

(2) (Optional) Select a color for the region from the color drop-down list.

(3) Draw a region by right clicking to determine the region boundary. Up to 10 edges are supported for a region.

- **Move the region:** Select and drag the region.
- **Adjust the region boundary:** Select the region and drag the endpoint of the region edge.
- **Delete the region:** Select the region and click **Delete**.


NOTE: Avoid overlapping regions.

A region should cover as much space as a queue may take.

Rule

Regional People Queuing-Up
 Waiting Time Detection

Area Settings | Arming Schedule | Linkage Method



Region: Region1
Region Name: Region1
Alarm Interval: 300 s

Regional People Queuing-Up Settings

OSD
Alarm Threshold: 5 persons
Alarm Interval: 300 s

Waiting Time Detection Settings

Alarm Threshold: 300 s

Add Region | Delete | Color:

Save

Figure 115, Queue Management – Rule Settings

- Set parameters for the added region.
 - (1) Set the region name and alarm interval.
 - **Region Name:** It will be displayed as OSD information.
 - **Alarm Interval:** In the set alarm interval, alarms of the same type trigger only one notification.
 - (2) Set people queuing-up settings.
 - Check OSD to display the region name and its real-time queuing-up people number.
 - **Alarm Threshold:** When the people number in the region exceeds the set threshold, an alarm is triggered.
 - (3) Set alarm threshold for waiting time detection. When waiting time of a person in the region exceeds the set value, an alarm is triggered.
 - Repeat above steps to set up other regions if needed. Up to three regions are supported.

2. **Arming Schedule.** Set the arming schedule for the function. In the armed periods, the function is active. Refer to *Task 2* in *Section 10.1.1*
3. **Linkage Method.** Set linkage method. For triggered alarm information, you can set the linkage action as a response to forward the information or trigger other actions. Refer to *Task 3* in *Section 10.1.1*

Chapter 11. Storage Settings

Before You Start

To configure record settings, make sure that you have the network storage device or local storage device configured.

11.1. Configuring Record Schedule

Purpose

There are two kinds of recording for the cameras: **Manual Recording** and **Scheduled Recording**. In this section, follow instructions to configure **Scheduled Recording**. By default, the record files of scheduled recording are stored in the local storage or in the network disk.

1. Enter the **Record Schedule Settings** interface: **Configuration > Storage > Schedule Settings > Record Schedule**.

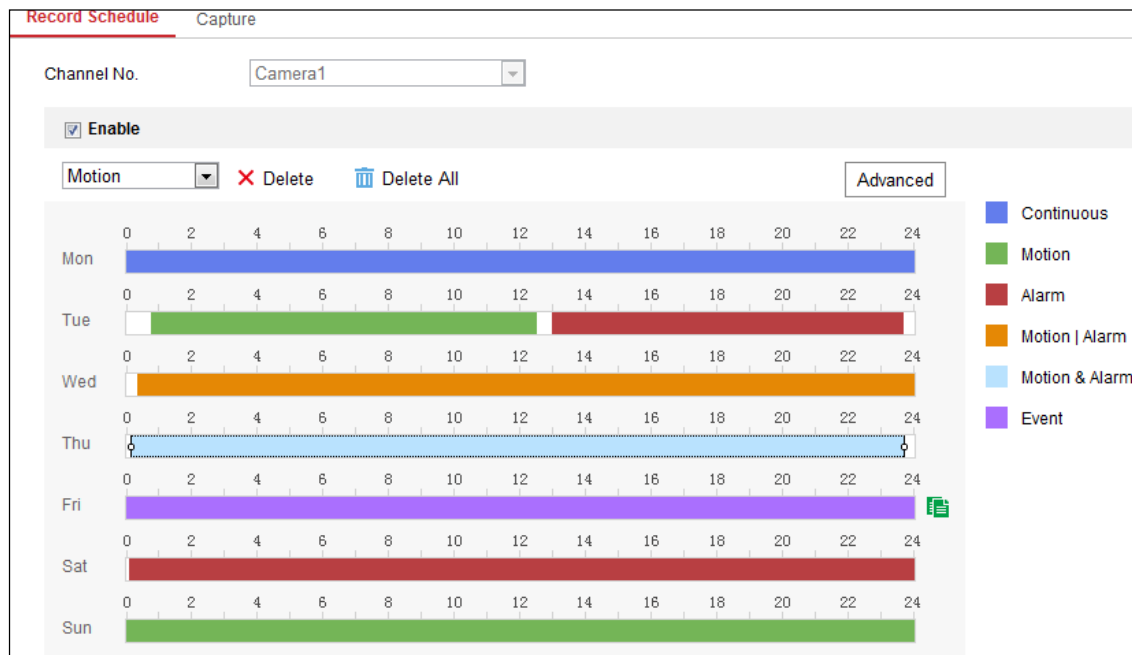


Figure 116, Recording Schedule Interface

2. Check the **Enable** checkbox to enable scheduled recording.
3. Click **Advanced** to set the camera record parameters.

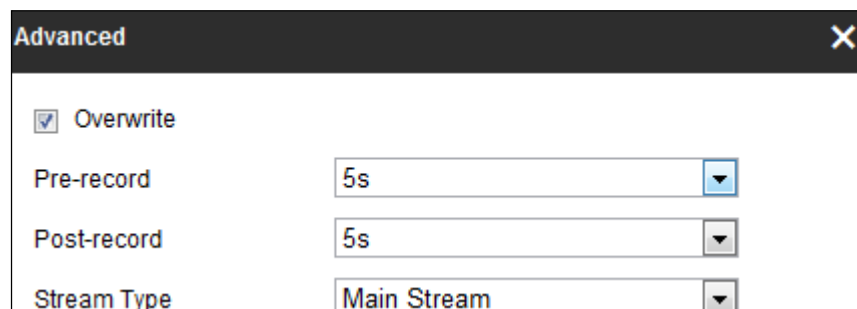


Figure 117, Record Parameters

- **Pre-Record:** The time you set to start recording before the scheduled time or event. For example, if an alarm triggers recording at 10:00, and the pre-record time is set as 5 seconds, the camera starts to record at 9:59:55.

The Pre-record time can be configured as **No Pre-record, 5s, 10s, 15s, 20s, 25s, 30s, or not limited.**

- **Post-Record:** The time you set to stop recording after the scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05.

The Post-record time can be configured as **5s, 10s, 30s, 1 min, 2 min, 5 min, or 10 min.**

- **Stream Type:** Select the stream type for recording.

NOTE: The **Record Parameter** configurations vary by camera model.

4. Select a **Record Type**. The record type can be **Continuous, Motion Detection, Alarm, Motion | Alarm, Motion & Alarm, and Event**.

- **Continuous:** The video will be recorded automatically according to the time of the schedule.
- **Record Triggered by Motion Detection:** The video will be recorded when motion is detected.

NOTE: Besides configuring the recording schedule, you have to set the motion detection area and check the **Trigger Channel** checkbox in the **Linkage Method of Motion Detection Settings** interface. For detailed information, refer to *Task 1: Set the Motion Detection Area* in *Section 10.1.1*.

- **Record Triggered by Alarm:** The video will be recorded when the alarm is triggered via an external alarm input channel.

NOTE: Besides configuring the recording schedule, you have to set the **Alarm Type** and check the **Trigger Channel** checkbox in the **Linkage Method of Alarm Input Settings** interface. For detailed information, refer to *Section 10.1.3*.

- **Record Triggered by Motion & Alarm:** The video will be recorded when the motion and alarm are triggered at the same time.

NOTE: Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. Refer to *Section 10.1.1* and *Section 10.1.3* for detailed information.

- **Record Triggered by Motion | Alarm:** The video will be recorded when an external alarm is triggered or motion is detected.

NOTE: Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. Refer to *Section 10.1.1* and *Section 10.1.3* for detailed information.

- **Record Triggered by Events:** The video will be recorded if any of the events is triggered. Besides configuring the recording schedule, you have to configure the event settings.

5. Select the record type, and click-and-drag the mouse on the time bar to set the record schedule.
6. Click **Save** to save the settings.

11.2. Configure Capture Schedule

Purpose

You can configure a **Scheduled Snapshot** and **Event-Triggered Snapshot**. The captured picture can be stored in the local storage or network storage.

1. Enter the **Capture Settings** interface: **Configuration > Storage > Storage Settings > Capture**.

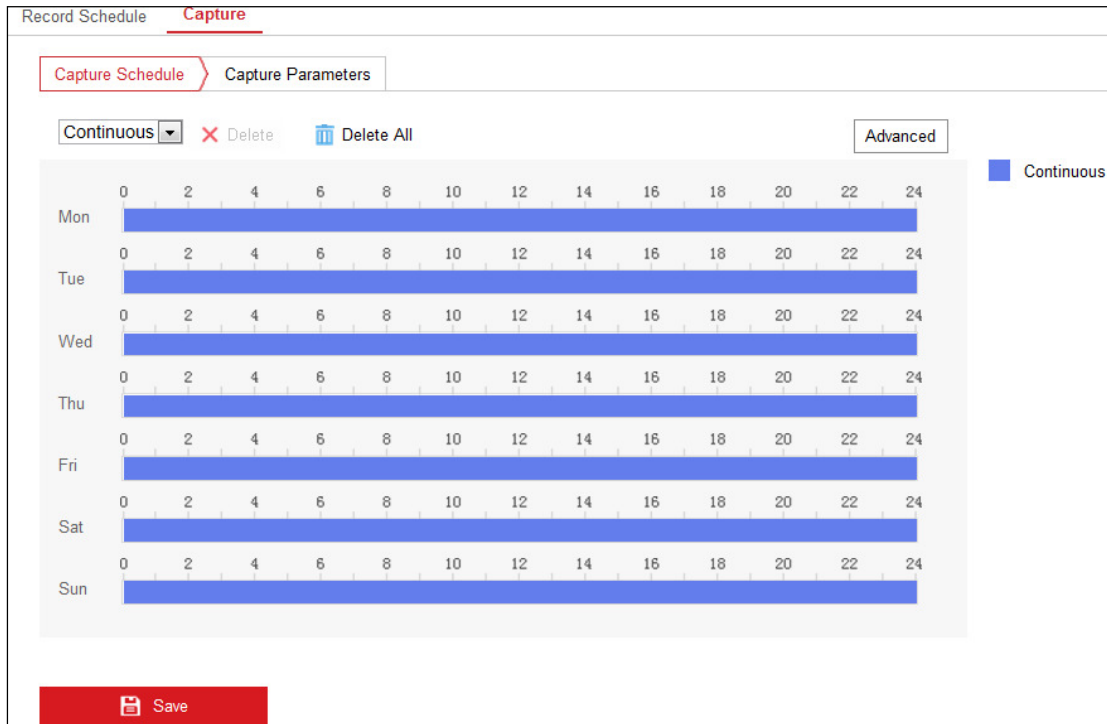


Figure 118, Capture Configuration

2. Go to the **Capture Schedule** tab to configure the capture schedule by clicking-and-dragging the mouse on the time bar. You can copy the record schedule to other days by clicking the green copy icon on the right of each time bar.
3. Click **Advanced** to select stream type.

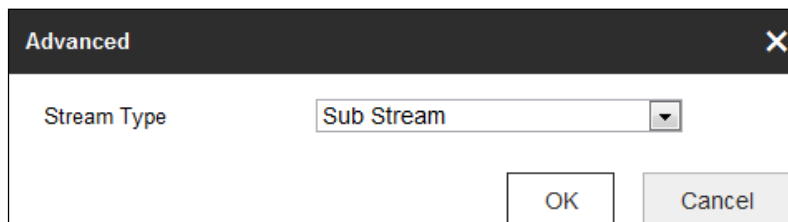


Figure 119, Advanced Setting of Capture Schedule

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

5. Go to the **Capture Parameters** tab to configure the capture parameters.
 - Check the **Enable Timing Snapshot** checkbox to enable continuous snapshot.
 - Select the picture format, resolution, quality, and capture interval.
 - Check the **Enable Event-triggered Snapshot** checkbox to enable event-triggered snapshot.
 - Select the picture format, resolution, quality, capture interval, and capture number.

The screenshot shows a web interface for configuring capture parameters. At the top, there are two tabs: 'Record Schedule' and 'Capture'. The 'Capture' tab is active, and within it, 'Capture Parameters' is selected. The interface is divided into two main sections: 'Timing' and 'Event-Triggered'. Both sections have a checked checkbox to enable snapshots. The 'Timing' section has settings for Format (JPEG), Resolution (704*576), Quality (High), and Interval (500 milliseconds). The 'Event-Triggered' section has the same settings for Format, Resolution, Quality, and Interval, plus a 'Capture Number' field set to 4. A red 'Save' button is located at the bottom of the form.

Figure 120, Set Capture Parameters

6. Set the time interval between two snapshots.
7. Click **Save** to save the settings.

11.2.1. Configuring Net HDD

Before You Start

The network disk should be available within the network and properly configured to store the recorded files, log files, pictures, etc.

1. Add Net HDD.

- 1) Enter the **Net HDD Settings** interface, **Configuration > Storage > Storage Management > Net HDD**.

HDD No.	Server Address	File Path	Type	Delete
1	10.10.36.61	/cxy_1	NAS	✘
2	10.10.36.252	/dvr/yanjian_1	NAS	✘
3			NAS	✘

Mounting Type: User Name: Password:

Figure 121, Add Network Disk

- 2) Enter the network disk IP address, and enter the file path.
- 3) Select the mounting type. **NFS** and **SMB/CIFS** are selectable. You can set the user name and password to guarantee the security if **SMB/CIFS** is selected.

NOTE: Refer to the *NAS User Manual* for creating the file path.



STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

- 4) Click **Save** to add the network disk.
2. Initialize the added network disk.
 - 1) Enter the **HDD Settings** interface, **Configuration > Storage > Storage Management > HDD Management**, where you can view the capacity, free space, status, type, and property of the disk.

HDD No.	Capacity	Free space	Status	Type	Property	Progress
9	9.84GB	0.00GB	Normal	NAS	R/W	
10	10.00GB	6.75GB	Normal	NAS	R/W	

Quota

Max. Picture Capacity:

Free Size for Picture:

Max. Record Capacity:

Free Size for Record:

Figure 122, Storage Management Interface

- 2) If the status of the disk is **Uninitialized**, check the corresponding checkbox to select the disk and click **Format** to start initializing the disk.
- 3) When the initialization completed, the disk status will become **Normal**.

HDD Management							Set	Format
<input checked="" type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress	
<input checked="" type="checkbox"/>	9	20.00GB	0.00GB	Formatting	NAS	R/W		

Figure 123, View Disk Status

3. Define the quota for records and pictures.
 - 1) Input the quota percentage for pictures and for records.
 - 2) Click **Save** and refresh the browser page to activate the settings.

Quota	
Max. Picture Capacity	<input type="text" value="4.75GB"/>
Free Size for Picture	<input type="text" value="4.75GB"/>
Max. Record Capacity	<input type="text" value="14.50GB"/>
Free Size for Record	<input type="text" value="14.50GB"/>
Percentage of Picture	<input type="text" value="25"/> %
Percentage of Record	<input type="text" value="75"/> %


 Save

Figure 124, Quota Settings

NOTE: Up to eight NAS disks can be connected to the camera.

11.3. Memory Card Detection

Purpose

With **Memory Card Detection**, you can view the memory card status, lock your memory card, and receive notification when your memory card is detected to be abnormal.

NOTE: The **Memory Card Detection** function is supported only by certain types of memory cards and camera models. If this tab page doesn't show on your Web page, it means either that your camera doesn't support the function or your installed memory card is not supported for this function. You can contact the dealer or the retailer for information of memory cards that support this function.

1. Enter the **Memory Card Detection** configuration interface, **Configuration > Storage > Storage Management > Memory Card Detection**.

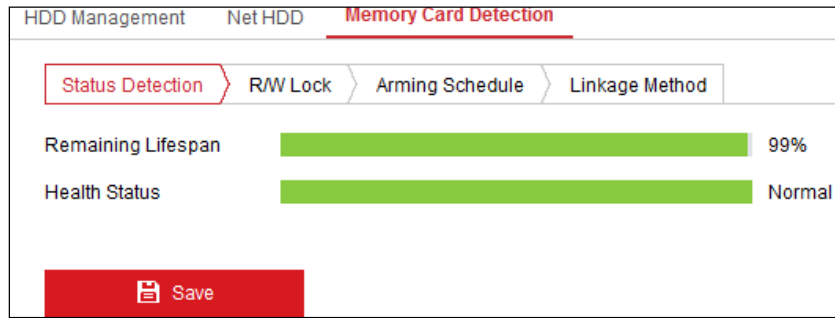


Figure 125, Memory Card Detection

2. View the memory card status on the **Status Detection** tab.

- **Remaining Lifespan:** Shows the percentage of remaining lifespan. The lifespan of a memory card may be influenced by factors such as its capacity and the bitrate. You need to change the memory card if the remaining lifespan is not enough.
- **Health Status:** Shows the condition of your memory card. There are three status descriptions, **good**, **bad**, and **damaged**. You will receive a notification if the health status is anything other than **good** when the **Arming Schedule** and **Linkage Method** are set.

NOTE: It is recommended that you change the memory card when the health status is other than "good."

3. Click the **R/W Lock** tab to add a lock to the memory card.

NOTE: With **R/W Lock** added, the memory card can be read and written to only when it is unlocked.

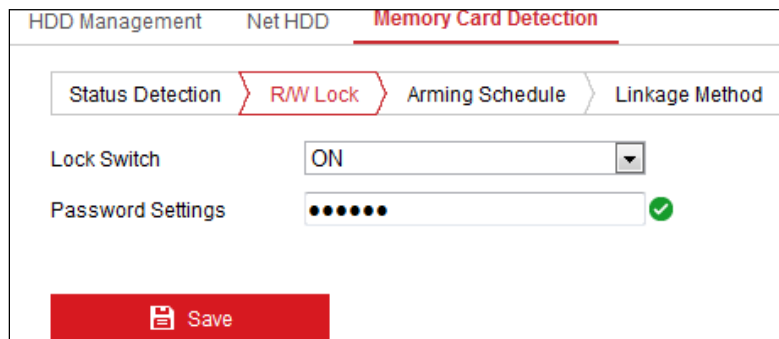


Figure 126, R/W Lock Setting

- **Add a Lock**

- (1) Select the **Lock Switch** to **ON**.
- (2) Input the password.
- (3) Click **Save** to save the settings.

- **Unlock**

- (1) If you use the memory card in the camera that locked it, unlocking will be done automatically and no unlocking procedures are required on the part of users.

- (2) If you use the memory card (with a lock) on a different camera, you can go to the **HDD Management** interface to unlock it manually. Select the memory card, and click the **Unlock** button next to the **Format** button. Then input the correct password to unlock it.

NOTES: The memory card can be read and written only if it is unlocked.

If the camera, which adds a lock to a memory card, is restored to the factory settings, you can go to the **HDD Management** interface to unlock the memory card.

- **Remove the Lock**

- (1) Set the **Lock Switch** to **OFF**.
 - (2) Input the correct password in the **Password Settings** text field.
 - (3) Click **Save** to save the settings.
4. Set the **Arming Schedule** and **Linkage Method** if you want to receive a notification when the memory card health status is anything other than good. Refer to *Task 2: Set the Arming Schedule for Motion Detection* and *Task 3: Set the Linkage Method for Motion Detection* in *Section 10.1.1*.
 5. Click **Save** to save the settings.

11.4. Configuring Lite Storage

Purpose

When there is no moving object in the monitored scene, the frame rate and bitrate of the video stream can be reduced to lengthen the storage time of the memory card.

NOTES: Lite Storage function varies by camera model.

The video files recorded in Lite Storage mode will be played back at full frame rate (25 fps/30 fps), and thus the playback appears speeded up.

1. Enter the **Lite Storage** interface, **Configuration > Storage > Storage Management > Lite Storage**.
2. Check the **Enable** checkbox to enable the **Lite Storage** function.
3. Input the storage time in the text field. You can view the available space of the SD card on the page.
4. Click **Save** to save the settings.

Chapter 12. Playback

This section explains how to view remotely recorded video files stored on network disks or SD cards.

1. Click **Playback** on the menu bar to enter the **Playback** interface.

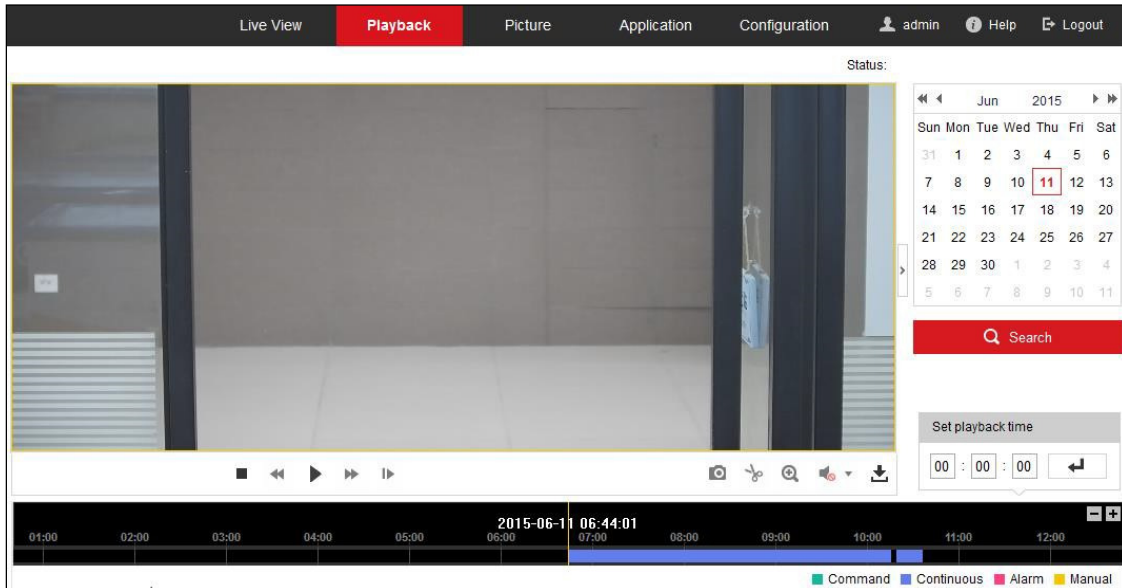


Figure 127, Playback Interface

2. Select the date and click **Search**.



Figure 128, Search Video

3. Click ► to play the video files found on this date.

NOTE: The toolbar on the bottom of the **Playback** interface can be used to control the playing process.



Figure 129, Playback Toolbar

Table 12-1 Button Descriptions

Button	Operation	Button	Operation
	Play		Capture a picture
	Pause		Start/Stop clipping video files
	Stop		Audio on and adjust volume/Mute
	Speed down		Download
	Speed up		Playback by frame
	Enable/disable digital zoom		

NOTE: You can choose the file paths locally for downloaded playback video files and pictures in the **Local Configuration** interface.

You can also input the time and click to locate the playback point in the **Set playback time** field. You can also click to zoom out/in the progress bar.

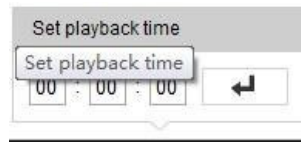


Figure 130, Set Playback Time

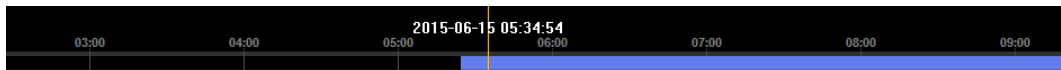


Figure 131, Progress Bar

The different colors of the video on the progress bar stand for the different video types.

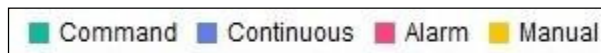


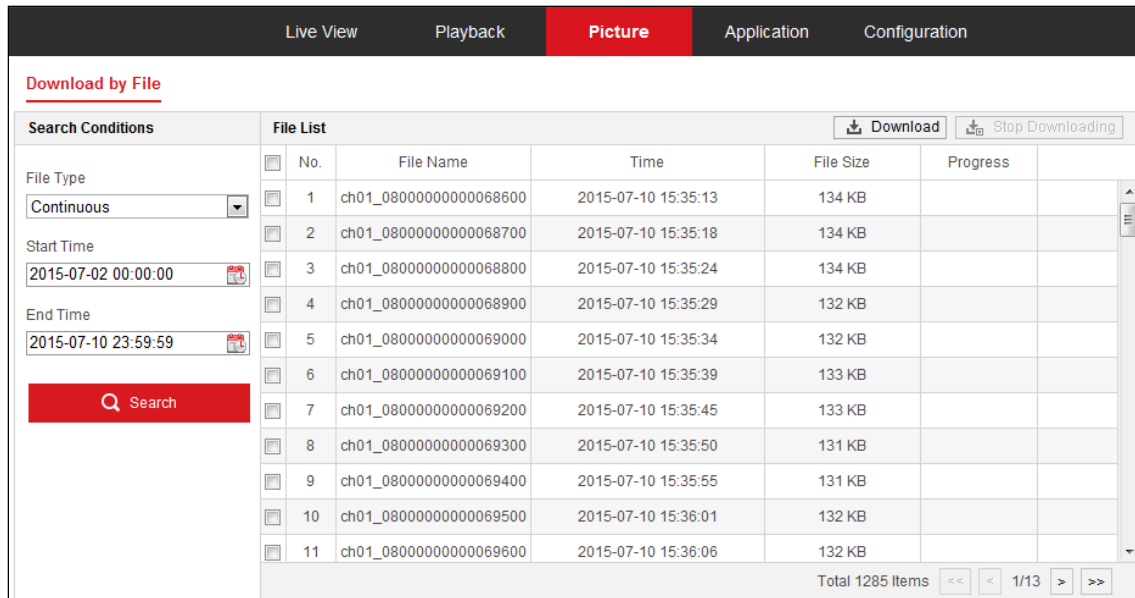
Figure 132, Video Types

Chapter 13. Picture

Click **Picture** to enter the **Picture Searching** interface. You can search, view, and download the pictures stored in the local storage or network storage.

NOTES: Make sure the HDD, NAS, or memory card are properly configured before you start the picture search.

Make sure the capture schedule is configured. Go to **Configuration > Storage > Schedule Settings > Capture** to set the capture schedule.



The screenshot shows the 'Picture' tab in the interface. On the left, under 'Search Conditions', there is a 'File Type' dropdown menu set to 'Continuous', 'Start Time' set to '2015-07-02 00:00:00', and 'End Time' set to '2015-07-10 23:59:59'. A red 'Search' button is located below these fields. On the right, the 'File List' table displays 11 items with columns for 'No.', 'File Name', 'Time', 'File Size', and 'Progress'. At the bottom right of the table, it indicates 'Total 1285 Items' with navigation arrows.

No.	File Name	Time	File Size	Progress
1	ch01_08000000000068600	2015-07-10 15:35:13	134 KB	
2	ch01_08000000000068700	2015-07-10 15:35:18	134 KB	
3	ch01_08000000000068800	2015-07-10 15:35:24	134 KB	
4	ch01_08000000000068900	2015-07-10 15:35:29	132 KB	
5	ch01_08000000000069000	2015-07-10 15:35:34	132 KB	
6	ch01_08000000000069100	2015-07-10 15:35:39	133 KB	
7	ch01_08000000000069200	2015-07-10 15:35:45	133 KB	
8	ch01_08000000000069300	2015-07-10 15:35:50	131 KB	
9	ch01_08000000000069400	2015-07-10 15:35:55	131 KB	
10	ch01_08000000000069500	2015-07-10 15:36:01	132 KB	
11	ch01_08000000000069600	2015-07-10 15:36:06	132 KB	

Figure 133, Picture Search Interface

1. Select the file type from the drop-down list. **Continuous, Motion, Alarm, Motion | Alarm, Motion & Alarm, Line Crossing, Intrusion Detection, and Scene Change Detection** are selectable.
2. Select the start time and end time.
3. Click **Search** to search for matched pictures.
4. Check the checkbox of the pictures, and then click **Download** to download the selected pictures.

NOTE: Up to 4000 pictures can be displayed at a time.

Chapter 14. Application

Click **Application** to enter the statistics counting interface. You can search, view, and download the counting data stored in the local storage or network storage.

NOTE: The **Application** function varies by camera model.

14.1. Face Capture Statistics

After you enable the **Face Capture** function, you can view and download the captured face data from the **Application** tab. To get more intuitive results, you can display the data in different charts.

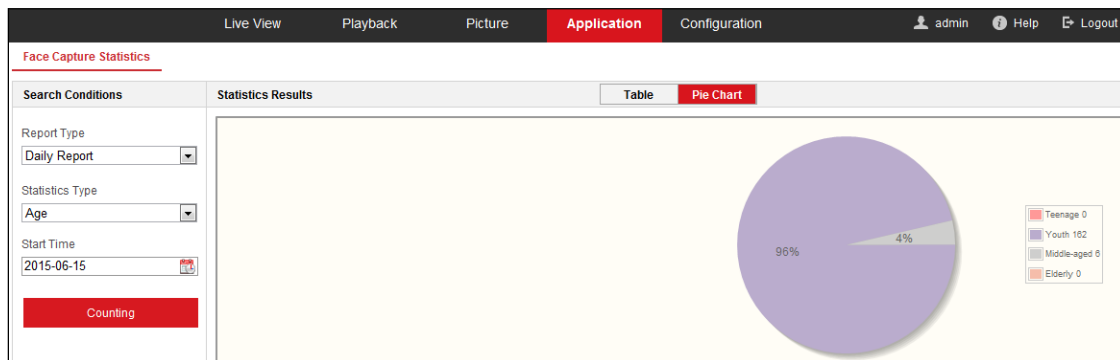


Figure 134, Application Interface

1. Select the report type. **Daily Report**, **Weekly Report**, **Monthly Report**, and **Annual Report** are selectable.
2. Select the statistics type.
3. Select the start time, and click **Counting**.

NOTE: The counting result displays in the statistic result area. Click **Table** or **Pie Chart** to display the result in different ways.

If you list the counting results in a table, you can export the data to a Microsoft Excel file.

14.2. People Counting Statistics

After you enable the **People Counting** function, you can view and download the people counting data from the **Application** tab. To get more intuitive results, you can display the data in different charts.

1. Select the report type. **Daily Report**, **Weekly Report**, **Monthly Report**, and **Annual Report** are selectable.

NOTE: **Daily Report** calculates the data on the date you select; **Weekly Report** calculates for the week your selected date belongs to; **Monthly Report** calculates for the month your selected date belongs to; and **Annual Report** calculates for the year your selected date belongs to.

2. Select the statistics type. **People Entered** and **People Exited** are selectable.
3. Select the start time, and click **Counting**.

NOTE: The counting result displays in the statistic result area. Click **Table**, **Bar Chart**, or **Line Chart** to

display the result in different way.

If you select table to display the statistics, there is an **Export** button to export the data to a Microsoft Excel file.

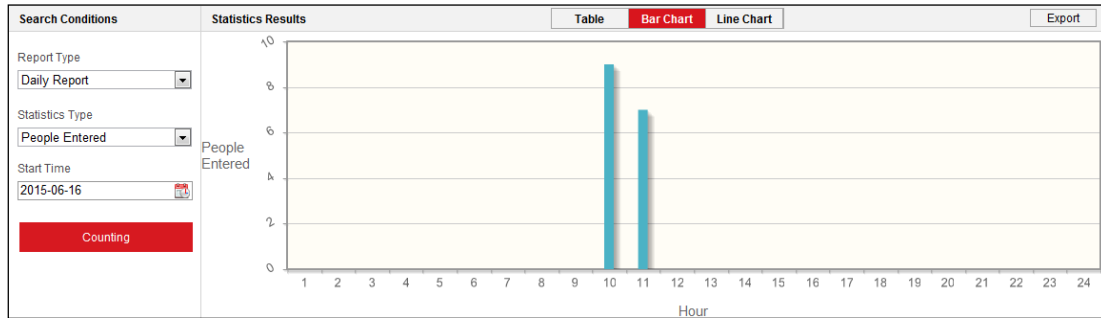


Figure 135, People Counting

14.3. Heat Map Statistics

After you enable the **Heat Map** function, you can view and download the heat map data from the **Application** tab. To get more intuitive results, you can display the data in different charts.

1. Select the report type. **Daily Report**, **Weekly Report**, **Monthly Report**, and **Annual Report** are selectable.

NOTE: **Daily Report** calculates the data on the date you selected; **Weekly Report** calculates for the week your selected date belongs to; **Monthly Report** calculates for the month your selected date belongs to; and **Annual Report** calculates for the year your selected date belongs to.

2. Select the start time, and click **Counting** to list the heat map data.
3. Select **Space Heat Map** or **Time Heat Map** to display the results.

NOTE: If you select the **Time Heat Map** to list the statistics, there is an **Export** button to export the data to a Microsoft Excel file.



Figure 136, Time Heat Map

NOTE: It is recommended that you do not adjust the electronic lens after the installation is completed, which may cause data inaccuracy to some degree.

14.4. Counting Statistics

After you enable the **Counting** function, you can view and download the counting data from the **Application** tab. To get more intuitive results, you can display the data in different charts.

1. Select the report type. **Daily Report**, **Weekly Report**, **Monthly Report**, and **Annual Report** are selectable.

NOTE: **Daily Report** calculates the data on the date you selected; **Weekly Report** calculates for the week your selected date belongs to; **Monthly Report** calculates for the month your selected date belongs to; and **Annual Report** calculates for the year your selected date belongs to.

2. Select the statistics type. People **Entered** and people **Exited** are selectable.
3. Select the start time, and click **Counting** to list the heat map data.
4. Select **Table**, **Bar Chart**, or **Line Chart** to display the results.

If you select **Table** to list the statistics, there is an **Export** button to export the data to a Microsoft Excel file.

14.5. Queue Management Statistics

Purpose

Queue Management supports data analysis and report output from multiple dimensions.

14.5.1. Commonly Used Data Analysis

- To see the number of queuing-up people of a certain waiting time level in a queue/region, use queuing-up time analysis, check a target region, and set a waiting time level.
- To compare the number of queuing-up people of a certain waiting time level in multiple queues/regions, use queuing-up time analysis, check target regions, and set a waiting time level.
- To compare the number of queuing-up people different waiting time levels in multiple queues/regions, use queuing-up time analysis, check target regions, and set waiting time levels.
- To see the time and duration that a queue stays a certain length in a queue/region, use queue status analysis, check a target region, and set a queue length level.
- To compare the time and duration that a queue stays a certain length in multiple queues/regions, use queue status analysis, check target regions, and set a queue length level.
- To compare the time and duration that a queue stays at different lengthd in multiple queues/regions, use queue status analysis, check target regions, and set queue length levels.

14.5.2. Queuing-Up Time Analysis

Purpose

Queuing-Up Time Analysis calculates the number of people of different waiting time levels. Regional comparison and multiple waiting time level comparison are supported.

1. Select Statistic Type.

- **Regional Comparison:** Compares the number of queuing-up people of different regions.

(1) Check one or more regions.

(2) Set waiting time level. Check desired time range radio button and input value.

EXAMPLE: If you want to see the number of people who wait longer than 10 minutes, check the third radio button, and input 600 in the corresponding text field.

- **Multi-Level Comparison:** Compares the number of queuing-up people of different waiting time levels.

(1) Check one or more regions.

(2) Set waiting time level. Check one or more desired time range checkboxes and input values.

EXAMPLE: If you want to compare the number of people who wait longer than 10 minutes and who wait shorter than 3 minutes, check the first and the third radio buttons and input 600 and 180 in the corresponding text fields.

2. Select **Report Type**. **Daily Report**, **Weekly Report**, **Monthly Report**, and **Custom** are supported.

3. Select **Statistics Time**.

4. Click **Counting** to generate report.
5. (Optional) Click **Export** in the upper right corner to export the data in desired format (.txt and .xls are selectable.).

14.5.3. Queue Status Analysis

Purpose

Queue Status Analysis calculates the time and duration that a queue stays a certain length. Regional comparison and multiple queue length level comparison are supported.

1. Select **Statistic Type**.
 - **Regional Comparison:** Compares the time and duration that a queue stays at a certain length in different regions.
 - (1) Check one or more regions.
 - (2) Set queue length level. Queue length here means the number of people in the region.

EXAMPLE: If you want to see how long the queue keeps more than 10 people in a region, check the third radio button and input 10 in the corresponding text field.
 - **Multi-Level Comparison:** Compares the time and duration of the queue at different queue length levels.
 - (1) Check one or more regions.
 - (2) Set the queue length level. Check one or more desired range checkboxes and input values.
2. Select **Report Type**. **Daily Report**, **Weekly Report**, **Monthly Report**, and **Custom** are supported.
3. Select **Statistics Time**.
4. Click **Counting** to generate the report.
5. (Optional) Click **Export** in the upper right corner to export the data in desired format (.txt and xls. are selectable).

14.5.4. Raw Data

Storage of Raw Data

Queue Management raw data is saved in the device's local storage.

With an on-board memory card installed, the device can save up to one month's data. With no memory card installed, the device can save only up to one week of data.

Raw Data Exporting

Raw data exporting of queue management is not available on a Web browser. For further analysis, you can get the data via RTSP protocol.

Chapter 15. Appendices

15.1. Appendix 1 SADP Software Introduction

Description of SADP

SADP (Search Active Devices Protocol) is a user-friendly and installation-free online device search tool. It searches the active online devices within your subnet and displays the information of the devices. You can also modify the basic network information of the devices using this software.

15.1.1. Search Active Devices Online

• Search Online Devices Automatically

After launching the SADP software, it automatically searches the online devices every 15 seconds from the subnet where your computer is located. It displays the total number and information of the searched devices in the **Online Devices** interface. Device information including the device type, IP address, port number, etc. will be displayed.

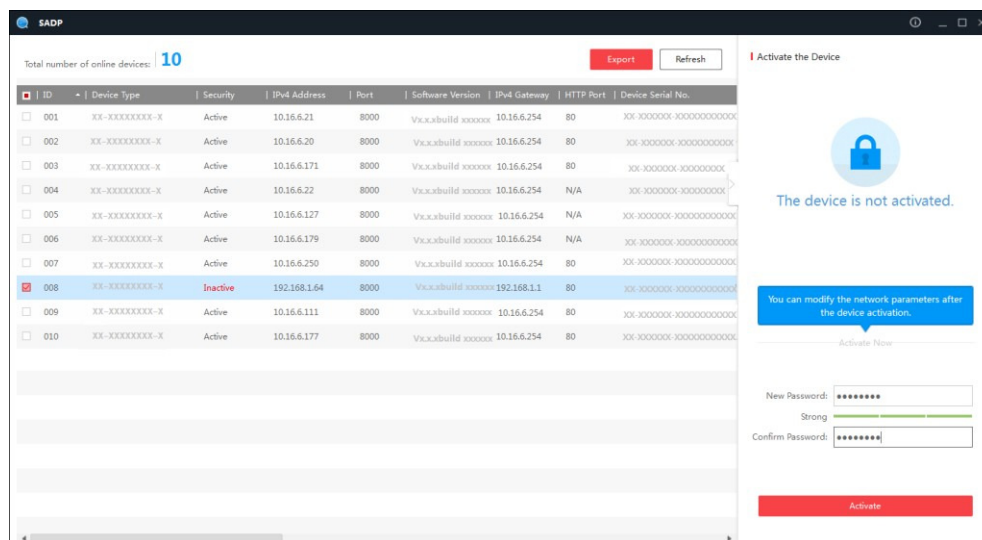


Figure 137, Searching Online Devices

NOTE: A device can be found and displayed on the list 15 seconds after it goes online; it will be removed from the list within 45 seconds after going offline.

• Search Online Devices Manually


You can also click to refresh the online device list manually. The newly found devices will be added to the list.

NOTE: You can click or on each column heading to order the information; you can click to expand the device table and hide the network parameter panel on the right side, or click to show the network parameter panel.

15.1.2. Modify Network Parameters

1. Select the device to be modified in the device list, and the device's network parameters will be

displayed in the **Modify Network Parameters** panel on the right side.

2. Edit the modifiable network parameters, e.g. IP address and port number.
3. Enter the device's admin account password in the **Admin Password** field, and click  to save the changes.



STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Modify Network Parameters

Enable DHCP
 Enable Hik-Connect

Device Serial No.: XX-XXXXXXXX-XXXXXXXXXXXXXXXXXX

IP Address: 192.168.1.64

Port: 8000

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Security Verification

Admin Password:

[Modify](#) [Forgot Password](#)

Figure 138, Modify Network Parameters

15.2. Appendix 2 Port Mapping

The following example settings are for a TP-LINK brand router (TL-WR641G). The settings will vary depending on the particular router used.

1. Select the **WAN Connection Type**, as shown below:

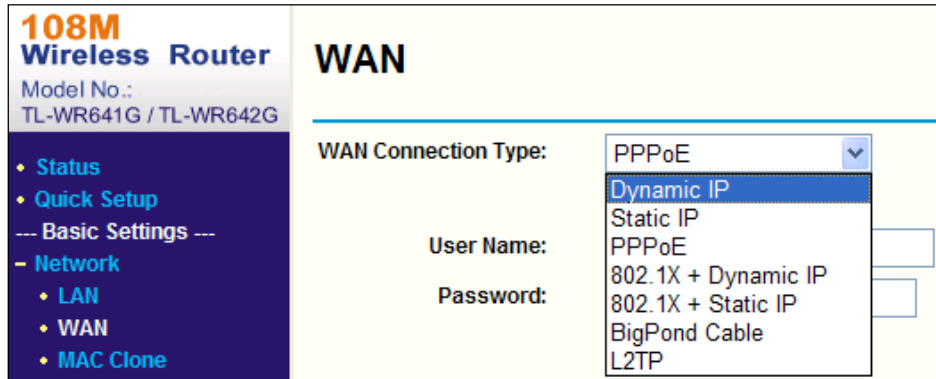


Figure 139, Select the WAN Connection Type

2. Set the router's **LAN** parameters as in the following figure, including IP address and subnet mask settings.

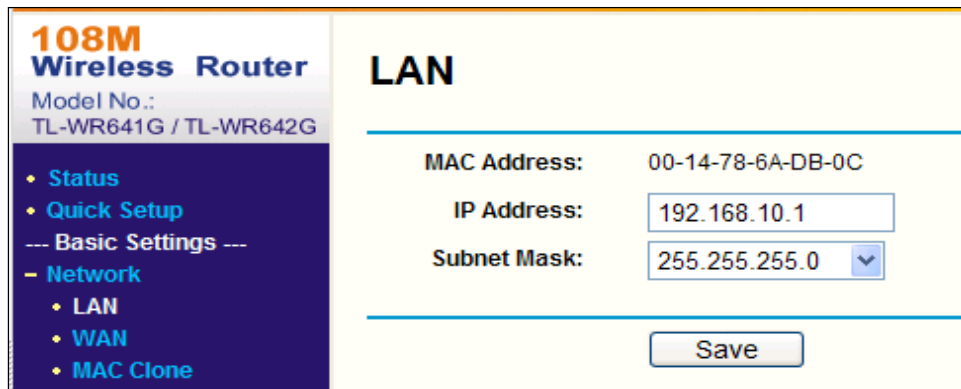


Figure 140, Set the LAN parameters

3. Set the port mapping in the **Forwarding** virtual servers. By default, the camera uses ports 80, 8000, and 554. You can change these port values with a Web browser or client software.

EXAMPLE: When the cameras are connected to the same router, you can configure the ports of a camera as 80, 8000, 554, and 8200 with IP address 192.168.1.23, and the ports of another camera as 81, 8001, 555 and 8201 with IP 192.168.1.24. Refer to the steps as below:

4. As the settings mentioned above, map ports 80, 8000, 554, and 8200 for the network camera at 192.168.1.23
5. Map ports 81, 8001, 555, and 8201 for the network camera at 192.168.1.24.
6. Enable **ALL** or **TCP** protocols.

7. Check the **Enable** checkbox and click **Save** to save the settings.

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	80	192.168.10.23	ALL	<input checked="" type="checkbox"/>
2	8000	192.168.10.23	ALL	<input checked="" type="checkbox"/>
3	554	192.168.10.23	ALL	<input checked="" type="checkbox"/>
4	8200	192.168.10.23	ALL	<input checked="" type="checkbox"/>
5	81	192.168.10.24	ALL	<input checked="" type="checkbox"/>
6	8001	192.168.10.24	ALL	<input checked="" type="checkbox"/>
7	555	192.168.10.24	ALL	<input checked="" type="checkbox"/>
8	8201	192.168.10.24	ALL	<input checked="" type="checkbox"/>

Common Service Port: DNS(53) Copy to ID 1

Previous Next Clear All Save

Figure 141, Port Mapping

NOTE: The network camera port cannot conflict with other ports. For example, some routers use Web management port 80. Change the camera port if it is the same as the management port.

