ANEXO II – MODELO DE PROPOSTA

Apresentamos nossa proposta para a prestação dos serviços/fornecimento dos produtos objeto da presente **DISPENSA DE LICITAÇÃO N° 09/2026** acatando todas as estipulações consignadas no respectivos Edital e seus anexos.

1. IDENTIFICAÇÃO DO CONCORRENTE

RAZÃO SOCIAL: **CATTO SEG LTDA**

CNPJ : **42.977.540/0001-70**

REPRESENTANTE E CARGO : **Thalles Camarotto Said -Sócio/Diretor Comercial**

ENDEREÇO: **Alameda Europa, 88 – 1° andar, sala 1, Tamboré – Santana de Parnáiba/SP**

TELEFONE E E-MAIL : **(11) 97543-5699 e -mail:thalles_said@hotmail.com**

BANCO: **033-Santander, Agência: 1229 – Conta: 13003390-9**

2. PROPOSTA

Item	Quantidade	Descrição	Valor de Referência
1	5 unidades	Câmera de reconhecimento facial (*)	**R$ 44.765,00**
2	1 unidade	Câmera PTZ 4MP zoom óptico 32x (*)	
3	3 unidades	Câmera LPR 4MP para leitura de placas veiculares até 120 km/h (*)	

(*) serviço de instalação/desinstalação incluso, considerando materias complementares tais como fios, conectores, switchs, etc. por conta da contratada.

DECLARO que a proposta apresentada atende todas as especificações exigidas neste **AVISO DE DISPENSA DE LICITAÇÃO N° 09/2026.**

DECLARO que o preço acima indicado contempla todos os custos diretos e indiretos referentes ao objeto ofertado.

3. CONDIÇÕES GERAIS

A proponente declara conhecer os termos do instrumento convocatório que rege a presente dispensa.

Santana de Parnaíba, 03 de fevereiro de 2026.

gov.br
Documento assinado digitalmente
THALLES CAMAROTTO SAID
Data: 04/02/2026 08:42:12-0300
Verifique em https://validar.iti.gov.br

CATTO SEG LTDA
Thalles Camarotto Said
Sócio/Diretor Comercial
RG: 33.294.867
CPF: 221.304.828-21

HIKVISION

Declaration of Conformity for RoHS Directive

Product Name:	ITS Products
Product Model:	iDS-TCM403-BI
Manufacturer:	Hangzhou Hikvision Digital Technology Co.,Ltd. No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China
Directives:	2011/65/EU and subsequent updates

The Product described above is in conformity with the relevant European Union harmonization legislation.

Sign for and on behalf of: Hangzhou Hikvision Digital Technology Co., Ltd.

Signature: Zhan Ye

Full Name: Zhan,Ye

Title: Global Certificaition Director, Hangzhou Hikvision Digital Technology Co., Ltd.

Date of Issue: 03/09/2024

Place: China

This declaration is issued under the sole responsibility of the manufacturer.

Document No.EU2025123100040

HIKVISION

Declaration of Conformity for RoHS Directive

Product Name: Project Network Cameras

Product Model: iDS-2CD7A46G2/LM-IZHS 2.8-12mm

Manufacturer: Hangzhou Hikvision Digital Technology Co.,Ltd.
No.555 Qianmo Road, Binjiang District, Hangzhou 310052,
China

Directives: 2011/65/EU and subsequent updates

The Product described above is in conformity with the relevant European Union harmonization legislation.

Sign for and on behalf of: Hangzhou Hikvision Digital Technology Co., Ltd.

Signature: Zhan Ye

Full Name: Zhan,Ye

Title: Global Certificaition Director, Hangzhou Hikvision Digital Technology Co., Ltd.

Date of Issue: 31/12/2025

Place: China

This declaration is issued under the sole responsibility of the manufacturer.

HIKVISION

Declaration of Conformity for RoHS Directive

Product Name:	PTZ Cameras
Product Model:	DS-2DE7A432IWG1-E
Manufacturer:	Hangzhou Hikvision Digital Technology Co.,Ltd. No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China
Directives:	2011/65/EU and subsequent updates

The Product described above is in conformity with the relevant European Union harmonization legislation.

Sign for and on behalf of: Hangzhou Hikvision Digital Technology Co., Ltd.

Signature: Zhan Ye

Full Name: Zhan,Ye

Title: Global Certificaition Director, Hangzhou Hikvision Digital Technology Co., Ltd.

Date of Issue: 26/09/2025

Place: China

This declaration is issued under the sole responsibility of the manufacturer.

República Federativa do Brasil
Agência Nacional de Telecomunicações

Certificado de Homologação

(Intransferível)

Nº **10491-24-10305**

Validade: **Indeterminada**

Emissão: **24/12/2024**

Requerente:
CNPJ: 15.431.830/0001-40
HIKVISION DO BRASIL COM DE EQUIP DE SEG LTDA

Fabricante:
HANGZHOU HIKVISION DIGITAL TECHNOLOGY CO., LTD.
NO. 555, QIANMO ROAD, BINJIANG DISTRICT
Nº

CHINA

Este documento homologa, nos termos da regulamentação de telecomunicações vigente, o Certificado de Conformidade nº CPQD 12056, emitido pelo **FUNDACAO CENTRO DE PESQUISA E DESENVOLVIMENTO DE TELECOMUNICACOES- CPQD.**. Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação de telecomunicações.

Tipo - Categoria:
Estação Terminal de Acesso - I

Modelo - Nome Comercial (s):
iDS-TCM403-BI /iDS-TCM203-BI /iDS-TCM803-BI /iDS-TCW403-BI /iDS-TCW803-BI

Características técnicas básicas:

Faixa de Frequências Tx (MHz)	Designação de Emissões	Tecnologia	Potência Máxima de Saída (W)	Tipo de Modulação
898,5 a 901,0	200KG7W	GPRS/EDGE	0,523	GMSK 8-PSK
824,0 a 849,0	200KG7W	GPRS/EDGE	0,492	GMSK 8-PSK
905,0 a 915,0	200KG7W	GPRS/EDGE	0,523	GMSK 8-PSK
1.710,0 a 1.785,0	200KG7W	GPRS/EDGE	0,294	GMSK 8-PSK
1.885,0 a 1.900,0	200KG7W	GPRS/EDGE	0,257	GMSK 8-PSK
824,0 a 849,0	5M00G7W	WCDMA/HSDPA/HSUPA	0,189	QPSK 16-QAM
898,5 a 901,0	5M00G7W	WCDMA/HSDPA/HSUPA	0,219	QPSK 16-QAM
905,0 a 915,0	5M00G7W	WCDMA/HSDPA/HSUPA	0,219	QPSK 16-QAM
1.885,0 a 1.900,0	5M00G7W	WCDMA/HSDPA/HSUPA	0,182	QPSK 16-QAM
1.920,0 a 1.980,0	5M00G7W	WCDMA/HSDPA/HSUPA	0,193	QPSK 16-QAM
703,0 a 748,0	3M00G7W - 5M00G7W – 10M0G7W - 15M0G7W - 20M0G7W	LTE	0,175	QPSK 16-QAM
824,0 a 849,0	1M40G7W – 3M00G7W - 5M00G7W - 10M0G7W	LTE	0,221	QPSK 16-QAM
898,5 a 901,0	1M40G7W – 3M00G7W - 5M00G7W - 10M0G7W	LTE	0,167	QPSK 16-QAM
905,0 a 915,0	1M40G7W – 3M00G7W - 5M00G7W - 10M0G7W	LTE	0,167	QPSK 16-QAM
1.710,0 a 1.785,0	1M40G7W - 3M00G7W - 5M00G7W	LTE	0,138	QPSK 16-QAM
1.710,0 a 1.785,0	10M0G7W - 15M0G7W - 20M0G7W	LTE	0,138	QPSK 16-QAM
1.895,0 a 1.900,0	1M40G7W - 3M00G7W - 5M00G7W	LTE	0,143	QPSK 16-QAM
1.895,0 a 1.900,0	10M0G7W - 15M0G7W - 20M0G7W	LTE	0,143	QPSK 16-QAM
1.920,0 a 1.980,0	5M00G7W – 10M0G7W - 15M0G7W - 20M0G7W	LTE	0,124	QPSK 16-QAM
2.300,0 a 2.400,0	5M00G7W – 10M0G7W - 15M0G7W - 20M0G7W	LTE	0,273	QPSK 16-QAM
2.500,0 a 2.570,0	5M00G7W – 10M0G7W - 15M0G7W - 20M0G7W	LTE	0,201	QPSK 16-QAM
2.570,0 a 2.620,0	5M00G7W – 10M0G7W - 15M0G7W - 20M0G7W	LTE	0,211	QPSK 16-QAM

- O produto possui protocolo IPv6.
- Interface: 1 RJ45.
- O requerente apresentou declaração em conformidade com os Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações.
- Ensaio de SAR não aplicável.

Na sua utilização o produto deve estar ajustado na(s) potência(s) e frequência(s) autorizadas pelo órgão técnico competente da Agência Nacional de Telecomunicações – Anatel.

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos da regulamentação de telecomunicações, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Davison Gonzaga da Silva
Gerente de Certificação e Numeração

HIKVISION

Network Speed Dome

User Manual

Initiatives on the Use of Video Products

Thank you for choosing Hikvision products.

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

Please read the following initiatives carefully:

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

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

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

Legal Information

About this Manual

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

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

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE

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

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

Contents

Chapter 1 Overview

1.1 Product Introduction

The Network Speed Dome is an integration of the HD zoom camera and the PT module, ideal for remote monitoring. The device is easy to install and operate. Through Ethernet control, the device is able to compress and transmit images to multiple users. With network attached storage (NAS), the device is able to store and retrieve data easily.

The device is well suited for HD monitoring in various places, such as rivers, forests, roads, railways, airports, ports, oil fields, posts, squares, parks, scenic areas, streets, stations, stadiums, residential blocks, libraries, shopping malls, hotels, government buildings, museums, and banks.

1.2 Key Function

The key functions of the device are as follows. Actual functions may vary for different models. You can enable the functions as you need.

Audio and Visual Alarm

The device supports flashing light alarm and audio alarm to warn intruders off.

Face Capture

The device captures human faces and uploads the pictures to the center.

Event Function

The device detects basic events and multiple smart events.

PTZ Function

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

1.3 System Requirement

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

	Recommended Specifications
Operating System	Microsoft Windows 7/ Windows 8/ Windows 10 Mac OS 10.13 or later
CPU	Intel® Pentium® IV 3.0 GHz or higher
RAM	1 GB or higher

	Recommended Specifications
Display	1024 × 768 resolution or higher
Web Browser	Internet Explorer 10 and above version, Apple Safari 12 and above version, Mozilla Firefox 52 and above version, Google Chrome 57 and above version.

Chapter 2 Device Activation and Accessing

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

Note

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

2.1 Activate Device

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

2.1.1 Activate Device via Web Browser

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

Before You Start

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

Steps

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

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

   Caution

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

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

   2) Change IP address.

   3) Save the settings.

2.1.2 Activate via SADP

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

Before You Start

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

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

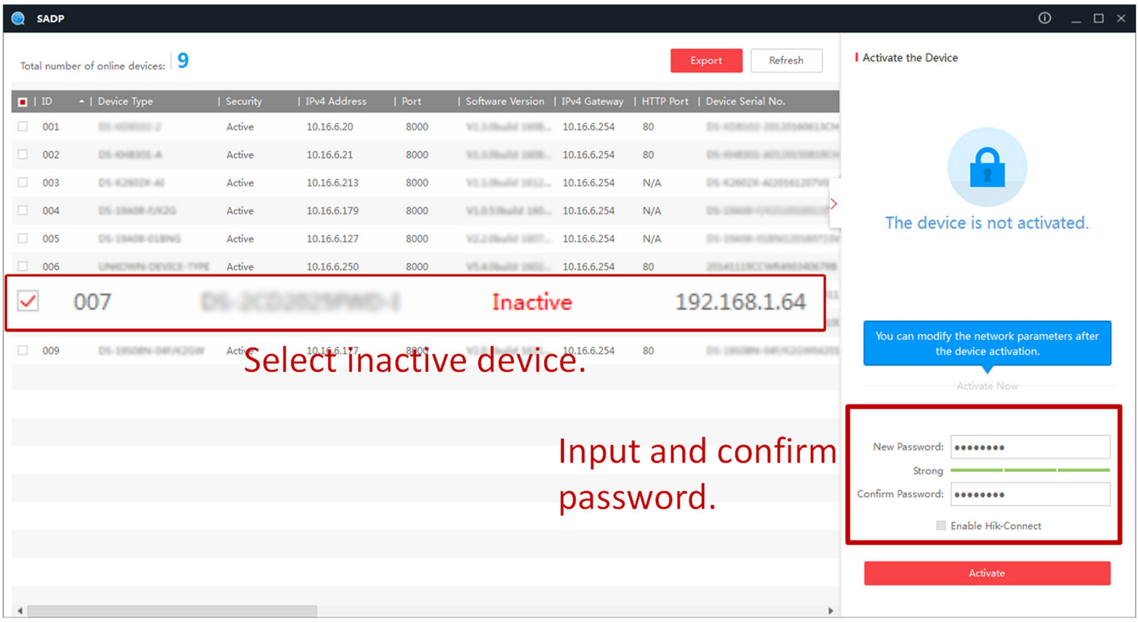
Steps

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

Caution

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

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



Total number of online devices: 9

☐ ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
☐ 001	[redacted]	Active	10.16.6.20	8000	[redacted]	10.16.6.254	80	[redacted]
☐ 002	[redacted]	Active	10.16.6.21	8000	[redacted]	10.16.6.254	80	[redacted]
☐ 003	[redacted]	Active	10.16.6.213	8000	[redacted]	10.16.6.254	N/A	[redacted]
☐ 004	[redacted]	Active	10.16.6.179	8000	[redacted]	10.16.6.254	N/A	[redacted]
☐ 005	[redacted]	Active	10.16.6.127	8000	[redacted]	10.16.6.254	N/A	[redacted]
☐ 006	[redacted]	Active	10.16.6.250	8000	[redacted]	10.16.6.254	80	[redacted]
☑ 007	[redacted]	Inactive	192.168.1.64					
☐ 009	[redacted]	Active	10.16.6.177	8000	[redacted]	10.16.6.254	80	[redacted]

Select inactive device.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

Activate Now

New Password: ••••••••

Strong

Confirm Password: ••••••••

☐ Enable Hik-Connect

Activate

Input and confirm password.

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

5. Modify IP address of the device.

   1) Select the device.

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

2.2 Access Device via Web Browser

Before You Start

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

Steps

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

Note

Illegal login lock is activated by default. If admin user performs seven failed password attempts (five attempts for user/operator), the IP address is blocked for 30 minutes.

If illegal login lock is not needed, go to **Configuration → System → Security → Security Service** to turn it off.

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

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

2.2.1 Plug-in Installation

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

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

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

Note

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

2.2.2 Admin Password Recovery

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

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

Note

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

Security Question

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

Email

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

2.2.3 Illegal Login Lock

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

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

Illegal Login Attempts

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

Locking Duration

The device releases the lock after the setting duration.

Chapter 3 Smart Function

3.1 Allocate VCA Resource

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

Steps

1. Go to **Open Platform → VCA Resource** .
2. Select desired VCA functions.
3. Save the settings.

Note

Certain VCA functions are mutually exclusive. When a certain function or functions are selected and saved, others will be hidden.

3.2 Set Camera Info

Customize specific information for the device. It may help identify a certain device when multiple devices are under management.

Go **Open Platform → General VCA Resource** to set **Camera No.** and **Camera Info**.

3.3 Face Capture

Face capture function detects faces and captures pictures. When the grading of the detected face exceeds an algorithm-defined value, the device captures the face and triggers linkage actions. Set up rule and parameters before using the function.

Note

- This function is only supported by certain device models.
- To enable this function, you may need to select **Face Capture** on **VCA Resource** page. See ***Allocate VCA Resource*** for details.

3.3.1 Set Auto Face Capture Rule

After setting the face capture rules and algorithm parameters, the device captures faces and triggers linkage actions automatically.

Steps

1. Go to **Open Platform → Face Capture → Rule** .

2. Check **Enable**.
3. Select a configuration mode.

    Normal One detection scene is allowed to set. The device captures face in the scene in set arming schedule.

    See ***Normal Mode Settings*** for details.

    Expert The device can patrol among the detection scenes and capture face images. Detection scenes and patrol schedule should be set in advance.

    See ***Expert Mode Settings*** for details.
4. Click **Save**.

What to do next

Go to **Picture** to search and view the captured pictures.
Go to **Smart Display** to see currently captured face pictures.

Normal Mode Settings

Steps

1. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

    Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
2. Use PTZ control panel or click 📍 to locate a scene with a face.
3. Click ⬡ , and draw a detection area on live image.
4. Input **Mounting Height** of the device.
5. Input or draw the min. pupil distance and the max. pupil distance.

    The **Min. Pupil Distance** and the **Max. Pupil Distance** are used to improve detection accuracy. Only targets whose pupil distance are between the maximum distance and the minimum distance trigger the capture.

    Click ▫ and □ to draw the distance on live image, or input values in the text fields of **Min. Pupil Distance** and **Max. Pupil Distance**.
6. Click **Save**.
7. Set arming schedule. See ***Set Arming Schedule*** .
8. Set linkage method. See ***Linkage Method Settings*** .

Expert Mode Settings

Steps

1. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.

2. Input **Mounting Height** of the device.
3. Set detection scenes and detection areas.
   1) Select a detection scene.
   2) Adjust the live image to a desired scene. You can use PTZ control buttons or click 📍 to locate a scene with a face.
   3) Click ⬡ , and draw a detection area on live image.
   4) Input or draw the min. pupil distance and the max. pupil distance.

      The **Min. Pupil Distance** and the **Max. Pupil Distance** are used to improve detection accuracy. Only targets whose pupil distance are between the maximum distance and the minimum distance trigger the capture.

      Click ▫ and □ to draw the distance on live image, or input values in the text fields of **Min. Pupil Distance** and **Max. Pupil Distance**.
   5) Click **Save**.
   6) Repeat above steps to set other detection scenes and areas.
4. Set patrol schedule.
   1) Click **Patrol Schedule**.
   2) Draw time bars as desired.
   3) Click a time bar and click **Configuration**.
   4) Edit patrol path and input dwell time for each detection scene.

+	Add a detection scene to the patrol path.
↓ ↑	Adjust the order of the scenes.
×	Delete the detection scene.

   5) Click **Save**.
5. Set linkage method. See ***Linkage Method Settings*** .

3.3.2 Operate Manual Face Capture

Capture the target face manually in live view image.

Steps

1. Click **Live View**.
2. Click ⛶ to start manual face capture.
3. Draw a frame to select the target face in live view image.

   The captured picture can be uploaded to the center.
4. Click the icon again to stop manual face capture.

3.3.3 Overlay and Capture

Choose to configure capture parameters and the information you want to display on stream and picture.

Display VCA Info. on Stream

Display smart information on stream, including the target and rules information.

Display Target Info. on Alarm Picture

Overlay the alarm picture with target information.

Target Picture Settings

You can set the face picture type by selecting **Custom**, **Head Shot**, **Half-Body Shot**, or **Full-Body Shot**. If you select **Custom**, you can define detailed picture width and height of a picture freely. If the captured pictures should have the same picture height, check **Fixed Value** and input desired picture height.

Background Picture Settings

Comparing to target picture, background picture is the scene image offers extra environmental information. You can set the background picture quality and resolution. If the background image need to be uploaded to surveillance center, check **Background Upload**.

Text Overlay

You can check desired items (Device No., Camera Info. and Capture Time) and adjust their order to display on captured pictures by ↓ ↑ .

See ***Set Camera Info*** to set **Device No.** and **Camera Info**.

3.3.4 Face Capture Algorithm Parameters

It is used to set and optimize the parameters of the algorithm library for face capture.

Face Capture Version

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

Restore Defaults

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

Capture Parameters

Best Shot

The device captures the target picture with the highest score after setting the parameters.

Capture Times

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

Capture Threshold

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

Remove Duplicated Faces

This function can filter out repeated captures of a face.

Similarity Threshold for Duplicates Removing

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

Duplicates Removing Library Grading Threshold

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

Duplicates Removing Library Update Time

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

Quick Shot

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

Quick Shot Threshold

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

Max. Capture Interval

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

Capture Times

It refers to the capture times that a face will be captured during its stay in the configured area. The device captures the target face according to the set times.

Face Exposure

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

Reference Brightness

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

Minimum Duration

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

Face Filtering

Face Filtering Time

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

3.4 Smart Display

This function displays real time pictures captured by smart functions and analyzes the target in real time.

Note

To use this function, your web browser version should be above IE11.0.9600.17843.

Live View Parameter

Icon	Function
📷	Capture a picture.
◉	Start or stop recording.
🔊	Adjust the volume of live view. Move the slider to right to turn up the volume and left to turn down the volume. Move to the left end to mute the live view.

Download Display Pictures

Click 🖼 and the device stores captured pictures to the browser cache. Hover the pointer over the icon to see the number of pictures in the cache. Click 🖼 again to download the pictures in a package.

Note

The browser cache has a limited size. The recommended number of pictures to download is no more than 200.

Layout

Click ⚙ and choose **Layout**. Check the display content you need to add it to the smart display page. When real-time analyze is selected, you can choose the contents you want to display.

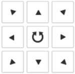
Chapter 4 PTZ

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

4.1 PTZ Control

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

PTZ Control Panel

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

Note

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

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

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

Zoom in/out

🔍+	Click the button, and the lens zooms in.
🔍−	Click the button, and the lens zooms out.

Note

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

Focus

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

Iris

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

4.2 Set Preset

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

Steps

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

   Note

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

4. Repeat the steps above to set multiple presets.

↷	Click the button to call the preset.
×	Click the button to delete the preset.

Note

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

What to do next

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

4.2.1 Special Presets

You can call the following presets with special demands to enable corresponding functions.

Preset No.	Function	Preset No.	Function
33	Auto flip	48	Alarm light off
34	Back to origin	92	Set manual limits
35	Call patrol 1	93	Save manual limits
36	Call patrol 2	94	Remote reboot
37	Call patrol 3	95	Call OSD menu
38	Call patrol 4	96	Stop a scan
39	Day mode	97	Start random scan
40	Night mode	98	Start frame scan
41	Call pattern 1	99	Start auto scan
42	Call pattern 2	100	Start tilt scan
43	Call pattern 3	101	Start panorama scan
44	Call pattern 4	102	Call patrol 5
45	One-touch patrol	103	Call patrol 6
46	Day/Night Mode	104	Call patrol 7
47	Alarm light on	105	Call patrol 8

4.3 Set Patrol Scan

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

Before You Start

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

Steps

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

   Preset

   Select predefined preset.

   Speed

   Set the speed of moving from one preset to another.

   Time

It is the duration staying on one patrol point.

×	Delete the presets in patrol.
↓ ↑	Adjust the preset order.

Note

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

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

▶	Call the patrol.
■	Stop patroling.
×	Delete the patrol.
⚙	Set the patrol.

Note

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

4.3.1 Set One-Touch Patrol

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

Steps

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

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

4.4 Set Pattern Scan

The device can move as the recorded pattern.

Steps

Note

This function is only supported by certain models.

1. Click ❙ to show the PTZ control panel, and click ↗ .

2. Select one pattern scan path that needs to be set.
3. Click ◉ to start recording pattern scan.
4. Click PTZ control buttons as demands.

Note

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

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

   ■ Stop pattern scan.

   ◉ Reset pattern scan path.

   × Delete the selected pattern scan.

Note

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

4.5 Set Limit

The device can only move within the limited range.

Steps

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

   Manual Stops

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

   Scan Stops

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

Note

Scan limit is only supported by the device that has scan function.

3. Click **Set** and set limits according to the prompt on the live image.
4. **Optional:** Click **Clear** to clear the limit settings of the selected mode.
5. Click **Save**.
6. Check **Enable Limit**.

Note

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

Result

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

4.6 Set Initial Position

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

Steps

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

   Call The device moves to the set initial position.

   Clear Clear the set initial position.

4.7 Set Scheduled Tasks

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

Steps

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

Note

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

4.8 Set Park Action

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

Before You Start

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

Steps

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

   When the action type is patrol, action type ID stands for patrol No. When the action type is preset, action type ID stands for preset No.
6. Click **Save**.

4.8.1 Set One-Touch Park

This function is used to start park instantly.

Steps

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

4.9 Set Privacy Mask

Privacy masks cover certain areas on the live image to protect personal privacy from being live viewed and recorded.

Steps

1. Go to **Configuration → PTZ → Privacy Mask** .
2. Adjust the live image to the target scene via PTZ control buttons.
3. Draw the area.

Draw Area	Click **Draw Area**, and click on the live view image to determine the boundary of the mask.
Stop Drawing	Click**Stop Drawing** after drawing the mask.

4. Click **Add**.

   It is listed in **Privacy Mask List**.
5. Edit **Name**, **Type**, and **Active Zoom Ratio** on your demand.

   Active Zoom Ratio

   When the actual zoom ratio is less than the set active zoom ratio, the set area can not be covered. When the actual zoom ratio is greater than the set active zoom ratio, the privacy mask is valid. The maximum value of active zoom ratio depends on the camera module.

Note

Active zoom ratio is only supported for the PTZ channel.

6. Repeat the steps above to set other privacy masks.
7. Check **Enable Privacy Masks**.

4.10 Set Device Position

Before You Start

Go to **Configuration → PTZ → Basic Settings → PTZ OSD** to enable **PT Status** display.
Use other direction indicating devices to find the North at the device location.

Steps

1. Go to **Configuration → PTZ → Position Settings** .
2. Manually set device direction by selecting the **PT Mode** as **Manual**.
   1) Adjust the tilt position of the device to 0 by controling the up arrow and down arrow on the PTZ panel.
   2) Adjust the pan position to show the live view of the north direction by controling the left arrow and right arrow on the PTZ panel.
   3) Click **Set as North**.
3. Input the longitude and latitude of the device manually.
4. Click **Save**.

What to do next

If you lost direction when operating the device, you can click **Point to North** to call the north position that is saved in the device.

4.11 Set Power Off Memory

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

Steps

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

4.12 Set PTZ Priority

The function can set the PTZ priority of different signals.

Steps

1. Go to **Configuration → PTZ → Prioritize PTZ** .
2. Set the priority signal and delayed time.

   Network

   The network signal controls the device with priority.

   RS-485

   The RS-485 signal controls the device with priority.

   Delay

   It refers to the time interval of PTZ operation controlled by different signals. When the operation with high priority is finished, the low priority signal controls the device after the setting interval.
3. Click **Save**.

4.13 Set Rapid Focus

Rapid focus is a function to reduce time of focusing comparing with that of normal focusing. To use the function, calibration should be done first. Rapid focus may not be supported by certain device models.

Steps

1. Go to **Configuration → PTZ → Rapid Focus** .
2. Add scenes for calibration.

   1) Adjust the live image to a desired scene via PTZ control buttons, and click **Add**.

   2) Set the **Rate** and the **Calibration Point Amount** of the added scene.

   Note

   More calibration points may increase calibration accuracy, but more focusing time is required. The default amount is recommended.
3. Select the scene to display the calibration line.

   A red line displays on live image.
4. Adjust the length and position of the line by dragging its two endpoints.

   Note

   The red line is recommended to stay in the center of the scene and to cover ground at the same time.

   Double click the image to enter full screen mode.
5. Click **Start Calibration**.

   Calibration status displays on the live image.
6. Repeat to add other scenes and complete the calibration.
7. Check **Enable Height Compensation** if the mounting height of the device is lower than 3 meters.
8. Check **Enable** after successful calibration.

9. Click **Save**.

Chapter 5 Live View

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

5.1 Live View Parameters

The supported functions vary depending on the model.

5.1.1 Start and Stop Live View

Click **Live View**. Click ▶ to start live view. Click ■ to stop live view.

5.1.2 Aspect Ratio

Aspect Ratio is the display ratio of the width to height of the image.

- 4:3 refers to 4:3 window size.
- 16:9 refers to 16:9 window size.
- 1× refers to original window size.
- ▣ refers to self-adaptive window size.
- ▣ refers to original ratio window size.

5.1.3 Live View Stream Type

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

5.1.4 Quick Set Live View

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

Steps

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

5.1.5 Select the Third-Party Plug-in

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

Steps

1. Click **Live View**.
2. Click to select the plug-in.
   - When you access the device via Internet Explorer, you can select Webcomponents or QuickTime.
   - When you access the device via the other browsers, you can select Webcomponents, QuickTime, VLC or MJPEG.

5.1.6 Start Digital Zoom

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

Steps

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

5.1.7 Conduct Regional Focus

You can enable the function to focus on certain area.

Steps

Note

This function varies with the device model.

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

5.1.8 Conduct Regional Exposure

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

Steps

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

3. Click to disable this function.

5.1.9 Count Pixel

It helps to get the height and width pixel of the selected region in the live view image.

Steps

1. Click to enable the function.
2. Drag the mouse on the image to select a desired rectangle area.
   The width pixel and height pixel are displayed on the bottom of the live view image.

5.1.10 Light

Click to turn on or turn off the illuminator.

5.1.11 Lens Initialization

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

You can initialize the lens in two ways:

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

5.1.12 Track Manually

In live view, manually select a target for the device to track.

Note

The function may not be supported by certain device models.

Steps

1. Click on the toolbar of the live view page.
2. Click a moving object in the live image.
   The device tracks the target and keeps it in the center of live view image.

5.1.13 Conduct 3D Positioning

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

Steps

1. Click to enable the function.

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

5.2 Set Transmission Parameters

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

Steps

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

Protocol

TCP

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

UDP

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

MULTICAST

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

Note

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

HTTP

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

Play Performance

Shortest Delay

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

Balanced

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

Fluent

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

Custom

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

3. Click **OK**.

Chapter 6 Video and Audio

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

6.1 Video Settings

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

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

6.1.1 Stream Type

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

Main Stream

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

Sub Stream

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

Other Streams

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

6.1.2 Video Type

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

Video

Only video content is contained in the stream.

Video & Audio

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

6.1.3 Resolution

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

6.1.4 Bitrate Type and Max. Bitrate

Constant Bitrate

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

Variable Bitrate

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

6.1.5 Video Quality

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

6.1.6 Frame Rate

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

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

6.1.7 Video Encoding

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

Note

Available compression standards vary according to device models.

H.264

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

H.264+

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

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

Note

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

H.265

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

H.265+

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

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

Note

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

MJPEG

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

6.1.8 Profile

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

6.1.9 I-Frame Interval

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

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

6.1.10 SVC

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

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

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

6.1.11 Smoothing

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

6.2 Audio Settings

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

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

6.2.1 Audio Input

If a built-in microphone or an external audio pick-up device is available, audio encoding, audio input mode and input volume are configurable.

Audio Encoding

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

Audio Input

Select **MicIn** for the built-in microphone, and **LineIn** for external audio pick-up device.

Note

MicIn is only supported by certain models.

Input volume

Adjust the volume of the audio input.

6.2.2 Audio Output

You can output audio through built-in speaker or line out. You can adjust the output volume according to your need.

Note

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

6.2.3 Environmental Noise Filter

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

6.3 Two-way Audio

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

Before You Start

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

Steps

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

6.4 ROI

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

6.4.1 Set ROI

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

Before You Start

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

Steps

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

   Note

   Select the fixed region that needs to be adjusted and drag the mouse to adjust its position.
5. Input the **Region Name** and **ROI Level**.
6. Click **Save**.

   Note

   The higher the ROI level is, the clearer the image of the detected region is.
7. **Optional:** Select other region No. and repeat the above steps if you need to draw multiple fixed regions.

6.5 Display Info. on Stream

The information of the objects (e.g. human, vehicle, etc.) is marked in the video stream. You can set rules on the connected rear-end device or client software to detect the events including line crossing, intrusion, etc.

Before You Start

This function is supported in smart events. Go to the **VCA Resource** page to enable **Smart Event**.

Steps

1. Go to **Configuration → Video/Audio → Display Info. on Stream** .
2. Check **Enable Dual-VCA**.
3. Click **Save**.

6.6 Display Settings

It offers the parameter settings to adjust image features.

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

Click **Default** to restore settings.

6.6.1 Scene Mode

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

Image Adjustment

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

Exposure Settings

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

Exposure Mode

Auto

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

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

Iris Priority

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

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

Shutter Priority

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

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

Manual

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

Slow Shutter

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

Focus

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

Focus Mode

Auto

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

Semi-auto

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

Manual

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

Min. Focus Distance

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

Day/Night Switch

Day/Night Switch function can provide color images in the day mode and black/white images in the night mode. Switch mode is configurable.

Day

The image is always in color.

Night

The image is always black/white

Auto

The camera switches between the day mode and the night mode according to the illumination automatically.

Scheduled-Switch

Set the **Start Time** and the **End Time** to define the duration for day mode.

Note

Day/Night Switch function varies according to models.

Set Supplement Light

Steps

1. Go to **Configuration → Maintenance → System Service** .
2. Check **Enable Supplement Light**.
3. Click **Save**.
4. Go to **Configuration → Image → Display Settings → Day/Night Switch** to set supplement light parameters.

   Smart Supplement Light

   This feature uses smart image processing technology to reduce overexposure caused by supplement light.

   IR Light Mode

   When the mode is set to **Auto**, the supplement light is automatically turned in or off according to the image brightness.

   Brightness Limit

   Adjust the upper limit of supplement light power.

BLC

If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC (backlight compensation) compensates light to the object in the front to make it clear. If BLC mode is set as **Custom**, you can draw a red rectangle on the live view image as the BLC area.

HLC

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

WDR

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

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

Note

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

DNR

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

Normal

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

Expert

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

White Balance

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

Defog

You can enable the defog function when the environment is foggy and the image is misty. It enhances the subtle details so that the image appears clearer.

EIS

Increase the stability of video image by using jitter compensation technology.

6.6.2 Image Parameters Switch

The device automatically switches image parameters in set time periods.

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

Set Scheduled-switch

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

Steps

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

   Note

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

Set Link to Preset

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

Steps

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

6.6.3 Mirror

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

Select the mirror mode as needed.

Note

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

6.6.4 Video Standard

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

6.7 OSD

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

Go to OSD setting page: **Configuration → Image → OSD Settings** . Set the corresponding parameters, and click **Save** to take effect.

Character Set

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

Displayed Information

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

Text Overlay

Set customized overlay text on image.

OSD Parameters

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

Chapter 7 Video Recording and Picture Capture

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

7.1 Storage Settings

This part introduces the configuration of several common storage paths.

7.1.1 Memory Card

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

Set New or Unencrypted Memory Card

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

Steps

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

   Note

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

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

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

   Note

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

6. Click **Save**.

Set Encrypted Memory Card

Before You Start

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

Steps

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

Note

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

3. Verify the encryption password.
   1) Click **Parity**.
   2) Enter the encryption password.
   3) Click **OK**.

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

Note

If the encryption password is forgotten and you still want to use this memory card, see ***Set New or Unencrypted Memory Card*** to format and set the memory card. All existing contents will be removed.

4. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.
5. Click **Save**.

Detect Memory Card Status

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

Before You Start

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

Steps

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

   Remaining Lifespan

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

Health Status

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

Note

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

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

Note

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

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

7.1.2 Set FTP

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

Before You Start
Get the FTP server address first.

Steps

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

   Server Address and Port

   The FTP server address and corresponding port.

   User Name and Password

   The FTP user should have the permission to upload pictures.

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

   Directory Structure

   The saving path of snapshots in the FTP server.

   Picture Filling Interval

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

   Picture Name

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

7.1.3 Set NAS

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

Before You Start

Get the IP address of the network disk first.

Steps

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

   Server Address

   The IP address of the network disk.

   File Path

   The saving path of network disk files.

   Mounting Type

Select file system protocol according to the operation system.

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

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

7.1.4 eMMC Protection

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

Note

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

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

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

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

7.1.5 Set Cloud Storage

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

Steps

Caution

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

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

Protocol Version	The protocol version of the cloud video manager.
Server IP	The IP address of the cloud video manager. It supports IPv4 address.
Serve Port	The port of the cloud video manager. You are recommended to use the default port.
AccessKey	The key to log in to the cloud video manager.
SecretKey	The key to encrypt the data stored in the cloud video manager.
User Name and Password	The user name and password of the cloud video manager.

Picture Storage Pool ID	The ID of the picture storage region in the cloud video manager. Make sure storage pool ID and the storage region ID are the same.

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

7.2 Video Recording

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

7.2.1 Record Automatically

This function can record video automatically during configured time periods.

Before You Start

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

Steps

1. Go to **Configuration → Storage → Schedule Settings → Record Schedule** .
2. Check **Enable**.
3. Select a record type.

Note

The record type is vary according to different models.

Continuous

The video will be recorded continuously according to the schedule.

Motion

When motion detection is enabled and trigger recording is selected as linkage method, object movement is recorded.

Alarm

When alarm input is enabled and trigger recording is selected as linkage method, the video is recorded after receiving alarm signal from external alarm input device.

Motion | Alarm

Video is recorded when motion is detected or alarm signal is received from the external alarm input device.

Motion & Alarm

Video is recorded only when motion is detected and alarm signal is received from the external alarm input device.

Event

The video is recorded when configured event is detected.

4. Set schedule for the selected record type. Refer to ***Set Arming Schedule*** for the setting operation.
5. Click **Advanced** to set the advanced settings.

Overwrite

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

Pre-record

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

Post-record

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

Stream Type

Select the stream type for recording.

Note

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

Recording Expiration

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

6. Click **Save**.

7.2.2 Record Manually

Steps

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

7.2.3 Playback and Download Video

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

Steps

1. Click **Playback**.
2. Set search condition and click **Search**.

   The matched video files showed on the timing bar.

3. Click ▶ to play the video files.
   - Click ✂ to clip video files.
   - Double click the live view image to play video files in full screen. Press **ESC** to exit full screen.

Note

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

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

   Note

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

7.3 Capture Configuration

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

7.3.1 Capture Automatically

This function can capture pictures automatically during configured time periods.

Before You Start

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

Steps

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

   Timing

   Capture a picture at the configured time interval.

   Event-Triggered

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

7.3.2 Capture Manually

Steps

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

   JPEG

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

   BMP

   The picture is compressed with good quality.
3. Click **Save**.
4. Click 📷 near the live view or play back window to capture a picture manually.

7.3.3 View and Download Picture

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

Steps

1. Click **Picture**.
2. Set search condition and click **Search**.

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

Note

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

Chapter 8 Event and Alarm

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

8.1 Basic Event

8.1.1 Set Motion Detection

This function detects moving objects in the detection region and triggers linkage actions.

Steps

Note

This function is not available when Smart Event is enabled.

1. Go to **Configuration → Event → Basic Event → Motion Detection** .
2. Check **Enable Motion Detection**.
3. **Optional:** Highlight moving objects in green.
   1) Check **Enable Dynamic Analysis for Motion**.
   2) Go to **Configuration → Local** to enable **Rules**.
4. Select **Configuration Mode**. Normal mode and expert mode are selectable.
   - For the information about normal mode, see ***Normal Mode*** .
   - For the information about expert mode, see ***Expert Mode*** .
5. Set the arming schedule. See ***Set Arming Schedule*** for details.
6. Set linkage methods. See ***Linkage Method Settings*** for details.
7. Click **Save**.

Normal Mode

You can set motion detection parameters according to the device default parameters.

Steps

1. Select normal mode in **Configuration**.
2. Set the sensitivity of normal mode. The higher the value of sensitivity is, the more sensitive the motion detection is. If the sensitivity is set to ***0***, motion detection and dynamic analysis do not take effect.
3. Click **Draw Area**. Click and drag the mouse on the live video, then release the mouse to finfish drawing one area.

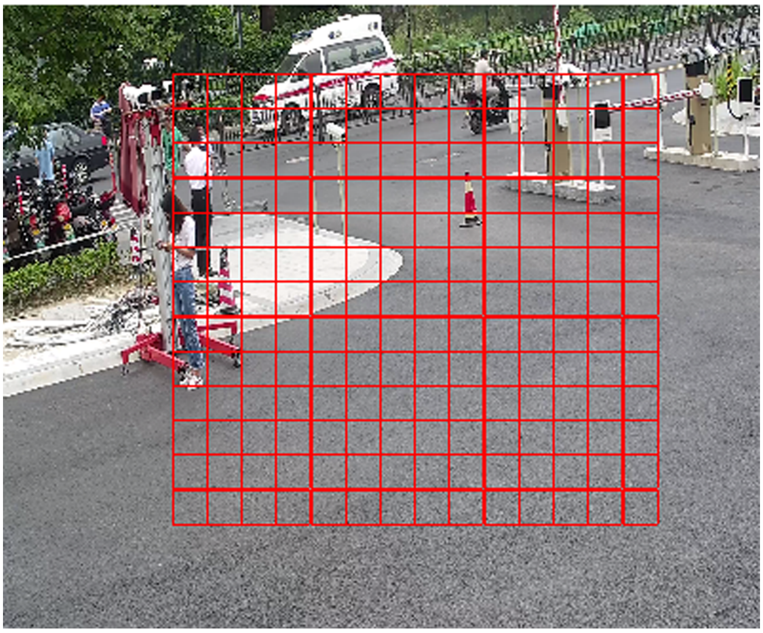


Figure 8-1 Set Rules

Stop Drawing Stop drawing one area.

Clear All Clear all the areas.

4. **Optional:** You can set the parameters of multiple areas by repeating the above steps.

Expert Mode

You can configure different motion detection parameters for day and night according to the actual needs.

Steps

1. Select **Expert Mode** in **Configuration**.
2. Set parameters of expert mode.

Scheduled Image Settings

OFF

Image switch is disabled.

Auto-Switch

The system switches day/night mode automatically according to environment. It displays colored image at day and black and white image at night.

Scheduled-Switch

The system switches day/night mode according to the schedule. It switches to day mode during the set periods and switches to night mode during the other periods.

Sensitivity

The higher the value of sensitivity is, the more sensitive the motion detection is. If scheduled image settings is enabled, the sensitivity of day and night can be set separately.

3. Select an **Area** and click **Draw Area**. Click and drag the mouse on the live image and then release the mouse to finish drawing one area.

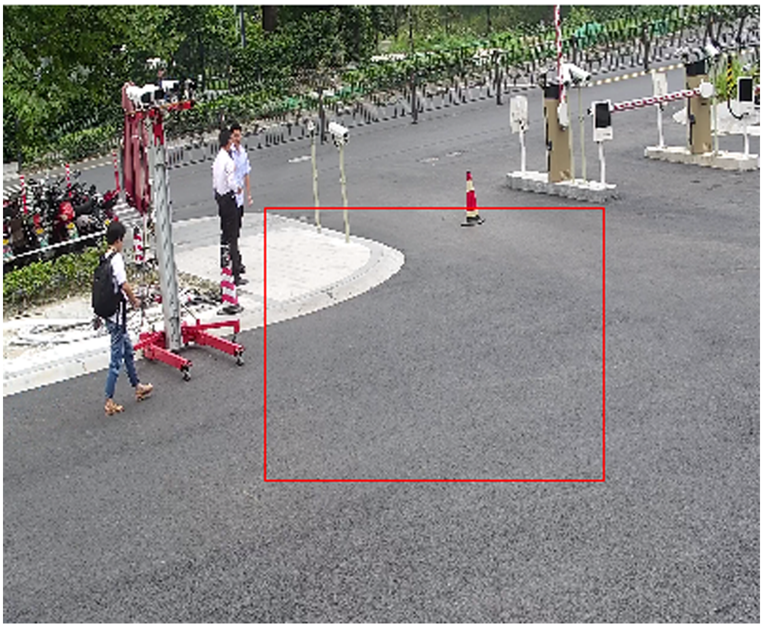


Figure 8-2 Set Rules

Stop Drawing	Finish drawing one area.
Clear All	Delete all the areas.

4. Click **Save**.
5. **Optional:** Repeat above steps to set multiple areas.

8.1.2 Set Video Tampering Alarm

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

Steps

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

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

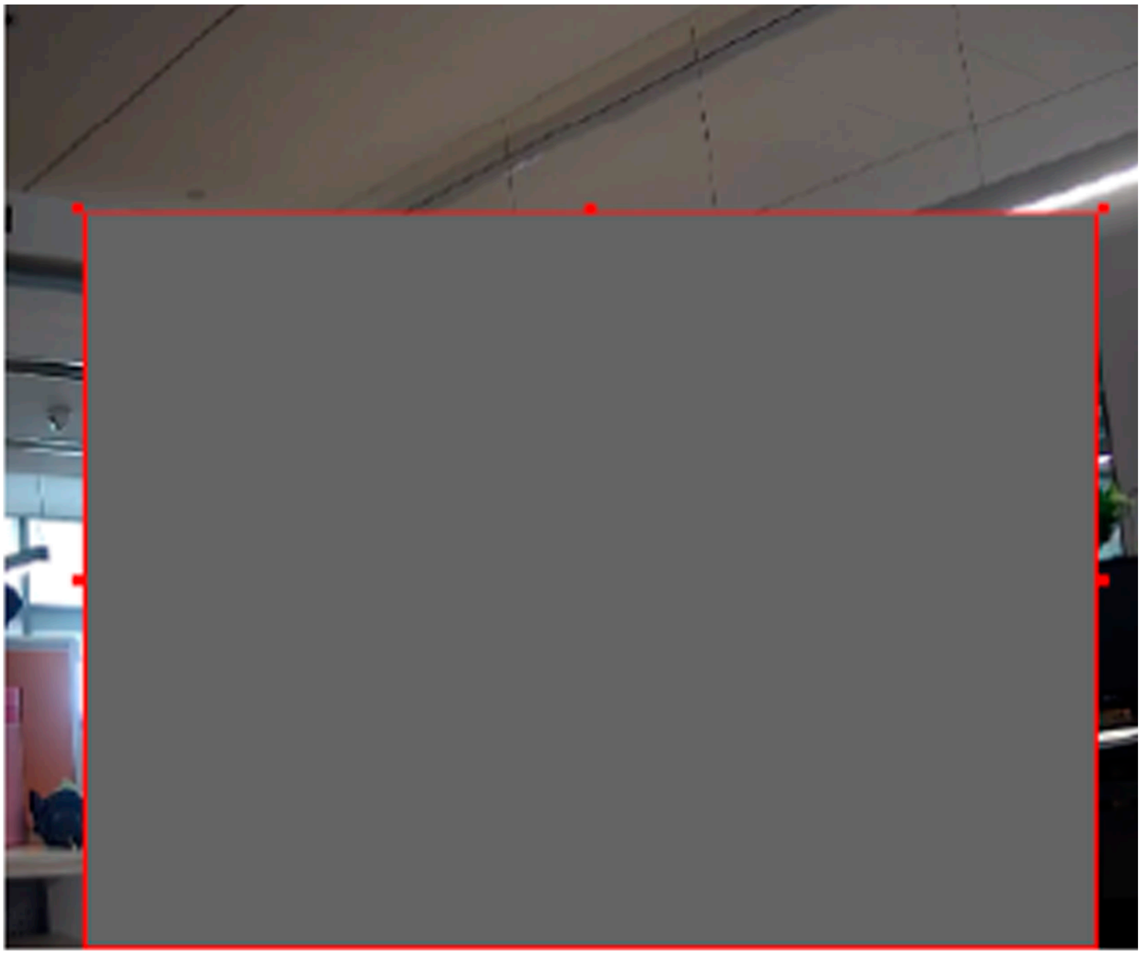


Figure 8-3 Set Video Tampering Area

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

8.1.3 Set Exception Alarm

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

Steps

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

HDD Full	The HDD storage is full.
HDD Error	Error occurs in HDD.
Network Disconnected	The device is offline.

IP Address Conflicted	The IP address of current device is same as that of other device in the network.
Illegal Login	Incorrect user name or password is entered.

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

8.1.4 Set Alarm Input

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

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

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

8.2 Smart Event

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

8.2.1 Detect Audio Exception

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

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

   Audio Loss Detection

   Detect sudden loss of audio track.

   Sudden Increase of Sound Intensity Detection

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

Note

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

Sudden Decrease of Sound Intensity Detection

Detect sudden decrease of sound intensity. **Sensitivity** is configurable.

3. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage methods.
4. Click **Save**.

Note

The function varies according to different models.

8.2.2 Set Intrusion Detection

Intrusion detection detects the object movement of entering and loitering in a predefined area. When intrusion occurs, the device takes linkage actions as response.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See ***Allocate VCA Resource*** for instructions.

Steps

1. Go to **Open Platform → Smart Event → Intrusion Detection** .
2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

   Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. Draw detection area.
   1) Select a **Region No.**. Up to 4 regions can be set.
   2) Click **Detection Area**.
   3) Click on the live image to draw the boundaries of the detection area, and right click to complete drawing.

6. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
   1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
   2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
7. Set detection parameters.

   Sensitivity It stands for the sensitivity of detecting an target. The higher the value of sensitivity is, the more easily the target is detected.

   Threshold Threshold stands for the time of the target loitering in the region. If the time that she/he stays in the region exceeds the threshold, the alarm is triggered.

   Detection Target You can specify the object type, and the device only detects the selected type of objects.

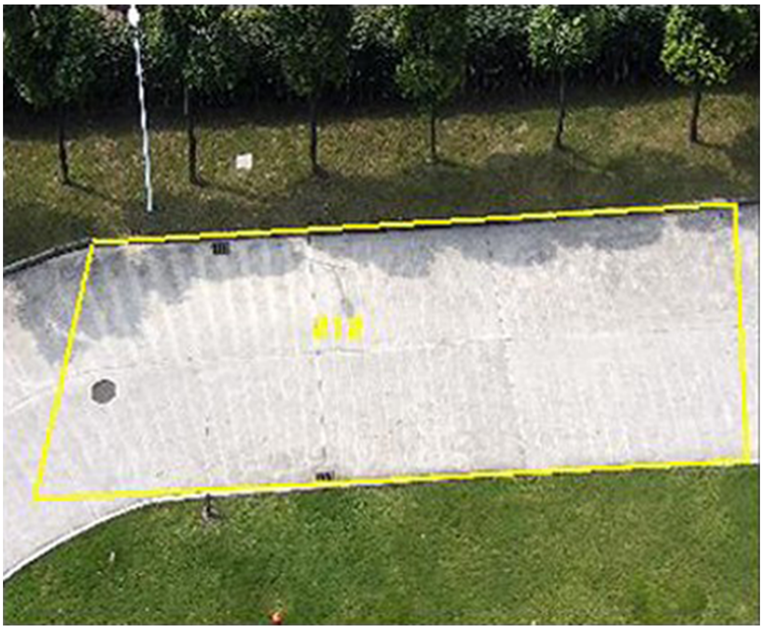


Figure 8-4 Draw Area

8. Click **Save**.
9. Repeat above steps to set other detection areas.
10. Set arming schedule. See ***Set Arming Schedule*** .
11. Set linkage method. See ***Linkage Method Settings*** .

8.2.3 Set Line Crossing Detection

Line crossing detection is used to detect the object movement of crossing a predefined line. When it occurs, the device takes linkage actions as response.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See ***Allocate VCA Resource*** for instructions.

Steps

1. Go to **Open Platform → Smart Event → Line Crossing Detection** .
2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

   Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. Draw detection line.
   1) Select a **Line No.**. Up to 4 lines can be set in the scene.
   2) Click **Detection Area**.

      A yellow line is displayed on live image.
   3) Click on the line, and drag its end points to adjust the length and position.
   4) Select the **Direction** for the detection line.

      Direction

      It stands for the direction from which the object goes across the line.

      A<->B

      The object going across the line from both directions can be detected and alarms are triggered.

      A->B

      Only the object crossing the configured line from side A to side B can be detected.

      B->A

      Only the object crossing the configured line from side B to side A can be detected.

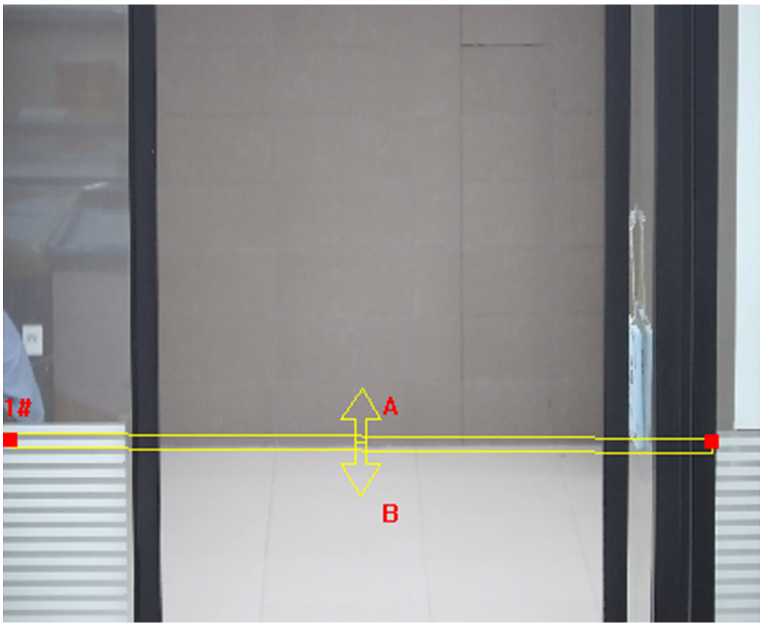


Figure 8-5 Draw Line

6. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
   1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
   2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
7. Set detection parameters.

   Sensitivity

   It stands for the sensitivity of detecting an target. The higher the value is, the more easily the target is detected.

   Detection Target

   You can specify the object type, and the device only detects the selected type of objects.
8. Click **Save**.
9. Repeat above steps to set other lines.
10. Set arming schedule. See ***Set Arming Schedule*** .
11. Set linkage method. See ***Linkage Method Settings*** .

8.2.4 Set Region Entrance Detection

Region entrance detection is used to detect the object movement of entering a predefined area. When it occurs, the device takes linkage actions as response.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See ***Allocate VCA Resource*** for instructions.

Steps

1. Go to **Open Platform → Smart Event → Region Entrance Detection** .
2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

   Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. Draw detection area.
   1) Select a **Region No.**. Up to 4 regions can be set.
   2) Click **Detection Area**.
   3) Click on the live image to draw the boundaries of the detection area, and right click to complete drawing.
6. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
   1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
   2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
7. Set detection parameters.

Sensitivity	It stands for the sensitivity of detecting an target. The higher the value is, the more easily the target is detected.
Detection Target	You can specify the object type, and the device only detects the selected type of objects.

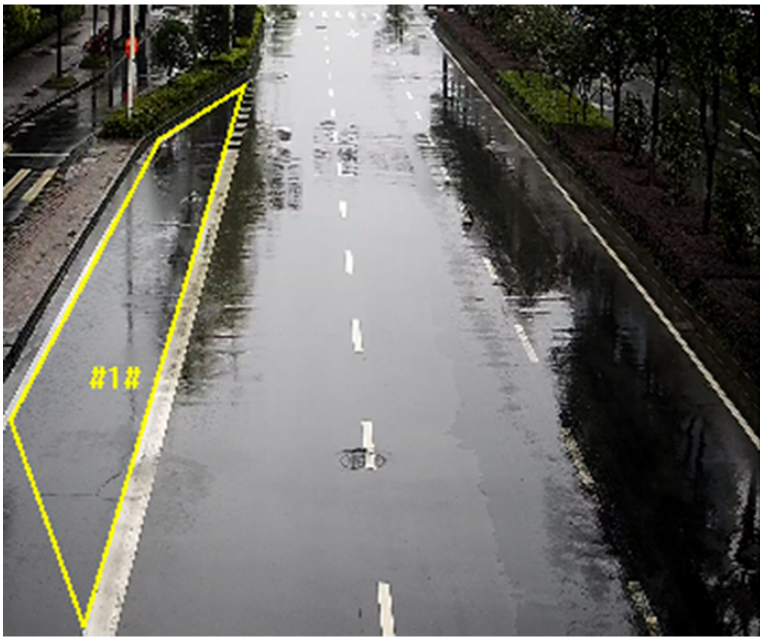


Figure 8-6 Draw Area

8. Click **Save**.
9. Repeat above steps to set other regions.
10. Set arming schedule. See ***Set Arming Schedule*** .
11. Set linkage method. See ***Linkage Method Settings*** .

8.2.5 Set Region Exiting Detection

Region exiting detection is used to detect the objects movement of exiting from a predefined area. When it occurs, the device takes linkage actions as response.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See ***Allocate VCA Resource*** for instructions.

Steps

1. Go to **Open Platform → Smart Event → Region Exiting Detection** .
2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

   Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. Draw detection area.

   1) Select a **Region No.**. Up to 4 regions can be set.

2) Click **Detection Area**.

3) Click on the live image to draw the boundaries of the detection area, and right click to complete drawing.

6. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.

1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.

2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.

7. Set detection parameters.

Sensitivity

It stands for the sensitivity of detecting an target. The higher the value is, the more easily the target is detected.

Detection Target

You can specify the object type, and the device only detects the selected type of objects.

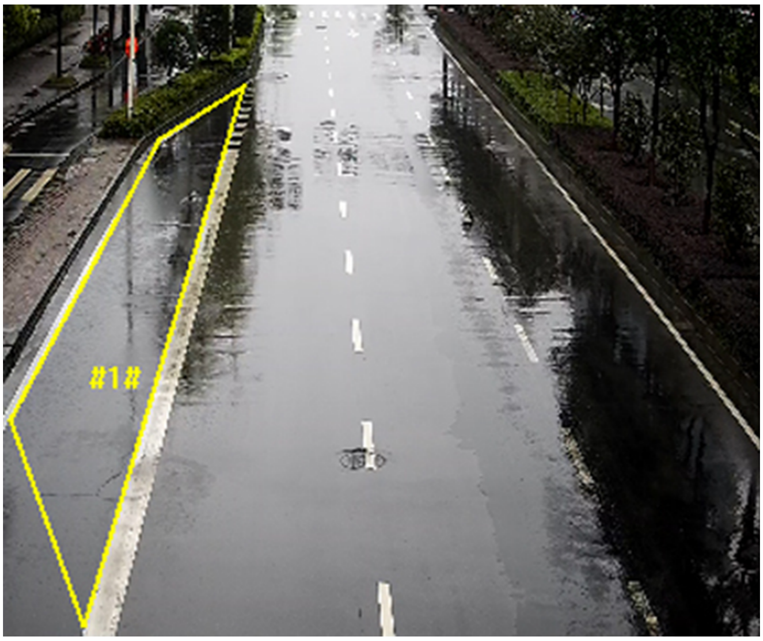


Figure 8-7 Draw Area

8. Click **Save**.
9. Repeat above steps to set other regions.
10. Set arming schedule. See ***Set Arming Schedule*** .
11. Set linkage method. See ***Linkage Method Settings*** .

8.2.6 Set Object Removal Detection

Object removal detection detects whether the objects are removed from the predefined detection area, such as exhibits on display. When it occurs, the device takes linkage actions as response.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See ***Allocate VCA Resource*** for instructions.

Steps

1. Go to **Open Platform → Smart Event → Object Removal Detection** .
2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

   Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. Draw detection area.
   1) Select a **Region No.**. Up to 4 regions can be set.
   2) Click **Detection Area**.
   3) Click on the live image to draw the boundaries of the detection area, and right click to complete drawing.
6. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
   1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
   2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
7. Set detection parameters.

   Sensitivity The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.

   Threshold The threshold is the time of the objects removed from the area. If you set the value as 10, alarm is triggered after the object disappears from the area for 10 seconds.

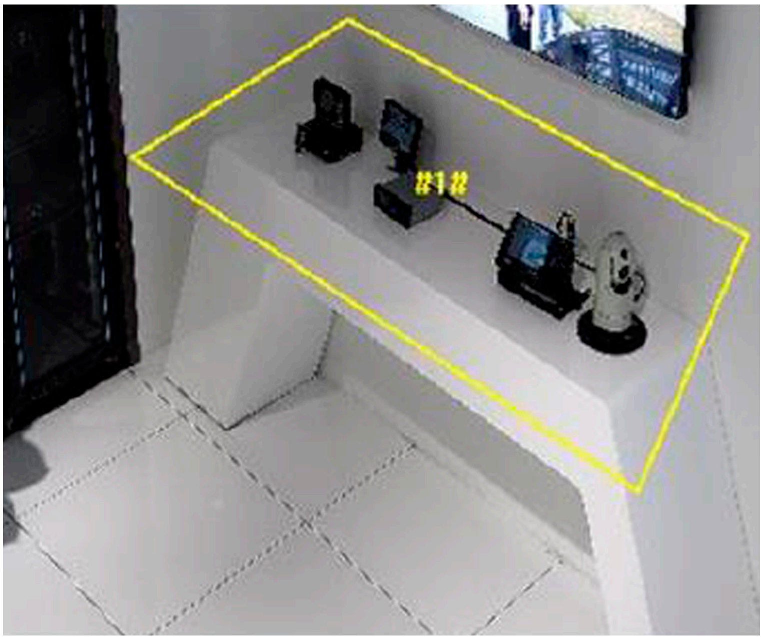


Figure 8-8 Draw Area

8. Click **Save**.
9. Repeat above steps to set other regions.
10. Set arming schedule. See ***Set Arming Schedule*** .
11. Set linkage method. See ***Linkage Method Settings*** .

8.2.7 Set Unattended Baggage Detection

Unattended baggage detection is used to detect the objects left over in the predefined area. Linkage methods are triggered after the object is left and stays in the area for a set time period.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See ***Allocate VCA Resource*** for instructions.

Steps

1. Go to **Open Platform → Smart Event → Unattended Baggage Detection** .
2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

   Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. Draw detection area.

   1) Select a **Region No.**. Up to 4 regions can be set.

2) Click **Detection Area**.
3) Click on the live image to draw the boundaries of the detection area, and right click to complete drawing.

6. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
   1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
   2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
7. Set detection parameters.

Sensitivity The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.

Threshold It stands for the time of the objects left in the area. Alarm is triggered after the object is left and stays in the area for the set time period.

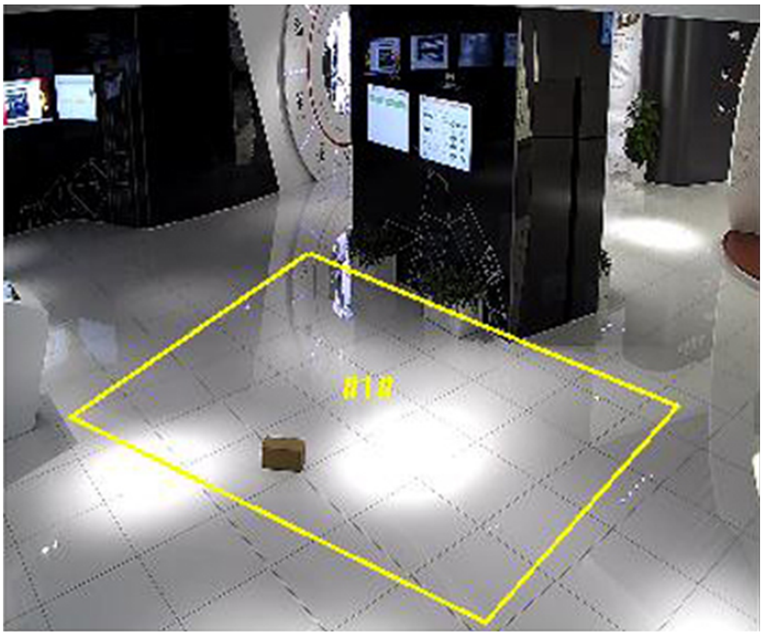


Figure 8-9 Draw Area

8. Click **Save**.
9. Repeat above steps to set other regions.
10. Set arming schedule. See ***Set Arming Schedule*** .
11. Set linkage method. See ***Linkage Method Settings*** .

8.2.8 Set Tracking Parameters

Adjust the motion parameters of the device for better target tracking performance.

Steps

Note

This function is only supported by certain models.

1. Go to **Open Platform → Smart Event → Advanced Parameters** .
2. **Optional:** Check **Tuning Mode**.

   Note

   Tuning mode is to display the information that helps debugging the function. This mode is reserved for technical support.
3. Set the **Duration**.

   The device stops tracking when it tracks a target uninterruptedly for the set duration.
4. Set the zooming control and other tracking parameters.

   Zooming Control

   Two modes are available. Controlled by target frame or by tilt angle of the device.

   By Tilt Angle

   The device calculates the tracking zoom ratio automatically according to the tilt angle of the device.

   Note

   The attitude of the device affects the accuracy of this zooming control mode. For the model with a built-in gyroscope, try to calibrate the attitude if some zooming problems happen during tracking. See ***Set Device Position*** for instructions.

   By Target Frame

   The tracked target has a virtual frame around. The device calculates a suitable zoom ratio according to the frame and the set **Tracking Zoom Ratio**. Larger value means bigger zoom ratio.

   Wait to Stop Tracking If Low Validity

   The validity is an internal parameter that helps judge whether the device should keep tracking or not. This parameter is the waiting time level before the device stops tracking when the validity is low. Larger value means longer waiting time.

   Wait to Lower Tracking Speed If Low Validity

   The validity is an internal parameter that helps judge whether the PTZ channel should lower the tracking speed or not. This parameter is the waiting time level before the device lowers the tracking speed when the validity is low. Larger value means longer waiting time.
5. Click **Save**.

Chapter 9 Arming Schedule and Alarm Linkage

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

9.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

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

Note

Up to 8 periods can be configured for one day.

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

9.2 Linkage Method Settings

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

9.2.1 Trigger Alarm Output

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

Steps

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

Automatic Alarm	For the information about the configuration, see ***Automatic Alarm*** .
Manual Alarm	For the information about the configuration, see ***Manual Alarm*** .

3. Click **Save**.

Automatic Alarm

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

Steps

1. Set automatic alarm parameters.

   Alarm Output No.

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

   Alarm Name

   Custom a name for the alarm output.

   Delay

   It refers to the time duration that the alarm output remains after an alarm occurs.
2. Set the alarming schedule. For the information about the settings, see ***Set Arming Schedule*** .
3. Click **Copy to...** to copy the parameters to other alarm output channels.
4. Click **Save**.

Manual Alarm

You can trigger an alarm output manually.

Steps

1. Set the manual alarm parameters.

   Alarm Output No.

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

   Alarm Name

   Edit a name for the alarm output.

   Delay

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

9.2.2 FTP/NAS/Memory Card Uploading

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

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

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

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

9.2.3 Send Email

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

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

Set Email

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

Before You Start

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

Steps

1. Go to email settings page: **Configuration → Network → Advanced Settings → Email** .
2. Set email parameters.
   1) Input the sender's email information, including the **Sender's Address**, **SMTP Server**, and **SMTP Port**.
   2) **Optional:** If your email server requires authentication, check **Authentication** and input your user name and password to log in to the server.
   3) Set the **E-mail Encryption**.
      - When you select **TLS**, and disable STARTTLS, emails are sent after encrypted by TLS. The SMTP port should be set as 465.
      - When you select **TLS** and **Enable STARTTLS**, emails are sent after encrypted by STARTTLS, and the SMTP port should be set as 25.

      Note

      If you want to use STARTTLS, make sure that the protocol is supported by your email server. If you check the **Enable STARTTLS** while the protocol is not supported by your email sever, your email is sent with no encryption.
   4) **Optional:** If you want to receive notification with alarm pictures, check **Attached Image**. The notification email has 3 attached alarm pictures about the event with configurable image capturing interval.
   5) Input the receiver's information, including the receiver's name and address.
   6) Click **Test** to see if the function is well configured.
3. Click **Save**.

9.2.4 Notify Surveillance Center

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

9.2.5 Smart Tracking

Check **Smart Tracking**, and the device tracks the target when an alarm event is detected.

Note

This function is only supported by certain models.

9.2.6 Trigger Recording

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

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

9.2.7 Flashing Light

After enabling **Flashing Light** and setting the **Flashing Light Alarm Output**, the light flashes when an alarm event is detected.

Set Flashing Alarm Light Output

When events occur, the flashing light on the device can be triggered as an alarm.

Steps

1. Go to **Configuration → Event → Basic Event → Flashing Alarm Light Output** .
2. Set **Flashing Duration**, **Flashing Frequency** and **Brightness**.

   Flashing Duration

   The time that the flashing lasts when one alarm happens.

   Flashing Frequency

   The rate at which the light flashes. High frequency, medium frequency, low frequency, and normally on are selectable.

   Brightness

   The brightness of the light.
3. Set the arming schedule. See ***Set Arming Schedule*** for details.
4. Click **Save**.

Note

Only certain device models support the function.

9.2.8 Audible Warning

After enabling **Audible Warning** and setting the **Audible Alarm Output**, the built-in speaker of the device or connected external speaker plays warning sounds when alarm happens.

For audible alarm output settings, refer to ***Set Audible Alarm Output*** .

Note

Before using the function, go to **Configuration → Video/Audio → Audio** to enable built-in speaker in advance.
The function is only supported by certain camera models.

Set Audible Alarm Output

When the device detects targets in the detection area, audible alarm can be triggered as a warning.

Steps

1. Go to **Configuration → Event → Basic Event → Audible Alarm Output** .
2. Select **Sound Type** and set related parameters.
   - Select **Prompt** and set the alarm times you need.
   - Select **Warning** and its contents. Set the alarm times you need.
   - Select **Custom Audio**. You can select a custom audio file from the drop-down list. If no file is available, you can click **Add** to upload an audio file that meets the requirement. Up to three audio files can be uploaded.
3. **Optional:** Click **Test** to play the selected audio file on the device.
4. Set arming schedule for audible alarm. See ***Set Arming Schedule*** for details.
5. Click **Save**.

Note

The function is only supported by certain device models.

Chapter 10 Network Settings

10.1 TCP/IP

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

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

NIC Type

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

IPv4

Two IPv4 modes are available.

DHCP

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

Note

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

Manual

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

IPv6

Three IPv6 modes are available.

Route Advertisement

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

Note

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

DHCP

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

Manual

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

MTU

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

The valid value range of MTU is 1280 to 1500.

DNS

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

Dynamic Domain Name

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

Note

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

10.1.1 Multicast

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

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

IP Address

It stands for the address of multicast host.

Stream Type

The stream type as the multicast source.

Video Port

The video port of the selected stream.

Audio Port

The audio port of the selected stream.

10.1.2 Multicast Discovery

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

10.2 Port

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

Caution

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

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

HTTP Port

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

HTTPS Port

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

RTSP Port

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

SRTP Port

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

Server Port

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

Enhanced SDK Service Port

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

WebSocket Port

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

WebSockets Port

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

Note

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

10.3 Port Mapping

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

Before You Start

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

Steps

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

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

3. Click **Save**.

10.3.1 Set Auto Port Mapping

Steps

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

Note

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

10.3.2 Set Manual Port Mapping

Steps

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

What to do next

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

10.3.3 Set Port Mapping on Router

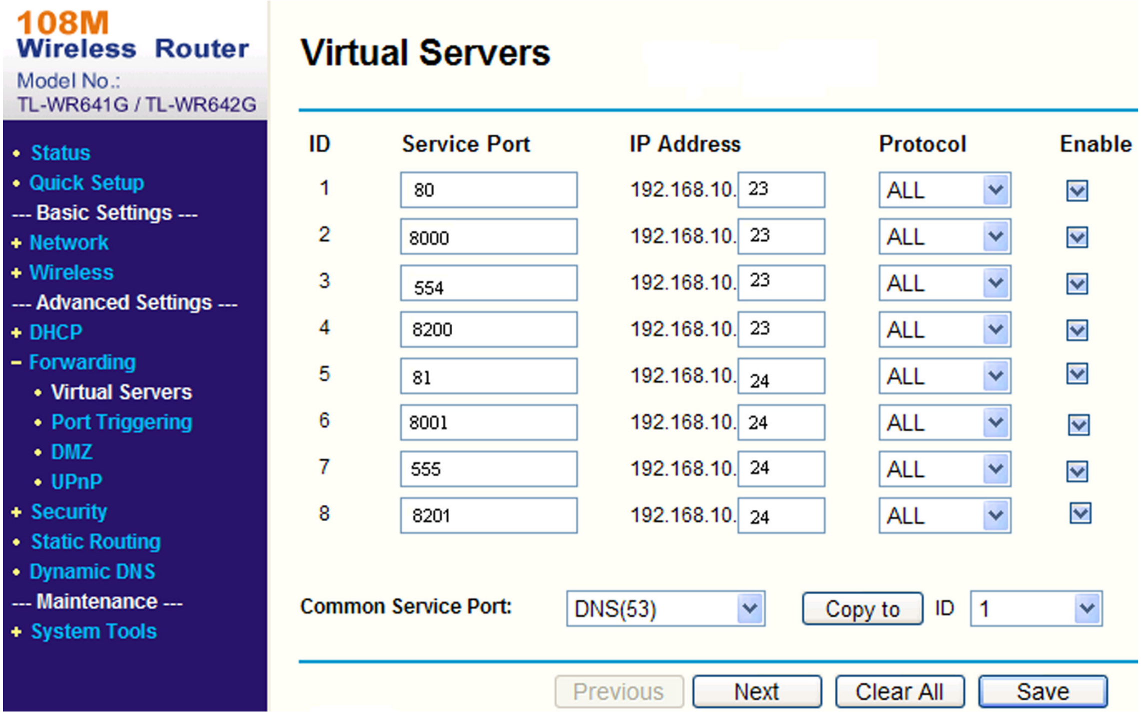
The following settings are for a certain router. The settings vary depending on different models of routers.

Steps

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

Example

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



Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10. 23	ALL	☑
2	8000	192.168.10. 23	ALL	☑
3	554	192.168.10. 23	ALL	☑
4	8200	192.168.10. 23	ALL	☑
5	81	192.168.10. 24	ALL	☑
6	8001	192.168.10. 24	ALL	☑
7	555	192.168.10. 24	ALL	☑
8	8201	192.168.10. 24	ALL	☑

Common Service Port: DNS(53) Copy to ID 1

Figure 10-1 Port Mapping on Router

Note

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

10.4 SNMP

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

Before You Start

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

Steps

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

   Note

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

10.5 Access to Device via Domain Name

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

Before You Start

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

Steps

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

   DynDNS

   Dynamic DNS server is used for domain name resolution.

   NO-IP

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

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

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

10.6 Access to Device via PPPoE Dial Up Connection

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

Steps

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

   Dynamic IP

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

   User Name

   User name for dial-up network access.

   Password

   Password for dial-up network access.

   Confirm

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

By Browsers	Enter the WAN dynamic IP address in the browser address bar to access the device.
By Client Software	Add the WAN dynamic IP address to the client software. Refer to the client manual for details.

Note

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

10.7 Accessing via Mobile Client

Hik-Connect is an application for mobile devices. Using the App, you can view live image, receive alarm notification and so on.

Note

Hik-Connect service should be supported by the camera.

10.7.1 Enable Hik-Connect Service on Camera

Hik-Connect service should be enabled on your camera before using the service.

You can enable the service through SADP software or Web browser.

Enable Hik-Connect Service via Web Browser

Follow the following steps to enable Hik-Connect Service via Web Browser.

Before You Start
You need to activate the camera before enabling the service.

Steps

1. Access the camera via web browser.
2. Enter platform access configuration interface. **Configuration → Network → Advanced Settings → Platform Access**
3. Select Hik-Connect as the **Platform Access Mode**.
4. Check **Enable**.
5. Click and read "Terms of Service" and "Privacy Policy" in pop-up window.
6. Create a verification code or change the old verification code for the camera.

   Note

   The verification code is required when you add the camera to Hik-Connect service.
7. Save the settings.

Enable Hik-Connect Service via SADP Software

This part introduce how to enable Hik-Connect service via SADP software of an activated camera.

Steps

1. Run SADP software.
2. Select a camera and enter **Modify Network Parameters** page.
3. Check **Enable Hik-Connect**.
4. Create a verification code or change the old verification code.

   Note

   The verification code is required when you add the camera to Hik-Connect service.
5. Click and read "Terms of Service" and "Privacy Policy".

6. Confirm the settings.

10.7.2 Set Up Hik-Connect

Steps

1. Get and install Hik-Connect application by the following ways.
   - Visit ***https://appstore.hikvision.com*** to download the application according to your mobile phone system.
   - Visit the official site of our company. Then go to **Support → Tools → Hikvision App Store** .
   - Scan the QR code below to download the application.

Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit ***https://appstore.hikvision.com/static/help/index.html*** to refer to the troubleshooting.
- Visit ***https://appstore.hikvision.com/*** , and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

2. Start the application and register for a Hik-Connect user account.
3. Log in after registration.

10.7.3 Add Camera to Hik-Connect

Steps

1. Connect your mobile device to a Wi-Fi.
2. Log into the Hik-Connect app.
3. In the home page, tap "+" on the upper-right corner to add a camera.
4. Scan the QR code on camera body or on the *Quick Start Guide* cover.

Note

If the QR code is missing or too blur to be recognized, you can also add the camera by inputting the camera's serial number.

5. Input the verification code of your camera.

Note

- The required verification code is the code you create or change when you enable Hik-Connect service on the camera.
- If you forget the verification code, you can check the current verification code on **Platform Access** configuration page via web browser.

6. Tap **Connect to a Network** button in the popup interface.
7. Choose **Wired Connection**.
8. Connect the camera to the router with a network cable and tap **Connected** in the result interface.

Note

The router should be the same one which your mobile phone has connected to.

9. Tap **Add** in the next interface to finish adding.

   For detailed information, refer to the user manual of the Hik-Connect app.

10.8 Set ISUP

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

Steps

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

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

10.9 Set Open Network Video Interface

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

Steps

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

Delete	Delete the selected Open Network Video Interface user.
Modify	Modify the selected Open Network Video Interface user.

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

10.10 Set Network Service

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

Steps

Note

This function varies according to different models.

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

   WebSocket & WebSockets

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

   If the device uses HTTP, enable WebSocket.

   If the device uses HTTPS, enable WebSockets.

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

   Note

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

   SDK Service & Enhanced SDK Service

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

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

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

   Note

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

   TLS (Transport Layer Security)

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

   Bonjour

   Uncheck to disable the protocol.
3. Click **Save**.

10.11 Set Alarm Server

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

Steps

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

Note

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

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

10.12 TCP Acceleration

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

10.13 Traffic Shaping

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

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

10.14 Set SRTP

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

Steps

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

Note

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

Chapter 11 System and Security

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

11.1 View Device Information

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

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

11.2 Restore and Default

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

Steps

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

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

   Default Reset all the parameters to the factory default.

   Note

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

11.3 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

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

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

11.4 Import and Export Configuration File

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

Steps

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

11.5 Export Diagnose Information

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

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

11.6 Reboot

You can reboot the device via browser.

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

11.7 Upgrade

Before You Start

You need to obtain the correct upgrade package.

⚠ **Caution**

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

Steps

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

Firmware	Locate the exact path of the upgrade file.

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

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

11.8 View Open Source Software License

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

11.9 Set Live View Connection

It controls the remote live view connection amount.

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

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

11.10 Time and Date

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

11.10.1 Synchronize Time Manually

Steps

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

11.10.2 Set NTP Server

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

Before You Start

Set up a NTP server or obtain NTP server information.

Steps

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

   Note

   Server Address is NTP server IP address.
5. Click **Test** to test server connection.
6. Click **Save**.

11.10.3 Set DST

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

Steps

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

11.11 Set RS-485

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

Before You Start

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

Steps

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

   Note

   You should keep the parameters of the device and the computer or terminal all the same.
3. Click **Save**.

11.12 Security

You can improve system security by setting security parameters.

11.12.1 Authentication

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

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

RTSP Authentication

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

RTSP Digest Algorithm

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

WEB Authentication

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

WEB Digest Algorithm

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

Note

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

11.12.2 Set IP Address Filter

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

IP address refers to IPv4.

Steps

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

   Forbidden IP addresses in the list cannot access the device.

Allowed	Only IP addresses in the list can access the device.

4. Edit the IP address filter list.

Add	Add a new IP address or IP address range to the list.
Modify	Modify the selected IP address or IP address range in the list.
Delete	Delete the selected IP address or IP address range in the list.

5. Click **Save**.

11.12.3 Set MAC Address Filter

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

Steps

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

Forbidden	MAC addresses in the list cannot access the device.
Allowed	Only MAC addresses in the list can access the device.

4. Edit the MAC address filter list.

Add	Add a new MAC address to the list.
Modify	Modify the selected MAC address in the list.
Delete	Delete the selected MAC address in the list.

5. Click **Save**.

11.12.4 Set HTTPS

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

Steps

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

Note

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

5. Click **Save**.

11.12.5 Security Audit Log

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

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

Search Security Audit Logs

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

Steps

Note

This function is only supported by certain camera models.

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

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

Set Log Server

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

Before You Start

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

Steps

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

11.12.6 Set QoS

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

Note

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

Steps

1. Go to **Configuration → Network → Advanced Configuration → QoS** .
2. Set **Video/Audio DSCP**, **Alarm DSCP** and **Management DSCP**.

   Note

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

11.12.7 Set IEEE 802.1X

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

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

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

Note

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

11.12.8 SSH

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

The SSH function is disabled by default.

Caution

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

11.12.9 Control Timeout Settings

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

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

11.12.10 Certificate Management

It manages the server/client certificates and CA certificate of the device.

Server Certificate/Client Certificate

Note

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

Create and Install Self-signed Certificate

Steps

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

   Note

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

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

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

5. **Optional:** Click **Certificate Property** to see the certificate details.

Install Self-signed Request Certificate

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

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

Steps

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

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

      Note

      The input certificate ID cannot be the same as the existed ones.
   3) Click **Browse** to select the certificate file.
   4) Select **Self-signed Request Certificate**.
   5) Click **OK**.

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

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

Install Other Authorized Certificate

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

Steps

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

Note

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

4. Click **Browse** to select the certificate file.
5. Select **Certificate and Key** and select a **Key Type** according to your certificate.

   Independent Key If your certificate has a independent key, select this option.

   Browse to select the private key and input the private-key password.

   PKCS#12 If your certificate has the key in the same certificate file, select this option and input the password.
6. Click **OK**.

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

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

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

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

   Note

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

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

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

Enable Certificate Expiration Alarm

Steps

1. Check **Enable Certificate Expiration Alarm**. If enabled, you will receive an email or the camera links to the surveillance center that the certificate will expire soon, or is expired or abnormal.
2. Set the **Remind Me Before Expiration (day)**, **Alarm Frequency (day)** and **Detection Time (hour)**.

Note

- If you set the reminding day before expiration to 1, then the camera will remind you the day before the expiration day. 1 to 30 days are available. Seven days is the default reminding days.
- If you set the reminding day before expiration to 1, and the detection time to 10:00, and the certificate will expire in 9:00 the next day, the camera will remind you in 10:00 the first day.

3. Click **Save**.

11.12.11 User and Account

Set User Account and Permission

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

Caution

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

Steps

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

   Administrator

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

   User

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

   Operator

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

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

Note

The administrator can add up to 31 user accounts.

3. Click **OK**.

Online Users

The information of users logging into the device is shown.

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

Simultaneous Login

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

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

Appendix A. Device Command

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

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

Appendix B. Device Communication Matrix

Scan the following QR code to get device communication matrix.

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

See Far, Go Further

Network Camera

User Manual

Legal Information

About this Document

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

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Symbol Conventions

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

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

Safety Instruction

Please scan the following QR code to obtain the " ***Safety Instruction*** " of the product, and read it carefully. These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

Figure 1-1 Safety Instruction

Contents

Chapter 1 Overview

1.1 Configuration Process

This section briefly explains the software configuration process of the network camera. Please set up the device according to the actual situation.

General Configuration Process

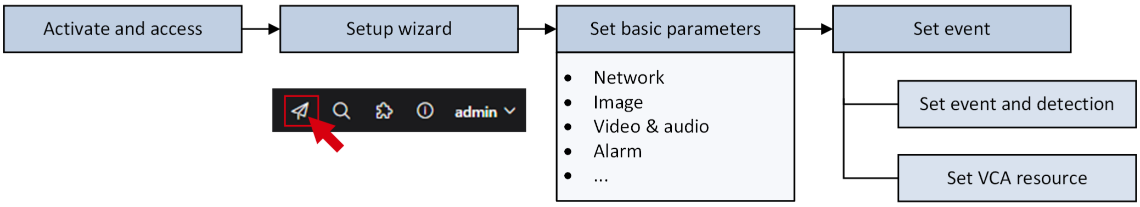


Figure 1-1 General Configuration Process

- ***Activate and access device via web browser.*** You should set a login password (for **admin** user) to activate the device when access the device via network. Open the web browser and enter the IP address. The default IP address of the device is 192.168.1.64.
- Follow the **Wizard** or click ◁ on the web page to quickly set the device parameters.
- Set the basic parameters, including network, image, video and audio, alarm, etc.
- Set event and detection rules. You can set basic ***event and detection*** rules or ***allocate VCA resources*** for deep learning function.

1.2 Firmware Update

For better user experience, we recommend you to update your device to the latest firmware.

Please get the latest firmware package from the official website or the local technical expert. For more information, please visit the official website: ***https://www.hikvision.com/en/support/download/firmware/*** .

For the upgrading settings, refer to ***Upgrade*** .

1.3 System Requirement

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

Operating System	Microsoft Windows XP SP1 and above version
CPU	2.0 GHz or higher
RAM	1G or higher
Display	1024×768 resolution or higher
Web Browser	For the details, see ***Plug-in Installation***

Chapter 2 Device Activation and Accessing

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

Note

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

2.1 Activate the Device via SADP

Search and activate the online devices via SADP software.

Before You Start

Access www.hikvision.com to get SADP software to install.

Steps

1. Connect the device to network using the network cable.
2. Run SADP software to search the online devices.
3. Check **Device Status** from the device list, and select **Inactive** device.
4. Create and input the new password in the password field, and confirm the password.

   Caution

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

   Device Status changes into **Active**.
6. **Optional:** Change the network parameters of the device in **Modify Network Parameters**.

2.2 Activate the Device via Browser

You can access and activate the device via the browser.

Steps

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

Note

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

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

Caution

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

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

2.3 Login

Log in to the device via Web browser.

2.3.1 Plug-in Installation

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

Operating System	Web Browser	Operation
Windows	• Internet Explorer 10+ • Google Chrome 57 and earlier version • Mozilla Firefox 52 and earlier version	Follow pop-up prompts to complete plug-in installation.
	• Google Chrome 57+ • Mozilla Firefox 52+ • Edge 89+	Click ⚙ to download and install plug-in.
Mac OS	• Google Chrome 57+ • Mozilla Firefox 52+ • Mac Safari 16+	Plug-in installation is not required. Go to **Configuration → Network → Network Service → WebSocket(s)** to enable WebSocket or WebSockets for normal view. Display and operation of certain functions are restricted. For example, Playback and Picture are not available. For detailed restricted function, refer to the actual device.

Note

- The device only supports Windows and Mac OS system, and does not support Linux system.
- To improve the user experience on certain devices, it's recommended to use a more advanced web browser for access. Please refer to the actual device or product specification.
- Certain device models do not support Internet Explorer web browser.

2.3.2 Admin Password Recovery

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

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

Note

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

Security Question

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

Email

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

2.3.3 Illegal Login Lock

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

Go to **Maintenance and Security → Security → Login Management** , and enable **Enable Illegal Login Lock**. **Illegal Login Attempts** and **Locking Duration** are configurable.

Illegal Login Attempts

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

Locking Duration

The device releases the lock after the setting duration.

Chapter 3 Live View

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

3.1 Live View Parameters

The supported functions vary depending on the model.

3.1.1 Start and Stop Live View

Click **Live View**. Click ▶ to start live view. Click ☒ to stop live view.

3.1.2 Aspect Ratio

Aspect Ratio is the display ratio of the width to height of the image.

- 4:3 refers to 4:3 window size.
- 16:9 refers to 16:9 window size.
- 1X refers to original window size.
- ⧉ refers to self-adaptive window size.
- ▭ refers to original ratio window size.

3.1.3 Live View Stream Type

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

3.1.4 Select the Third-Party Plug-in

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

Steps

1. Click **Live View**.
2. Click ⚙ to select the plug-in.
   - When you access the device via Internet Explorer, you can select Webcomponents or QuickTime.
   - When you access the device via the other browsers, you can select Webcomponents, QuickTime or MJPEG.

3.1.5 Light

Click 💡 to turn on or turn off the illuminator.

⚠ **Caution**

For the device with laser:

- DO NOT stare at operating light source. May be harmful to the eyes.
- If appropriate shielding or eye protection is not available, turn on the light only at a safe distance or in the area that is not directly exposed to the light.
- When assembling, installing or maintaining the device, DO NOT turn on the light, or wear eye protection.

3.1.6 Count Pixel

It helps to get the height and width pixel of the selected region in the live view image.

Steps

1. Click ▣ to enable the function.
2. Drag the mouse on the image to select a desired rectangle area.

   The width pixel and height pixel are displayed on the bottom of the live view image.

3.1.7 Start Digital Zoom

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

Steps

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

3.1.8 Auxiliary Focus

It is used for motorized device. It can improve the image if the device cannot focus clearly.

For the device that supports ABF, adjust the lens angle, then focus and click ABF button on the device. The device can focus clearly.

Click ⊡ to focus automatically.

Note

- If the device cannot focus with auxiliary focus, you can use ***Lens Initialization*** , then use auxiliary focus again to make the image clear.
- If auxiliary focus cannot help the device focus clearly, you can use manual focus.

3.1.9 Lens Initialization

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

Click to operate lens initialization.

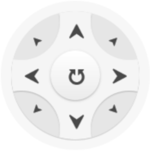
3.1.10 Lens Parameters Adjustment

PTZ is an abbreviation for pan, tilt, and zoom. It means the movement options of the device. In live view interface, you can click the direction control buttons to control the pan/tilt movement, and click the zoom/focus/iris buttons to realize lens control.

Note

- Supported PTZ functions may vary according to different camera models.
- For the devices which support lens movements only, the direction buttons are invalid.

Direction Control



Click and hold the direction button to pan/tilt the device.

Zoom

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

Focus

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

Iris

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

PTZ Speed

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

PTZ Lock

PTZ lock means to disable the zoom, focus and PTZ rotation functions of the corresponding channel, so that to reduce the target missing caused by PTZ adjustment.

Note

The function is only supported by certain device models.

Click 🔒 to lock the PTZ operation, or click 🔓 to unlock it.

PTRZ Adjustment

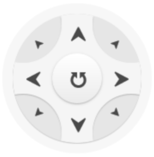
PTRZ is an abbreviation for pan, tilt, rotate and zoom. It means the movement options of the device. In the interface, you can use the control buttons to adjust the movement of the device, such as device panning, tilting, rotating, and zooming.

Note

The function is only supported by certain device models.

Go to **Configuration → PTZ → PTRZ** .

Control Panel

	Click and hold the directional button to pan/tilt the device.
• ⟲ • ⟳	Click and hold the button to adjust rotating position.

Auto Recovery

Click ◎ , the device will correct the rotating position automatically to make the live view image positive. Make sure the **Self-Test Status** is **Initialized**.

Note

- Go to **Configuration → PTZ → PTZ** to view the **Self-Test Status**.
- If you want to initialize PTZ and enable PTZ self-check manually, go to **Configuration → PTZ → PTZ** and click **Self-Test**, then the PTZ is initialized.

Refer to ***Lens Parameters Adjustment*** for more detailed settings of lens adjustment.

3.1.11 Conduct 3D Positioning

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

Steps

1. Click 3D to enable the function.
2. Select a target area in live image.
   - Left click on a point on live image: the point is relocated to the center of the live image. With no zooming in or out effect.
   - Hold and drag the mouse to a lower right position to frame an area on the live: the framed area is zoomed in and relocated to the center of the live image.
   - Hold and drag the mouse to an upper left position to frame an area on the live: the framed area is zoomed out and relocated to the center of the live image.
3. Click the button again to turn off the function.

3.2 Set Transmission Parameters

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

Steps

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

   Protocol

   TCP

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

   UDP

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

   MULTICAST

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

Note

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

HTTP

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

Playing Performance

Shortest Delay

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

Balanced

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

Fluent

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

Custom

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

3. Click **Save**.

3.3 Set Smooth Streaming

It is a function to tackle the latency and network congestion caused by unstable network condition, and keep the live view stream on the web browser or the client software smooth.

Before You Start

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

Be sure that the **Bit Rate Type** is selected as **Constant** and the **SVC** is selected as **OFF** before enabling the function. Go to **Configuration → Video/Audio → Video** to set the parameters.

Note

The function is only supported by certain device models.

Steps

1. Go to the settings page: **Configuration → Network → Network Service → Smooth Streaming** .
2. Check **Enable Smooth Streaming**.
3. Select the mode for smooth streaming.

Auto

The resolution and bit rate are adjusted automatically and resolution takes the priority. The upper limits of these two parameters will not exceed the values you set on **Video** page. Go to **Configuration → Video/Audio → Video** , set the **Resolution** and **Max. Bit Rate** before you enable smooth streaming function. In this mode, the frame rate will be adjusted to the maximum value automatically.

Resolution Priority

The resolution stays the same as the set value on **Video** page, and the bit rate will be adjusted automatically. Go to **Configuration → Video/Audio → Video** , set the **Max. Bit Rate** before you enable smooth streaming function. In this mode, the frame rate will be adjusted to the maximum value automatically.

Frame Rate Priority

The image is still smooth even under the poor network, while the image quality may be not good.

Error Correction

The resolution and bit rate stay the same as the set values on **Video** page. The mode is used to correct the data error during transmission to ensure the image quality. You can set the **Error Correction Proportion** within range of 0-100.

When the proportion is 0, the data error will be corrected by data retransmission. When 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 is, the more redundant date will be generated, the more data error would be corrected, but the larger bandwidth would be required. When the proportion is 100, the redundant data will be as large as the original data, and the bandwidth is twice required.

Note

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

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

Chapter 4 Video and Audio

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

4.1 Video Settings

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

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

4.1.1 Stream Type

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

Main Stream

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

Sub Stream

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

Other Streams

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

4.1.2 Video Type

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

Video Stream

Only video content is contained in the stream.

Video&Audio

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

4.1.3 Resolution

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

4.1.4 Bitrate Type and Max. Bitrate

Constant Bitrate

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

Variable Bitrate

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

4.1.5 Video Quality

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

4.1.6 Frame Rate

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

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

4.1.7 Video Encoding

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

Note

Available compression standards vary according to device models.

H.264

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

H.264+

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

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

Note

When H.264+ is enabled, **I Frame Interval** is not configurable.

H.265

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

H.265+

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

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

Note

When H.265+ is enabled, **I Frame Interval** is not configurable.

I-Frame Interval

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

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

SVC

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

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

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

MPEG4

MPEG4, referring to MPEG-4 Part 2, is a video compression format developed by Moving Picture Experts Group (MPEG).

MJPEG

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

Profile

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

4.1.8 Smoothing

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

4.2 Audio Settings

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

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

Note

Only certain camera models support the function.

4.2.1 Audio Encoding

Select the audio encoding compression of the audio.

4.2.2 Audio Input

Note

- Connect the audio input device as required.
- The audio input display varies with the device models.

LineIn	Set **Audio Input** to **LineIn** when the device connects to the audio input device with the high output power, such as MP3, synthesizer or active pickup.
MicIn	Set **Audio Input** to **MicIn** when the device connects to the audio input device with the low output power, such as microphone or passive pickup.

4.2.3 Audio Output

Note

Connect the audio output device as required.

It is a switch of the device audio output. When it is disabled, all the device audio cannot output. The audio output display varies with the device modes.

4.2.4 Environmental Noise Filter

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

4.3 Two-way Audio

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

Before You Start

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

Steps

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

4.4 ROI

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

4.4.1 Set ROI

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

Before You Start

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

Steps

1. Go to **Configuration → Video/Audio → ROI** .
2. Check **Enable**.
3. Select **Stream Type**.
4. Select **Region No.** and click to draw ROI region on the live view.

   Note

   Select the fixed region that needs to be adjusted and drag the mouse to adjust its position.
5. Input the **Area Name** and **ROI Level**.
6. Click **Save**.

   Note

   The higher the ROI level is, the clearer the image of the detected region is.
7. **Optional:** Select other region No. and repeat the above steps if you need to draw multiple fixed regions.

4.5 Set Target Cropping

You can crop the image, transmit and save only the images of the target area to save transmission bandwidth and storage.

Steps

1. Go to **Configuration → Video/Audio → Target Cropping** .
2. Check **Enable** and set **Third Stream** as the **Stream Type**.

   Note

   After enabling target cropping, the third stream resolution cannot be configured.
3. Select a **Cropping Resolution**.

   A red frame appears in the live view.
4. Drag the frame to the target area.
5. Click **Save**.

   Note

   - Only certain models support target cropping and the function varies according to different camera models.
   - Some functions may be disabled after enabling target cropping.

4.6 Display Info. on Stream

The information of the objects (e.g. human, vehicle, etc.) is marked in the video stream. You can set rules on the connected rear-end device or client software to detect the events including line crossing, intrusion, etc.

Before You Start

This function is supported in smart events. Go to **VCA** , select **Smart Event** and click **Next** to enable **Smart Event**.

Steps

1. Go to **Configuration → Video/Audio → Display Info. on Stream** .
2. Check **Enable Dual-VCA**.
3. Click **Save**.

4.7 Display Settings

It offers the parameter settings to adjust image features.

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

Click **Default** to restore settings.

4.7.1 Scene Mode

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

Image Adjustment

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

Exposure Settings

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

In manual mode, you need to set **Exposure Time**, **Gain** and **Slow Shutter**.

Focus

It offers options to adjust the focus mode.

Focus Mode

Auto

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

Semi-auto

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

Manual

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

Day/Night Switch

Day/Night Switch function can provide color images and black/white images in day and night mode. Switch mode is configurable.

Day

The image is always in color.

Night

The image is black/white or colorful and the supplement light will be enabled to ensure clear live view image at night.

Note

Only certain device models support the supplement light and colorful image.

Auto

The camera switches between the day mode and the night mode according to the light condition of environment.

Scheduled-Switch

Set the **Start Time** and the **End Time** to define the duration for day mode.

Triggered by alarm input

You can set **Triggering Status** as **Day** or **Night**. For example, if the **Triggering Status** is **Night**, the mode turns into **Night** when the device receives alarm input signal.

Triggered by video

The camera switches between the day mode and the night mode according to the light condition of environment. This mode is applicable when the device supports road traffic and vehicle detection.

Note

- Day/Night Switch function varies according to models.
- You can turn on the smart supplement light for better image effect. For supplement light settings, refer to ***Supplement Light Settings*** .

Supplement Light Settings

You can set supplement light and refer to the actual device for relevant parameters.

Smart Supplement Light

Smart supplement light avoids over exposure when the supplement light is on.

Supplement Light Mode

When the device supports supplement light, you can select supplement light mode.

IR Supplement Light

IR light is enabled.

White Light

White light is enabled.

Mixed Light

Both IR light and white light are enabled.

Smart

When you select this mode after enabling certain smart events or motion detection, in the night state, the default supplement light mode is IR supplement light mode. When the alarm is triggered, the white light is enabled and the device captures the target. After the alarm ends, the supplement light mode will switch to IR supplement light mode.

Only device models with IR and white light or hybrid supplement light with IR and white light support this function.

Off

Supplement light is disabled.

Note

The supplement light mode may vary according to different device models.

Brightness Adjustment Mode

Auto

The brightness adjusts according to the actual environment automatically.

Manual

You can drag the slider or set value to adjust the brightness.

BLC

If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC (backlight compensation) compensates light to the object in the front to make it clear. If BLC mode is set as **Custom**, you can draw a red rectangle on the live view image as the BLC area.

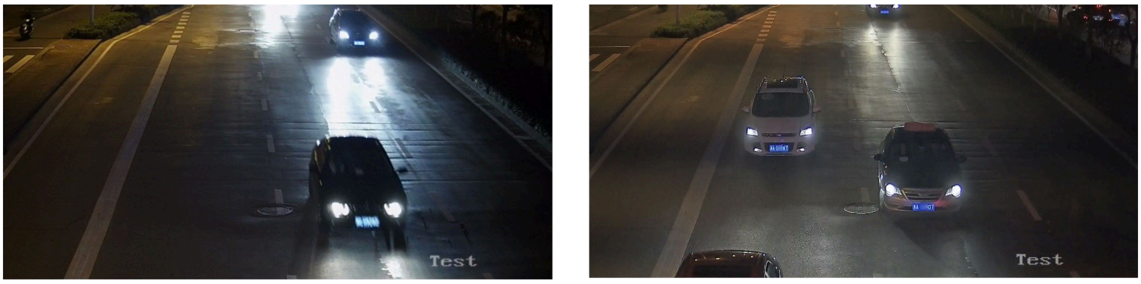
WDR

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

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

Note

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



WDR Off

WDR On

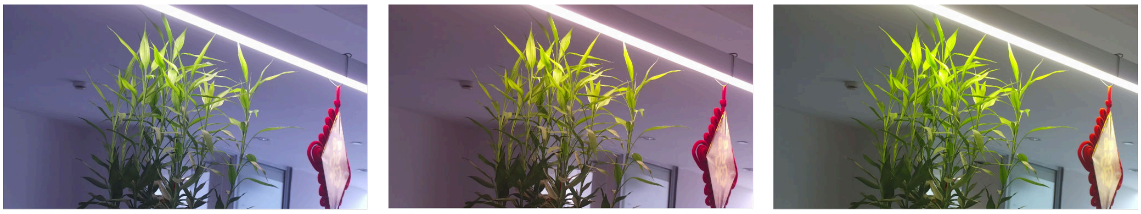
Figure 4-1 WDR

HLC

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

White Balance

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



Cold

Warm

Auto White Balance

Figure 4-2 White Balance

DNR

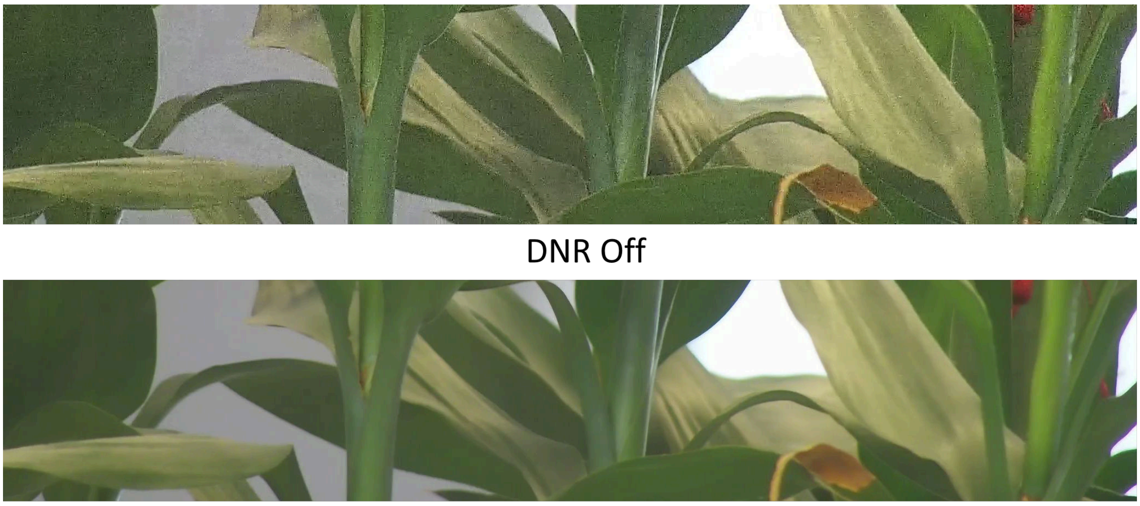
Digital Noise Reduction is used to reduce the image noise and improve the image quality. **Normal** and **Expert** modes are selectable.

Normal

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

Expert

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



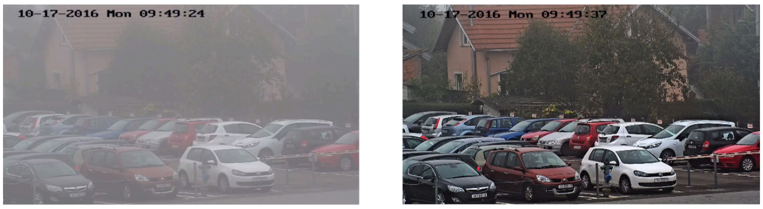
DNR Off

DNR On

Figure 4-3 DNR

Defog

You can enable the defog function when the environment is foggy and the image is misty. It enhances the subtle details so that the image appears clearer.



Defog Off

Defog On

Figure 4-4 Defog

EIS

Increase the stability of video image by using jitter compensation technology.

Gray Scale

You can choose the range of the **Gray Scale** as [0-255] or [16-235].

Mirror

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

Select the mirror mode as needed.

Note

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

Rotate

When this function is enabled, the live view will rotate 90° counterclockwise. For example, 1280 × 720 is rotated to 720 × 1280.

Enabling this function can change the effective range of monitoring in the vertical direction.

Note

This function is supported under certain settings.

Lens Distortion Correction

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

Note

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

4.7.2 Image Parameters Switch

The device automatically switches image parameters in set time periods.

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

Set Scheduled-switch

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

Steps

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

   Note

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

4.7.3 Video Standard

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

4.7.4 Local Video Output

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

Select the output mode as ON/OFF to control the output.

4.7.5 ShotN

It is available when Multi-Target-Type Detection is enabled, which can be used to optimize the effect of captured picture.

Note

- For certain device models, you should go to VCA and enable **Multi-Target-Type Detection** first.
- The function varies according to different device models.

Normal Mode

The mode is used to adaptively adjust the image capture effect of face and license plate, which can solve the overexposure of different types of targets captured in the same scene.

It can split the stream into 2 channels for face capture and license plate capture, and you can set the image parameters of 2 streams separately in the expert mode.

Close

Do not split the stream.

4.8 OSD

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

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

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

Character Set

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

Display

Set camera name, date, week, and their related display formats. For certain device models, you can also set tilt angle as the displayed information.

Format Settings

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

Text Overlay

Set customized overlay text on image.

4.9 Set Privacy Mask

The function blocks certain areas in the live view to protect privacy. No matter how the device moves, the blocked scene will never be seen.

Steps

1. Go to **Configuration → Image → Privacy Mask** .
2. Check **Enable**.
3. Click ▭ . Drag the mouse in the live view to draw a closed area.

Drag the corners of the area	Adjust the size of the area.
Drag the area	Adjust the position of the area.
Click 🗑	Clear all the areas you set.

4. Click **Add** to add a privacy mask and set **Region Name** and **Mask Type**.
5. Click **Save**.

4.10 Overlay Picture

Overlay a customized picture on live view.

Before You Start

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

Steps

1. Go to **Configuration → Image → Picture Overlay** .
2. Check **Enable**.
3. Click **Upload** to select a picture and open it.

   The picture with a red rectangle will appear in live view after successfully uploading.
4. Drag the red rectangle to adjust the picture position.
5. Click **Save**.

Chapter 5 Video Recording and Picture Capture

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

5.1 Storage Settings

This part introduces the configuration of several common storage paths.

5.1.1 Memory Card

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

Set New or Unencrypted Memory Card

Before You Start

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

Steps

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

   Note

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

3. Click **Format** to initialize the memory card.

   When the **Status** of memory card turns from **Uninitialized** to **Normal**, the memory card is ready for use.

4. **Optional:** Encrypt the memory card.

   1) Click **Encrypted Format**.
   2) Set the encryption password.
   3) Click **OK**.

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

   Note

   Keep your encryption password properly. Encryption password cannot be found if forgotten.

5. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.

6. Click **Save**.

Set Encrypted Memory Card

Before You Start

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

Steps

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

   Note

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

3. Verify the encryption password.
   1) Click **Parity**.
   2) Enter the encryption password.
   3) Click **OK**.

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

   Note

   If the encryption password is forgotten and you still want to use this memory card, see ***Set New or Unencrypted Memory Card*** to format and set the memory card. All existing contents will be removed.

4. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.
5. Click **Save**.

Detect Memory Card Status

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

Before You Start

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

Steps

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

   Remaining Lifespan

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

Health Status

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

Note

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

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

Note

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

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

5.1.2 Set FTP

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

Before You Start

Get the FTP server address first.

Steps

1. Go to **Configuration → Event → Alarm Setting → FTP** .
2. Configure FTP settings.

   FTP Protocol

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

   Server IP Address and Port No.

   The FTP server address and corresponding port.

   User Name and Password

   The FTP user should have the permission to upload pictures.

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

   Note

   Anonymous login is not supported when SFTP protocol is selected.

   Directory Structure

   The saving path of snapshots in the FTP server.
3. **Optional:** Check **Upload Picture** to enable uploading snapshots to the FTP server.

   Picture Filing Interval

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

   Picture Name

   Set the naming rule for captured pictures. You can choose **Default** in the drop-down list to use the default rule, that is, IP address_channel number_capture time_event type.jpg (e.g., 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg). Or you can customize it by adding a **Custom Prefix** to the default naming rule.
4. **Optional:** Check **Enable Automatic Network Replenishment**.

   Note

   Upload to FTP/Memory Card/NAS in **Linkage Method** and **Enable Automatic Network Replenishment** should be both enabled simultaneously.
5. Click **Test** to verify the FTP server.
6. Click **Save**.

5.1.3 Set NAS

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

Before You Start

Get the IP address of the network disk first.

Steps

1. Go to NAS setting page: **Configuration → Storage → Storage Management → Net HDD** .
2. Click **Add**.
3. Set **Mounting Type**.

   Mounting Type

   Select file system protocol according to the operation system.

   Enter user name and password of the net HDD to guarantee the security if **SMB/CIFS** is selected.
4. Set the **Server Address** and **File Path** for the disk.

   Server Address

   The IP address of the network disk.

   File Path

   The saving path of network disk files.
5. Click **Test** to check whether the network disk is available.
6. Click **OK** to finish the steps to add a Net HDD.
7. **Optional:** Configure the Net HDD.

   Edit Click ✎ to edit the parameter setting.

   Delete Delete the Net HDD.

   - Click 🗑 .
   - Select the Net HDD, click **Delete**.
8. Click **Save**.

5.1.4 eMMC Protection

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

Note

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

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

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

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

5.1.5 Set Cloud Storage

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

Steps

⚠**Caution**

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

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

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

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

5.2 Video Recording

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

5.2.1 Record Automatically

This function can record video automatically during configured time periods.

Before You Start

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

Steps

1. Go to **Configuration → Storage → Schedule Settings → Record Schedule** .
2. Check **Enable**.
3. Select a record type.

Note

The record type is vary according to different models.

Continuous

The video will be recorded continuously according to the schedule.

Motion

When motion detection is enabled and trigger recording is selected as linkage method, object movement is recorded.

Alarm

When alarm input is enabled and trigger recording is selected as linkage method, the video is recorded after receiving alarm signal from external alarm input device.

Motion | Alarm

Video is recorded when motion is detected or alarm signal is received from the external alarm input device.

Motion & Alarm

Video is recorded only when motion is detected and alarm signal is received from the external alarm input device.

Event

The video is recorded when configured event is detected.

4. Set schedule for the selected record type. Refer to ***Set Arming Schedule*** for the setting operation.
5. Set the advanced recording parameters.

Overwrite

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

Pre-record

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

Post-record

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

Stream Type

Select the stream type for recording.

Note

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

Recording Expiration

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

6. Click **Save**.

5.2.2 Record Manually

Steps

1. Go to **Configuration → Local** .
2. Set the **Video Size** and **Video Saving Path** for recorded video files.
3. Click **Save**.
4. Click ◎ in the live view interface to start recording. Click ◉ to stop recording.

What to do next

View the recorded video files.

Go to **Configuration → Local** and click **Open** behind **Video Saving Path** to open the saving path and view the files.

5.2.3 Playback and Download Video

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

Steps

1. Go to **Playback → Video** .
2. Set search condition and click **Search**.

   The matched video files showed on the timing bar.
3. Click ▶ to play the video files.
   - Click ⛶ to play video files in full screen. Press **ESC** to exit full screen.
   - Click ⧠ to stop video playback for all channels.
4. **Optional:** Click ✂ to clip video files. Click ✂ again to stop clipping video files

   Note

   Go to **Configuration → Local → Clip Saving Path** , view and change the saving path of clipped video files.
5. **Optional:** Click ⤓ on the playback interface to download files.

   Note

   Go to **Configuration → Local → Downloaded File Saving Path** , view and change the saving path of downloaded video files.

5.3 Capture Configuration

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

5.3.1 Capture Automatically

This function can capture pictures automatically during configured time periods.

Before You Start

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

Steps

1. Go to **Configuration → Storage → Schedule Settings → Picture Capture** .
2. Set capture schedule. Refer to ***Set Arming Schedule*** for configuring schedule time.

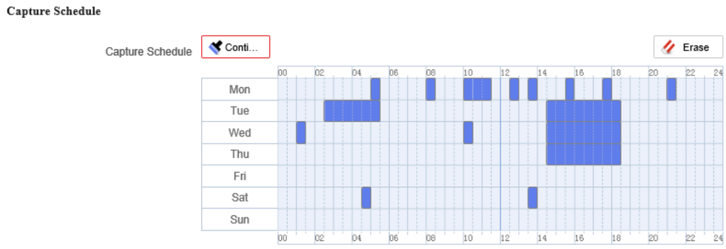


Figure 5-1 Set Capture Schedule

3. Set the capture type.

   Scheduled

   Capture a picture at the configured time interval.

   Event-Triggered

   Capture a picture when an event is triggered.

4. Set the **Format**, **Resolution**, **Quality**, **Interval**, and **Capture Number**.

   Note

   The resolution of the captured picture is the same as the resolution of the captured picture stream. You can select **Stream Type** in **Advanced**.

5. Click **Save**.

5.3.2 Capture Manually

Steps

1. Go to **Configuration → Local** .

2. Set the **Image Format** and saving path to for snapshots.

   JPEG

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

   BMP

   The picture is compressed with good quality.
3. Click **Save**.
4. Click 📷 near the live view or play back window to capture a picture manually.

5.3.3 View and Download Picture

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

Steps

1. Go to **Playback → Picture** .
2. Set search condition and click **Search**.

   The matched pictures showed in the file list.
3. Download the pictures.
   - Select the pictures then click **Download** to download them.
   - Click **Download This Page** to download the pictures of this page.
   - Click **Download All** to download all the pictures.

Note

Go to **Configuration → Local → Playback Capture Saving Path** , view and change the saving path of captured pictures when playback.

Chapter 6 Event and Alarm

This part introduces the configuration of events. The device takes certain response to triggered alarm. Certain events may not be supported by certain device models.

6.1 Set Motion Detection

It helps to detect the moving objects in the detection region and trigger the linkage actions.

Steps

1. Go to **Configuration → Event → Event and Detection → Motion Detection** .
2. Check **Enable**.
3. **Optional:** Highlight to display the moving object in the image in green.
   1) Check **Enable Dynamic Analysis for Motion**.
   2) Go to **Configuration → Local** .
   3) Set **Rules** to **Enable**.
4. Select mode in **Configuration**, and set rule region and rule parameters.
   - For the information about normal mode, see ***Normal Mode*** .
   - For the information about expert mode, see ***Expert Mode*** .
5. Set the arming schedule and linkage methods. For the information about arming schedule settings, see ***Set Arming Schedule*** . For the information about linkage methods, see ***Linkage Method Settings*** .
6. Click **Save**.

6.1.1 Expert Mode

You can configure different motion detection parameters for day and night according to the actual needs.

Steps

1. Select **Expert Mode** in **Configuration**.
2. Set parameters of expert mode.

   Scheduled Image Settings

   OFF

   Image switch is disabled.

   Auto-Switch

   The system switches day/night mode automatically according to environment. It displays colored image at day and black and white image at night.

   Scheduled-Switch

The system switches day/night mode according to the schedule. It switches to day mode during the set periods and switches to night mode during the other periods.

Sensitivity

The higher the value of sensitivity is, the more sensitive the motion detection is. If scheduled image settings is enabled, the sensitivity of day and night can be set separately.

3. Select an **Area** and click ▭ . Click and drag the mouse on the live image and then release the mouse to finish drawing one area.

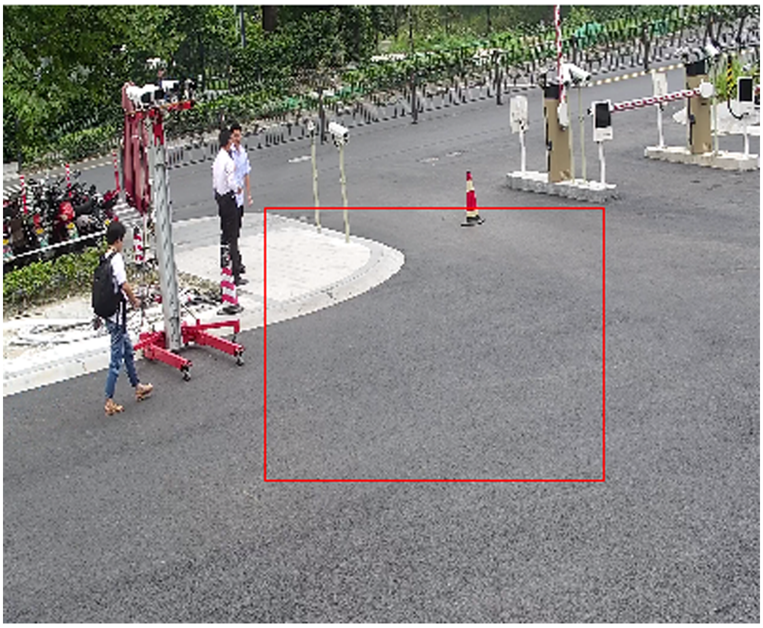


Figure 6-1 Set Rules

4. Click 🗑 to clear all the areas.
5. Click **Save**.
6. **Optional:** Repeat above steps to set multiple areas.

6.1.2 Normal Mode

You can set motion detection parameters according to the device default parameters.

Steps

1. Select **Normal Mode** in **Configuration**.
2. Set the **Sensitivity** of normal mode. The higher the value of sensitivity is, the more sensitive the motion detection is. If the sensitivity is set to ***0***, motion detection and dynamic analysis do not take effect.
3. Set **Detection Target**. Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including the human and vehicle. This function allows alarm triggering by specified target types (human and vehicle).

Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

4. Click ▭ . Click and drag the mouse on the live image, and then right click the mouse to finish drawing one area.
5. **Optional:** Click 🗑 to clear all the areas.
6. **Optional:** You can set the parameters of multiple areas by repeating the above steps.

6.2 Set Video Tampering Alarm

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

Steps

1. Go to **Configuration → Event → Event and Detection → Video Tampering** .
2. Check **Enable**.
3. Set the **Sensitivity**. The higher the value is, the easier to detect the area covering.
4. Click ▭ and drag the mouse in the live view to draw the area.

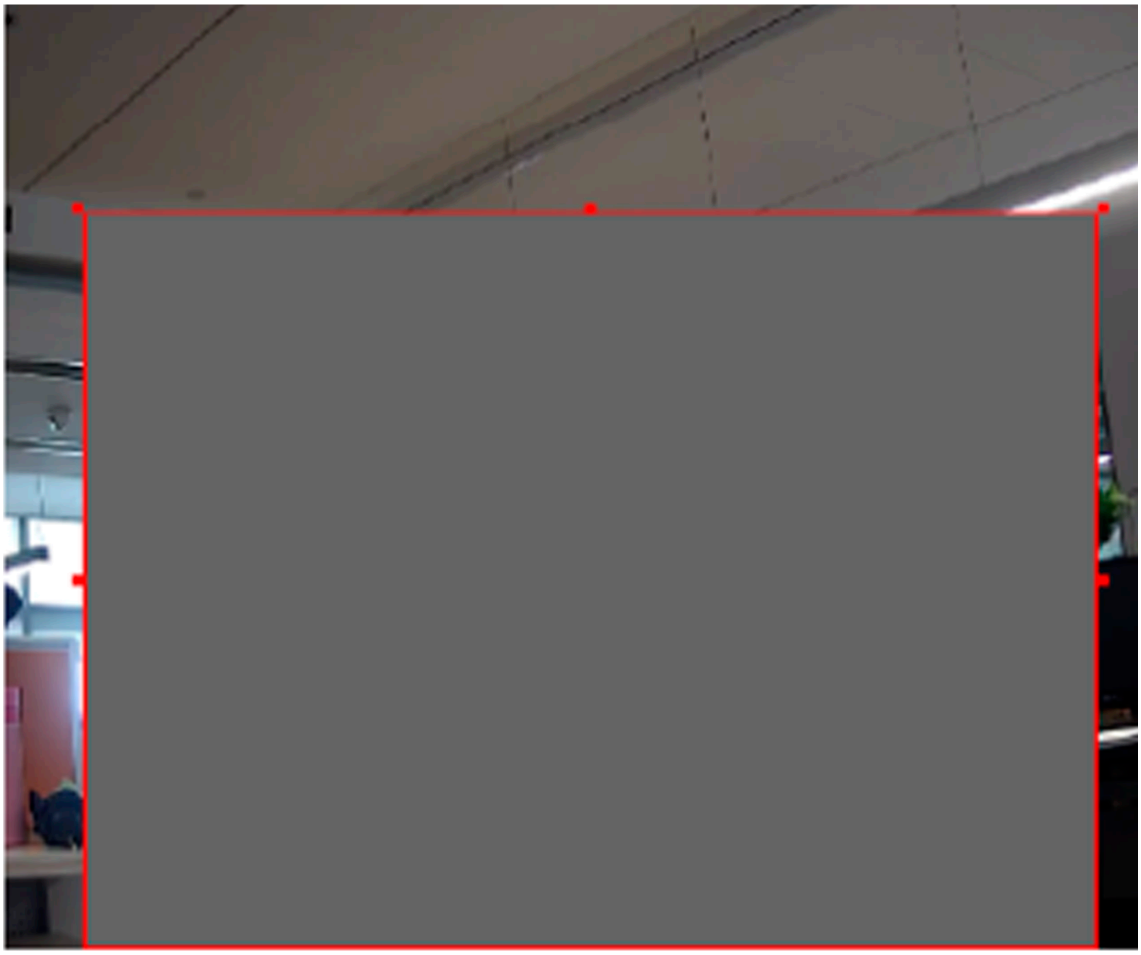


Figure 6-2 Set Video Tampering Area

5. **Optional:** Click 🗑 to delete all the drawn areas.
6. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
7. Click **Save**.

6.3 Set Alarm Input

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

Before You Start

Note

This function is only supported by certain models.

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

Steps

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

6.4 Set Exception Alarm

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

Steps

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

   HDD Full

   The HDD storage is full.

   HDD Error

   Error occurs in HDD.

   Network Disconnected

   The device is offline.

   IP Address Conflicted

   The IP address of current device is same as that of other device in the network.

   Illegal Login

   Incorrect user name or password is entered.

   Abnormal Restart

   The device restarts abnormally.
3. Refer to ***Linkage Method Settings*** for setting linkage method.
4. Click **Save**.

6.5 Set Video Quality Diagnosis

When the video quality of the device is abnormal and the alarm linkage is set, the alarm will be triggered automatically.

Steps

1. Go to **Configuration → Event → Event and Detection → Video Quality Diagnosis** .
2. Select **Diagnosis Type**.

3. Set the corresponding parameters.

   Alarm Detection Interval

   The time interval to detect the exception.

   Sensitivity

   The higher the value is, the more easily the exception will be detected, and the higher possibility of misinformation would be.

   Alarm Delay Times

   The device uploads the alarm when the alarm reaches the set number of times.
4. Check the selected diagnosis type, and the related type will be detected.
5. Set arming schedule. See ***Set Arming Schedule*** .
6. Set linkage method. See ***Linkage Method Settings*** .
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with models.

6.6 Set Vibration Detection

It is used to detect whether the device is vibrating. The device reports an alarm and triggers linkage actions if the function is enabled.

Steps

1. Go to **Configuration → Event → Event and Detection → Vibration Detection** .
2. Check **Enable**.
3. Drag the slider to set the detection sensitivity. You can also enter number to set the sensitivity.
4. Set the arming schedule. See ***Set Arming Schedule*** .
5. Set the linkage method. See ***Linkage Method Settings*** .
6. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with models.

6.7 Set Audio Exception Detection

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

Steps

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

Audio Loss Detection

Detect sudden loss of audio track.

Sudden Increase of Sound Intensity Detection

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

Note

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

Sudden Decrease of Sound Intensity Detection

Detect sudden decrease of sound intensity. **Sensitivity** is configurable.

3. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage methods.
4. Click **Save**.

Note

The function is only supported by certain models. The actual function varies according to different models.

6.8 Set Defocus Detection

The blurred image caused by lens defocus can be detected. If it occurs, the device can take linkage actions.

Steps

1. Go to **Configuration → Event → Event and Detection → Defocus Detection** .
2. Check **Enable**.
3. Set **Sensitivity**. The higher the value is, the more easily the defocus image can trigger the alarm. You can adjust the value according to the actual environment.
4. For the linkage method settings, refer to ***Linkage Method Settings*** .
5. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with models.

6.9 Set Scene Change Detection

Scene change detection function detects the change of the scene. Some certain actions can be taken when the alarm is triggered.

Steps

1. Go to **Configuration → Event → Event and Detection → Scene Change Detection** .
2. Click **Enable**.
3. Set the **Sensitivity**. The higher the value is, the more easily the change of scene can be detected. But the detection accuracy is reduced.
4. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
5. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with models.

Chapter 7 Arming Schedule and Alarm Linkage

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

7.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

1. **Optional:** Click **Arming Schedule and Linkage Method** in the related event interface.
2. Click **Edit** behind **Arming Schedule**.
3. Click **Draw**, and drag the time bar to draw desired valid time.

Note

- Each cell represents 30 minutes.
- Move the mouse over the drawn time period to see specific time periods and fine-tune the start time and end time.
- Up to 8 periods can be configured for one day.

4. Click **Erase**, and drag the time bar to clear selected valid time.
5. Click **OK** to save the settings.

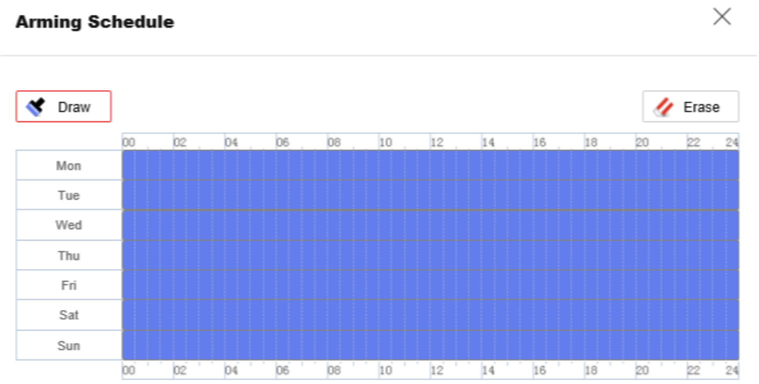


Figure 7-1 Set Arming Schedule

7.2 Linkage Method Settings

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

7.2.1 Trigger Alarm Output

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

Steps

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

   Automatic Alarm For the information about the configuration, see ***Automatic Alarm*** .

   Manual Alarm For the information about the configuration, see ***Manual Alarm*** .

Manual Alarm

You can trigger an alarm output manually.

Before You Start

Make sure the alarm output device is connected to the device.

Steps

1. Select the **Alarm Output No.** according to the alarm interface connected to the external alarm device. Click ✎ to set alarm parameters.

   Alarm Name

   Custom a name for the alarm output.
2. Click **Manual Alarm** to enable manual alarm output.
3. **Optional:** Click **Clear Alarm** to disable manual alarm output.

Automatic Alarm

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

Before You Start

Make sure the alarm output device is connected to the device.

Steps

1. Select the **Alarm Output No.** according to the alarm interface connected to the external alarm device. Click ✎ to set alarm parameters.

   Alarm Name

   Custom a name for the alarm output.

   Delay

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

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

7.2.2 FTP/NAS/Memory Card Uploading

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

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

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

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

7.2.3 Send Email

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

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

Set Email

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

Before You Start

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

Steps

1. Go to email settings page: **Configuration → Event → Alarm Setting → Email** .
2. Set email parameters.
   1) Input the sender's email information, including the **Sender's Address**, **SMTP Server**, and **SMTP Port**.
   2) **Optional:** If your email server requires authentication, check **Authentication** and input your user name and password to log in to the server.
   3) Set the **E-mail Encryption**.
      - When you select **TLS**, and disable STARTTLS, emails are sent after encrypted by TLS. The SMTP port should be set as 465.
      - When you select **TLS** and check **Enable STARTTLS**, emails are sent after encrypted by STARTTLS, and the **SMTP Port** should be set as 25.

Note

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

4) **Optional:** If you want to receive notification with alarm pictures, check **Attached Picture**. The notification email has a certain number of attached alarm pictures about the event with configurable image capturing interval.

Note

The number of alarm pictures may vary according to different device models and different events.

5) Input the recipient's information, including the recipient's name and address.
6) Click **Test** to see if the function is well configured.

3. Click **Save**.

7.2.4 Notify Surveillance Center

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

7.2.5 Trigger Recording

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

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

7.2.6 Audible Warning

After enabling **Audible Warning** and setting **Audible Alarm Output**, the built-in speaker of the device or connected external speaker plays warning sounds when an alarm happens.

For audible alarm output settings, refer to ***Set Audible Alarm Output*** .

Note

The function is only supported by certain camera models.

Set Audible Alarm Output

When the device detects targets in the detection area, audible alarm can be triggered as a warning.

Steps

1. Go to **Configuration → Event → Alarm Setting → Audible Alarm Output** .

2. Select **Sound Type** and set related parameters.
   - Select **Prompt** and set the alarm times you need.
   - Select **Warning** and its contents. Set the alarm times you need.
   - Select **Custom Audio**. You can select a custom audio file from the drop-down list. If no file is available, you can click **Set → Add** to upload an audio file that meets the requirement. Up to three audio files can be uploaded.
3. **Optional:** Click **Test** to play the selected audio file on the device.
4. Set arming schedule for audible alarm. See ***Set Arming Schedule*** for details.
5. Click **Save**.

Note

The function is only supported by certain device models.

7.2.7 Alarm Server

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

Set Alarm Server

Steps

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

Note

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

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

Chapter 8 Network Settings

8.1 TCP/IP

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

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

NIC Type

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

IPv4

Two IPv4 modes are available.

DHCP

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

Note

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

Manual

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

IPv6

Three IPv6 modes are available.

Route Advertisement

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

Note

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

DHCP

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

Manual

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

MTU

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

The valid value range of MTU is 1280 to 1500.

DNS

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

Domain Name Settings

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

Note

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

8.2 Access to Device via Domain Name

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

Before You Start

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

Steps

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

   DynDNS

   Dynamic DNS server is used for domain name resolution.

   NO-IP

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

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

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

8.3 Access to Device via PPPoE Dial Up Connection

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

Steps

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

   Dynamic IP

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

   User Name

   User name for dial-up network access.

   Password

   Password for dial-up network access.

   Confirm

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

By Browsers	Enter the WAN dynamic IP address in the browser address bar to access the device.
By Client Software	Add the WAN dynamic IP address to the client software. Refer to the client manual for details.

Note

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

8.4 SNMP

You can set the SNMP (Simple Network Management Protocol) to get device information in network management.

Before You Start

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

Steps

1. Go to **Configuration → Network → Network Settings → SNMP** .
2. Check **Enable SNMPv1**, **Enable SNMP v2c** or **Enable SNMPv3**.

   Note

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

8.5 Set IEEE 802.1X

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

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

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

Note

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

8.6 Set QoS

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

Note

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

Steps

1. Go to **Configuration → Network → Network Settings → QoS** .
2. Set **Video/Audio DSCP**, **Event/Alarm DSCP** and **Management DSCP**.

Note

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

3. Click **Save**.

8.7 HTTP(S)

HTTP is an application-layer protocol for transmitting hypermedia documents. HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Configuration → Network → Network Service → HTTP(S)** .
2. Enter **HTTP Port**.

   Note

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

   Note

   You can click **TLS Settings** to set the TLS version that the device supports. Refer to for details.
4. Enter **HTTPS Port**.
5. **Optional:** Check **HTTPS Browsing** to access the device only via HTTPS protocol.
6. Select **Server Certificate**.
7. Set **Web Authentication**.

   Authentication

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

   Digest Algorithm

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

8.8 Multicast

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

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

IP Address

It stands for the address of multicast host.

8.8.1 Multicast Discovery

Go to **Configuration → Network → Network Settings → TCP/IP** to enable this function.

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

8.9 RTSP

RTSP (Real Time Streaming Protocol) is an application-layer controlling protocol for streaming media.

Steps

1. Go to **Configuration → Network → Network Service → RTSP** .
2. Enter **Port**.
3. Set **Multicast** parameters.

   Stream Type

   The stream type as the multicast source.

   Video Port

   The video port of the selected stream.

   Audio Port

   The audio port of the selected stream.
4. Set **RTSP Authentication**.

   Authentication

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

   Digest Algorithm

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

5. Click **Save**.

8.10 Set SRTP

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

Steps

1. Go to **Configuration → Network → Network Service → SRTP** .
2. Enter the **Port** number.
3. Set **Multicast** parameters.

   Stream Type

   The stream type as the multicast source.

   Video Port

   The video port of the selected stream.

   Audio Port

   The audio port of the selected stream.
4. Select **Server Certificate**.
5. Select **Encrypted Algorithm**.
6. Click **Save**.

Note

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

8.11 Bonjour

It is an implementation of zero-configuration networking (zeroconf), a group of technologies that includes service discovery, address assignment, and hostname resolution. Bonjour locates devices such as printers, other computers, and the services that those devices offer on a local network using multicast Domain Name System (mDNS) service records.

Go to **Configuration → Network → Network Service → Bonjour** to enable the function, and click **Save**.

After enabling the function, the device spread and receive service information in local area network.

8.12 WebSocket(s)

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

Go to **Configuration → Network → Network Service → WebSocket(s)** to set parameters, and click **Save**.

WebSocket

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

WebSockets

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

8.13 Port Mapping

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

Steps

1. Go to **Configuration → Network → Network Service → NAT** .
2. Select the port mapping mode.

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

3. Click **Save**.

8.13.1 Set Auto Port Mapping

Steps

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

Note

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

8.13.2 Set Manual Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the device, or you can use the default name.

2. Select the port mapping mode to **Manual**, and set the external port to be the same as the internal port.
3. Click **Save**.

What to do next

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

8.13.3 Set Port Mapping on Router

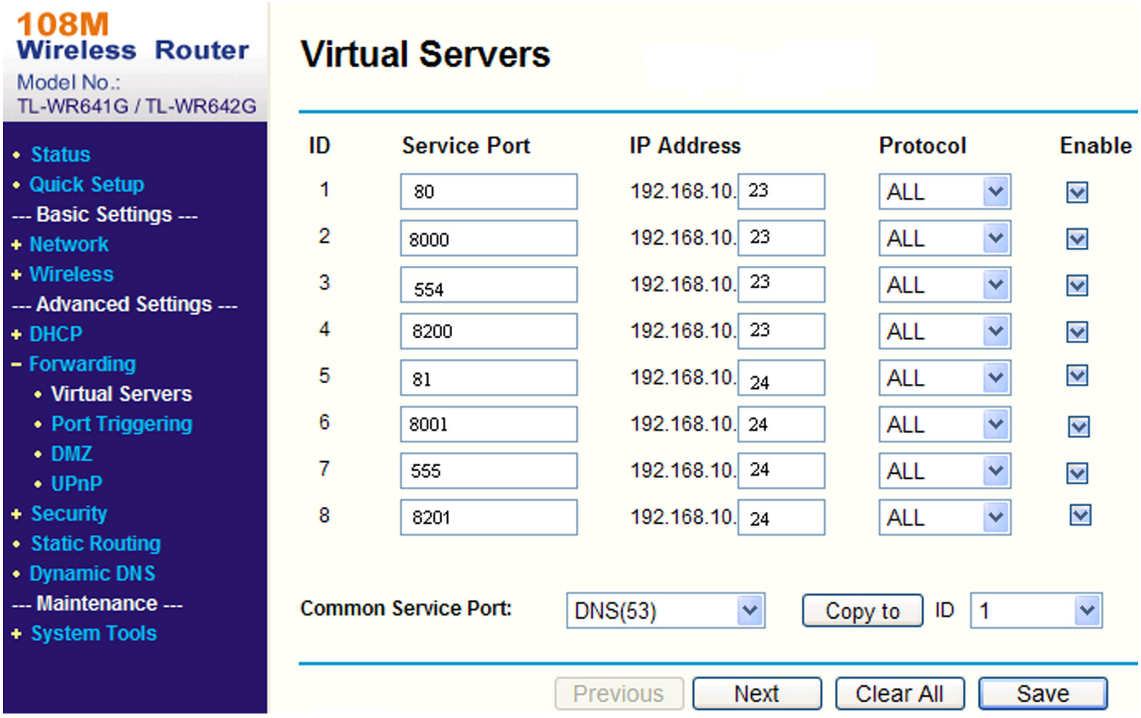
The following settings are for a certain router. The settings vary depending on different models of routers.

Steps

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

Example

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



Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10. 23	ALL	☑
2	8000	192.168.10. 23	ALL	☑
3	554	192.168.10. 23	ALL	☑
4	8200	192.168.10. 23	ALL	☑
5	81	192.168.10. 24	ALL	☑
6	8001	192.168.10. 24	ALL	☑
7	555	192.168.10. 24	ALL	☑
8	8201	192.168.10. 24	ALL	☑

Common Service Port: DNS(53) Copy to ID 1

Figure 8-1 Port Mapping on Router

Note

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

8.14 RTCP

The device relies on RTCP (Real-time Transport Control Protocol) to deliver packets sequentially to provide a reliable delivery mechanism and to provide services for flow control or congestion control.

Go to **Configuration → Network → Network Service → RTCP** and check **Enable** to enable the function.

8.15 Wireless Dial

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

Note

The function is only supported by certain device models.

8.15.1 Set Wireless Dial

The built-in wireless module offers dial-up access to the Internet for the device.

Before You Start

Get a SIM card, and activate 3G/4G services. Insert the SIM card to the corresponding slot.

Steps

1. Go to **Configuration → Network → Network Settings → Wireless Dial** .
2. Check to enable the function.
3. Go to **Dial Parameters** to configure and save the parameters.
4. Click **Settings** behind **Dial Plan**. See ***Set Arming Schedule*** for detailed information.
5. View the **Dial Status**.

Click Refresh	Refresh the dial status.
Click Disconnect	Disconnect the 3G/4G wireless network.

   When the **Dial Status** turns to **Connected**, it means a successful dial.
6. Access the device via the **IP Address** of the computer in the network.
   - Input the IP address in the browser to access the device.
   - Add the device in client application. Select **IP/Domain**, and input IP address and other parameters to access the device.

7. **Optional:** You can view 4G SIM card information and network carrier information.

Note

For certain device models working on **Performance Mode** or **Proactive Mode**, the wireless mode can be upgraded. If necessary, please upgrade the wireless mode under the guidance of a professional.

8. **Optional:** Click **Re-Camp** to reconnect the device to wireless network manually. The device will maintain airplane mode for 10 seconds and then connects to network automatically.
9. **Optional:** Check **Enable** to enable **Auto Re-Camp**, and then set the **Re-Camp Interval**. The device will reconnect to the wireless network at set **Re-Camp Interval** automatically.

Note

The function may vary according to different device models.

8.15.2 Wireless Expert Settings

Wireless expert settings provide more details of the 3G/4G wireless network to which the device connects and help the professionals troubleshoot potential network issues.

Cell Radio Frequency Parameters

Cell radio frequency parameters provides the current wireless network information to which the device is connected.

Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings** to view cell radio frequency parameters.

Network Info

It displays the current cellular network information. You can click **Refresh** to view the frequency information of different cells.

Radio Frequency Fluctuation

It records the fluctuation of the cellular network to which the device has connected during the past 7 days. Click **Export Report** and set and confirm the encryption password to export the fluctuation report.

Lock Band

You can lock a set of bands that get the device faster data rates to improve the network speed.

Steps

1. Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings → Lock Band** .
2. Check **Enable**.

3. Click **Add** and enter the band.

Note

- The band you enter should be B + number or N + number. For example, you can enter B1 or N1.
- Up to five bands are supported.

4. **Optional:** Click 🗑 to delete the selected band. You can also click **Clear All** to clear the list.

Capture Baseband Packet

This function can capture the protocol interaction packet to help the professionals to locate the communication failures between 4G module and the base station.

Steps

Note

This function is reserved for the professionals and technical support staff.

1. Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings** .
2. Click **Configuration** behind **Capture Baseband Packet** to enter the setting interface.
3. Check **Enable** to enable this function.
4. Set capture duration and the saving path. The saving path depends on the actual storage method of the device. You can click **Delete Captured Packet Under This Path** to delete the captured packet.
5. Click **Save**.
6. Click **Start Capturing Packet** to capture the baseband packet.
7. **Optional:** Click **Stop Capturing** to stop the capturing process.
8. After the capturing is completed, click **Export Captured Packet** to save the report.

Speed Test

Steps

1. Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings** .
2. Click **Configuration** behind **Speed Test** to enter the setting interface.
3. Select the default server or enter the server address. You can follow the steps below to get the nearby server address.

Note

You can follow the steps below to get the nearby server address.

a. Visit this website to get the nearby server address: ***https://www.speedtest.net/speedtest-servers-static.php*** .

b. Select and copy the URL of the nearby speed test station and paste it in **Server Address**.

4. Click **Speed Test** to start the test.

   You can view the speed details after the test is completed. You can also click **Export Speed Test Result**.

8.16 Traffic Shaping

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

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

8.17 Data Monitoring

You can view and manage the SIM card data or wired network data used by the device. SIM card data is the data service provided by network carriers; wired network data is usually provided through a 4G router.

Steps

1. Go to **Configuration → Network → Network Settings → Data Monitoring** .
2. Check **Enable**.
3. Set the following parameters according to your data plan.

   Plan Type

   Daily, **Monthly**, or **Annually** can be selected.

   Data Plan

   Enter the amount of usable data and select the unit.

   Pre-Alarm Threshold

   When the used data reaches the set percentage of data plan, the device sends an alarm message, and shows notification on the OSD or pop-up window.
4. Select **Normal Linkage**.

   If **Send Email** or **Notify Surveillance Center** is selected, the device sends an alarm message by Email or to surveillance center when the used data reaches the threshold.
5. Click **Save**.

Note

The function varies with different device models.

8.18 Set ISUP

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

Steps

1. Go to **Configuration → Network → Platform Access → ISUP** .
2. **Optional:** Select an access center.
3. Check **Enable**.
4. Select a protocol version and enter related parameters.
5. Click **Save**.

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

8.19 Set OTAP

The device can be accessed to the maintenance platform via OTAP protocol, in order to search and acquire device information, upload device status and alarm information, reboot and update the device.

Steps

1. Go to **Configuration → Network → Platform Access → OTAP** to enable the function.
2. Set related parameters.
3. Click **Test** to check if the device connects to server.
4. Click **Save**.

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

8.20 Access Camera via Hik-Connect

Hik-Connect is an application for mobile devices. Using the App, you can view live image, receive alarm notification and so on.

Before You Start

Connect the camera to network with network cables.

Steps

1. Get and install Hik-Connect application by the following ways.
   - Visit ***https://appstore.hikvision.com*** to download the application according to your mobile phone system.
   - Visit the official site of our company. Then go to **Support → Tools → Hikvision App Store** .
   - Scan the QR code below to download the application.

Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit ***https://appstore.hikvision.com/static/help/index.html*** to refer to the troubleshooting.
- Visit ***https://appstore.hikvision.com/*** , and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

2. Start the application and register for a Hik-Connect user account.
3. Log in after registration.
4. In the app, tap "+" on the upper-right corner and then scan the QR code of the camera to add the camera. You can find the QR code on the camera or on the cover of the Quick Start Guide of the camera in the package.
5. Follow the prompts to set the network connection and add the camera to your Hik-Connect account.

   For detailed information, refer to the user manual of the Hik-Connect app.

8.20.1 Enable Hik-Connect Service on Camera

Hik-Connect service should be enabled on your camera before using the service.

You can enable the service through SADP software or Web browser.

Enable Hik-Connect Service via Web Browser

Follow the following steps to enable Hik-Connect Service via Web Browser.

Before You Start

You need to activate the camera before enabling the service.

Steps

1. Access the camera via web browser.
2. Enter platform access configuration interface. **Configuration → Network → Platform Access → Hik-Connect** .
3. Check **Enable**.
4. Click and read "Terms of Service" and "Privacy Policy" in pop-up window.
5. Create a verification code or change the old verification code for the camera.

   Note

   The verification code is required when you add the camera to Hik-Connect service.

6. Save the settings.

Enable Hik-Connect Service via SADP Software

This part introduce how to enable Hik-Connect service via SADP software of an activated camera.

Steps

1. Run SADP software.
2. Select a camera and enter **Modify Network Parameters** page.
3. Check **Enable Hik-Connect**.
4. Create a verification code or change the old verification code.

Note

The verification code is required when you add the camera to Hik-Connect service.

5. Click and read "Terms of Service" and "Privacy Policy".
6. Confirm the settings.

8.20.2 Set Up Hik-Connect

Steps

1. Get and install Hik-Connect application by the following ways.
   - Visit ***https://appstore.hikvision.com*** to download the application according to your mobile phone system.
   - Visit the official site of our company. Then go to **Support → Tools → Hikvision App Store** .
   - Scan the QR code below to download the application.

Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit ***https://appstore.hikvision.com/static/help/index.html*** to refer to the troubleshooting.
- Visit ***https://appstore.hikvision.com/*** , and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

2. Start the application and register for a Hik-Connect user account.
3. Log in after registration.

8.20.3 Add Camera to Hik-Connect

Steps

1. Connect your mobile device to a Wi-Fi.
2. Log into the Hik-Connect app.
3. In the home page, tap "+" on the upper-right corner to add a camera.
4. Scan the QR code on camera body or on the *Quick Start Guide* cover.

Note

If the QR code is missing or too blur to be recognized, you can also add the camera by inputting the camera's serial number.

5. Input the verification code of your camera.

Note

- The required verification code is the code you create or change when you enable Hik-Connect service on the camera.
- If you forget the verification code, you can check the current verification code on **Platform Access** configuration page via web browser.

6. Tap **Connect to a Network** button in the popup interface.
7. Choose **Wired Connection** or **Wireless Connection** according to your camera function.

Wireless Connection	Input the Wi-Fi password that your mobile phone has connected to, and tap **Next** to start the Wi-Fi connection process. (Locate the camera within 3 meters from the router when setting up the Wi-Fi.)
Wired Connection	Connect the camera to the router with a network cable and tap **Connected** in the result interface.

Note

The router should be the same one which your mobile phone has connected to.

8. Tap **Add** in the next interface to finish adding.

For detailed information, refer to the user manual of the Hik-Connect app.

8.21 Set Open Network Video Interface

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

Steps

1. Go to **Configuration → Network → Platform Access → Open Network Video Interface** .
2. Check **Enable**.
3. Select an authentication mode.
   - If you select **Digest**, the device only supports digest authentication.

- If you select **Digest&ws-username token**, the device supports digest authentication or ws-username token authentication.

4. Click **Add** to configure the Open Network Video Interface user.
5. Click **Save**.
6. **Optional:** Repeat the steps above to add more Open Network Video Interface users.
7. **Optional:** Manage the user.
   - Click 🗑 to delete the selected Open Network Video Interface user.
   - Click ✎ to modify the selected Open Network Video Interface user.

8.22 Set SDK Service

If you want to add the device to the client software, you should enable SDK Service or Enhanced SDK Service.

Steps

1. Go to **Configuration → Network → Platform Access → SDK Service** .
2. Set **SDK Service** parameters.
   1) Check **Enable** to add the device to the client software with SDK protocol.
   2) Enter the **Port** number.
3. Set **Enhanced SDK Service** parameters.
   1) Check **Enable** to add the device to the client software with SDK over TLS protocol.
   2) **Optional:** Click **TLS Settings** to enable the TLS version that the device supports. Refer to ***TLS*** for details.
   3) Enter the **Port** number.
   4) Select a server certificate to make sure the data transmission security. You can click **Certificate Management** to add a certificate. Refer to ***Certificate Management*** for details.
4. Click **Save**.

Chapter 9 System and Security

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

9.1 System Settings

9.1.1 View Device Information

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

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

9.1.2 Time and Date

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

Synchronize Time Manually

Steps

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

Set NTP Server

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

Before You Start
Set up a NTP server or obtain NTP server information.

Steps

1. Go to **Configuration → System → System Settings → Time Settings** .
2. Select **Time Zone**.

3. Click **NTP**.
4. Set **Server Address**, **NTP Port** and **Interval**.

Note

Server Address is NTP server IP address.

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

Synchronize Time by Satellite

Note

This function varies depending on different devices.

Steps

1. Enter **Configuration → System → System Settings → Time Settings** .
2. Select **Satellite Time Sync.**.
3. Set **Interval**.
4. Click **Save**.

Set DST

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

Steps

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

9.1.3 Set RS-232

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

Before You Start

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

Steps

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

9.1.4 Set RS-485

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

Before You Start

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

Steps

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

   Note

   You should keep the parameters of the device and the computer or terminal all the same.
3. Click **Save**.

9.1.5 Set Live View Connection

It controls the remote live view connection amount.

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

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

9.1.6 Location Settings

Location displays and uploads the current longitude and latitude of the device.

Auto Uploading

Check **Enable** and set **Location Upload Interval**.

The device will upload its location at the set interval. You can also click **Refresh** to upgrade the device location manually.

Manual Settings

Check **Enable** and set **Location Upload Interval**. Enter the longitude and latitude of the device and click **Save**.

The device will upload the set location at the set interval.

Note

This function may vary according to different device models.

9.1.7 External Device

For the device supporting external devices, including the supplement light, wiper on the housing, the LED light, and heater, you can control them via the Web browser when it is used with the housing. External devices vary with models.

Operate Wiper

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

Before You Start

- Make sure your device supports wiper.
- Wiper operation and settings vary according to device models.

Steps

1. Go to **Configuration → System → System Settings → External Device**.
2. Select a wiper mode.

   Cleaning Mode:

   - When **Cleaning Mode** is selected as **Auto**, the device determines whether to clean based on image abnormalities caused by the issues including dirty lenses, water droplets on the window viewport, etc.
   - In **Auto** mode, the maximum number of cleaning times is 4 times in 24 hours.
   - **Threshold**: Set the threshold value to judge the degree of dirtiness based on the complexity of the image texture to determine whether to clean or not.

   Note

   - For the device with water box, the cleaning mode is used to clean the sand and dust from the lens window by spraying water and wiping in dry and rainless areas.
   - As for cleaning, the water box automatically sprays water for 2 seconds before the wipers start working. The water spray from the water box lasts for 10 seconds and the wiper wipes 5 times.

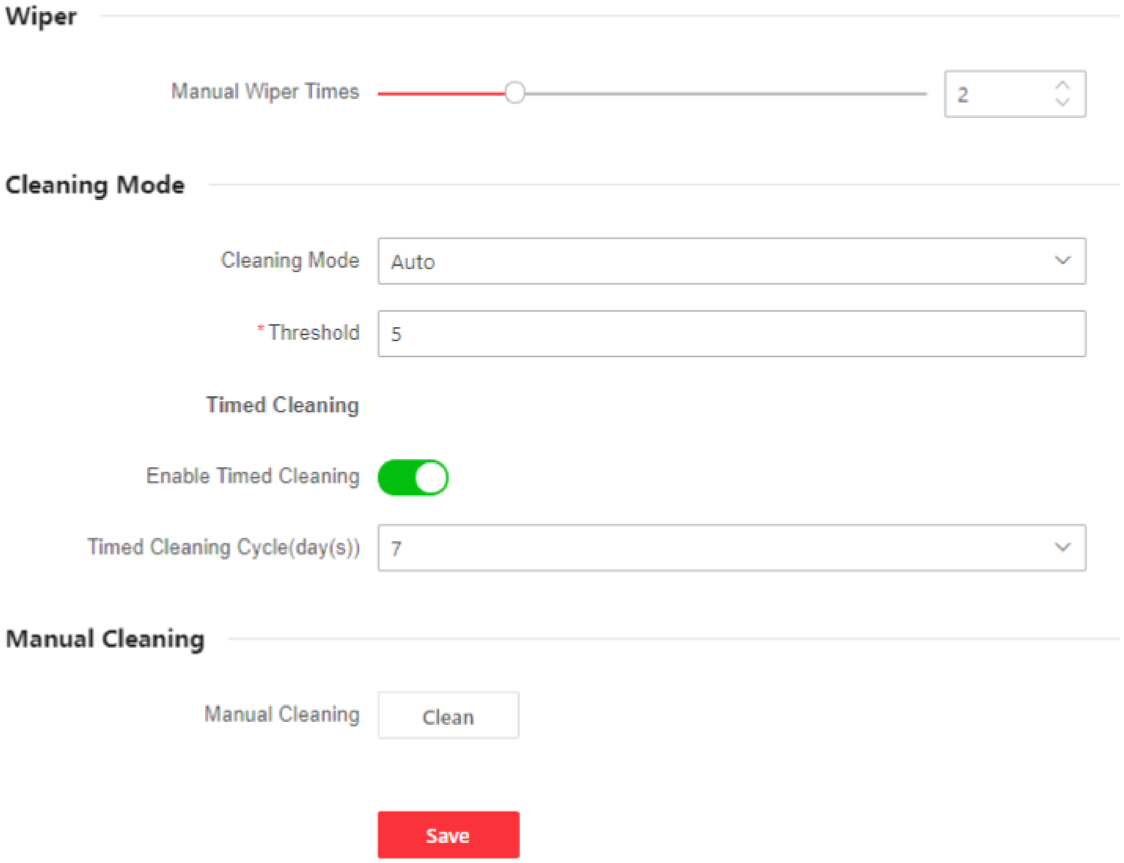
   Normal Mode: Only For Wiping
   You can set **Manual Wiper Times**, and the wiper wipes the set manual wiper times when you click ⌒ on live view page.

   Cleaning Mode: Timed Cleaning
   The wiper works on schedule and the water box (if supported) sprays water for cleaning at set wiping interval.

   Check **Enable Timed Cleaning** and set **Timed Cleaning Cycle (day(s))**. If the cycle is set to ***7*** days, the device will clean at 2:00 AM after 7 days, and then clean once every 7 days.

   Cleaning Mode:
   For the device with water box:

Manual Cleaning	• Click **Clean**, and the water box automatically sprays water for 2 seconds before the wipers start working. The water spray from the water box lasts for 10 seconds and the wiper wipes 5 times. • You can also click 💧 on live view page for manual cleaning or test. **For the device without water box:** • Click **Clean** to test the wiper function, and the wiper wipes.



Wiper

Manual Wiper Times: 2

Cleaning Mode

Cleaning Mode: Auto

*Threshold: 5

Timed Cleaning

Enable Timed Cleaning: ●

Timed Cleaning Cycle(day(s)): 7

Manual Cleaning

Manual Cleaning: Clean

Save

Figure 9-1 Operate Wiper

3. Click **Save**.

9.1.8 View Open Source Software License

On the top-right corner, click ⓘ and select **Open Source Software Description** to download the license. You can view the license in the editor.

9.1.9 Wiegand

Note

This function is only supported by certain camera models.

Check **Enable** and select the protocol. The default protocol is SHA-1 26bit.

If enabled, the recognized license plate number will be output via the selected Wiegand protocol.

9.2 User and Account

9.2.1 Set User Account and Permission

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

Caution

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

Steps

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

   Administrator

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

   User

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

   Operator

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

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

   Delete Select a user and click 🗑 .

Note

The administrator can add up to 31 user accounts.

3. Click **OK**.

9.2.2 Simultaneous Login

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

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

9.2.3 Online Users

The information of users logging into the device is shown.

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

9.3 Maintenance

9.3.1 Restart

You can restart the device via browser.

Go to **Maintenance and Security → Maintenance → Restart** , and click **Restart**.

9.3.2 Upgrade

Before You Start

You need to obtain the correct upgrade package.

Caution

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

Steps

1. Go to **Maintenance and Security → Maintenance → Upgrade** .
2. Choose one method to upgrade.

Firmware	Locate the exact path of the upgrade file.
Firmware Directory	Locate the directory which the upgrade file belongs to.

3. Click 🗀 to select the upgrade file.

4. Click **Upgrade**.

9.3.3 Restore and Default

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

Steps

1. Go to **Maintenance and Security → Maintenance → Backup and Restore** .
2. Click **Restore** or **Default** according to your needs.

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

   Default Reset all the parameters to the factory default.

   Note

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

9.3.4 Import and Export Configuration File

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

Steps

1. Export configuration file.
   1) Go to **Maintenance and Security → Maintenance → Backup and Restore → Backup** .
   2) Click **Export** and input the encryption password to export the current configuration file.
   3) Set the saving path to save the configuration file in local computer.
2. Import configuration file.
   1) Access the device that needs to be configured via web browser.
   2) Go to **Maintenance and Security → Maintenance → Backup and Restore → Reset** .
   3) Click 🗀 to select the saved configuration file.
   4) Input the encryption password you have set when exporting the configuration file.
   5) Click **Import**.

9.3.5 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

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

   The matched log files will be displayed on the log list.

4. **Optional:** Click **Export** to save the log files in your computer.

9.3.6 Search Security Audit Logs

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

Steps

Note

This function is only supported by certain camera models.

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

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

9.3.7 SSH

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

Go to **Maintenance and Security → Maintenance → Device Debugging** , and click **Settings** of **SSH**. You can edit the number of the port. Click **Save**.

Caution

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

9.3.8 Export Diagnose Information

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

Go to **Maintenance and Security → Maintenance → Device Debugging → Diagnose Information** . Click **Export**. In the pop-up window, check desired diagnose information and click **Export** to export corresponding diagnose information of the device.

9.4 Security

You can improve system security by setting security parameters.

9.4.1 Set IP Address Filter

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

IP address refers to IPv4.

Steps

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

   Blocklist IP addresses in the list cannot access the device.

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

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

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

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

9.4.2 Set MAC Address Filter

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

Steps

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

   Blocklist MAC addresses in the list cannot access the device.

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

   Add Add a new MAC address to the list.

   ✎ Modify the selected MAC address in the list.

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

9.4.3 Control Timeout Settings

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

Go to **Maintenance and Security → Security → Login Management → Control Timeout Settings** to complete settings.

9.4.4 Certificate Management

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

Note

The function is only supported by certain device models.

Server Certificate/Client Certificate

Note

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

Create and Install Self-signed Certificate

Steps

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

   Note

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

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

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

Install Self-signed Request Certificate

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

Before You Start

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

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Select a self-signed certificate from the **Server/Client Certificate** list.
3. Click **Create Certificate Request**.
4. Input request information.
5. Click **Save**.

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

   Note

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

   3) Click 🗀 to select the certificate file.
   4) Select **Self-signed Request Certificate**.
   5) Click **Save**.

   The imported certificate is displayed in the **Server/Client Certificate** list.

   If the certificate is used by certain function, the function name is shown in the column **Functions**.
9. **Optional:** Click **Property** see the certificate details.

Install Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Click **Import** in the **Server/Client Certificate** list.
3. Input **Certificate ID**.

Note

The input certificate ID cannot be the same as the existed ones.

4. Click 📁 to select the certificate file.
5. Select **Certificate and Key** and select a **Key Type** according to your certificate.

   Independent Key If your certificate has an independent key, select this option.

   Browse to select the private key and input the private-key password.

   PKCS#12 If your certificate has the key in the same certificate file, select this option and input the password.

6. Click **Save**.

   The imported certificate is displayed in the **Server/Client Certificate** list.

   If the certificate is used by certain function, the function name is shown in the column **Functions**.

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Click **Import** in the **CA Certificate** list.
3. Input **Certificate ID**.

Note

The input certificate ID cannot be the same as the existing ones.

4. Click 📁 to select the certificate file.
5. Click **Save**.

   The imported certificate is displayed in the **CA Certificate** list.

   If the certificate is used by certain functions, the function name is shown in the **Functions** column.

Enable Certificate Expiration Alarm

Steps

1. Check **Enable Certificate Expiration Alarm**. If enabled, you will receive an email or the camera links to the surveillance center that the certificate will expire soon, or is expired or abnormal.
2. Set the **Remind Me Before Expiration (day)**, **Alarm Frequency (day)** and **Detection Time (hour)**.

Note

- If you set the reminding day before expiration to 1, then the camera will remind you the day before the expiration day. 1 to 30 days are available. Seven days is the default reminding days.
- If you set the reminding day before expiration to 1, and the detection time to 10:00, and the certificate will expire in 9:00 the next day, the camera will remind you in 10:00 the first day.

3. Click **Save**.

9.4.5 TLS

The Transport Layer Security (TLS) protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. TLS settings are effective for HTTP(S) and enhanced SDK service.

Go to **Maintenance and Security → Security → TLS** , and enable the desired TLS protocol. Click **Save**.

Caution

Use the function with caution. The security risk of device internal information leakage exists when the function is enabled.

Chapter 10 Device Management

10.1 Add Alarm Box

You can add an alarm box to the device through the network protocol and view the alarm input/ output interface of the alarm box.

Steps

1. Click **Add Device** to add the alarm box as needed.
2. Set the parameters of the device, such as the IP address and the description of the alarm box.
3. Click **Save**.

Note

The function is only supported by certain device models.

Chapter 11 VCA Resource

VCA resource is a collection of smart functions supported by the device.

11.1 Allocate VCA Resource

VCA resource offers you options to enable certain VCA functions according to actual needs. It helps allocate more resources to the desired functions.

Steps

1. Click **VCA** on the left tab.
2. Enable the desired VCA function.
3. Click **Next** to finish settings.

Note

Certain VCA functions are mutually exclusive.

11.2 General Settings

Set the general parameters which are related to the smart applications.

Go to **VCA → Set Application → General Settings** to set the following parameters.

Camera Info.

For camera information settings, refer to ***Set Camera Info*** .

FTP

For FTP settings, refer to ***Set FTP*** .

Email

For Email settings, refer to ***Set Email*** .

Alarm Output

For alarm output settings, refer to ***Automatic Alarm*** .

Audible Alarm Output

For audible alarm output settings, refer to ***Set Audible Alarm Output*** .

Alarm Server

For alarm server settings, refer to ***Alarm Server*** .

Metadata

For metadata settings, refer to ***Metadata*** .

11.2.1 Set Camera Info

Customize specific information for the device. It may help identify a certain device when multiple devices are under management.

Go to **VCA → Set Application → General Settings → Camera Info** to set **Device No.** and **Camera Info**.

11.2.2 Metadata

Metadata is the raw data that the device collects before algorithm processing. It is often used for the third party integration.

Go to **VCA → Set Application → General Settings → metadata Settings** to enable metadata uploading of the desired function.

Note

This function varies according to different camera models.

Smart Event

The metadata of the smart event includes the target ID, target coordinate, time, etc.

You can check **Enable Stream Rule** to overlay the stream rule on the live view image. Make sure you have checked **Sub-Stream** and selected the sub-stream in the live view.

You can check **Overlay Rule Frame and Target Frame on Background Picture** to overlay the rule and target information on the sub-stream. Make sure you have checked **Sub-Stream** and selected the sub-stream in the live view.

Face Capture

The metadata of face capture includes the rule information, target ID, target coordinate, time information, etc. The camera detects the whole image by default. If the area is configured in the face capture settings, the camera detects the configured area.

Multi-Target-Type Detection

The metadata of multi-target-type detection includes the vehicle information and face capture information, such as the target ID, target coordinate, time information, vehicle moving direction, etc.

Road Traffic

The metadata of road traffic is detected vehicle information, including the vehicle location in the scene, vehicle ID, license plate, validity, moving direction, country/region, etc.

11.2.3 Dynamic Mosaic Mask

The function masks the detection target picture in the detection area. It is effective for preview, playback and recording.

Go to **VCA → Set Application → General Settings → Dynamic Mosaic Mask** to set the following parameters.

Note

- The function is supported only when certain VCA function is enabled.
- The function varies according to different models.

Face Mosaic Mask

When **Face Mosaic Mask** is enabled, the face image in the detection area will be mosaicked.

Human Body Mosaic Mask

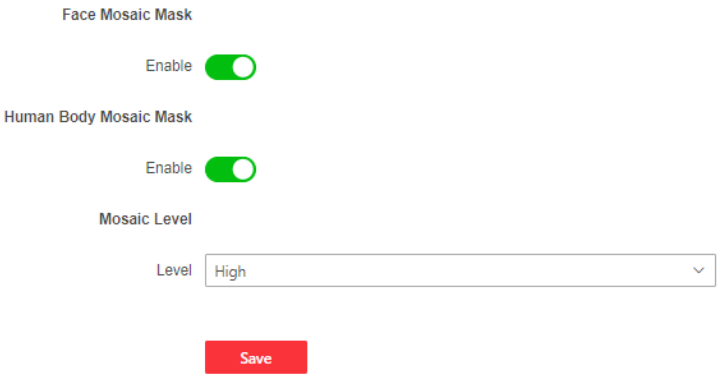
When **Human Body Mosaic Mask** is enabled, the whole body image in the detection area will be mosaicked.

License Plate Mosaic Mask

When **License Plate Mosaic Mask** is enabled, the license plate image in the detection area will be mosaicked.

Mosaic Level

The higher the level, the less clear the target is.



Face Mosaic Mask

Enable ●

Human Body Mosaic Mask

Enable ●

Mosaic Level

Level: High

Figure 11-1 Set Dynamic Mosaic Mask

11.2.4 AcuSearch

The device transmits the POS information of the target to network video recorder after detecting the target. It is to achieve accurate and quick search on the connected network video recorder.

Before You Start

- Make sure the connected network video recorder (NVR) supporting AcuSearch to do with the function.
- After the function is enabled, the ongoing smart application will be disabled while **Smart Event** or **Multi-Target-Type Detection** will be enabled.
- The function is only supported by certain models. The actual display varies with the models.

Steps

1. Enable the function for the device.
2. Set the function on the connected network video recorder.
   1) Enable AcuSearch function for the selected channel (refer to the configured camera device) on the network video recorder.
   2) Click the AcuSearch button on the playback page of the network video recorder.
   3) Click a target on a network video recorder to search for pictures that contain the target.
   4) Click a picture to play a video before and after that moment.

   Note

   Refer to the *User Manual* of NVR for the actual settings on NVR.

11.3 Smart Event

Note

- For certain device models, you need to enable the smart event function on **VCA** page first to show the function configuration page.
- The function varies according to different models.

11.3.1 Set Intrusion Detection

It is used to detect objects entering and loitering in a predefined virtual region. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Intrusion Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click ⬠, click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.

2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click and , then drag the mouse in the live view to draw the minimum and maximum target size.
3) **Optional:** Click to delete all the setting areas.

4. Set parameters.

Detection Target

This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.

Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

Threshold

Threshold stands for the threshold for the time of the object loitering in the region. If the time that one object stays exceeds the threshold, the alarm is triggered. The larger the value of the threshold is, the longer the alarm triggering time is.

Sensitivity

Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missed.

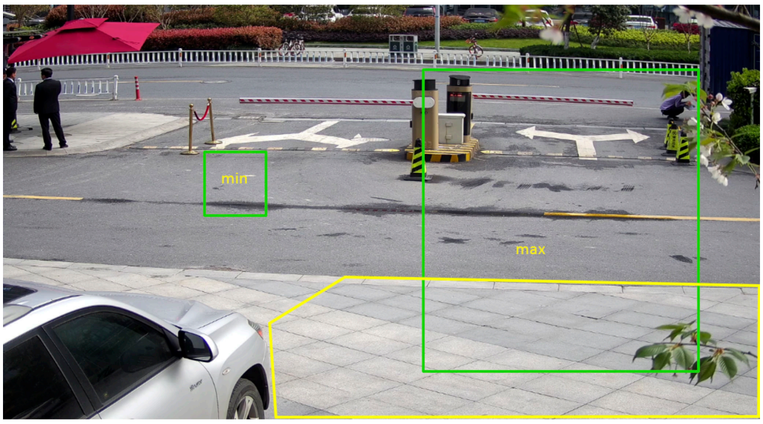


Figure 11-2 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.

6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. **Optional:** Set **Custom Alarm**.

   This function is used to send the custom alarm messages to alarm servers. Click and set the **Custom Alarm Content** to customize alarm messages in HTTP text format, up to 512 characters in length. Alarm messages can be sent to up to 3 servers.

   Note

   The function is only supported by certain camera models.
8. Click **Save**.

11.3.2 Set Line Crossing Detection

It is used to detect objects crossing a predefined virtual line. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Line Crossing Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection line. Click and a line with an arrow appears in the live view. Drag the line to the location on the live view as desired.
   2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click and , then drag the mouse in the live view to draw the minimum and maximum target size.
   3) **Optional:** Click to delete all the setting areas.
4. Set parameters.

   Detection Target

   This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.

   Note

   This function is only available for certain device models under certain settings. Please refer to the actual settings.

   Direction

   It stands for the direction from which the object goes across the line.

A<->B: The object going across the line from both directions can be detected and alarms are triggered.

A->B: Only the object crossing the configured line from the A side to the B side can be detected.

B->A: Only the object crossing the configured line from the B side to the A side can be detected.

Sensitivity

It stands for the percentage of the body part of an acceptable target that goes across the pre-defined line. 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. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

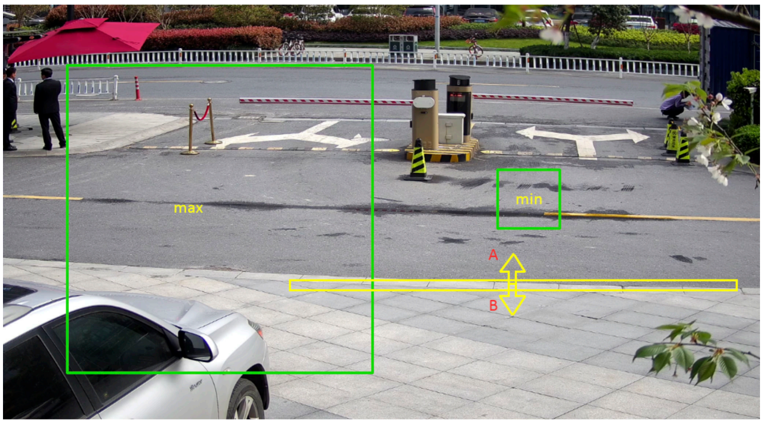


Figure 11-3 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. **Optional:** Set **Custom Alarm**.

   This function is used to send the custom alarm messages to alarm servers. Click and set the **Custom Alarm Content** to customize alarm messages in HTTP text format, up to 512 characters in length. Alarm messages can be sent to up to 3 servers.

   Note

   The function is only supported by certain camera models.
8. Click **Save**.

11.3.3 Set Region Entrance Detection

It is used to detect objects entering a predefined virtual region from the outside place. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Region Entrance Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
   2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click and , then drag the mouse in the live view to draw the minimum and maximum target size.
   3) **Optional:** Click to delete all the setting areas.
4. Set parameters.

Detection Target

This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.

Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

Sensitivity

It stands for the percentage of the body part of an acceptable target that goes across the predefined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

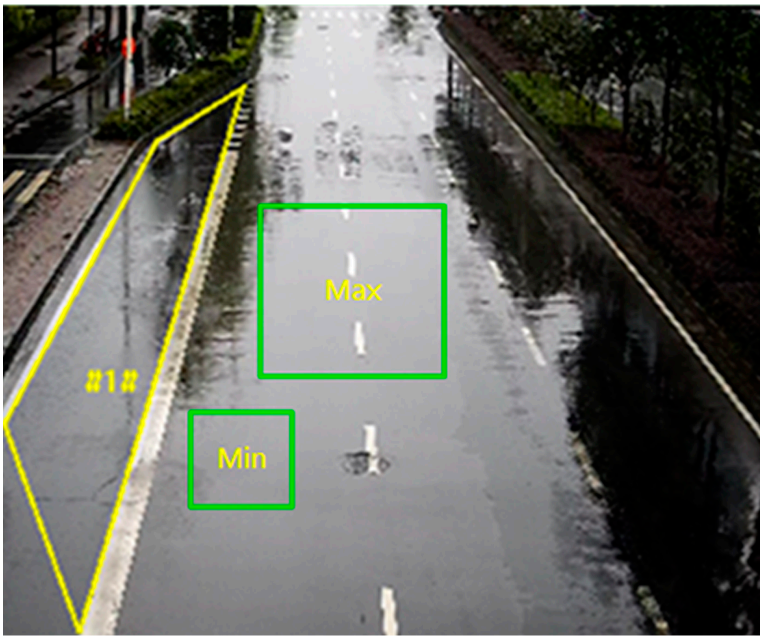


Figure 11-4 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. **Optional:** Set **Custom Alarm**.

   This function is used to send the custom alarm messages to alarm servers. Click and set the **Custom Alarm Content** to customize alarm messages in HTTP text format, up to 512 characters in length. Alarm messages can be sent to up to 3 servers.

   Note

   The function is only supported by certain camera models.
8. Click **Save**.

11.3.4 Set Region Exiting Detection

It is used to detect objects exiting from a predefined virtual region. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Region Exiting Detection** .
2. Check **Enable**.

3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click ⬭ , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
   2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click ⬚ and ☐ , then drag the mouse in the live view to draw the minimum and maximum target size.
   3) **Optional:** Click 🗑 to delete all the setting areas.
4. Set parameters.

Detection Target

This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.

Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

Sensitivity

It stands for the percentage of the body part of an acceptable target that goes across the predefined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

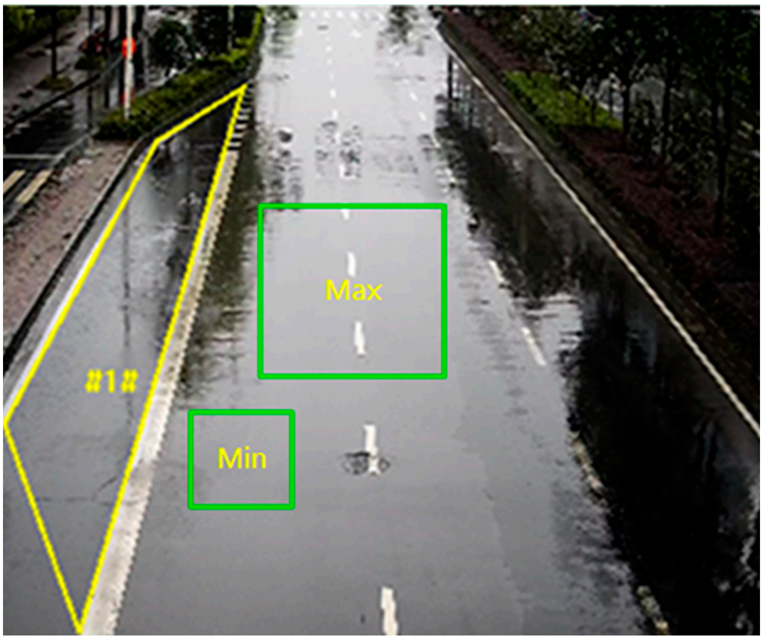


Figure 11-5 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. **Optional:** Set **Custom Alarm**.

   This function is used to send the custom alarm messages to alarm servers. Click and set the **Custom Alarm Content** to customize alarm messages in HTTP text format, up to 512 characters in length. Alarm messages can be sent to up to 3 servers.

   Note

   The function is only supported by certain camera models.
8. Click **Save**.

11.3.5 Set Unattended Baggage Detection

It is used to detect the objects left over in the predefined region. Linkage methods can be triggered after the object is left and stays in the region for a set time period.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Unattended Baggage Detection** .
2. Check **Enable**.

3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
   2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click and , then drag the mouse in the live view to draw the minimum and maximum target size.
   3) **Optional:** Click to delete all the setting areas.
4. Set parameters.

   Sensitivity

   Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

   Threshold

   It stands for the time of the objects left in the region. Alarm is triggered after the object is left and stays in the region for the set time period.

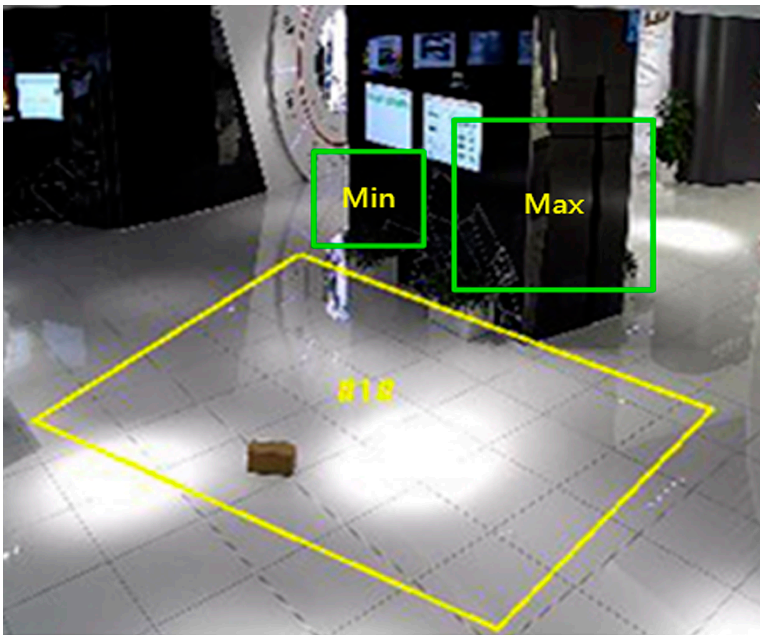


Figure 11-6 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with the models.

11.3.6 Set Object Removal Detection

It detects whether the objects are removed from the predefined detection region, such as the exhibits on display. If it occurs, the device can take linkage actions and the staff can take measures to reduce property loss.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Object Removal Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
   2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click and , then drag the mouse in the live view to draw the minimum and maximum target size.
   3) **Optional:** Click to delete all the setting areas.
4. Set parameters.

   Sensitivity

   Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

   Threshold

   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.

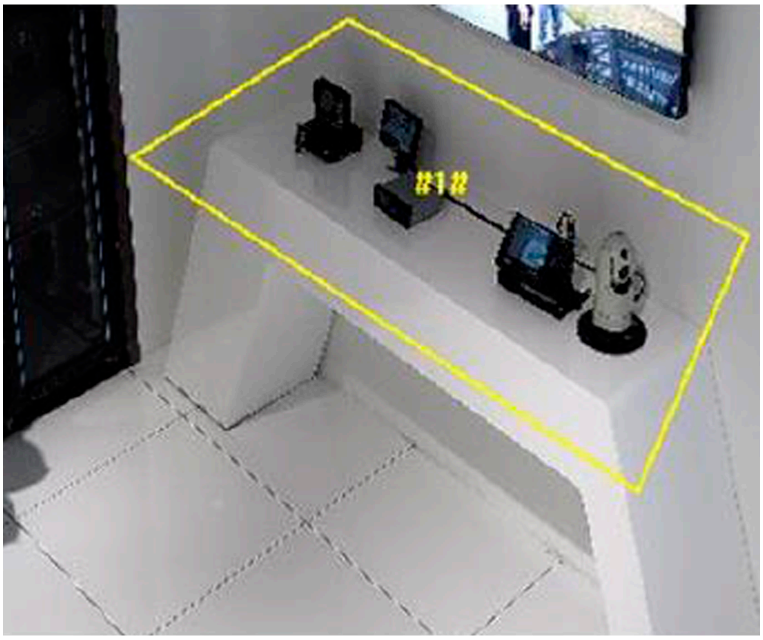


Figure 11-7 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, see ***Set Arming Schedule*** . For the linkage method settings, see ***Linkage Method Settings*** .
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with the models.

11.3.7 Set Loitering Detection

It detects whether there is any target loitering in a predefined area. If the time that the target loiters in the set region reaches the set threshold, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Loitering Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click ⬠, click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.

2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click and , then drag the mouse in the live view to draw the minimum and maximum target size.
3) **Optional:** Click to delete all the setting areas.

4. Set rules.

Threshold

Threshold stands for the threshold for the time of the object loitering in the region. If the time that one object stays exceeds the threshold, the alarm is triggered. The larger the value of the threshold is, the longer the alarm triggering time is.

Sensitivity

Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

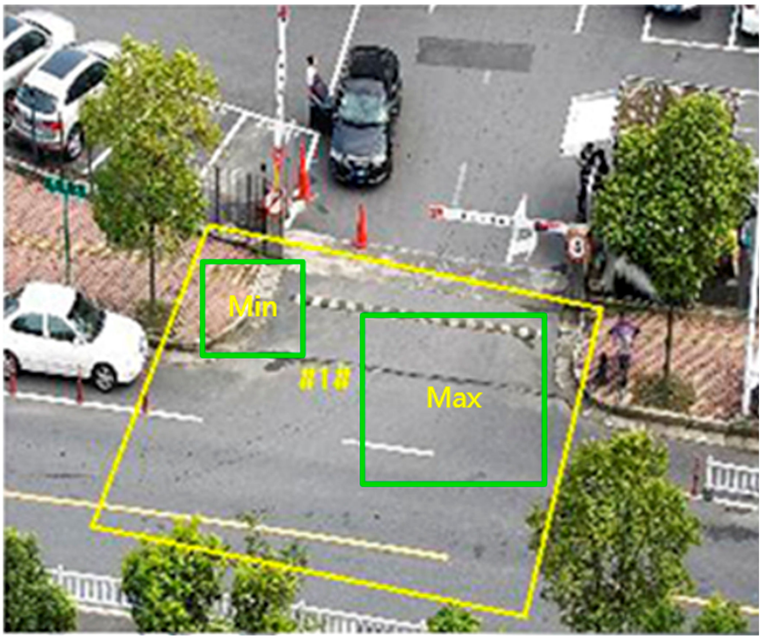


Figure 11-8 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with the models.

11.3.8 Set People Gathering Detection

It detects the people density in a predefined area. If the people density exceeds the set percentage, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → People Gathering Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click ⬠, click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
   2) **Optional:** Click 🗑 to delete all the setting areas.
4. Set rules.

   Percentage

   It stands for the percentage of people in the predefined area. When the people percentage in the live view exceeds the set value, the device will trigger an alarm.

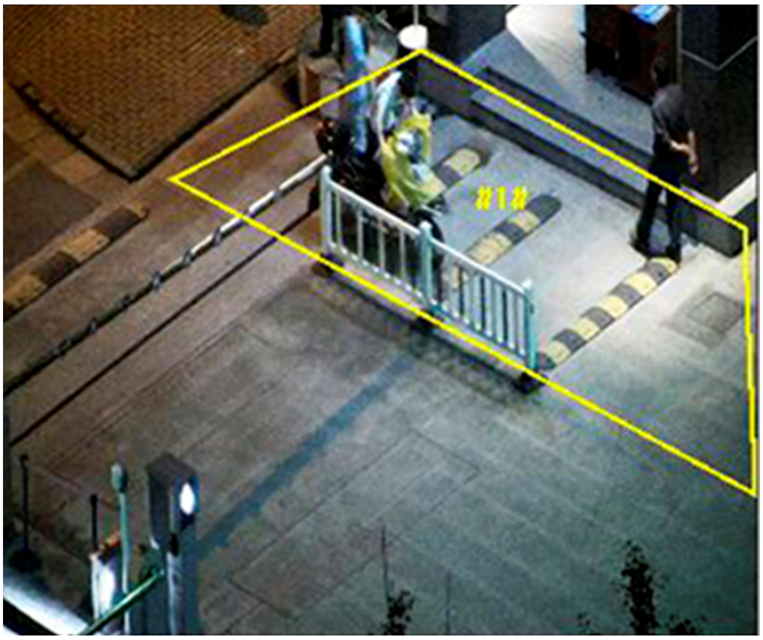


Figure 11-9 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings***
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with the models.

11.3.9 Set Fast Moving Detection

When there are targets moving at a high speed in a predefined area, the device will take linkage actions and trigger an alarm.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Fast Moving Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click ▭ , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
   2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click ⬚ and ▢ , then drag the mouse in the live view to draw the minimum and maximum target size.
   3) **Optional:** Click 🗑 to delete all the setting areas.
4. Set Rules.

   Sensitivity

   Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region. 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. The higher the value of sensitivity is, the more easily the alarm can be triggered.

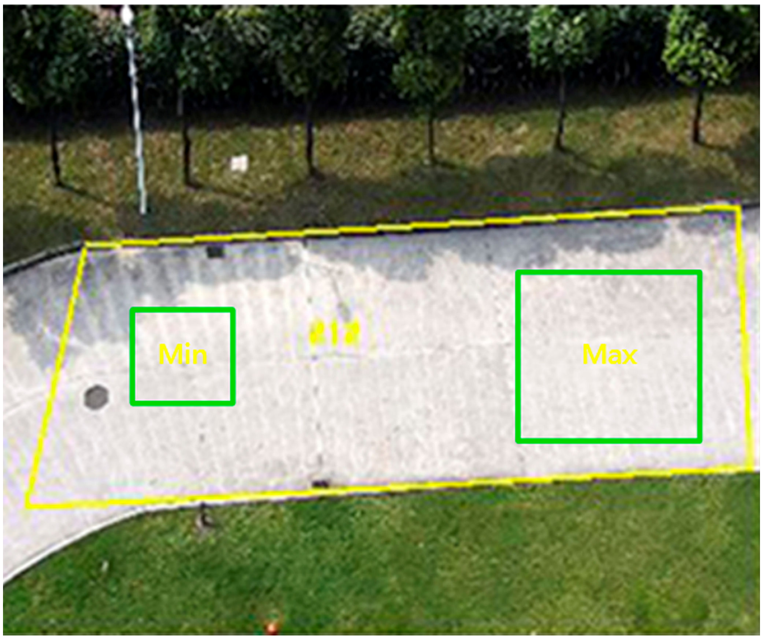


Figure 11-10 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with the models.

11.3.10 Set Parking Detection

It detects parking violation in a predefined area. When the parking time exceeds a set threshold, the device can take linkage actions. It is applicable in expressway and one-way street.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Parking Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.

2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click ⬚ and ⬚ , then drag the mouse in the live view to draw the minimum and maximum target size.
3) **Optional:** Click 🗑 to delete all the setting areas.

4. Set rules.

   Threshold

   Threshold stands for the threshold for the parking time in the region. If the parking time exceeds the threshold, an alarm is triggered. The larger the value of the threshold is, the longer the alarm triggering time is.

   Sensitivity

   Sensitivity stands for the percentage of the part of an acceptable target that enters the pre-defined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target part that goes across the pre-defined region. ST stands for the complete target. The higher the value of sensitivity is, the more easily the alarm can be triggered.

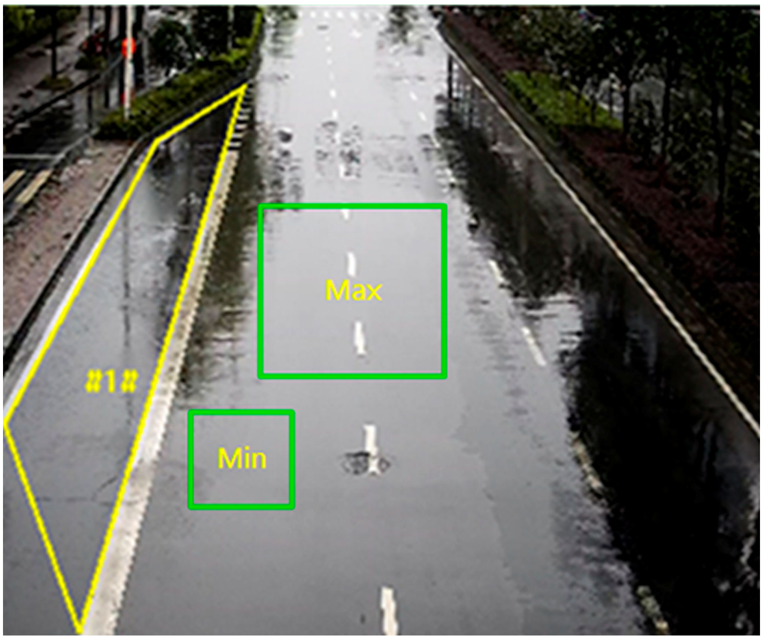


Figure 11-11 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings***
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with the models.

11.3.11 Set Combined Event

This function is used to combine the perimeter protection events, including Intrusion Detection, Line Crossing Detection, Region Entrance Detection and Region Exiting Detection, and trigger the alarm after all the sub event alarm rules are triggered in sequence.

Before You Start

Enable at least one of the smart events first before enabling the combined event. Individual event alarms cannot be triggered when the combined event is enabled.

Note

The function is only supported by certain camera models.

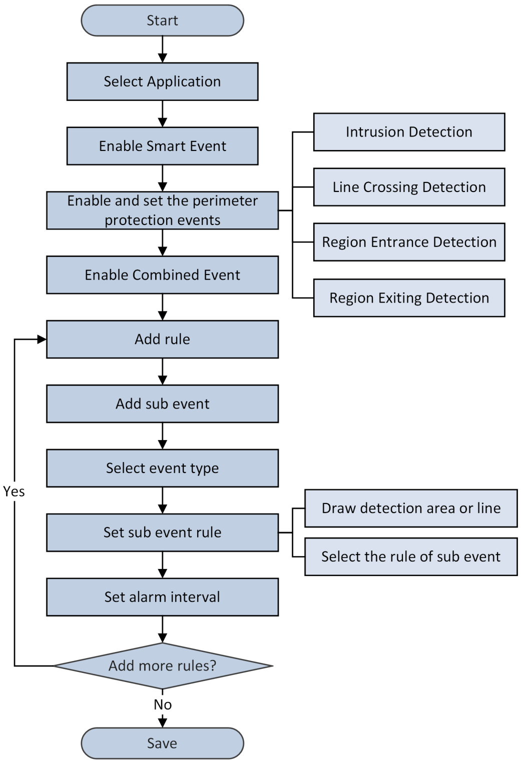
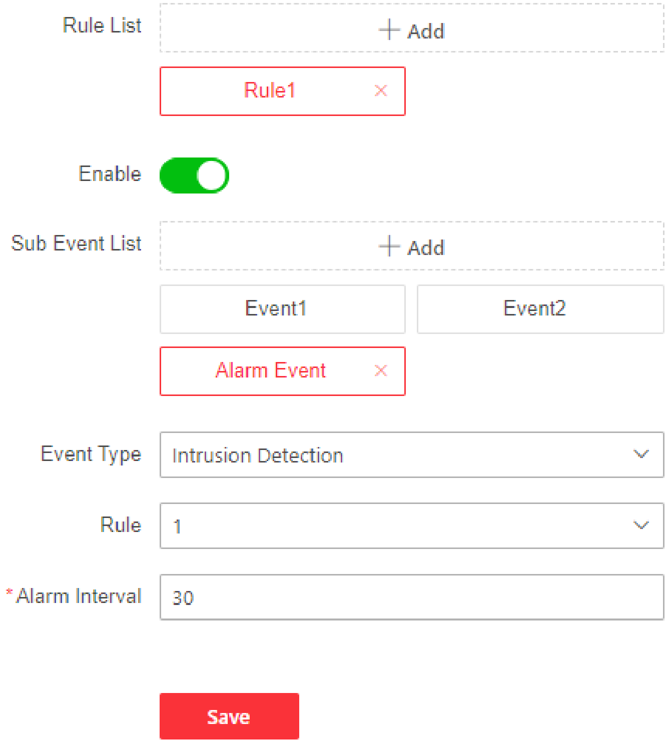


Figure 11-12 Set Combined Event

Steps

1. Go to **VCA → Set Application → Smart Event → Combined Event** .
2. Check **Enable**.



Rule List: + Add

Rule1 ×

Enable: ●

Sub Event List: + Add

Event1 | Event2

Alarm Event ×

Event Type: Intrusion Detection

Rule: 1

* Alarm Interval: 30

Figure 11-13 Set Rules

3. Click **Add** behind **Rule List** to add a new rule of the combined event.
   1) Click **Add** behind **Sub Event List** to add a sub event for the sub event list.
   2) Select the event type.

      Enable any of the perimeter protection events (including **Intrusion Detection**, **Line Crossing Detection**, **Region Entrance Detection** and **Region Exiting Detection**) first so that the event can be selected in the sub event list.

      Example

      - If **Intrusion Detection** and **Line Crossing Detection** are enabled and others are not, then **Intrusion Detection** and **Line Crossing Detection** can be selected.
      - If **Intrusion Detection** and **Object Removal Detection** are enabled and others are not, then only **Intrusion Detection** can be selected.
   3) Select the rule of the sub event according to the selected event type. You can draw the detection area or line.

      Note

      The detection rule of the current sub event is shared by all combined events. Please edit it carefully.
   4) Set the **Alarm Interval**. It refers to the maximum interval between alarms triggered by different sub events in the same combined event.
   5) Click **Save**.

4. Repeat the above steps to set other rules. Up to 4 rules can be set. The detection area should be a convex polygon area.
5. The arming schedule and linkage method of the combined event refers to the arming schedule and linkage method of the alarm event.
6. Click **Save**.

11.4 Face Capture

The device can capture the face that meets the rules in the configured rule area, and the captured picture will be uploaded.

Note

- For certain device models, you need to enable this function on **VCA** page first.
- The function is only supported by certain device models.

11.4.1 Set Face Capture

The face that appears in the configured area can be captured.

Before You Start

- Go to **VCA** and select the application. Select **Face Capture** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Face Capture**.

Steps

1. Go to **VCA → Set Application → Face Capture → Rule** .
2. Check **Enable** to enable the rule settings.
3. Click ⬠ to draw the detection area you want the face capture to take effect. Draw area by left-clicking end-points in the live view window, and right-clicking to finish the area drawing. It is recommended that the drawn area occupies 1/2 to 2/3 of the live view image.
4. Draw pupil distance.

   Min. Pupil Distance

   Click ☺ to draw the minimum pupil distance. If the pupil distance of the face in the video image is smaller than the minimum pupil distance, the face will not be detected.

   Max. Pupil Distance

   Click ☺ to draw the maximum pupil distance. If the pupil distance of the face in the video image is larger than the maximum pupil distance, the face will not be detected.

   You can also input the value of distance in the text field.
5. **Optional:** For shield region settings, refer to ***Set Shield Region*** .
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. Click **Save**.

8. For overlay and capture settings, refer to ***Overlay and Capture*** . For advanced parameters settings, refer to ***Face Capture Algorithms Parameters*** .

Result

You can view and download captured pictures in **Playback → Picture** . Refer to ***View and Download Picture*** for details.

11.4.2 Overlay and Capture

Choose to configure capture parameters and the information you want to display on stream and picture.

Note

The function varies according to different device models.

Overlay

Display VCA Info. on Stream

Display smart information on stream, including the target and rules information.

Display Target Info. on Alarm Picture

Overlay the alarm picture with target information.

Background Picture Settings

Background Picture Settings

Comparing to target picture, background picture is the scene image which offers extra environmental information. You can set the background picture quality and resolution.

Background Upload

If the background image need to be uploaded to surveillance center, check **Background Upload**.

Face Picture

For some devices, you can also check **Face Picture** as needed. The device will upload the captured face picture.

Compress Background Picture

The device uploads a compressed captured background picture. The higher the compression level, the smaller the picture file size.

Target Picture Settings

Target Picture Settings

Custom, Head Shot, Half-Body Shot and Full-Body Shot are selectable.

Note

If you select **Custom**, you can customize **Width**, **Head Height** and **Body Height** as required.

You can check **Fixed Value** to set the picture height.

Face Beautification

Check **Face Beautification** and adjust the beautification level as needed.

Note

Face Beautification slightly adjusts the captured face pictures and reduces noise of captured face picture.

Face Enhancement

Check **Face Enhancement** and the device is able to capture better and clearer face pictures when it is dark.

Text Overlay

Text Overlay

You can check desired items and adjust their order to display on captured pictures.

See ***Set Camera Info*** to set **Device No.** and **Camera Info**.

11.4.3 Face Capture Algorithms Parameters

It is used to set and optimize the parameters of the algorithm library for face capture function.

Version

It stands for the current algorithm version.

Capture Parameters

Best Shot

The best shot after target leaves the detection area.

Capture Threshold

It stands for the quality of face to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.

Capture Times

It refers to the capture times a face will be captured during its stay in the configured area. The default value is 1.

Quick Shot

When the face picture grading value is higher than the quick shot threshold, the face picture will be captured and uploaded. Otherwise, the picture with the highest grading value that reaches the max. capture interval will be selected for upload.

Quick Shot Threshold

It stands for the quality of face to trigger quick shot.

Max. Capture Interval

It refers to the max. time occupation for one quick shot.

Capture Times

It refers to the capture times a face will be captured during its stay in the configured area.

Remove Duplicated Faces

This function can help filter out repeated captures of certain face.

Similarity Threshold for Duplicates Removing

It is the similarity between the newly captured face and the picture in the duplicates removing library. When the similarity value is higher than the value you set, the captured picture is regarded as a duplicated face and will be dropped.

Duplicates Removing Library Grading Threshold

It is the face grading threshold that triggers duplicates checking. When the face grading is higher than the set value, the captured face is compared with the face pictures that are already in the duplicates removing library.

Duplicates Removing Library Update Time

The time from when each face picture is added to the duplicates removing library until when it is deleted.

Face Exposure

Check the checkbox to enable the face exposure.

Reference Brightness

The reference brightness of a face in the 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 is.

Min. Duration

The minimum duration of the camera exposures the face.

Note

If the face exposure is enabled, please make sure the WDR function is disabled, and the manual iris is selected.

Face Filtering Time

It means the time interval between the camera detecting a face and taking a capture. If the detected face stays in the scene for a time shorter than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.

Note

The face filtering time (longer than 0 s) may increase the possibility of the actual capture times less than the set value above.

Facial Posture Filter

Facial posture filter can filter out face of certain postures. The figure on the right of the slider stands for the posture angle which is acceptable in the face capture action. Click ⓘ to display the diagram illustrating the face turning direction when setting up this filter.

Upload Feature

Feature stands for the feature information the algorithm can tell from face pictures. Check the function to upload the information.

Restore Parameters

Restore Defaults

Click **Restore** to restore all the settings in advanced configuration to the factory default.

11.4.4 Set Shield Region

The shield region allows you to set the specific region in which the set smart function rule is invalid.

Steps

1. Select **Shield Region**.
2. Click ▭ to draw shield region. Repeat this step above to set more shield regions.
3. **Optional:** Select and click on the drawn region, then click ✕ to delete the selected drawn region.
4. **Optional:** Click 🗑 to delete all drawn regions.
5. Click **Save**.

11.5 Multi-Target-Type Detection

Multi-Target-Type Detection is to detect, capture and upload data of targets in multiple types, such as human face, human body, and vehicle.

Note

- For certain device models, you need to enable **Multi-Target-Type Detection** on **VCA** page first.
- The function is only supported by certain device models.

11.5.1 Set Multi-Target-Type Detection Rule

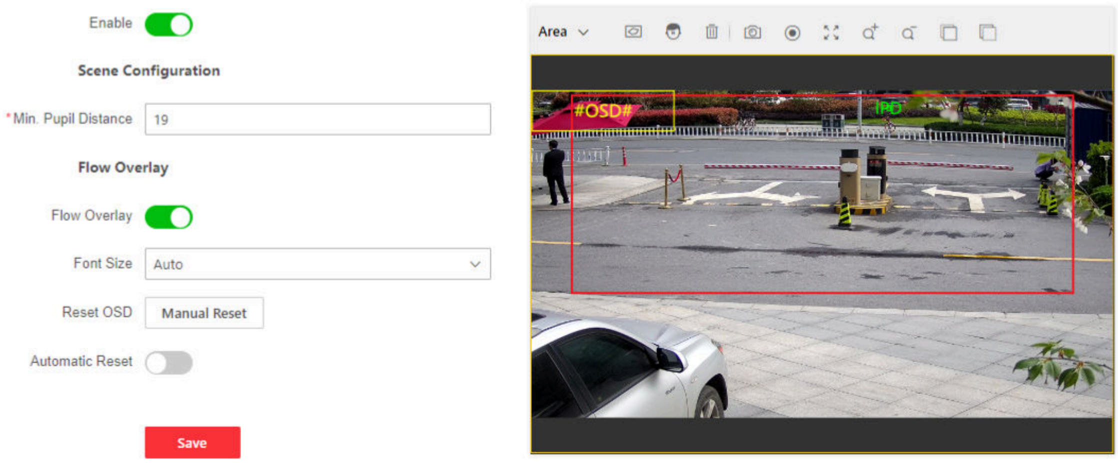
After setting the multi-target-type detection rules and algorithm parameters, the device captures targets of multiple types and triggers linkage actions automatically.

Before You Start

Go to **VCA** and select the application. Select **Multi-Target-Type Detection** and click **Next** to enable the function.

Steps

1. Go to **VCA → Set Application → Multi-Target-Type Detection → Rule** .
2. Check **Enable**.



Enable ●

Scene Configuration

*Min. Pupil Distance: 19

Flow Overlay

Flow Overlay ●

Font Size: Auto

Reset OSD: Manual Reset

Automatic Reset ○

Save

Figure 11-14 Set Rules

3. Click to draw a detection area. Click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
4. Enter the min. pupil distance in the text field, or click to draw min. pupil distance.

   Min. Pupil Distance

   The min. pupil distance refers to the minimum area between two pupils, and it is basic for the device to recognize a face.
5. Check to enable the **Flow Overlay**, and set the parameters.
6. Click **Save**.
7. **Optional:** For shield region settings, refer to ***Set Shield Region*** .
8. Set arming schedule. See ***Set Arming Schedule*** .
9. Set linkage method. See ***Linkage Method Settings*** .

10. **Optional:** For overlay and capture settings, refer to ***Overlay and Capture*** . For advanced parameters settings, refer to ***Multi-Target-Type Detection Advanced Parameters*** .

What to do next

Go to **Playback → Picture** to search and view the captured pictures. Refer to ***View and Download Picture*** for details.
Go to **Application Display → Display Alarm** to see currently captured target pictures. Refer to ***Smart Display*** for details.

11.5.2 Set Multi-Target-Type Counting Rule

This function is used to count the number of line crossing targets by type and detect the line crossing direction.

Before You Start

Go to **VCA** and select the application. Select **Multi-Target-Type Detection** and click **Next** to enable the function.

Steps

1. Check **Enable** to enable the function.

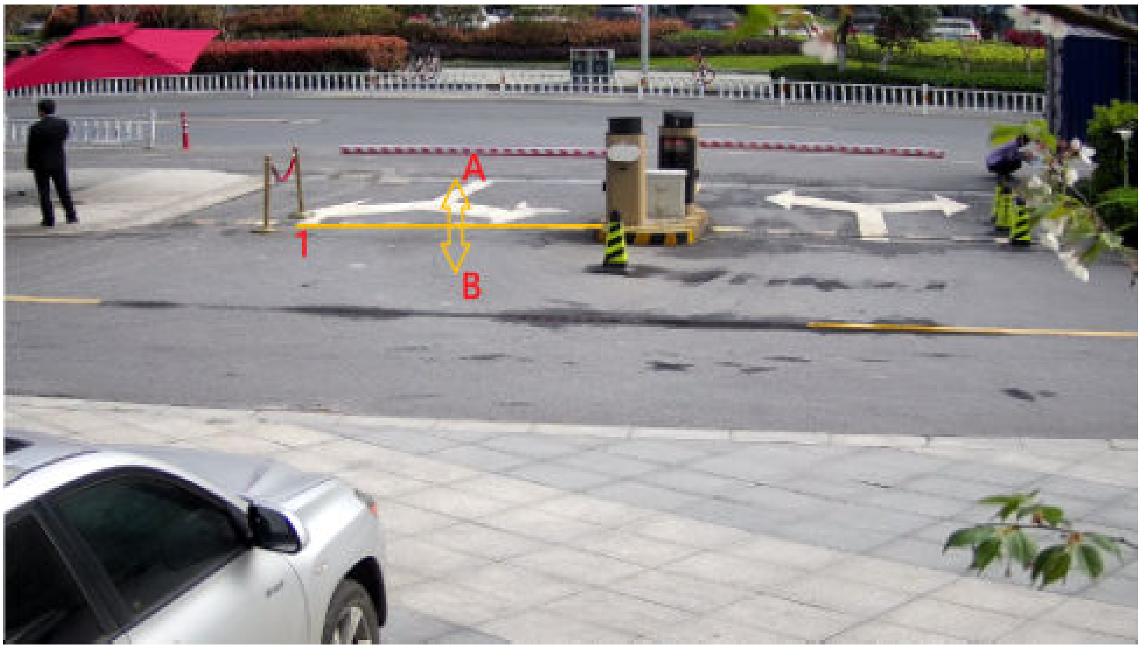


Figure 11-15 Set Multi-Target-Type Counting Rule

2. Check the desired counting target.
3. Draw and adjust the detection line.
   - Click ⟋ to draw the detection line. Drag the line to the location on the live view as desired.
   - Click 🗑 to delete the drawn lines.
4. **Optional:** Set the flow overlay parameters.

1) Check **Enable** to enable the flow overlay function.
2) Select the counting direction.
3) Set the **OSD Custom Content** for the counting direction name to be overlaid on the live view video.
4) Set a daily reset time for **Reset OSD**, or you can also click **Manual Reset** to reset manually.

5. **Optional:** Set the data uploading parameters.

   Real-Time Data Uploading

   If checked, the device uploads the counting data in real-time.

   Scheduled Uploading

   If checked, the device uploads the counting data according to the statistical period. In this case, **Interval** needs to be set.

6. **Optional:** Set email report parameters.

   If you want to send the report by email, select the data type and report format as required. When the device has statistics on multi-target-type counting and the mailbox is set correctly, the corresponding type of report information can be sent by email.

7. Click **Save**.

Note

The function is only supported by certain device models.

What to do next

You can view and export the counting data in **Application Display**. Refer to ***View Multi-Target-Type Counting Statistics*** for details.

11.5.3 Overlay and Capture

Choose to configure capture parameters and the information you want to display on stream and picture.

Note

The function varies according to different device models.

Overlay

Display VCA Info. on Stream

Display smart information on stream, including the target and rules information.

Display Target Info. on Alarm Picture

Overlay the alarm picture with target information.

Display Target Pattern Info. on Alarm Picture

Overlay the target moving pattern on the alarm picture.

Display Motor Vehicle Tracking Pattern on Alarm Picture

Overlay the motor vehicle target moving pattern on the alarm picture.

Target Picture Settings

Target Picture Settings

Custom, Head Shot, Half-Body Shot and Full-Body Shot are selectable.

Note

If you select **Custom**, you can customize **Width**, **Head Height** and **Body Height** as required.

You can check **Fixed Value** to set the picture height.

Face Beautification

Check **Face Beautification** and adjust the beautification level as needed.

Note

Face Beautification slightly adjusts the captured face pictures and reduces noise of captured face picture.

Face Enhancement

Check **Face Enhancement** and the device is able to capture better and clearer face pictures when it is dark.

License Plate Enhancement

Check it and the device is able to capture better and clearer license plate pictures.

Close-up Face Picture Settings

Close-up Face Picture Settings

Aspect Ratio

Width × Height

Central Point Offset

The height of the center point of the face picture. The higher the value, the closer the point is to the top of the head.

Expansion Ratio

The larger the expansion ratio, the smaller the close-up face in the picture.

Background Picture Settings

Background Picture Settings

Comparing to target picture, background picture is the scene image which offers extra environmental information. You can set the background picture quality and resolution.

Background Upload

If the background image need to be uploaded to surveillance center, check **Background Upload**.

Share Background for Face and Body

For some devices, you can check **Share Background for Face and Body**. After the function is enabled, a background picture with human face and full-body image will be uploaded.

Face Picture

For some devices, you can also check **Face Picture** as needed. The device will upload the captured face picture.

Compress Background Picture

The device uploads a compressed captured background picture. The higher the compression level, the smaller the picture file size.

Text Overlay

Text Overlay

You can check desired items and adjust their order to display on captured pictures.

See ***Set Camera Info*** to set **Device No.** and **Camera Info**.

11.5.4 Multi-Target-Type Detection Advanced Parameters

It is used to set and optimize the parameters of the algorithm library for Multi-Target-Type Detection.

Note

The function varies according to different device models.

HMS Version

It refers to the current algorithm version, which cannot be edited.

Overlay Intelligent Information

Overlay the related intelligent information or POS information in the video.

Capture Parameters

Best Shot

Capture Threshold

It refers for the quality of face to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.

Quick Shot

When the face picture grading value is higher than the quick shot threshold, the face picture will be captured and uploaded. Otherwise, the picture with the highest grading value that reaches the max. capture interval will be selected for upload.

Quick Shot Threshold

It stands for the quality of face to trigger quick shot.

Max. Capture Interval

It refers to the max. time occupation for one quick shot.

Remove Duplicated Faces

This function can help filter out repeated captures of certain face.

Similarity Threshold for Duplicates Removing

It is the similarity between the newly captured face and the picture in the duplicates removing library. When the similarity value is higher than the value you set, the captured picture is regarded as a duplicated face and will be dropped.

Duplicates Removing Library Grading Threshold

It is the face grading threshold that triggers duplicates checking. When the face grading is higher than the set value, the captured face is compared with the face pictures that are already in the duplicates removing library.

Duplicates Removing Library Update Time

The time from when each face picture is added to the duplicates removing library until when it is deleted.

Face Exposure

Check the checkbox to enable the face exposure.

Reference Brightness

It refers to the reference brightness of a face in the face exposure mode. If a face in the actual scene is brighter than the set reference brightness, the device lowers the exposure level. If a face in the actual scene is darker than the set reference, the device increases the exposure level.

Minimum Duration

The extra time the device keeps the face exposure level after the face disappears in the scene.

Face Filtering Time

It means the time interval between the camera detecting a face and taking a capture. If the detected face stays in the scene for a time shorter than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.

Note

The face filtering time (longer than 0 s) may increase the possibility of the actual capture times less than the set value above.

Simultaneous Frame Capture of Face and Human Body

The device will capture both face and human body pictures from the same frame when the alarm is triggered, ensuring that the captured face and body pictures are associated with the same target.

Note

The function is only supported by certain device models.

Data Upload

Data Upload

Check one or more desired target types for picture uploading.

Restore Parameters

Restore Defaults

Click **Restore** to restore all the settings in advanced configuration to the factory default.

11.5.5 Set Shield Region

The shield region allows you to set the specific region in which the set smart function rule is invalid.

Steps

1. Select **Shield Region**.
2. Click ⬠ to draw shield region. Repeat this step above to set more shield regions.
3. **Optional:** Select and click on the drawn region, then click ✕ to delete the selected drawn region.
4. **Optional:** Click 🗑 to delete all drawn regions.
5. Click **Save**.

11.5.6 View Multi-Target-Type Counting Statistics

For the device that supports **Multi-Target-Type Counting**, you can view, generate a report of, and report the counting data by its counting data statistics.

Before You Start

For multi-target-type counting settings, refer to ***Set Multi-Target-Type Counting Rule*** for details.

Steps

1. Go to **Application Display → Multi-Target-Type Counting Statistics** .
2. Set the search condition.
3. Click **Search** to generate the report.

   The data information that matches the conditions will be displayed.
4. When the statistics result is displayed in list, you can click **Export** to export the data.

11.6 Face Picture Comparison

Face picture comparison serves the purpose of face recognition by comparing the captured face pictures with those in face picture library.

Note

- For certain device models, you need to enable **Face Picture Comparison** on **VCA** page first.
- The function is only supported by certain device models.

11.6.1 Set Face Picture Library

Face picture library is used to store modeled human faces and information.

Steps

1. Go to **VCA → General Settings → Face Picture Library** .
2. Create a face picture library.
   1) Click **Add** to add a face picture library.
   2) Input library name, threshold and remarks.

      Threshold

      Face similarity higher than the set threshold triggers face picture comparison alarm uploading.
   3) Click **OK**.
   4) **Optional:** Modify a face picture library. Select the desired library and click **Modify** and change related parameters.
   5) **Optional:** Delete a library. Select the desired library and click **Delete**.
3. Add face pictures to the library.

   Note

   The picture format should be JPG or JPEG, and the size no larger than 300 KB per file.

Add one face picture	Click **Add** and upload the face picture with detailed face information.
Import face pictures in batch	Click **Import** and select picture path. You can select and import multiple face pictures as required.

Note

When you import face pictures in batch, the picture name is saved as the face name. For other face information, you should modify one by one manually.

4. **Optional:** Modify face information.
   1) Select a face picture library.
   2) Select the target face picture. You can use the search function to locate the picture by inputting search conditions, and click **Search**.
   3) Click **Modify**.
   4) Edit detailed information.

      Note

      Face picture is not allowed to change.
   5) Click **OK**.
5. Click **Batch Modeling** to create models for each face picture in library.

   Note

   Modeling process builds up face model for each selected face picture. Face model is required for face picture comparison to take effect.
6. **Optional:** Repeat to create more face picture libraries.

11.6.2 Set Face Picture Comparison

The function compares captured pictures with face pictures in library and outputs comparison result. Comparison result can trigger certain actions when arming schedule and linkage method are set.

Before You Start

- Go to **VCA** and select the application. Select **Face Picture Comparison** and click **Next** to enable the function.
- You should first set face capture function. See ***Set Face Capture*** .
- You should first create a face picture library and add face pictures. See ***Set Face Picture Library*** .

Steps

1. Go to **VCA → Set Application → Face Picture Comparison** and select **Comparison and Modeling**.
2. Check **Enable**.
3. Select a comparison mode.

   Best Comparison
   The device captures and compares the target face continuously when the face target stays in the detection area, and upload the best scored face picture and related alarm information when the target face leaves the area.

Quick Comparison

The device captures and compares the target face when the face grading exceeds the set **Face Grading Threshold for Capture**.

Face Grading Threshold for Capture

The face grading threshold for the device to judge whether to capture and upload the face or not.

Max. Capture Interval

The max. interval between two captures when the target is in the detection area. The camera takes the capture when it reaches the max. interval even if the face grading does not reach the set threshold.

Quick Setup Mode

Select the mode according to actual using scenarios. In custom mode, you can set **Comparison Timeout** and **Comparison Times**.

4. **Optional:** Set data uploading.
   - Select desired information to upload.
   - Select the desired linked comparison alarm.
5. Select a face picture library as the reference. Refer to ***Set Face Picture Library*** for details.
6. Set arming schedule. See ***Set Arming Schedule*** .
7. Set linkage method. See ***Linkage Method Settings*** .
8. Click **Save**.

What to do next

Go to **Application Display → Face Picture Comparison Result** to view the face picture comparison statistics. Refer to ***View Face Picture Comparison Result*** for details.

11.6.3 View Face Picture Comparison Result

Steps

1. Go to **Application Display → Face Picture Comparison Result** .
2. Set search condition and click **Search**.

Result

Matched results are shown in the right area.

11.7 People Management

People management is used to detect and analyze people number and changes in a predefined region. It can be applied to the entrances and exits, supermarkets, etc.

Note

- For certain device models, you need to enable **People Management** on **VCA** page first.
- The function is only supported by certain device models.

11.7.1 Regional People Counting

It counts people in a predefined area and detects people number changes and crowded situation. When the people number exception or waiting time exception occurs, the device can trigger an alarm.

Refer to ***Set People Density*** to set people density detection.

Refer to ***Set People Exception Detection*** to set people exception detection.

Refer to ***Waiting Time Exception Detection*** to set waiting time exception detection.

Set People Density

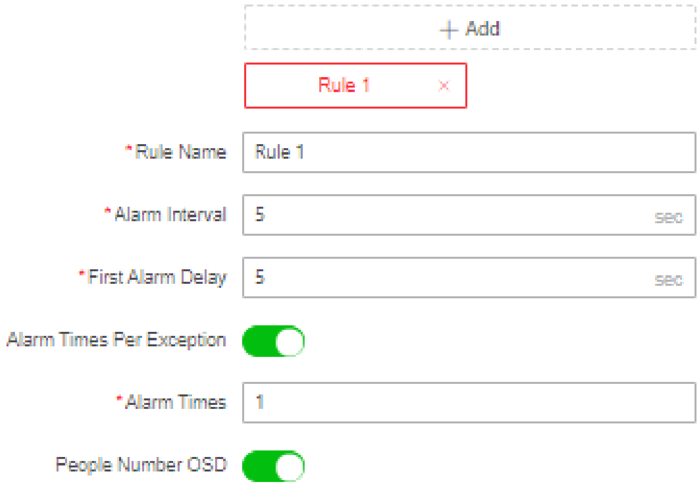
This function detects the level of people density in the set rule region.

Before You Start

- Go to **VCA → Select Application** , select **People Management** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Management**.

Steps

1. Go to **VCA → Set Application → People Management → Regional People Counting → Rule** .
2. Click **Add** to add a rule and set its name.
3. Set a rule.



+ Add

Rule 1

*Rule Name: Rule 1

*Alarm Interval: 5 sec

*First Alarm Delay: 5 sec

Alarm Times Per Exception: ON

*Alarm Times: 1

People Number OSD: ON

Figure 11-16 Set Rules

People Number OSD

It displays the real-time people number in the live view window. You can drag the mouse to adjust the OSD window location.

Note

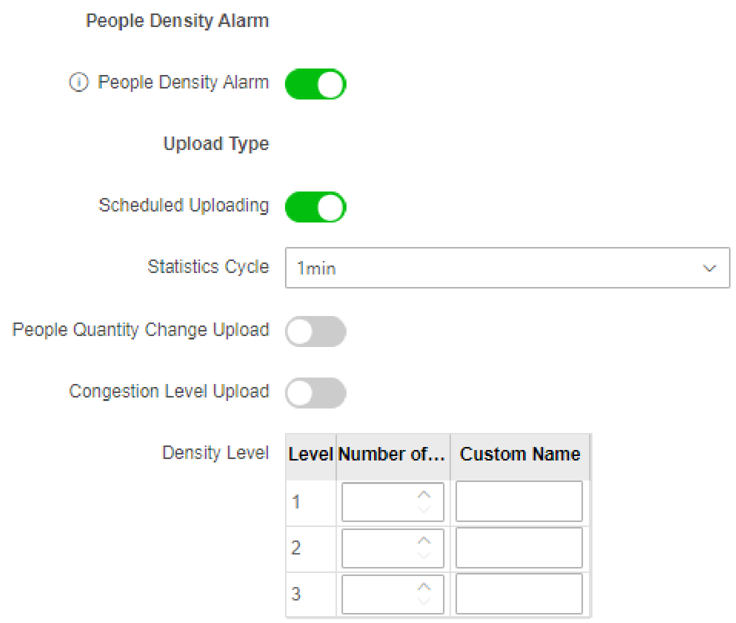
People density alarm does not support **Alarm Times Per Exception**, **Alarm Interval** and **First Alarm Delay** settings.

4. Click ▭ to draw a region in the live view window, left click the end-points in the live view window to define the boundary of the set rule region, and right click to finish drawing.

Note

- Up to 8 regions can be set at the same time.
- Try not to overlap the regions.

5. Check **People Density Alarm** to enable the function.



People Density Alarm

ⓘ People Density Alarm ●

Upload Type

Scheduled Uploading ●

Statistics Cycle 1min

People Quantity Change Upload ○

Congestion Level Upload ○

Density Level

Level	Number of...	Custom Name
1		
2		
3		

Figure 11-17 People Density Alarm

Scheduled Uploading

The device uploads people density information within the set statistics cycle.

People Quantity Change Upload

The device uploads the people quantity change information if there is any change in the set rule region.

Congestion Level Upload

The device uploads the congestion information when there is any change of congestion level in the set rule region.

Density Level

Number of People

The range for each level by inputting the lower limit of the number of people in the set rule region.

Custom Name

The name of the level.

Note

- Set the **Number of People** before the **Custom Name**.
- Up to three levels can be configured. The density increases from level 1 to level 3.

6. Set arming schedule. See ***Set Arming Schedule*** .
7. Set linkage method. See ***Linkage Method Settings*** .
8. Click **Save**.

9. **Optional:** Set overlay and capture parameters. For detailed settings, refer to ***Overlay and Capture*** .
10. **Optional:** View version and set filtering condition. For detailed settings, refer to ***Advanced Settings*** .

Set People Exception Detection

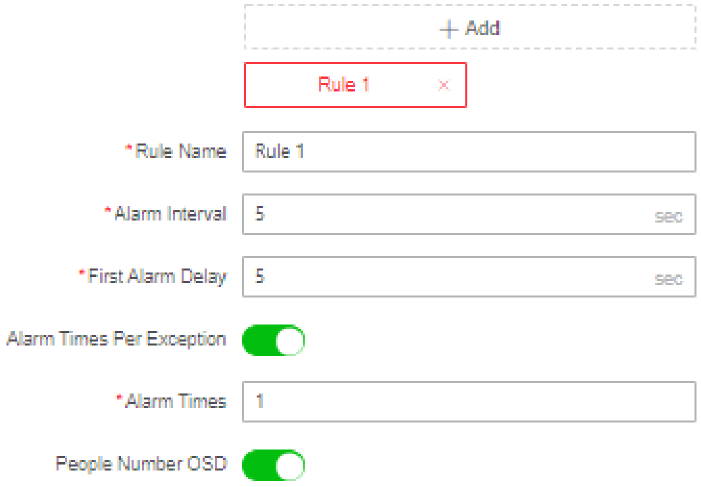
This function detects the number of people in the set rule region and an alarm is triggered when the situation meets the alarm-triggering condition.

Before You Start

- Go to **VCA → Select Application** , select **People Management** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Management**.

Steps

1. Go to **VCA → Set Application → People Management → Regional People Counting → Rule** .
2. Click **Add** to add a rule and set its name.
3. Set a rule.



+ Add

Rule 1 ×

*Rule Name: Rule 1

*Alarm Interval: 5 sec

*First Alarm Delay: 5 sec

Alarm Times Per Exception: on

*Alarm Times: 1

People Number OSD: on

Figure 11-18 Set Rules

People Number OSD

It displays the real-time people number in the live view window. You can drag the mouse to adjust the OSD window location.

Alarm Times Per Exception

It refers to the alarm times after an alarm is triggered. If you do not check it and set the times, the device will keep sending alarms.

Alarm Interval

Within the set **Alarm Interval**, the same alarm will not be uploaded.

First Alarm Delay

When the first alarm is triggered, the alarm will be uploaded after a set time period.

4. Click ⬠ to draw a region in the live view window, left click the end-points in the live view window to define the boundary of the set rule region, and right click to finish drawing.

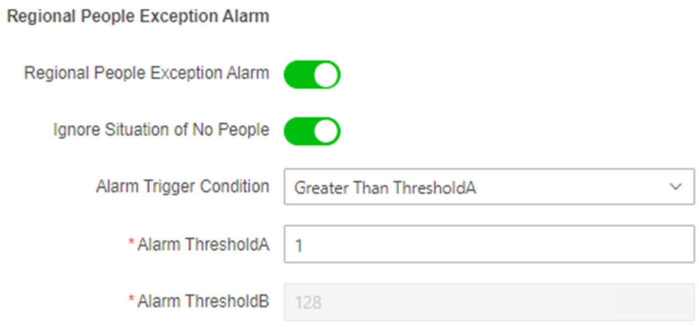
Note

- Up to 8 regions can be set at the same time.
- Try not to overlap the regions.

5. Check **Regional People Exception Alarm**, and set **Alarm Trigger Condition** and **Alarm Threshold**.

Note

- After enabling **Ignore Situation of No People**, the device will not trigger an alarm when there is no people in the region.
- This function can filter the potential alarm condition under which the value is less than the set **Alarm Threshold** and no people in the region.



Regional People Exception Alarm

Regional People Exception Alarm: On

Ignore Situation of No People: On

Alarm Trigger Condition: Greater Than ThresholdA

*Alarm ThresholdA: 1

*Alarm ThresholdB: 128

Figure 11-19 Regional People Exception Alarm

6. Set arming schedule. See ***Set Arming Schedule*** .
7. Set linkage method. See ***Linkage Method Settings*** .
8. Click **Save**.
9. **Optional:** Set overlay and capture parameters. For detailed settings, refer to ***Overlay and Capture*** .
10. **Optional:** View version and set filtering condition. For detailed settings, refer to ***Advanced Settings*** .

Waiting Time Exception Detection

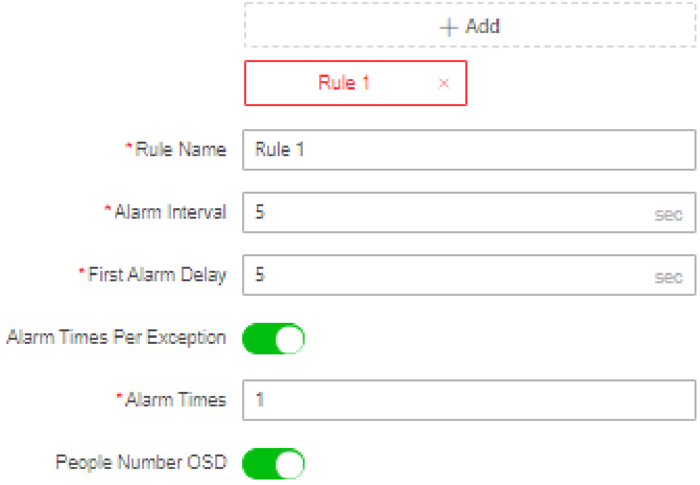
This function detects the waiting time of the set rule region and an alarm is triggered when the waiting time meets the alarm-triggering condition.

Before You Start

- Go to **VCA → Select Application** , select **People Management** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Management**.

Steps

1. Go to **VCA → Set Application → People Management → Regional People Counting → Rule** .
2. Click **Add** to add a rule and set its name.
3. Set a rule.



+ Add

Rule 1 ×

*Rule Name: Rule 1

*Alarm Interval: 5 sec

*First Alarm Delay: 5 sec

Alarm Times Per Exception: on

*Alarm Times: 1

People Number OSD: on

Figure 11-20 Set Rules

People Number OSD

It displays the real-time people number in the live view window. You can drag the mouse to adjust the OSD window location.

Alarm Times Per Exception

It refers to the alarm times after an alarm is triggered. If you do not check it and set the times, the device will keep sending alarms.

Alarm Interval

Within the set **Alarm Interval**, the same alarm will not be uploaded.

First Alarm Delay

When the first alarm is triggered, the alarm will be uploaded after a set time period.

Note

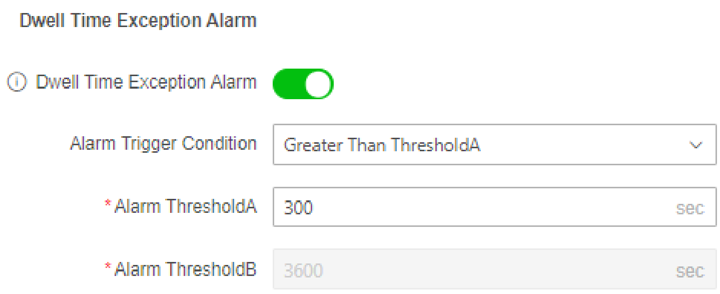
Dwell time exception alarm supports **Alarm Times Per Exception**, **Alarm Interval** and **First Alarm Delay** settings only on the condition that the **Alarm Trigger Condition** is **Greater Than Threshold A**.

4. Click ▢ to draw a region in the live view window, left click the end-points in the live view window to define the boundary of the set rule region, and right click to finish drawing.

Note

- Up to 8 regions can be set at the same time.
- Try not to overlap the regions.

5. Check **Dwell Time Exception Alarm**, and set **Alarm Trigger Condition** and **Alarm Threshold**.



Dwell Time Exception Alarm

ⓘ Dwell Time Exception Alarm	●
Alarm Trigger Condition	Greater Than ThresholdA
* Alarm ThresholdA	300 sec
* Alarm ThresholdB	3600 sec

Figure 11-21 Dwell Time Exception Alarm

6. Set arming schedule. See ***Set Arming Schedule*** .
7. Set linkage method. See ***Linkage Method Settings*** .
8. Click **Save**.
9. **Optional:** Set overlay and capture parameters. For detailed settings, refer to ***Overlay and Capture*** .
10. **Optional:** View version and set filtering condition. For detailed settings, refer to ***Advanced Settings*** .

11.7.2 On/Off Duty Detection

When a target in a predefined area triggers an on/off duty rule, the device can take linkage actions. It can detect the on/off duty status and people number changes in a predefined area.

Before You Start

- Go to **VCA** and select the application. Select **People Management** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Management**.

Steps

1. Go to **VCA → Set Application → People Management → On/Off Duty Detection → Rule** .
2. Click **Add** and edit the rule name according to your need.
3. Select a rule and set the rule parameters.

   Absence Detection

   If the people number in the set area is less than the value of **Person On Duty** and the lasting time is longer than the **Absence Duration**, an alarm is triggered.

On/Off Duty Detection

It includes on/off duty situation detection.

People Number OSD

It overlays the real-time people number on the live view. You can adjust the OSD location by dragging the mouse.

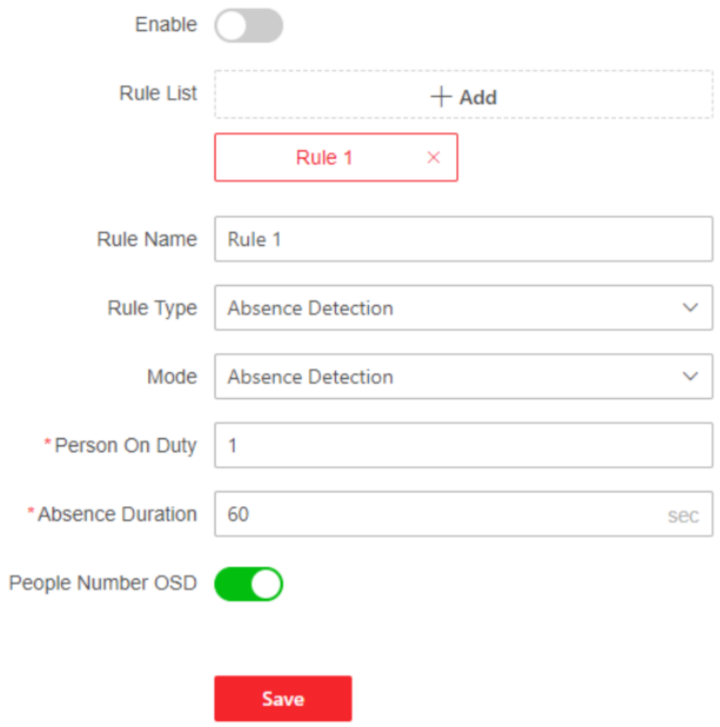

Enable: ○
Rule List: + Add
Rule 1 ×
Rule Name: Rule 1
Rule Type: Absence Detection
Mode: Absence Detection
*Person On Duty: 1
*Absence Duration: 60 sec
People Number OSD: ●

Figure 11-22 Set Rules

4. Click ⬭ to draw a rule area in the live view window. Left click the end-points in the live view window to define the boundary of the set rule area, and right click to finish drawing.

Note

- Up to 8 areas can be set at the same time.
- Try not to overlap the areas.

5. Click **Save**.

Note

You can set the parameters of multiple areas by repeating the above steps.

6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .

Note

Select the rule in the rule list, and click **Copy to...** to copy the related arming schedule and linkage method settings to the other rules.

7. **Optional:** Set overlay and capture parameters. For detailed settings, refer to ***Overlay and Capture*** .
8. **Optional:** View version and set filtering condition. For detailed settings, refer to ***Advanced Settings*** .

11.7.3 Queue Management

It is used to calculate and analyze the number of people and queue status in the area, and output results.

Refer to ***Set Queue Duration Prediction*** to set queue duration prediction.

Refer to ***Set Regional People Queuing-Up*** to set regional people queuing-up detection.

Refer to ***Set Waiting Time Detection*** to set waiting time detection.

Refer to ***Queue Management Statistics*** to set and view queue management statistics.

Note

- Queue management is only supported by certain models.
- **Queue Duration Prediction** is mutually exclusive with some functions, such as **On/Off Duty Detection**, **Regional People Queuing-Up** and **Waiting Time Detection**. Enable this function may make other functions unavailable, and vice versa.

Set Queue Duration Prediction

It is used to calculate and predict the queue duration in the predefined area.

Before You Start

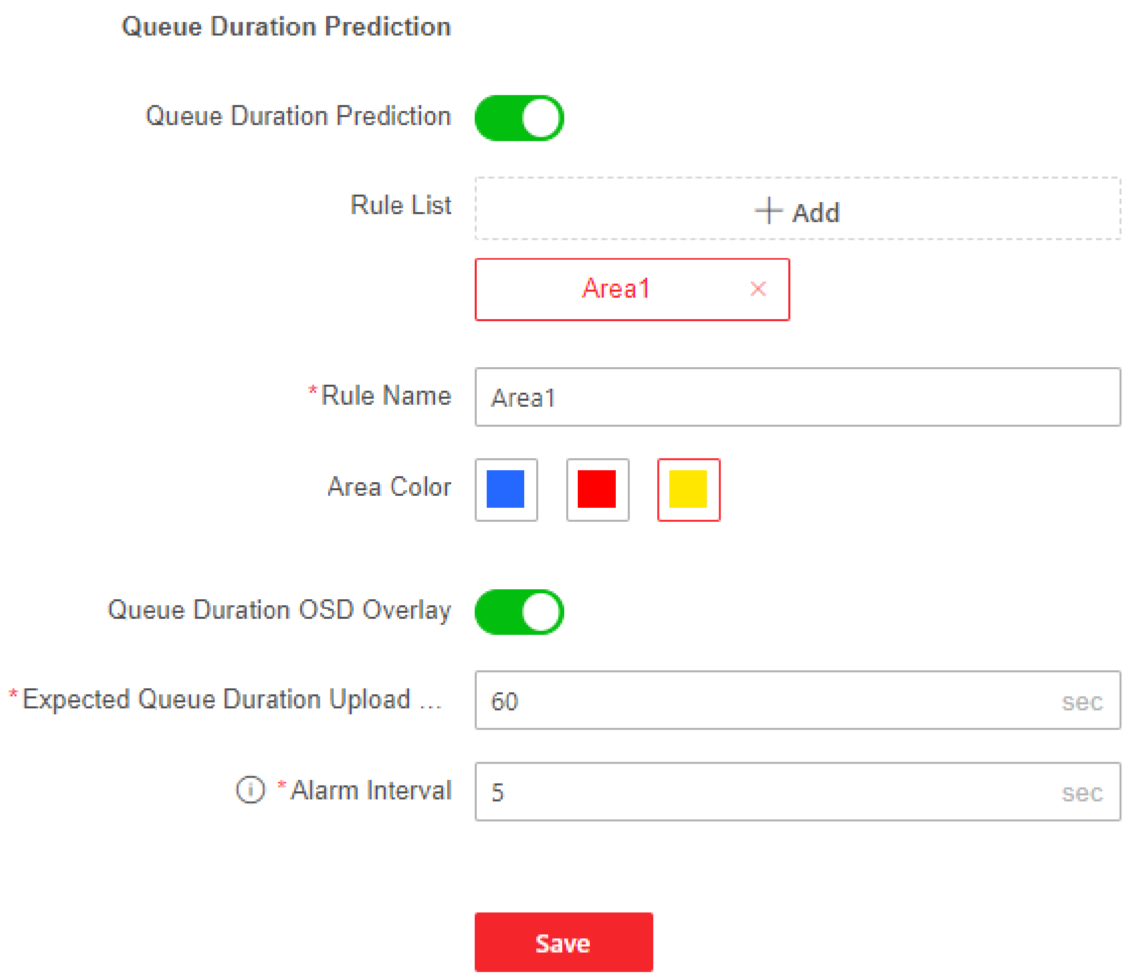
- Go to **VCA** and select the application. Select **People Management** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Management**.

Steps

1. Go to **VCA → Set Application → People Management → Queue Management → Rule** .
2. Check **Queue Duration Prediction** to enable the function.

Note

Queue Duration Prediction is mutually exclusive with some functions, such as **On/Off Duty Detection**, **Regional People Queuing-Up** and **Waiting Time Detection**. Enable this function may make the other functions unavailable, and vice versa.



Queue Duration Prediction

Queue Duration Prediction ●

Rule List: + Add

Area1 ×

*Rule Name: Area1

Area Color: 🟦 🟥 🟨

Queue Duration OSD Overlay ●

*Expected Queue Duration Upload ...: 60 sec

ⓘ *Alarm Interval: 5 sec

Save

Figure 11-23 Set Queue Duration Prediction

3. Draw areas.

Note

You can click **View Drawing Example** for a drawing example of the actual scene.

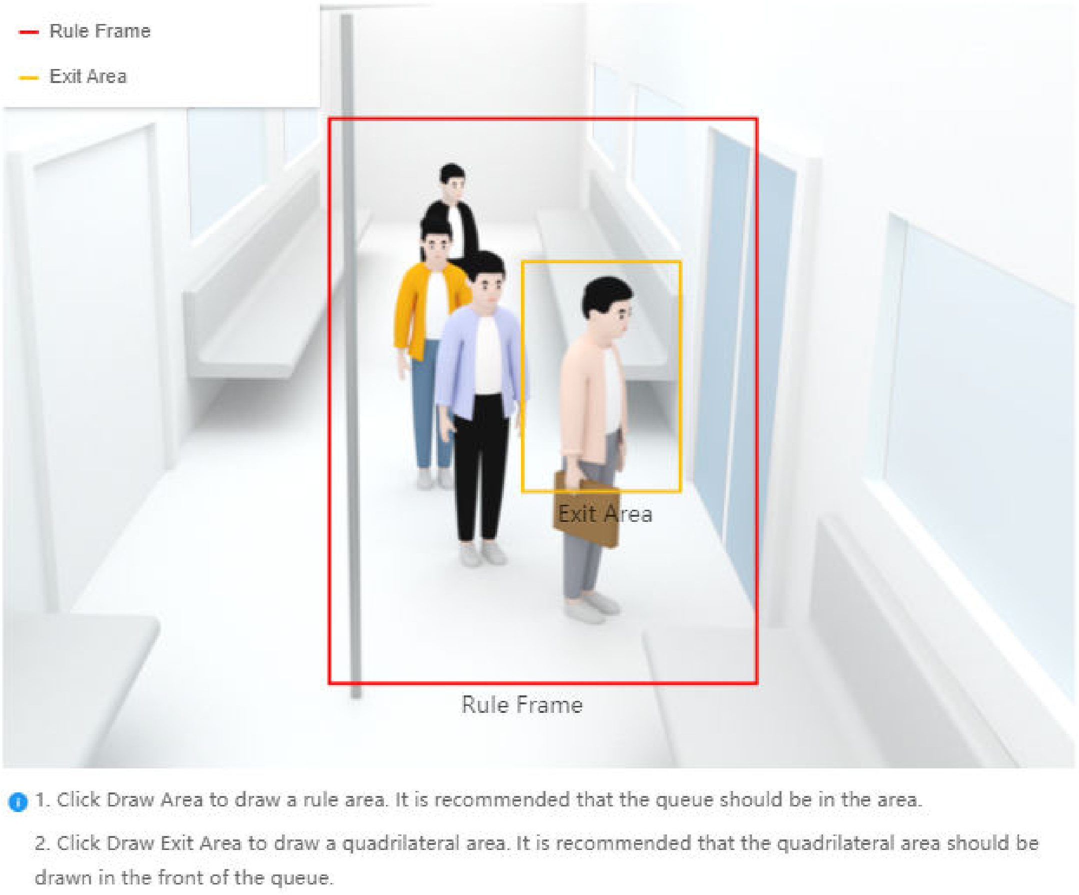
1) Click **Add** and edit the rule name according to your need.

2) Select an **Area color** and click ▭ to draw a rule area. Left click the end-points in the live view window to define the boundary of the set rule area, and right click to finish drawing. It is recommended that the queue should be in the area.

3) Click ▭ to draw a quadrilateral area. It is recommended that the quadrilateral area should be drawn in the front of the queue.

Note

- Up to 8 areas can be set at the same time.
- Try not to overlap the areas.



1. Click Draw Area to draw a rule area. It is recommended that the queue should be in the area.

2. Click Draw Exit Area to draw a quadrilateral area. It is recommended that the quadrilateral area should be drawn in the front of the queue.

Figure 11-24 Drawing Example of Queue Duration Prediction

4. Set rule parameters.

   Queue Duration OSD Overlay

   When enabled, the queue duration will be displayed in the image, and you can adjust the display position of the OSD overlay on the live view image.

   Expected Queue Duration Upload Interval and Alarm Interval

   The device uploads queue duration information at each upload interval. In the set **Alarm Interval**, only one notification is triggered for repeated alarms.

5. Click **Save**.

Note

You can set the parameters of multiple areas by repeating the above steps.

6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .

Note

Select the rule in the rule list, and click 📄 or click **Copy to...** to copy the related arming schedule and linkage method settings to the other rules.

7. **Optional:** Set overlay and capture parameters. For detailed settings, refer to ***Overlay and Capture*** .
8. **Optional:** View version and set filtering condition. For detailed settings, refer to ***Advanced Settings*** .

What to do next

Go to **Application Display → Queue Management Statistics** to view detailed data analysis. For detailed settings, refer to ***Queue Management Statistics*** .

Set Regional People Queuing-Up

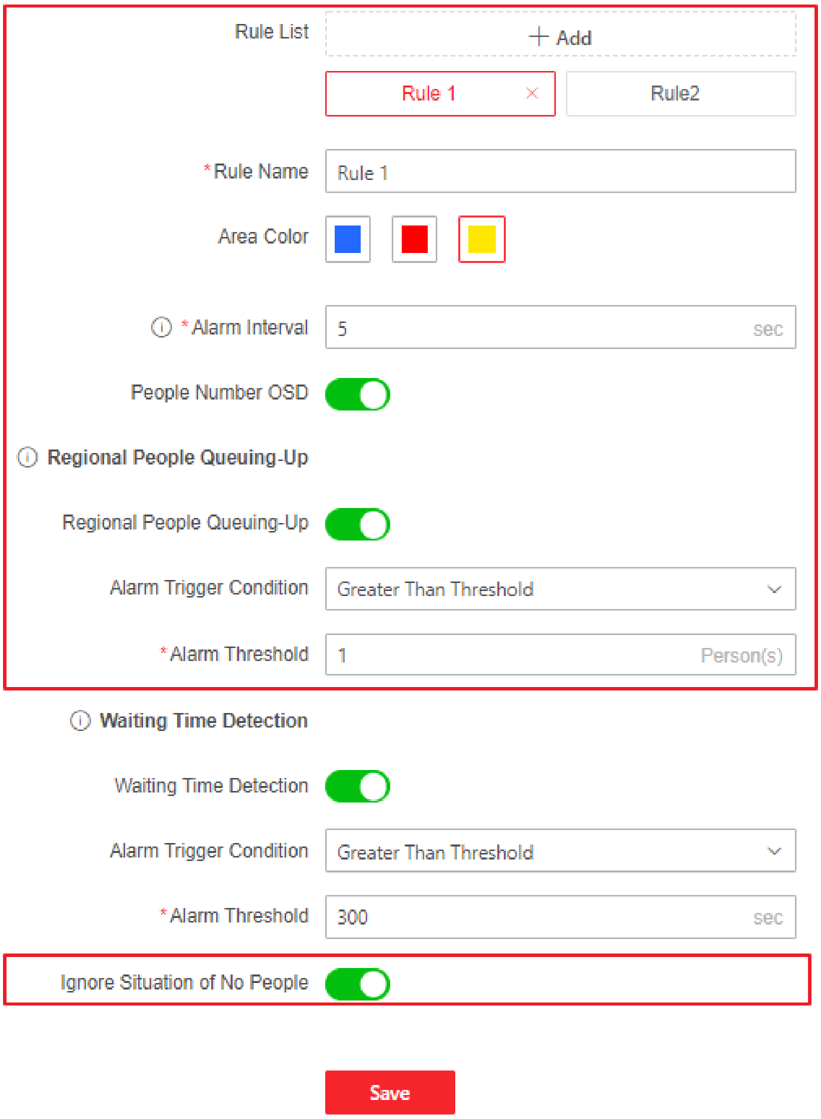
It is used to count queuing-up persons in defined areas. Alarms are triggered when the alarm threshold condition and the alarm trigger are both met.

Before You Start

- Go to **VCA** and select the application. Select **People Management** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Management**.

Steps

1. Go to **VCA → Set Application → People Management → Queue Management → Rule** .
2. Click **Add** and edit the rule name according to your need.



Rule List	+ Add
	Rule 1 × | Rule2
* Rule Name	Rule 1
Area Color	🟦 🟥 🟨
ⓘ * Alarm Interval	5 sec
People Number OSD	On
ⓘ **Regional People Queuing-Up**	
Regional People Queuing-Up	On
Alarm Trigger Condition	Greater Than Threshold
* Alarm Threshold	1 Person(s)
ⓘ **Waiting Time Detection**	
Waiting Time Detection	On
Alarm Trigger Condition	Greater Than Threshold
* Alarm Threshold	300 sec
Ignore Situation of No People	On

3. Select an **Area color** and click ▭ to draw a rule area. Left click the end-points in the live view window to define the boundary of the set rule area, and right click to finish drawing.

Note

- Up to 8 areas can be set at the same time.
- Try not to overlap the areas.

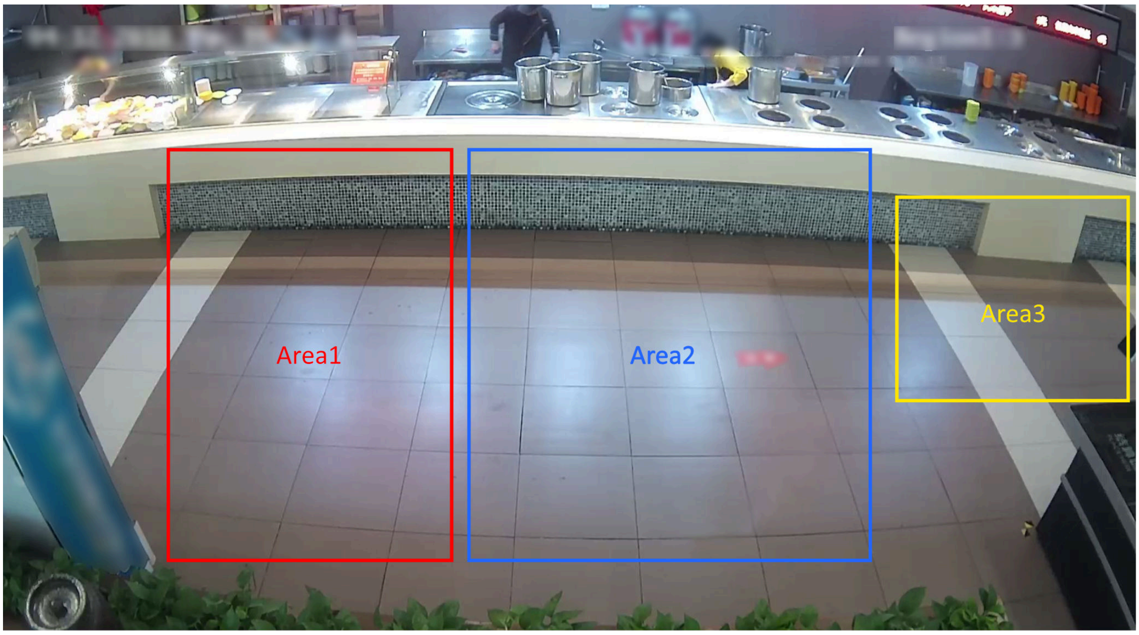


Figure 11-25 Draw Area

4. Set rule parameters.

   Alarm Interval

   During the set alarm interval, alarms of the same type only trigger one notification.

   People Number OSD

   It displays the number of people in the live view window.

   Ignore Situation of No People

   The device will not trigger an alarm when there is no people in the scene. This function can filter the potential alarm condition under which the value is less than the set alarm threshold and no people is in the scene.

5. Select **Regional People Queuing-Up** and set **Alarm Trigger Condition** and **Alarm Threshold**.

   When the people number in the set area reaches alarm threshold and triggering condition, an alarm will be triggered.

6. Click **Save**.

   Note

   You can set the parameters of multiple areas by repeating the above steps.

7. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .

   Note

   Select the rule in the rule list, and click 📄 or click **Copy to...** to copy the related arming schedule and linkage method settings to the other rules.

8. **Optional:** Click **Data Upload** to set data uploading. Both real-time uploading and scheduled uploading are supported. Click **Save** after finishing the settings.

   Real-Time Uploading

   Check **Real-Time Upload** and the device uploads the detected target ID, waiting duration, and regional people number in real-time.

   Scheduled Uploading

   The device uploads the people number whose waiting duration is equal to or larger than the **Min. Duration of Stay** at the integral point.

   For example, if the min. duration of stay is set as 10 sec and two areas are covered, the device, at the integral point, will upload the people number when the duration of stay is equal to or longer than 10 sec in two areas respectively.
9. **Optional:** Set overlay and capture parameters. For detailed settings, refer to ***Overlay and Capture*** .
10. **Optional:** View version and set filtering condition. For detailed settings, refer to ***Advanced Settings*** .

What to do next

Go to **Application Display → Queue Management Statistics** to view detailed data analysis. For detailed settings, refer to ***Queue Management Statistics*** .

Set Waiting Time Detection

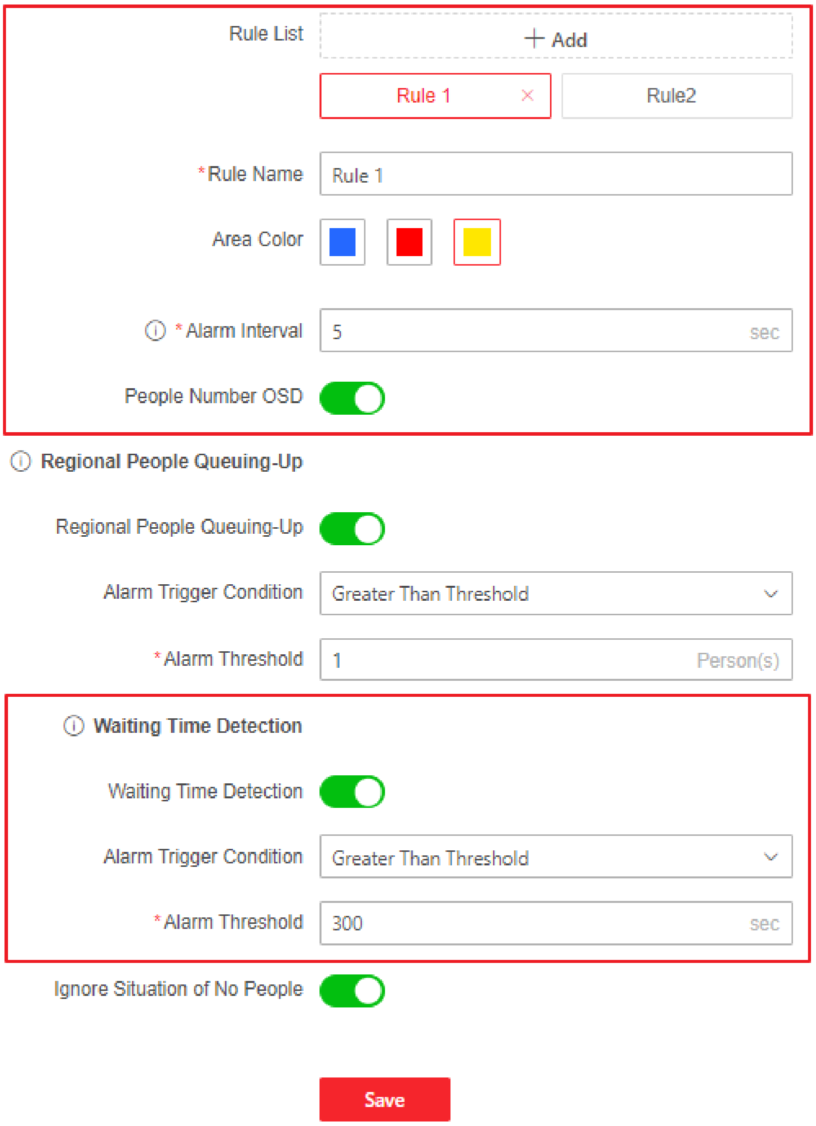
It is used to count the waiting time of each person that enters a detection area. Alarms are triggered when the alarm threshold condition and the alarm trigger are both met.

Before You Start

- Go to **VCA** and select the application. Select **People Management** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Management**.

Steps

1. Go to **VCA → Set Application → People Management → Queue Management → Rule** .
2. Click **Add** and edit the rule name according to your need.



Rule List: + Add

Rule 1 × Rule2

*Rule Name: Rule 1

Area Color: 🟦 🟥 🟨

ⓘ *Alarm Interval: 5 sec

People Number OSD: ●

ⓘ **Regional People Queuing-Up**

Regional People Queuing-Up: ●

Alarm Trigger Condition: Greater Than Threshold

*Alarm Threshold: 1 Person(s)

ⓘ **Waiting Time Detection**

Waiting Time Detection: ●

Alarm Trigger Condition: Greater Than Threshold

*Alarm Threshold: 300 sec

Ignore Situation of No People: ●

3. Select an **Area color** and click ▭ to draw a rule area. Left click the end-points in the live view window to define the boundary of the set rule area, and right click to finish drawing.

Note

- Up to 8 areas can be set at the same time.
- Try not to overlap the areas.

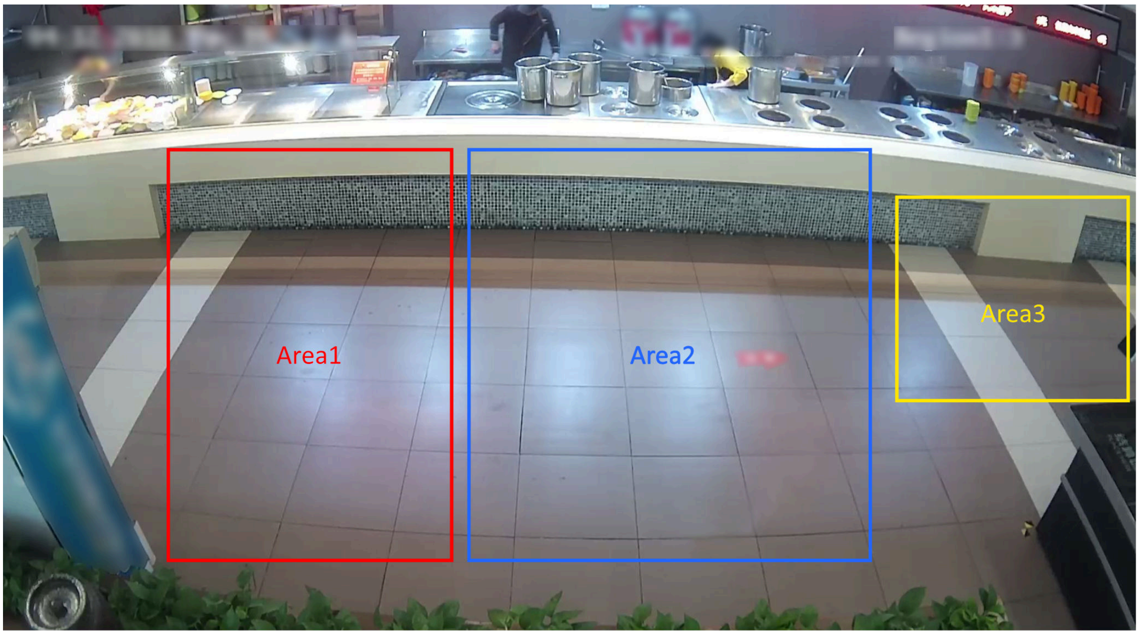


Figure 11-26 Draw Area

4. Set rule parameters.

   Alarm Interval

   During the set alarm interval, alarms of the same type only trigger one notification.

   People Number OSD

   It displays the number of people in the live view window.
5. Select **Waiting Time Detection** and set **Alarm Trigger Condition** and **Alarm Threshold**.

   When the waiting time in the set area reaches alarm threshold and triggering condition, an alarm will be triggered.
6. Click **Save**.

   Note

   You can set the parameters of multiple areas by repeating the above steps.
7. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .

   Note

   Select the rule in the rule list, and click 📄 or click **Copy to...** to copy the related arming schedule and linkage method settings to the other rules.
8. **Optional:** Click **Data Upload** to set data uploading. Both real-time uploading and scheduled uploading are supported. Click **Save** after finishing the settings.

   Real-Time Uploading

Check **Real-Time Upload** and the device uploads the detected target ID, waiting duration, and regional people number in real-time.

Scheduled Uploading

The device uploads the people number whose waiting duration is equal to or larger than the **Min. Duration of Stay** at the integral point.

For example, if the min. duration of stay is set as 10 sec and two areas are covered, the device, at the integral point, will upload the people number when the duration of stay is equal to or longer than 10 sec in two areas respectively.

9. **Optional:** Set overlay and capture parameters. For detailed settings, refer to ***Overlay and Capture*** .
10. **Optional:** View version and set filtering condition. For detailed settings, refer to ***Advanced Settings*** .

What to do next

Go to **Application Display → Queue Management Statistics** to view detailed data analysis. For detailed settings, refer to ***Queue Management Statistics*** .

Queue Management Statistics

Queue management supports data analysis and report output.

Before You Start

For queue management settings, refer to ***Set Regional People Queuing-Up*** and ***Set Waiting Time Detection*** .

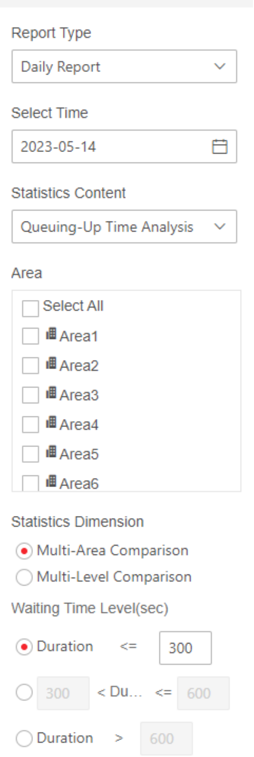
- Select **Queuing-Up Time Analysis** and **Multi-Area Comparison** to compare queuing-up people number of different areas.
- Select **Queuing-Up Time Analysis** and **Multi-Level Comparison** to compare queuing-up people number of different waiting time levels.
- Select **Queue Status Analysis** and **Multi-Area Comparison** to compare the time and duration that a queue stays at a certain length in different areas.
- Select **Queue Status Analysis** and **Multi-Level Comparison** to compare the time and duration of the queue at different queue length levels.

Steps

Note

With an on-board memory card installed, the device can save up to one mouth's data. With NO memory card installed, the device can only save up to one week's data.

1. Go to **Application Display → Queue Management Statistics** .



Report Type

Daily Report

Select Time

2023-05-14

Statistics Content

Queuing-Up Time Analysis

Area

□ Select All

□ Area1

□ Area2

□ Area3

□ Area4

□ Area5

□ Area6

Statistics Dimension

● Multi-Area Comparison

○ Multi-Level Comparison

Waiting Time Level(sec)

● Duration <= 300

○ 300 < Du... <= 600

○ Duration > 600

Figure 11-27 Queue Management Statistics

2. Select **Report Type** and **Statistics Time**.
3. Select **Statistics Content**.

   Queuing-Up Time Analysis

   Queuing-up time analysis calculates people number of different waiting time levels.

   Queue Status Analysis

   Queue status analysis calculates the time and duration that a queue stays a certain length.
4. Select **Statistics Dimension**.

   Multi-Area Comparison

   Multiple areas and one level can be selected for analysis, and an analysis chart can be drawn.

   Multi-Level Comparison

   Multiple levels and areas can be selected for analysis, and one analysis chart is drawn for each area.
5. Check one or more areas.
6. Set **Waiting Time Level**. Check one desired range and enter values.
7. Click **Search** to generate the report.
8. **Optional:** Click **Export** to export the data.

11.7.4 Overlay and Capture

Choose to configure capture parameters and the information you want to display on stream and picture.

Note

The function varies according to different device models.

Go to **VCA → People Management → Overlay & Capture** .

Display VCA Info. on Stream

Display smart information on stream, including the target and rules information.

Display Target Info. on Alarm Picture

Overlay the alarm picture with target information.

Text Overlay

You can check desired items and adjust their order to display on captured pictures.

See ***Set Camera Info*** to set **Device No.** and **Camera Info**.

11.7.5 Advanced Settings

Set the advanced parameters for people management function and click **Save**.

Version

It stands for the current algorithm version.

Overlay Intelligent Information

Overlay the related intelligent information or POS information in the video.

Algorithm Mode

Select a mode according to the installation scene.

Filter

Target Size

It stands for the size of the target detection window. A target larger than this pixel can be counted as a real target. It can remove the false alarm of a certain fixed target.

Displacement

It stands for target displacement or the target width. A target will not be counted if its displacement is less than the set percentage.

Min. Waiting Duration

Waiting time shorter than the set value will be filtered.

Confidence

The higher the threshold is, the more difficult a target will be detected, but the higher the accuracy is.

Note

The filtering settings should be operated by the professionals. The filter settings can adjust the algorithm for detection to change the detection range, sensitivity, etc.

Clear Storage Data

Clear all people counting data stored in the device. This function must be used with caution.

11.8 Heat Map

Heat map is a graphical representation of data represented in colors. The heat map function of the camera is used to analyze the visiting times and dwelling time of customers in a configured area.

Note

The function is only supported by certain device models.

11.8.1 Set Heat Map

If you want to query statistical data of heat map, please configure the camera first.

Before You Start

- Go to **VCA** and select the application. Select **People Management** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Management**.
- Set the storage path first before searching heat map data. For the storage settings, refer to ***Storage Settings*** .

Steps

1. Go to **VCA → Set Application → People Management → Heat Map Configuration** .
2. Check **Enable** to enable the function.
3. Draw a detection area. Click ⬠, click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.

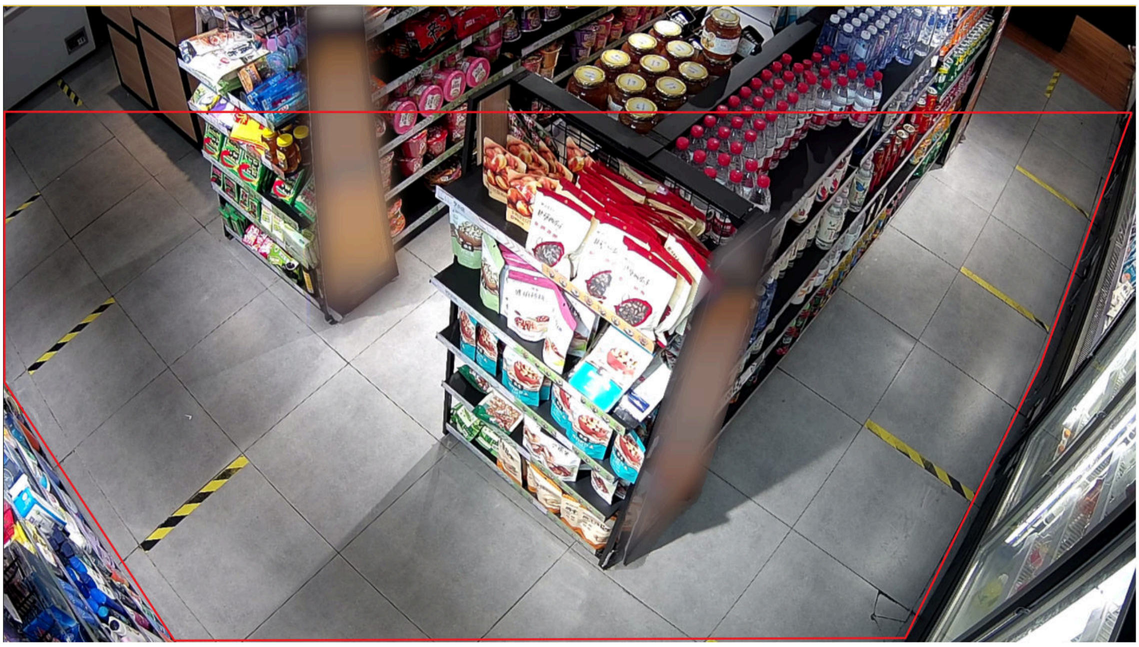


Figure 11-28 Draw Area

4. Configure the parameters for the drawn area.

   Expected Number of People

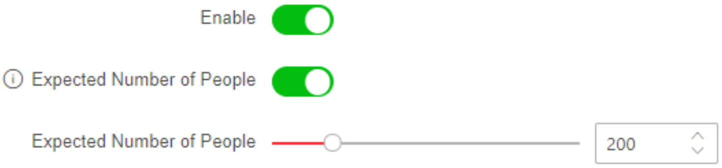
   It refers to the max. number of people for heat map counting.

   ON

   It refers to that the camera will compare the max. number of the people in the actual scene with the set expected number of people and take the larger one as the max. number of people for heat map.

   OFF

   It refers to that the camera will take the actual number of people as the max. value of heat map.



Enable ●

ⓘ Expected Number of People ●

Expected Number of People 200

Figure 11-29 Set Rules

5. Click **Save**.
6. Set arming schedule. See ***Set Arming Schedule*** .
7. Set linkage method. See ***Linkage Method Settings*** .

8. **Optional:** Click **Data Upload** to set the data uploading information. Click **Save** to save the settings.

   Uploading Data Type

   Dwell Time

   It refers to the target's dwelling time in the detection area.

   Dwell Time and Number of People

   It refers to the target's dwelling time in the detection area and the people number in the detection area.

What to do next

The heat map statistics will be calculated under **Application Display** tab. Go to **Application Display** to check the heat map statistics.

11.8.2 View Heat Map Data

Heat map can observe and calculate the people flow in a predefined area and display the flow statistics in graphical form. It can be applied to scenes of large passenger flow such as malls, supermarkets, and museums. You can find the customers' preferences to adjust the places of merchandise through heat map.

Before You Start

Finish heat map configuration. For details, refer to ***Set Heat Map*** .

Steps

1. Go to **Application Display → Heat Map** .
2. Select **Report Type**. Daily report, weekly report, monthly report, and annual report are selectable.
3. Select **Heat Map Type**. Spatial heat map and time heat map are selectable.
4. Select **Statistics Type**. By dwell time and by people number are selectable.
5. Select **Statistics Time**.
6. Click **Search**.

   Daily report calculates the data on the date you selected; weekly report calculates the week data your selected date belongs to; monthly report calculates the data for the month your selected date belongs to; and the annual report calculates the data for the year your selected date belongs to.

Example

After the calculating, you can view the data in the spatial heat map and time heat map.

Spatial Heat Map

Perform a statistical analysis on the cumulative dwelling of people in different areas in the entire image.

Different heat values correspond to different colors, among which red (255, 0, 0) represents the highest heat, and blue (0, 0, 255) represents the lowest heat. The highest heat value and lowest heat value are divided into N levels, corresponding to different colors.

Time Heat Map

Perform a statistical analysis on the total dwelling time of all people in the entire image.

The time heat map is presented in a line chart, and you can click **Export** to export the data in an excel file.

11.9 Multi-Dimension People Counting

This function is used to calculate the number of people entering in or exiting from the specified scene.

Note

- For certain device models, you need to enable **Multi-Dimension People Counting** on **VCA** page first.
- The function is only supported by certain device models.

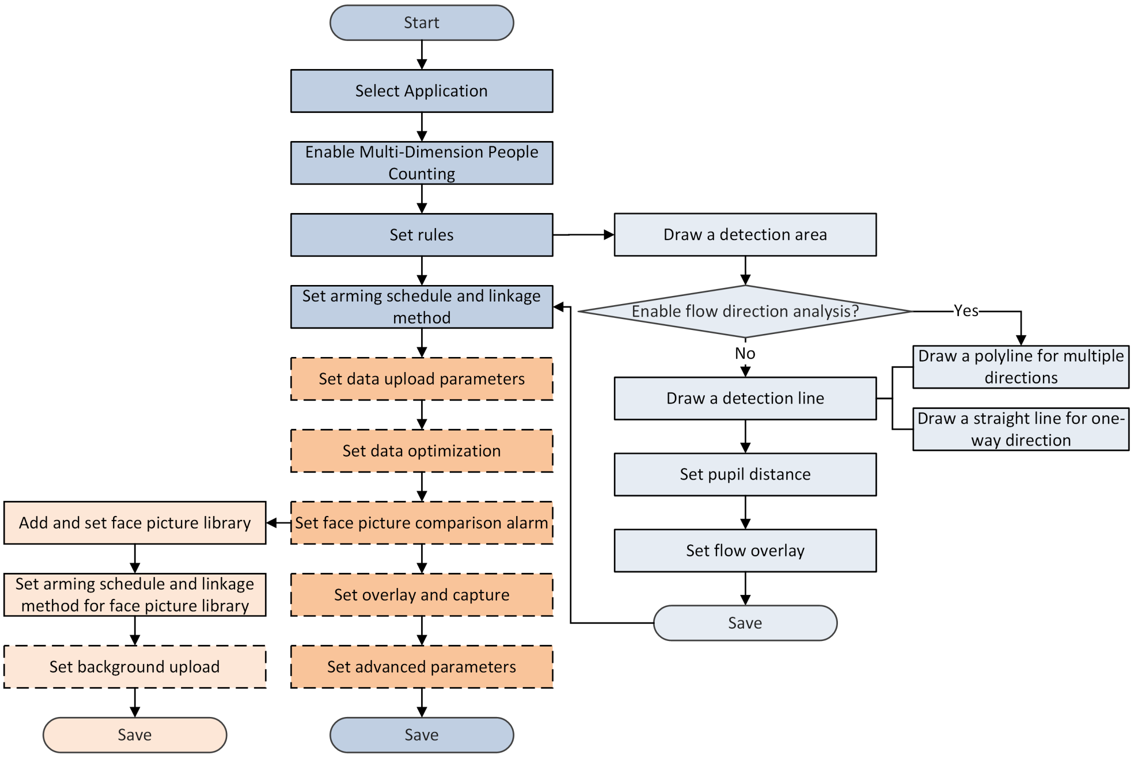

Start
Select Application
Enable Multi-Dimension People Counting
Set rules
Draw a detection area
Set arming schedule and linkage method
Enable flow direction analysis?
Yes
No
Draw a polyline for multiple directions
Draw a detection line
Draw a straight line for one-way direction
Set data upload parameters
Set data optimization
Set pupil distance
Add and set face picture library
Set face picture comparison alarm
Set flow overlay
Set arming schedule and linkage method for face picture library
Set overlay and capture
Save
Set background upload
Set advanced parameters
Save
Save

Figure 11-30 Set Multi-Dimension People Counting

11.9.1 Set Multi-Dimension People Counting Rule

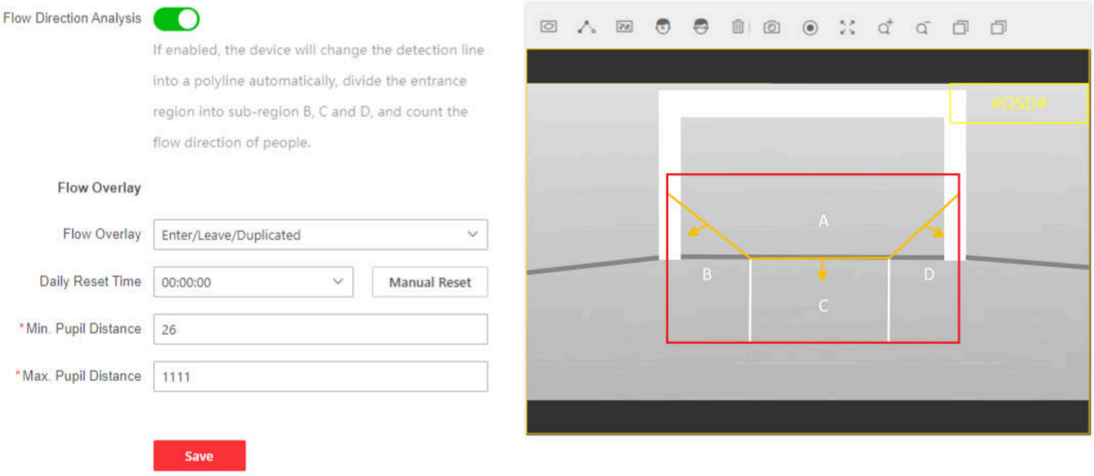
After setting the detection rules and algorithm parameters, the device calculates the number of people entering or exiting in the rule area, triggers linkage actions and uploads data automatically.

Before You Start

Go to **VCA → Select Application** , select **Multi-Dimension People Counting** and click **Next** to enable the function.

Steps

1. Go to **VCA → Set Application → Multi-Dimension People Counting → Rule** .



Flow Direction Analysis ●

If enabled, the device will change the detection line into a polyline automatically, divide the entrance region into sub-region B, C and D, and count the flow direction of people.

Flow Overlay

Flow Overlay: Enter/Leave/Duplicated

Daily Reset Time: 00:00:00 | Manual Reset

*Min. Pupil Distance: 26

*Max. Pupil Distance: 1111

Save

Figure 11-31 Set Rules

2. Click to draw a convex red rule frame. The rule frame should be larger than the actual detection area, such as door.
3. Draw a detection line.
   - When the detection area only supports one-way direction, it is recommended to click to draw a straight detection line.
   - When the detection area supports multiple directions, or there are walls and obstacles in the detection area, it is recommended to click to draw a polyline.

Note

- The detection line should be within and in the middle of the rule area. It is recommended to draw the line on people chest position in the live view.
- The arrow of the detection line shows entering direction.

4. **Optional:** When the detection area supports multiple directions, you can enable **Flow Direction Analysis**. If the function is enabled, the device will change the detection line into a polyline automatically, divide the entrance region into sub-region B, C and D, and count the flow direction of people.
5. **Optional:** Adjust the detection area and detection line.

Click ⇄ Change the detection line direction if the direction is different from the actual flow direction.

Click ✕ Clear all detection areas and lines.

6. Draw pupil distance.

   Min. Pupil Distance

   Click ☺ to draw the minimum pupil distance. If the pupil distance of the face in the video image is smaller than the minimum pupil distance, the face will not be detected.

   Max. Pupil Distance

   Click ☺ to draw the maximum pupil distance. If the pupil distance of the face in the video image is larger than the maximum pupil distance, the face will not be detected.

7. Set the flow counting parameters.

   Flow Overlay

   Select the data to be displayed on the live view from the drop-down list.

   Daily Reset Time

   Select a time point through the drop-down list. After selecting, the flow counting data will be automatically cleared at this time point every day. Click **Manual Reset** to manually trigger a data reset.

8. Set arming schedule. See ***Set Arming Schedule*** .
9. Set linkage method. See ***Linkage Method Settings*** .
10. **Optional:** Set the people counting data uploading parameters.

    Real-Time Upload Data

    If it is checked, the flow counting data will be uploaded to the platform for update in real time.

    Upload Data Periodically

    If it is checked, the flow counting data will be uploaded to the platform for update according to the statistical period. In this case, **Data Statistics Cycle** needs to be set.

11. Click **Save**.
    - When the target crosses the detection area along the entering direction and passes the detection line, the target is counted as one entering target.
    - When the target crosses the detection area along the leaving direction and passes the detection line, the target will be counted as one exiting target.
    - When the target crosses the detection area along the entering direction multiple times within the **Filtering Time Interval**, and passes the detection line, the target will be counted as one duplicate target.
12. **Optional:** Set data optimization parameters. Click **Save** after setting the parameters.

    Special Attribute Deduplication

    If enabled, the device will determine whether the target is a duplicate target with the same attribute. If it is a duplicate target, it will be counted as one entering target, and also counted as one duplicate target.

Dynamic Deduplication

Persons who appear repeatedly within the **Filtering Time Interval** are not counted as an effective target. In other words, if it is a duplicate target, it will be counted as one duplicate target and one entering target. If the **Filtering Time Interval** is set to 0, the function is not enabled.

Face Picture Library Deduplication

If enabled, the device compares the target with the modeling data in the face library to determine whether it is a duplicate target. If it is a duplicate target, it will be counted as one entering target, and also counted as one duplicate target.

Note

For detailed settings about face picture library, refer to ***Set Face Picture Library*** .

13. **Optional:** Set face picture comparison alarm. See ***Set Face Picture Comparison Alarm*** .
14. **Optional:** Set overlay and capture parameters.

Display VCA Info. on Stream

Display smart information on stream, including the target and rules information.

Display Target Info. on Alarm Picture

Overlay the alarm picture with target information.

Text Overlay

You can check desired items and adjust their order to display on captured pictures by sorting.

15. **Optional:** Set advanced parameters. Refer to ***Multi-Dimension People Counting Advanced Settings*** for details.

What to do next

Go to **Application Display** to view detailed people counting data analysis. For detailed settings, refer to ***View People Counting Statistics*** .

11.9.2 Multi-Dimension People Counting Advanced Settings

Go to **VCA → Set Application → Multi-Dimension People Counting → Advanced** to view and set the advanced parameters.

Note

The function varies according to different device models.

Parameters

Multi-Dimension People Counting Version

It stands for the current algorithm version.

Overlay Intelligent Information

Overlay the related intelligent information or POS information in the video.

Algorithm Mode

View and select a mode according to the installation scene.

Data Management

Clear Storage Data

This action clears all counting data stored in the device. Pay attention to this.

11.9.3 Set Face Picture Library

Face picture library is used to store modeled human faces and information.

Steps

1. Go to **VCA → General Settings → Face Picture Library** .
2. Create a face picture library.
   1) Click **Add** to add a face picture library.
   2) Input library name, threshold and remarks.

      Threshold

      Face similarity higher than the set threshold triggers face picture comparison alarm uploading.
   3) Click **OK**.
   4) **Optional:** Modify a face picture library. Select the desired library and click **Modify** and change related parameters.
   5) **Optional:** Delete a library. Select the desired library and click **Delete**.
3. Add face pictures to the library.

   Note

   The picture format should be JPG or JPEG, and the size no larger than 300 KB per file.

   Add one face picture

   Click **Add** and upload the face picture with detailed face information.

   Import face pictures in batch

   Click **Import** and select picture path. You can select and import multiple face pictures as required.

   Note

   When you import face pictures in batch, the picture name is saved as the face name. For other face information, you should modify one by one manually.
4. **Optional:** Modify face information.
   1) Select a face picture library.

2) Select the target face picture. You can use the search function to locate the picture by inputting search conditions, and click **Search**.
3) Click **Modify**.
4) Edit detailed information.

Note

Face picture is not allowed to change.

5) Click **OK**.

5. Click **Batch Modeling** to create models for each face picture in library.

Note

Modeling process builds up face model for each selected face picture. Face model is required for face picture comparison to take effect.

6. **Optional:** Repeat to create more face picture libraries.

11.9.4 Set Face Picture Comparison Alarm

The function compares captured pictures with face pictures in library and outputs comparison result. Comparison result can trigger certain actions when arming schedule and linkage method are set.

Before You Start

Go to **VCA → Select Application** , select **Multi-Dimension People Counting** and click **Next** to enable the function.
You should first create a face picture library and add face pictures. Go to **VCA → General Settings → Face Picture Library** to configure and manage the face pictures in library.

Steps

1. Go to **VCA → Set Application → Multi-Dimension People Counting → Face Picture Comparison Alarm** .
2. Check **Background Upload** if you need to attach captured pictures to alarm information. Comparing to target picture, background picture is the scene image which offers extra environmental information. You can set the **Background Picture Resolution**.
3. Select a face picture library.
4. Set arming schedule of the related face picture library.
   1) Click ⊕ .
   2) Click **Draw**, and drag the time bar to draw desired valid time.

Note

- Each cell represents 30 minutes.
- Move the mouse over the drawn time period to see specific time periods and fine-tune the start time and end time.
- Up to 8 periods can be configured for one day.

3) Click **Erase**, and drag the time bar to clear selected valid time.

4) Click **OK** to save the settings.

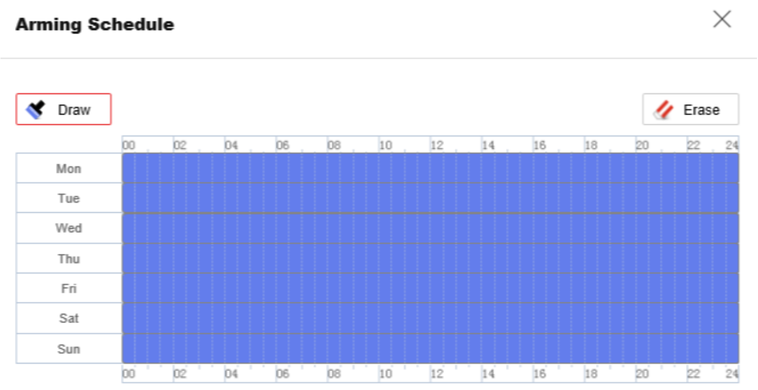


Figure 11-32 Set Arming Schedule

5. Set linkage method of the related face picture library. Click 🔗 to set linkage method and save the settings. For detailed settings, refer to ***Linkage Method Settings*** .
6. Click **Save**.
7. **Optional:** Repeat the above steps to configure the face picture comparison for the other face picture library.

What to do next

Go to **Application Display** to view detailed data analysis. For detailed settings, refer to ***View Face Picture Comparison Result*** .

11.9.5 View Face Picture Comparison Result

Steps

1. Go to **Application Display → Face Picture Comparison Result** .
2. Set search condition and click **Search**.

Result

Matched results are shown in the right area.

11.9.6 View People Counting Statistics

You can view the people counting data stored in the device through the table, bar chart and line chart.

Steps

1. Go to **Application Display → People Counting** .
2. Set **Report Type**, **Statistics Type** and **Start Time**.

3. Click **Search**.

   You can select **Line Chart**, **Bar Chart** and **Table** to view the data, and you can export the people counting data through Excel.

11.10 AI Open Platform

AI Open Platform is to generate a model library based on the training material provided by the user, then load the model library into the device and allow user to configure tasks and rules. When a target in the scene is detected to trigger the rules, the device can take linkage actions, which can realize personalized smart applications.

Note

- The function is only supported by certain device models.
- For certain device models, you need to enable **AI Open Platform** on **VCA** page first.

11.10.1 Set AI Open Platform

Steps

1. Go to **VCA → Set Application → AI Open Platform** .

   Note

   - Specific smart functions are supported for configuration via the AI Open Platform, such as hard hat detection.
   - After selecting a specific function, the device will load the model package of the corresponding function.
   - The function varies according to different device models, please refer to the actual device.

   - For **Hard Hat Detection**, it detects targets in the set detection area who do not wear the hard hat and triggers an alarm.
2. **Optional:** Add a model into **Model Library**. Select the **Model Library** and related **Label File** from the local path, then set the **Model Name**. The model types are as follows.

   Detection Model

   Detects a specific target in the live view and provides the detection result and coordinate position of the target.

   Classification Model

   Classifies pictures or targets with attributes.

   Mixed Model

   Detects targets in the live view and classifies them.

Note

Max. Number of Model Packages refers to the maximum number of model packages that the device supports.

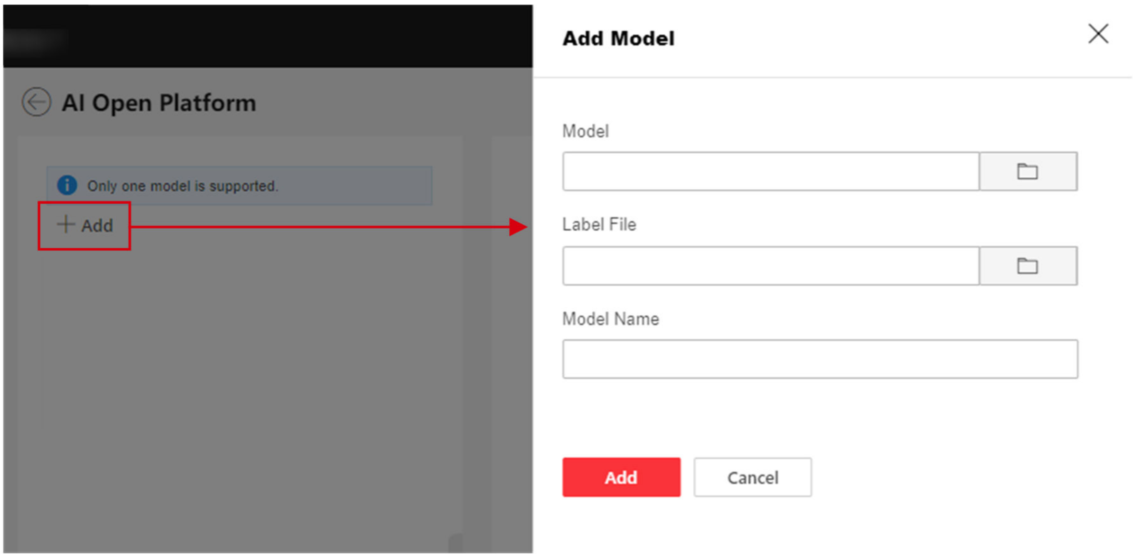
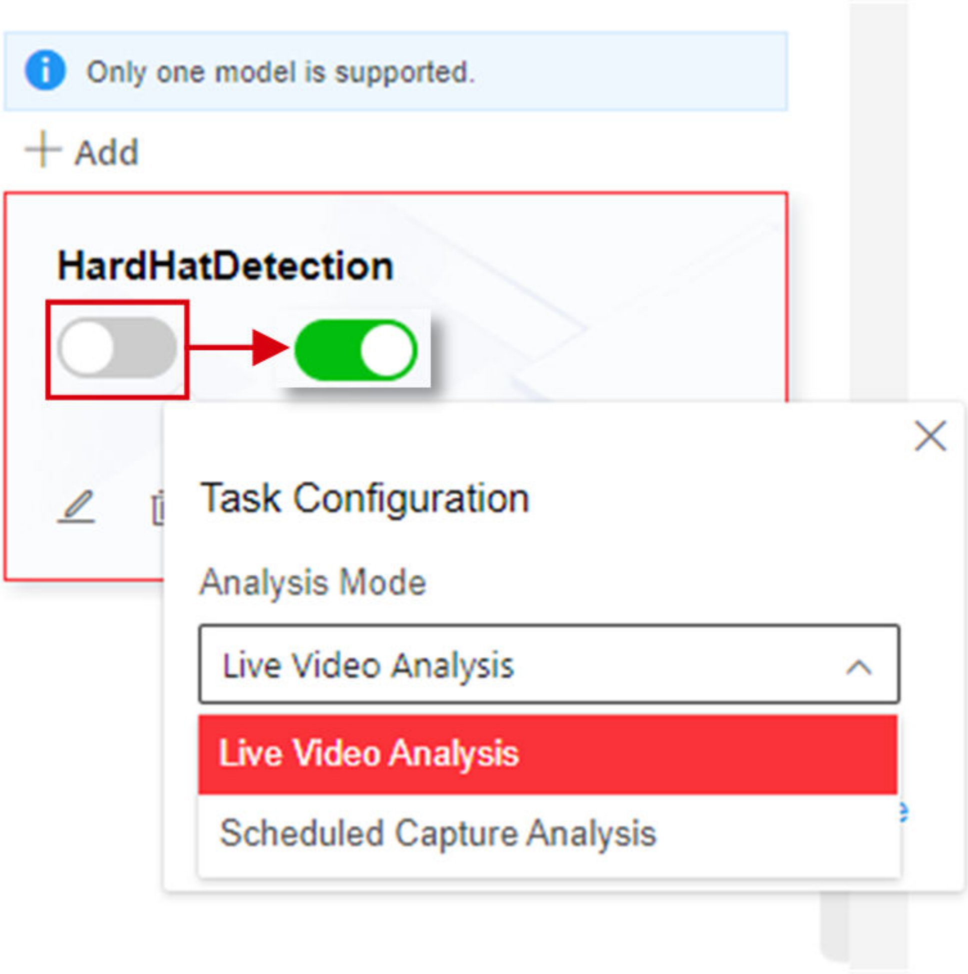


Figure 11-33 Add Model

3. Go to engine list to bind and set if the platform supports multiple engines.
4. Select a model and enable it.



Only one model is supported.

+ Add

HardHatDetection

Task Configuration

Analysis Mode

Live Video Analysis

Live Video Analysis

Scheduled Capture Analysis

Figure 11-34 Set Task

5. Select an **Analysis Mode**.

Live Video Analysis
The device analyzes the live video to realize target detection and result uploading.

Scheduled Capture Analysis
The device captures based on the set **Auto-Switch Interval** to analyze the captured picture and upload results.

Note

If the mode is enabled and set, you can click the mode to change the current analysis mode.

6. Set rules for the linked channel. Refer to ***Set Rules*** for details.
7. Set the arming schedule and linkage method. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
8. **Optional:** Set advanced parameters. Enable **Overlay Target Frame** and **Rule Overlay** according to your needs.

Overlay Target Frame
Overlay the alarm picture with target frame.

Rule Overlay	Overlay the alarm picture with rule information.

9. Click **Save**.

11.10.2 Set Rules

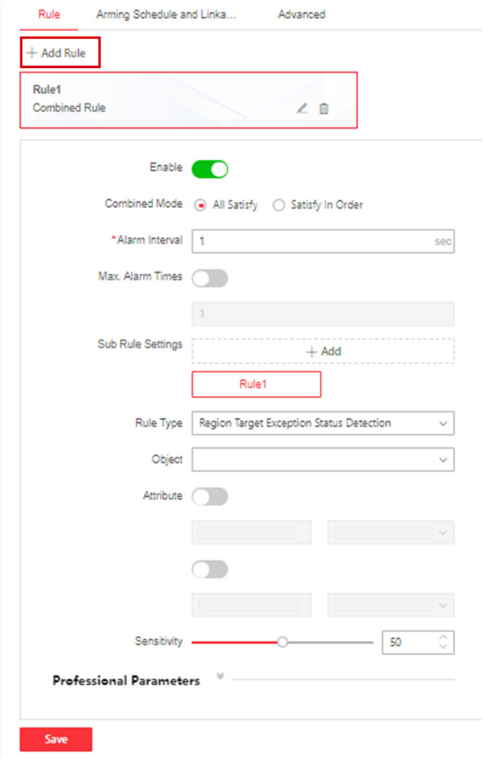
Set rules for the linked channel.

Before You Start

Make sure the related model in **VCA → AI Open Platform** is selected, and the task configuration is finished.

Steps

1. Click **Add Rule**. Select the rule and click ✎ to rename the rule and select the rule type.



Rule | Arming Schedule and Linka... | Advanced

+ Add Rule

Rule1
Combined Rule

Enable: on

Combined Mode: ● All Satisfy ○ Satisfy In Order

*Alarm Interval: 1 sec

Max. Alarm Times: off, 1

Sub Rule Settings: + Add

Rule1

Rule Type: Region Target Exception Status Detection

Object:

Attribute: off

Sensitivity: 50

Professional Parameters

Save

Figure 11-35 Set Rules

Region Target Exception Status Detection

Detects and counts the number of the target in the predefined virtual rule area, and compares it with the setting rule. When satisfying the triggering condition, it will trigger the alarm.

Line Crossing Target Detection

Detects if any targets crossing the predefined virtual rule line and triggers the alarm when detects.

Full Analysis Rule

Detects and analyzes all targets in the predefined virtual rule area.

Line Crossing Target Counting

Detects and counts the number of the target crossing the predefined virtual rule line.

Region Target Number Counting

Detects and counts the number of the target in the predefined virtual rule area.

Combined Rule

Supports **Region Target Exception Status Detection** and **Line Crossing Target Detection** in the predefined virtual rule area. You can set **Combined Mode** as **All Satisfy** or **Satisfy In Order** for the detection order.

Note

Rule types vary according to different model packages, please refer to the actual device.

2. Set the detection rule and draw rule area or line.
   - Draw a rule area: click ⬠ to draw a convex area in the live view window, left click the end-points in the live view window to define the boundary of the set rule area, and right click to finish drawing.
   - Draw a rule line: click ⁄ and a line with an arrow appears in the live video. Drag the line to the location in the live view window as desired.
3. Set rule parameters.

Object

The detection target type of the model.

Attribute

The detection target property of the model.

Duration

The duration of the status. The alarm will be triggered when the set time duration is reached.

Alarm Interval

During the set alarm interval, alarms of the same type only trigger one notification.

Sensitivity

The higher the value of sensitivity is, the easier the alarm can be triggered. If the sensitivity value is too large, the false alarm may be produced easier. Please set it according to the actual situation.

Max. Alarm Times

The maximum number of times an alarm can be triggered in the status that triggers the alarm.

Counting Interval

The time interval for counting.

Algorithm Validity

When the confidence threshold given by the algorithm is greater than or equal to the set validity, an alarm is triggered and uploaded.

Line Crossing

The direction from which the target goes across the line.

Quantity

Check **Quantity** and select the alarm rule from the drop-down box. Set **Threshold** or the range (**Min** and **Max**) according to the alarm rule. When the number of the target satisfies the setting alarm rule, the device will trigger the alarm.

Report Time Interval

It refers to the time interval for uploading the counting results when selecting **Region Target Number Counting**.

Note

Rule parameters vary according to different rules, please refer to the actual device.

4. Click **Save**.

11.11 Road Traffic

Vehicle Detection and Mixed-Traffic Detection are available for the road traffic monitoring. The device captures the passing motor vehicles and non-motor vehicles and uploads the relevant information together with the captured pictures.

Note

- For certain device models, you need to select **Road Traffic** on **VCA** page first.
- The function is only supported by certain device models.

11.11.1 Set Vehicle Detection

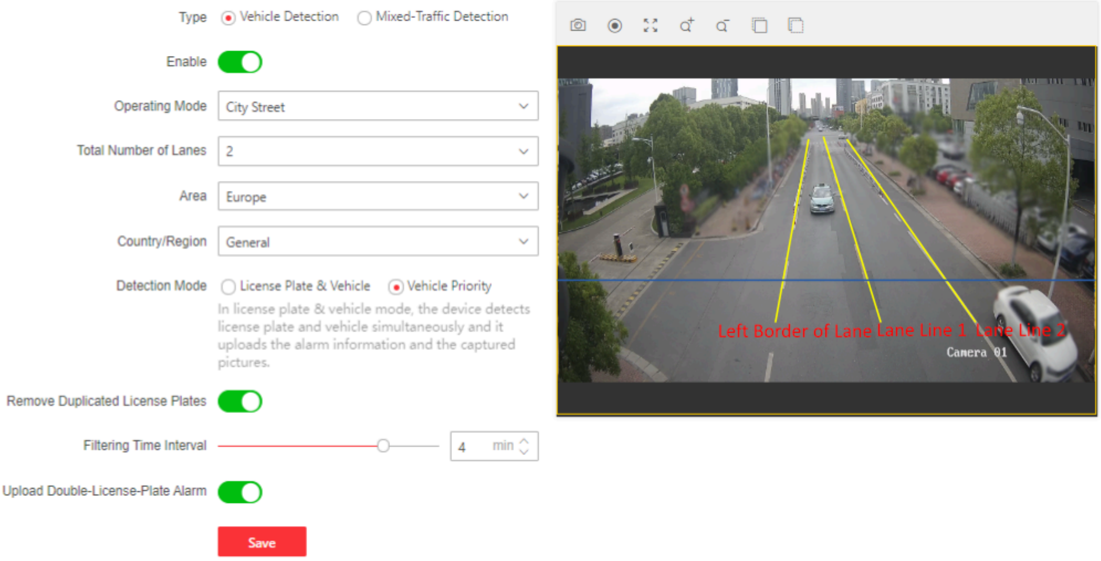
The vehicles that enter the set lane can be detected and the picture of the vehicle and its license plate can be captured and stored. Alarms will be triggered and captures can be uploaded.

Before You Start

- Go to **VCA** and select the application. Select **Road Traffic** and click **Next** to enable the function.
- Make sure the device is installed properly. Refer to the installation recommendation in ***ANPR Camera FAQ*** for details.
- Make sure the image parameters are properly configured. Refer to the recommended image parameters settings in ***ANPR Camera FAQ*** for details.
- Make sure the captured license plate picture is clear enough. Refer to the imaging requirements for license plate capture in ***ANPR Camera FAQ*** for details.

Steps

1. Go to **VCA → Set Application → Road Traffic → Rule** , and select **Vehicle Detection** as detection type.
2. Check **Enable**.



Type ● Vehicle Detection ○ Mixed-Traffic Detection

Enable: on

Operating Mode: City Street

Total Number of Lanes: 2

Area: Europe

Country/Region: General

Detection Mode ○ License Plate & Vehicle ● Vehicle Priority

In license plate & vehicle mode, the device detects license plate and vehicle simultaneously and it uploads the alarm information and the captured pictures.

Remove Duplicated License Plates: on

Filtering Time Interval: 4 min

Upload Double-License-Plate Alarm: on

Figure 11-36 Vehicle Detection

3. Select the operating mode.

Entrance/Exit

The license plate information of the detected vehicle will be uploaded when the vehicle passes the detection area and triggers the detection in the entrance/exit.

City Street

The license plate information of the detected vehicle will be uploaded when the vehicle passes the detection area and triggers the detection in the city street.

Alarm Input

It means the input alarm will trigger a license plate capture and recognition action.

Note

- When **Alarm Input** is selected, the alarm input A<-1 will automatically be assigned to trigger vehicle detection and its alarm type is always NO.
- If the A<-1 alarm input is used to trigger vehicle detection, it cannot be used for other basic events.
- When **Alarm Input** is selected and saved, previously configured linkage method for A<-1 will be canceled.

4. Select the total number of lanes.
5. 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.

The blue detection line is the trigger line of the license plate, which is mainly used in the **Entrance/Exit** scene to improve the capture efficiency. It is recommended to put it in the lower middle of the screen to make sure that the full-size car with the plate can pass it.

6. 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 1 license plate can be captured at one time for each lane.

7. Select **Area** and **Country/Region**.
8. **Optional:** Check to select **License Plate Category**.

   In certain countries/regions, the license plate number includes the license plate category and the license plate main number. This function is used to configure whether the license plate category is included in the license plate number.

   - If the function is not enabled, only the license plate main number is displayed in the license plate number.
   - When this function is enabled, the license plate category is included in the license plate number.

Note

This function is only supported in certain countries/regions.

9. Set the detection mode.

   Vehicle Priority

   The device will detect the vehicle scale first, then catch the plate out to make the analysis. It will get the better accuracy but sometimes it will lose some results in the not-satisfied installation scenario.

   License Plate & Vehicle

   In license plate & vehicle mode, the device detects license plate and vehicle simultaneously and it uploads the alarm information and the captured pictures.

Note

It is recommended to select **Vehicle Priority** mode if there are no issues on installation and supplement light. After the issues of plate recognition are carried out, you can switch the mode to **License Plate & Vehicle** mode.

10. Check **Remove Duplicated License Plates** and set the **Time Interval**. The default time interval is 4 minutes.
11. **Optional:** Set the following parameters according to the installation scene.

    Low-Installation Mode

    If the camera height is not higher than the vehicle headlight height, enable **Low-Installation Mode** to switch the algorithm to accommodate the camera installation scenario.

    Quick Lift

It is used in the entrance and exit with a wide angle view and short detection distance scene. When you enable **Quick Lift**, the camera can identify the license plate quickly, trigger alarm output, and lift the barrier gate.

Note

The functions are only supported by certain device models in certain modes.

12. **Optional:** Check to enable **Upload Motorcycle Alarm**, and the device uploads the both motor vehicle and non-motor vehicle (i.e., motorcycle) alarm information, otherwise it uploads only the motor vehicle alarm information.

Note

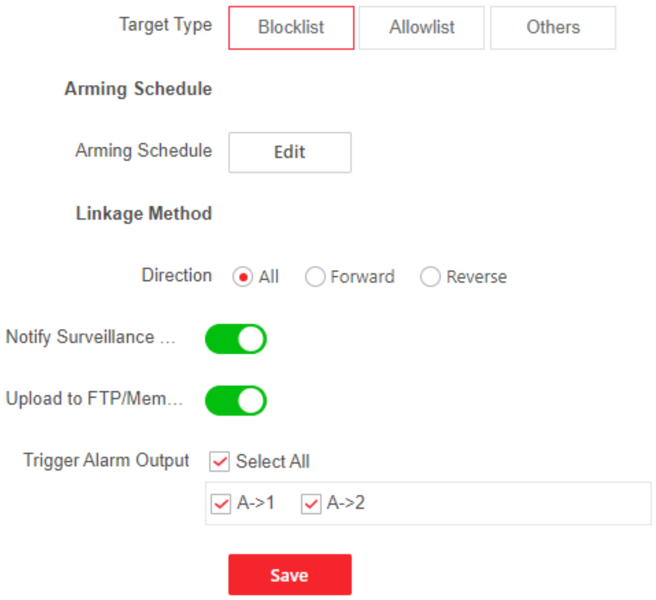
This function is only supported in **Entrance/Exit** mode.

13. **Optional:** Check to enable **Upload Double-License-Plate Alarm**, and the device can detect and recognize two license plates in one vehicle and upload the alarm.
    - When **Upload Double-License-Plate Alarm** is enabled, **Remove Duplicated License Plates** and **Wiegand Linkage** is only available for the primary license plate.
    - When **Upload Double-License-Plate Alarm** is enabled, the blocklist and allowlist is distinguished only for the primary license plate. If the secondary license plate is recognized but not the primary license plate, the blocklist and allowlist are not available, and the linkage will be performed according to the setting of **Other List**.
    - When two license plates in one vehicle are recognized, if the license plate number is set to be overlaid, both license plate numbers can be overlaid, and the license plate picture can be captured and uploaded. License plate number, license plate close-up picture of both primary and secondary license plates can be displayed in **Smart Display**.

Note

This function is not supported in **License Plate & Vehicle** mode.

14. **Optional:** Check to enable **Fuzzy Match License Plate**. In the entrance/exit scene, to improve the convenience, vehicles with a one-bit mismatch between the recognized license plate and the one in the blocklist/allowlist are allowed to pass, and the alarm is uploaded.
15. Click **Save**.
16. Go to **Arming Schedule and Linkage Method**. You can set the arming schedule and linkage method independently for blocklist, allowlist and other list, and you should set them one by one.



Target Type: Blocklist | Allowlist | Others

Arming Schedule

Arming Schedule: Edit

Linkage Method

Direction: ● All ○ Forward ○ Reverse

Notify Surveillance ...: on

Upload to FTP/Mem...: on

Trigger Alarm Output: ☑ Select All

☑ A->1 ☑ A->2

Figure 11-37 Arming Schedule and Linkage Method

1) Click to select the blocklist, allowlist and other list.
2) Set the arming schedule. Refer to ***Set Arming Schedule*** for details.
3) Set the linkage method. Check the checkbox of corresponding linkage method for each rule, and click **Save** to save the settings.

Direction

Only the vehicles moving as the selected direction can trigger the selected linkage methods.

All

All means that the vehicles in all moving directions will be considered. It is highly recommended to choose **All** if there is no special use.

Forward

Forward means that the vehicle moves toward the camera.

Reverse

Reverse means that the vehicle moves away from the camera.

Wiegand Linkage

The device can send reports to the third-party platform via the Wiegand protocol.

Make sure the device supports Wiegand interface and the device is connected by Wiegand interface carefully.

Make sure the Wiegand is enabled and the protocol is properly configured in the system settings. Refer to ***Wiegand*** for details.

Enable **Wiegand Linkage** and select the wiegand interface connected to the external device.

The linkage will be triggered only when the detected vehicle driving direction is the same as the configured direction.

17. Go to **Road Traffic → Overlay & Capture** to set the image parameters and text overlay of the captured pictures. Refer to ***Overlay and Capture*** for details.
18. Import or export the license plate blocklist and allowlist. Refer to ***Import or Export Blocklist & Allowlist*** for details.
19. **Optional:** Set the advanced parameters. Refer to ***Advanced Parameters Configuration*** for details.
20. **Optional:** Set the traffic flow statistics. Refer to ***Traffic Flow Statistics*** for details.

11.11.2 Set Mixed-Traffic Detection Rule

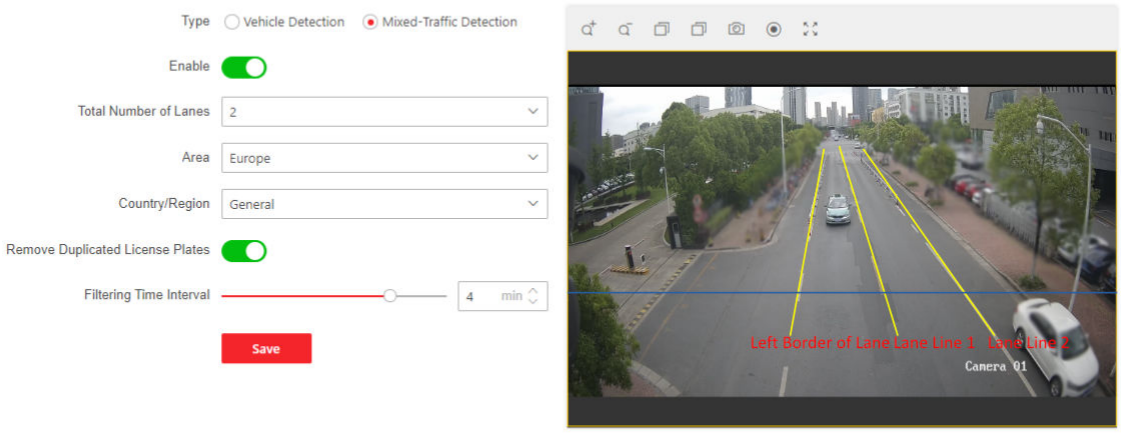
The motor vehicles and non-motor vehicles that enter the set lane can be detected, and the picture of targets can be captured and stored. Alarms will be triggered and captures can be uploaded.

Before You Start

- Go to **VCA** and select the application. Select **Road Traffic** and click **Next** to enable the function.
- Make sure the device is installed properly. Refer to the installation recommendation in ***ANPR Camera FAQ*** for details.
- Make sure the image parameters are properly configured. Refer to the recommended image parameters settings in ***ANPR Camera FAQ*** for details.
- Make sure the captured license plate picture is clear enough. Refer to the imaging requirements for license plate capture in ***ANPR Camera FAQ*** for details.

Steps

1. Go to **VCA → Set Application → Road Traffic → Rule** , and select **Mixed-traffic Detection** as detection type.
2. Check **Enable**.



Type ○ Vehicle Detection ● Mixed-Traffic Detection

Enable: On

Total Number of Lanes: 2

Area: Europe

Country/Region: General

Remove Duplicated License Plates: On

Filtering Time Interval: 4 min

Figure 11-38 Mixed-Traffic Detection

3. Select the total number of lanes.
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.

   The blue detection line is the trigger line of the license plate, which is mainly used in the **Entrance/Exit** scene to improve the capture efficiency. It is recommended to put it in the lower middle of the screen to make sure that the full-size car with the plate can pass it.
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 1 license plate can be captured at one time for each lane.
6. Select **Area** and **Country/Region**.
7. **Optional:** Check to select **License Plate Category**.

   In certain countries/regions, the license plate number includes the license plate category and the license plate main number. This function is used to configure whether the license plate category is included in the license plate number.

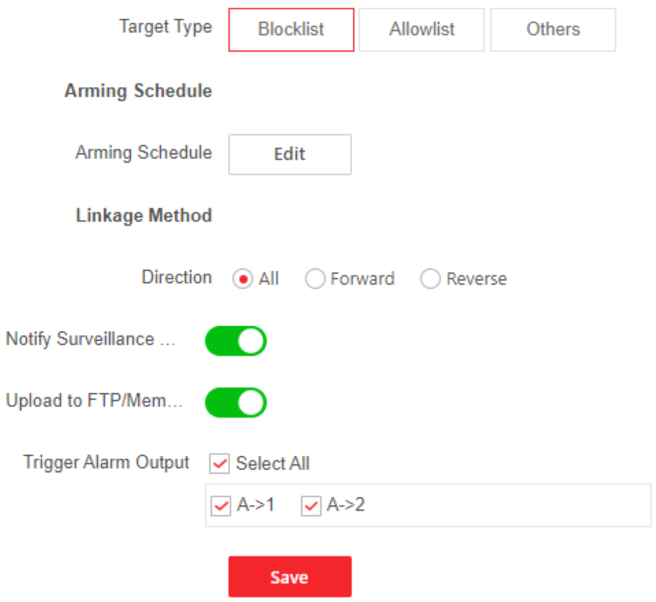
   - If the function is not enabled, only the license plate main number is displayed in the license plate number.
   - When this function is enabled, the license plate category is included in the license plate number.

   Note

   This function is only supported in certain countries/regions.
8. Check **Remove Duplicated License Plates** and set the **Time Interval**. The default time interval is 4 minutes.
9. **Optional:** Check to enable **Upload Double-License-Plate Alarm**, and the device can detect and recognize two license plates in one vehicle and upload the alarm.

- When **Upload Double-License-Plate Alarm** is enabled, **Remove Duplicated License Plates** and **Wiegand Linkage** is only available for the primary license plate.
- When **Upload Double-License-Plate Alarm** is enabled, the blocklist and allowlist is distinguished only for the primary license plate. If the secondary license plate is recognized but not the primary license plate, the blocklist and allowlist are not available, and the linkage will be performed according to the setting of **Other List**.
- When two license plates in one vehicle are recognized, if the license plate number is set to be overlaid, both license plate numbers can be overlaid, and the license plate picture can be captured and uploaded. License plate number, license plate close-up picture of both primary and secondary license plates can be displayed in **Smart Display**.

10. Click **Save**.
11. Go to **Arming Schedule and Linkage Method**. You can set the arming schedule and linkage method independently for blocklist, allowlist and other list, and you should set them one by one.



Target Type: Blocklist | Allowlist | Others

Arming Schedule

Arming Schedule: Edit

Linkage Method

Direction: ● All ○ Forward ○ Reverse

Notify Surveillance ... (on)

Upload to FTP/Mem... (on)

Trigger Alarm Output: ☑ Select All

☑ A->1 ☑ A->2

Save

Figure 11-39 Arming Schedule and Linkage Method

1) Click to select the blocklist, allowlist and other list.

2) Set the arming schedule. Refer to ***Set Arming Schedule*** for details.

3) Set the linkage method. Check the checkbox of corresponding linkage method for each rule, and click **Save** to save the settings.

Direction

Only the vehicles moving as the selected direction can trigger the selected linkage methods.

All

All means that the vehicles in all moving directions will be considered. It is highly recommended to choose **All** if there is no special use.

Forward

Forward means that the vehicle moves toward the camera.

Reverse

Reverse means that the vehicle moves away from the camera.

Wiegand Linkage

The device can send reports to the third-party platform via the Wiegand protocol.

Make sure the device supports Wiegand interface and the device is connected by Wiegand interface carefully.

Make sure the Wiegand is enabled and the protocol is properly configured in the system settings. Refer to ***Wiegand*** for details.

Enable **Wiegand Linkage** and select the wiegand interface connected to the external device.

The linkage will be triggered only when the detected vehicle driving direction is the same as the configured direction.

12. Go to **Road Traffic → Overlay & Capture** to set the image parameters and text overlay of the captured pictures. Refer to ***Overlay and Capture*** for details.
13. Import or export the license plate blocklist and allowlist. Refer to ***Import or Export Blocklist & Allowlist*** for details.
14. **Optional:** Set the advanced parameters. Refer to ***Advanced Parameters Configuration*** for details.
15. **Optional:** Set the traffic flow statistics. Refer to ***Traffic Flow Statistics*** for details.

11.11.3 Overlay and Capture

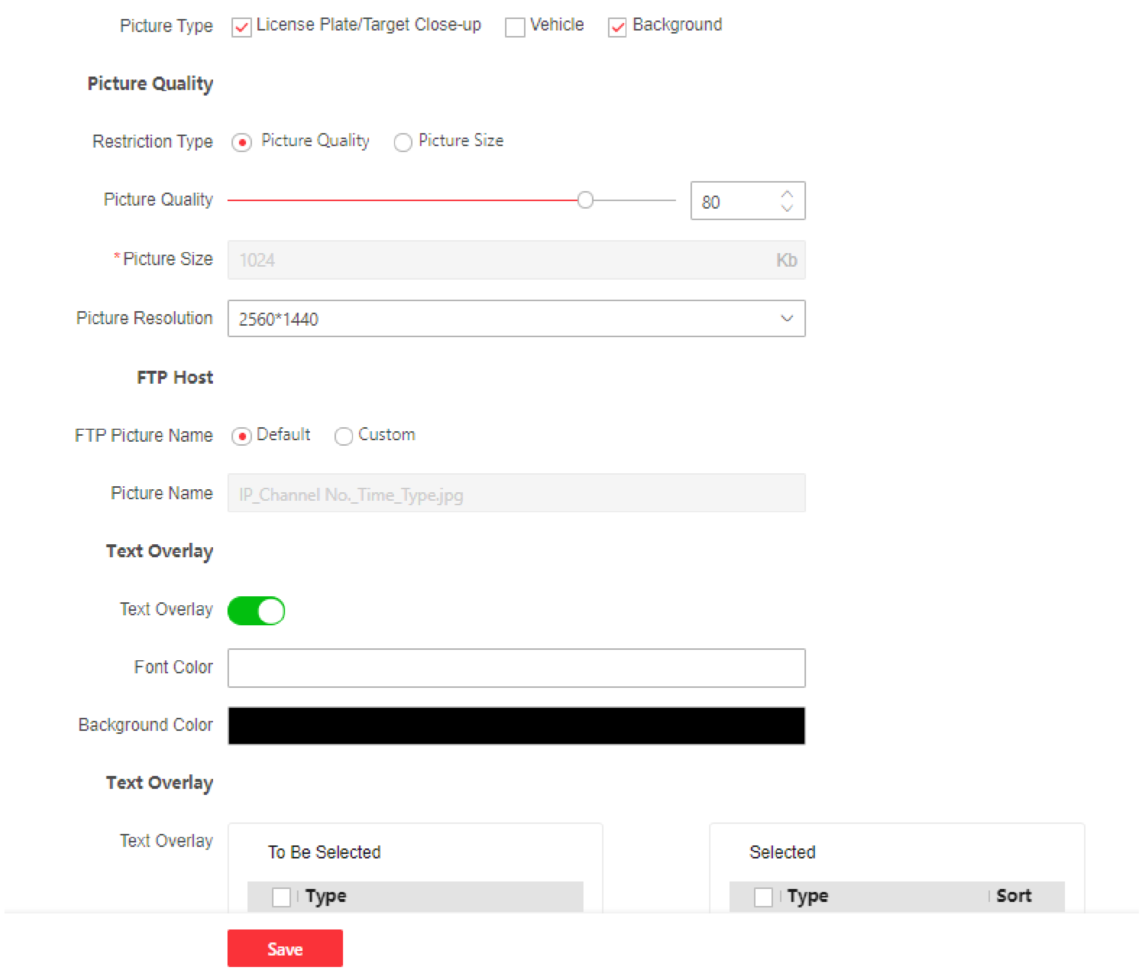
You can set the image parameters of the captured images in vehicle detection and mixed-traffic detection.

Go to **VCA** and select **Road Traffic**.

Go to **VCA → Set Application → Road Traffic → Overlay & Capture** .

Note

The function varies according to different device models.



Picture Type ☑ License Plate/Target Close-up □ Vehicle ☑ Background

Picture Quality

Restriction Type ● Picture Quality ○ Picture Size

Picture Quality 80

*Picture Size 1024 Kb

Picture Resolution 2560*1440

FTP Host

FTP Picture Name ● Default ○ Custom

Picture Name IP_Channel No._Time_Type.jpg

Text Overlay

Text Overlay

Font Color

Background Color

Text Overlay

Text Overlay

To Be Selected

□ Type

Selected

□ Type Sort

Figure 11-40 Overlay & Capture

Picture Quality

The larger the value is, the clearer the picture is, but larger storage space is also required.

Picture Size

The larger the value is, the larger the storage space is needed. And the level of network transmission requirement is also higher.

Picture Resolution

The captured background picture resolution.

Picture Capture Interval

The camera supports continuously trigger the alarm and upload captured picture each interval. Check **Capture Interval** and set the interval.

FTP Picture Name

You can set the naming rule for captured pictures in vehicle detection and mixed-traffic detection in the FTP server.

Select **Default** to use the default rule.

Select **Custom**, select information for the picture name, and click ↑ ↓ to adjust the order of picture name parameters. If **Capture Time** is not selected in custom mode, the captured picture triggered by the same vehicle later will replace the captured picture before due to the same picture name.

Note

For more information about FTP settings, refer to ***Set FTP*** .

Text Overlay

You can overlay camera, device or vehicle information on the captured image and click ↑ ↓ to adjust the order of overlay texts.

Set the font color and background color by selecting the color box, and click the desired color in the pop-up palette or the drop-down box.

11.11.4 Import or Export Blocklist & Allowlist

You can import and export the blocklist and allowlist as desired, and check the list content in this interface.

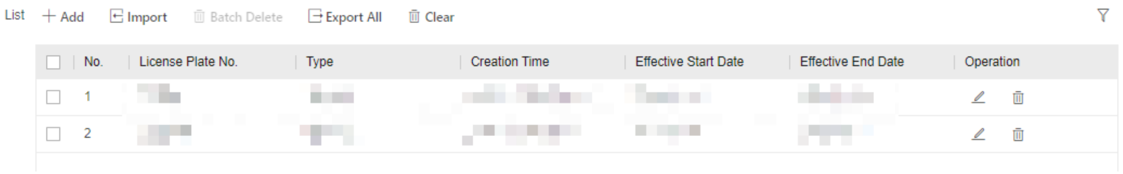
Steps

1. Click **Import** to import the selected file.
2. Click 🗀 to open the PC local directory.
3. Find the blocklist & allowlist file and click to select it. Click **Open** to confirm.

Note

- The file to import should corresponds with the file template that is required by the camera. You are recommended to export an empty blocklist & allowlist file from the camera as the template and fill in the content.
- The file should be in the .xls, .xml or .csv format and the cell format should be Text.

4. Click **Import** to import the selected file.
5. Click **Export All** to export the license plate list.



□	No.	License Plate No.	Type	Creation Time	Effective Start Date	Effective End Date	Operation
□	1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	✎ 🗑
□	2	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	✎ 🗑

Figure 11-41 Import or Export Blocklist & Allowlist

6. **Optional:** Click **Add** to add a license plate and set its related information one by one.

7. **Optional:** Click ▽ to select the filtering type. **All Types**, **Wiegand CardID**, **License Plate No.** and **Type** are selectable. As for **Type**, you can select **Keywords** to define the specific filtering type. Click **Search** to view the results.
8. **Optional:** You can select a plate No. and click 🗑 to delete a plate from the blocklist or allowlist.
9. **Optional:** You can select a plate No. and click ✎ to edit the related information of the license plate from the blocklist or allowlist.

11.11.5 Advanced Parameters Configuration

Go to **VCA** and select the application. Enter the application configuration interface and click **Advanced** to set advanced parameters. Click **Save** after finishing the configuration.

Note

The function varies according to different device models.

Version

It stands for the current algorithm version.

Overlay Intelligent Information

Overlay the related intelligent information or POS information in the video.

11.11.6 Traffic Flow Statistics

You can set the vehicle counting parameters in vehicle detection and mixed-traffic detection.

Go to **VCA** and select **Road Traffic**.

Go to **VCA → Set Application → Road Traffic → Traffic Flow Statistics** . Check **Enable** to enable the function. Set the parameters and click **Save**.

Counting Type

Select the counting vehicle type as required.

Flow Overlay

Check **Flow Overlay** and select **OSD Overlay Content**. Select the overlaid vehicle flow direction type. **None**, **All**, and **Forward/Reverse** are selectable.

The counting data will be displayed on the image, and you adjust the display position of counting data in the live view image.

Note

OSD overlay only counts the number of vehicle on the current day. The data will be cleared automatically when the device restarts or at the daily reset time.

Daily Reset Time

The device clears the data in 00:00 each day by default. You can set the time for the daily reset.

Manual Reset

Clear the current counting data.

Real-Time Upload

Check **Real-Time Upload** and the device uploads the counting data in real-time.

Go to **Application Display → Traffic Flow Statistics** to view related data statistics and export data.

11.12 Parking Management

Parking Management is applicable to the parking lots, which performs parking detection such as parking space status detection by recognizing vehicles and license plates in close view and distant view scenes. This function can be used to guide vehicle parking and reasonably allocate parking spaces according to the parking situation.

Note

- For certain device models, you need to select **Parking Management** on **VCA** page first.
- The function is only supported by certain device models.

11.12.1 Close View Mode

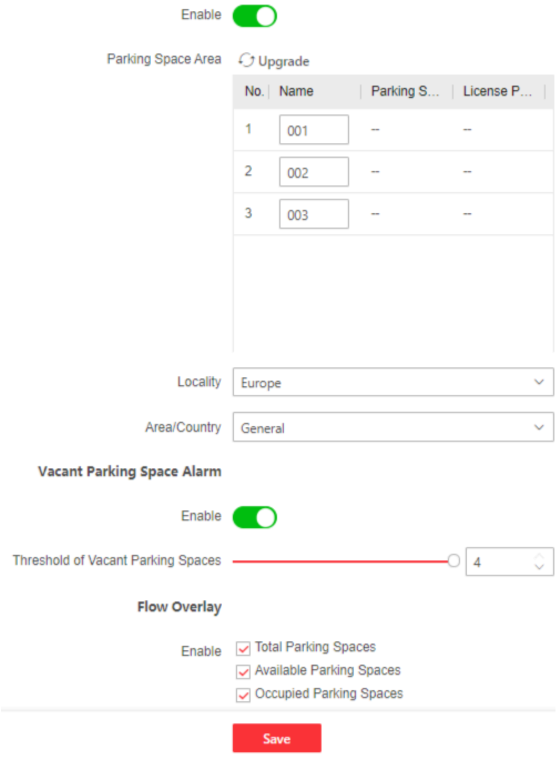
In close view mode, the device can detect at close range and can recognize the vehicle and license plate.

Before You Start

Go to **VCA** and select the application. Select **Parking Management** and click **Next** to enable the function.

Steps

1. Go to **VCA → Set Application → Parking Management** , and select **Close View Mode** as the detection mode. Click **Save** or **Save and Next**.
2. Go to **Rule** interface to set the rule.



Enable

Parking Space Area ⟳ Upgrade

No.	Name	Parking S...	License P...
1	001	--	--
2	002	--	--
3	003	--	--

Locality: Europe

Area/Country: General

Vacant Parking Space Alarm

Enable

Threshold of Vacant Parking Spaces: 4

Flow Overlay

Enable
☑ Total Parking Spaces
☑ Available Parking Spaces
☑ Occupied Parking Spaces

Save

Figure 11-42 Set Rules

3. Check **Enable** to enable the function.
4. Draw a detection area. Click to draw a detection area. Click on the live view to specify the vertexes of the area, and right click to complete drawing. The detection area should be a convex polygon area.
5. Draw the parking space area. Click to draw a parking space area in the detection area. Click on the live view to specify the vertexes of the area, and right click to complete drawing. The areas will be displayed in the parking space area list.

Note

- The parking space area should be in the detection area.
- Parking space area cannot overlap.
- You can select and click 🗑 to delete a certain parking space area in the parking space area list.
- For **Close View Mode**, up to 4 parking space areas can be set. The parking space area should be a convex polygon area.

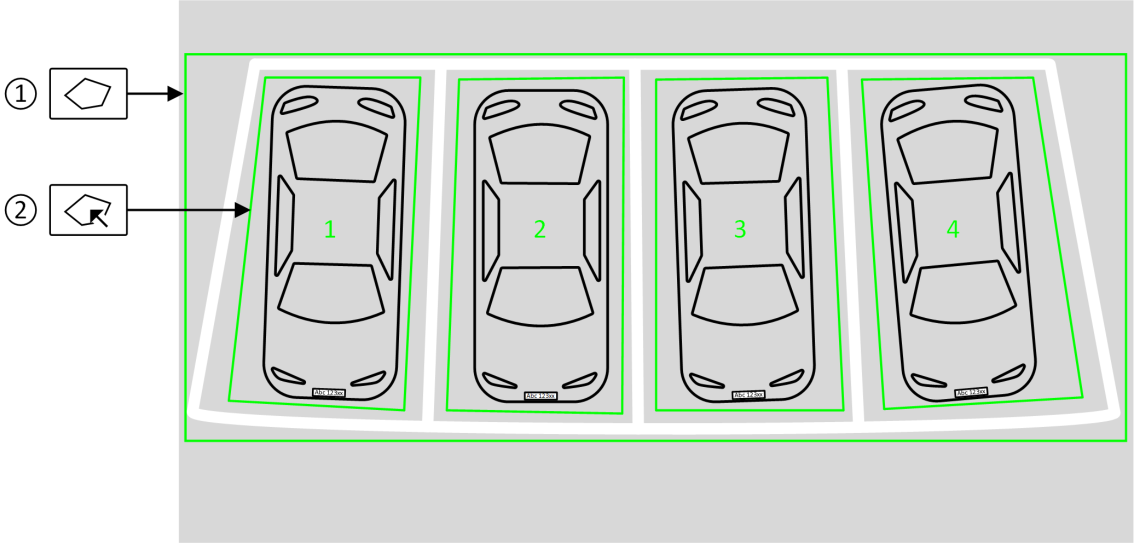


Figure 11-43 Draw Area (Close View Mode)

6. View the parking space area parameters, including the parking space name, parking space status, license plate No. and the parking duration. Click **Refresh** to refresh the parameters.

Note

- The license plate No. is only supported in the close view mode.
- The supported parameters may vary according to different device models.

7. Select **Locality** and **Area/Country**.
8. **Optional:** Check **Enable** to enable **Vacant Parking Space Alarm**.

Threshold of Vacant Parking Spaces

When the number of vacant parking spaces is less than the set threshold value, an alarm will be triggered until the number of vacant parking spaces is greater than the set threshold value.

9. Set the OSD overlay. **Total Parking Spaces**, **Available Parking Spaces** and **Occupied Parking Spaces** are selectable.
10. Click **Save** to save the rule settings.
11. Go to **Arming Schedule and Linkage Method** to set the arming schedule and linkage method. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
12. Set the data uploading parameters.

Note

The function varies according to different models.

Parking Space Status

Check **Scheduled Upload**, and the device will upload the **Parking Space Status** every **Upload Interval**.

Parking Timeout Alarm

When the actual parking time of the vehicle exceeds the set parking threshold, the alarm will be triggered and the device will upload the related alarm information.

Parking Duration

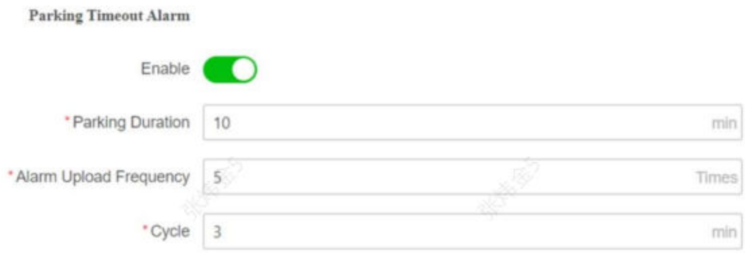
The set parking duration threshold. If the actual parking duration exceeds the set threshold, the alarm will be triggered and the device will upload the related alarm and vehicle information.

Alarm Upload Frequency and Cycle

If the alarm upload frequency is set as ***5*** times and the cycle time is ***3*** minutes, the alarm will be uploaded once every 3 minutes for a total of 5 times when the actual parking duration exceeds the set parking threshold.

Example

If you set the parameters as shown in the following figure, it means that the alarm will be triggered after the vehicle parking duration is over 10 minutes. The alarm will be uploaded every 3 minutes for a total of 5 times and will take a total of 15 minutes.



Parking Timeout Alarm

Enable ●

*Parking Duration 10 min

*Alarm Upload Frequency 5 Times

*Cycle 3 min

13. Set the image parameters and text overlay of the captured pictures. Refer to ***Overlay and Capture*** for details.
14. Import or export the license plate blocklist and allowlist. Refer to ***Import or Export Blocklist & Allowlist*** for details.
15. **Optional:** Set the advanced parameters. Refer to ***Advanced Parameters Configuration*** for details.

11.12.2 Distant View Mode

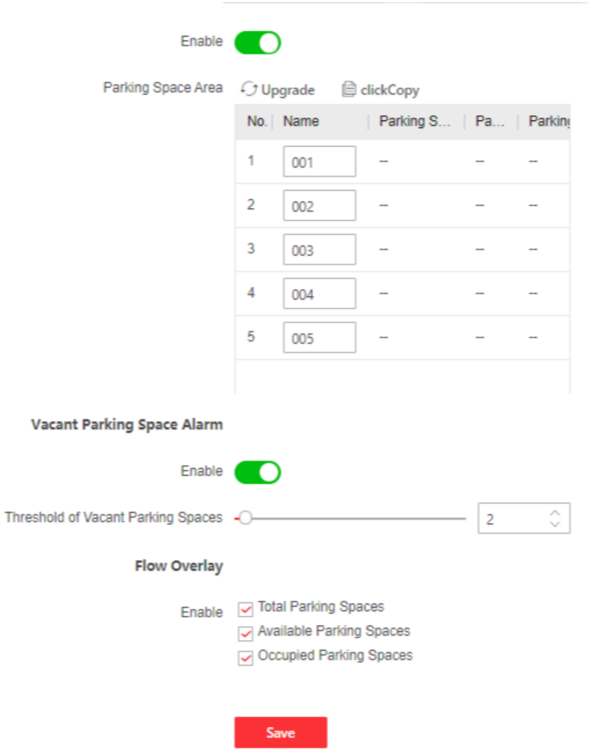
In distant view mode, the device can detect at high altitude from an overlook view and identify the vehicles entering the detection area.

Before You Start

Go to **VCA** and select the application. Select **Parking Management** and click **Next** to enable the function.

Steps

1. Go to **VCA → Set Application → Parking Management** , and select **Distant View Mode** as the detection mode. Click **Save** or **Save and Next**.
2. Go to **Rule** interface to set the rule.



Enable

Parking Space Area Upgrade clickCopy

No.	Name	Parking S...	Pa...	Parkin
1	001	--	--	--
2	002	--	--	--
3	003	--	--	--
4	004	--	--	--
5	005	--	--	--

Vacant Parking Space Alarm

Enable

Threshold of Vacant Parking Spaces 2

Flow Overlay

Enable ☑ Total Parking Spaces
☑ Available Parking Spaces
☑ Occupied Parking Spaces

Figure 11-44 Set Rules

3. Check **Enable** to enable the function.
4. Draw a detection area. Click to draw a detection area. Click on the live view to specify the vertexes of the area, and right click to complete drawing. The detection area should be a convex polygon area.
5. Draw the parking space area. Click to draw a parking space area in the detection area. Click on the live view to specify the vertexes of the area, and right click to complete drawing. The areas will be displayed in the parking space area list.

Note

- The parking space area should be in the detection area.
- Parking space area cannot overlap.
- You can select and click to delete a certain parking space area in the parking space area list.
- For **Distant View Mode**, up to 40 parking space areas can be set. The parking space area should be convex polygon area.

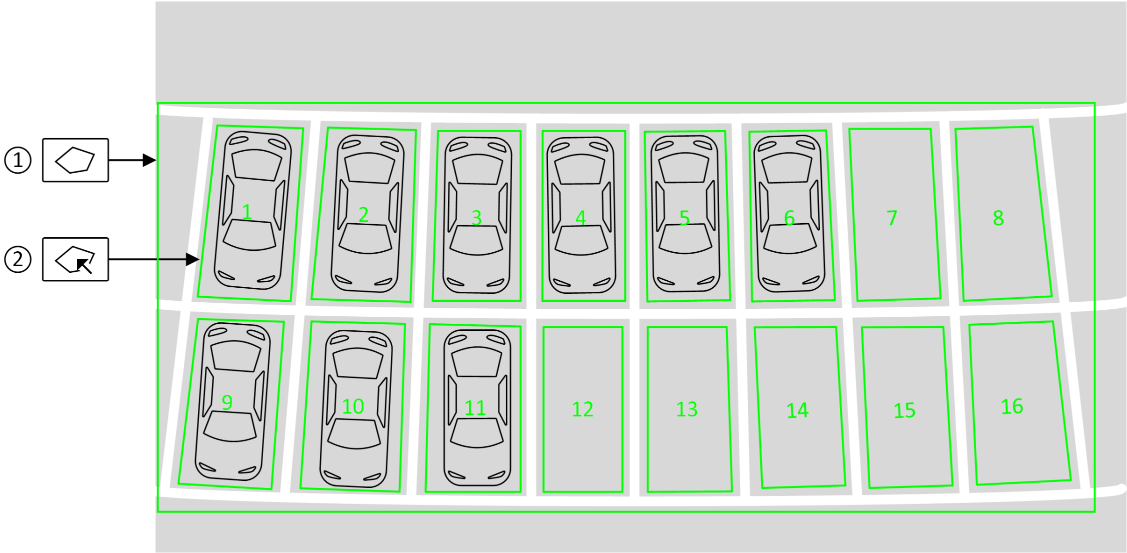


Figure 11-45 Draw Area (Distant View Mode)

6. View the parking space area parameters, including the parking space name, parking space status and the parking duration. Click **Refresh** to refresh the parameters.

Note

The supported parameters may vary according to different device models.

7. **Optional:** Check **Enable** to enable **Vacant Parking Space Alarm**.

   Threshold of Vacant Parking Spaces

   When the number of vacant parking spaces is less than the set threshold value, an alarm will be triggered until the number of vacant parking spaces is greater than the set threshold value.

8. Set the OSD overlay. **Total Parking Spaces**, **Available Parking Spaces** and **Occupied Parking Spaces** are selectable.
9. Click **Save** to save the rule settings.
10. Go to **Arming Schedule and Linkage Method** to set the arming schedule and linkage method. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
11. Set the data uploading parameters.

Note

The function varies according to different models.

Parking Space Status

Check **Scheduled Upload**, and the device will upload the **Parking Space Status** every **Upload Interval**.

Parking Timeout Alarm

When the actual parking time of the vehicle exceeds the set parking threshold, the alarm will be triggered and the device will upload the related alarm information.

Parking Duration

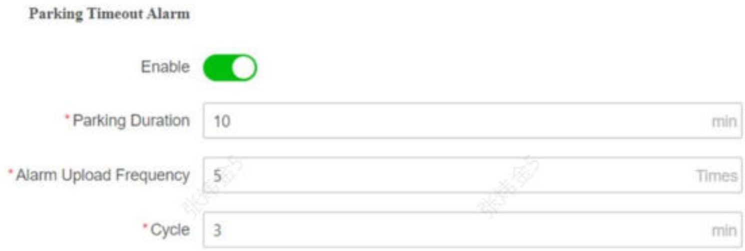
The set parking duration threshold. If the actual parking duration exceeds the set threshold, the alarm will be triggered and the device will upload the related alarm and vehicle information.

Alarm Upload Frequency and Cycle

If the alarm upload frequency is set as ***5*** times and the cycle time is ***3*** minutes, the alarm will be uploaded once every 3 minutes for a total of 5 times when the actual parking duration exceeds the set parking threshold.

Example

If you set the parameters as shown in the following figure, it means that the alarm will be triggered after the vehicle parking duration is over 10 minutes. The alarm will be uploaded every 3 minutes for a total of 5 times and will take a total of 15 minutes.



Parking Timeout Alarm

Enable

*Parking Duration 10 min

*Alarm Upload Frequency 5 Times

*Cycle 3 min

12. Set the image parameters and text overlay of the captured pictures. Refer to ***Overlay and Capture*** for details.
13. **Optional:** Set the advanced parameters. Refer to ***Advanced Parameters Configuration*** for details.

11.12.3 Overlay and Capture

You can set the image parameters of the captured images.

Go to **VCA** and select **Parking Management**.

Go to **VCA → Set Application → Parking Management → Overlay & Capture** .

Note

The function varies according to different device models.

Picture Quality

The larger the value is, the clearer the picture is, but larger storage space is also required.

Picture Size

The larger the value is, the larger the storage space is needed. And the level of network transmission requirement is also higher.

Picture Resolution

The captured background picture resolution.

FTP Picture Name

You can set the naming rule for captured pictures in vehicle detection and mixed-traffic detection in the FTP server.

Select **Default** to use the default rule.

Select **Custom**, select information for the picture name, and click ↑ ↓ to adjust the order of picture name parameters. If **Capture Time** is not selected in custom mode, the captured picture triggered by the same vehicle later will replace the captured picture before due to the same picture name.

Note

For more information about FTP settings, refer to ***Set FTP*** .

Text Overlay

You can overlay camera, device or vehicle information on the captured image and click ↑ ↓ to adjust the order of overlay texts.

Set the font color and background color by selecting the color box, and click the desired color in the pop-up palette or the drop-down box.

11.12.4 Import or Export Blocklist & Allowlist

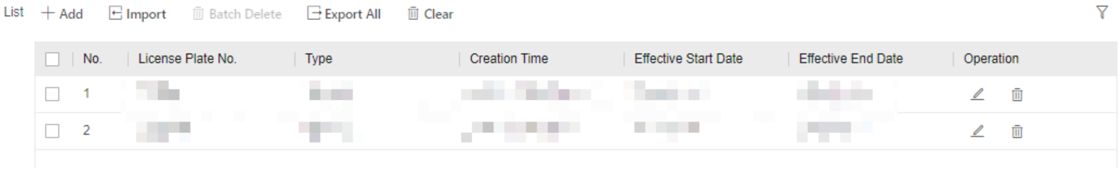
You can import and export the blocklist and allowlist as desired, and check the list content in this interface.

Steps

1. Click **Import** to import the selected file.
2. Click 📁 to open the PC local directory.
3. Find the blocklist & allowlist file and click to select it. Click **Open** to confirm.

   Note

   - The file to import should corresponds with the file template that is required by the camera. You are recommended to export an empty blocklist & allowlist file from the camera as the template and fill in the content.
   - The file should be in the .xls, .xml or .csv format and the cell format should be Text.
4. Click **Import** to import the selected file.
5. Click **Export All** to export the license plate list.



List + Add Import Batch Delete Export All Clear

□	No.	License Plate No.	Type	Creation Time	Effective Start Date	Effective End Date	Operation
□	1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	✎ 🗑
□	2	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	✎ 🗑

Figure 11-46 Import or Export Blocklist & Allowlist

6. **Optional:** Click **Add** to add a license plate and set its related information one by one.
7. **Optional:** Click ▽ to select the filtering type. **All Types**, **Wiegand CardID**, **License Plate No.** and **Type** are selectable. As for **Type**, you can select **Keywords** to define the specific filtering type. Click **Search** to view the results.
8. **Optional:** You can select a plate No. and click 🗑 to delete a plate from the blocklist or allowlist.
9. **Optional:** You can select a plate No. and click ✎ to edit the related information of the license plate from the blocklist or allowlist.

11.12.5 Advanced Parameters Configuration

Go to **VCA** and select the application. Enter the application configuration interface and click **Advanced** to set advanced parameters. Click **Save** after finishing the configuration.

Note

The function varies according to different device models.

Version

It stands for the current algorithm version.

Overlay Intelligent Information

Overlay the related intelligent information or POS information in the video.

11.13 Tunnel Event Detection

Set the basic information for the camera, rule and arming schedule for the function.

Note

- For certain device models, you need to select **Tunnel Event Detection** on **VCA** page first.
- The function is only supported by certain device models.

11.13.1 Basic Settings

You can set the basic information, listening server, and ANR.

Go to **VCA → Set Application → Tunnel Event Detection → Basic Configuration** to complete the settings.

Basic Information

Application Scene

Select the type of road that the device is applied to, and the detection algorithm adapts accordingly.

Country/Region

Select the country or region where the device is used, and the detection algorithm adapts accordingly.

Listening Server

If the device uploads alarms in listening mode via our company's SDK, you should set the IP address and port for the listening server.

ANR

When the network is disconnected, data is temporarily saved on the memory card. When the network connection is resumed, the device automatically uploads the saved data to the arming host, in which case, the arming host IP address is required.

Note

A memory card should be installed in the device. Memory card settings should be completed. See ***Memory Card*** for instructions.

11.13.2 Set Rules

Set rules for the tunnel event detection.

Before You Start

Go to **VCA** and select the application. Select **Tunnel Event Detection** and click **Next** to enable the function.

Steps

1. Go to **VCA → Set Application → Tunnel Event Detection → Panoramic Rule Settings**.
2. Add lanes or polygon areas to the actual situation. Select the area type and click **Add Area**. Refer to ***Set Polygon Area*** and ***Set Lane Area*** for details.
3. Select and set the event. Refer to ***Traffic Event Detection*** for details.
   1) Click **Add Event** to add an event. You can select the event to be detected and set the rule.
   2) Select arming type and check desired arming lane or arming polygon to enable arming.
4. Click **Save**.

Set Polygon Area

A polygon area is where you want to set the detection rules. Draw the area according to the actual situation.

Steps

1. Go to **VCA → Set Application → Tunnel Event Detection → Panoramic Rule Settings** and click **Polygon Area**.
2. Click **Add Area**.
3. Click to mark the corner points of the polygon area. Right click to complete drawing.

   Note

   - You can click ⛶ to enlarge the live view window. Press **ESC** on the keyboard to exit.
   - Polygon areas cannot overlap.
   - Click on the area and you can drag the corner points to adjust the area.
4. Select the line type of the left and right side lines according to the actual situation.
5. **Optional:** Repeat the steps above to set multiple polygon areas.

   Note

   When there are multiple polygon areas, you can click on one area and click 🗑 to delete it.
6. Click **Save**.

Set Lane Area

A lane area is where you want to set the detection rules. Mark the lane area according to the actual lanes in the view.

Steps

1. Go to **VCA → Set Application → Tunnel Event Detection → Panoramic Rule Settings** and click **Lane Area**.
2. Click **Add Area**.

   Blue lane lines and a trigger line show on the live view.
3. Drag the lane lines to frame the actual lane on the image.

   Note

   - You can click ⛶ to enlarge the live view window. Press **ESC** on the keyboard to exit.
   - Lane lines cannot overlap.
4. Select the direction of the traffic and line type of the left and right lane lines according to the actual situation.
5. Drag the triggering line to adjust its length and position.

   The triggering line is where the device captures the vehicle license plate pictures in some detections and where traffic data collection is triggered.

6. **Optional:** Repeat the steps above to set multiple lane areas.
7. Click **Save**.

11.13.3 Traffic Event Detection

Traffic event detection includes detection of incidents happens on the road, for example, thrown objects and traffic congestion. The device captures pictures and uploads alarm data.

Set Parking Detection

The device detects parking violations in tunnels and captures pictures.

Before You Start
Set detection areas. See ***Set Polygon Area*** and ***Set Lane Area*** for details.

Steps

1. Go to **VCA → Set Application → Tunnel Event Detection → Panoramic Rule Settings** .
2. Click **Add Event** and select **Parking Detection**.
3. Select **Arming Polygon**.

   Parking detection takes effect in the selected areas.
4. Set the parameters.

   Sensitivity

   With higher sensitivity, the device is more sensitive to detect and recognize targets.

   If you enable **No Alarm When Congestion Occurs in Detection Area**, the congestion threshold changes as the sensitivity changes. The higher the sensitivity, the higher the congestion threshold and the easier it is to trigger the alarm. The lower the sensitivity, the lower the congestion threshold and the easier it is to filter the parking detection.

   No Alarm When Congestion Occurs in Detection Area

   The alarm will not be triggered if the congestion level in the detection area reaches the set congestion threshold.

   Parking Tolerance

   It stands for the threshold for the parking time in the area. If the parking time exceeds the threshold, an alarm is triggered. The larger the value of the threshold is, the longer the alarm triggering time is.
5. Click **Save**.

What to do next
Set the arming schedule and linkage and alarm. See ***Set Arming Schedule*** and ***ITS Linkage and Alarm*** for details.

Set Fallen Object Detection

The device detects fallen objects on the road and captures pictures.

Before You Start
Set detection areas. See ***Set Polygon Area*** and ***Set Lane Area*** for details.

Steps

1. Go to **VCA → Set Application → Tunnel Event Detection → Panoramic Rule Settings** .
2. Click **Add Event** and select **Fallen Object Detection**.
3. Select **Arming Lane** or **Arming Polygon**.

   Fallen object detection takes effect in the selected lanes or areas.
4. Set **Sensitivity**.

   With higher sensitivity, the device is more sensitive to detect and recognize targets.
5. Click **Save**.

What to do next
Set the arming schedule and linkage and alarm. See ***Set Arming Schedule*** and ***ITS Linkage and Alarm*** for details.

Set Pedestrian Detection

The device detects pedestrians and non-motor vehicles in the detection area and captures pictures.

Before You Start
Set detection areas. See ***Set Polygon Area*** and ***Set Lane Area*** for details.

Steps

1. Go to **VCA → Set Application → Tunnel Event Detection → Panoramic Rule Settings** .
2. Click **Add Event** and select **Pedestrian Detection**.
3. Select **Arming Lane** or **Arming Polygon**.

   Pedestrian detection takes effect in the selected lanes or areas.
4. Set **Sensitivity**.

   With higher sensitivity, the device is more sensitive to detect and recognize targets.
5. Set **Duration**.

   When the target stays in the detection area longer than the duration (at night, three times the duration), an alarm is triggered.
6. Set **Filtering Time**.

   Within the set filtering time, the same target will not trigger the alarm repeatedly.
7. Select the target types in **Detection Target**.

   Only selected target types trigger linkage and alarm.
8. Click **Save**.

What to do next
Set the arming schedule and linkage and alarm. See ***Set Arming Schedule*** and ***ITS Linkage and Alarm*** for details.

Set Construction Detection

The device detects ongoing construction in the detection area and captures pictures.

Before You Start
Set detection areas. See ***Set Polygon Area*** and ***Set Lane Area*** for details.

Steps

1. Go to **VCA → Set Application → Tunnel Event Detection → Panoramic Rule Settings** .
2. Click **Add Event** and select **Construction Detection**.
3. Select **Arming Lane** or **Arming Polygon**.

   Construction detection takes effect in the selected lanes or areas.
4. Set **Sensitivity**.

   With higher sensitivity, the device is more sensitive to detect and recognize targets.
5. Set **Duration**.

   When the construction in the detection area lasts longer than the duration, an alarm is triggered.
6. Set **Filtering Time**.

   Within the set filtering time, the construction in the same detection area will not trigger the alarm repeatedly.
7. Click **Save**.

What to do next
Set the arming schedule and linkage and alarm. See ***Set Arming Schedule*** and ***ITS Linkage and Alarm*** for details.

Set Congestion Detection

The device detects traffic congestion in the detection area and captures pictures.

Before You Start
Set detection areas. See ***Set Polygon Area*** and ***Set Lane Area*** for details.

Steps

1. Go to **VCA → Set Application → Tunnel Event Detection → Panoramic Rule Settings** .
2. Click **Add Event** and select **Congestion Detection**.
3. Select **Arming Lane** or **Arming Polygon**.

   Congestion detection takes effect in the selected lanes or areas.
4. Set **Sensitivity**.

With higher sensitivity, the device is more sensitive to detect and recognize targets.

5. Set **Duration**.

   When the congestion in the detection area lasts longer than the duration, an alarm is triggered.

6. Set **Filtering Time**.

   Within the set filtering time, the congestion in the same detection area will not trigger the alarm repeatedly.

7. Click **Save**.

What to do next

Set the arming schedule and linkage and alarm. See ***Set Arming Schedule*** and ***ITS Linkage and Alarm*** for details.

11.13.4 ITS Linkage and Alarm

When traffic events are detected, the device can perform linkage actions, for example, uploading captured pictures and sending alarm messages.

Note

Some linkage actions may not be supported by certain device models.

Upload Pictures

Set the parameters for the device to automatically upload captured pictures to FTP server or other platforms.

See ***Upload by FTP*** to upload captured pictures by FTP.

See ***Upload by SDK*** or ***Set ISUP*** to upload captured pictures to platforms.

Upload by FTP

Upload the data of vehicle detection to an FTP server.

Before You Start

The FTP server is configured.

Steps

1. Go to **VCA → Set Application → Tunnel Event Detection → Advanced Configuration → FTP Host** .
2. Check **Enable**.
3. Select a **Character Encoding Mode**.
4. Enter the **IP Address**, **Port**, **User Name**, and **Password** of the FTP server.
5. Set the picture names and saving paths of detections.
6. Click **Save**.

Upload by SDK

Upload the alarm messages by SDK in listening and arming mode.

Go to **VCA → Set Application → Tunnel Event Detection → Basic Configuration** to set **Listening Server** and **ANR**. See ***Basic Settings*** for details.

11.13.5 Advanced Settings

You can set the advanced settings according to your need to get better vehicle arming effect.

Advanced Parameters

Go to **VCA → Set Application → Tunnel Event Detection → Advanced Configuration → Advanced** to set the following parameters.

Text Overlay on Video

Target Information

When target information is enabled, the target is highlighted with a frame in the video.

Rule Information

When rule information is enabled, the rule frames (for example, detection areas) show in the video.

Other Parameters

Tuning Mode

The tuning mode is for professional technicians. It is not recommended to other users as it may affect the live view image.

Uploading Picture Settings

Go to **VCA → Set Application → Tunnel Event Detection → Advanced Configuration → Picture** to set the parameters of alarm pictures.

Picture Quality

Pictures with higher resolution and better quality have more details and larger file size.

Enable OSD Overlay (Flow Overlay)

The device OSD is overlaid on alarm pictures.

Text Overlay on Single Alarm Picture

Check and set the text overlaid information on the single alarm picture.

Display Target Info. on Alarm Picture

Check to display target information on alarm pictures.

Display Rule Info. on Alarm Picture

Check to display rule information on alarm pictures.

11.14 Schedule Switch Application

Set the corresponding applications in multiple time periods.

Before You Start

Go to **VCA** , select the application and set the related detection rules and parameters.

Steps

1. Go to **VCA → Select Application** . For the device supporting HEOP, go to **VCA** for the setting. Click **Scheduled-Switch** to set the schedule for switching the application.
2. Check **Scheduled-Switch** to enable the function.
3. Click to select an application to set the schedule.
4. Click **Draw**, and drag the time bar to draw desired valid time.

Note

- Each cell represents 30 minutes.
- Move the mouse over the drawn time period to see specific time periods and fine-tune the start time and end time.
- Up to 8 periods can be configured for one day.

5. Click **Erase**, and drag the time bar to clear selected valid time.
6. Click **OK** to save the settings.

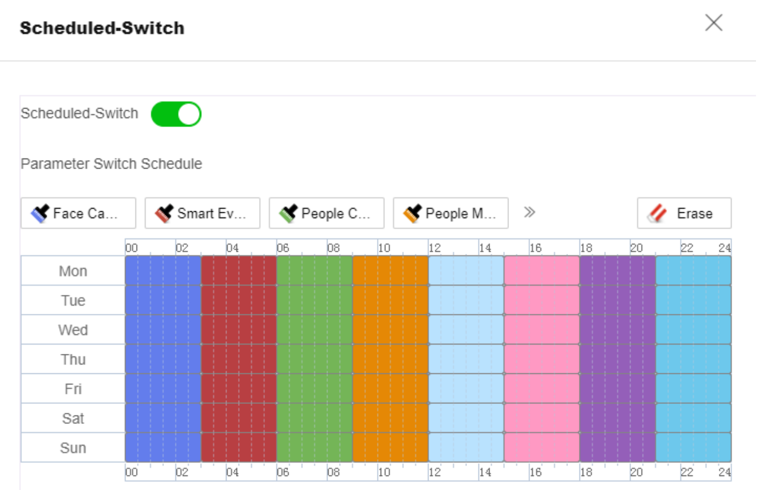


Figure 11-47 Set Application Scheduled-Switch

Result

The device will execute the corresponding application in the set time period.

11.15 Search and Export Data Aware Information

The data aware function is used to search and export the data of the restart, arming and capture alarm statistics.

Before You Start
Log in to the device via admin user account.

Steps

1. Go to **Application Display → Data Aware** .
2. Select the search condition.

Statistics Type	Options
Restart Records	Type of restarting, start time and end time.
Arming	Arming type, start time and end time.
Capture Alarm Statistics	Report type, alarm target, protocol, arming IP address and start time.
Alarm Quality Statistics	Report type, alarm target and start time.

3. Click **Search**.

   The data information that match the conditions will be displayed.
4. **Optional:** Click **Export** to save the data information to the local device.

11.16 Search and View Power Consumption Statistics

Before You Start
Log in to the device with an administrator account or an operator account with remote configuration permission.

Steps

1. Go to **Application Display → Power Statistics** .
2. Set the search condition. Select **Statistics Type**, **Report Type** and **Time**.
3. Click **Search**.

Result

When you select **Power Consumption** as **Statistics Type**, the power consumption information that match the conditions will be displayed.

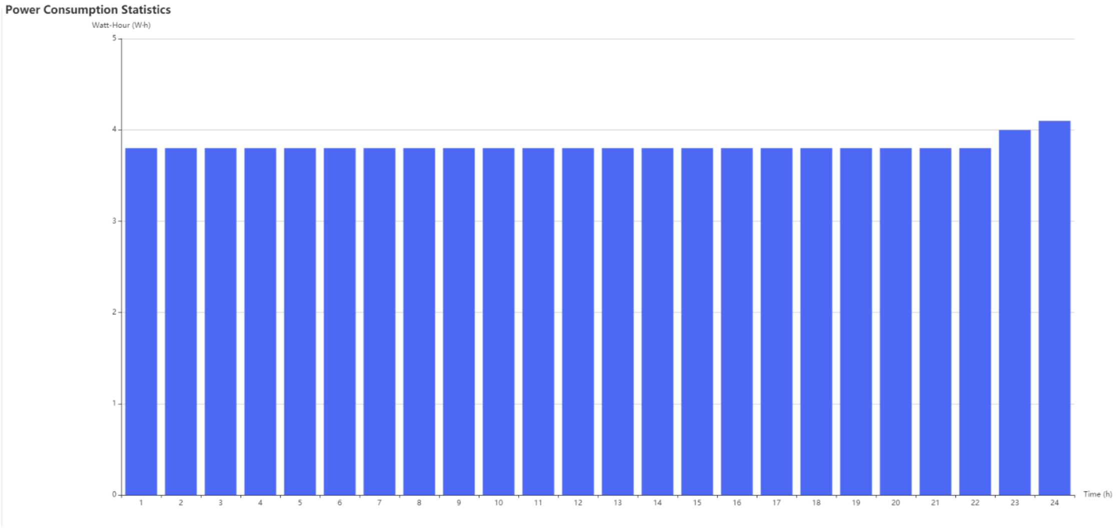


Figure 11-48 Power Consumption Statistics

Chapter 12 Smart Display

This function displays real time pictures captured by smart functions and analyzes the target in real time.

Go to **Application Display → Display Alarm** to view the real-time images. Click ⌂ to go back to **Application Display**.

Note

- To use this function, you should first enable and configure certain smart functions.
- To use this function, your web browser version should be above IE11.0.9600.17843.

Live View Parameter

Icon	Function
📷	Capture a picture.
◉	Start or stop recording.
🔇	Mute.
🔊 🔉 ━━○── 50	Adjust the volume of live view. Move the slider to right to turn up the volume and left to turn down the volume. Move to the left end to mute the live view.

Download Display Pictures

Click ⤓ and the device stores captured pictures to the browser cache. Hover the pointer over the icon to see the number of pictures in the cache. Click ⤓ again to download the pictures in a package.

Note

The browser cache has a limited size. The recommended number of pictures to download is no more than 200.

Layout

Click ⚙ and choose **Layout**. Check the display content you need to add it to the smart display page. When real-time analyze is selected, you can choose the contents you want to display.

Detect Feature

Click ⚙ and choose **Detect Feature**. Check the corresponding checkbox to display the features of the detection target.

Chapter 13 EPTZ

EPTZ (Electronic PTZ) is a high-resolution function that digitally zooms and pans into portions of the image, with no physical camera movement. If you want to use the EPTZ function, make sure your device supports the **Third Stream**. Third stream and EPTZ should be both enabled simultaneously.

Note

The function is only supported by certain device models.

13.1 Patrol

Steps

1. Go to **Configuration → EPTZ** .
2. Check **Enable**.
3. The default **Stream Type** is **Third Stream** and cannot be configured.
4. Select **Patrol** in **Application Mode**.
5. Click **Save**.

What to do next

For the detailed information about the patrol settings, see the PTZ operations on live view page.

13.2 Auto-Tracking

Steps

1. Go to **Configuration → EPTZ** .
2. Check **Enable**.
3. The default **Stream Type** is **Third Stream** and cannot be configured.
4. Select **Auto-tracking** in **Application Mode**.
5. Click to start drawing. Click on the live view video to specify the four vertexes of the detection area, and right click to complete drawing.
6. Set rules.

   Detection Target

   Human and vehicle are available. If the detection target is not selected, all the detected targets will be tracked, including the human and vehicle.

   Note

   Only certain camera models support this function.

   Sensitivity

It stands for the percentage of the body part of an acceptable target that is tracked. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that enters the pre-defined area. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the target can be tracked.

7. Click **Save**.

Appendix A. FAQ

Scan the following QR code to find the frequently asked questions of the device.

Note that some frequently asked questions only apply to certain models.

Table A-1 FAQ QR Code

QR Code Type	QR Code Image
Network Camera General FAQ	
ANPR Camera FAQ	

See Far, Go Further

Smart Monitoring Camera

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision’s trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ **Danger**	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
⚠ **Caution**	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
ℹ **Note**	Provides additional information to emphasize or supplement important points of the main text.

Contents

Chapter 1 Activation and Login

1.1 Activation

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. The device supports multiple activation methods, such as activation via SADP software, web browser, and iVMS-4200 Client.

Note

Refer to the user manual of iVMS-4200 Client for the activation via client software.

1.1.1 Default Information

The device default information is shown as below.

- Default IP address: 192.168.1.64
- Default user name: admin

1.1.2 Activate via SADP

SADP is a tool to detect, activate, and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website (***http://www.hikvision.com/***), and install it according to the prompts.
- The device and the computer that runs the SADP tool should belong to the same network segment.

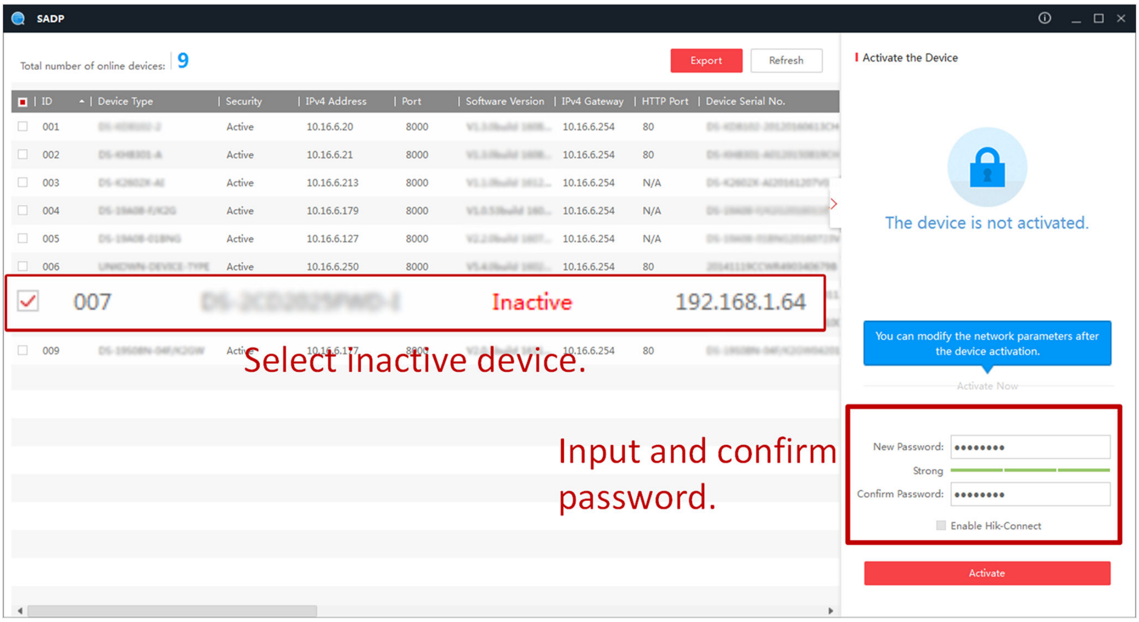
The following steps show how to activate one device and modify its IP address. For batch activation and IP address modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Enter a new password (admin password) and confirm the password.

   Caution

   STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
4. Click **Activate** to start activation.



Total number of online devices: 9

□	ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
□	001	[illegible]	Active	10.16.6.20	8000	[illegible]	10.16.6.254	80	[illegible]
□	002	DS-KH8301-A	Active	10.16.6.21	8000	[illegible]	10.16.6.254	80	[illegible]
□	003	DS-K2602X-AI	Active	10.16.6.213	8000	[illegible]	10.16.6.254	N/A	[illegible]
□	004	DS-19A08-F/K2G	Active	10.16.6.179	8000	[illegible]	10.16.6.254	N/A	[illegible]
□	005	DS-19A08-01BNG	Active	10.16.6.127	8000	[illegible]	10.16.6.254	N/A	[illegible]
□	006	UNKOWN-DEVICE-TYPE	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑	007	[illegible]	Inactive	192.168.1.64					
□	009	DS-19508N-04F/K2GW	Active	10.16.6.177	8000	[illegible]	10.16.6.254	80	[illegible]

Select inactive device.

Input and confirm password.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

Activate Now

New Password: ••••••••

Strong

Confirm Password: ••••••••

□ Enable Hik-Connect

Activate

Figure 1-1 Activate via SADP

Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same network segment as your computer by either modifying the IP address manually or checking **Enable DHCP** (Dynamic Host Configuration Protocol).
   3) Enter the admin password and click **Modify** to activate your IP address modification.

1.1.3 Activate via Web Browser

Use web browser to activate the device. For the device with the DHCP enabled by default, use SADP software or client software to activate the device.

Before You Start

Ensure the device and the computer are in the LAN with the same network segment.

Steps

1. Change the IP address of your computer to the same network segment as the device.
2. Open the web browser, and enter the default IP address of the device to enter the activation interface.
3. Create and confirm the admin password.

⚠ **Caution**

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click **OK** to complete activation.
5. Go to the network settings interface to modify IP address of the device.

1.2 Login

You can log in to the device via web browser for further operations such as live view and local configuration.

Before You Start

Connect the device to the network directly, or via a switch or a router.

Steps

1. Open the web browser, and enter the IP address of the device to enter the login interface.
2. **Optional:** Select the language.
3. Enter **User Name** and **Password**.
4. Click **Login**.

ℹ **Note**

- If live view failed, click 🧩 on the upper right corner of the interface to download the plug-in and install it.
- Close the web browser to install the plug-in, or the installation may fail. If you still cannot realize live view after installing the plug-in, try to uninstall the plug-in and reinstall.

5. Reopen the web browser after the installation of the plug-in and repeat steps 1 to 4 to login.
6. **Optional:** Click ⇥ on the upper right corner of the interface to log out of the device.

1.3 Download Plug-in

No plug-in mode is enabled by default. In no plug-in mode, the resolution of the live view image will be decreased and the live view may not be smooth. You can download and install plug-in to improve the live view condition.

In no-plug in mode, "No Plug-in Mode" prompt will appear on the upper right corner of the interface. You can click 🧩 to download the plug-in. Close the browser to install the plug-in to the computer. Then access to the IP address of the device again, and the "No Plug-in Mode" prompt will disappear from the upper right corner of the interface.

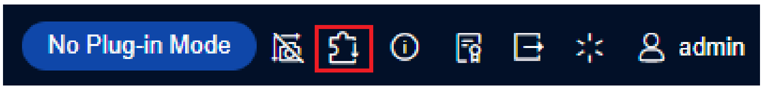


Figure 1-2 Download Plug-in

Chapter 2 Quick Configuration

Click **Quick Configuration** and follow the instructions to complete the basis configuration of the device.

Table 2-1 Quick Configuration

Configuration Sequence	Details
Application Mode	Select **Trigger Mode** and set the corresponding parameters. Refer to ***Application Mode Configuration*** for details.
Basic Parameters	• **Device Information**: Refer to ***View Device Information*** for details. • **Time Settings**: Refer to ***Synchronize Time*** and ***Set DST*** for details. • **Network Parameters**: Refer to ***Set IP Address*** for details.
Supplement Light Parameters	Refer to ***Set Supplement Light Parameters*** for details.
OSD Configuration	• **Text Overlay on Video**: Refer to ***Set OSD*** for details. • **Text Overlay on Picture**: Refer to ***Set Information Overlay*** for details.
Picture Configuration	Refer to ***Set Picture Composition*** for details.
Upload Picture	• **Arm Upload**: Refer to ***Set Arming Host*** for details. • **SDK Listening**: Refer to ***Set SDK Listening*** for details. • **FTP**: Refer to ***Set FTP*** for details. • **ISAPI Listening**: Refer to ***Set ISAPI Listening*** for details. • **ISUP**: Refer to ***Connect to ISUP Platform*** for details. • **OTAP**: Refer to ***Connect to OTAP*** for details. • **Hik-Connect Platform**: Refer to ***Connect to Hik-Connect*** for details. • **Integration Protocol**: Refer to ***Set Integration Protocol*** for details.

Chapter 3 Network Configuration

3.1 Set IP Address

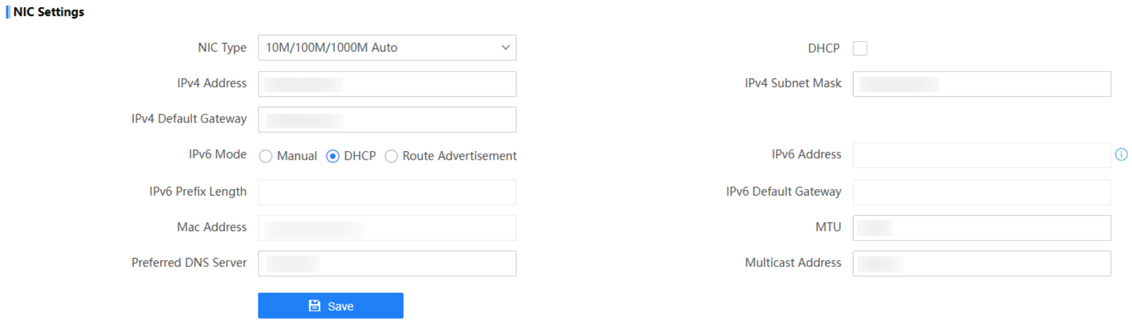
IP address must be properly configured before you operate the device over network. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.

Steps

Note

The supported parameters vary with different models. The actual device prevails.

1. Go to **Configuration → Network → Network Parameters → Network Interface** .



NIC Settings

NIC Type: 10M/100M/1000M Auto

IPv4 Address

IPv4 Default Gateway

IPv6 Mode: ○ Manual ● DHCP ○ Route Advertisement

IPv6 Prefix Length

Mac Address

Preferred DNS Server

DHCP □

IPv4 Subnet Mask

IPv6 Address

IPv6 Default Gateway

MTU

Multicast Address

Figure 3-1 Set IP Address

2. Set network parameters.

NIC Type

Select a NIC (Network Interface Card) type according to your network condition.

IPv4

Two modes are available.

DHCP

The device automatically gets the IP parameters from the network if you check **DHCP**. The device IP address is changed after enabling the function. You can use SADP to get the device IP address.

Note

The network that the device is connected to should support DHCP (Dynamic Host Configuration Protocol).

Manual

You can set the device IP parameters manually. Enter **IPv4 Address**, **IPv4 Subnet Mask**, and **IPv4 Default Gateway**.

IPv6

Three IPv6 modes are available.

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.

Note

Route advertisement mode requires the support from the router that the device is connected to.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Enter **IPv6 Address**, **IPv6 Prefix Length**, and **IPv6 Default Gateway**. Consult the network administrator for required information.

MTU

It stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.

The valid value range of MTU is 1280 to 1500.

Multicast Address

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneously. After setting the IP address of the multicast host, you can send the source data efficiently to multiple receivers.

DNS

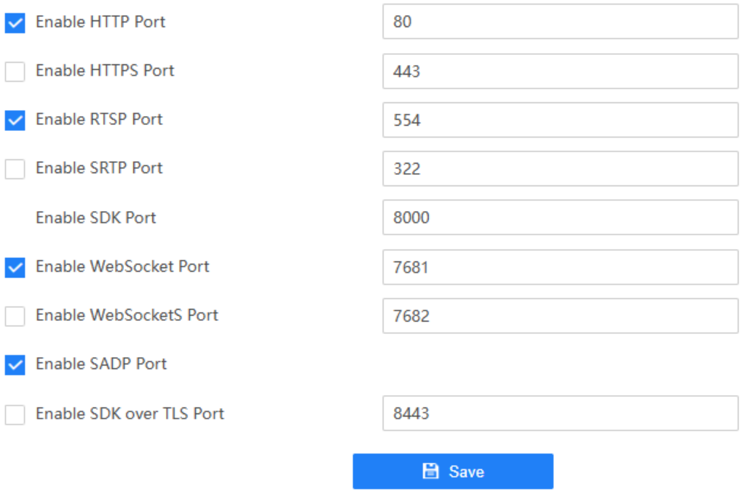
It stands for domain name server. It is required if you need to visit the device with domain name. And it is also required for some applications (e.g., sending email). Set **Preferred DNS Address** properly if needed.

3. Click **Save**.

3.2 Set Port

The device port can be modified when the device cannot access the network due to port conflicts.

Go to **Configuration → Network → Network Parameters → Port** for port settings.



☑ Enable HTTP Port 80

□ Enable HTTPS Port 443

☑ Enable RTSP Port 554

□ Enable SRTP Port 322

Enable SDK Port 8000

☑ Enable WebSocket Port 7681

□ Enable WebSocketS Port 7682

☑ Enable SADP Port

□ Enable SDK over TLS Port 8443

Figure 3-2 Set Port

Enable HTTP Port

It refers to the port through which the browser accesses the device. For example, when the HTTP port is modified to 81, you need to enter ***http://192.168.1.64:81*** in the browser address bar for login.

Enable HTTPS Port

It refers to the port through which the browser accesses the device, but certificate verification is needed.

Enable RTSP Port

RTSP (Real-Time Streaming Protocol) is a communication protocol used to control servers that stream media content over the Internet. It helps in setting up and managing connections between devices for streaming audio or video. RTSP ensures that media players and servers can communicate smoothly, allowing users to play, pause, adjust volume, and perform other actions while streaming content.

Enable SRTP Port

SRTP (Secure Real-Time Transport Protocol) is an extension to RTP (Real-Time Transport Protocol) that incorporates enhanced security features.

Enable SDK Port

It refers to the port through which the client adds the device.

Enable WebSocket Port

It refers to the full-duplex communication protocol port based on TCP. Enable the port for live view without plug-in.

Enable WebSocketS Port

It refers to the full-duplex communication protocol port based on TCP. Enable the port for live view without plug-in. It can only be accessed via certificate verification with high security.

Enable SADP Port

It refers to the port through which the SADP software searches the device.

Enable SDK over TLS Port

It refers to the port that adopts TLS protocol over the SDK service, to provide safer data transmission.

Note

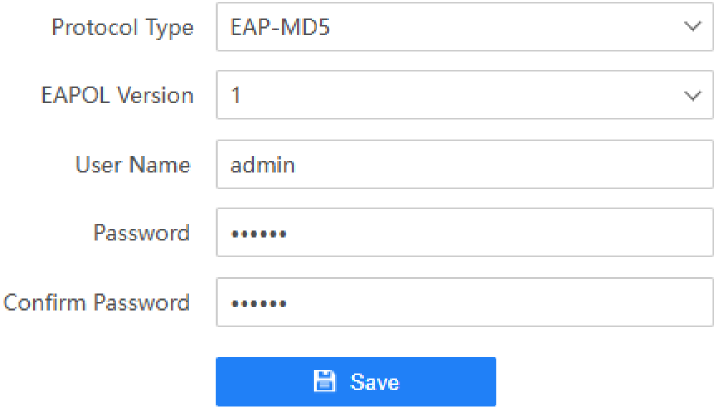
- After editing the port, access to the device via the new port.
- Reboot the device to bring the new settings into effect.
- The supported ports vary with different models. The actual device prevails.

3.3 Set IEEE 802.1X

IEEE 802.1X is a port-based network access control. It enhances the security level of the LAN/ WLAN. When devices connect to the network with IEEE 802.1X standard, the authentication is needed.

Steps

1. Go to **Configuration → Network → Network Parameters → 802.1X** .
2. Enable 802.1X.



Protocol Type	EAP-MD5
EAPOL Version	1
User Name	admin
Password	••••••
Confirm Password	••••••

Figure 3-3 Set IEEE 802.1X

3. Select **Protocol Type** and **EAPOL Version**.

   Protocol Type

   The authentication server must be configured. Register a user name and password for 802.1X in the server in advance. Enter the user name and password for authentication.

   EAPOL Version

   The EAPOL version must be identical with that of the router or the switch.
4. Enter **User Name** and **Password** registered in the server.

5. Confirm the password.
6. Click **Save**.

3.4 Set DDNS

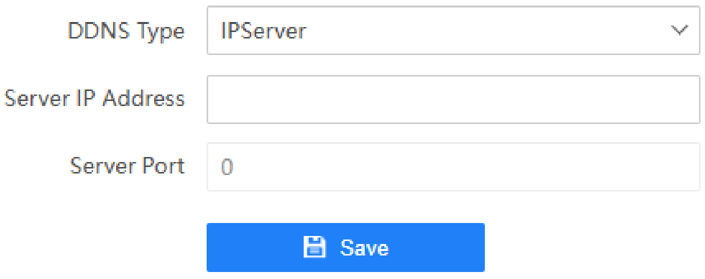
You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

Before You Start

- Register the domain name on the DDNS server.
- Set the LAN IP address, subnet mask, gateway, and DNS server parameters. Refer to ***Set IP Address*** for details.
- Complete port mapping. The default ports are 80, 8000, and 554.

Steps

1. Go to **Configuration → Network → Network Parameters → DDNS** .
2. Enable DDNS.



DDNS Type: IPServer

Server IP Address:

Server Port: 0

Figure 3-4 Set DDNS

3. Enter the server address and other information.

Note

You can select **IPServer**, **DynDNS**, and **NO-IP** for the DDNS type.

4. Click **Save**.
5. Access the device.

By Browsers Enter the domain name in the browser address bar to access the device.

By Client Software Add domain name to the client software. Refer to the client software manual for specific adding methods.

3.5 Set SNMP

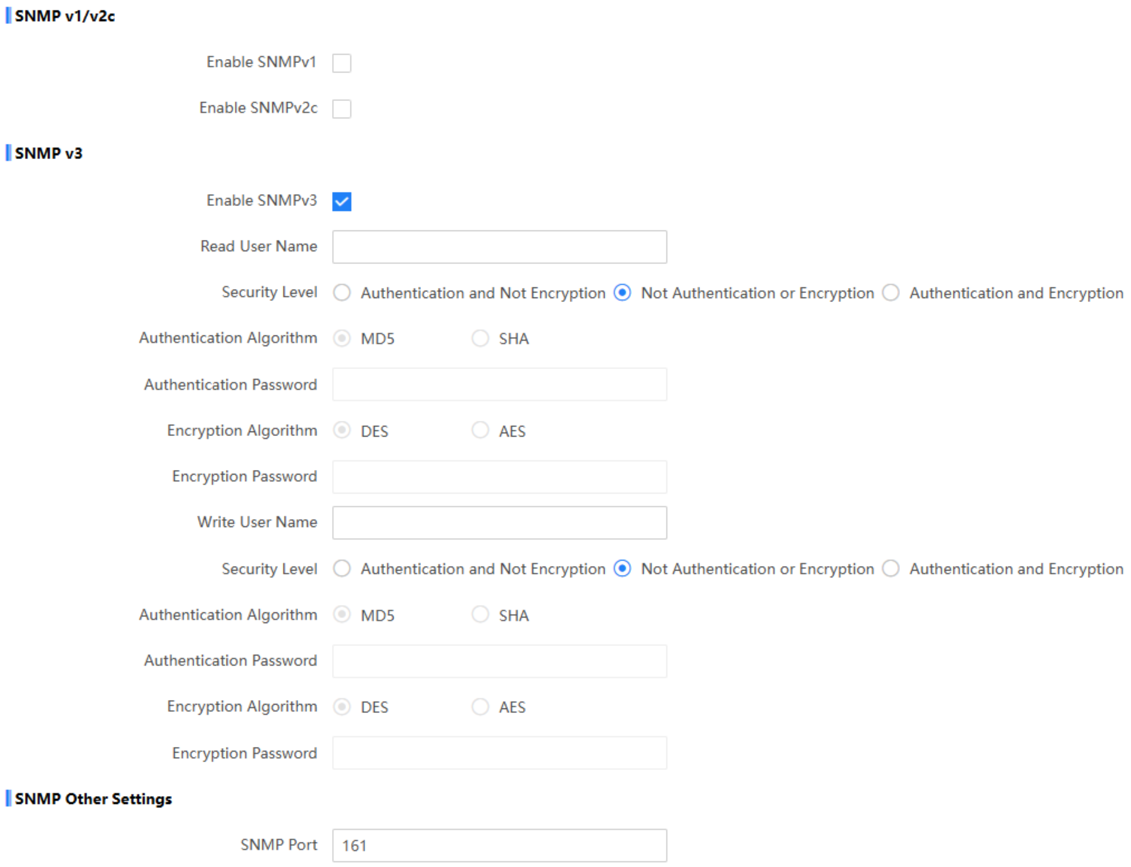
You can set the SNMP network management protocol to get the alarm event and exception messages in network transmission.

Before You Start

Download the SNMP software and manage to receive the device information via SNMP port.

Steps

1. Go to **Configuration → Network → Network Parameters → SNMP** .



SNMP v1/v2c

Enable SNMPv1 □

Enable SNMPv2c □

SNMP v3

Enable SNMPv3 ☑

Read User Name

Security Level ○ Authentication and Not Encryption ● Not Authentication or Encryption ○ Authentication and Encryption

Authentication Algorithm ● MD5 ○ SHA

Authentication Password

Encryption Algorithm ● DES ○ AES

Encryption Password

Write User Name

Security Level ○ Authentication and Not Encryption ● Not Authentication or Encryption ○ Authentication and Encryption

Authentication Algorithm ● MD5 ○ SHA

Authentication Password

Encryption Algorithm ● DES ○ AES

Encryption Password

SNMP Other Settings

SNMP Port 161

Figure 3-5 Set SNMP

2. Check **Enable SNMPv1/Enable SNMP v2c/Enable SNMPv3**.

Note

- The SNMP version you select should be the same as that of the SNMP software.
- Use different versions according to the security levels required. There exists information leakage using SNMP v1 or v2. You're recommended to use SNMP v3, which provides encryption and is safer. If you use v3, HTTPS protocol must be enabled.

3. Set the SNMP parameters.

Note

For SNMP v3, you need to set **Authentication Algorithm** and **Authentication Password**, and **Encryption Algorithm** and **Encryption Password**.

4. Click **Save**.

3.6 Set QoS

QoS (Quality of Service) can help improve the network delay and network congestion by setting the priority of data sending.

Note

QoS needs support from network devices such as routers and switches.

Steps

1. Go to **Configuration → Network → Network Parameters → QoS** .
2. Enable DSCP according to the actual needs and set the value.

   Note

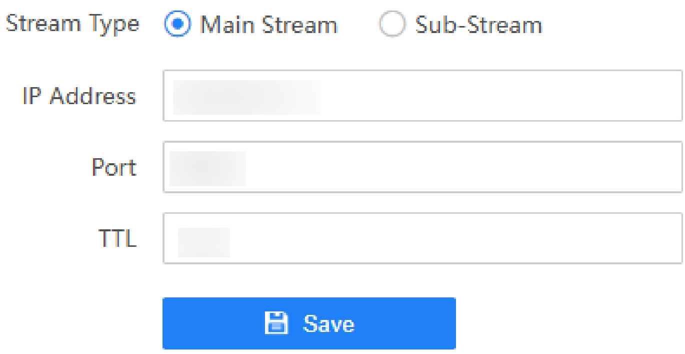
   Network can identify the priority of data transmission. The bigger the DSCP value is, the higher the priority is. Same settings need to be set in the router for configuration.
3. Click **Save**.

3.7 Set Multicast

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneously.

Steps

1. Go to **Configuration → Network → Network Parameters → Multicast** .



Stream Type ● Main Stream ○ Sub-Stream

IP Address

Port

TTL

Figure 3-6 Set Multicast

2. Set the parameters.

   Stream Type

   The stream type as the multicast source.

   IP Address

   It stands for the address of multicast host.

Port

The port of the selected stream.

TTL

TTL (Time to Live) is a crucial setting in networking and computing that determines how long data packets remain valid and available within a network before being discarded by a router. It is used in various contexts, including DNS, IP headers, and caching mechanisms.

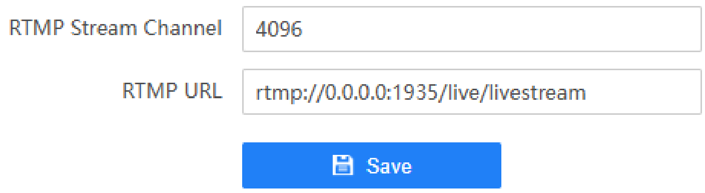
3. Click **Save**.

3.8 Set RTMP

RTMP (Real-Time Messaging Protocol) is designed for transmitting audio and video over the Internet. It is used to stream multimedia content on demand and supports live streaming.

Steps

1. Go to **Configuration → Network → Network Parameters → RTMP** .



RTMP Stream Channel 4096

RTMP URL rtmp://0.0.0.0:1935/live/livestream

Figure 3-7 Set RTMP

2. Set the parameters.

RTMP Stream Channel

The size of the RTMP stream channel. It is 4096 by default.

RTMP URL

The RTMP streaming URL. It is ***rtmp://192.168.1.64:1935/live/livestream*** by default.

3. Click **Save**.

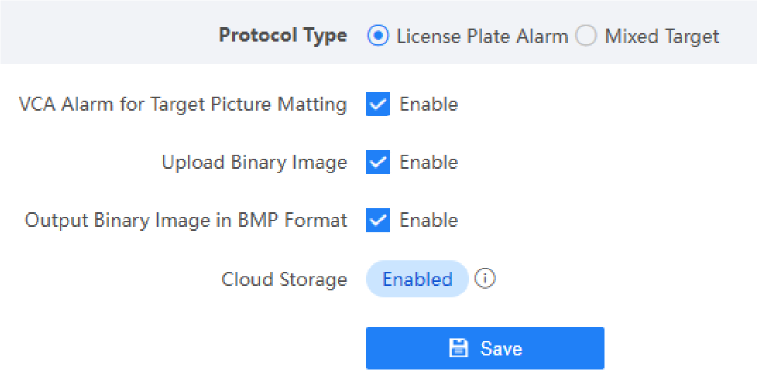
3.9 Connect to Platform

3.9.1 Set Arming Host

The device can upload the captured pictures via the arming host.

Steps

1. Go to **Configuration → Network → Data Connection → Arm Upload** .



Protocol Type ● License Plate Alarm ○ Mixed Target

VCA Alarm for Target Picture Matting ☑ Enable

Upload Binary Image ☑ Enable

Output Binary Image in BMP Format ☑ Enable

Cloud Storage Enabled

Figure 3-8 Set Arming Host

2. Select **Protocol Type**.

Note

Supported functions vary with different models. The actual device prevails.

License Plate Alarm

Uploads arming alarm images of the license plate. You can enable the functions below.

VCA Alarm for Target Picture Matting

If you have enabled motor vehicle/non-motor vehicle/pedestrian capture and target picture matting, you can enable the function to upload a scene picture, a license plate picture, and a target matting picture for the captured target.

Upload Binary Image

Enable the function to upload binary images full of black or white pixel points.

Output Binary Image in BMP Format

Enable the function to output images in BMP format. Disable the function to output images in JPEG format by default.

Mixed Target

Uploads images of multiple targets such as humans and vehicles. You can enable the body property to recognize clothes, bags, and other properties.

3. **Optional:** If you want to save the alarm information and pictures to the cloud storage, go to **Configuration → Network → Data Connection → Cloud Storage** to set the parameters. Refer to ***Set Cloud Storage*** for details.
4. Click **Save**.

3.9.2 Set SDK Listening

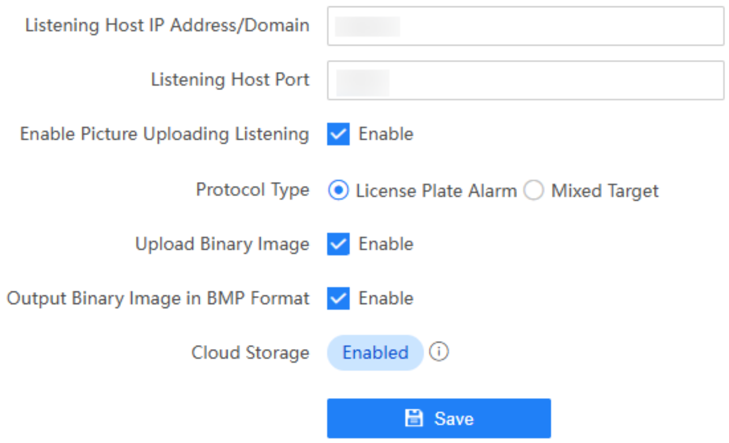
The SDK listening can be used to receive the uploaded information and pictures of the device arming alarm.

Before You Start

The listening service has been enabled for the SDK listening, and the network communication with the device is normal.

Steps

1. Go to **Configuration → Network → Data Connection → SDK Listening** .
2. Enable SDK listening.



Listening Host IP Address/Domain [redacted]

Listening Host Port [redacted]

Enable Picture Uploading Listening ☑ Enable

Protocol Type ● License Plate Alarm ○ Mixed Target

Upload Binary Image ☑ Enable

Output Binary Image in BMP Format ☑ Enable

Cloud Storage Enabled ⓘ

Figure 3-9 Set SDK Listening

3. Set **Listening Host IP Address/Domain** and **Listening Host Port** if you need to upload the alarm information and pictures.
4. **Optional:** The device will transmit images via the SDK listening if you enable picture uploading listening.
5. Select **Protocol Type**.

Note

Supported functions vary with different models. The actual device prevails.

License Plate Alarm

Uploads arming alarm images of the license plate. You can enable the functions below.

Upload Binary Image

Enable the function to upload binary images full of black or white pixel points.

Output Binary Image in BMP Format

Enable the function to output images in BMP format. Disable the function to output images in JPEG format by default.

Mixed Target

Uploads images of multiple targets such as humans and vehicles. You can enable the body property to recognize clothes, bags, and other properties.

6. **Optional:** If you want to save the alarm information and pictures to the cloud storage, go to **Configuration → Network → Data Connection → Cloud Storage** to set the parameters. Refer to ***Set Cloud Storage*** for details.
7. Click **Save**.

3.9.3 Set FTP

Set FTP parameters if you want to upload the captured pictures to the FTP server.

Before You Start

Set the FTP server, and ensure the device can communicate normally with the server.

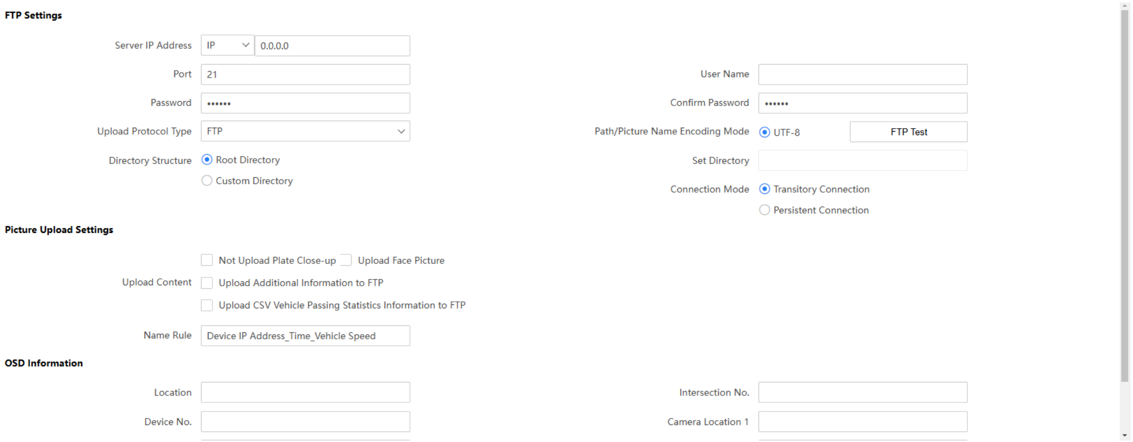
Steps

1. Go to **Configuration → Network → Data Connection → FTP** .
2. Enable the FTP server.

Note

- You can only enable one FTP if the device does not support the violation capture. If more than one FTP is enabled, you should set **Upload Content** for each FTP according to your needs.
- Enable **FTP1** if you want to upload to only one FTP server.

3. Set FTP parameters.



FTP Settings

Server IP Address: IP 0.0.0.0
Port: 21
Password: ••••••
Upload Protocol Type: FTP
Directory Structure: ● Root Directory ○ Custom Directory
User Name:
Confirm Password: ••••••
Path/Picture Name Encoding Mode: ● UTF-8
Set Directory:
Connection Mode: ● Transitory Connection ○ Persistent Connection

Picture Upload Settings

Upload Content: □ Not Upload Plate Close-up □ Upload Face Picture □ Upload Additional Information to FTP □ Upload CSV Vehicle Passing Statistics Information to FTP
Name Rule: Device IP Address_Time_Vehicle Speed

OSD Information

Location:
Device No.:
Intersection No.:
Camera Location 1:

Figure 3-10 Set FTP

1) Select **Sever IP Address** type and enter corresponding information.
2) Enter **Port**.
3) Enter **User Name** and **Password**, and confirm the password.
4) Select **Upload Protocol Type**.

SFTP

SFTP (SSH File Transfer Protocol) is a network protocol that provides file transfer and manipulation functionality over any reliable data stream. SFTP service is typically used with the SSH-2 protocol (TCP port 22) to provide secure file transfer, but is intended to be usable with other protocols as well.

FTPS

FTPS (File Transfer Protocol Secure) is used to provide a number of ways that FTP software can perform secure file transfers. Each way involves the use of a SSL/TLS layer below the standard FTP protocol to encrypt the control and/or data channels. It requires a certificate, and needs the additional configuration of a supported FTP server.

5) Select **Directory Structure**.

Note

You can customize the directory structure according to your needs.

6) Select **Path/Picture Name Encoding Mode**.

UTF-8

UNICODE encoding.

7) Select **Connection Mode**.

Transitory Connection

The connection is temporarily made for one data transmission task. After this task, the connection will be broken.

Persistent Connection

The connection is made for long-term data transmission, which will be broken only when the device is disconnected from the FTP server.

4. **Optional:** Enable upload functions.

Note

Supported functions vary with different models. The actual device prevails.

Not Upload Plate Close-up

The close-up pictures of a license plate will not be uploaded.

Upload Face Picture

Upload face close-up pictures to the FTP server.

Upload Target Picture

Upload the pictures of the target detection area to the FTP server.

Upload Additional Information to FTP

Add related information when uploading data to the FTP server.

Upload CSV Vehicle Passing Statistics Information to FTP

Upload the CSV vehicle passing statistics information to the FTP server.

5. **Optional:** Click **FTP Test** to check the FTP server.
6. Click the text filed of **Name Rule** to set the directory and separator for the file storage.

Note

For the European version, select **Custom** and enter ***adr*** or ***ADR*** in the text field, and the ADR (Autorisation Dangerous Road) vehicle plate number will be added in the corresponding vehicle picture name.

7. **Optional:** Edit **OSD Information** which can be uploaded to the FTP server with the pictures to make it convenient to view and distinguish the data.
8. Click **Save**.

3.9.4 Set ISAPI Listening

ISAPI listening and SDK listening are mutually exclusive protocols. If you enable the picture uploading listening, the device will transmit images via the SDK listening. If not, the device will upload images via ISAPI protocol after the ISAPI parameters are set.

Before You Start

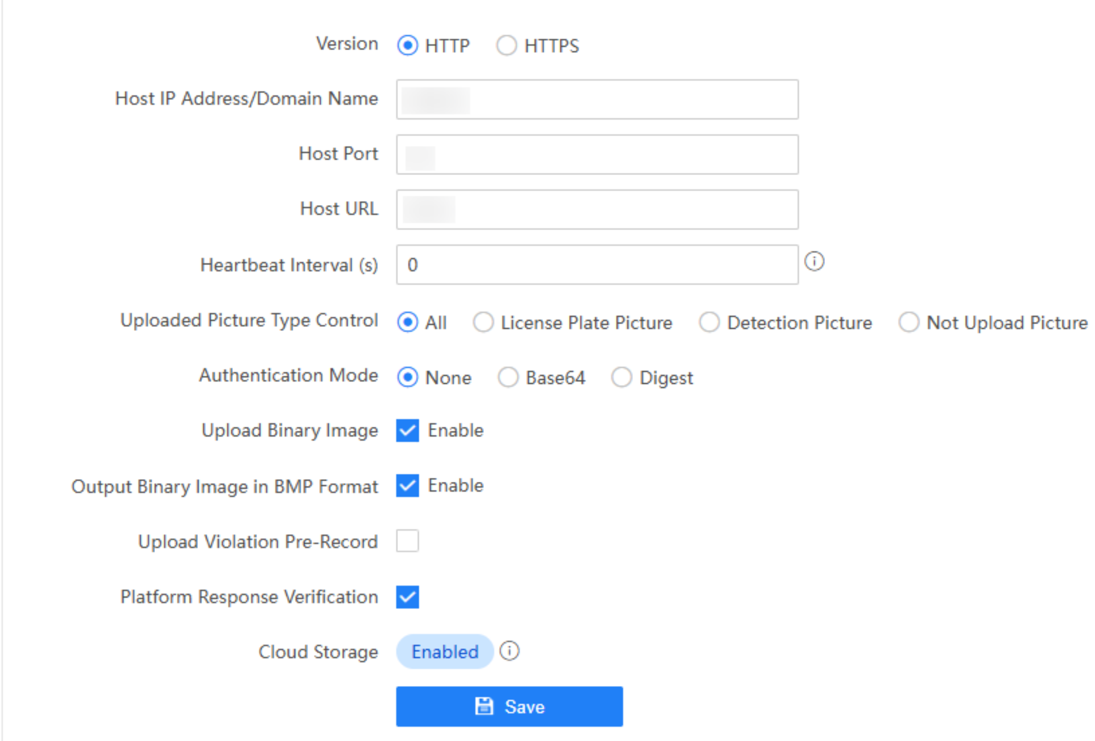
The listening service has been enabled for the ISAPI host, and the network communication with the device is normal.

Steps

1. Go to **Configuration → Network → Data Connection → ISAPI Listening** .
2. Enable **ISAPI1** or **ISAPI2**.

Note

For some application modes, only one ISAPI is supported. The actual interface prevails.



Version ● HTTP ○ HTTPS

Host IP Address/Domain Name [redacted]

Host Port [redacted]

Host URL [redacted]

Heartbeat Interval (s) 0 ⓘ

Uploaded Picture Type Control ● All ○ License Plate Picture ○ Detection Picture ○ Not Upload Picture

Authentication Mode ● None ○ Base64 ○ Digest

Upload Binary Image ☑ Enable

Output Binary Image in BMP Format ☑ Enable

Upload Violation Pre-Record □

Platform Response Verification ☑

Cloud Storage Enabled ⓘ

Figure 3-11 Set ISAPI Listening

3. Select **Version**.
4. Set **Host IP Address/Domain Name**, **Host Port**, and **Host URL**.
5. Set the parameters.

Heartbeat Interval

If you set it as 0, the heartbeat is disabled.

Uploaded Picture Type Control

You can upload license plate pictures and detection pictures (the capture scene pictures), or do not upload pictures.

Authentication Mode

Only the authorized users can access the device. If you select **None**, the device will not verify the authentication condition of the access users. It is recommended to select an authentication mode to guarantee the device information security.

Upload Binary Image

Enable the function to upload images which are full of black or white pixel points.

Output Binary Image in BMP Format

Enable the function to output images in BMP format. Disable the function to output images in JPEG format by default.

Upload Violation Pre-Record

Enable the function to upload the pre-recorded videos of violations to the host.

Platform Response Verification

Enable the function, and the device will get the platform response result.

Incident Mode

For the application modes of incident detection and data collection, select the data to be uploaded. If you select **All**, all the data will be uploaded. If you select **Specified**, select corresponding **Alarm Event** to be uploaded.

6. **Optional:** If you want to save the alarm information and pictures to the cloud storage, go to **Configuration → Network → Data Connection → Cloud Storage** to set the parameters. Refer to ***Set Cloud Storage*** for details.
7. Click **Save**.

3.9.5 Connect to ISUP Platform

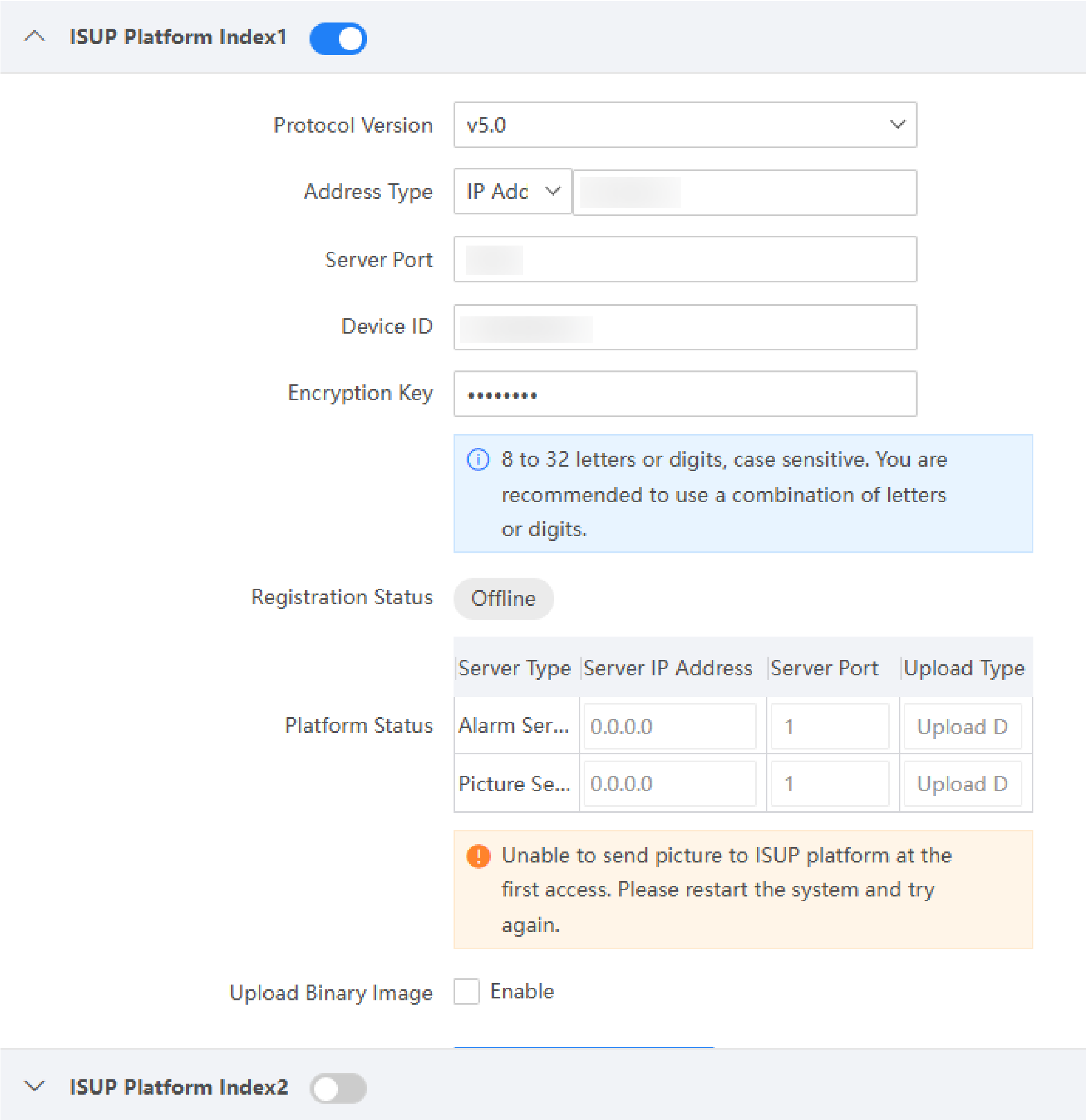
ISUP is a platform access protocol. The device can be remotely accessed via this platform.

Before You Start

- Create the device ID on ISUP platform.
- Ensure the device can communicate with the platform normally.

Steps

1. Go to **Configuration → Network → Data Connection → ISUP** .
2. Enable ISUP Platform Index1 or 2.



ISUP Platform Index1

Protocol Version: v5.0

Address Type: IP Adc [redacted]

Server Port: [redacted]

Device ID: [redacted]

Encryption Key: ••••••••

ⓘ 8 to 32 letters or digits, case sensitive. You are recommended to use a combination of letters or digits.

Registration Status: Offline

Platform Status

Server Type	Server IP Address	Server Port	Upload Type
Alarm Ser...	0.0.0.0	1	Upload D
Picture Se...	0.0.0.0	1	Upload D

! Unable to send picture to ISUP platform at the first access. Please restart the system and try again.

Upload Binary Image: ☐ Enable

ISUP Platform Index2

Figure 3-12 Connect to ISUP Platform

3. Select **Protocol Version**.
4. Select **Address Type** and enter IP address or domain name of the platform.
5. Enter **Server Port**, **Device ID**, and **Encryption Key**.

Note

The device ID should be the same with the added one on the platform.

6. **Optional:** You can enable **Upload Binary Image** if you need to upload images which are full of black or white pixel points.

Note

Enable **Output Binary Image in BMP Format** if you want to output images in BMP format.

7. Click **Save**.

What to do next

When the registration status is online, you can manage the device via the platform or server.

3.9.6 Connect to OTAP

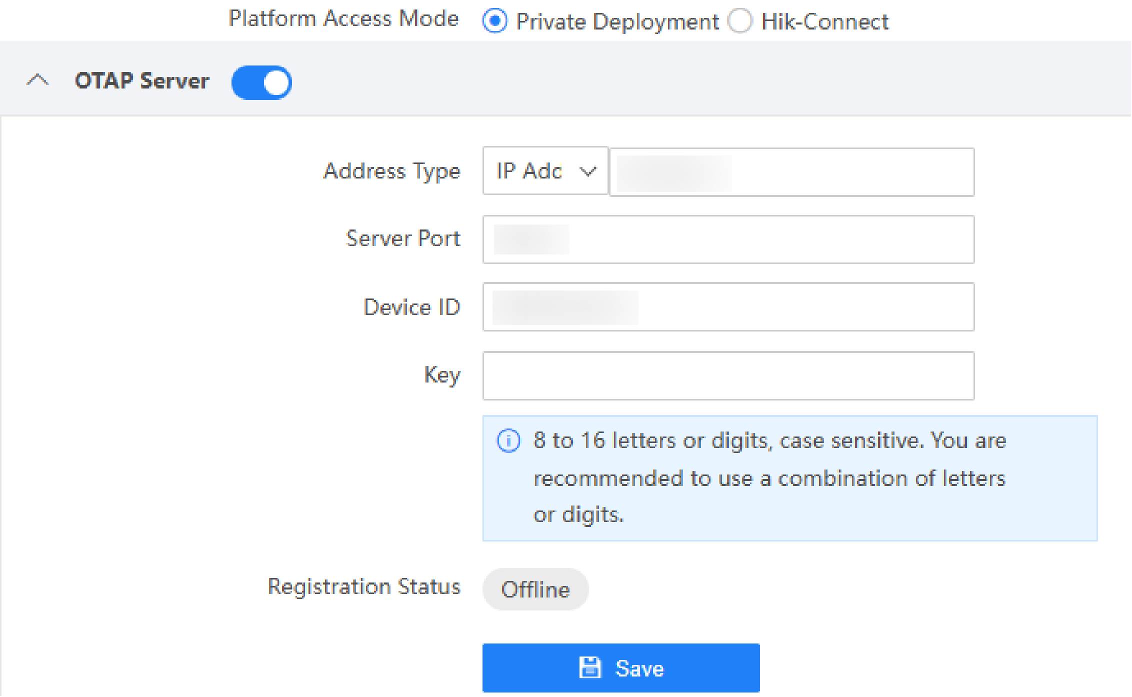
The device can be accessed to the platform via OTAP protocol to realize live view, view incident information, manage the devices, etc. via the platform.

Before You Start

- Set the network parameters including device IP address, gateway, DNS, etc. to get access to the network.
- Disable the other platform accesses conflicting with OTAP.

Steps

1. Go to **Configuration → Network → Data Connection → OTAP** .
2. Select **Platform Access Mode** as **Private Deployment**.
3. Enable **OTAP Server**.



Platform Access Mode ● Private Deployment ○ Hik-Connect

OTAP Server (enabled)

Address Type: IP Adc

Server Port:

Device ID:

Key:

8 to 16 letters or digits, case sensitive. You are recommended to use a combination of letters or digits.

Registration Status: Offline

Figure 3-13 Connect to OTAP

4. Set corresponding parameters.

Address Type

Select the address type of the connected platform or server, and enter the IP address or domain name.

Server Port

The port of the connected platform or server.

Device ID

The device ID should be the same with the added one on the OTAP platform.

Key

Set a custom key to encrypt the data connection between the device and the platform or server.

5. Click **Save**.

What to do next

When the registration status is online, you can manage the device via the platform or server.

3.9.7 Connect to Hik-Connect

The device can be remotely accessed via Hik-Connect.

Before You Start

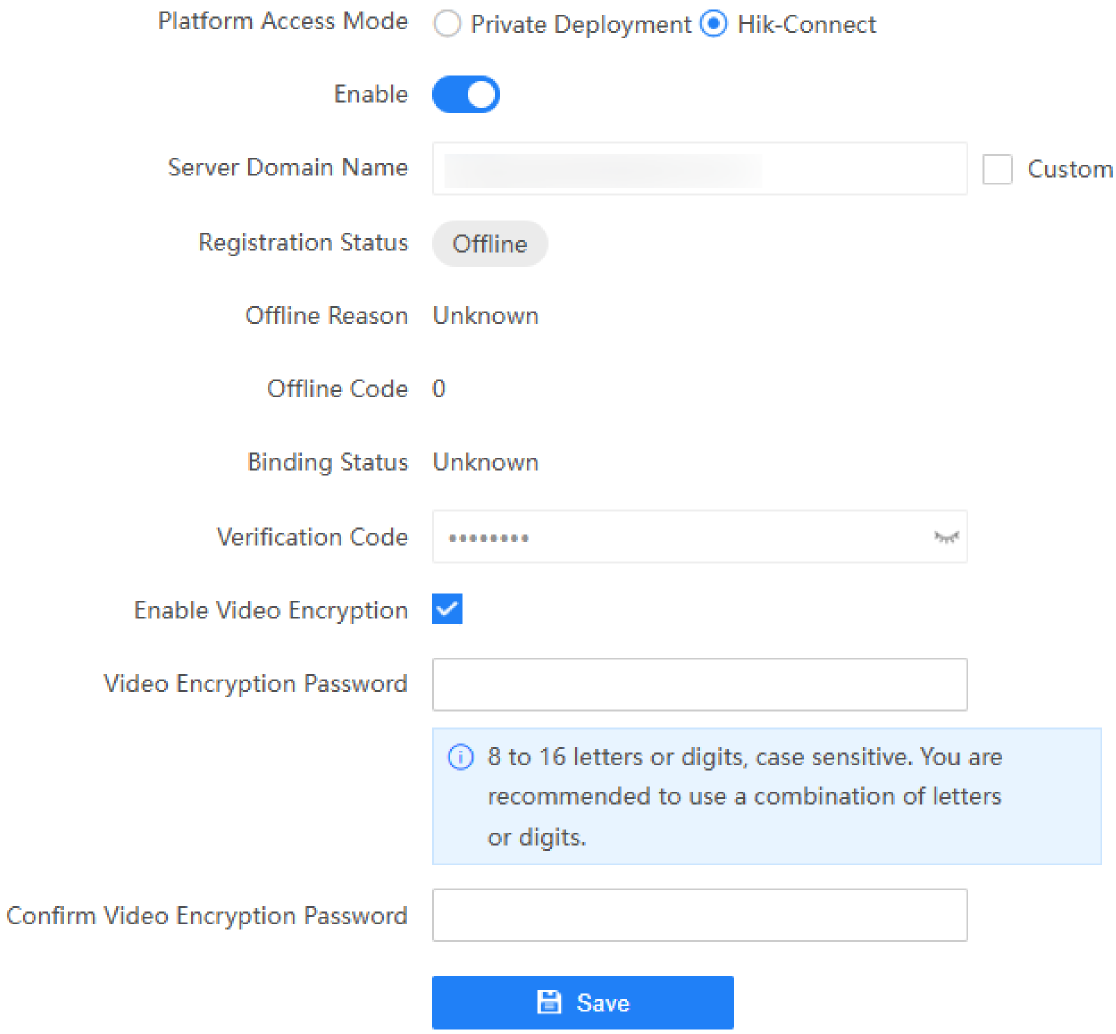
- Set the network parameters including device IP address, gateway, DNS, etc. to get access to the network.
- OTAP connection is disabled.

Steps

Note

This function varies with different models. The actual device prevails.

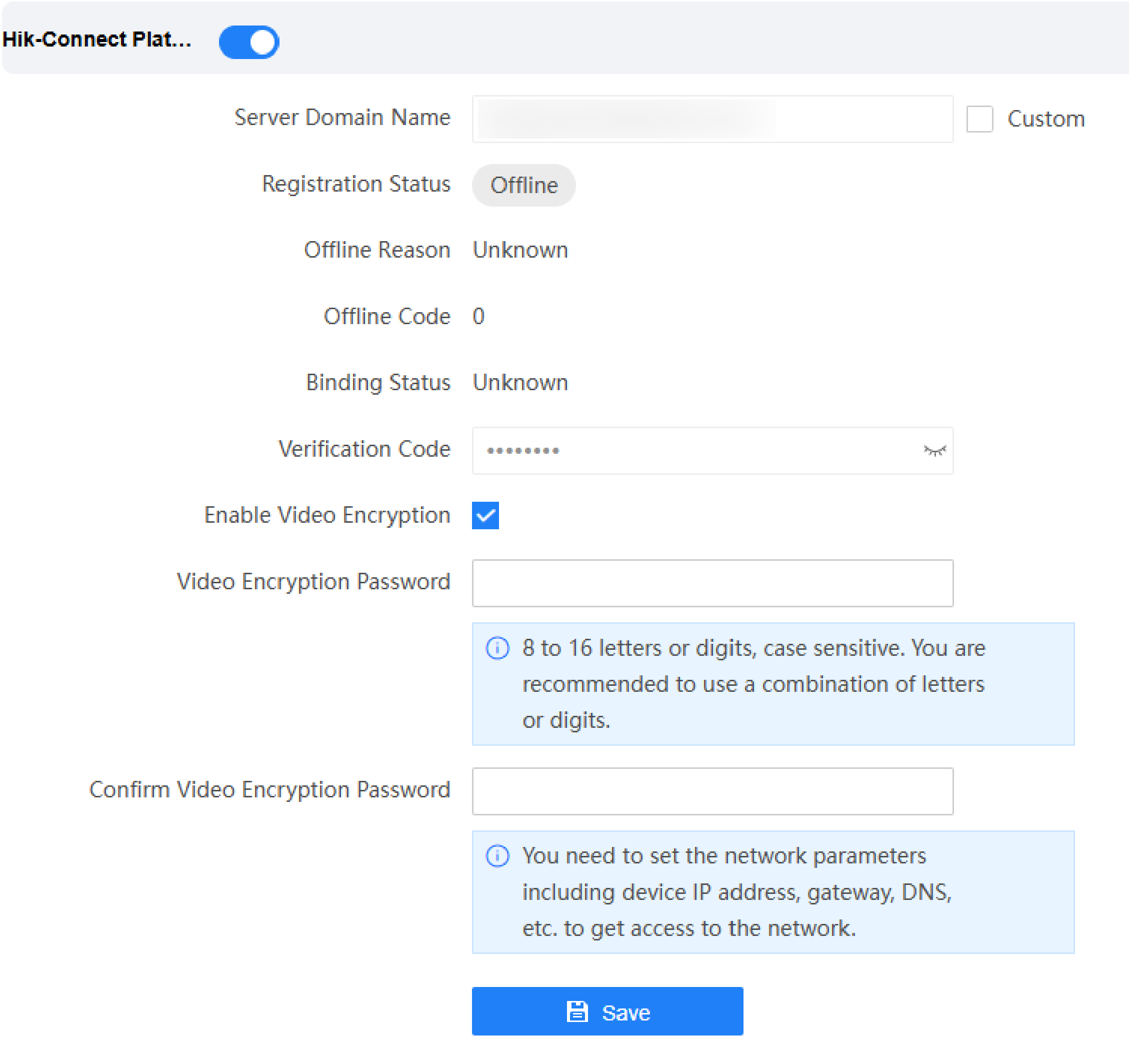
1. Enable Hik-Connect in two ways.
   - Get access to Hik-Connect V2.0. Go to **Configuration → Network → Data Connection → OTAP** , and select **Platform Access Mode** as **Hik-Connect**. Enable the function.



Platform Access Mode	○ Private Deployment ● Hik-Connect
Enable	●
Server Domain Name	[redacted] □ Custom
Registration Status	Offline
Offline Reason	Unknown
Offline Code	0
Binding Status	Unknown
Verification Code	•••••••••
Enable Video Encryption	☑
Video Encryption Password	
	ⓘ 8 to 16 letters or digits, case sensitive. You are recommended to use a combination of letters or digits.
Confirm Video Encryption Password	

Figure 3-14 Connect to Hik-Connect (V2.0)

- Get access to Hik-Connect V3.0. Go to **Configuration → Network → Data Connection → Hik-Connect Platform** . Enable **Hik-Connect Platform**.



Hik-Connect Plat...

Server Domain Name: [redacted] □ Custom

Registration Status: Offline

Offline Reason: Unknown

Offline Code: 0

Binding Status: Unknown

Verification Code: ••••••••

Enable Video Encryption: ☑

Video Encryption Password:

ⓘ 8 to 16 letters or digits, case sensitive. You are recommended to use a combination of letters or digits.

Confirm Video Encryption Password:

ⓘ You need to set the network parameters including device IP address, gateway, DNS, etc. to get access to the network.

Figure 3-15 Connect to Hik-Connect (V3.0)

2. **Optional:** If you have allocated a custom server, check **Custom** and enter the custom **Server Domain Name**.
3. Enter a custom **Verification Code** used to add the device via **Hik-Connect**.

⚠ **Caution**

The verification code should be 6 letters or digits, case sensitive. You are recommended to use a combination of letters or digits.

4. **Optional:** Check **Enable Video Encryption** and set **Video Encryption Password** to encrypt the videos transmission. Confirm the password.
5. Click **Save**.
6. Add the device to Hik-Connect.

   1) Get and install Hik-Connect application by the following ways.

- Visit ***https://appstore.hikvision.com*** to download the application according to your mobile phone system.
- Visit the official site of our company. Then go to **Support → Tools → Installation & Maintenance Tools → Hikvision APP Store** .
- Scan the QR code below to download the application.

Figure 3-16 Hik-Connect

Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit ***https://appstore.hikvision.com/static/help/index.html*** to refer to the troubleshooting.
- Visit ***https://appstore.hikvision.com/*** , and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

2) Start the application and register a user account to log in.
3) Add device by the serial No. on the device body and the verification code.

Note

Refer to the user manual of Hik-Connect application for details.

3.9.8 Set Integration Protocol

You can connect the device via ONVIF protocol.

Steps

1. Go to **Configuration → Network → Data Connection → Integration Protocol** .
2. Enable **ONVIF**.
3. Select **Authentication Mode**, and click **Save**.
4. Add a user.
   1) Click **Add**.
   2) Set user name, password, and user type, and confirm the password.
   3) Click **OK**.
   4) **Optional:** You can select the added user and click ✎ to edit the user information, or click 🗑 to delete the user.

Result

Only the added users can access the device via ONVIF protocol.

3.9.9 Set Cloud Storage

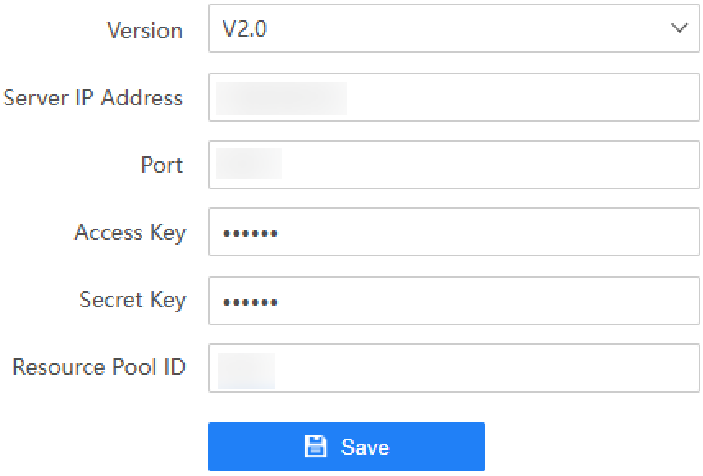
Cloud storage is a kind of network storage. It can be used as the extended storage to save the captured pictures.

Before You Start

- Arrange the cloud storage server.
- You have enabled listening or arming.

Steps

1. Go to **Configuration → Network → Data Connection → Cloud Storage** .
2. Enable **Cloud Storage**.



Version: V2.0
Server IP Address:
Port:
Access Key: ••••••
Secret Key: ••••••
Resource Pool ID:

Figure 3-17 Set Cloud Storage

3. Select **Version**.

V1.0
a. Enter **Server IP Address** and **Port**
b. Enter **User Name** and **Password**.
c. Enter **Cloud Storage ID** and **Violation Cloud Storage ID** according to the server storage area No.

V2.0
a. Enter **Server IP Address** and **Port**
b. Enter **Access Key** and **Secret Key**.
c. Enter **Resource Pool ID** according to the server storage area No. of uploading pictures.

4. Click **Save**.

Chapter 4 Application Mode Configuration

Note

- The supported application modes vary with different models. The actual device prevails.
- When you draw lane lines or detection areas on **Application Mode** interface, you can refer to the drawing guide displayed below the live view window. You can click **Guide Disable** to hide the guide, or click **Drawing Guide** to display the guide.

Caution

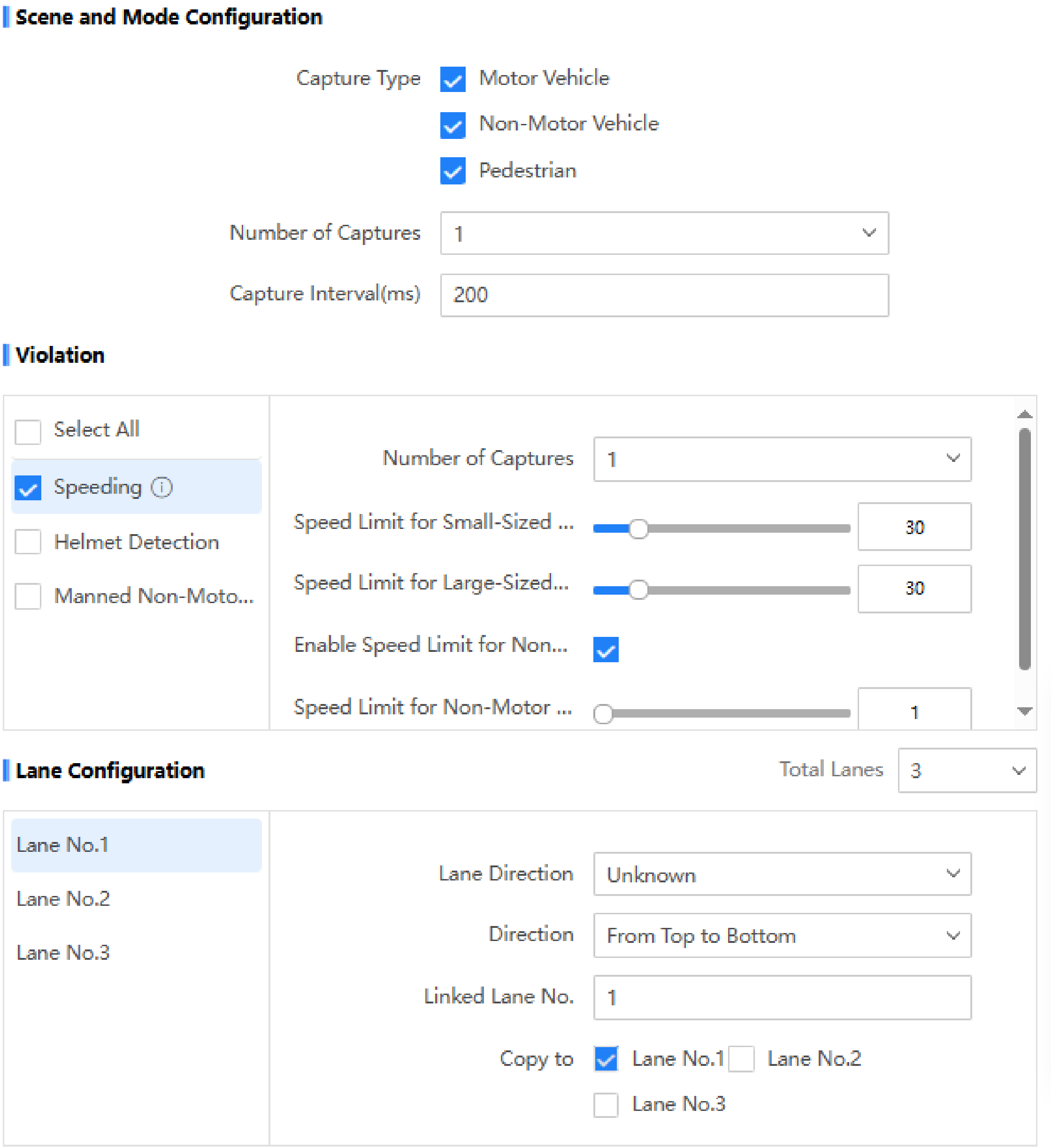
You can click **Default** on **Application Mode** interface to restore all the set parameters to the default settings. Please operate with care.

4.1 Set Smart Monitoring Capture

The smart monitoring mode supports capturing motor vehicles, non-motor vehicles, and pedestrians via video triggering.

Steps

1. Go to **Configuration → Capture → Application Mode** .
2. Select **Trigger Mode** as **Smart Mode**.



Scene and Mode Configuration

Capture Type ☑ Motor Vehicle ☑ Non-Motor Vehicle ☑ Pedestrian

Number of Captures 1

Capture Interval(ms) 200

Violation

□ Select All

☑ Speeding ⓘ

□ Helmet Detection

□ Manned Non-Moto...

Number of Captures 1

Speed Limit for Small-Sized ... 30

Speed Limit for Large-Sized... 30

Enable Speed Limit for Non... ☑

Speed Limit for Non-Motor ... 1

Lane Configuration

Total Lanes 3

Lane No.1

Lane No.2

Lane No.3

Lane Direction Unknown

Direction From Top to Bottom

Linked Lane No. 1

Copy to ☑ Lane No.1 □ Lane No.2 □ Lane No.3

Figure 4-1 Set Smart Monitoring Capture

3. Set scene and mode parameters.

Capture Type

Select the targets to be recognized and captured in the scene.

Number of Captures

The number of captured picture(s).

Capture Interval

The time between the adjacent captures.

4. Check the violation types and set the corresponding parameters.

Table 4-1 Violation Type Description

Violation Type	Parameters Description
Speeding	The motor or non-motor vehicle is driven in the speed larger than the max. speed limit of the lane. Check it and select the number of captured picture(s). Set the parameters below. • **Speed Limit for Small/Large-Sized Vehicle**: The actual speed limit for the vehicles. When the vehicle speed exceeds the value, speeding capture will be triggered. **Note** The speed limit of large-sized vehicles should be smaller than that of the small-sized vehicles. • **Enable Speed Limit for Non-Motor Vehicle**: Enable the function to capture speeding of non-motor vehicles. Set **Speed Limit for Non-Motor Vehicle**.
Helmet Detection	To detect if the driver of a non-motor vehicle wears the helmet. Check it and select the number of captured picture(s).
Manned Non-Motor Vehicle	The non-motor vehicle carries a person illegally. Check it and select the number of captured picture(s). You can also enable **Only Capture Manned Multi-Persons** to capture the violation that the non-motor vehicle carries 2 persons or more.

5. Select **Total Lanes**, and select a lane No. to set the lane parameters.

Lane Direction

The guidance direction of the lane.

Direction

If you select **From Top to Bottom**, the targets from the approaching direction towards the device will be captured. If you select **From Bottom to Top**, the targets from the leaving direction away from the device will be captured. If you set the direction as **From Top to Bottom**, then the vehicle will be judged as wrong-way driving if it comes from bottom to top, and vice versa.

Linked Lane No.

The device will number the lane in ascending order from left to right automatically. The lane No. will be marked in the capture pictures and alarm information.

Copy to

Check the other lane(s) to copy the same settings.

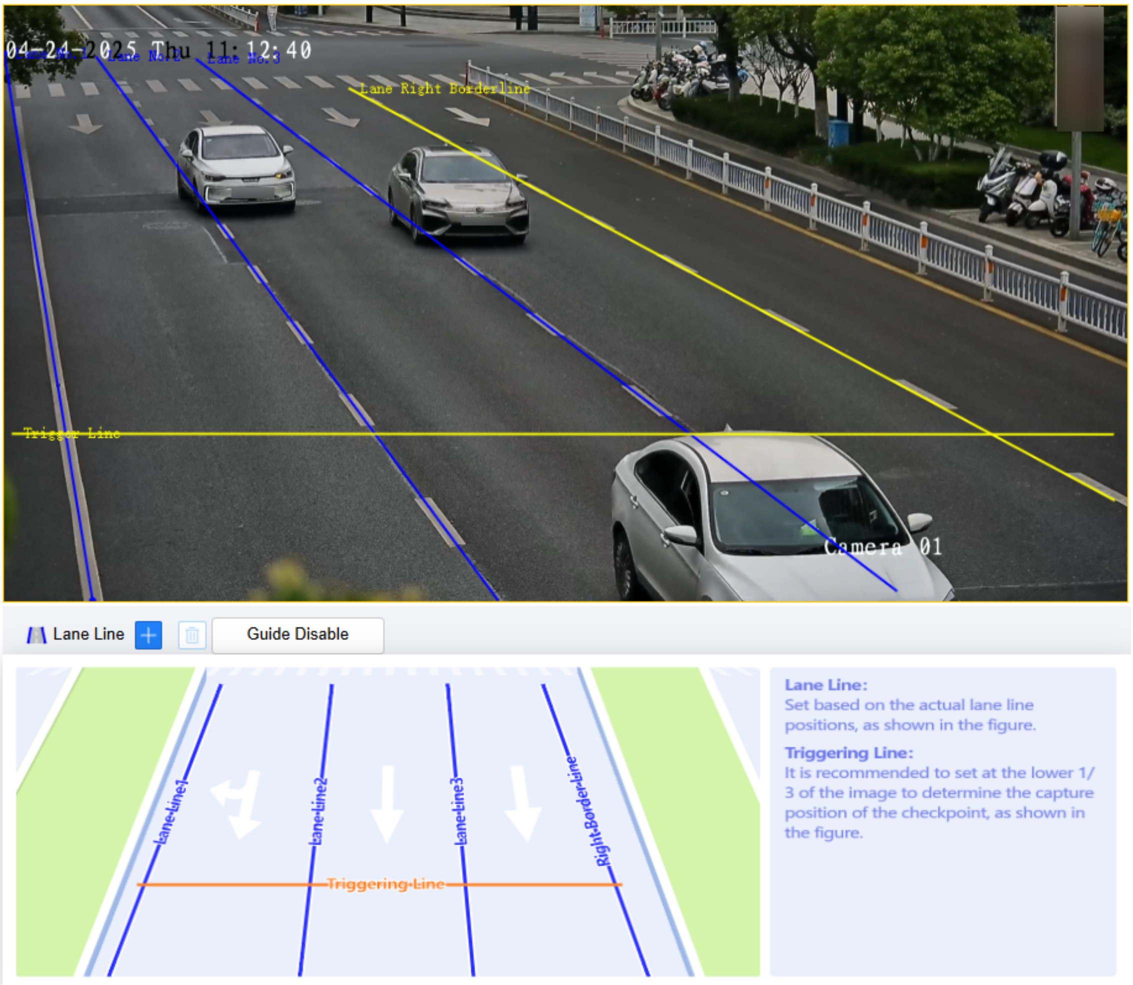
6. Draw lane lines.

1) Refer to the drawing guide below the live view image on the interface.

2) Select the default lane lines, right border line, and trigger line, and drag the two end points of the line or drag the whole line to adjust its position according to the actual scene.
3) **Optional:** You can select a lane line, and click 🗑 to delete the lane. Or click + to add a new lane line if the icon is available.

Note

The lane right borderline and trigger line cannot be deleted.



Lane Line:
Set based on the actual lane line positions, as shown in the figure.

Triggering Line:
It is recommended to set at the lower 1/3 of the image to determine the capture position of the checkpoint, as shown in the figure.

Figure 4-2 Draw Lane Lines

7. Click **Save**.

4.2 Set Incident Detection

The device supports to capture various traffic incidents.

Steps

1. Go to **Configuration → Capture → Application Mode** .

2. Select **Trigger Mode** as **Incident Detection**.
3. Click **Incident Detection**.
4. Set the parameters according to the instructions below, and click **Save**.

4.2.1 Set Linked Lane Parameters

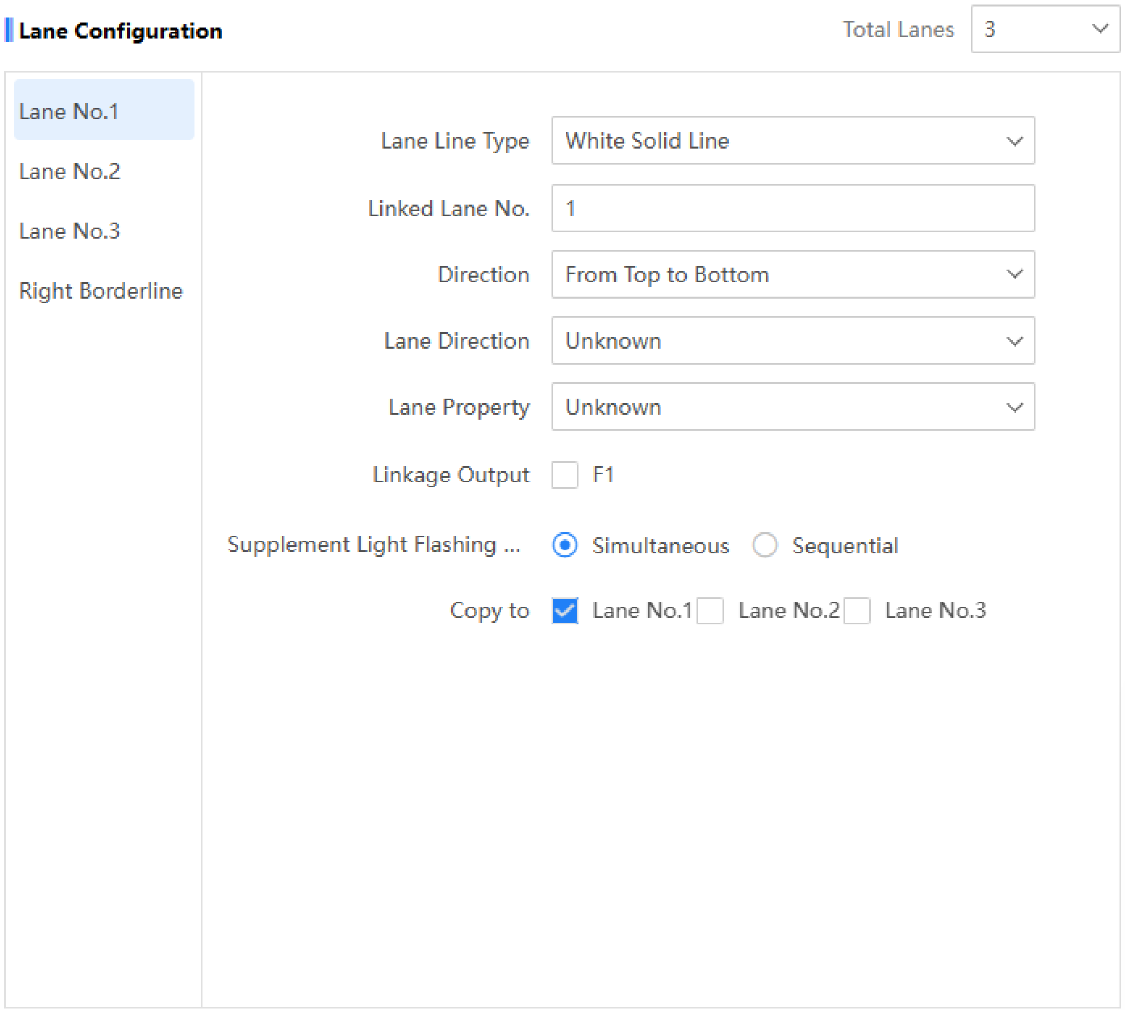
You can set the properties and parameters of the linked lanes.

Steps

Note

The linked lane parameters vary with different models. The actual device prevails.

1. Click **Lane Configuration**.
2. Select **Total Lanes**.
3. Select a lane No. to set the lane parameters.



Lane Configuration

Total Lanes: 3

Lane Line Type: White Solid Line

Linked Lane No.: 1

Direction: From Top to Bottom

Lane Direction: Unknown

Lane Property: Unknown

Linkage Output: □ F1

Supplement Light Flashing ...: ● Simultaneous ○ Sequential

Copy to: ☑ Lane No.1 □ Lane No.2 □ Lane No.3

Figure 4-3 Lane Configuration of Incident Detection

Lane Line Type

Select the lane line type according to the actual scene.

Linked Lane No.

The device will number the lane in ascending order from left to right automatically. The lane No. will be marked in the capture pictures and alarm information.

Direction

If you select **From Top to Bottom**, the targets from the approaching direction towards the device will be captured. If you select **From Bottom to Top**, the targets from the leaving direction away from the device will be captured.

Lane Direction

The guidance direction of the lane.

Lane Property

Select the current lane property according to its usage.

Linkage Output

Check the capture linked supplement light channel(s).

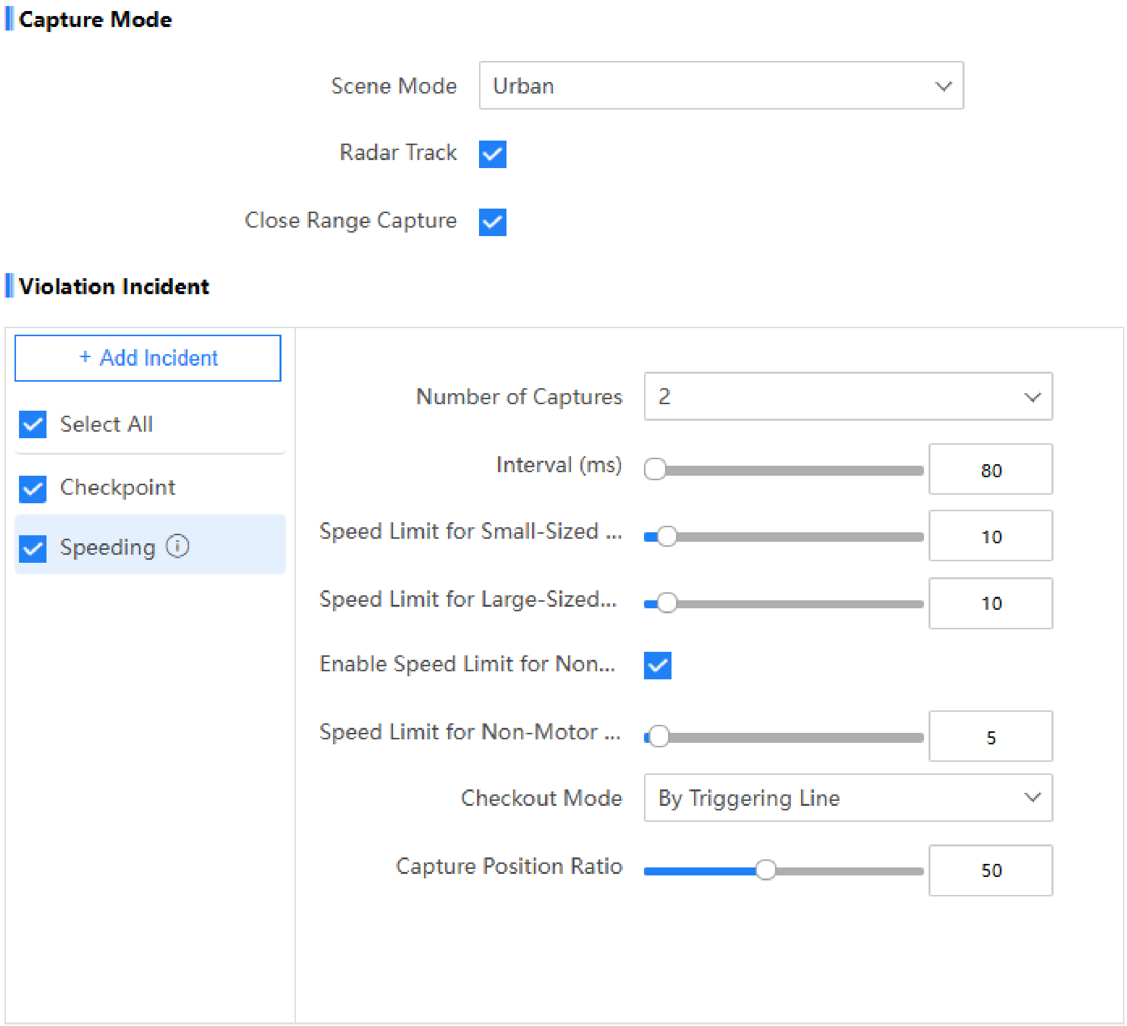
Supplement Light Flashing Mode

Select **Simultaneous**, and the supplement lights will flash simultaneously. Select **Sequential**, and the supplement lights will flash one by one.

4. **Optional:** Check the other lane(s) to copy the same settings.
5. Click **Save**.

4.2.2 Set Violation Incident

The device can capture pictures of the targets passing the checkpoint in the linked lanes according to the set rules.



Capture Mode

Scene Mode: Urban

Radar Track ☑

Close Range Capture ☑

Violation Incident

☑ Select All

☑ Checkpoint

☑ Speeding ⓘ

Number of Captures: 2

Interval (ms): 80

Speed Limit for Small-Sized ...: 10

Speed Limit for Large-Sized...: 10

Enable Speed Limit for Non... ☑

Speed Limit for Non-Motor ...: 5

Checkout Mode: By Triggering Line

Capture Position Ratio: 50

Figure 4-4 Set Violation Incident

Capture Mode

Go to **Violation Incident → Capture Mode** . Set the parameters, and click **Save**.

Scene Mode

Select the scene according to the actual device installation environment.

Radar Track

When the radar is connected, enable it to generate and overlay the radar tracks.

Note

The function is only available for the device supporting radar.

Close Range Capture

The device will track the target until one more picture is captured in close distance.

Violation Incident

Go to **Violation Incident → Violation Incident** . Click **Add Incident** to select the incident types to detect, and click **OK**. Check the incident types to enable the functions and click each type to set the corresponding parameters.

Note

The supported incident types vary with different models. The actual device prevails.

Table 4-2 Incident Type Description

Incident Type	Parameters Description
Checkpoint	Check it and select the number of captured picture(s). Select **Capture Type**.
Speeding	The motor or non-motor vehicle is driven in the speed larger than the max. speed limit of the lane. Check it and select the number of captured picture(s). Set the parameters. • **Interval**: The interval between two captures. • **Speed Limit for Small/Large-Sized Vehicle**: The max. speeds for the small-sized and large-sized vehicles respectively. When the vehicle speed exceeds the value, speeding capture will be triggered. • **Enable Speed Limit for Non-Motor Vehicle**: Check it to enable the speeding capture for the non-motor vehicles. Set **Speed Limit for Non-Motor Vehicle**. • **Checkout Mode**: If you select **By Triggering Line**, when the vehicle passes over the triggering line and the passing ratio is larger than the set **Capture Position Ratio**, speeding capture will be triggered. If you select **By Duration**, when the speeding incident lasts for more than the set **Duration**, speeding capture will be triggered.

4.2.3 Draw Lane Lines and Incident Areas

Draw lane lines and incident areas to detect and capture the violations or incidents in the linked areas.

Before You Start

Set lane and violation incident parameters.

Steps

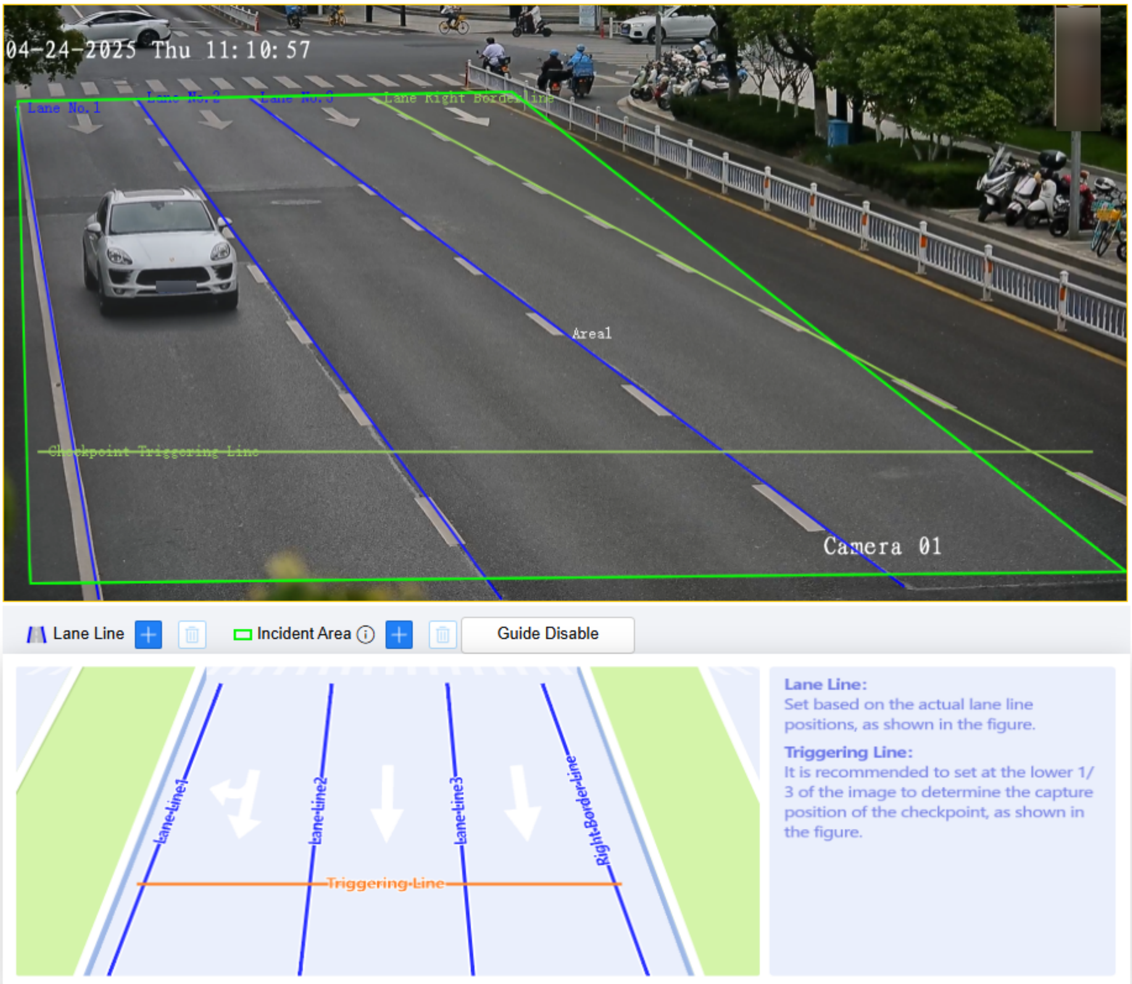
1. Refer to the drawing guide below the live view image on the interface.

2. Select the default lane lines, right border line, and trigger line, and drag the two end points of the line or drag the whole line to adjust its position according to the actual scene.
3. **Optional:** You can select a lane line, and click 🗑 on the right of **Lane Line** to delete the lane. Or click + on the right of **Lane Line** to add a new lane line if the icon is available.

Note

The lane right borderline and trigger line cannot be deleted.

4. Click + on the right of **Incident Area**, and click the left button of the mouse to draw a rectangular or polygonal frame, and then click the right button of the mouse to save the area.
5. **Optional:** You can select an area, and click 🗑 on the right of **Incident Area** to delete the area. Or click + on the right of **Incident Area** to add a new area.



Lane Line:
Set based on the actual lane line positions, as shown in the figure.

Triggering Line:
It is recommended to set at the lower 1/3 of the image to determine the capture position of the checkpoint, as shown in the figure.

Figure 4-5 Draw Lane Lines and Incident Areas

6. Click **Save**.

4.3 Set Data Collection

The device supports to detect the traffic flow, POS, and other information.

Steps

1. Go to **Configuration → Capture → Application Mode** .
2. Select **Trigger Mode** as **Incident Detection**.
3. Click **Data Collection**.
4. Set the parameters according to the instructions below, and click **Save**.

4.3.1 Set Linked Lane Parameters

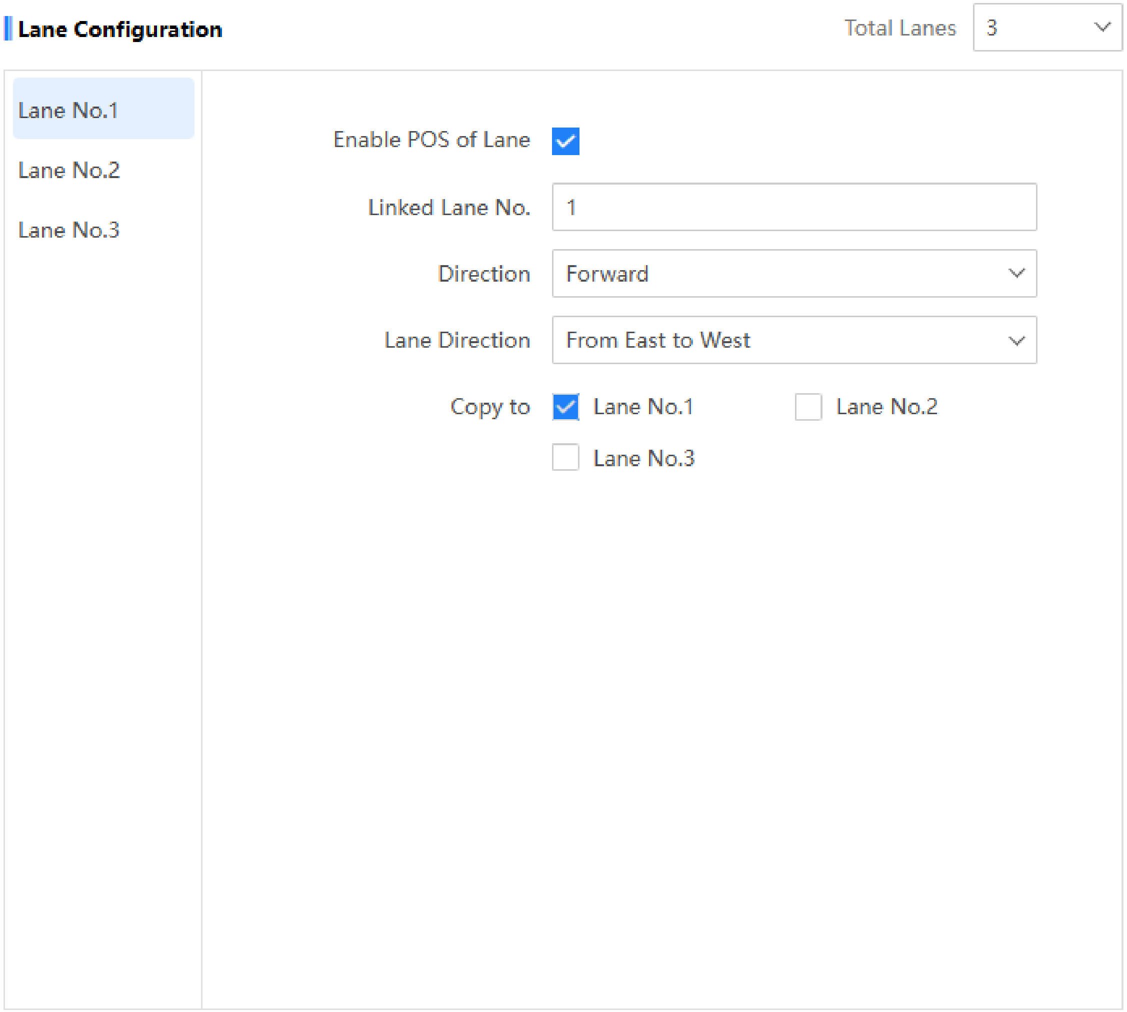
You can set the properties and parameters of the linked lanes.

Steps

Note

The linked lane parameters vary with different models. The actual device prevails.

1. Click **Lane Configuration**.
2. Select **Total Lanes**.
3. Select a lane No. to set the lane parameters.



Lane Configuration

Total Lanes: 3

Lane No.1

Lane No.2

Lane No.3

Enable POS of Lane ☑

Linked Lane No. 1

Direction: Forward

Lane Direction: From East to West

Copy to ☑ Lane No.1 □ Lane No.2 □ Lane No.3

Figure 4-6 Set Lane Parameters

Enable POS of Lane

Check it to enable the POS information (feature information) collection of the lane.

Linked Lane No.

The device will number the lane in ascending order from left to right automatically. The lane No. will be marked in the capture pictures and alarm information.

Direction

If you select **Forward**, the targets from the approaching direction towards the device will be captured. If you select **Backward**, the targets from the leaving direction away from the device will be captured.

Lane Direction

The guidance direction of the lane.

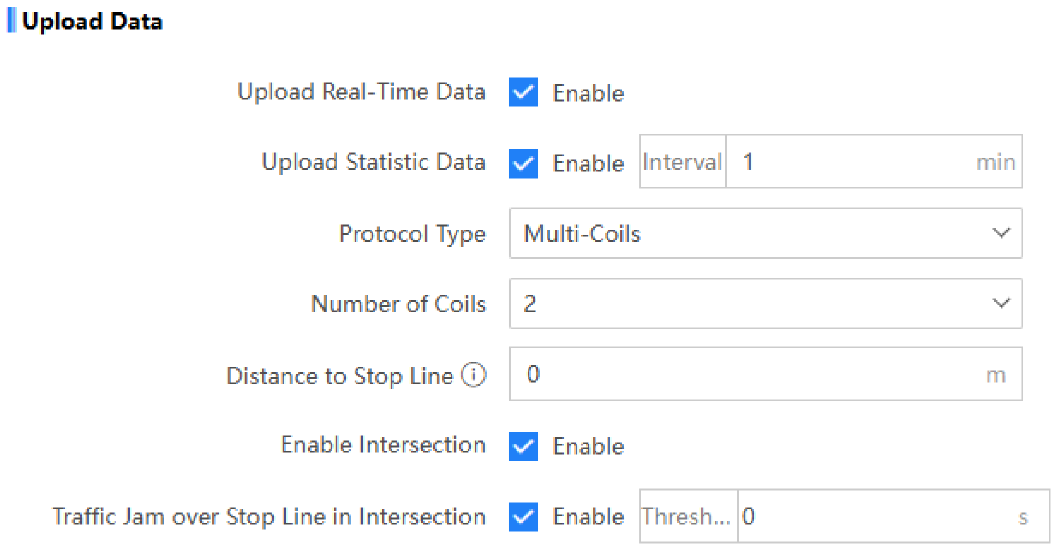
4. **Optional:** Check the other lane(s) to copy the same settings.

5. Click **Save**.

4.3.2 Set Traffic Flow Detection

Steps

1. Click **Traffic Flow Detection**.



Upload Data

Upload Real-Time Data ☑ Enable

Upload Statistic Data ☑ Enable Interval 1 min

Protocol Type Multi-Coils

Number of Coils 2

Distance to Stop Line ⓘ 0 m

Enable Intersection ☑ Enable

Traffic Jam over Stop Line in Intersection ☑ Enable Thresh... 0 s

Figure 4-7 Set Traffic Flow Detection

2. Set the data upload parameters.

Note

The supported functions vary with different models. The actual device prevails.

Upload Real-Time Data

The device will upload the real-time data to the server. The real-time data include road status, time, lane No., entrance/exit status, instantaneous speed, space headway, time headway, congestion traffic flow, driving direction, queue length, congestion level, and intersection dedicated data such as the signals when leaving the left turn line, right turn line, going straight line, and stop line at intersections (only supported for multi-coils protocol).

Upload Statistic Data

The device will upload the statistic data to the server according to the set **Interval**. The statistic data include lane No., traffic, average speed, traffic state, lane queue length, time interval of vehicle head, headway distance, lane space occupancy, lane time occupancy, average delay, and average number of stops.

Protocol Type

Unicoil

One coil for each lane.

Double Coil

Two coils for each lane.

Multi-Coils

Multi-coils for each lane. Select **Number of Coils**.

Distance to Stop Line

It is the distance from the device blind spot to the stop line at the intersection.

Enable Intersection

If you select **Protocol Type** as **Multi-Coils**, you can enable intersection and the scene will be an intersection with a stop line, a left turn border line, and a right turn border line.

Traffic Jam over Stop Line in Intersection

In multi-coils protocol, if you enable intersection, you can enable the function to detect the traffic jam at intersection, and set **Threshold**. When the vehicle queue over the stop line has lasted for the set threshold, it is regarded as traffic jam over stop line at intersection.

3. Draw lane lines and virtual coil areas.
   1) Refer to the drawing guide below the live view image on the interface. The left drawing guide is applicable to the scene with an intersection in multi-coils protocol. The right drawing guide is applicable to the scene without an intersection.
   2) Select the default lines and coils, and adjust their positions and shapes according to the actual scene.
   3) **Optional:** You can select a lane line, and click 🗑 on the right of **Lane Line** to delete the lane. Or click + on the right of **Lane Line** to add a new lane line if the icon is available.

   Note

   The lane right borderline and trigger line cannot be deleted.

   4) **Optional:** If you want to redraw the coil areas, you can select the default coil on the live view image, and click 🗑 on the right of **Coil** to delete it. Then click + ⌄ on the right of **Coil**. Select the corresponding coil, and click the left button of the mouse to draw a rectangular or polygonal frame, and then click the right button of the mouse to save the coil area. You can enable **Aided Line Drawing with Virtual Coil** to generate the coils automatically.

   Note

   - It is recommended that the virtual coil height is half of the small-sized vehicle length and the width is the lane width.
   - The virtual coils should be set at the positions where the radar and video can both detect.

   5) **Optional:** You can click 🔍 , and drag the mouse on the live view image to zoom the area in. Click the icon again to exit from digital zoom.

Note

The digital zoom function is only available after you download the plug-in.

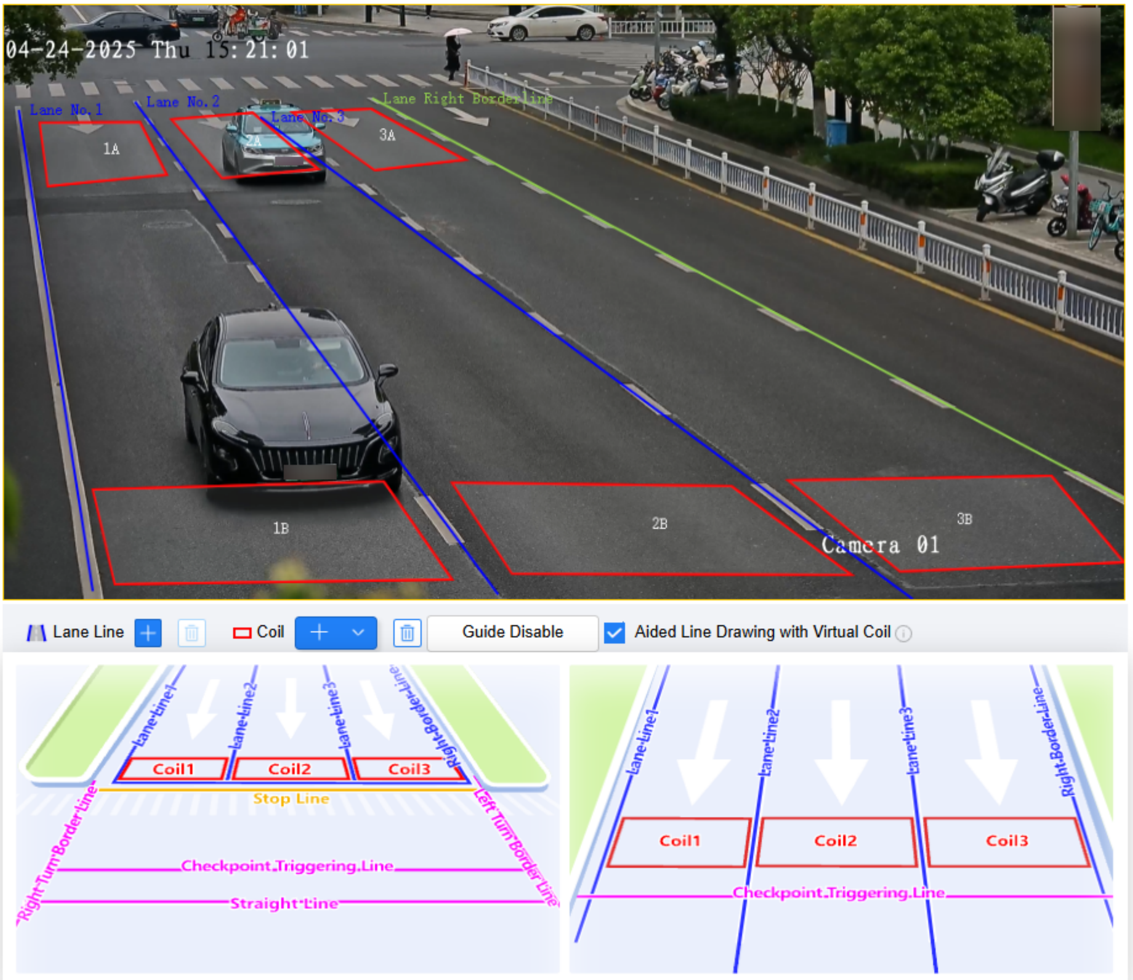


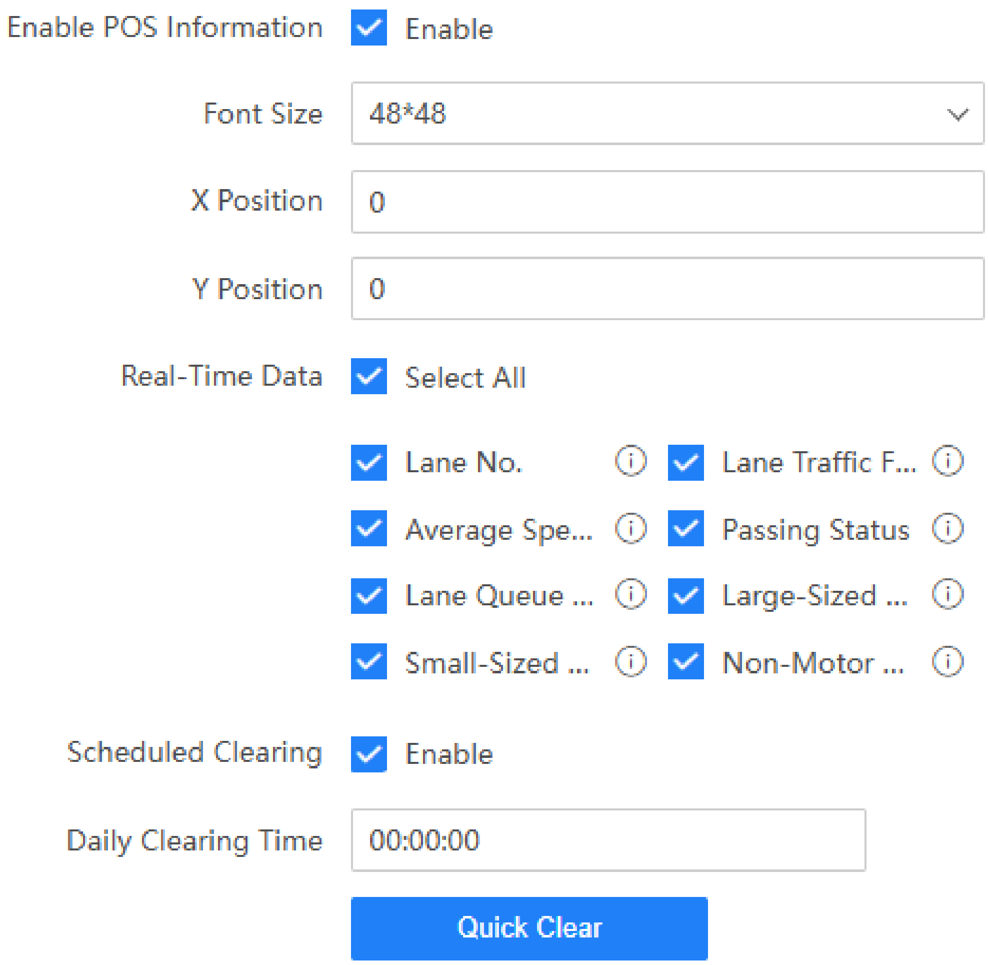
Figure 4-8 Draw Lane Lines and Virtual Coils Areas

4. Click **Save**.

4.3.3 Set Traffic Flow Information Overlay

Steps

1. Click **Overlay Traffic Flow Info.**



Enable POS Information ☑ Enable

Font Size 48*48

X Position 0

Y Position 0

Real-Time Data ☑ Select All

☑ Lane No. ⓘ ☑ Lane Traffic F... ⓘ

☑ Average Spe... ⓘ ☑ Passing Status ⓘ

☑ Lane Queue ... ⓘ ☑ Large-Sized ... ⓘ

☑ Small-Sized ... ⓘ ☑ Non-Motor ... ⓘ

Scheduled Clearing ☑ Enable

Daily Clearing Time 00:00:00

Figure 4-9 Set Traffic Flow Information Overlay

2. Set the information overlay.

Enable POS Information

Check it to overlay the feature information on the video stream and display on the live view image.

Font Size

Select the font size for the overlaid information.

X/Y Position

Enter **X Position** and **Y Position** to display on the image.

Real-Time Data

Select the real-time data to overlay on the image.

3. **Optional:** Clear the traffic flow data if needed.
   - Click **Quick Clear** to clear all the traffic flow data quickly.

- If you want to clear the traffic flow data at the fixed time daily, enable **Scheduled Clearing** and set **Daily Clearing Time**.

4. Click **Save**.

4.4 Set Enclosed Area Speeding

The device supports target speed detection in an enclosed area, speed information display on the connected screen, and incident detection and capture in the scenes of enclosed area main roads, curves, and entrances and exits of parking lots, in which speeding may easily to happen.

Steps

1. Go to **Configuration → Capture → Application Mode** .
2. Select **Trigger Mode** as **Enclosed Area Speeding**.
3. Set the parameters according to the instructions below, and click **Save**.

4.4.1 Set Linked Lane Parameters

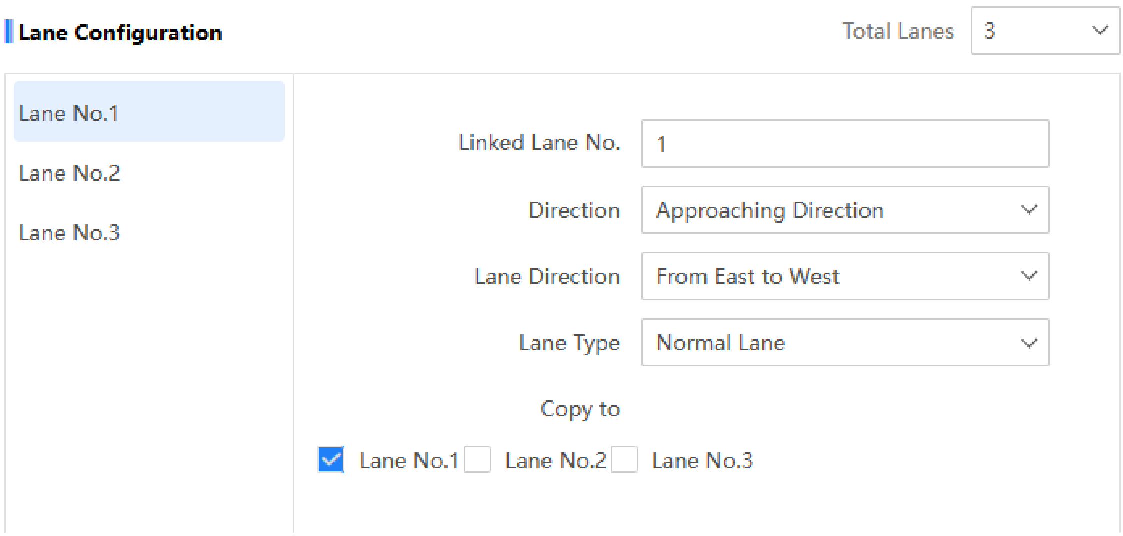
You can set the properties and parameters of the linked lanes.

Steps

Note

The linked lane parameters vary with different models. The actual device prevails.

1. Click **Lane Configuration**.
2. Select **Total Lanes**.
3. Select a lane No. to set the lane parameters.



Lane Configuration

Total Lanes: 3

Lane No.1
Lane No.2
Lane No.3

Linked Lane No.: 1

Direction: Approaching Direction

Lane Direction: From East to West

Lane Type: Normal Lane

Copy to

☑ Lane No.1 □ Lane No.2 □ Lane No.3

Figure 4-10 Set Lane Parameters

Linked Lane No.

The device will number the lane in ascending order from left to right automatically. The lane No. will be marked in the capture pictures and alarm information.

Direction

If you select **Approaching Direction**, the targets from the approaching direction towards the device will be captured. If you select **Leaving Direction**, the targets from the leaving direction away from the device will be captured.

Lane Direction

The guidance direction of the lane.

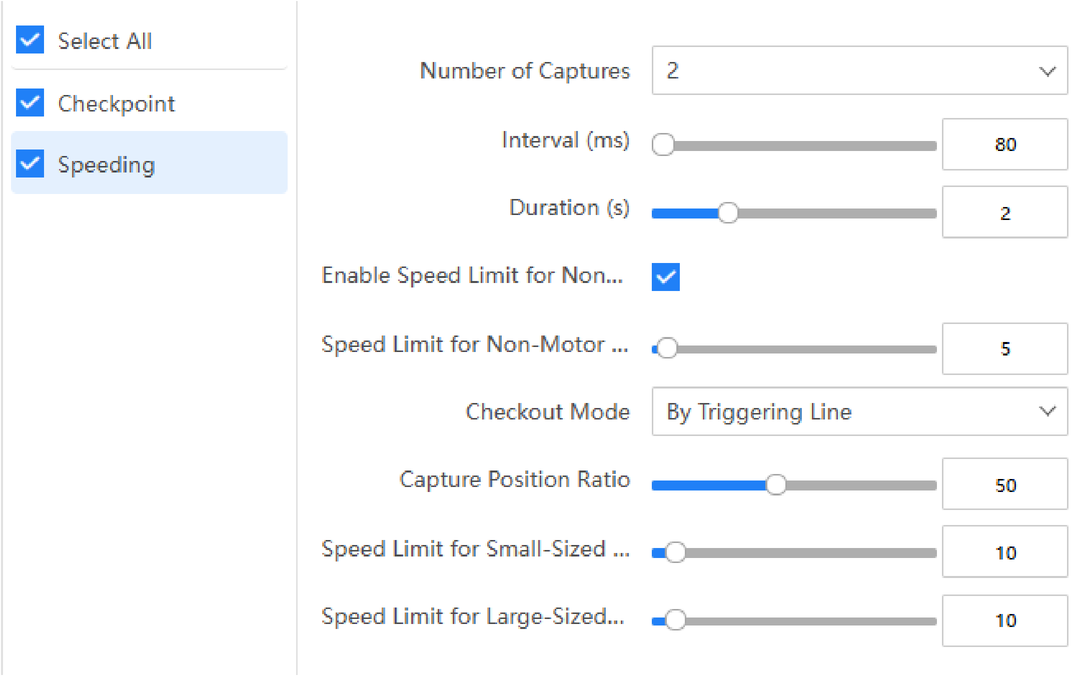
Lane Type

Select the lane type according to its usage.

4. **Optional:** Check the other lane(s) to copy the same settings.
5. Click **Save**.

4.4.2 Set Violation Incident

The device can capture pictures of the targets passing the checkpoint in the linked lanes according to the set rules.



☑ Select All

☑ Checkpoint

☑ Speeding

Number of Captures: 2

Interval (ms): 80

Duration (s): 2

Enable Speed Limit for Non...: ☑

Speed Limit for Non-Motor ...: 5

Checkout Mode: By Triggering Line

Capture Position Ratio: 50

Speed Limit for Small-Sized ...: 10

Speed Limit for Large-Sized...: 10

Figure 4-11 Set Violation Incident

Table 4-3 Incident Type Description

Incident Type	Parameters Description
Checkpoint	Check it and select the number of captured picture(s). Select **Capture Type**.
Speeding	The motor or non-motor vehicle is driven in the speed larger than the max. speed limit of the lane. Check it and select the number of captured picture(s). Set the parameters. • **Interval**: The interval between two captures. • **Enable Speed Limit for Non-Motor Vehicle**: Check it to enable the speeding capture for the non-motor vehicles. Set **Speed Limit for Non-Motor Vehicle**. • **Checkout Mode**: If you select **By Triggering Line**, when the vehicle passes over the triggering line and the passing ratio is larger than the set **Capture Position Ratio**, speeding capture will be triggered. If you select **By Duration**, when the speeding incident lasts for more than the set **Duration**, speeding capture will be triggered. • **Speed Limit for Small/Large-Sized Vehicle**: The max. speeds for the small-sized and large-sized vehicles respectively. When the vehicle speed exceeds the value, speeding capture will be triggered.

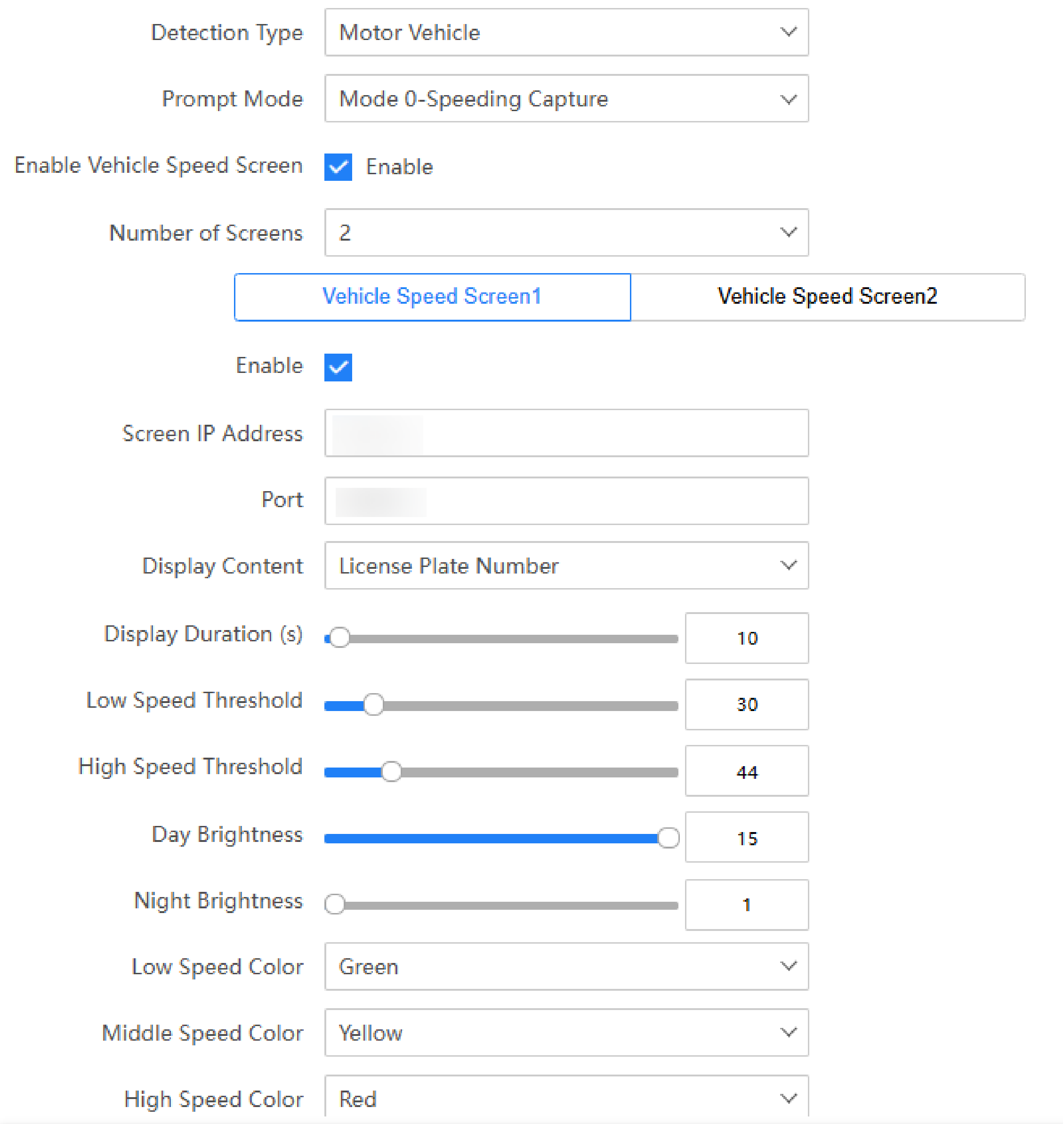
4.4.3 Set Speed Detection

Set speed detection and connected vehicle speed screen parameters.

Before You Start
The vehicle speed screen has been connected to the device.

Steps

1. Click **Speed Detection**.
2. Select **Detection Type**.
3. Select **Prompt Mode** and set corresponding parameters.



Detection Type: Motor Vehicle

Prompt Mode: Mode 0-Speeding Capture

Enable Vehicle Speed Screen: ☑ Enable

Number of Screens: 2

Enable: ☑

Screen IP Address: [redacted]

Port: [redacted]

Display Content: License Plate Number

Display Duration (s): 10

Low Speed Threshold: 30

High Speed Threshold: 44

Day Brightness: 15

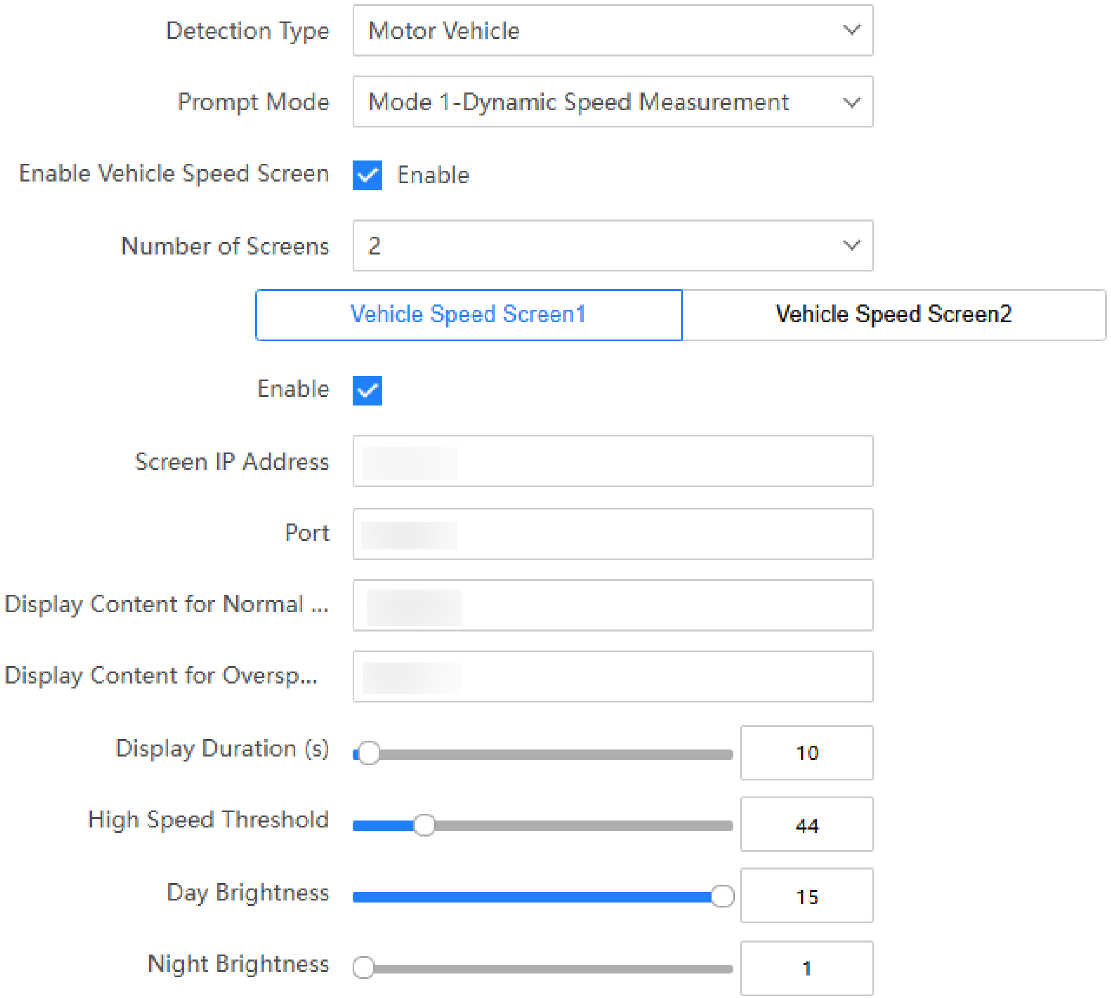
Night Brightness: 1

Low Speed Color: Green

Middle Speed Color: Yellow

High Speed Color: Red

Figure 4-12 Mode 0-Speeding Capture



Detection Type: Motor Vehicle

Prompt Mode: Mode 1-Dynamic Speed Measurement

Enable Vehicle Speed Screen: ☑ Enable

Number of Screens: 2

Enable: ☑

Screen IP Address:

Port:

Display Content for Normal ...:

Display Content for Oversp...:

Display Duration (s): 10

High Speed Threshold: 44

Day Brightness: 15

Night Brightness: 1

Figure 4-13 Mode 1-Dynamic Speed Measurement

Table 4-4 Prompt Mode Description

Prompt Mode	Parameters Description
Mode 0-Speeding Capture	To capture the speeding violation and upload the license plate number and speed information. Check **Enable Vehicle Speed Screen**. Select **Number of Screens**, enable the screen, and set the corresponding parameters. • **Screen IP Address/Port**: The IP address and port of the vehicle speed screen. • **Display Content**: Select the display content on the screen. If you select **Custom Content**, set **Display Content for Normal Speed** and **Display Content for Overspeed** respectively.

Prompt Mode	Parameters Description
	• **Display Duration**: Set the display duration of the content on the screen. • **Low/High Speed Threshold**: When the target speed is higher than the high speed threshold, speeding capture will be triggered. • **Day/Night Brightness**: Set the brightness of the screen at daytime and night. • **Low/Middle/High Speed Color**: Set **Low Speed Color** of the display content for the speeds lower than the set **Low Speed Threshold**. Set **Middle Speed Color** of the display content for the speeds between the set **Low Speed Threshold** and **High Speed Threshold**. Set **High Speed Color** of the display content for the speeds higher than the set **High Speed Color**.
Mode 1-Dynamic Speed Measurement	When the target appears in the radar detection range, the screen will display the speed of the target. When multi-targets are detected, the speed of the nearest target will be displayed. If the speed is higher than the set **High Speed Threshold**, the screen will display the set **Display Content for Overspeed** in red color. If the speed is not higher than the set **High Speed Threshold**, the screen will display the set **Display Content for Normal Speed** in green color. The color of the speed and display content is consistent. If the target speed is still larger than the set **High Speed Threshold** when passing the capture trigger line, the license plate number will be displayed too. Set the corresponding parameters. You can refer to the parameters description in Mode 0.

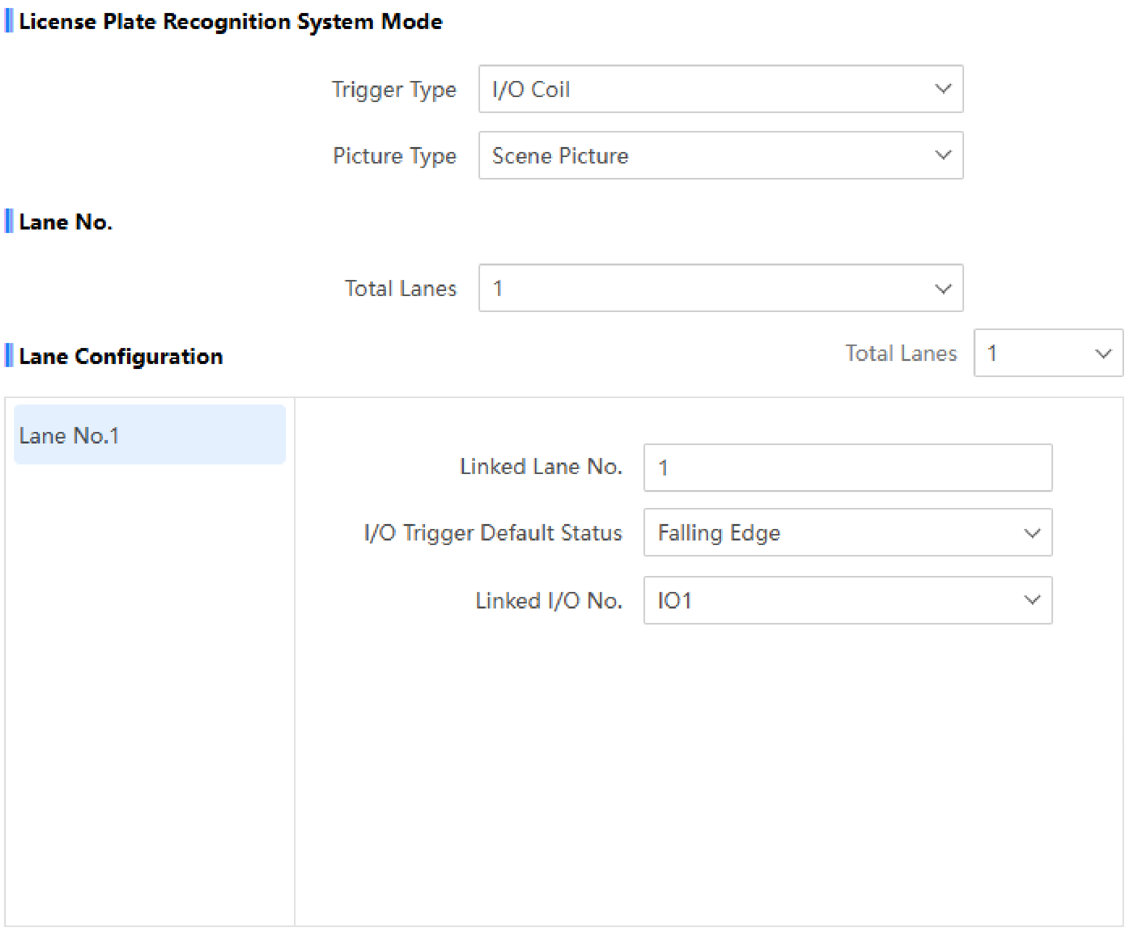
4. Click **Save**.

4.5 Set License Plate Recognition System Capture

If you want to trigger capture of the passing vehicles and recognize the license plate numbers, set license plate recognition system capture.

Steps

1. Go to **Configuration → Capture → Application Mode** .
2. Select **Trigger Mode** as **License Plate Recognition System**.



License Plate Recognition System Mode

Trigger Type: I/O Coil

Picture Type: Scene Picture

Lane No.

Total Lanes: 1

Lane Configuration

Total Lanes: 1

Lane No.1

Linked Lane No.: 1

I/O Trigger Default Status: Falling Edge

Linked I/O No.: IO1

Figure 4-14 Set License Plate Recognition System

3. Select **Trigger Type**.

Video Detection

The passing vehicles will be recognized via videos. The **Capture Type** is recommended as **Strobe Light Mode**.

I/O Coil

Select it when the device has been connected to I/O signal.

Note

The trigger types vary with different models. The actual device prevails.

4. Select **Picture Type**.

Scene Picture

Only one passing vehicle picture will be output.

5. Select **Total Lanes**. Only one lane is supported.
6. Select the lane No. to set the lane parameters.

Linked Lane No.

The device will number the lane in ascending order from left to right automatically. The lane No. will be marked in the capture pictures and alarm information.

I/O Trigger Default Status

It is available if you select **Trigger Type** as **I/O Coil**. Capture is triggered according to the level signal status. If you select **Falling Edge**, the device will trigger capture at the moment that the high level falls to low level. If you select **Rising Edge**, the device will trigger capture at the moment that the low level rises to high level.

Linked I/O No.

It is available if you select **Trigger Type** as **I/O Coil**. When the coil detects that there is a vehicle passing, a rising or falling edge signal is sent to the linked I/O of the device to trigger capture.

7. Draw lane lines.

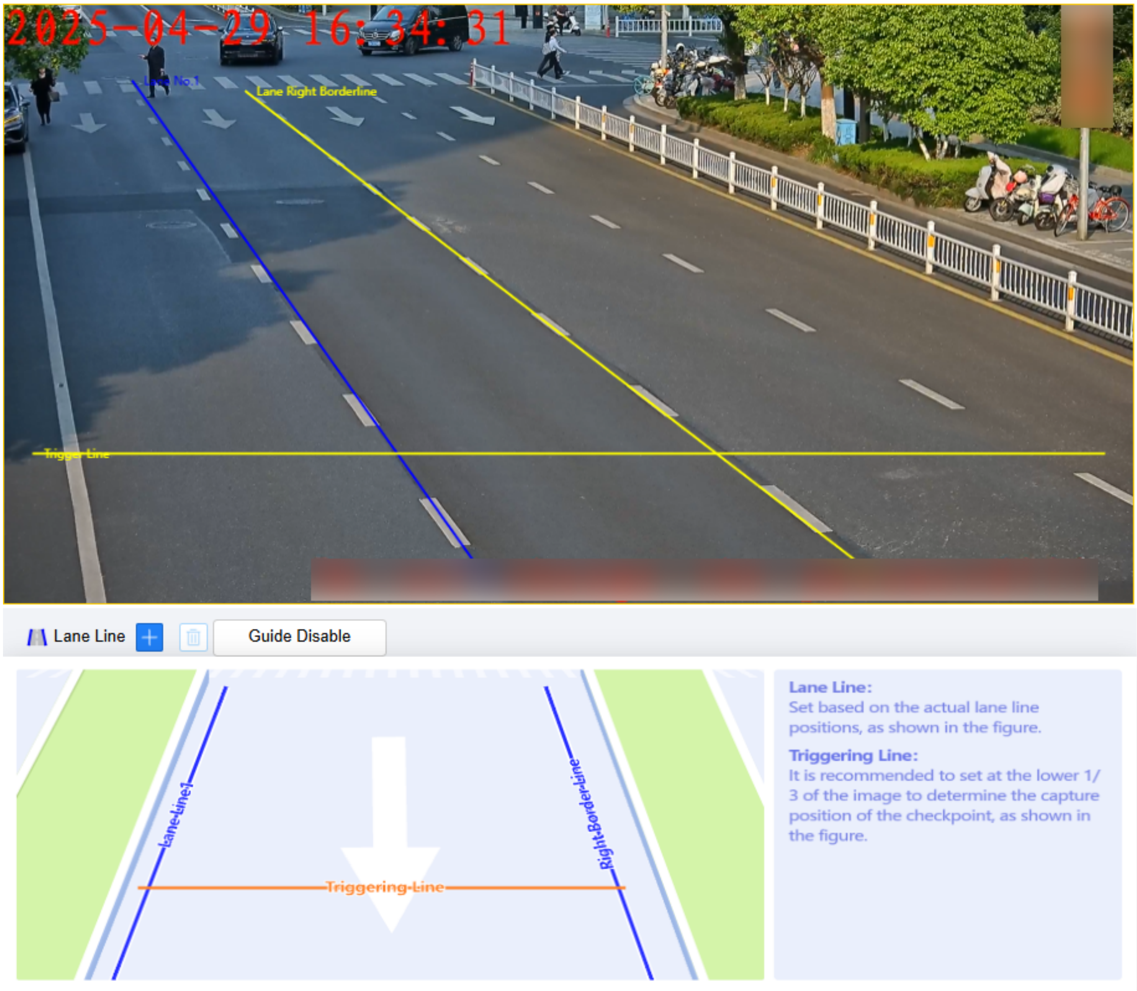
1) Refer to the drawing guide below the live view image on the interface.
2) Select the default lane line, right border line, and trigger line, and drag the two end points of the line or drag the whole line to adjust its position according to the actual scene.
3) **Optional:** You can select a lane line, and click 🗑 to delete the lane. Or click + to add a new lane line if the icon is available.

Note

The lane right borderline and trigger line cannot be deleted.

Note

It is recommended to draw the trigger line at the position which is 1/3 to 1/4 of the lane line. The license plate pixel should be between 120 to 180 at the capture position.



Lane Line:
Set based on the actual lane line positions, as shown in the figure.

Triggering Line:
It is recommended to set at the lower 1/3 of the image to determine the capture position of the checkpoint, as shown in the figure.

Figure 4-15 Draw Lane Line

8. Click **Save**.

Chapter 5 Entrance and Exit Configuration

If a barrier gate has been connected to the device, you can link barrier gate to realize the control and management of the vehicles at the entrance or exit.

Note

The function is only supported for the application modes of smart mode and license plate recognition system. The actual device prevails.

5.1 Set Allowlist and Blocklist

Set allowlist and blocklist if you want to control the passing vehicles at the entrance or exit via the barrier gate.

Before You Start

- Connect the barrier gate to the relay output interface of the device.
- Install the storage card, and ensure the storage status is normal.

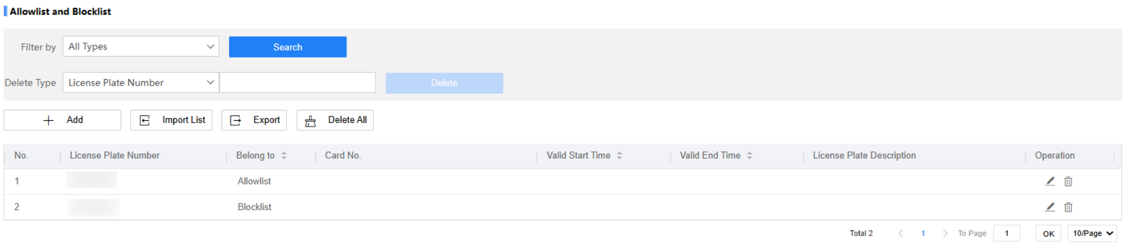
Steps

1. Go to **Configuration → Capture → Entrance and Exit → Allowlist and Blocklist** .
2. Add an allowlist or blocklist.
   1) Click **Add**.
   2) Set **License Plate Number** and **Card No.**, and select the list type.
   3) **Optional:** If you want to control allowlist vehicles during fixed time period, enable **Time Settings**, and set the effective start time and end time.
   4) Click **OK**.

   Note

   Wait for 15 minutes to let the added allowlist or blocklist write into the storage. Do not reboot the device during the process.

   The information of the added vehicles in the allowlist or blocklist will be listed below.



Allowlist and Blocklist

Filter by: All Types

Delete Type: License Plate Number

No.	License Plate Number	Belong to	Card No.	Valid Start Time	Valid End Time	License Plate Description	Operation
1	[redacted]	Allowlist					
2	[redacted]	Blocklist					

Total 2 < 1 > To Page 1 OK 10/Page

Figure 5-1 Set Allowlist and Blocklist

3. You can search, modify, delete, import, or export the allowlist and blocklist.

Search Select the search type, or enter the keywords. Click **Search**. The searched vehicle information will be listed below.

Modify Select an item from the list, and click ✎ . Modify the information, and click **OK**.

Delete

- Select the delete type, or enter the keywords. Click **Delete** to delete the lists of the same type.
- Select an item from the list, and click 🗑 to delete the item.
- Click **Delete All** to delete all the lists.

Import

a. Click **Import List**.
b. Click **Download Template**, and save the template.
c. Open the template, edit the information, and save it.
d. Click **Import List** again.
e. Click **Browse** to select the edited template.
f. Click **Import** to import the information to the device.

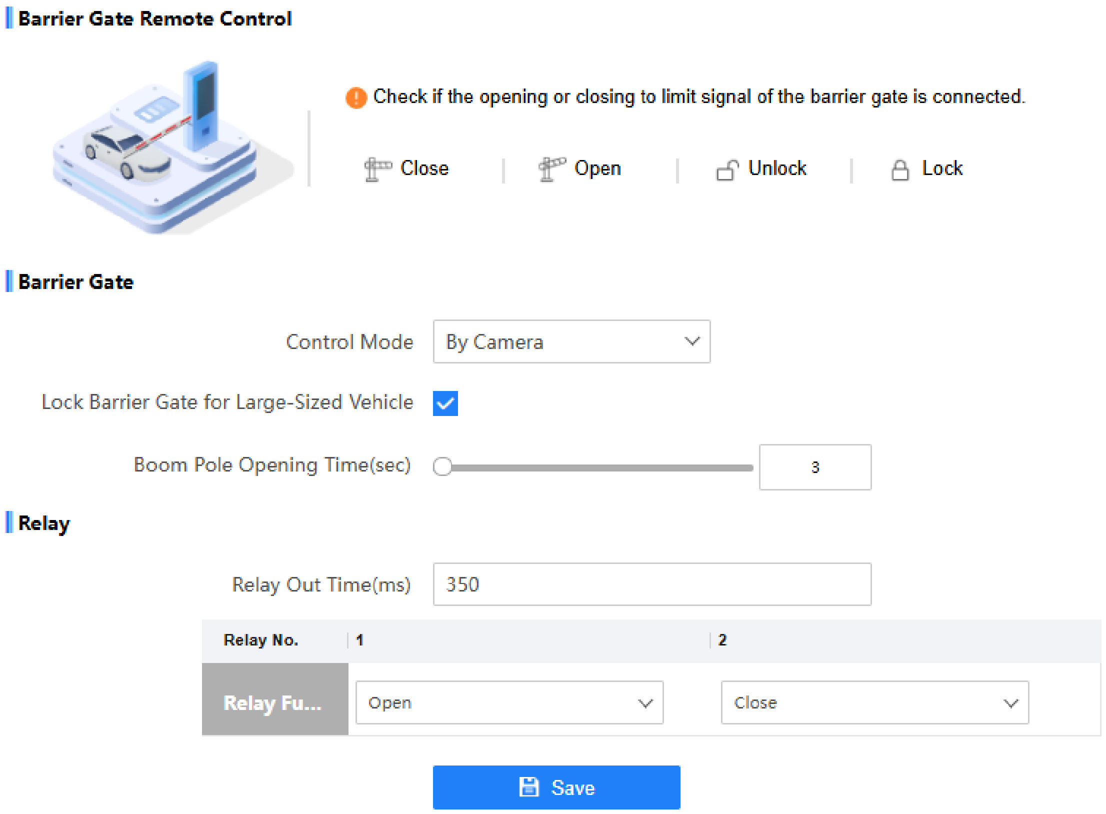
Export Click **Export**, and the list will be saved to the default downloading directory of the browser in the format of .xls.

5.2 Control Barrier Gate

Link the barrier gate to realize the control and management of the vehicles at the entrance or exit.

Steps

1. Go to **Configuration → Capture → Entrance and Exit → Barrier Gate** .



Barrier Gate Remote Control

Check if the opening or closing to limit signal of the barrier gate is connected.

Barrier Gate

Control Mode: By Camera

Lock Barrier Gate for Large-Sized Vehicle ☑

Boom Pole Opening Time(sec): 3

Relay

Relay Out Time(ms): 350

Relay No.	1	2
Relay Fu...	Open	Close

Figure 5-2 Control Barrier Gate

2. Set **Barrier Gate** parameters.

Control Mode

- Select **By Camera** in single camera scene (no control software) and allowlist scene in which the camera controls the barrier gate in advance according to the set passing rules in **Pass Control**.
- Select **By Platform** in the scene in which the entry permissions are controlled by the software.
- Select **By Mixed**, and the platform control and camera control are effective simultaneously. It is applicable to the scene in which different vehicle passing permissions are managed by software and camera. E.g., the software controls the passing of blocklist vehicles and temporary vehicles, and the camera controls the passing of allowlist vehicles and controls the barrier gate in advance for allowlist vehicles.

Lock Barrier Gate for Large-Sized Vehicle

Enable the function and set **Boom Pole Opening Time**. If a large-sized vehicle is passing, the barrier gate will be locked during the set time.

3. Set **Relay** parameters.

Relay Out Time

Alarms will be output during the set time.

Relay Function

Select the functions of corresponding relays. Relay 1 corresponds to the 1A and 1B of the terminal. Relay 2 corresponds to the 2A and 2B of the terminal.

4. **Optional:** Click **Close**, **Open**, **Unlock**, or **Lock** in **Barrier Gate Remote Control** to control the barrier gate remotely.

Note

The functions of remote control of barrier gate vary with different models. The actual device prevails.

5. Click **Save**.

5.3 Pass Control

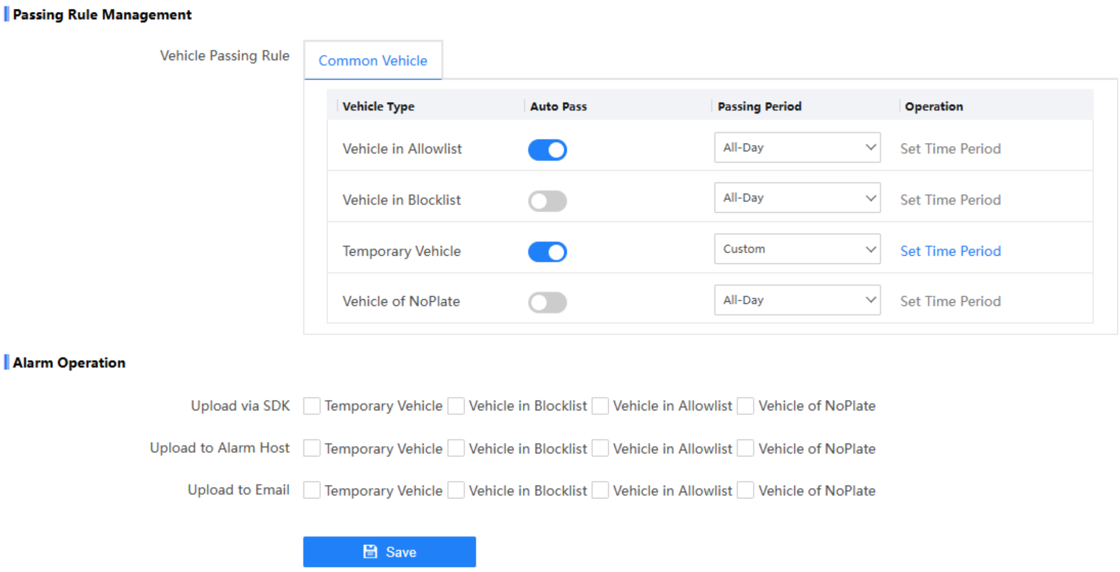
The camera can control the passing rules of different types of vehicles, and upload alarm information.

Before You Start

- Select the barrier gate control mode as **By Camera**. Refer to ***Control Barrier Gate*** for details.
- Set the allowlist and blocklist. Refer to ***Set Allowlist and Blocklist*** for details.

Steps

1. Go to **Configuration → Capture → Entrance and Exit → Pass Control** .



Passing Rule Management

Vehicle Passing Rule: Common Vehicle

Vehicle Type	Auto Pass	Passing Period	Operation
Vehicle in Allowlist	●	All-Day	Set Time Period
Vehicle in Blocklist	○	All-Day	Set Time Period
Temporary Vehicle	●	Custom	Set Time Period
Vehicle of NoPlate	○	All-Day	Set Time Period

Alarm Operation

Upload via SDK □ Temporary Vehicle □ Vehicle in Blocklist □ Vehicle in Allowlist □ Vehicle of NoPlate

Upload to Alarm Host □ Temporary Vehicle □ Vehicle in Blocklist □ Vehicle in Allowlist □ Vehicle of NoPlate

Upload to Email □ Temporary Vehicle □ Vehicle in Blocklist □ Vehicle in Allowlist □ Vehicle of NoPlate

Figure 5-3 Pass Control

2. Set the passing rules for different types of vehicles.

1) Enable **Auto Pass** or not for vehicles in allowlist, vehicles in blocklist, temporary vehicles, and vehicles of no plates.

2) Set **Passing Period**.

All-Day

The corresponding type of vehicles can pass automatically all day.

Custom

The corresponding type of vehicles can pass automatically at the set time period. Click **Set Time Period** to set the auto passing time period of each day. Up to 5 passing periods can be set for each day. The setting method is same with setting capture schedule. Refer to ***Set Capture Schedule*** for details.

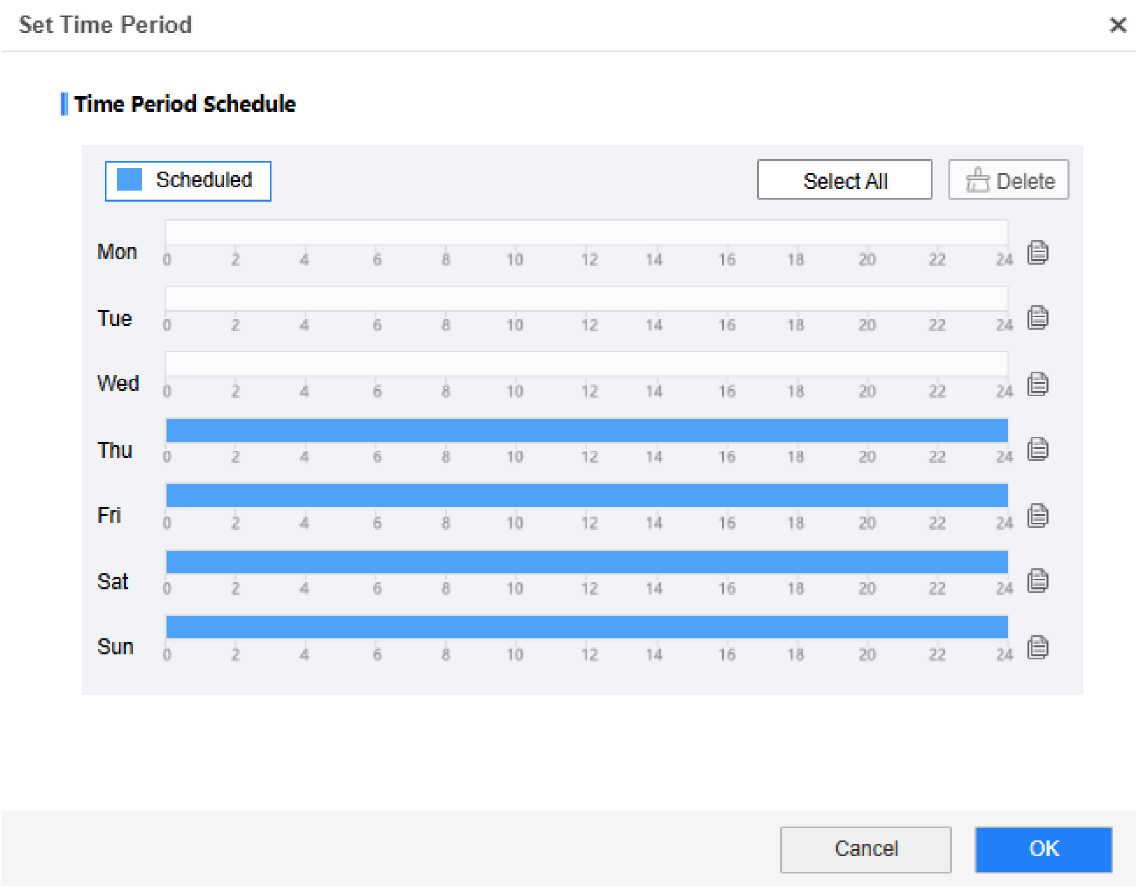


Figure 5-4 Set Custom Auto Passing Time Period

3. Select the vehicle type(s) of which the alarm information will be uploaded via SDK, to the alarm host, or to the email.

Upload via SDK

If the device has been connected to the platform, you can arm and upload the vehicle information to the arming terminal via SDK.

Upload to Alarm Host

If the device has been connected to the alarm device, when the barrier gate is open, the alarm device will be triggered to alarm.

Upload to Email

When the email is enabled and set, the device will send an email notification to all designated receivers if an alarm event is detected for the selected vehicles.

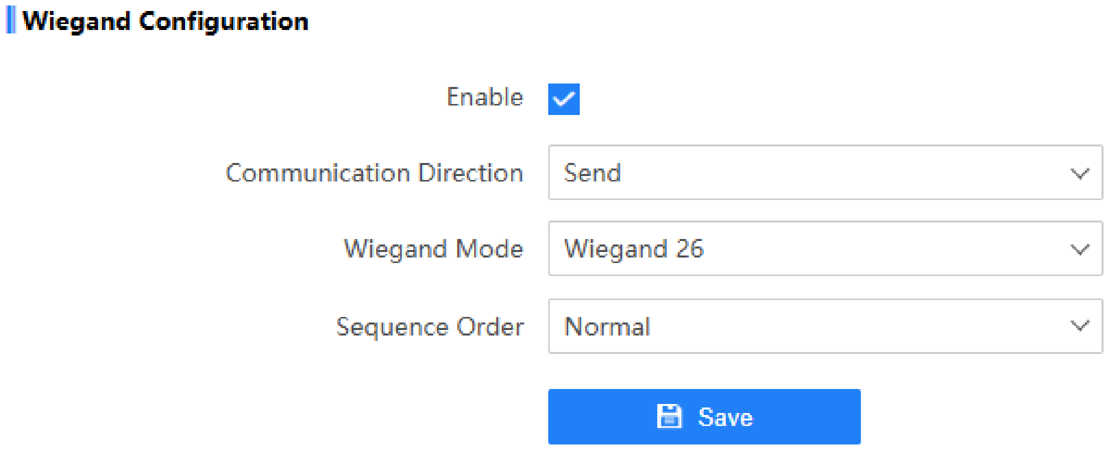
4. Click **Save**.

5.4 Set Wiegand Parameters

The device can get access to the access control system or other system supporting Wiegand protocols to send data in the entrance and exit scenes.

Steps

1. Go to **Configuration → Capture → Entrance and Exit → Wiegand Parameters** .
2. Check **Enable**.



Wiegand Configuration

Enable ☑

Communication Direction: Send

Wiegand Mode: Wiegand 26

Sequence Order: Normal

Figure 5-5 Set Wiegand Parameters

3. Select **Communication Direction**.

Send

The barrier gate can be connected to the device via Wiegand 26 or Wiegand 34 mode.

4. Select **Wiegand Mode**.

Wiegand 26

It is applicable to all the access control projects. The device will get the card No. (pure numbers with no more than 8 digits) from the allowlist and blocklist related to the captured license plate number and send the card No. to the access control system or other system supporting Wiegand protocols via Wiegand 26 protocol.

Wiegand 34

It is applicable to all the access control projects. The device will get the card No. (pure numbers with no more than 10 digits) from the allowlist and blocklist related to the captured license plate number and send the card No. to the access control system or other system supporting Wiegand protocols via Wiegand 34 protocol.

Wiegand 26-SHA-1

It is a data transmission format integrating Wiegand protocol and SHA-1 hash algorithm. This format increases SHA-1 hash value based on the standard Wiegand 26-bit data frame to raise the data security and integrity.

5. Select **Sequence Order**.

Normal

The data are sent in the normal order.

Reverse

The data are sent in the reversed order.

6. Click **Save**.

Chapter 6 Capture Parameters Configuration

6.1 Set License Plate Recognition Parameters

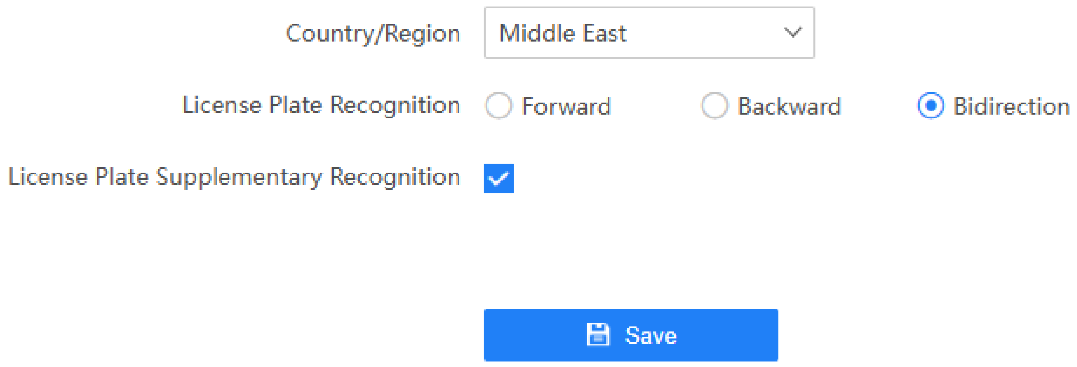
When there are vehicles of different types passing from different directions, set the license plate recognition parameters.

Steps

Note

The supported parameters vary with different models. The actual device prevails.

1. Go to **Configuration → Capture → Capture Parameters → LPR Parameters** .



Country/Region: Middle East

License Plate Recognition: ○ Forward ○ Backward ● Bidirection

License Plate Supplementary Recognition: ☑

Figure 6-1 Set License Plate Recognition Parameters

2. Set **Country/Region** according to the actual needs.
3. Select **License Plate Recognition**.
   - Select **Forward** when license plates of vehicles from the approaching direction need to be recognized.
   - Select **Backward** when license plates of vehicles from the leaving direction need to be recognized.
   - Select **Bidirection** when license plates of vehicles from both the approaching direction and the leaving direction need to be recognized.
4. **Optional:** Enable **License Plate Supplementary Recognition** to re-recognize the targets whose license plates are not recognized for the first time.
5. Click **Save**.

6.2 Set Supplement Light Parameters

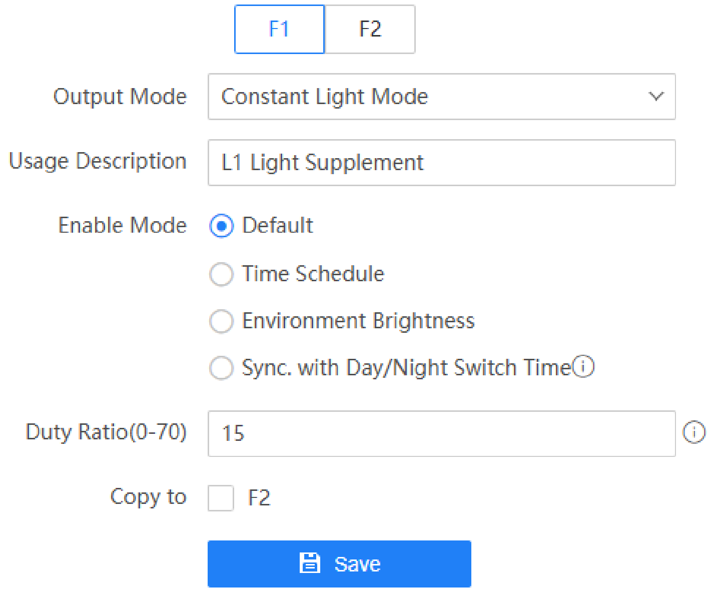
Supplement light can enhance the image stabilization and adjust the brightness and color temperature.

Steps

Note

- This chapter is only applicable to the device supporting supplement light.
- The supported parameters vary with different models. The actual device prevails.

1. Go to **Configuration → Capture → Capture Parameters → Supplement Light Parameters** .



Output Mode: Constant Light Mode

Usage Description: L1 Light Supplement

Enable Mode: ● Default ○ Time Schedule ○ Environment Brightness ○ Sync. with Day/Night Switch Time

Duty Ratio(0-70): 15

Copy to: □ F2

Figure 6-2 Set Supplement Light Parameters

2. Select the I/O and set the supplement light parameters.

Output Mode

Constant Light Mode

The constant light supplements light for the scene.

Usage Description

Enter the usage description of the supplement light.

Duty Ratio

It is the time occupation of the high level in a certain period. The higher the duty ratio, the brighter the light. High duty ratio will cut life span of the light.

3. Set the supplement light control mode.
   - Select **Default** to disable the supplement light.
   - Select **Time Schedule** when you want the supplement light to be enabled during a fixed time period. Set the start time and end time.
   - Select **Environment Brightness** when you want the supplement light to be controlled by detecting the surroundings brightness automatically. Set the brightness threshold. The higher the threshold is, the harder the supplement light can be enabled.

  - Select **Sync. with Day/Night Switch Time** to keep the day/night switch of the supplement light consistent with ICR.

4. **Optional:** Select other I/O(s) to copy the same settings.
5. Click **Save**.

6.3 Set Feature Recognition

Set the feature parameters for different targets if you need to detect the features of the corresponding targets.

Steps

Note

The parameters vary with different models. The actual device prevails.

1. Go to **Configuration → Capture → Capture Parameters → Feature Recognition Settings** .
2. Check the feature(s) that needed to be detected, and set the corresponding sensitivity if supported.
3. Click **Save**.

6.4 Set Target Picture Matting

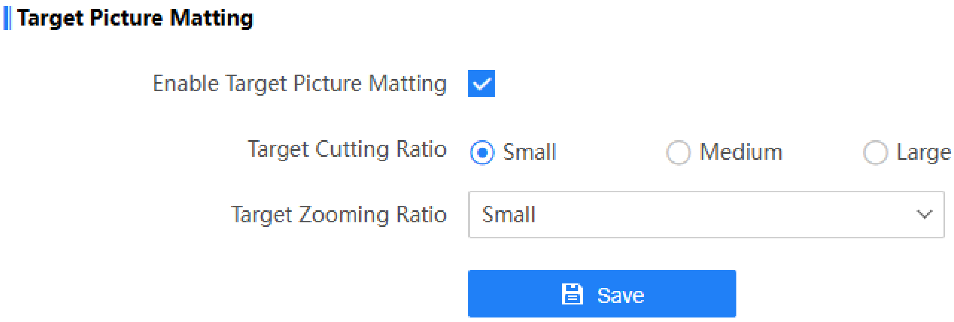
Set target picture matting first if you need to upload target pictures to the platform.

Steps

Note

The function varies with different models. The actual device prevails.

1. Go to **Configuration → Capture → Capture Parameters → Target Picture Matting** .
2. Check **Enable Target Picture Matting**.



Target Picture Matting

Enable Target Picture Matting ☑

Target Cutting Ratio ● Small ○ Medium ○ Large

Target Zooming Ratio Small

Figure 6-3 Set Target Picture Matting

3. Select **Target Cutting Ratio** to be small, medium, or large.

4. Set **Target Zooming Ratio**.
5. Click **Save**.

Result

If the device is level 1 armed, the matting pictures will be uploaded to this device directly.

6.5 Set Information Overlay

6.5.1 Set Single Picture Overlay

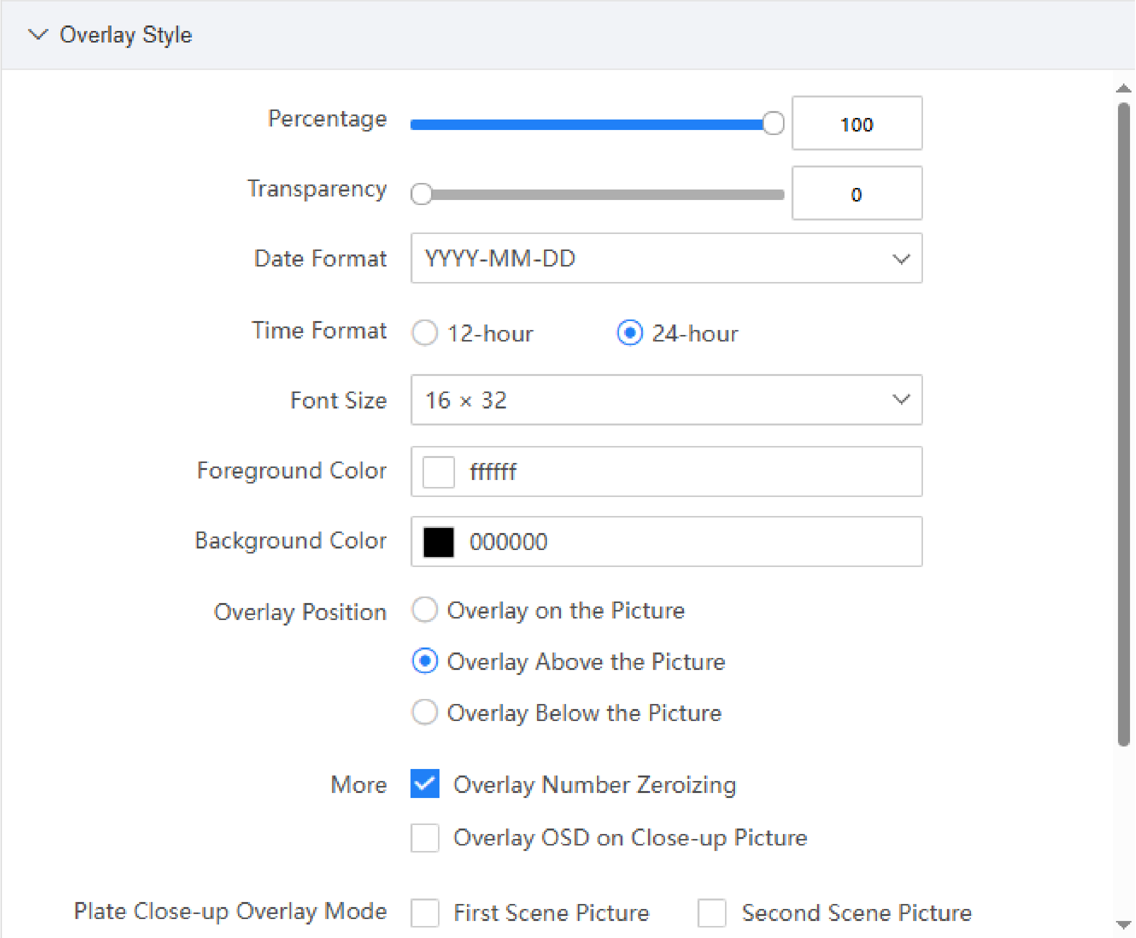
If you want to overlay information on the captured single pictures, set capture overlay.

Steps

Note

The supported parameters vary with different models. The actual device prevails.

1. Go to **Configuration → Capture → Capture Parameters → Capture Overlay Configuration** .
2. Click the single type.
3. Enable text overlay.
4. Set **Overlay Style**.



Overlay Style

Percentage 100

Transparency 0

Date Format YYYY-MM-DD

Time Format ○ 12-hour ● 24-hour

Font Size 16 × 32

Foreground Color ffffff

Background Color 000000

Overlay Position ○ Overlay on the Picture ● Overlay Above the Picture ○ Overlay Below the Picture

More ☑ Overlay Number Zeroizing □ Overlay OSD on Close-up Picture

Plate Close-up Overlay Mode □ First Scene Picture □ Second Scene Picture

Figure 6-4 Set Single Picture Overlay Style

Percentage

It is the percentage that the overlaid information occupies on the picture. For example, if you set the percentage to 50, the overlaid information in a row will occupy up to half of the image width, and the excess content will be overlaid from a new line.

Transparency

It is the condition of viewing the live view image through the overlaid information.

Overlay Number Zeroizing

When the overlaid number digits are smaller than the fixed digits, 0 will be overlaid before the overlaid number. E.g., the fixed digits for lane No. is 2. If the lane No. is 1, 01 will be overlaid on the picture.

Overlay OSD on Close-up Picture

Check it to overlay the OSD information on the close-up pictures.

Plate Close-up Overlay Mode

Select the picture type(s) to overlay the license plate close-up pictures. You can select multiple picture types. Please select one scene picture at least. Set **Plate Picture Close-Up Zooming Ratio** to adjust the close-up picture size.

Font Color Inversion

Enable the function to detect the gray level of the image overlaid position automatically. When the image color is dark, the overlaid characters will be displayed as white automatically. When the image color is light, the overlaid characters will be displayed as black automatically.

Capture Time Type

Select the time type to overlay information on the captured pictures.

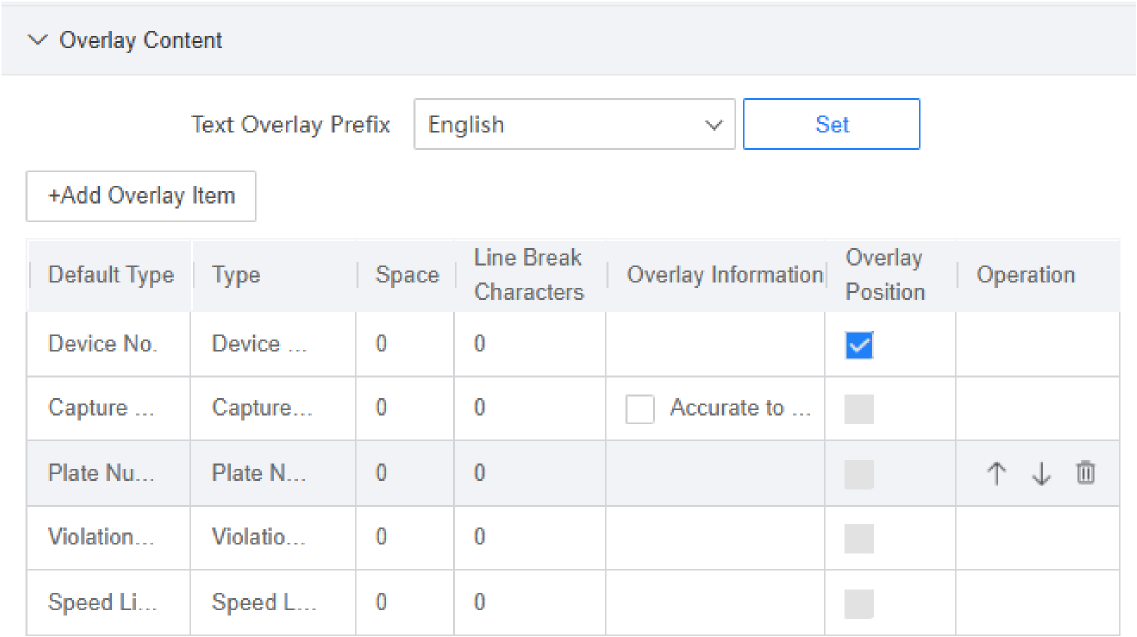
Picture Upload Time

The information will be overlaid when the captured picture starts to upload.

Picture Generation Time

The information will be overlaid when the captured picture is output.

5. Set **Overlay Content**.



Overlay Content

Text Overlay Prefix: English

Set

+Add Overlay Item

Default Type	Type	Space	Line Break Characters	Overlay Information	Overlay Position	Operation
Device No.	Device ...	0	0		☑	
Capture ...	Capture...	0	0	□ Accurate to ...	□	
Plate Nu...	Plate N...	0	0		□	↑ ↓ 🗑
Violation...	Violatio...	0	0		□	
Speed Li...	Speed L...	0	0		□	

Figure 6-5 Set Single Picture Overlay Content

1) Select **Text Overlay Prefix** language to overlay the information in corresponding language, and click **Set** to save.

Note

The supported languages depend on the selected LPR **Country/Region** in **Configuration → Capture → Capture Parameters → LPR Parameters** .

Result: You can edit the custom information name in the selected language.

2) Click **Add Overlay Item** to select the information to overlay, and click **OK**.

Note

The overlay information varies with different models. The actual device prevails.

3) Set the parameters below.

- **Default Type**: You can view the default overlay information name. If you have edited the name, you can refer to the default name for the definition.
- **Type**: You can edit a custom overlay information name.
- **Space**: Edit the number of space between the current information and the next one from 0 to 255. 0 means there is no space.
- **Line Break Characters**: Edit the number of characters from 0 to 100 between the current information line and the previous information line. 0 means no line break.
- **Overlay Information**: For some information types, you can edit the detailed information.
- **Overlay Position**: If you check it, the current information will be displayed from a new line.
- **Operation**: You can click ↑ / ↓ to adjust the display sequence of the overlay information, or click 🗑 to delete the item.

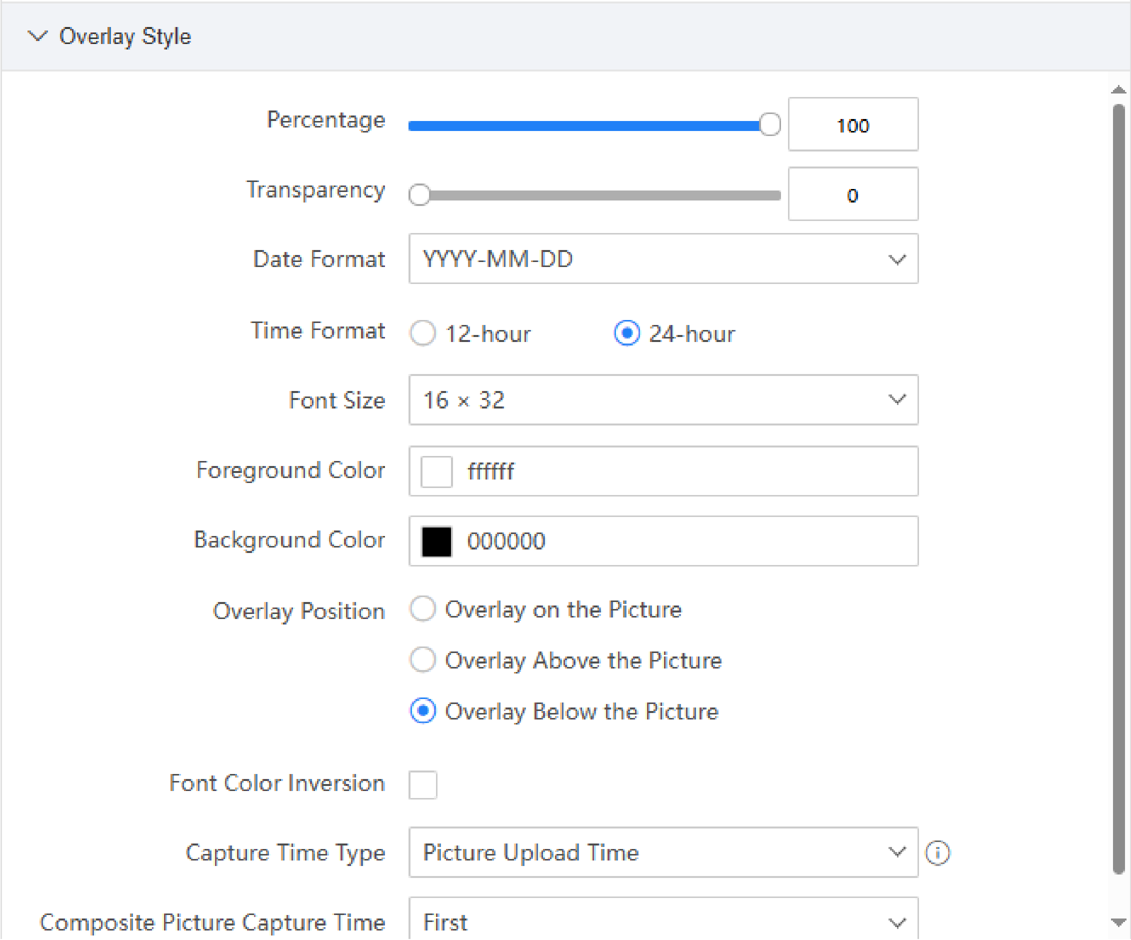
6. **Optional:** Check the other channel(s) to copy the same settings.
7. Click **Capture Test** to test the information overlay effect.
8. Click **Save**.

6.5.2 Set Composite Picture Overlay

If you want to overlay information on the composite pictures, set composite picture overlay.

Steps

1. Go to **Configuration → Capture → Capture Parameters → Capture Overlay Configuration** .
2. Click the composite type.
3. Enable text overlay.
4. Set **Overlay Style**.



Overlay Style

Percentage: 100

Transparency: 0

Date Format: YYYY-MM-DD

Time Format: ○ 12-hour ● 24-hour

Font Size: 16 × 32

Foreground Color: □ ffffff

Background Color: ■ 000000

Overlay Position:
○ Overlay on the Picture
○ Overlay Above the Picture
● Overlay Below the Picture

Font Color Inversion: □

Capture Time Type: Picture Upload Time ⓘ

Composite Picture Capture Time: First

Figure 6-6 Set Composite Picture Overlay Style

Percentage

It is the percentage that the overlaid information occupies on the picture. For example, if you set the percentage to 50, the overlaid information in a row will occupy up to half of the image width, and the excess content will be overlaid from a new line.

Transparency

It is the condition of viewing the live view image through the overlaid information.

Font Color Inversion

Enable the function to detect the gray level of the image overlaid position automatically. When the image color is dark, the overlaid characters will be displayed as white automatically. When the image color is light, the overlaid characters will be displayed as black automatically.

Capture Time Type

Select the time type to overlay information on the captured pictures.

Picture Upload Time

The information will be overlaid when the captured picture starts to upload.

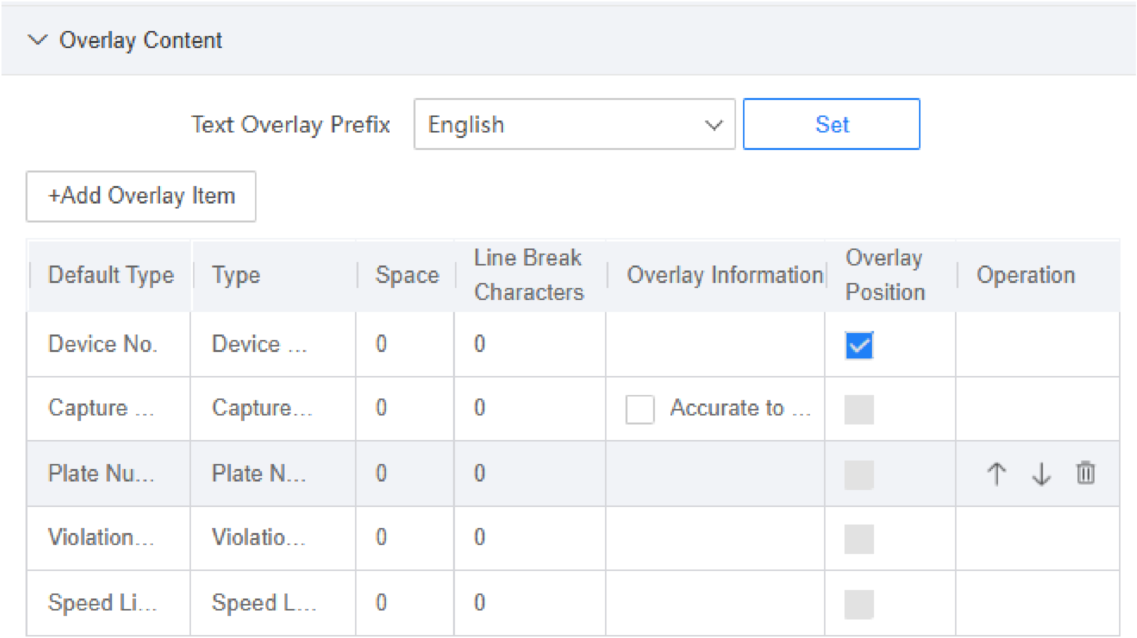
Picture Generation Time

The information will be overlaid when the captured picture is output.

Composite Picture Capture Time

The capture time of the selected picture sequence will be overlaid on the composite picture.

5. Set **Overlay Content**.



Overlay Content

Text Overlay Prefix: English

Default Type	Type	Space	Line Break Characters	Overlay Information	Overlay Position	Operation
Device No.	Device ...	0	0		☑	
Capture ...	Capture...	0	0	☐ Accurate to ...	☐	
Plate Nu...	Plate N...	0	0		☐	↑ ↓ 🗑
Violation...	Violatio...	0	0		☐	
Speed Li...	Speed L...	0	0		☐	

Figure 6-7 Set Composite Picture Overlay Content

1) Select **Text Overlay Prefix** language to overlay the information in corresponding language, and click **Set** to save.

Note

The supported languages depend on the selected LPR **Country/Region** in **Configuration → Capture → Capture Parameters → LPR Parameters** .

Result: You can edit the custom information name in the selected language.

2) Click **Add Overlay Item** to select the information to overlay, and click **OK**.

Note

The overlay information varies with different models. The actual device prevails.

3) Set the parameters below.

- **Default Type**: You can view the default overlay information name. If you have edited the name, you can refer to the default name for the definition.
- **Type**: You can edit a custom overlay information name.

- **Space**: Edit the number of space between the current information and the next one from 0 to 255. 0 means there is no space.
- **Line Break Characters**: Edit the number of characters from 0 to 100 between the current information line and the previous information line. 0 means no line break.
- **Overlay Information**: For some information types, you can edit the detailed information.
- **Overlay Position**: If you check it, the current information will be displayed from a new line.
- **Operation**: You can click ↑ / ↓ to adjust the display sequence of the overlay information, or click 🗑 to delete the item.

6. **Optional:** Check the other channel(s) to copy the same settings.
7. Click **Capture Test** to test the information overlay effect.
8. Click **Save**.

6.6 Set Image Encoding Parameters

If the captured pictures are not clear, set the resolution, size, and quality of the captured pictures.

Steps

1. Go to **Configuration → Capture → Capture Parameters → Image Encoding and Composition → Image Encoding** .

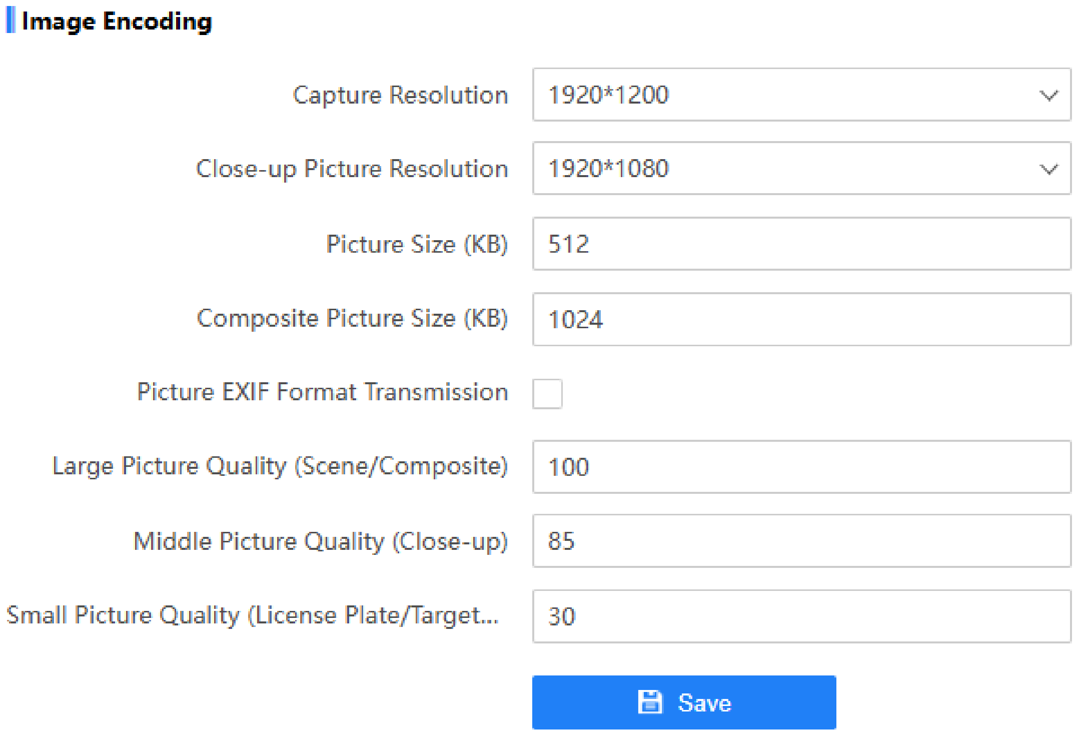


Image Encoding

Capture Resolution	1920*1200
Close-up Picture Resolution	1920*1080
Picture Size (KB)	512
Composite Picture Size (KB)	1024
Picture EXIF Format Transmission	□
Large Picture Quality (Scene/Composite)	100
Middle Picture Quality (Close-up)	85
Small Picture Quality (License Plate/Target...	30

Figure 6-8 Set Image Encoding Parameters

2. Set the parameters below.

Capture Resolution

Select the resolution of the captured scene picture. When the picture size keeps the same, the higher the resolution, the more the picture will be compressed, and the slower the picture will be handled.

Close-up Picture Resolution

Select the resolution of the target close-up picture. When the picture size keeps the same, the higher the resolution, the more the picture will be compressed, and the slower the picture will be handled.

Picture Size

The size of the compressed captured picture. The actual size is related to the scene complexity.

Composite Picture Size

The size of the compressed composite picture. The actual size is related to the scene complexity.

Note

Only the device supporting picture composition supports composite picture size settings. The actual device prevails.

Picture EXIF Format Transmission

The captured pictures will be transmitted in the EXIF format.

Large Picture Quality (Scene/Composite)

Set the quality of the scene pictures and composite pictures. The value ranges from 1 to 100. The higher the value, the better the quality of the captured pictures.

Middle Picture Quality (Close-up)

Set the quality of the target close-up pictures. The value ranges from 1 to 100. The higher the value, the better the quality of the captured pictures.

Small Picture Quality (License Plate/Target/Face)

Set the quality of the license plate, target, or face pictures. The value ranges from 1 to 100. The higher the value, the better the quality of the captured pictures.

3. Click **Save**.

6.7 Set Picture Composition

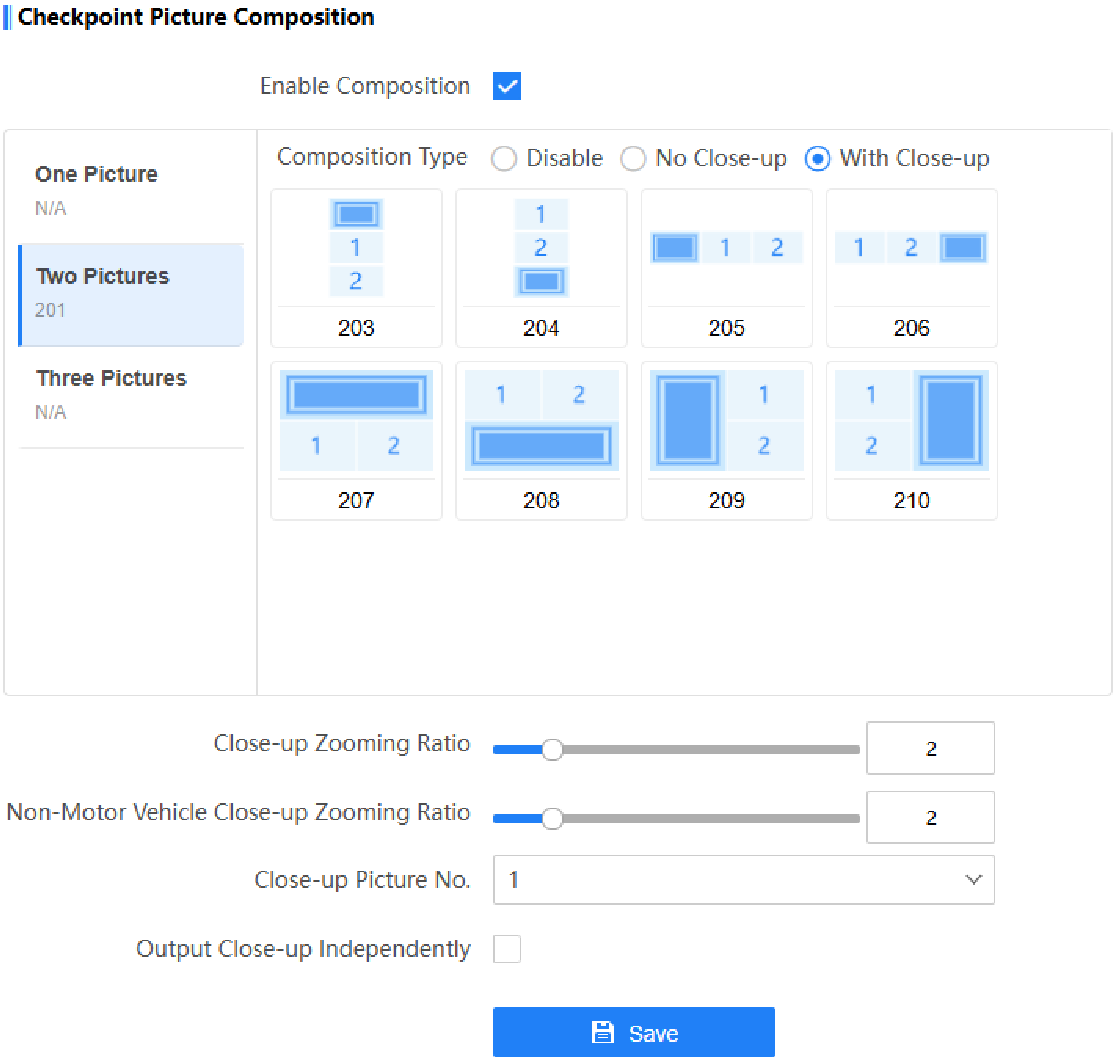
You can enable the picture composition to composite several pictures into one to make it convenient to view the violation captured pictures.

Steps

Note

Functions and parameters vary with different models. The actual device prevails.

1. Go to **Configuration → Capture → Capture Parameters → Image Encoding and Composition → Picture Composition** .



Checkpoint Picture Composition

Enable Composition ☑

Composition Type ○ Disable ○ No Close-up ● With Close-up

Close-up Zooming Ratio 2

Non-Motor Vehicle Close-up Zooming Ratio 2

Close-up Picture No. 1

Output Close-up Independently □

Figure 6-9 Set Picture Composition

2. Check **Enable Composition**.
3. Set **Composition Type** for different picture quantities. Refer to the layout displayed on the interface to view the composition effect.
4. Set other composition parameters.

   Close-up Zooming Ratio

The higher the value, the larger the close-up picture.

Non-Motor Vehicle Close-up Zooming Ratio

The higher the value, the larger the non-motor vehicle close-up picture.

Close-up Picture No.

It is the scene picture No. where the close-up comes from.

Output Close-up Independently

Enable the function to output a close-up picture before or after the scene picture independently.

Note

Enabling composition and outputting close-up independently functions conflict with each other. You can only enable one.

5. Click **Save**.

6.8 Set Capture Schedule

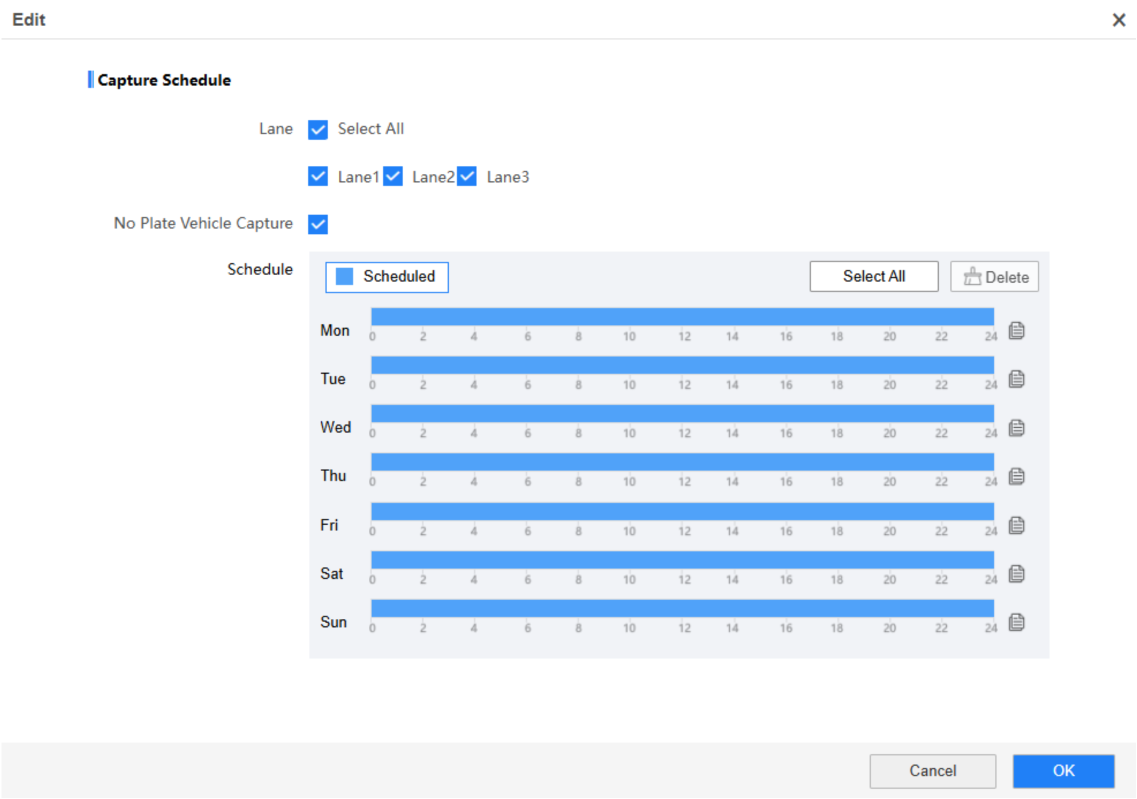
You can set the schedule for the violation behavior capture or checkpoint capture if needed.

Steps

Note

The function varies with different models. The actual device prevails.

1. Go to **Configuration → Capture → Capture Parameters → Capture Schedule** .
2. Click ✎ to set the capture schedule according to the actual needs.



Edit

Capture Schedule

Lane ☑ Select All

☑ Lane1 ☑ Lane2 ☑ Lane3

No Plate Vehicle Capture ☑

Schedule

Figure 6-10 Set Capture Schedule

3. Select **Lane**.
4. **Optional:** Check **No Plate Vehicle Capture** according to the actual needs.
5. Adjust the time period.
   - Click on the selected time period, and enter the desired value. Click **Save**.
   - Click on the selected time period. Drag the both ends to adjust the time period.
6. **Optional:** Click 📋 to copy the same settings to other days.
7. Click **OK**.
8. **Optional:** Check **Upload to Mailbox** to email the capture schedule to the user.
9. Click **Save**.

6.9 Set Captured Image Parameters

Set the parameters of captured images to raise the image quality.

Steps

1. Go to **Configuration → Capture → Capture Images → Image Parameters** .

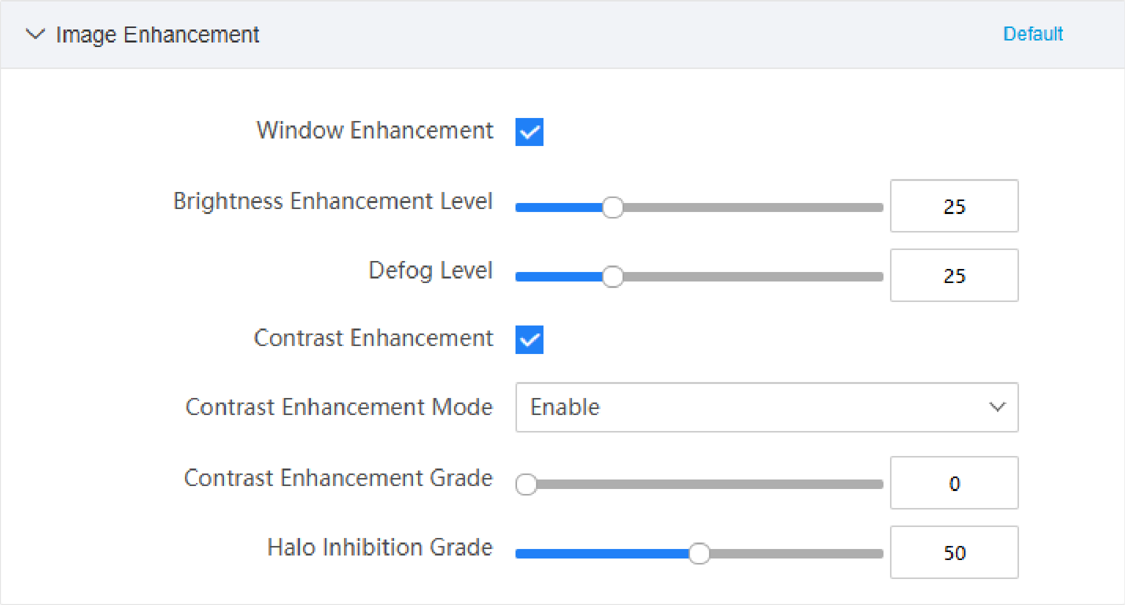


Image Enhancement

Default

Window Enhancement ☑

Brightness Enhancement Level 25

Defog Level 25

Contrast Enhancement ☑

Contrast Enhancement Mode Enable

Contrast Enhancement Grade 0

Halo Inhibition Grade 50

Figure 6-11 Set Captured Image Parameters

2. Set the captured image parameters.

Note

You can click **Default** to restore all the set parameters to the default settings.

Image Enhancement

Window Enhancement

In front light or back light scene, the flash light may not pass through the vehicle window, or the image effect of the window is bad caused by the light. In this condition, you can check **Window Enhancement**. The higher the **Brightness Enhancement Level** is, the brighter the window image is. The higher the **Defog Level** is, the better the permeability of the window image is.

Contrast Enhancement

Check **Contrast Enhancement** to capture clearer images. Select **Contrast Enhancement Mode**, and set corresponding parameters.

Contrast Enhancement Mode	Description
Enable	The contrast enhancement mode is always enabled.
Time	The contrast enhancement mode is enabled during the set start time and end time. In other time, it is disabled.
Brightness	The contrast enhancement mode is enabled according to the brightness of the surroundings. In this case, you can set **Brightness Grade**.

Contrast Enhancement Grade

The higher the grade is, the more the contrast is enhanced.

Halo Suppression Grade

Halo suppression is to suppress the halo of the vehicle headlights. The higher the grade is, the more the halo is suppressed.

6.10 Set ICR

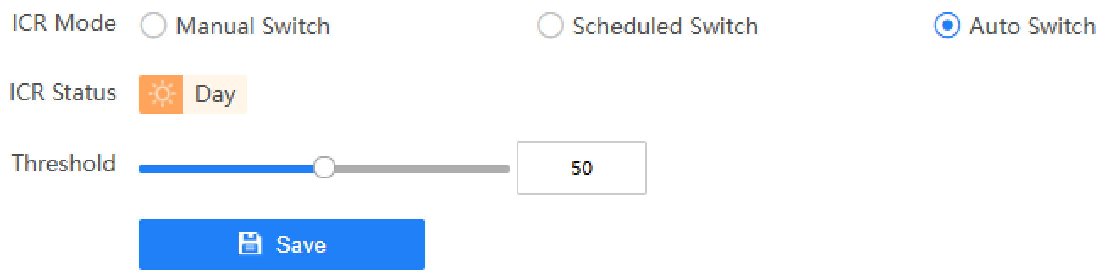
ICR adopts mechanical IR filter to filter IR in the day to guarantee the image effect, and to remove the IR filter at night to guarantee full-spectrum rays can get through the device.

Steps

Note

For the device supporting black and white mode at night, when the day-night mode is night, and **Black and White Mode at Night** has been enabled in **Configuration → Video → Camera Parameters → Camera Parameters → Image Enhancement** , the image displays as black and white. When **Black and White Mode at Night** is disabled, the image displays as color.

1. Go to **Configuration → Capture → Capture Images → ICR** .



ICR Mode ○ Manual Switch ○ Scheduled Switch ● Auto Switch

ICR Status Day

Threshold 50

Figure 6-12 ICR

2. Select **ICR Mode**.

Auto Switch	The ICR mode will switch to day or night mode automatically according to the surrounding light conditions. When the surrounding light is sufficient and higher than the set **Threshold**, the ICR mode will switch to day. When the surrounding light is insufficient and lower than the set **Threshold**, the ICR mode will switch to night.
Manual Switch	Select **Day-night Mode** to switch to the day or night manually.
Scheduled Switch	Set **Day-night Mode**, **Start Time**, and **End Time** to switch to the day or night mode only during the set time period.

3. Click **Save**.

6.11 Advanced Configuration

Note

The advanced configurations below are only provided to debug the device by the professionals.

6.11.1 System Service

You can enable the functions to debug the device.

Steps

1. Go to **Configuration → Capture → Advanced → System Service** .
2. Enable the functions according to your needs.

Note

The supported parameters vary with different models. The actual device prevails.

Enable Algorithm POS Information Debug

The algorithm POS information will be overlaid on the playback image when you play back the video with the dedicated tool.

Enable Positioning Frame Debug

The positioning frames of vehicle bodies and license plates will be overlaid on the captured pictures.

Enable Closed Positioning Frame

The bottom lines of the positioning frames on the captured pictures will be displayed. The frames will be closed.

Enable LPR Area Frame

In some application modes, the license plate may not be included in the LPR area, and the LPR rate is low. To solve the problem, you can enable the function to add a green frame on the captured picture to check whether the license plate is included in the LPR area.

LPR Area Frame Y-Direction Deviation

If the license plate is not included in the LPR area frame, adjust the LPR area frame position in the Y-direction by pixel. Enter the deviation pixel in the text field. The value = image height × (deviation distance/100). Set the value according to the actual needs. Range: -100% to 100%. The LPR area frame moves up if the value is negative, and it moves down if the value is positive.

Enable License Plate Frame

The license plate frames will be overlaid on the captured pictures.

Enable Multi-Way Upload

Data will be uploaded in multiple set ways simultaneously.

Enable Lane Line Debug

Check it to overlay lane lines on a captured picture.

License Plate POS Font Size

Set the font size of the POS information overlay. The font size ranges from 32 to 128.

3. Click **Save**.

6.11.2 Vehicle Capture and Recognition Service

Set the vehicle capture and recognition service to debug the device.

Steps

Note

The function varies with different models. The actual device prevails.

1. Go to **Configuration → Capture → Advanced → Vehicle Capture and Recognition Service** .
2. Check the service(s) according to your needs.

   Note

   The supported services vary with different models. The actual device prevails.

   Checkpoint Parameters

   Filter Checkpoint Capture of Same Vehicle

   It is used to debug the device with the same vehicle. When the same vehicle is triggered many times during a short period in the scene, the checkpoint pictures of the vehicle will not be captured. Set **Time of Filtering Checkpoint Duplicate License Plates** to filter the vehicle during the set time.

Do Not Capture Reverse-driving Vehicle

The reverse-driving vehicles will not be captured. For example, if you need to capture the vehicles driven from the west to the east, enable the function and the vehicles driven from the east to the west will not be captured.

Filter Two-Wheelers Without License

Check it to not capture the two-wheelers without license plates.

Enable ANR

Enable ANR (Automatic Network Replenishment) to save the videos in the condition of network disconnection, and synchronize data after the network is recovered.

Enable Pure License Plate Recognition

In smart mode, enable the function to capture once a license plate is recognized, no matter whether the target is tracked or not.

Filter Capture Pictures with Unknown Speeds

Enable the function to filter the capture results of vehicles with unknown speeds.

3. Click **Save**.

6.11.3 Set Image Format

You can enable smartJPEG which can save the storage space without influencing the resolution.

Steps

1. Go to **Configuration → Capture → Advanced → Image Service** .
2. Check **smartJPEG**.
3. **Optional:** Set **Expansion Ratio of License Plate Image** to expand the cutout scale of license plate image.
4. Click **Save**.

6.11.4 View Traffic Statistics

View Real-Time Traffic Statistics

You can view the real-time traffic statistics if the device supports this function.

Steps

Note

This function varies with different models. The actual device prevails.

1. Go to **Configuration → Capture → Advanced → Traffic Statistics Parameters → TPS Parameters** , or **Live View → Traffic Statistics** .

2. Enable **TPS Statistics Collection**.
3. Set **Statistics Interval**.

What to do next

Go to **Live View → Traffic Statistics** to view the arming status. You can click 🛡 to arm, and the captured pictures during the set interval will be saved as a .zip file in the browser default downloading directory. Click 🛡 to disarm.

View Traffic Flow Statistics

The device supports counting and uploading traffic follow data.

Steps

Note

This function varies with different models. The actual device prevails.

1. Go to **Configuration → Capture → Advanced → Traffic Statistics Parameters → Traffic Statistics Parameters** , or **Live View → Traffic Statistics** .
2. Enable **Traffic Flow Statistics Collection**.
3. Set **Statistics Interval**.
4. Click **Save**.

What to do next

Go to **Live View → Traffic Statistics** to view the arming status. You can click 🛡 to arm, and the captured pictures during the set interval will be saved as a .zip file in the browser default downloading directory. Click 🛡 to disarm.

Chapter 7 Radar Detection

Radar is used to detect the target and link the capture. Set radar detection parameters before capturing vehicle pictures.

Note

The function is only supported for the application mode of smart mode. The actual device prevails.

7.1 Set Detection Parameters

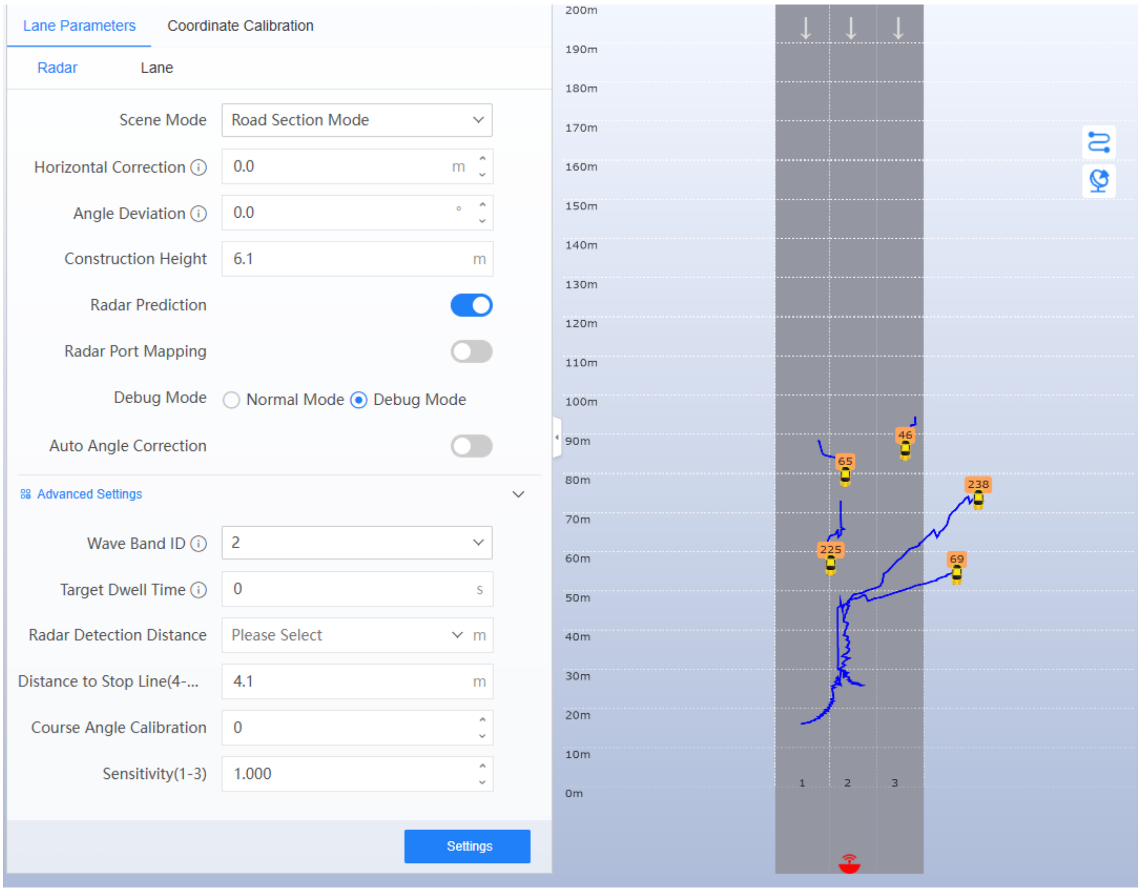
For speed detection via radar, there is no strong relationship between the detected speed results and vehicle targets, which may result in the consequence that the speed result is linked to incorrect target or the speed result is lost. To solve the problems, speed detection via both radar and video is recommended. In this mode, the radar not only outputs the speed result of the target, but also outputs the coordinates of the position relationship between the target and radar. You can create the relationship between the radar position coordinates and vehicle pixel coordinates in the video via calibration to realize the linkage of the speed result and the vehicle target.

Before You Start

- Go to **Configuration → System → System Settings → Device Status** to view the radar status. If the status is normal, you can debug it. If the radar is in upgrading status, do not reboot the device.
- Go to **Configuration → Local** to enable **Rules Information** and **Radar Track**.

Steps

1. Go to **Radar → Lane Parameters → Radar** .



Scene Mode: Road Section Mode

Horizontal Correction: 0.0 m

Angle Deviation: 0.0 °

Construction Height: 6.1 m

Radar Prediction ☑

Radar Port Mapping □

Debug Mode ○ Normal Mode ● Debug Mode

Auto Angle Correction □

Wave Band ID: 2

Target Dwell Time: 0 s

Radar Detection Distance: Please Select m

Distance to Stop Line(4-...: 4.1 m

Course Angle Calibration: 0

Sensitivity(1-3): 1.000

Figure 7-1 Set Radar Parameters

2. Set the basic parameters of the radar.

Scene Mode

Select the scene mode according to the actual construction scene of the device.

Horizontal Correction

It is the horizontal position deviation between the radar detected lane and the actual lane. You can set it in two ways.

- Method 1: Move the detected lane in the diagram leftwards or rightwards to overlap it with the actual lane to correct the difference.
- Method 2: Enter the horizontal distance(m) from the radar installation position to the middle line of the actual lane to correct the difference.

Angle Deviation

It is the angle deviation between the radar detected lane and the actual lane. Rotate the angle of the detected lane in the diagram to overlap it with the actual lane to correct the difference.

Construction Height

Set the construction height of the radar according to construction at the actual scene.

Radar Prediction

It is only used for debug by the professionals. Enable the function, and the radar will predict the target track which can be displayed on the interface according to the detected coordinates.

Radar Port Mapping

Enable the function and **SSH Service**, and the debugging command with radar configuration information will be sent to the device. The radar specified port can be mapped to the camera, and the radar can be debugged via the camera IP address with the radar debug software.

Debug Mode

Select **Debug Mode**. In this mode, the vehicles outside the drawn area will be displayed, to make it convenient to debug the radar. After debug, you should switch to **Normal Mode**.

Auto Angle Correction

After enabling radar debug mode, you can enable it to get the radar deviation angle according to the moving path of vehicle.

3. Click **Advanced Settings** to expand the advanced settings menu. Set advanced parameters of the radar.

Wave Band ID

0 to 4 stand for five frequencies. Set different wave bands for different radars in the same scene to prevent the radars in the same wave band from influencing each other.

Target Dwell Time

The dwell time of the vehicle. If the target dwell time is longer than the set time, vehicle data statistics will not be operated. Set it as 0 when measuring the queue length. It is only effective for the static targets.

Radar Detection Distance

It is the farthest distance that the radar can detect. The default value is 200 m. You can select the value to match the radar detection distance.

Distance to Stop Line

It is the distance from the point on the ground just below the installed radar to the stop line at the intersection. The targets detected in this range will be filtered.

Course Angle Calibration

Set the angle between the driving direction and the device installation direction. The radar course angle information of the current frame will be included when matching the video detected targets and radar detected targets.

Sensitivity

The lower the sensitivity is, the more sensitive the detection will be. For the detection which is too sensitive (e.g., some fixed facilities, such as the bus station on the lane, are detected as vehicles), you can adjust the sensitivity higher.

4. Click **Settings**.
5. **Optional:** You can click the icons on the upper right corner of the target track area to adjust the display status.

Table 7-1 Icon Description

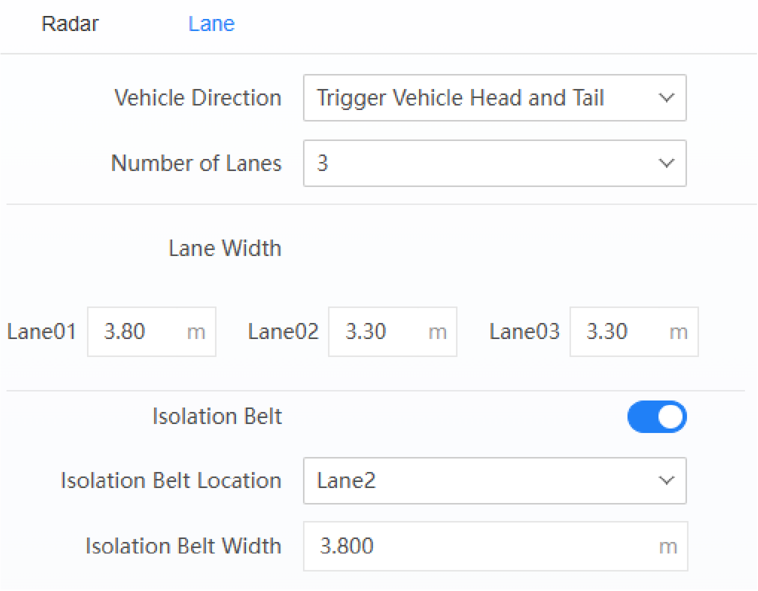
Icon	Description
⇆ / ⇆	Click to enable or disable the radar targets tracks display.
◎ / ◎	Click to switch to the radar track or fusion track. The fusion track refers to the target track fused with the video detection and radar detection. In fusion track mode, you can view the targets detected by single radar, single video, or both radar and video according to the different colors displayed on the interface, and the detected vehicle information will be displayed in the vehicle list.

7.2 Set Lane Parameters

Set the parameters of the radar detected lanes.

Steps

1. Go to **Radar → Lane Parameters → Lane** .



Vehicle Direction: Trigger Vehicle Head and Tail

Number of Lanes: 3

Lane Width

Lane01 3.80 m   Lane02 3.30 m   Lane03 3.30 m

Isolation Belt: On

Isolation Belt Location: Lane2

Isolation Belt Width: 3.800 m

Figure 7-2 Set Lane Parameters

2. Set the lane parameters below.

Vehicle Direction

Trigger Vehicle Head

The vehicles are driven towards the construction position of the camera.

Trigger Vehicle Tail

The vehicles are driven far away from the construction position of the camera.

Trigger Vehicle Head and Tail

There are vehicles driven both towards and far away from the construction position of the camera.

Number of Lane

The number of lanes should be consistent with the total lanes in the application mode settings.

Lane Width

Set the width of corresponding lane according to the actual scene.

Isolation Belt

When there is a isolation belt between the lanes of opposite directions, enable the function. Select the lane No. on the left of the isolation belt as **Isolation Belt Location**, and set **Isolation Belt Width** according to the actual scene.

3. Click **Settings**.

7.3 Set Radar Calibration

Calibrate radar in order to transfer the detected vehicle actual distance into the positions in the video.

Before You Start

Enable **Rules Information** and **Radar Track** in **Configuration → Local** to display the recognized license plate number, red speed frames, and green target frames in the live view image to make it convenient for calibration.

Steps

1. After enabling debug mode, click **Coordinate Calibration**.
2. Set the radar calibration.
   - Set manual calibration. Refer to ***Manual Calibration*** for details.
   - Set auto calibration. Refer to ***Auto Calibration*** for details.
   - Set force auto calibration. Refer to ***Force Auto Calibration*** for details.

Note

You're recommended to use auto calibration.

7.3.1 Manual Calibration

Steps

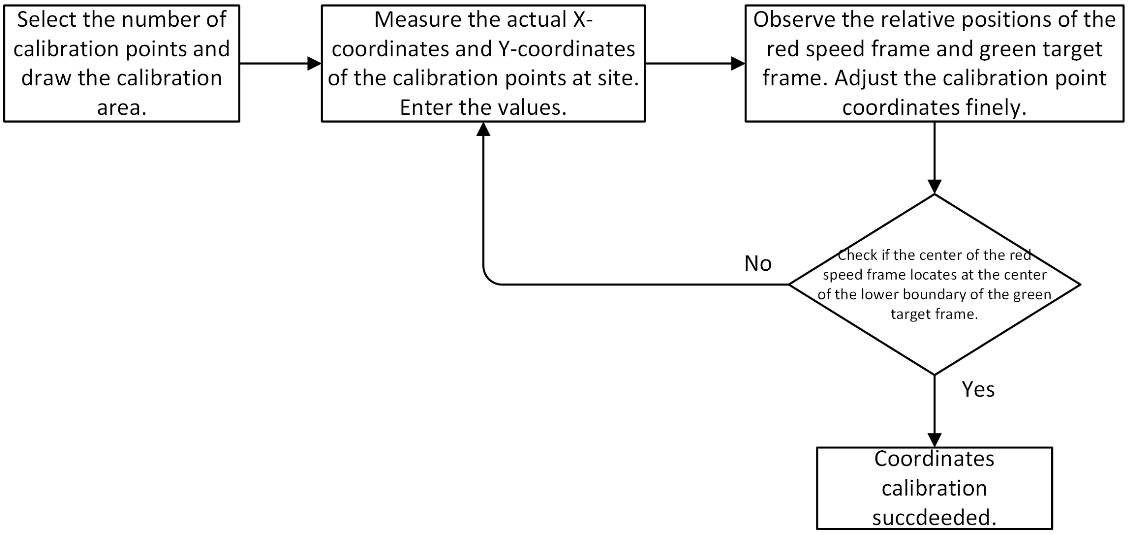
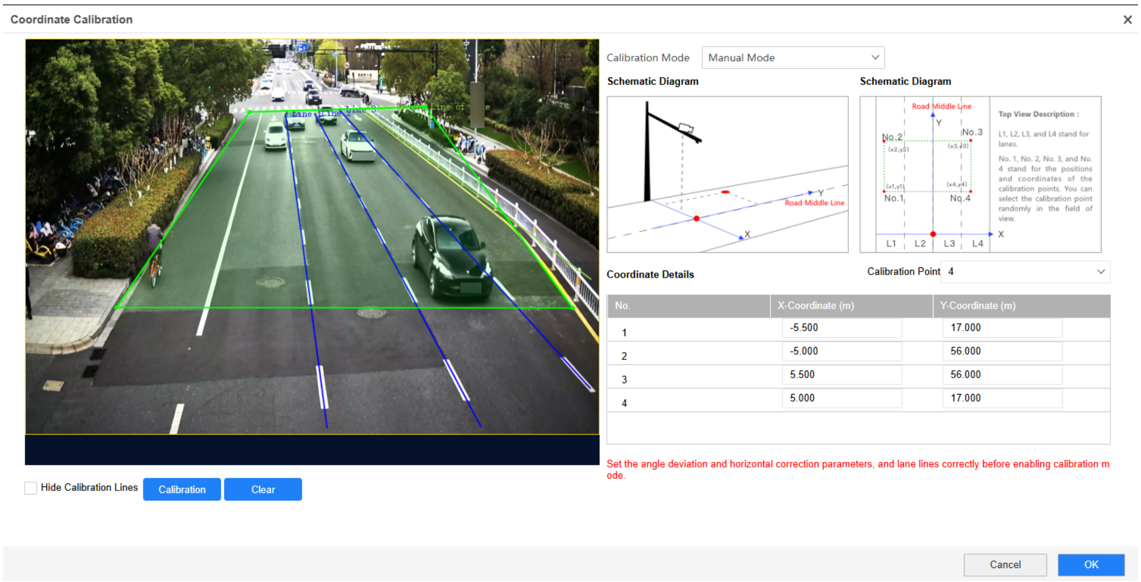

Select the number of calibration points and draw the calibration area.
Measure the actual X-coordinates and Y-coordinates of the calibration points at site. Enter the values.
Observe the relative positions of the red speed frame and green target frame. Adjust the calibration point coordinates finely.
Check if the center of the red speed frame locates at the center of the lower boundary of the green target frame.
No
Yes
Coordinates calibration succdeeded.

Figure 7-3 Manual Calibration Flow

1. Click **Coordinate Calibration**.
2. Select **Calibration Mode** as **Manual Calibration**.



Calibration Mode: Manual Mode

Top View Description :

L1, L2, L3, and L4 stand for lanes.

No. 1, No. 2, No. 3, and No. 4 stand for the positions and coordinates of the calibration points. You can select the calibration point randomly in the field of view.

Coordinate Details

Calibration Point: 4

No.	X-Coordinate (m)	Y-Coordinate (m)
1	-5.500	17.000
2	-5.000	56.000
3	5.500	56.000
4	5.000	17.000

Set the angle deviation and horizontal correction parameters, and lane lines correctly before enabling calibration mode.

Figure 7-4 Manual Calibration

3. Drag the two end points of the default lines on the live view image or drag the whole lines to adjust their positions according to the actual scene.
4. Draw the calibration area.

1) Select **Calibration Point**.

Note

4-point calibration by default.

2) Adjust the default calibration area on the live view image according to the actual scene, or click **Calibration** to redraw the area.
3) Click the left button of the mouse to locate the vertexes of the calibration area on the live view image clockwise, and click the right button of the mouse to finish the drawing.

Note

The number of vertexes should be consistent with the selected number of **Calibration Point**.

4) Measure the X-coordinates and Y-coordinates of the calibration points with measurement tool at site accurately, and enter the values in the corresponding coordinate text fields.

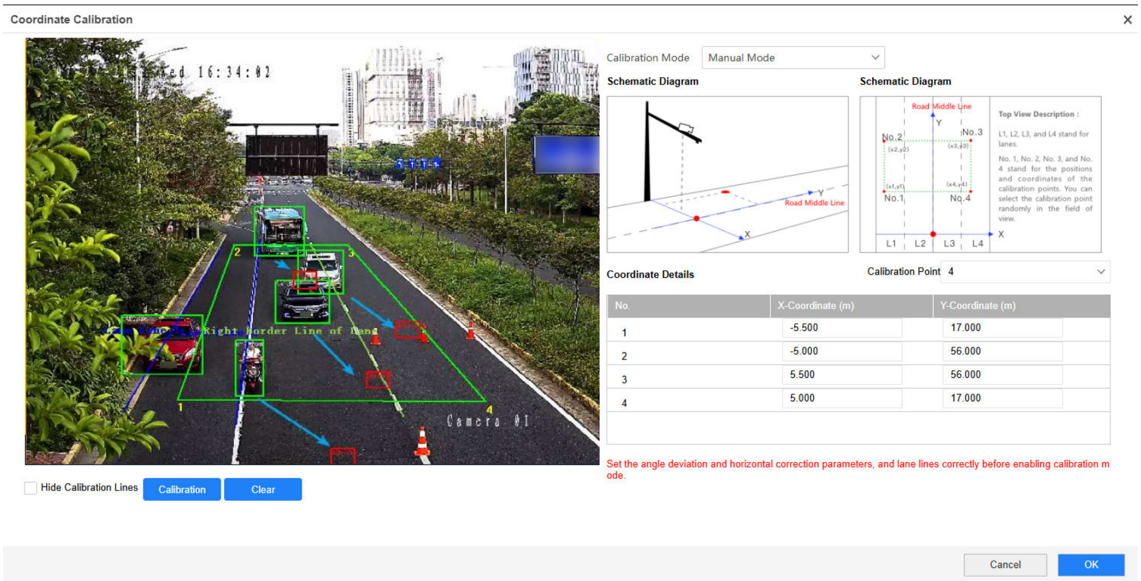
Note

- X-coordinate stands for the horizontal distance from the calibration point to the origin of the radar coordinates. Y-coordinate stands for the vertical distance from the calibration point to the origin of the radar coordinates. The origin (0, 0) of the radar coordinates locates in the middle of the whole lanes detected by the radar. You can refer to the schematic diagram on the right of the interface.
- If there are 4 points for the calibration area, the X-coordinates of point 1 and 2 should be negative values.
- If the speed displayed on the live view image is 0, you need to calibrate again. The best calibration effect is that the center of the red speed frame locates at the center of the lower boundary of the green target frame.

5) **Optional:** Click **Clear** to clear the drawn calibration area.

5. **Optional:** If there is no condition to measure the coordinates of the calibration points accurately at site, you can draw a calibration area and estimate the coordinates of the calibration points first, and then perform fine adjustment to the coordinates as the steps below.

1) Find a vehicle passing the calibration point in the live view image, and observe the relative position relationship between the vehicle target and the red speed frame. The distance between the position of the red speed frame and that of the green target frame may be large before calibration. You need to observe the moving tendency of the target frame and the speed frame. As shown below, you can see that the red speed frames and the green target frames are moving relatively.



Calibration Mode: Manual Mode

Top View Description :

L1, L2, L3, and L4 stand for lanes.

No. 1, No. 2, No. 3, and No. 4 stand for the positions and coordinates of the calibration points. You can select the calibration point randomly in the field of view.

Coordinate Details

Calibration Point: 4

No.	X-Coordinate (m)	Y-Coordinate (m)
1	-5.500	17.000
2	-5.000	56.000
3	5.500	56.000
4	5.000	17.000

Set the angle deviation and horizontal correction parameters, and lane lines correctly before enabling calibration m ode.

Figure 7-5 Fine Adjustment Example

2) According to the relative positions, if the red speed frame is in front of the green target frame, decrease the Y-coordinate value. If the red speed frame is behind the green target frame, increase the Y-coordinate value. Adjust the values until the lower boundaries of the red speed frame and the green target frame are on the same horizontal line.

3) According to the relative positions, if the red speed frame is in the left position of the lower boundary center of the green target frame, decrease the X-coordinate value. If the red speed frame is in the right position of the lower boundary center of the green target frame, increase the X-coordinate value. Adjust the values until the lower boundaries of the red speed frame and the green target frame are on the same vertical line.

4) Adjust the other calibration points according to the methods above until all the vehicles in the detection area satisfy the requirement.

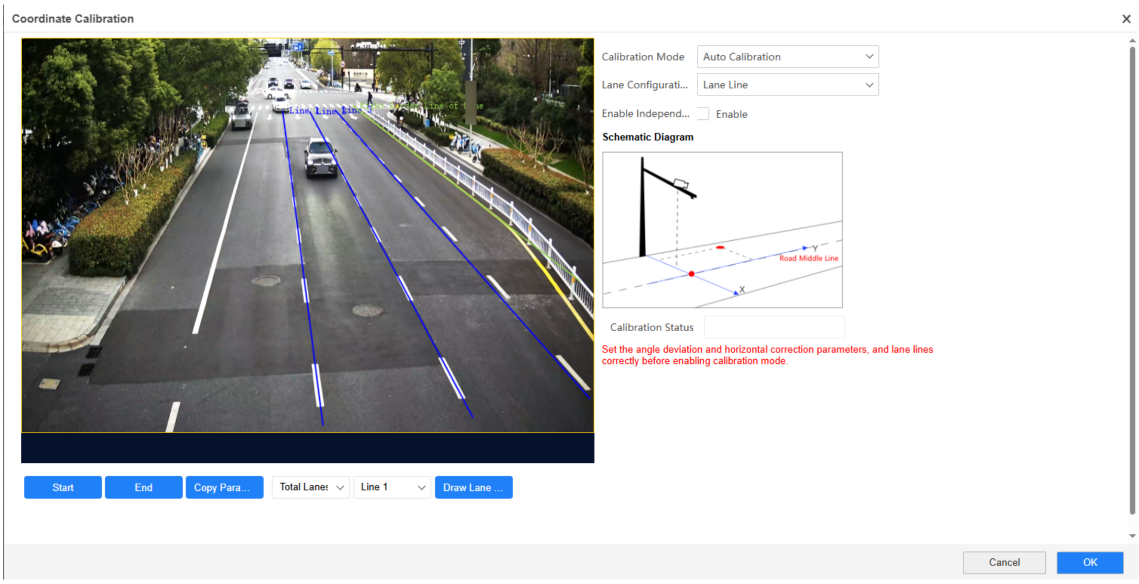
6. **Optional:** Check **Hide Calibration Lines** to hide the lines on the live view image.

7. Click **OK**.

7.3.2 Auto Calibration

Steps

1. Click **Coordinate Calibration**.
2. Select **Calibration Mode** as **Auto Calibration**.



Calibration Mode: Auto Calibration

Lane Configurati...: Lane Line

Enable Independ... □ Enable

Schematic Diagram

Calibration Status

Set the angle deviation and horizontal correction parameters, and lane lines correctly before enabling calibration mode.

Figure 7-6 Auto Calibration

3. Enable or disable independent lane settings.
   - If you disable independent lane settings, the device will recognize the lane lines in the scene and match the drawn lines according to the selected number of total lanes.
   - If you enable independent lane settings and select the number of total lanes, the corresponding number of lane lines will display on the live view image, and you need to adjust the lines according to the scene manually.

Note

If the lanes are bidirectional ways, or the lane range to be calibrated is inconsistent with the lanes set in the application mode, you are recommended to enable independent lane settings to draw the lane lines independently.

4. **Optional:** Select the lane line No. and click **Draw Lane Line** to redraw the corresponding lane line.

Note

The lane lines must be set accurately before auto calibration. For the scenes to which auto calibration is not applicable, like congestion, vehicles are waiting for the red traffic light, there are too few vehicles passing, etc., manual calibration is recommended.

5. Click **Start**.

   The auto calibration starts, and you can view the calibration status and progress. 100% means the auto calibration is finished.
6. **Optional:** Click **End** if the speed detection effect via radar and video fusion mode has met the requirement during the process.
7. **Optional:** Click **Copy Parameters to Coordinate Mode** to copy the auto calibrated coordinates to the manual calibration mode.

8. Click **OK**.

What to do next

- After auto calibration, exit from the interface. Observe the calibration effect after a period of time. As shown below, if the red speed frame locates at the lower boundary center of the green target frame, that is, the red speed frame locates at the license plate position, the calibration effect satisfies the requirements. Otherwise, you need to calibrate again, or perform fine adjustment to the coordinates by the methods for the manual calibration. Refer to step 5 of ***Manual Calibration*** for details.

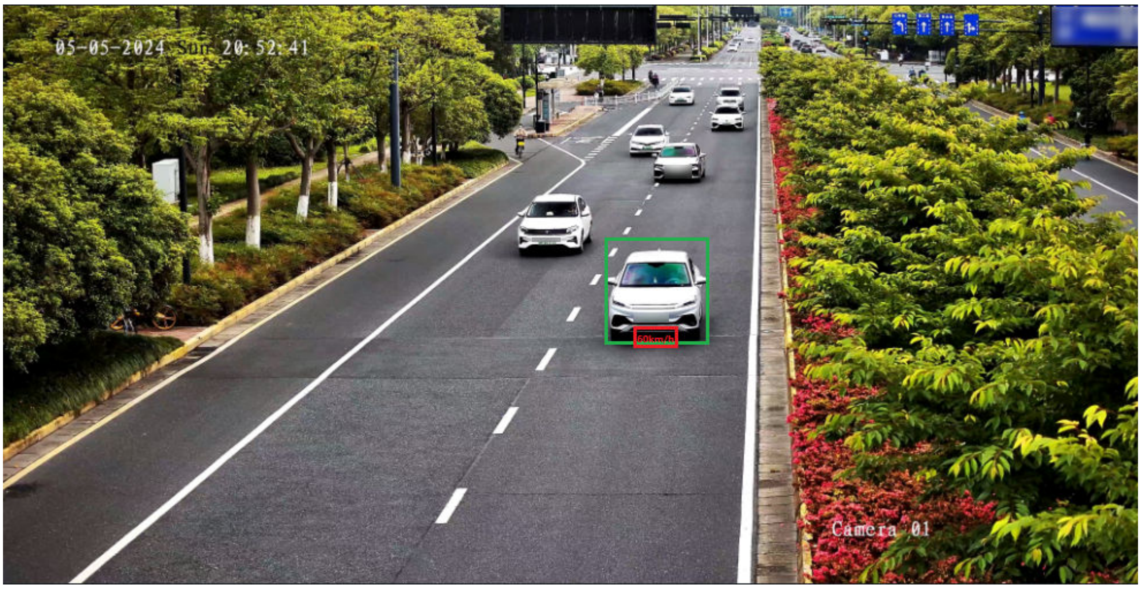


Figure 7-7 Good Calibration Effect Example

- For the scene with multiple lanes and congestion, observe the auto calibration effect. If the fusion effect is not good after the auto calibration is finished, you need to calibrate again manually. Refer to ***Manual Calibration*** for details.

7.3.3 Force Auto Calibration

You can select force auto calibration for the scene that the personnel at the site drives a car or SUV to pass in the visual field of the device to complete the calibration quickly.

Before You Start

- There is up to one moving target (a car or a SUV) in the visual field of the device during calibration.
- The vehicle speed keeps 20 to 40 km/h during calibration.

Steps

1. The personnel at the site drives a car or SUV to pass far away from the visual field of the device along the far left/right lane until the vehicle disappears from the video/radar detection area

completely, and then enter into the video/radar detection area along the far left/right lane alternately for four times. If there is only one lane in the scene, drive along the far left/right lane line. You're recommended to drive the vehicle along the marked routes shown in the figure below.

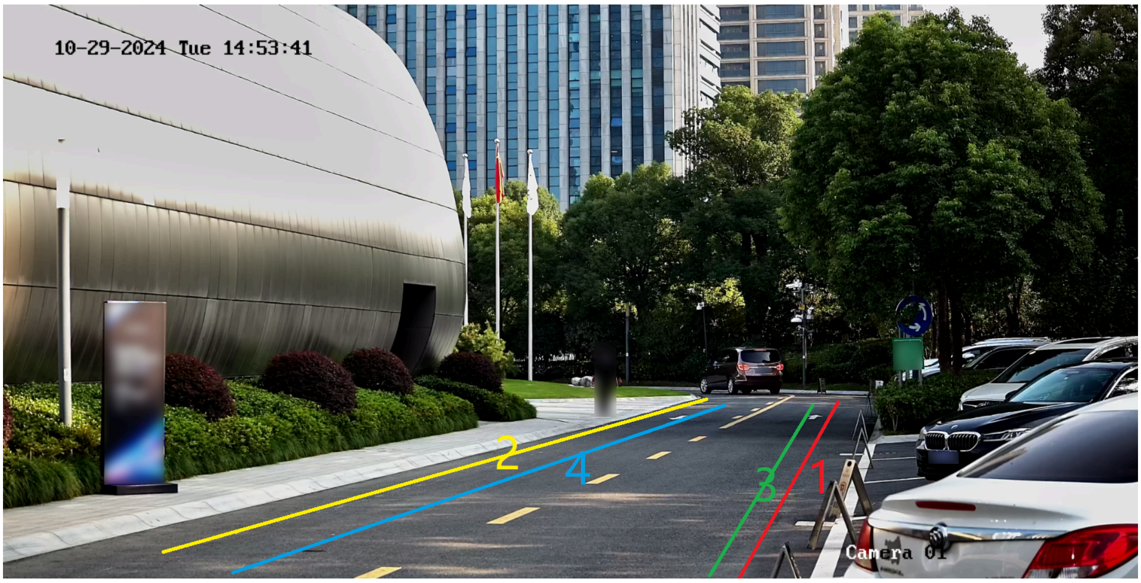
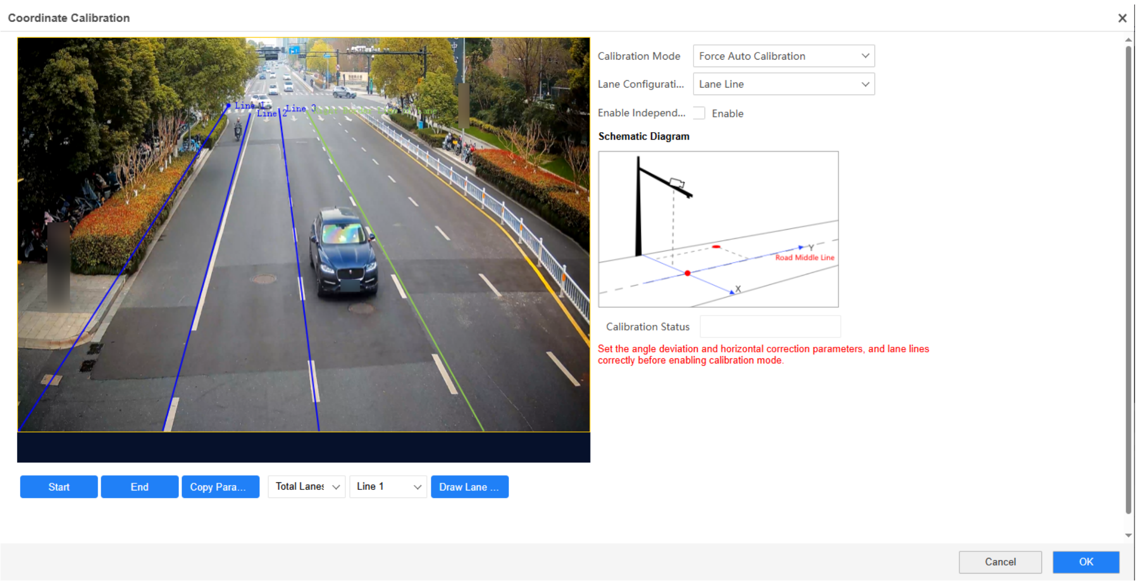


Figure 7-8 Recommended Driving Routes for Force Auto Calibration

2. Click **Coordinate Calibration**.
3. Select **Calibration Mode** as **Force Auto Calibration**.



Coordinate Calibration

Calibration Mode: Force Auto Calibration

Lane Configurati...: Lane Line

Enable Independ... □ Enable

Schematic Diagram

Calibration Status

Set the angle deviation and horizontal correction parameters, and lane lines correctly before enabling calibration mode.

Figure 7-9 Force Auto Calibration

4. Enable or disable independent lane settings.

- If you disable independent lane settings, the device will recognize the lane lines in the scene and match the drawn lines according to the selected number of total lanes.
- If you enable independent lane settings and select the number of total lanes, the corresponding number of lane lines will display on the live view image, and you need to adjust the lines according to the scene manually.

Note

If the lanes are bidirectional ways, or the lane range to be calibrated is inconsistent with the lanes set in the application mode, you are recommended to enable independent lane settings to draw the lane lines independently.

5. **Optional:** Select the lane line No. and click **Draw Lane Line** to redraw the corresponding lane line.

Note

The lane lines must be set accurately before auto calibration. For the scenes to which auto calibration is not applicable, like congestion, vehicles are waiting for the red traffic light, there are too few vehicles passing, etc., manual calibration is recommended.

6. Click **Start**.

   The auto calibration starts, and you can view the calibration status and progress. 100% means the auto calibration is finished.
7. **Optional:** Click **End** if the speed detection effect via radar and video fusion mode has met the requirement during the process.
8. **Optional:** Click **Copy Parameters to Coordinate Mode** to copy the auto calibrated coordinates to the manual calibration mode.
9. Click **OK**.

What to do next

- After auto calibration, exit from the interface. Observe the calibration effect after a period of time. As shown below, if the red speed frame locates at the lower boundary center of the green target frame, that is, the red speed frame locates at the license plate position, the calibration effect satisfies the requirements. Otherwise, you need to calibrate again, or perform fine adjustment to the coordinates by the methods for the manual calibration. Refer to step 5 of ***Manual Calibration*** for details.

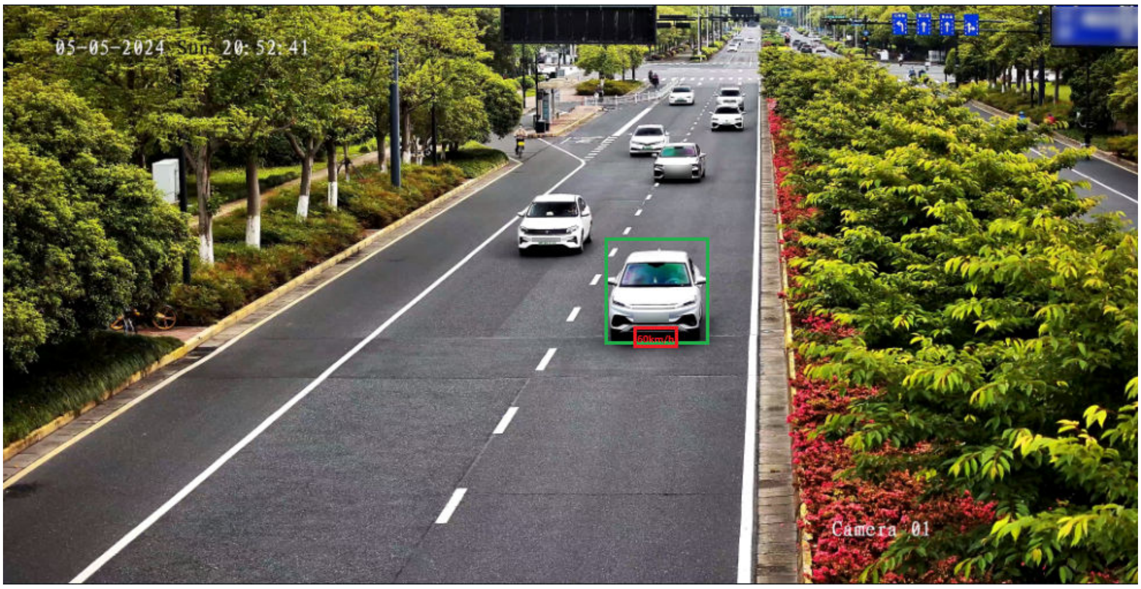


Figure 7-10 Good Calibration Effect Example

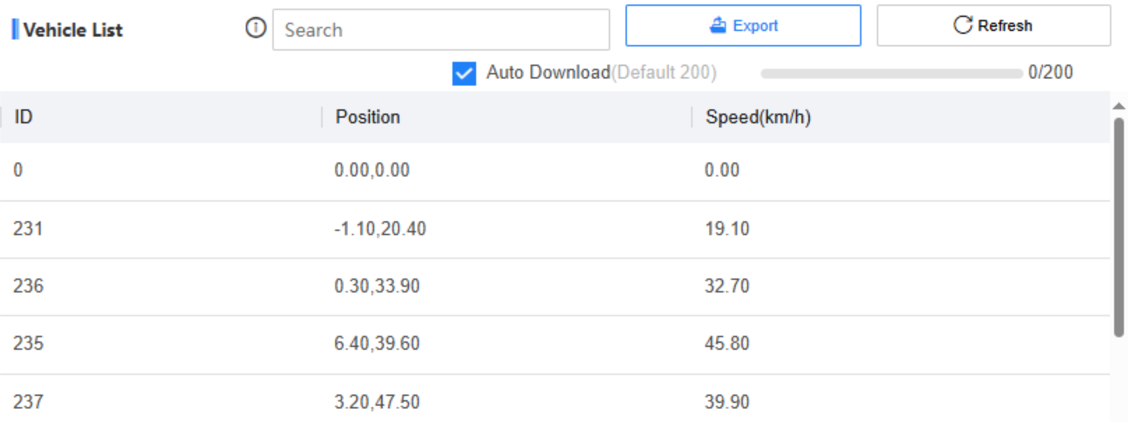
- For the scene with multiple lanes and congestion, observe the auto calibration effect. If the fusion effect is not good after the auto calibration is finished, you need to calibrate again manually. Refer to ***Manual Calibration*** for details.

7.4 Search Detected Vehicles

You can search the radar detected vehicles and export the information.

Steps

1. Click **Radar**.
2. View the detected vehicle information in the vehicle list.



☑ Auto Download(Default 200) 0/200

ID	Position	Speed(km/h)
0	0.00,0.00	0.00
231	-1.10,20.40	19.10
236	0.30,33.90	32.70
235	6.40,39.60	45.80
237	3.20,47.50	39.90

Figure 7-11 Vehicle List

3. Enter the vehicle No. in the text field, and press **Enter** to search the vehicle information.

4. **Optional:** Export the vehicle information.
   - Search the vehicle first, and click **Export** to export the searched vehicle information to the selected directory of the computer.
   - Click **Export** directly to export the information of all the detected vehicles to the selected directory of the computer.
5. **Optional:** In no plug-in mode, you can enable **Auto Download** to download the captured pictures to the computer directly.

Note

- If you have downloaded and installed plug-in, auto download is not supported.
- The latest captured pictures will be downloaded and compressed as a file in the format of .zip automatically. There are up to 200 pictures in one compressed file. If you exit from the current interface, the auto downloading will stop. The auto downloaded files will be saved to the default downloading directory of the browser in the format of .zip. You can go to the directory, decompress the file, and view the captured pictures.
- If you disable **Auto Download**, when you exit from the current interface, the dialogue box will pop up to prompt you if you need to download the arming captures. Click **OK** and the latest captured pictures will be downloaded and compressed as a file in the format of .zip automatically.

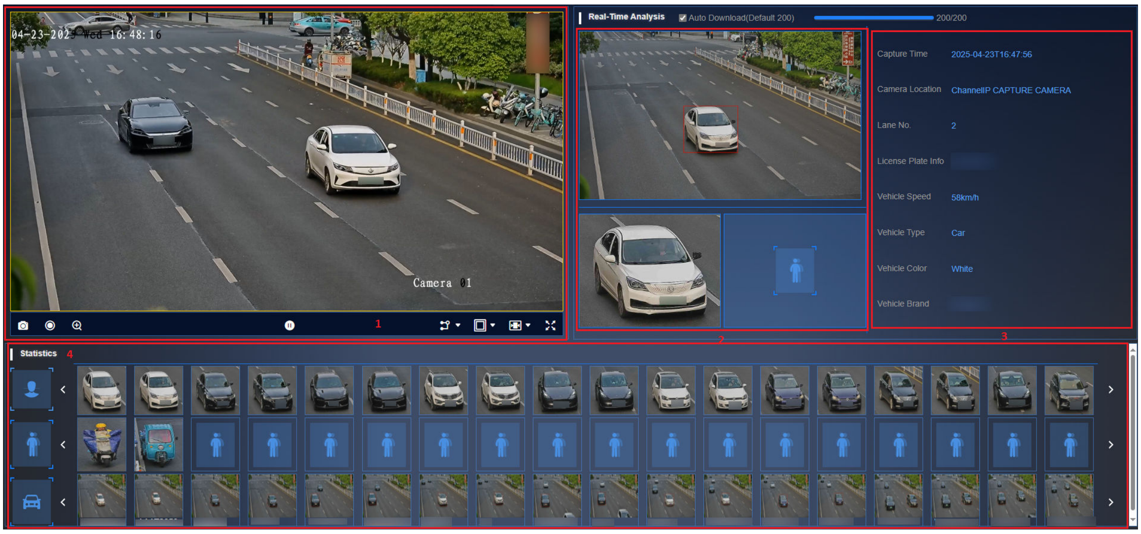
Chapter 8 Smart Display

You can view the live view image and the captured pictures in real time. The properties of the captured targets can be analyzed in real time and you can view the detailed information of the captured targets and data statistics results of the captured face pictures, motor vehicles, and non-motor vehicles.

Note

The smart display is only available for the browsers of IE 9 or above, Google Chrome 45 or above, Edge, and Firefox.

Click **Smart Display**. Refer to the figure and table below for the description of the interface.



Real-Time Analysis ☑ Auto Download(Default 200) 200/200

Capture Time 2025-04-23T16:47:56

Camera Location ChannelIP CAPTURE CAMERA

Lane No. 2

License Plate Info [redacted]

Vehicle Speed 58km/h

Vehicle Type Car

Vehicle Color White

Vehicle Brand [redacted]

Figure 8-1 Smart Display

Table 8-1 Smart Display Interface Description

No.	Description
1	The live view image. You can click the icons below the image to operate. Refer to ***Live View*** for details.
2	To display the captured pictures of motor vehicles, non-motor vehicles, and faces.
3	To view the detailed information of the captured targets.
4	To view the data statistics of the captured targets. You can click < or > to view more pictures.

Note

In no plug-in mode, you can enable **Auto Download** to download the captured pictures to the computer directly. The latest captured pictures will be downloaded and compressed as a file in the format of .zip automatically. The max. number of pictures in one compressed file depends on the selected **Number of Auto Captured Pictures** in **Configuration → Local** in no plug-in mode. If you exit from the interface, the auto downloading will stop. The auto downloaded files will be saved to the default downloading directory of the browser in the format of .zip. You can go to the directory, decompress the file, and view the captured pictures. If you disable **Auto Download**, when you exit from the interface, the dialogue box will pop up to prompt you if you need to download the arming captures. Click **OK** and the latest captured pictures will be downloaded and compressed as a file in the format of .zip automatically.

Chapter 9 View Real-Time Picture

You can view the real-time captured pictures and license plate information.

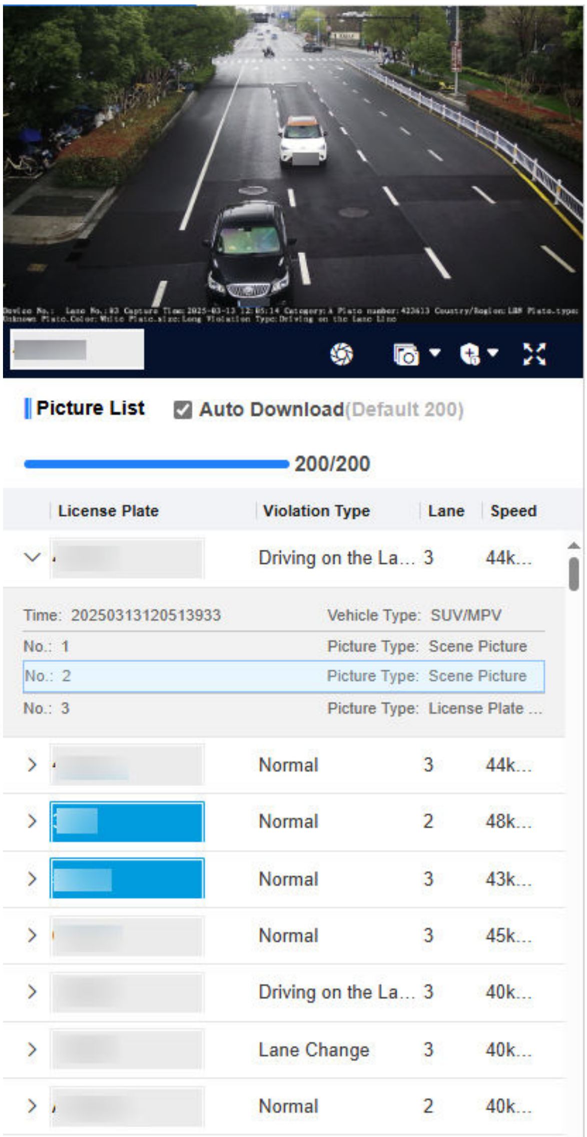
Steps

Note

- The supported parameters vary with different models. The actual device prevails.
- The supported functions are different in plug-in mode and no plug-in mode. In no plug-in mode, level 2 arming, measuring license plates, and enabling ruler are not supported.

1. Go to **Live View → Real-Time Capture** .
2. Click **Arming**.

   The device will capture pictures automatically according to the set application mode parameters.
3. Select an item from the list, and you can view the capture scene picture, vehicle type, violation type, speed, and recognized license plate information.



Device No.: Lane No.:03 Capture Time:2025-03-13 12:05:14 Category:A Plate number:422613 Country/Region:LBN Plate.type: Unknown Plate.Color:White Plate.size:Long Violation Type:Driving on the Lane Line

[redacted]

Picture List ☑ Auto Download(Default 200)

200/200

	License Plate	Violation Type	Lane	Speed
⌄	[redacted]	Driving on the La...	3	44k...

Time: 20250313120513933 Vehicle Type: SUV/MPV

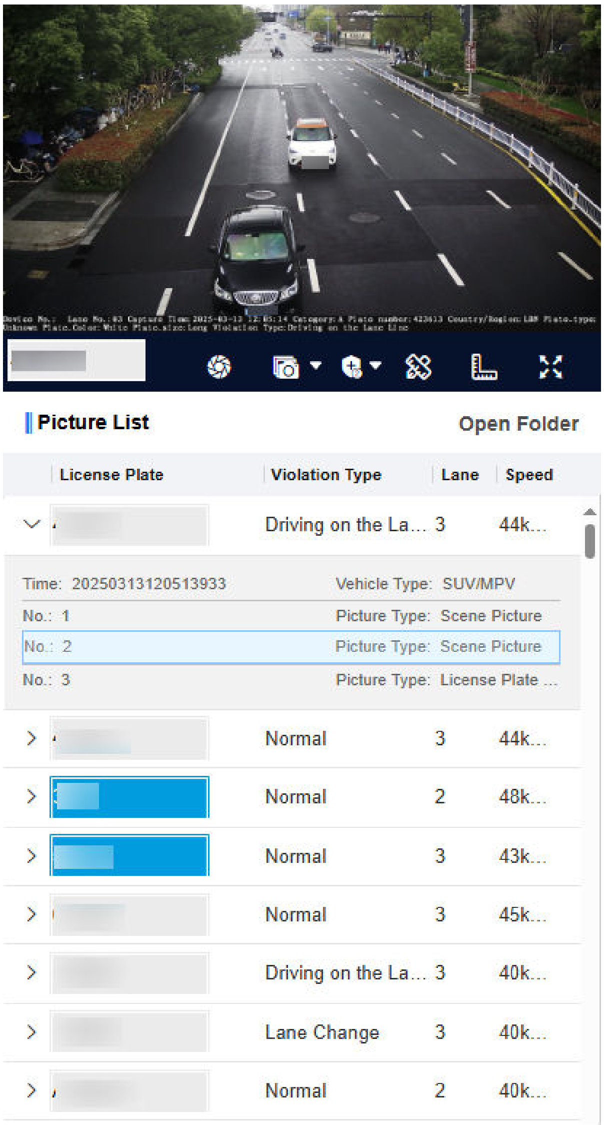
No.: 1 Picture Type: Scene Picture

No.: 2 Picture Type: Scene Picture

No.: 3 Picture Type: License Plate ...

	License Plate	Violation Type	Lane	Speed
>	[redacted]	Normal	3	44k...
>	[redacted]	Normal	2	48k...
>	[redacted]	Normal	3	43k...
>	[redacted]	Normal	3	45k...
>	[redacted]	Driving on the La...	3	40k...
>	[redacted]	Lane Change	3	40k...
>	[redacted]	Normal	2	40k...

Figure 9-1 Real-Time Capture (No Plug-in)



Device No.: Lane No.:03 Capture Time:2025-03-13 12:05:14 Category:A Plate number:423613 Country/Region:LBN Plate.type: Unknown Plate.Color:White Plate.size:Long Violation Type:Driving on the Lane Line

[redacted]

Picture List

Open Folder

	License Plate	Violation Type	Lane	Speed
∨	[redacted]	Driving on the La...	3	44k...

Time: 20250313120513933	Vehicle Type: SUV/MPV
No.: 1	Picture Type: Scene Picture
No.: 2	Picture Type: Scene Picture
No.: 3	Picture Type: License Plate ...

	License Plate	Violation Type	Lane	Speed
>	[redacted]	Normal	3	44k...
>	[redacted]	Normal	2	48k...
>	[redacted]	Normal	3	43k...
>	[redacted]	Normal	3	45k...
>	[redacted]	Driving on the La...	3	40k...
>	[redacted]	Lane Change	3	40k...
>	[redacted]	Normal	2	40k...

Figure 9-2 Real-Time Capture (with Plug-in)

4. **Optional:** You can do the following operations.

/ /	• **Level 1 Arming**: Only the current computer can arm the device and receive the captured pictures in real time. The pictures will not be stored in the storage card. The pictures in the storage card will be uploaded to the level 1 arming terminal. • **Level 2 Arming** can connect three clients or webs. The pictures will be uploaded to the client/web, and stored in the storage card. • **Disarming**: Disable the real-time capture function.
	Click it to capture a picture manually.

📷▾	Click the arrow to set continuous capture parameters and then click the icon to enable continuous capture manually. The device will capture pictures according to the set interval. • **Trigger Channel**: If the camera has multiple channels, enter the channel No. to enable continuous capture. • **Waiting Time**: Set the interval between continuous captures when triggering continuous capture continuously. • **Capture Times**: Select the number of captured pictures per continuous capture. • **Interval**: Set the interval between each capture in the continuous capture. Up to four intervals can be set, and the default interval is 100 ms.
⊠	The function is only available in plug-in mode. Click it to measure the license plate pixel. Click it again to disable the measurement.
📐	The function is only available in plug-in mode. Click it to enable the ruler to measure the license plate.
⛶	Click it to display the captured picture in full screen mode. Press **Esc** on the keyboard to exit from the full screen mode.
Open Folder	The button is available in plug-in mode. You can click it to open the saving path of captured pictures.
Auto Download	In no plug-in mode, you can enable **Auto Download** to download the captured pictures to the computer directly. The latest captured pictures will be downloaded and compressed as a file in the format of .zip automatically. The max. number of pictures in one compressed file depends on the selected **Number of Auto Captured Pictures** in **Configuration → Local** in no plug-in mode. If you disarm, the auto downloading will stop. You can view the downloading progress on the interface. The auto downloaded files will be saved to the default downloading directory of the browser in the format of .zip. You can go to the directory, decompress the file, and view the captured pictures. If you disable **Auto Download**, when you disarm, the dialogue box will pop up to prompt you if you need to download the arming captures. Click **OK** and the latest captured pictures will be downloaded and compressed as a file in the format of .zip automatically.

Chapter 10 Live View and Local Configuration

10.1 Live View

10.1.1 Start/Stop Live View

Click ▶ to start live view. Click ⏸ to stop live view.

10.1.2 Select Image Display Mode

Click ▣▾ to select an image display mode.

10.1.3 Select Window Division Mode

Click ▣▾ to select a window division mode.

10.1.4 Select Stream Type

Click ▾ to select the stream type. It is recommended to select the main stream to get the high-quality image when the network condition is good, and select the sub-stream to get the fluent image when the network condition is not good enough. The third stream is custom.

Note

The third stream varies with different models. The actual device prevails.

10.1.5 Capture Picture Manually

You can capture pictures manually on the live view image and save them to the computer.

Steps

1. Click 📷 to capture a picture.
2. **Optional:** Go to **Configuration → Local → Live View Parameters** and select **Image Format**.
3. **Optional:** Go to **Configuration → Local → Picture and Clip Settings** to view the saving path of snapshots in live view.

10.1.6 Record Manually

You can record videos manually on the live view image and save them to the computer.

Steps

1. Click ▶ to start live view.
2. Click ◎ to start recording.
3. Click ⏸ to stop recording.
4. **Optional:** Go to **Configuration → Local → Record File Settings** to view the saving path of record files.

10.1.7 Start/Stop Two-Way Audio

The device supports two-way audio with terminals, such as computers.

Before You Start

The device is equipped with an audio input interface and audio output interface, which support connecting with the corresponding devices, such as microphones and loudspeakers.

Steps

Note

The function varies with different models. The actual device prevails.

1. Select a window to start two-way audio.
2. Click ▶ to start live view.
3. Click 🎤 to start two-way audio.

   When speaking at the computer end, you can hear the voice at the device end and vice versa.
4. Click the icon again to stop two-way audio.

10.1.8 Enable/Disable Audio

Enable the audio if necessary after connecting an audio input device under the audio & video stream. Click 🔈▾ to enable and adjust it. Click again to disable this function.

Note

The function varies with different models. The actual device prevails.

10.1.9 Enable Digital Zoom

You can enable digital zoom to zoom in a certain part of the live view image.

Steps

1. Click ▶ to start live view.
2. Click 🔍 to enable digital zoom.
3. Place the cursor on the live view image position which needs to be zoomed in. Drag the mouse rightwards and downwards to draw an area.

The area will be zoomed in.

4. Click any position of the image to restore to normal image.
5. Click ⊕ to disable digital zoom.

10.1.10 Enable Regional Focus

Steps

Note

The function varies with different models. The actual device prevails.

1. Click ⊡ .
2. Drag the cursor from the upper left corner to the lower right corner to select the area that needs to be focused.

Result

The selected area is focused.

10.1.11 Select Video Mode

Set the video mode when adjusting the device focus during construction.

Click ▶ ▾ and select the normal mode when the device is running normally.

10.2 Set Snapshot Mode

Click **Live View**, and you can enable or disable snapshot mode on the upper right corner of the interface.

- 📷 : The snapshot mode is enabled. In this mode, only the image in the live view interface is in real-time streaming, and the live view images in other interfaces are just pictures. You can refresh the interfaces to refresh the pictures. For the conditions that the network is unstable, or the computer performance is not that good, you're recommended to enable snapshot mode to raise the operation efficiency.
- ⊠ : The snapshot mode is disabled. All the live view images are in real-time streaming.

Note

Disable snapshot mode before drawing areas for cropping capture pictures, ROI, privacy mask, and regional exposure.

10.3 PTZ Operation

Click **Live View**. The **PTZ Control** menu is displayed on the left.

Note

- The PTZ supports power-off memory. When the device is suddenly cut off power or restarted normally, it can automatically return to the position before the power cut or reboot.
- The PTZ function varies with different models. The actual device prevails.
- Other unmentioned buttons are reserved buttons.

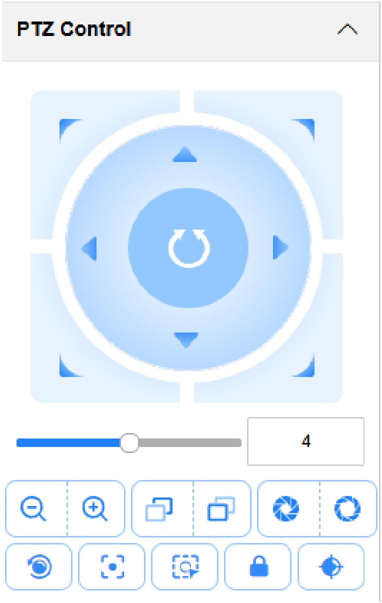


Figure 10-1 PTZ Control Panel

Table 10-1 Button Description

Button	Description
━━○── 4	Adjust the PTZ speed.
⊕ / ⊖	Zoom + and Zoom - • Hold ⊕ to zoom in the scene. • Hold ⊖ to zoom out the scene.
⧉ / ⧉	Focus + and Focus - • Hold ⧉ to make near objects become clear and distant objects become vague. • Hold ⧉ to make distant objects become clear and near objects become vague.
○ / ●	Iris + and Iris –

Button	Description
	• Hold ○ to increase the iris diameter when in a dark environment. • Hold ● to decrease the iris diameter when in a bright environment.
◉	Lens Initialization It is applicable to devices with motorized lenses. You can use this function when overcoming image blurs caused by overtime zooming or focusing.
⊡	Auxiliary Focus It is applicable to devices with motorized lenses. Use this function to focus the lens automatically and make images become clear.
⊡	Regional Auto Focus Click it and drag a rectangle on the live view image, and the area will be auto focused.
🔒 / 🔓	Lock/Unlock Click 🔒 to lock PTZ control, and click 🔓 to unlock PTZ control.
⌖	Zoom Calibration Click it and the lens will perform zoom calibration automatically.

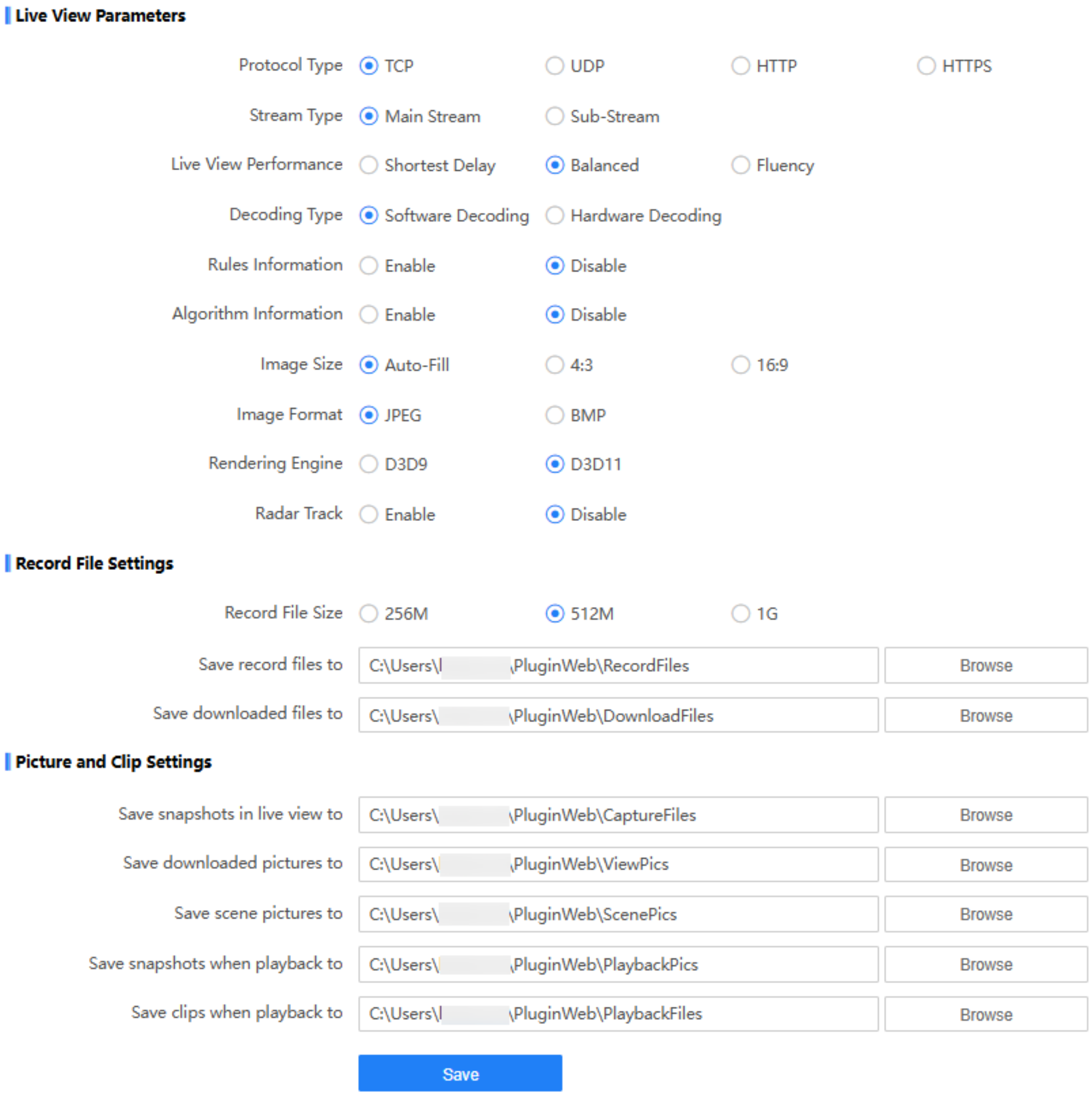
10.4 Local Configuration

Go to **Configuration → Local** to set the live view parameters and change the saving paths of videos, captured pictures, scene pictures, etc.

Note

The interfaces in no plug-in mode and plug-in mode are different.

Local Configuration in Plug-in Mode



Live View Parameters

Protocol Type ● TCP ○ UDP ○ HTTP ○ HTTPS

Stream Type ● Main Stream ○ Sub-Stream

Live View Performance ○ Shortest Delay ● Balanced ○ Fluency

Decoding Type ● Software Decoding ○ Hardware Decoding

Rules Information ○ Enable ● Disable

Algorithm Information ○ Enable ● Disable

Image Size ● Auto-Fill ○ 4:3 ○ 16:9

Image Format ● JPEG ○ BMP

Rendering Engine ○ D3D9 ● D3D11

Radar Track ○ Enable ● Disable

Record File Settings

Record File Size ○ 256M ● 512M ○ 1G

Save record files to C:\Users\[redacted]\PluginWeb\RecordFiles Browse

Save downloaded files to C:\Users\[redacted]\PluginWeb\DownloadFiles Browse

Picture and Clip Settings

Save snapshots in live view to C:\Users\[redacted]\PluginWeb\CaptureFiles Browse

Save downloaded pictures to C:\Users\[redacted]\PluginWeb\ViewPics Browse

Save scene pictures to C:\Users\[redacted]\PluginWeb\ScenePics Browse

Save snapshots when playback to C:\Users\[redacted]\PluginWeb\PlaybackPics Browse

Save clips when playback to C:\Users\[redacted]\PluginWeb\PlaybackFiles Browse

Figure 10-2 Local Configuration in Plug-in Mode

Protocol Type

Select the network transmission protocol according to the actual needs.

TCP

Ensures complete delivery of streaming data and better video quality, but the real-time transmission will be affected.

UDP

Provides real-time audio and video streams.

HTTP

Gets streams from the device by a third party client.

HTTPS

Gets streams in https format.

Stream Type

Main Stream

Select it to get the high-quality image when the network condition is good.

Sub-Stream

Select it to get the fluent image when the network condition is not good enough.

Live View Performance

Shortest Delay

The video is real-time, but its fluency may be affected.

Balanced

Balanced mode considers both the real time and fluency of the video.

Fluency

When the network condition is good, the video is fluent.

Decoding Type

Software Decoding

Decode via software. It takes up more CPU resources but provides images with better quality when it compares to the hardware decoding.

Hardware Decoding

Decode via GPU. It takes up less CPU resources but provides images with worse quality when it compares to the software decoding.

Rules Information

If you enable this function, tracking frames will be displayed on the live view interface when there are vehicles passing.

Algorithm Information

Enable it to overlay algorithm information of the stream.

Image Size

The display ratio of the live view image.

Image Format

The saving format of manually captured images.

Rendering Engine

Select the rendering API of the browser. D3D9 uses fixed rendering pipeline. D3D11 uses programmable graphics pipeline, in which the shader replaces the traditional fixed rendering pipeline to improve visual effects and enhance the picture quality.

Radar Track

When the radar is connected, enable it to generate and overlay the radar tracks.

Note

The function is only applicable to the device supporting radar.

Record File Size

Select the packed size of the manually recorded video files. After the selection, the max. record file size is the value you selected.

Save record files to

Set the saving path of the manually recorded video files.

Save downloaded files to

Set the saving path of the download files.

Save snapshots in live view to

Set the saving path of the manually captured pictures in live view mode.

Save downloaded pictures to

Set the saving path of the downloaded pictures.

Save scene picture to

Set the saving path of the captured pictures in **Live View → Real-Time Capture** .

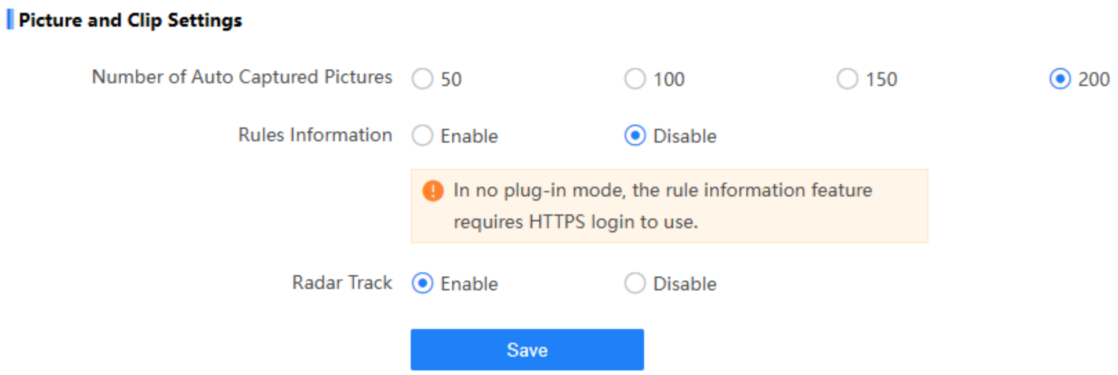
Save snapshots when playback to

Set the saving path of the manually captured pictures in playback mode.

Save clips when playback to

Set the saving path of the clips in playback mode.

Local Configuration in No Plug-in Mode



Picture and Clip Settings

Number of Auto Captured Pictures ○ 50 ○ 100 ○ 150 ● 200

Rules Information ○ Enable ● Disable

In no plug-in mode, the rule information feature requires HTTPS login to use.

Radar Track ● Enable ○ Disable

Figure 10-3 Local Configuration in No Plug-in Mode

Number of Auto Captured Pictures

Select the max. number of auto downloaded pictures in one compressed file in **Live View → Real-Time Capture** in no plug-in mode.

Rules Information

If you enable this function, tracking frames will be displayed on the live view interface when there are vehicles passing.

Note

In no plug-in mode, the rule information function requires access via HTTPS.

Radar Track

When the radar is connected, enable it to generate and overlay the radar tracks.

Note

The function is only applicable to the device supporting radar.

Chapter 11 Record and Capture

11.1 Set Storage Card

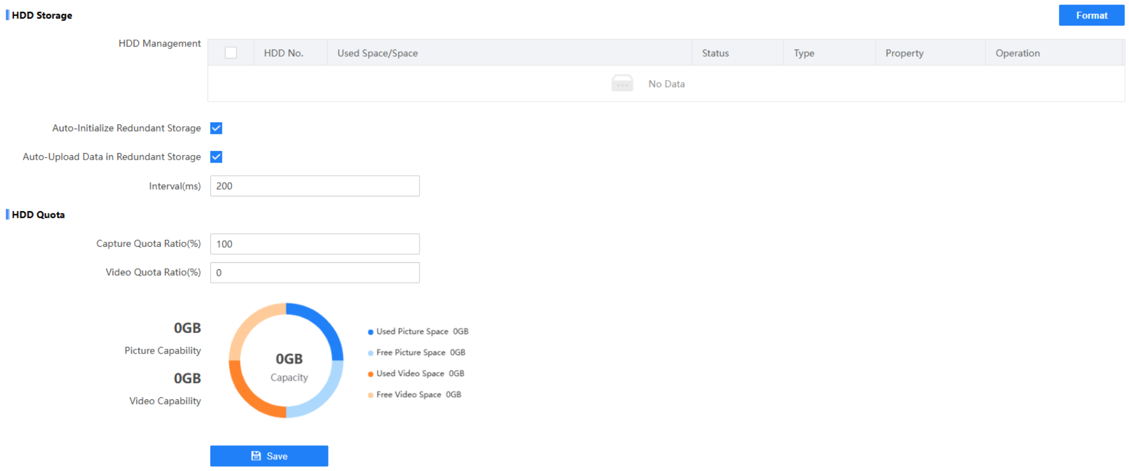
If you want to store the files to the storage card, make sure you insert and format the storage card in advance.

Before You Start

Insert the storage card to the device.

Steps

1. Go to **Configuration → Storage → Storage Management → HDD Management** .



HDD Storage

HDD Management

□	HDD No.	Used Space/Space	Status	Type	Property	Operation
No Data						

Auto-Initialize Redundant Storage ☑

Auto-Upload Data in Redundant Storage ☑

Interval(ms) 200

HDD Quota

Capture Quota Ratio(%) 100

Video Quota Ratio(%) 0

0GB Picture Capability

0GB Video Capability

0GB Capacity

- ● Used Picture Space 0GB
- ● Free Picture Space 0GB
- ● Used Video Space 0GB
- ● Free Video Space 0GB

Figure 11-1 Set Storage Card

2. Format the storage card in two ways.
   - Check the storage card, and click **Format** to format it manually.

     Note

     For the newly installed storage card, you need to format it manually before using it normally.
   - If you want to format the storage card automatically when the card is abnormal, enable **Auto-Initialize Redundant Storage**.

     Note

     If you enable **Auto-Initialize Redundant Storage**, reboot the device to take the settings into effect.
3. Set other parameters.

   Auto-Upload Data in Redundant Storage

   If the device has been connected to the platform, and you want to upload the storage card information automatically, enable the function and set the interval.

4. Set **Capture Quota Ratio** and **Video Quota Ratio** according to the actual needs.

Note

The percentage sum of the capture and video quota ratio should be 100%.

5. Click **Save**.

11.2 Set Record Schedule

Set record schedule to record video automatically during configured time periods.

Before You Start

Install the storage card.

Steps

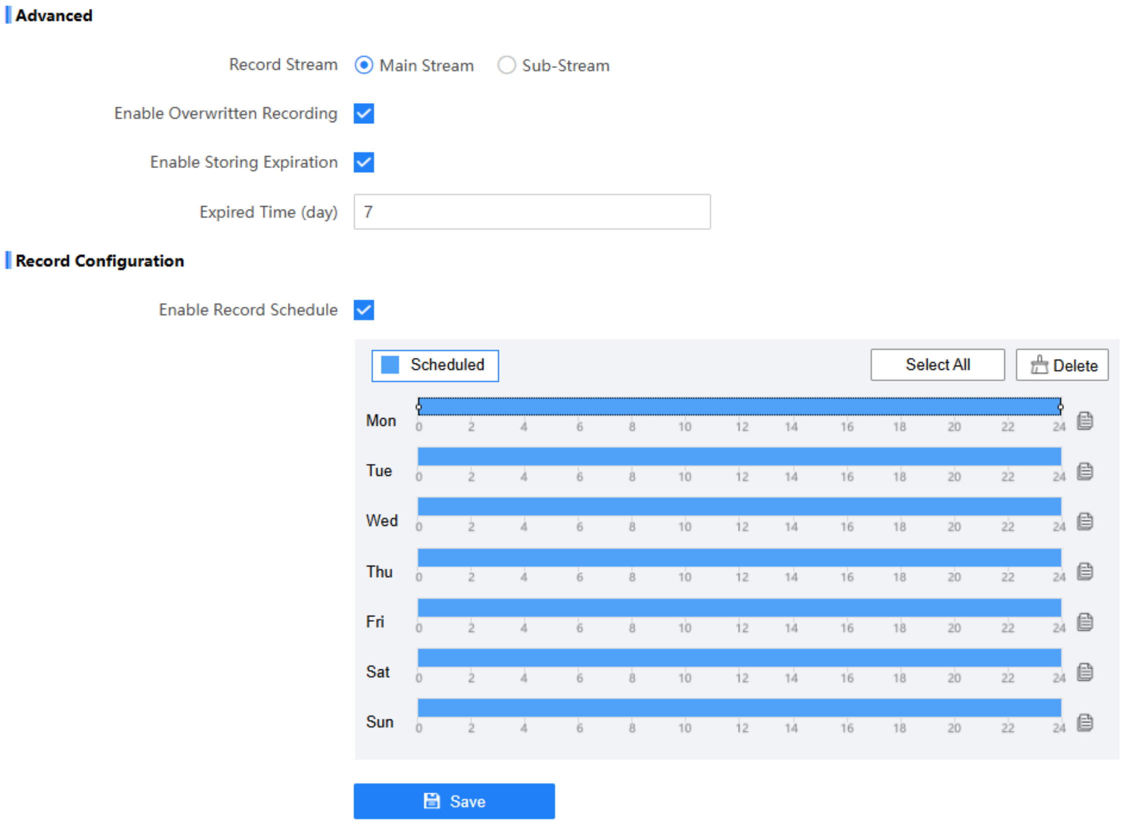
1. Go to **Configuration → Storage → Schedule Settings → Record Schedule** .
2. Select **Record Stream**.
3. **Optional:** Enable the functions below according to your needs.

   Enable Overwritten Recording

   When the storage is full, the earliest videos will be overwritten.

   Enable Storing Expiration

   Enable the function and set **Expired Time** for the recorded videos stored in the storage card. Beyond the time, the files will be overwritten.
4. Enable the record schedule.



Advanced

Record Stream ● Main Stream ○ Sub-Stream

Enable Overwritten Recording ☑

Enable Storing Expiration ☑

Expired Time (day) 7

Record Configuration

Enable Record Schedule ☑

Figure 11-2 Set Record Schedule

5. Click **Select All** to enable the device to record the whole days. Or drag the cursor on the time bar to set a recording time.

Note

Up to 8 time periods can be set on a time bar.

6. Adjust the recording time.
   - Click a set recording period and enter the start time and end time in the pop-up window.
   - Drag two ends of the set recording period bar to adjust the length.
   - Drag the whole set recording period bar and relocate it.
7. **Optional:** Delete recording periods.
   - Click a set recording period and click **Delete** in the pop-up window.
   - Click **Delete** on the record configuration interface to delete all the schedules.
8. **Optional:** Click 🗐 to copy the settings to other days.
9. Click **Save**.

Result

The device will only record at the set periods.

11.3 Set Snapshot Schedule

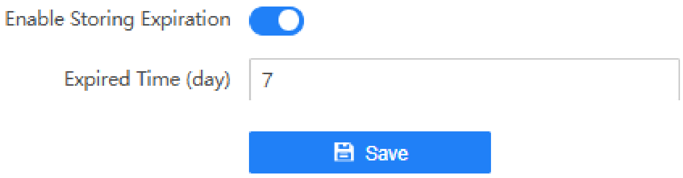
You can enable storage expiration of the snapshots saved in the storage card.

Before You Start

Install the storage card.

Steps

1. Go to **Configuration → Storage → Schedule Settings → Snapshot Schedule** .
2. Enable storing expiration.



Enable Storing Expiration

Expired Time (day) 7

Figure 11-3 Set Snapshot Schedule

3. Set **Expired Time**.
4. Click **Save**.

Result

Beyond the set expired time, the snapshots saved in the storage card will be overwritten.

11.4 Search Picture

You can search the captured pictures stored in the storage card and export the pictures you need.

Before You Start

Install the storage card, and ensure the storage status is normal.

Steps

1. Click **Picture**.
2. Set search conditions.

   Note

   Search conditions vary with different models. The actual device prevails.
3. Click **Search**.

   The searched pictures information will be displayed in the picture list.

Note

If you have set level 1 arming for the device, the captured pictures will not be saved in the storage card. Go to the saving path of scene pictures to view them. You can go to **Configuration → Local** to check the saving path.

4. **Optional:** You can do the following operations.

Download pictures	Check picture(s) and click **Download** to save them to local. The downloaded picture(s) will be marked as "Downloaded". You can go to **Configuration → Local** to check the saving path.
View picture details	Click **Live View** to view the picture details, such as the license plate number, vehicle type, etc.

11.5 Playback

You can search, play back, and download videos that stored on the storage card.

Steps

1. Click **Playback**.
2. Select a channel.
3. Select a date.
4. Click **Search**.
5. Click ▶ to start playback.
6. **Optional:** You can also do the following operations.

Set playback time	• Drag the time bar to the target time and click ▶ to play the video. • Click the current time point showed above the time bar and enter the target time point in the popup window. Click **OK** and click ▶ to play the video.
Capture image	Click 📷 to capture an image.
Clip record	Click ✂ / ✂ to start/stop clipping the record.
Play back in single frame	Click ⏯ once to play back the video in one frame.
Download record	a. Click ⤓ . b. Select the start time and end time. c. Click **Search**. d. Check record files that need to be downloaded. e. Click **Download**.
Stop playback	Click ■ to stop playback.
Slow forward	Click « to slow down the playback.
Fast forward	Click » to speed up the playback.

Digital zoom	Click 🔍 to enable digital zoom. Click 🔍 to disable digital zoom.

Chapter 12 Encoding and Display

12.1 Set Camera Parameters

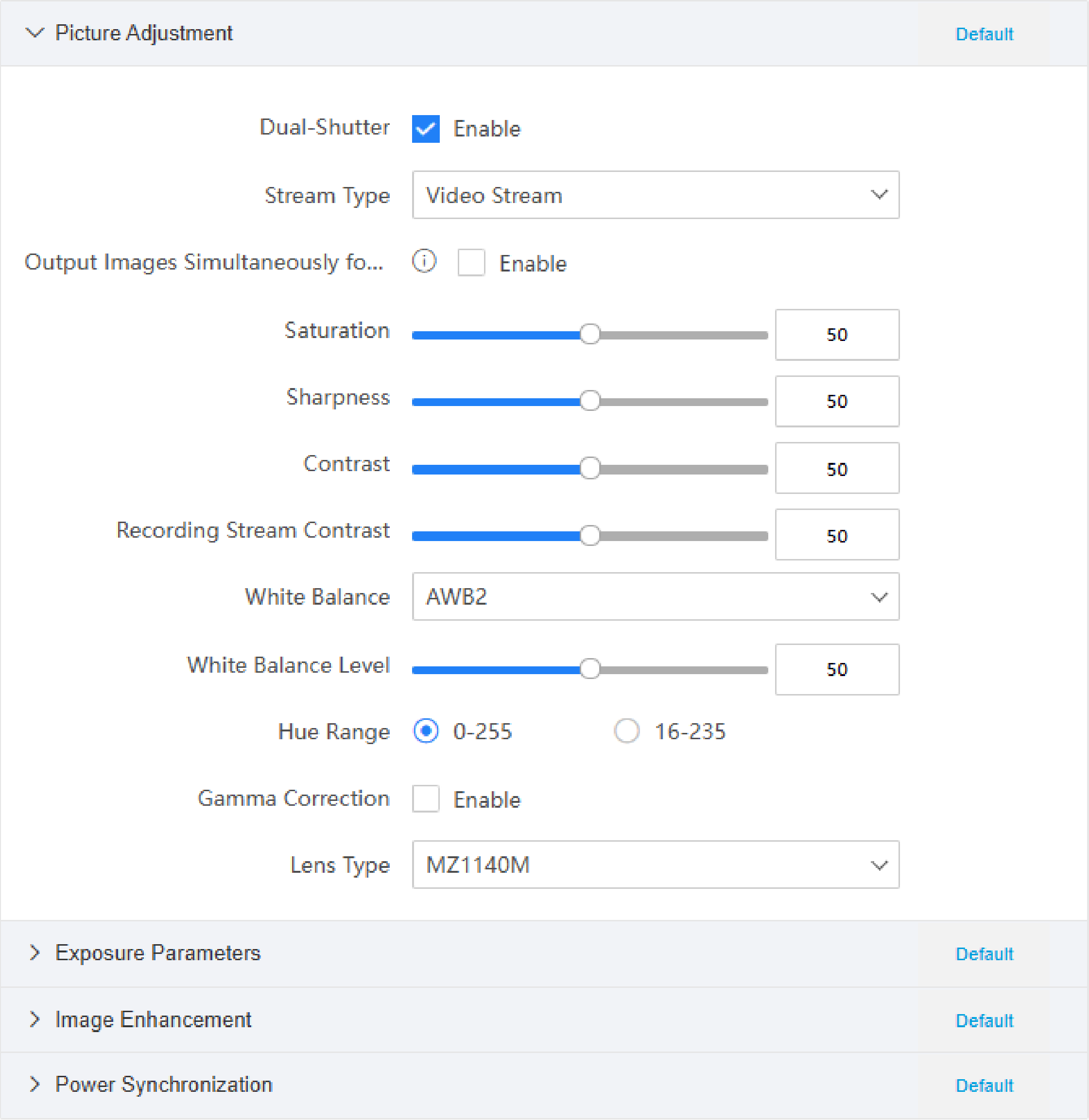
You can adjust the image parameters to get clear image.

Steps

Note

The supported parameters may vary with different models. The actual device prevails.

1. Go to **Configuration → Video → Camera Parameters → Camera Parameters** .
2. Set the camera parameters.



Picture Adjustment — Default

Dual-Shutter ☑ Enable

Stream Type: Video Stream

Output Images Simultaneously fo... ⓘ □ Enable

Saturation: 50

Sharpness: 50

Contrast: 50

Recording Stream Contrast: 50

White Balance: AWB2

White Balance Level: 50

Hue Range ● 0-255 ○ 16-235

Gamma Correction □ Enable

Lens Type: MZ1140M

Exposure Parameters — Default

Image Enhancement — Default

Power Synchronization — Default

Figure 12-1 Set Camera Parameters

Note

- The supported parameters vary with different models. The actual device prevails.
- You can click **Default** to restore the parameters to default settings.

Picture Adjustment

Dual-Shutter

Select **Stream Type** and enable **Output Images Simultaneously for Video and Recording Streams** (Recording stream does not produce images in flash light mode.) if needed after enabling it. Reboot the device to take the settings into effect.

Saturation

It refers to the colorfulness of the image color.

Sharpness

It refers to the edge contrast of the image.

Contrast

It refers to the contrast of the image. Set it to adjust the levels and permeability of the image.

White Balance

It is the white rendition function of the device used to adjust the color temperature according to the environment. Set **White Balance Level**.

Hue Range

Select the range to adapt to the display.

Gamma Correction

The higher the gamma correction value is, the stronger the correction strength is.

WDR Mode

Wide Dynamic Range (WDR) can be used when there is a high contrast of the bright area and the dark area of the scene.

Select **WDR Switch Mode** and set corresponding parameters according to your needs.

Enable

Set **WDR Level**. The higher the level is, the higher the WDR strength is.

Time

Enable WDR according to the set time period and level.

Brightness

Set **Brightness Threshold** and **WDR Level**. When the brightness reaches the threshold, WDR will be enabled.

Lens Type

Select the lens type according to the actual needs.

Exposure Parameters

Brightness

It refers to the brightness the image.

Shutter

If the shutter speed is quick, the details of the moving objects can be displayed better. If the shutter speed is slow, the outline of the moving objects will be fuzzy and trailing will appear.

Gain

It refers to the upper limit value of limiting image signal amplification. It is recommended to set a high gain if the illumination is not enough, and set a low gain if the illumination is enough.

Slow Shutter

This function can be used in underexposure condition. It lengthens the shutter time to ensure full exposure. The higher **Slow Shutter Level** is, the slower the shutter speed is.

Video Standard

Select the video standard according to the actual power supply frequency.

Image Enhancement

Brightness Enhancement at Night

The scene brightness will be enhanced at night automatically.

Plate Brightness Compensation

Check it. The plate brightness compensation can be realized, and various light supplement conditions can be adapted via setting license plate expectant brightness and supplement light correction coefficient. The higher the sensitivity is, the easier this function can be enabled.

3D DNR

Digital Noise Reduction (DNR) reduces the noise in the video stream.

In **Normal Mode**, the higher the **3D DNR Level** is, the stronger the noise will be reduced. But if it is too high, the image may become fuzzy.

In **Expert Mode**, set **Spatial Intensity** and **Time Intensity**. If the space domain intensity is too high, the outline of the image may become fuzzy and the details may lose. If the time domain intensity is too high, trailing may appear.

2D DNR

The higher the **2D DNR Level** is, the stronger the noise will be reduced. But if it is too high, the image may become fuzzy.

Defog

Enable defog to get a clear image in foggy days.

Black and White Mode at Night

When ICR is in night mode, you can check it to keep the video in black and white mode at night.

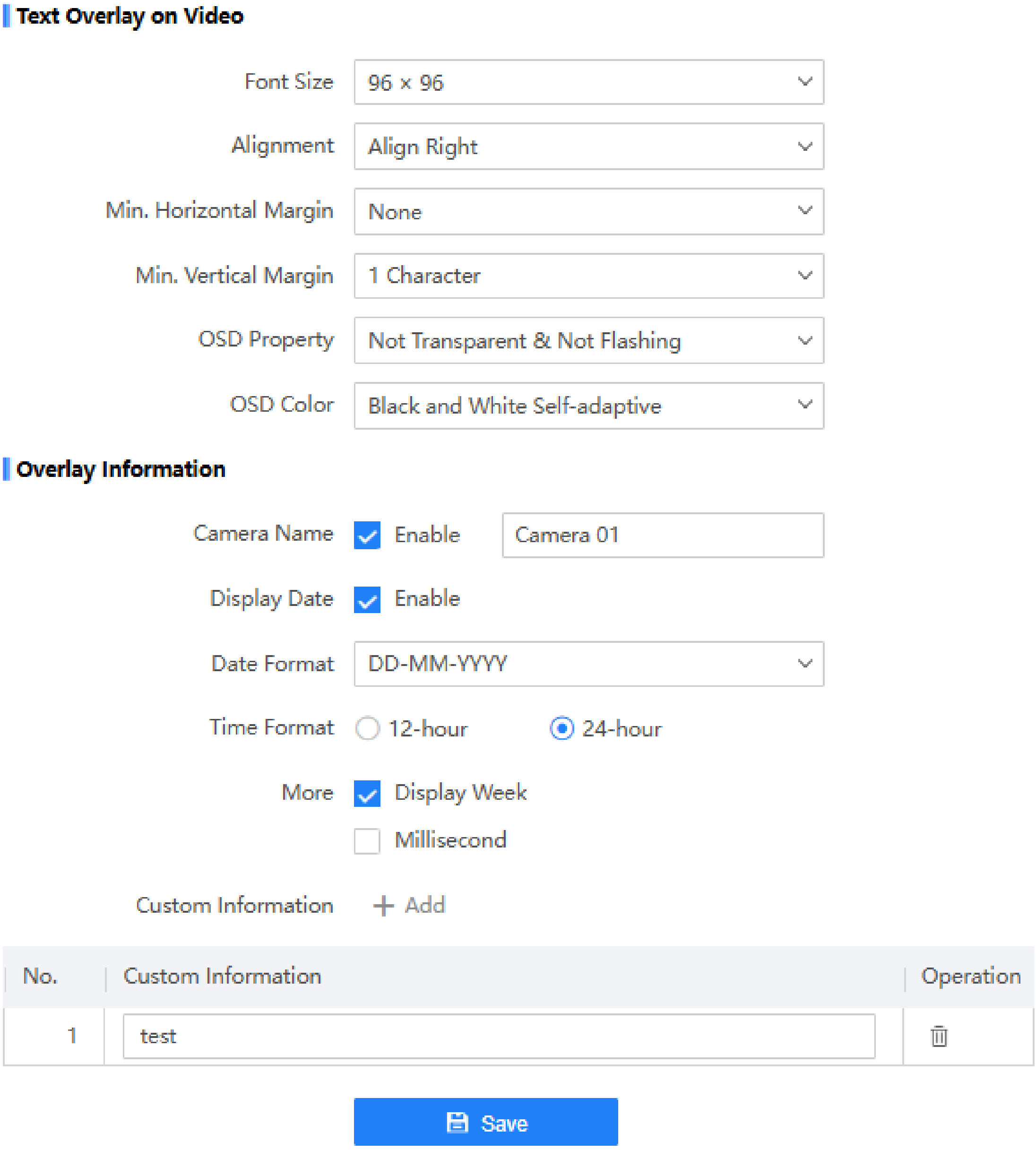
3. **Optional:** Click **Capture Test** to check the image effect.

12.2 Set OSD

You can customize OSD information on the live view.

Steps

1. Go to **Configuration → Video → Text Overlay on Video** .



Text Overlay on Video

Font Size: 96 × 96

Alignment: Align Right

Min. Horizontal Margin: None

Min. Vertical Margin: 1 Character

OSD Property: Not Transparent & Not Flashing

OSD Color: Black and White Self-adaptive

Overlay Information

Camera Name: ☑ Enable Camera 01

Display Date: ☑ Enable

Date Format: DD-MM-YYYY

Time Format: ○ 12-hour ● 24-hour

More: ☑ Display Week

☐ Millisecond

Custom Information: + Add

No.	Custom Information	Operation
1	test	🗑

Figure 12-2 Set OSD

2. Set display properties (font, color, etc.).

   Alignment

If you select **Align Left** or **Align Right**, set **Min. Horizontal Margin** and **Min. Vertical Margin**.

3. Set display contents.
   1) Enable **Camera Name**, and enter the camera name.
   2) Enable **Display Date**, and set the time and date format.
   3) Enable **Display Week** or **Millisecond** according to your needs.
4. **Optional:** Click **Add** and enter information if you want to add custom information.

   Note

   Up to 6 items of custom information can be added.
5. Drag the red frames on the live view image to adjust the OSD positions.
6. Click **Save**.

Result

The set OSD will be displayed in live view image and recorded videos.

12.3 Set Video Encoding Parameters

Set video encoding parameters to adjust the live view and recording effect.

- When the network signal is good and the speed is fast, you can set high resolution and bitrate to raise the image quality.
- When the network signal is bad and the speed is slow, you can set low resolution, bitrate, and frame rate to guarantee the image fluency.
- When the network signal is bad, but the resolution should be guaranteed, you can set low bitrate and frame rate to guarantee the image fluency.
- Main stream stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually means larger storage space and higher bandwidth requirements in transmission. Sub-stream usually offers comparatively low resolution options, which consumes less bandwidth and storage space. Third stream is offered for customized usage.

Steps

Note

The supported parameters vary with different models. The actual device prevails.

1. Go to **Configuration → Video → Video Encoding → Video Encoding** .
2. Set the parameters for different streams.

   Stream Type

   Select the stream type according to your needs.

   Note

   The supported stream types vary with different models. The actual device prevails.

Bitrate

Select relatively large bitrate if you need good image quality and effect, but more storage spaces will be consumed. Select relatively small bitrate if storage requirement is in priority.

Frame Rate

It is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Resolution

The higher the resolution is, the clearer the image will be. Meanwhile, the network bandwidth requirement is higher.

SVC

Scalable Video Coding (SVC) is an extension of the H.264/AVC and H.265 standard. Enable the function and the device will automatically extract frames from the original video when the network bandwidth is insufficient.

Bitrate Type

Select the bitrate type to constant or variable.

Video Quality

When bitrate type is variable, 6 levels of video quality are selectable. The higher the video quality is, the higher requirements of the network bandwidth.

Profile

When you select H.264 or H.265 as video encoding, you can set the profile. Selectable profiles vary according to device models.

I Frame Interval

It refers to the number of frames between two key frames. The larger the I frame interval is, the smaller the stream fluctuation is, but the image quality is not that good.

Video Encoding

The device supports multiple video encoding types, such as H.264, H.265, and MJPEG. Supported encoding types 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.

3. Click **Save**.

12.4 Set ROI

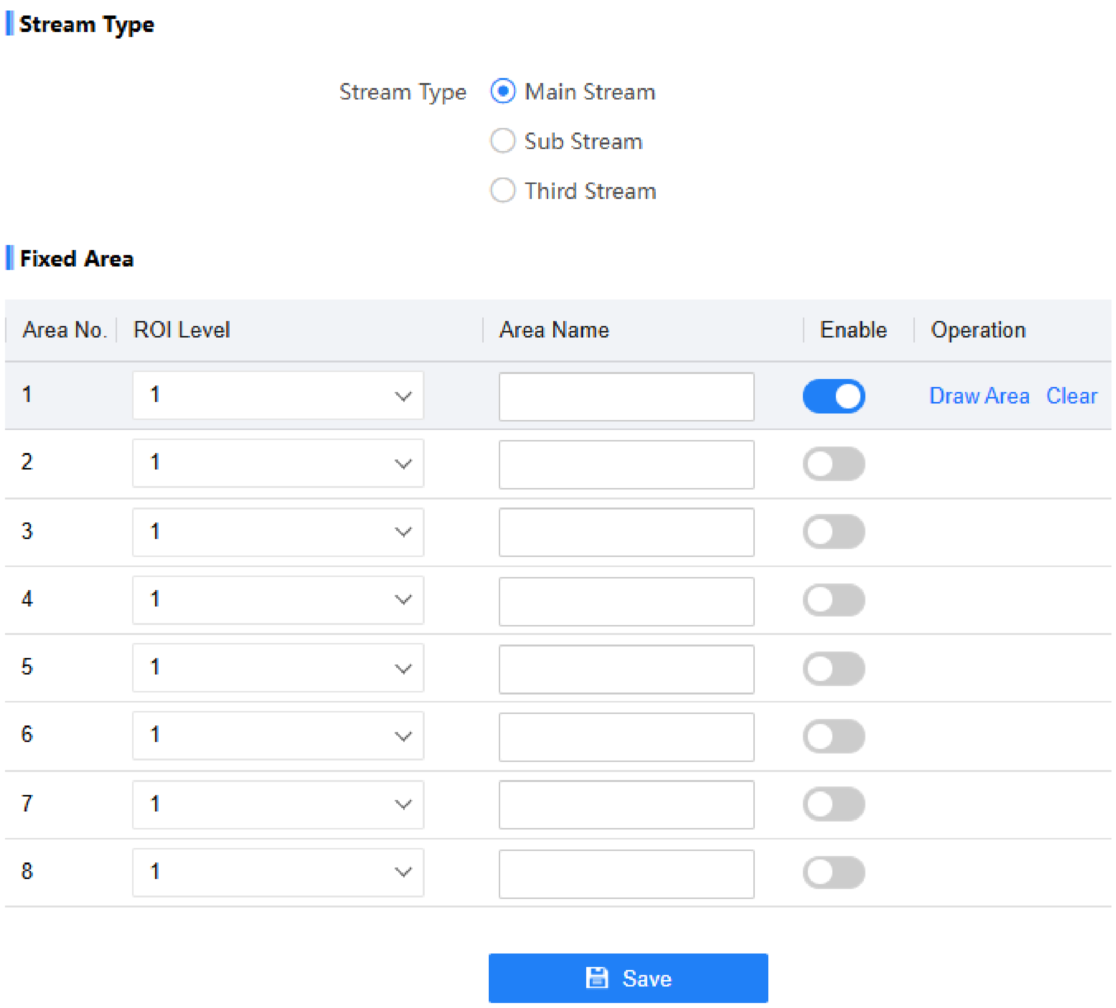
ROI (Region of Interest) encoding helps to assign more encoding resources to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

Before You Start

Please check the video encoding type. ROI is supported when the video encoding type is H.264 or H.265.

Steps

1. Go to **Configuration → Video → Video Encoding → ROI** .



Stream Type

Stream Type ● Main Stream
○ Sub Stream
○ Third Stream

Fixed Area

Area No.	ROI Level	Area Name	Enable	Operation
1	1		●	Draw Area Clear
2	1		○	
3	1		○	
4	1		○	
5	1		○	
6	1		○	
7	1		○	
8	1		○	

Figure 12-3 Set ROI

2. Select **Stream Type**.
3. Set ROI area.
   1) Enable the corresponding area.
   2) Select **ROI Level**.

   Note

   The higher the ROI level is, the clearer the image of the detected area is.

   3) Enter **Area Name**.
   4) Click **Draw Area**.

5) Drag the mouse on the live view image to draw the fixed area.
6) Select the fixed area that needs to be adjusted and drag the mouse to adjust its position.
7) Click **Stop Drawing**.
8) Repeat the steps above to set more areas. Up to 8 areas are supported.
9) **Optional:** If you want to delete the area, click **Clear** to delete.

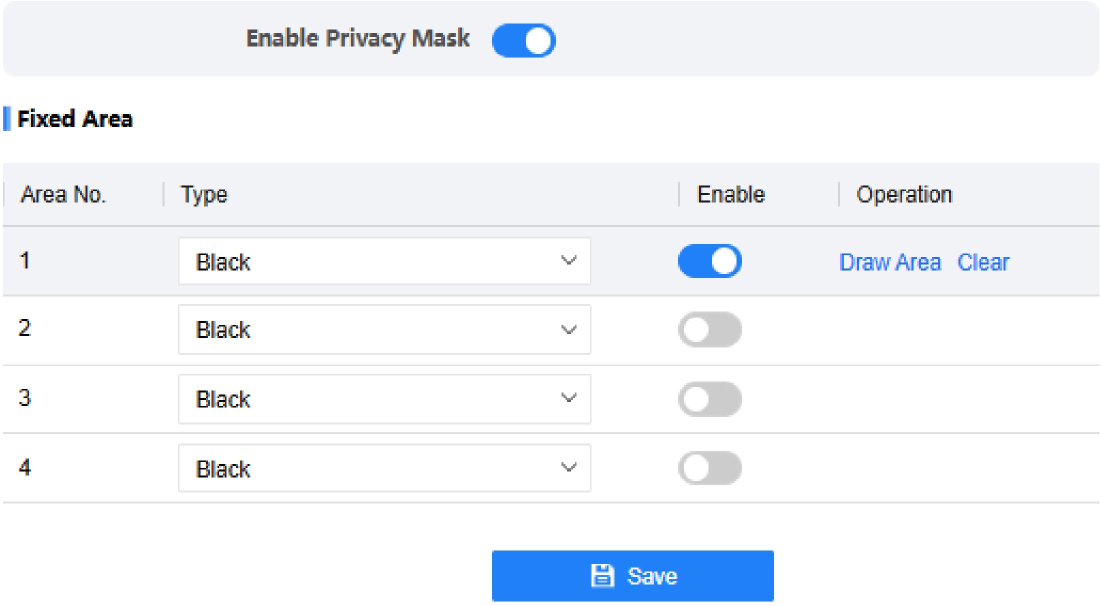
4. Click **Save**.

12.5 Set Privacy Mask

The privacy mask can be used to protect personal privacy by concealing parts of the image from view or recording with a masked area.

Steps

1. Go to **Configuration → Video → Video Encoding → Privacy Mask** .
2. Enable privacy mask.



Enable Privacy Mask ●

Fixed Area

Area No.	Type	Enable	Operation
1	Black	●	Draw Area Clear
2	Black	○	
3	Black	○	
4	Black	○	

Figure 12-4 Set Privacy Mask

3. Set the privacy mask area.
   1) Enable the corresponding privacy mask area.
   2) Select **Type**.
   3) Click **Draw Area**.
   4) In the live view image, drag the mouse to draw the privacy mask area of the selected area No.
   5) Click **Stop Drawing**.
   6) Repeat the steps above to set more areas. Up to 4 areas are supported.
   7) **Optional:** If you want to delete the area, click **Clear** to delete.
4. Click **Save**.

12.6 Enable Regional Exposure

Enable regional exposure to expose partial area of the live view image.

Steps

1. Go to **Configuration → Video → Video Encoding → BLC** .
2. Enable **Regional Exposure**.
3. Drag the mouse to draw an area in the live view image.

   The drawn area will be exposed.
4. Click **Save**.

Chapter 13 Serial Port Configuration

13.1 Set RS-485

Set RS-485 parameters if the device needs to be connected to other peripheral devices controlled by RS-485 serial port.

Before You Start

The corresponding device has been connected via the RS-485 serial port.

Steps

Note

The number of available RS-485 serial port varies with different models.

1. Go to **Configuration → System → System Settings → Serial Port → RS-485** .
2. Set **Baud Rate**, **Data Bit**, **Stop Bit**, etc.

   Note

   The parameters should be same with those of the connected device.
3. Set **Work Mode**.

   Note

   - The supported work modes vary with different models. The actual device prevails.
   - You need to reboot the device after editing the work mode to take effect.

   Application Trigger

   Select it when a signal trigger device (such as a radar) is connected to the RS-485 serial port of the device.

   Transparent Channel

   Select it when the other peripheral device is connected to the RS-485 serial port of the device for communication transmission.

   Traffic Signal Controller Mode

   Select it when a traffic signal controller is connected to the RS-485 serial port of the device for communication transmission.
4. Click **Save**.

13.2 Set RS-232

Set RS-232 parameters if you need to debug the device via RS-232 serial port.

Before You Start

The debugging device has been connected via the RS-232 serial port.

Steps

1. Go to **Configuration → System → System Settings → Serial Port → RS-232** .
2. Set **Baud Rate**, **Data Bit**, **Stop Bit**, etc.

   Note

   The parameters should be same with those of the connected device.
3. Select **Work Mode**.

   Note

   - The supported work modes vary with different models. The actual device prevails.
   - You need to reboot the device after editing the work mode to take effect.

   Console

   Select it when you need to debug the device via RS-232 serial port.

   Transparent Channel

   Select it, and the network command can be transmitted to RS-232 control command via the RS-232 serial port.

   Narrow Bandwidth Transmission

   Reserved.
4. Click **Save**.

Chapter 14 Event and Alarm

14.1 Exception Alarm

Set exception alarm when the network is disconnected, the IP address is conflicted, etc.

Steps

Note

The supported exception types vary with different models. The actual device prevails.

1. Go to **Configuration → Event → Alarm Linkage → Exception** .
2. Select the exception type(s) and the linkage method.
3. Click **Save**.

14.2 Set Email

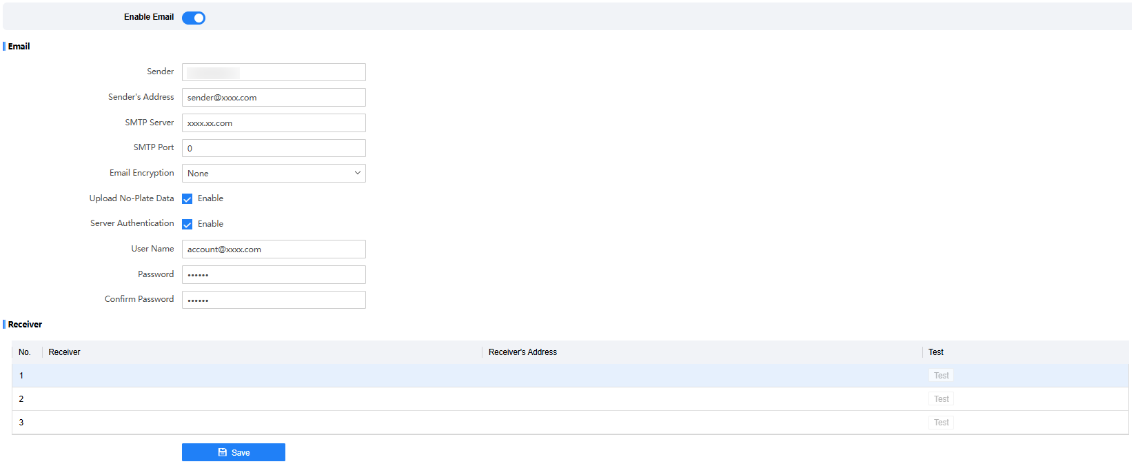
When the email is enabled and set, the device will send an email notification to all designated receivers if an alarm event is detected.

Before You Start

Set the DNS server before using the email function. Go to **Configuration → Network → Network Parameters → Network Interface** for DNS settings.

Steps

1. Go to **Configuration → Network → Data Connection → Email** .
2. Enable Email.



Enable Email ●

Email

Sender

Sender's Address: sender@xxxx.com

SMTP Server: xxxx.xx.com

SMTP Port: 0

Email Encryption: None

Upload No-Plate Data: ☑ Enable

Server Authentication: ☑ Enable

User Name: account@xxxx.com

Password: ······

Confirm Password: ······

Receiver

No.	Receiver	Receiver's Address	Test
1			Test
2			Test
3			Test

Figure 14-1 Set Email

3. Set email parameters.

1) Enter the sender's email information, including **Sender**, **Sender's Address**, **SMTP Server**, and **SMTP Port**.
2) Select **Email Encryption**.

   None

   Emails are sent without encryption.

   TLS

   Emails are sent after being encrypted by TLS.
3) **Optional:** If you want to upload no-plate data, enable **Upload No-Plate Data**.
4) **Optional:** If your email server requires authentication, enable **Server Authentication** and enter your user name and password to log in to the server.
5) Enter the receiver's information, including the receiver's name and address.
6) **Optional:** Click **Test** to test if the function is well configured.

4. Click **Save**.

14.3 Set Email Event

When the set event occurs, the device can be set to send an email with alarm information to the user.

Before You Start

The email has been enabled and related email parameters have been configured.

Steps

1. Go to **Configuration → Event → Alarm Linkage → Email Event** .
2. Enable linkage to trigger an email for login alarm.
3. Click **Save**.

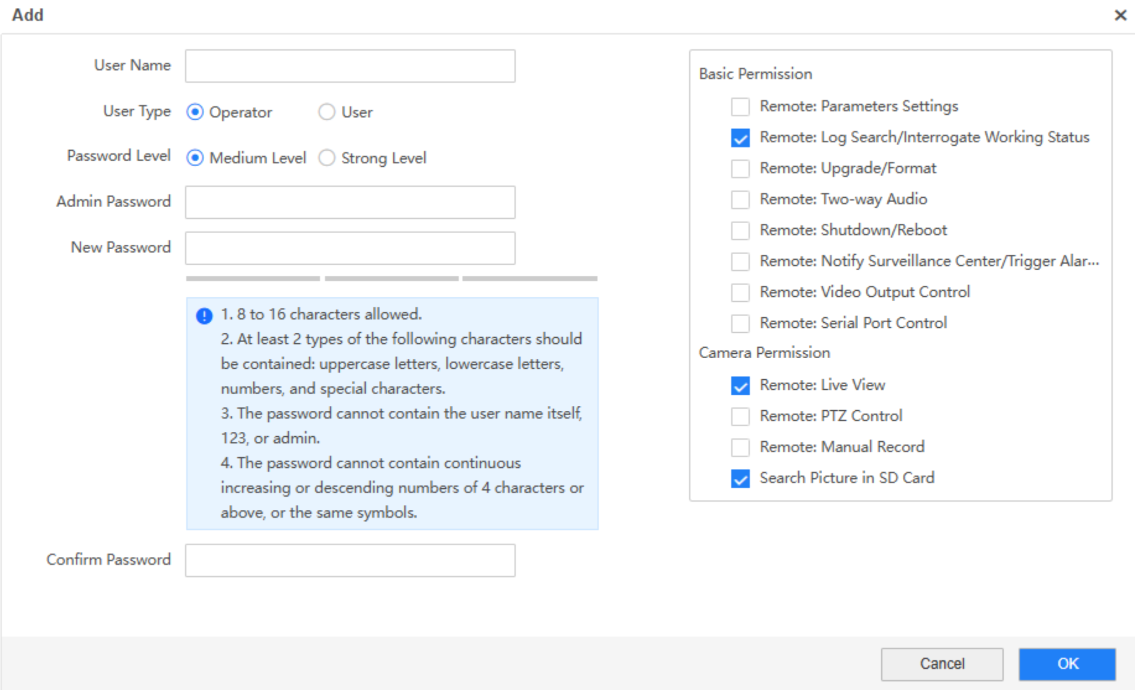
Chapter 15 Safety Management

15.1 Manage User

The administrator can add, modify, or delete other accounts, and grant different permissions to different user levels.

Steps

1. Go to **Configuration → System → User Management → User List** .
2. Add a user.



Add

User Name

User Type ● Operator ○ User

Password Level ● Medium Level ○ Strong Level

Admin Password

New Password

1. 8 to 16 characters allowed.
2. At least 2 types of the following characters should be contained: uppercase letters, lowercase letters, numbers, and special characters.
3. The password cannot contain the user name itself, 123, or admin.
4. The password cannot contain continuous increasing or descending numbers of 4 characters or above, or the same symbols.

Confirm Password

Basic Permission

- □ Remote: Parameters Settings
- ☑ Remote: Log Search/Interrogate Working Status
- □ Remote: Upgrade/Format
- □ Remote: Two-way Audio
- □ Remote: Shutdown/Reboot
- □ Remote: Notify Surveillance Center/Trigger Alar...
- □ Remote: Video Output Control
- □ Remote: Serial Port Control

Camera Permission

- ☑ Remote: Live View
- □ Remote: PTZ Control
- □ Remote: Manual Record
- ☑ Search Picture in SD Card

Figure 15-1 Add User

1) Click **Add**.
2) Enter **User Name** and select **User Type**.
3) Select **Password Level**. The password level of the added user should conform to the selected level.
4) Enter **Admin Password**, **New Password**, and confirm the password.

Caution

To increase security of using the device on the network, please change the password of your account regularly. Changing the password every 3 months is recommended. If the device is used in high-risk environment, it is recommended that the password should be changed every month or week.

5) Assign remote permissions to users based on needs.

User

Users can be assigned permissions of viewing live video and changing their own passwords, but no permissions for other operations.

Operator

Operators can be assigned all permissions except for operations on the administrator and creating accounts.

6) Click **OK**.

3. **Optional:** You can do the following operations.

Edit the user information	Click ✎ to edit the user information.
Delete the user	Click 🗑 to delete the user.

15.2 Enable User Lock

To raise the data security, you are recommended to lock the current IP address.

Steps

1. Go to **Configuration → System → Security → Security Service → Software** .
2. Check **Enable User Lock**.
3. Click **Save**.

Result

When the times you entered incorrect passwords have reached the limit, the current IP address will be locked automatically.

15.3 Set SSH

To raise network security, you are recommended to disable SSH service. The configuration is only used to debug the device for the professionals.

Steps

1. Go to **Configuration → System → Security → Security Service → Software** .
2. Enable or disable **SSH Service**, and set **SSH Port** if you enable the function.
3. Click **Save**.

15.4 Prohibit PING

You can prohibit the external devices to operate network connection volume test to the current device.

Steps

1. Go to **Configuration → System → Security → Security Service → Software**
2. Enable **Prohibit PING**.
3. Click **Save**.

15.5 Set SDK Protocol Authentication Mode

When you need to operate development integration or data collection via SDK protocol, you are recommended to enable SDK protocol authentication to enhance the information security.

Steps

1. Go to **Configuration → System → Security → Security Service → Authentication Settings** .
2. Select **SDK Protocol Authentication Mode**.

   Note

   You are recommended to select **Safety Mode**. In this mode, the device cannot be logged in via an invertible password of SDK protocol, which can enhance the information security.
3. Click **Save**.

15.6 Set RTSP Authentication

You can improve network access security by setting RTSP authentication.

Steps

1. Go to **Configuration → System → Security → Security Settings → Authentication Settings** .
2. Select **RTSP Authentication**.

   digest

   The device only supports digest authentication.
3. Click **Save**.

15.7 Set Timeout Logout

You can improve network access security by setting timeout logout.

Steps

1. Go to **Configuration → System → Security → Security Service → Login Management** .
2. Enable timeout logout for static page.
3. Set **Max. Timeout**.
4. Click **Save**.

Result

When the page static time exceeds the set time, the device will automatically log out.

15.8 Set Password Validity Period

You can improve network access security by setting password validity period.

Steps

1. Go to **Configuration → System → Security → Security Service → Login Management** .
2. Select **Password Validity Period**.
   - Select **Permanent**. The password will be permanently valid.
   - Select **Daily** and set **Password Expiry Time**. It will prompt you that the password is expired according to the set password expiry time, and you need to set the new password.
3. Click **Save**.

15.9 Set IP Address Filtering

You can set the IP addresses allowable and not allowable to access the device.

Steps

1. Go to **Configuration → System → Security → Security Settings** .
2. Enable IP address filtering.
3. Set **Filtering Mode**.

   Blocklist Mode

   The added IP addresses are not allowed to access the device.

   Allowlist Mode

   The added IP addresses are allowed to access the device.
4. Click **Add**, enter the IP address, and click **OK**.

   Note

   The IP address only refers to the IPv4 address.
5. **Optional:** Edit, delete, or clear the added IP addresses.
6. Click **Save**.

15.10 Set HTTPS

15.10.1 Create and Install Self-signed Certificate

HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Configuration → Network → Network Parameters → HTTPS** .

2. Select **Create Self-signed Certificate**.
3. Click **Create**.
4. Follow the prompt to enter **Country/Region**, **Domain/IP**, **Validity**, and other parameters.
5. Click **OK**.

Result

The device will install the self-signed certificate by default.

15.10.2 Install Authorized Certificate

If the demand for external access security is high, you can create and install authorized certificate via HTTPS protocol to ensure the data transmission security.

Steps

1. Go to **Configuration → Network → Network Parameters → HTTPS** .
2. Select **Create certificate request first and continue the installation**.
3. Click **Create**.
4. Follow the prompt to enter **Country/Region**, **Domain/IP**, **Validity**, and other parameters.
5. Click **Download** to download the certificate request and submit it to the trusted authority for signature.
6. Import certificate to the device.
   - Select **Signed certificate is available, start the installation directly**. Click **Browse** and **Install** to import the certificate to the device.
   - Select **Create the certificate request first and continue the installation**. Click **Browse** and **Install** to import the certificate to the device.
7. Click **Save**.

Chapter 16 Maintenance

16.1 View Device Information

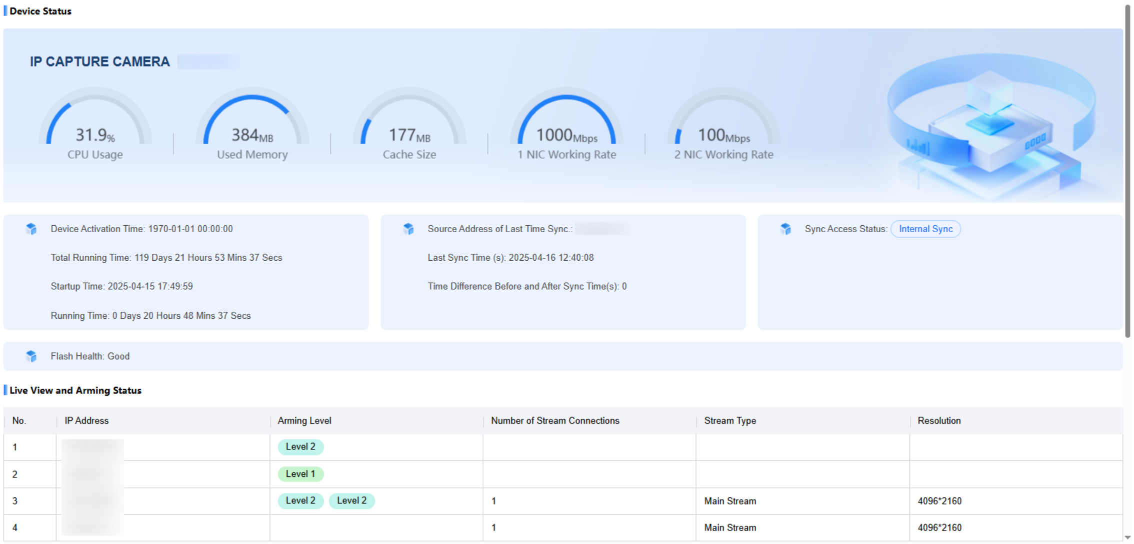
Basic Information and Algorithms Library Version

Go to **Configuration → System → System Settings → Basic Information** to view the basic information and algorithms version of the device.

You can edit **Device Name** and **Device No.** The device No. is used to control the device. It is recommended to reserve the default value.

Device Status

Go to **Configuration → System → System Settings → Device Status** to view the device status, live view and arming status, and data upload monitoring.



Device Status

IP CAPTURE CAMERA [redacted]

31.9% CPU Usage

384MB Used Memory

177MB Cache Size

1000Mbps 1 NIC Working Rate

100Mbps 2 NIC Working Rate

Device Activation Time: 1970-01-01 00:00:00

Total Running Time: 119 Days 21 Hours 53 Mins 37 Secs

Startup Time: 2025-04-15 17:49:59

Running Time: 0 Days 20 Hours 48 Mins 37 Secs

Source Address of Last Time Sync.: [redacted]

Last Sync Time (s): 2025-04-16 12:40:08

Time Difference Before and After Sync Time(s): 0

Sync Access Status: Internal Sync

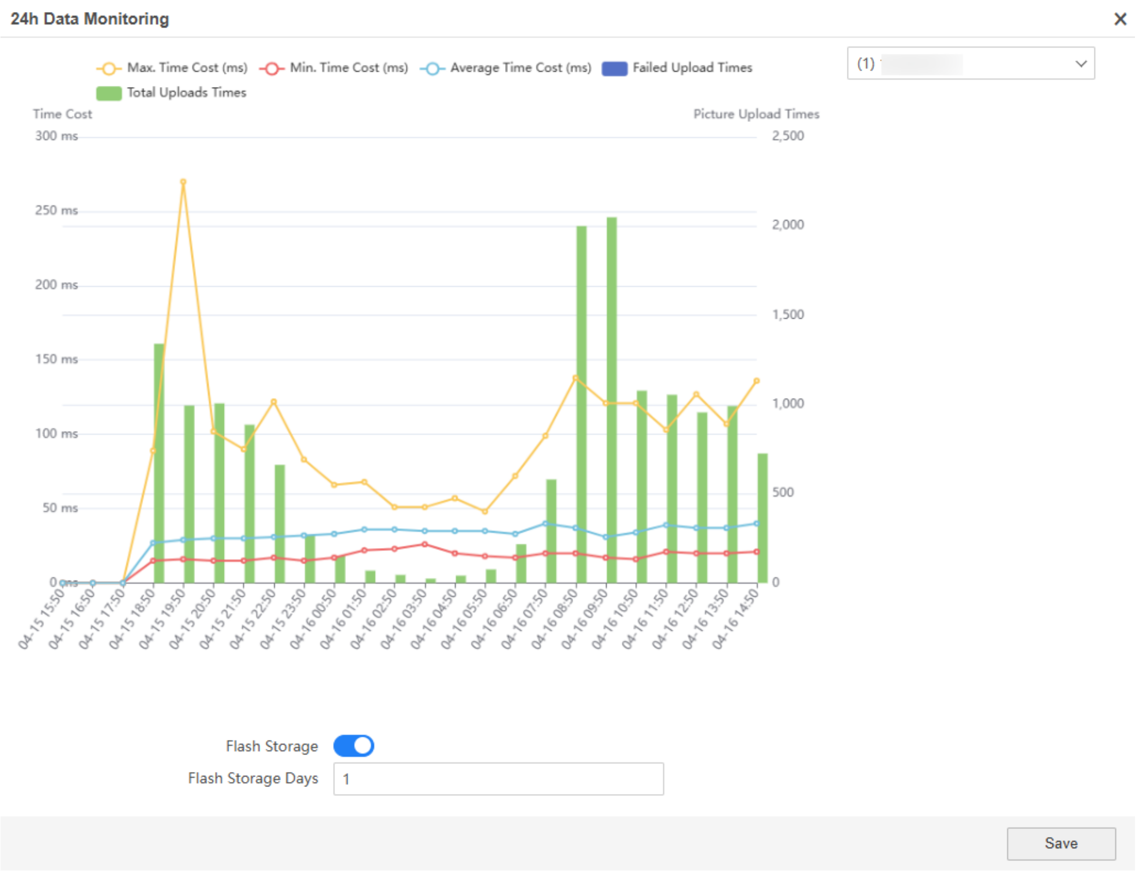
Flash Health: Good

Live View and Arming Status

No.	IP Address	Arming Level	Number of Stream Connections	Stream Type	Resolution
1	[redacted]	Level 2			
2	[redacted]	Level 1			
3	[redacted]	Level 2 Level 2	1	Main Stream	4096*2160
4	[redacted]		1	Main Stream	4096*2160

Figure 16-1 Device Status

You can click **24h Data Monitoring**, and select the IP address of the picture upload server to view the data upload statistics in 24 hours. The statistics data will be cleared if the device is rebooted by default. You can enable **Flash Storage** and set **Flash Storage Days** to keep the statistics data not to be cleared when the device is rebooted within the set time.



Flash Storage ●

Flash Storage Days 1

Figure 16-2 24h Data Monitoring

16.2 Synchronize Time

Synchronize the device time when it is inconsistent with the actual time.

Steps

1. Go to **Configuration → System → System Settings → Time Settings** .
2. Select **Time Zone**.
3. Select **Sync Mode**.

   NTP Time Sync.

   Select it to synchronize the device time with that of the NTP server. Set **Server IP**, **NTP Port**, and **Interval**. Click **NTP Test** to test if the connection between the device and the server is normal.

   Manual Time Sync.

   Select it to synchronize the device time with that of the computer. Set time manually, or check **Sync. with computer time**.

SDK

If the remote host has been set for the device, select it to synchronize time via the remote host.

ONVIF

Select it to synchronize time via the third-party device.

No

Select it to disable time synchronization.

All

Select it, and you can select any mode above.

PTP Time Sync.

Select it to synchronize time more accurately. Precision Time Protocol (PTP) is a protocol to synchronize clocks in a computer network, similar to NTP. NTP is accurate, under ten milliseconds. PTP, however, is accurate up to less than a microsecond and is measured in nanoseconds.

Note

The time synchronization modes vary with different models. The actual device prevails.

4. Click **Save**.

16.3 Set DST

If the region where the device is located adopts Daylight Saving Time (DST), you can set this function.

Steps

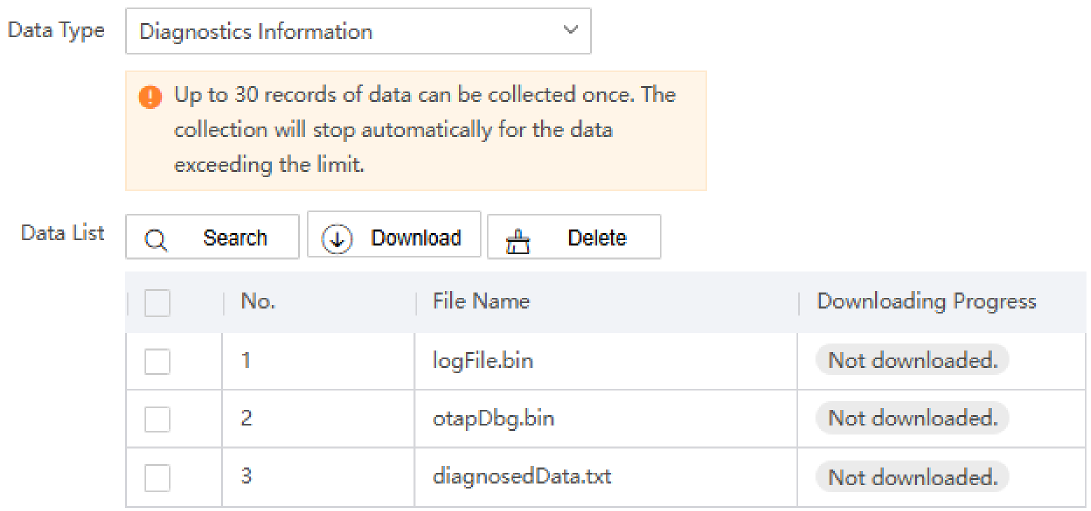
1. Go to **Configuration → System → System Settings → DST** .
2. Enable **DST**.
3. Set **Start Time**, **End Time**, and **DST Bias**.
4. Click **Save**.

16.4 Download Debug Data

You can search and download the diagnostics information, video BAYER, capture picture BAYER, and capture picture YUV of the device to debug the device.

Steps

1. Go to **Configuration → System → Maintenance → Debug Data Download** .



Data Type: Diagnostics Information

Up to 30 records of data can be collected once. The collection will stop automatically for the data exceeding the limit.

Data List

□	No.	File Name	Downloading Progress
□	1	logFile.bin	Not downloaded.
□	2	otapDbg.bin	Not downloaded.
□	3	diagnosedData.txt	Not downloaded.

Figure 16-3 Download Debug Data

2. Select **Data Type**.

   Diagnostics Information

   The diagnostics information includes kernel, status, version information, etc.

Note

Up to 30 records of data can be collected once. The collection will stop automatically for the data exceeding the limit.

3. Click **Search** to search the data list.
4. Select the file(s) to be downloaded, and click **Download** to download the file(s). You can view the downloading progress.
5. **Optional:** Select the file(s) to be deleted, and click **Delete** to delete the file(s).

16.5 Search Log

Log helps to locate and troubleshoot problems.

Steps

1. Go to **Configuration → System → Maintenance → Log Search** .
2. Set search conditions.
3. Click **Search**.

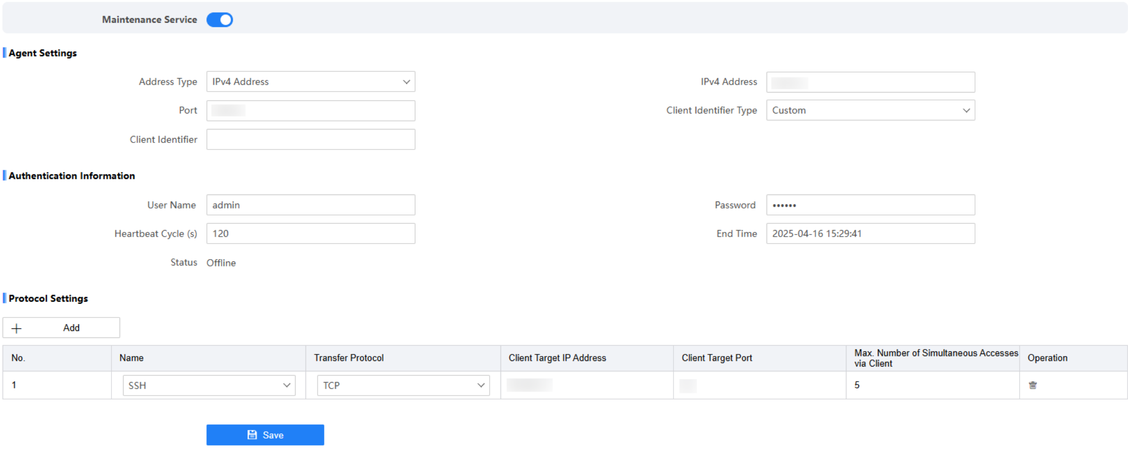
   The matched log files will be displayed on the log list.
4. **Optional:** Click **Export** to save the log files to your computer.

16.6 Enable Maintenance Service

If you want to realize remote camera maintenance and debug via the platform server, enable maintenance service and set the access mode.

Steps

1. Go to **Configuration → System → Maintenance → Maintenance Service** .
2. Enable maintenance service.



Maintenance Service ●

Agent Settings

Address Type: IPv4 Address
IPv4 Address:
Port:
Client Identifier Type: Custom
Client Identifier:

Authentication Information

User Name: admin
Password: ••••••
Heartbeat Cycle (s): 120
End Time: 2025-04-16 15:29:41
Status: Offline

Protocol Settings

+ Add

No.	Name	Transfer Protocol	Client Target IP Address	Client Target Port	Max. Number of Simultaneous Accesses via Client	Operation
1	SSH	TCP			5	🗑

Save

Figure 16-4 Maintenance Service

3. Set agent parameters.
   1) Select **Address Type**.
   2) Set the IP address/domain name and port of the agent.
   3) Select **Client Identifier Type** and set **Client Identifier** according to the actual supporting conditions of the camera. The identifier serves as a unique mark of the camera.
4. Set the authentication information.

   User Name/Password

   The user name and password of the camera for the authentication via the platform server access.

   Heartbeat Cycle(s)

   You are recommended to keep the default value.

   End Time

   The camera will disconnect with the platform server when reaching the set end time.
5. Set protocol parameters.
   1) Click **Add** to add a protocol.
   2) Set the corresponding parameters of the protocol.

Note

You can login and access up to 5 cameras (clients) simultaneously via HTTP or SSH protocol.

6. Click **Save**.

What to do next

After settings, refresh the interface and check the authentication status of the camera. If the status is online, you can access and debug the camera via the platform server.

16.7 Reboot

When the device needs to be rebooted, reboot it via the software instead of cutting off the power directly.

Steps

1. Go to **Configuration → Upgrade & Maintenance → Device Maintenance** .
2. Click **Reboot**.
3. Click **OK** to reboot the device.

Note

You can also click ⏻ on the upper right corner of the interface to reboot the device.

16.8 Restore Parameters

When the device is abnormal caused by the incorrect set parameters, you can restore the parameters.

Steps

1. Go to **Configuration → Upgrade & Maintenance → Device Maintenance** .
2. Select the restoration mode.
   - Click **Restore**, and select the parameters to be saved instead of being restored. Click **OK**. Then the parameters except the IP parameters, user parameters, and the saved parameters will be restored to the default settings.
   - Click **Restore Factory Settings** and click **OK** to restore all the parameters to the factory settings.
3. Click **OK**.

16.9 Export Parameters

You can export the parameters of one device, and import them to another device to set the two devices with the same parameters.

Steps

1. Go to **Configuration → Upgrade & Maintenance → Backup and Import Parameters** .
2. Click **Export** after **Configuration Parameters**.
3. Set an encryption password, confirm the password, and click **OK**.

Note

The password is used for importing the configuration file of the current device to other devices.

4. Select the saving path, and enter the file name.
5. Click **Save**.

16.10 Import Configuration File

Import the configuration file of another device to the current device to set the same parameters.

Before You Start

Save the configuration file to the computer.

Steps

Caution

Importing configuration file is only available to the devices of the same model and same version.

1. Go to **Configuration → Upgrade & Maintenance → Backup and Import Parameters** .
2. Select **Importing Method**.

   Note

   If you select **Import Part**, check the parameters to be imported.
3. Click **Browse** to select the configuration file.
4. Click **Import**.
5. Enter the password which is set when the configuration file is exported, and click **OK**.
6. Click **OK** on the popup window.

Result

The parameters will be imported, and the device will reboot.

16.11 Upgrade

Upgrade the system when you need to update the device version.

Before You Start

- Update the plugin before upgrade.
- Prepare the upgrade file in .dav format.

Steps

1. Go to **Configuration → Upgrade & Maintenance → Device Upgrade** .
2. Click **Browse** to select the upgrade file.
3. Click **Upgrade**.
4. Click **OK** in the popup window.

Note

The upgrading process will take minutes. Do not power off the device. The device will restart automatically after upgrading. If the network condition is poor, it may take more time.

Result

The device will reboot automatically after upgrade.

See Far, Go Further