Guidance Terminal

User Manual

About this Document

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

About this Product

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

Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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

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

Symbol Conventions

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

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

Table of Contents

Chapter 1 Introduction

1.1 Introduction

Guidance terminal (hereinafter referred to as device), based on the 4-core ARM Cortex-A17 processor, is a remarkable intelligent management system used for underground garage. Adopting the advanced parking guidance and find my car system, the guidance terminal is capable of connecting multiple parking cameras to realize parking space detection, license plate recognition, guidance screen information control, video storage, playback, etc.

The guidance terminal is widely used in the parking lot of the community, business center and hotels. It greatly shortens the parking time and vehicle searching time of customers, and improves the utilization of the spare parking spaces.

1.2 Features and Functions

- Supports access to dual-lens parking cameras or single-lens parking cameras.
- Supports Hikvision PoE power supply for parking cameras.
- Supports TPM cascade and data upload.
- Supports LED display control, able to show remaining parking spaces both online and offline.
- Supports IP address automatic allocation.
- HDD slots with large capacity distributed storage, storing recordings up to 30 days.
- 220 VDC/110 VDC optional power supply.

1.3 Application Scenario

Parking cameras can be connected to the guidance terminal via network to realize the integrated management, video search, record, playback, etc. Refer to the following figure for the application scenario of the guidance terminal.

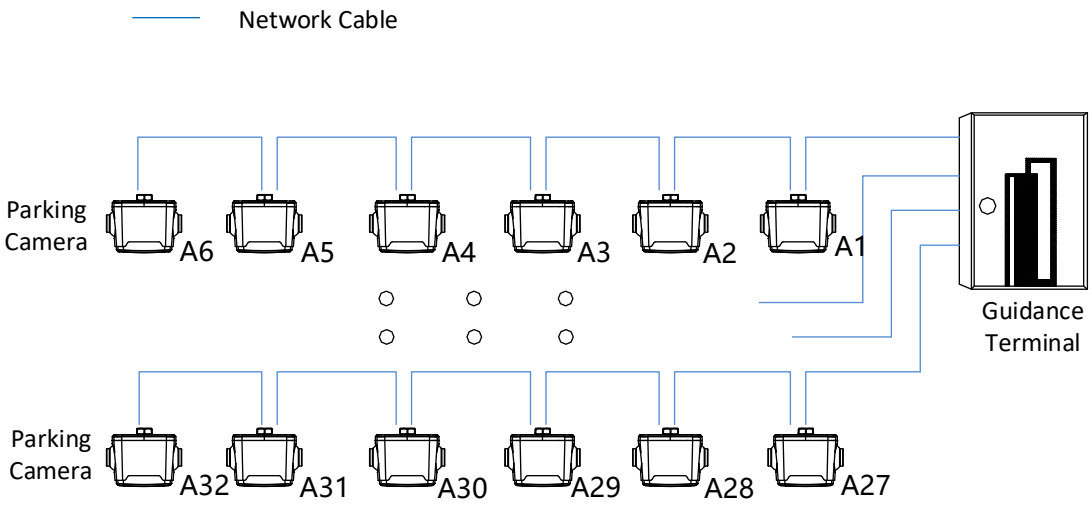


Figure 1-1 Application Scenario

NOTE

- Only the Hikvision PoE parking camera can be connected to the guidance terminal.
- The parking cameras shown in the figure above are for reference only. The actual device shall prevail.

Chapter 2 Activation and Login

2.1 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 and web browser.

2.1.1 Default Information

Device default information are as follows.

- Default IP address: 192.168.1.64
- Default port: 8000
- Default user name: admin

2.1.2 Activate via SADP

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

Before You Start:

- Get the SADP software from the supplied disk or the official website (***https://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.

WARNING

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.

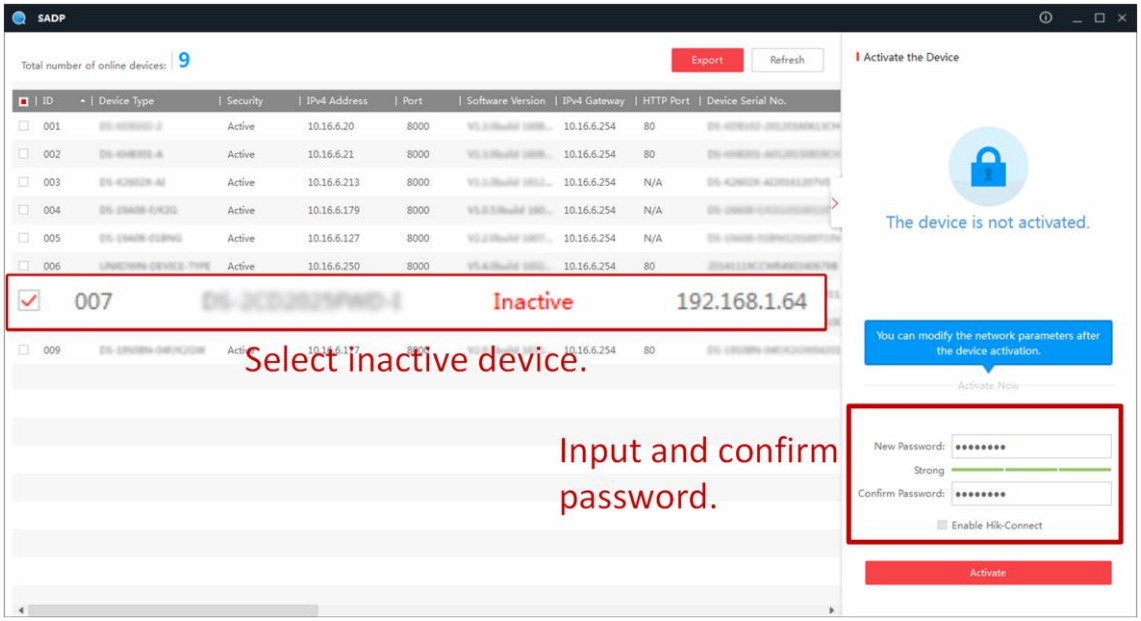


Figure 2-1 Activate via SADP

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**.
3) Enter the admin password and click **Modify** to activate your IP address modification.

2.1.3 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 connect to the same LAN.

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.

WARNING

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.

2.2 Login

You can log in to the guidance terminal via web browser for further operations such as live view, playback, local configuration, etc.

Steps:

1. Open the web browser, and enter the IP address of the device to enter the login interface.

NOTE

You are recommended to use web browser of IE 8 or above.

2. Input the user name and password of the guidance terminal.
3. Click **Login.**

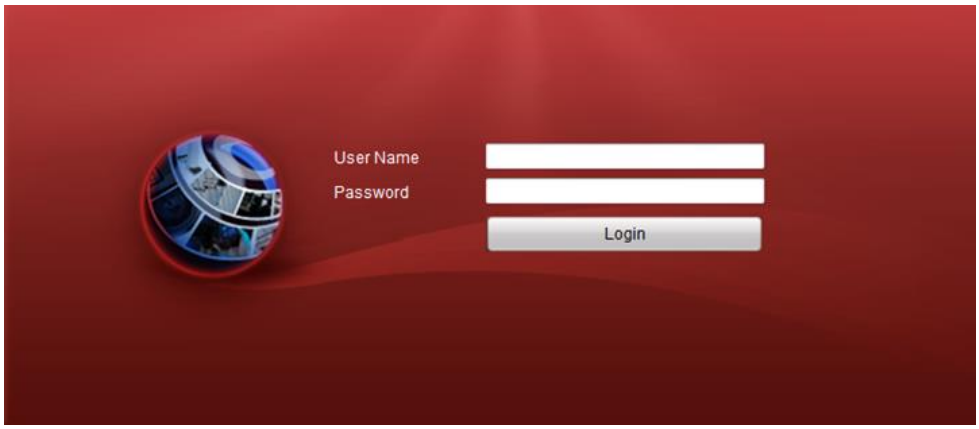


Figure 2-1 Login Interface

4. For the first time to login, you should install the plug-in before you can access the functions. Run and install the plug-in according to the prompt. After the installation of plug-in, re-open the web browser and login.

NOTE

Please close your web browser during the installation of the plug-in.

Chapter 3 Configuration

Purpose:

The parameters, such as protocol, stream type, network, alarm, etc., can be configured via the web browser.

Click **Configuration** tab to enter the Configuration page.

3.1 Local Configuration

Steps:

1. Go to **Configuration > Local Configuration**.

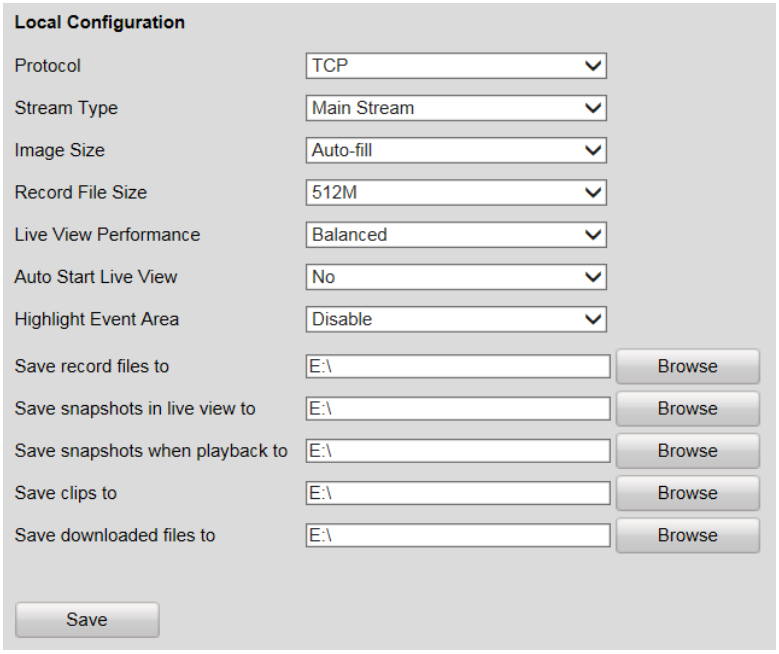


Figure 3-1 Local Configuration

2. Set the following parameters such as protocol, stream type, image size, etc. as desired.

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.

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.

Image Size

The display ratio of the live view image.

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.

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.

Real Time

The priority is given to real-time transmission.

Auto Start Live View

Enable it to start live view automatically.

Highlight Event Area

Enable it to highlight event areas on the live view image.

Save record files to

Set the saving path of the manually recorded video files.

Save snapshots in live view to

Set the saving path of the manually captured pictures in live view mode.

Save snapshots when playback to

Set the saving path of the manually captured pictures in playback mode.

Save clips to

Set the saving path of the captured pictures in **Live View** > **Real-Time Capture**.

Save downloaded files to

Set the saving path of the downloaded files.

3. Click **Browse** to select a local saving path for the files.
4. Click **Save** to save the settings.

3.2 Remote Configuration

3.2.1 Configure Device Parameters

Configure Device Information

Go to **Configuration** > **Remote Configuration** > **Device Parameters** > **Device Information**. You can edit the Device Name and Device No., and view the device Model, Serial No., Firmware Version, Encoding Version, Number of Channels, Number of HDDs, Number of Alarm Input, and Number of Alarm Output.

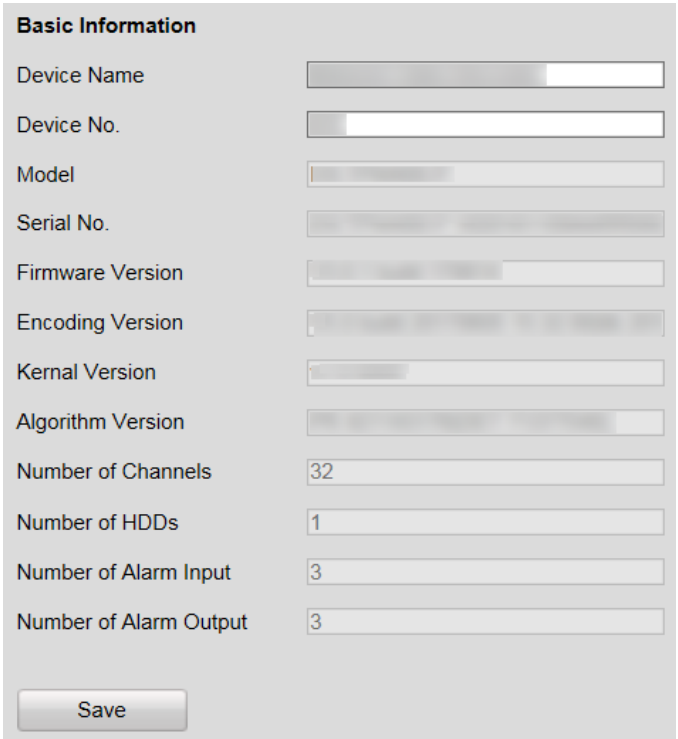


Figure 3-2 Basic Information

Configure Time

Go to **Configuration** > **Remote Configuration** > **Device Parameters** > **Time Settings**. You can configure the time, including Time Zone, synchronization (NTP Time Synchronization or Manual

Time Synchronization).

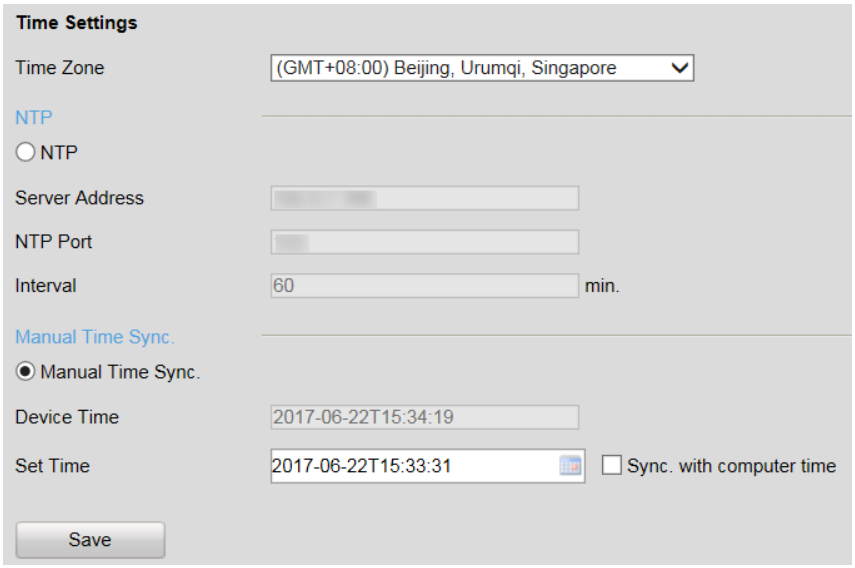


Figure 3-3 Time Settings

NTP: After enabling NTP, the NTP server will synchronize the device time at regular intervals.

Enable **NTP**, and input the Server Address, NTP Port and Interval.

Manual Time Sync.: After enabling Manual Time Synchronization, the device time can be synchronized with the setting time or the computer time. Enable **Manual Time Sync.**, and input the time as desired. Or you can check the checkbox of **Sync. with computer time.**

Configure DST

Go to **Configuration** > **Remote Configuration** > **Device Parameters** > **DST**. You can configure DST, set the start time and end time, and DST bias.

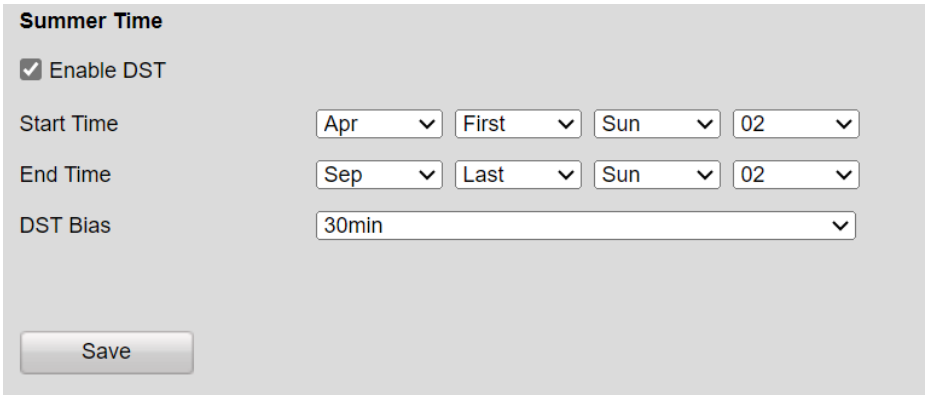


Figure 3-4 DST Settings

Enable DST: Enable Daylight Saving Time (DST) to adjust the device clock automatically in the time

zone.

DST Bias: A time zone's offset during DST. Select the DST bias according to the actual needs.

Configure Application Mode

Go to **Configuration** > **Remote Configuration** > **Device Parameters** > **Application Mode**, you can set camera control mode.

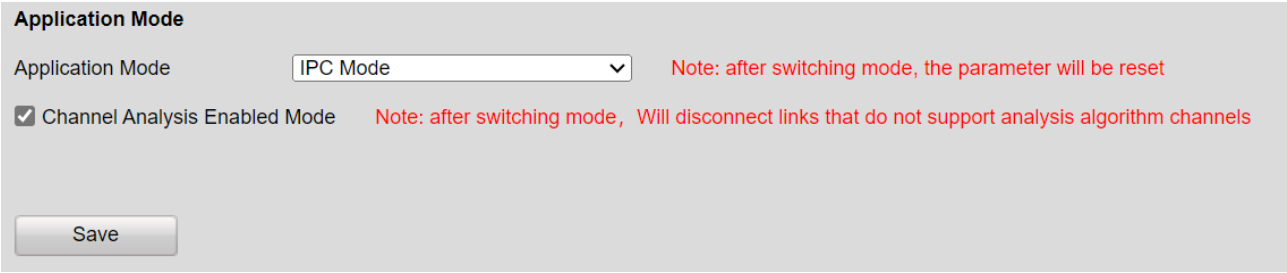


Figure 3-5 Application Mode

Application Mode: Select IPC Mode to control the connected cameras.

Channel Analysis Enabled Mode: Check it to disconnect channels that do not support analysis algorithm.

3.2.2 Manage Camera

Go to **Configuration** > **Remote Configuration** > **Camera Management** > **IP Camera**, you can add, activate, and manage cameras. The guidance terminal is capable of connecting up to 32 parking cameras.

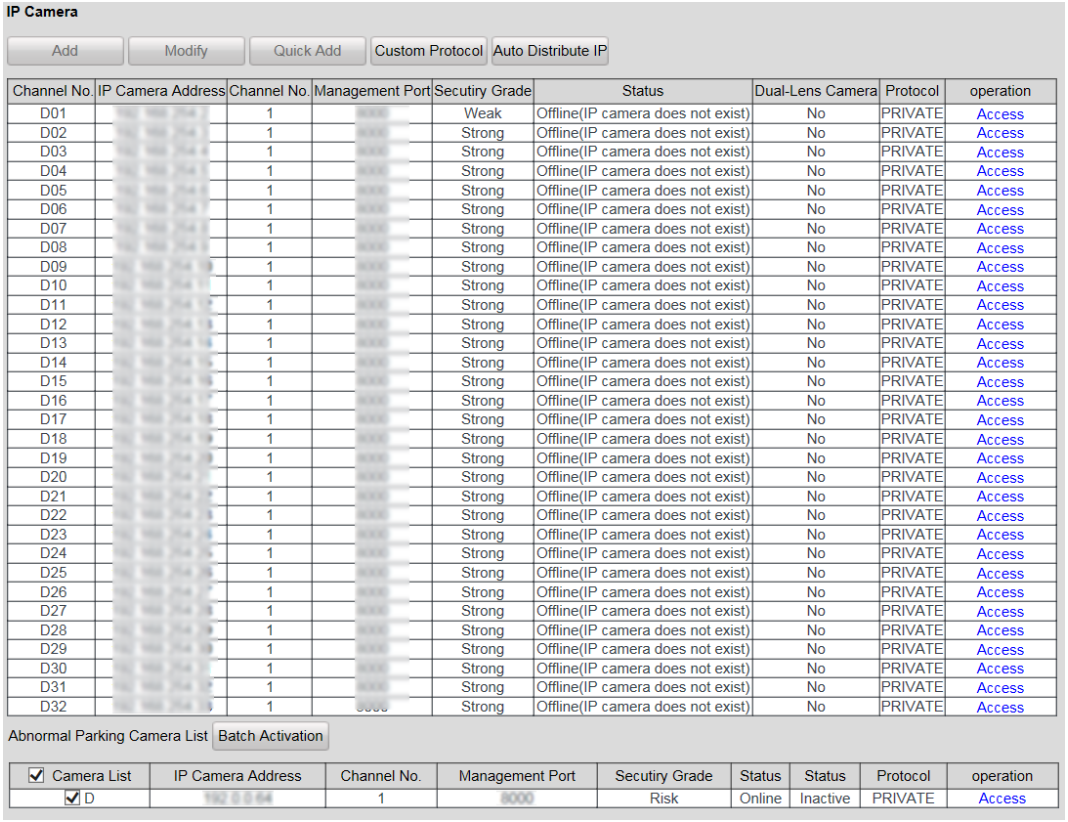


Figure 3-6 IP Camera Management

Activate Parking Camera

If the parking camera is inactive, it will be listed in the Abnormal Parking Camera List. You can activate the inactive cameras in batch.

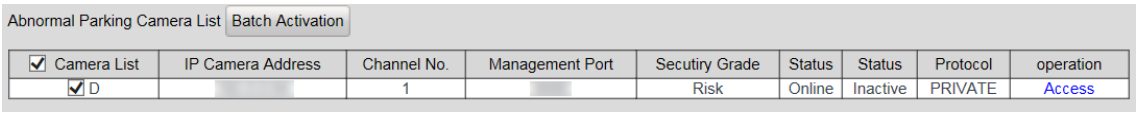


Figure 3-7 Batch Activation

1. Check the inactive parking camera(s).
2. Click **Batch Activation**.
3. Enter the password, and confirm it.

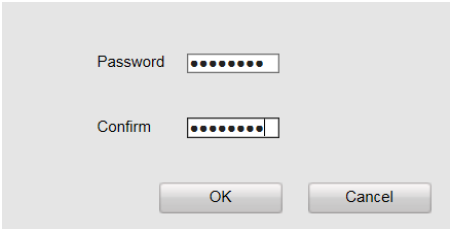


Figure 3-8 Batch Activation

WARNING

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 activate the camera(s).

Add Parking Camera

- Click **Auto Distribute IP** and the IP address of the camera is auto-allocated. The fourth number of the host ranges from 2 to 33. If the IP is occupied, the number will be extended and if the IP is not in the specified network segment of the guide terminal, the IP of camera will be modified to be in the same network segment with the system.
- The status of the camera will be **Offline** if the camera is not connected.
- When the camera is connected, the IP address will be allocated according to the network interface of the camera and the fourth number of the host ranges from 2 to 33. The status of the camera will be **Online.**

Modify Parking Camera

1. Select a camera and the item becomes blue.
2. Click **Modify** and you can modify the information including user name and password.

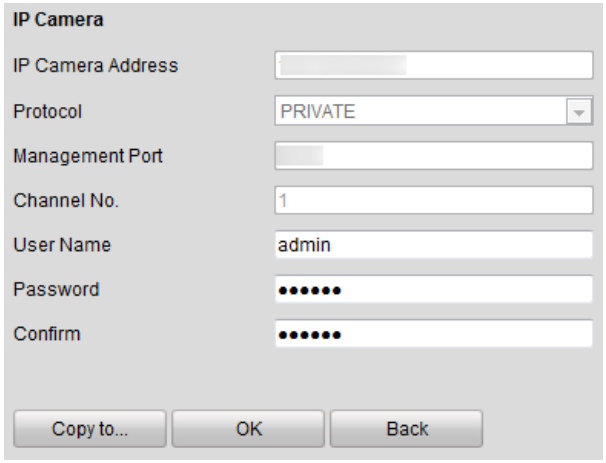


Figure 3-9 Modify Parking Camera

3. (Optional) Click **Copy to** to copy the settings to other camera(s).

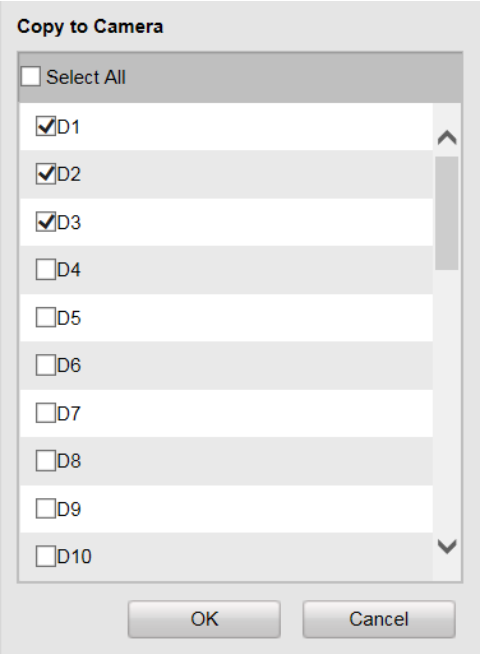


Figure 3-10 Copy Camera Settings

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

Configure Custom Protocol

Click **Custom Protocol** to configure the protocol as follows.

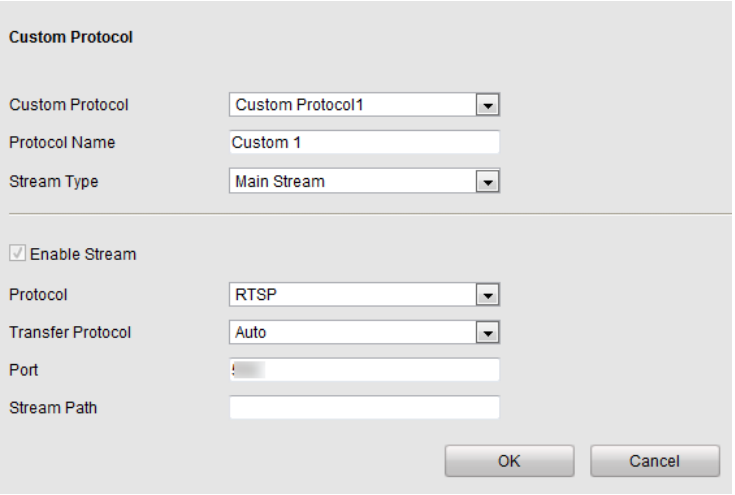


Figure 3-11 Custom Protocol

Get Access to Parking Camera

When the camera is online, you can click **Access** and a login interface for a camera is linked. Log in to the camera to configure the parking camera parameters.

NOTE

You must configure the IP address of parking camera remote host and port before the parking camera data is received by the guidance terminal.

3.2.3 Configure Camera

Configure Display

Go to **Configuration** > **Remote Configuration** > **Camera Settings** > **Display Settings**, you can configure the channel name and OSD settings.

Channel No.: Select the channel number from the dropdown list.

Camera Name: Customize a camera name.

OSD Settings: You can check the checkbox to display camera name, date and week information on the live view image. You can also set the time and data format and display mode.

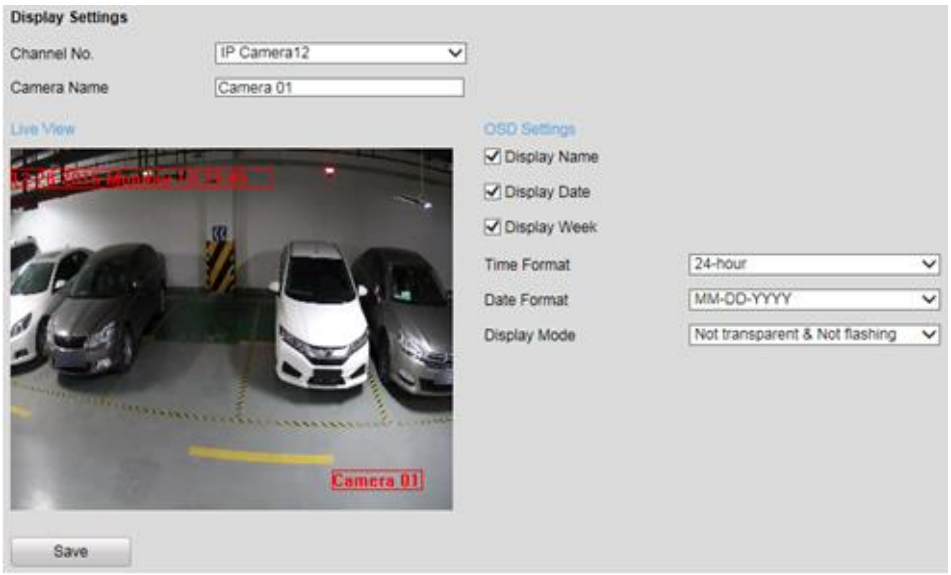


Figure 3-12 OSD Settings

NOTE

You can drag the name, date, week, and time information to any position of the live view window.

Configure Parking Space

You can configure the recognized parking space number, parking space area, and special parking space in parking space allocation.

1. Go to **Configuration > Remote Configuration > Camera Settings > Parking Space Settings**.

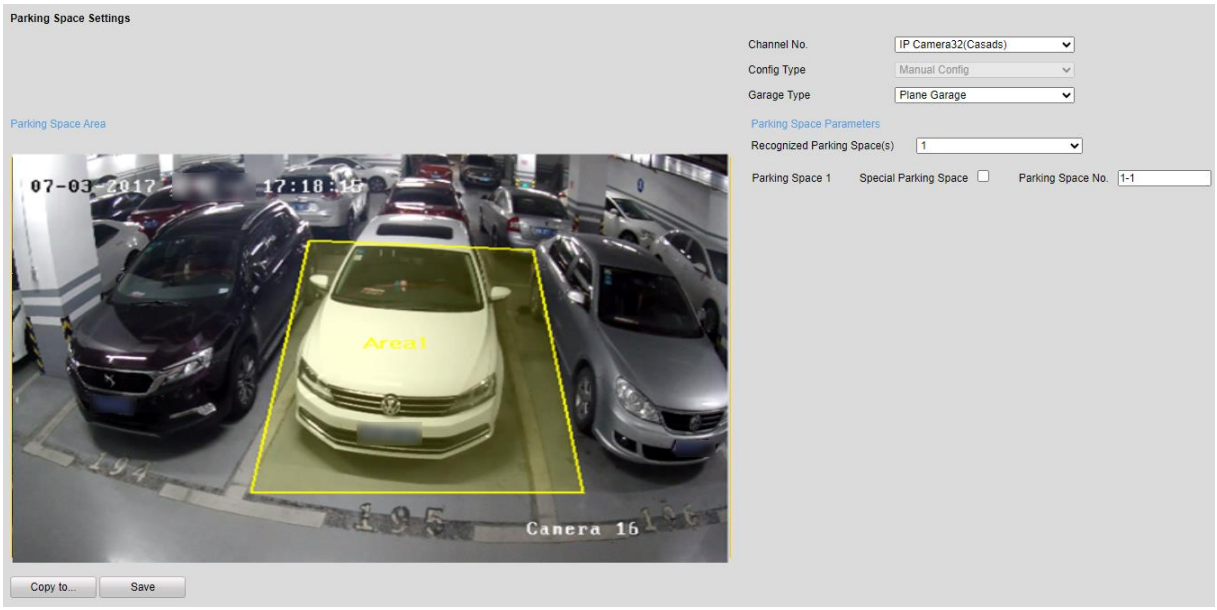


Figure 3-13 Parking Space Settings

2. Select **Channel No.**
3. Select the garage type**.**
4. Select the number of the **Recognized Parking Space(s)** from the drop-down list.

   NOTE

   The selectable value may vary according the camera models.

5. Input the **Parking Space No.** in the text filed.

   NOTE

   Parking space No. only allows “-”, letters, and digits.

6. (Optional) If the space is a special space, check **Special Parking Space** checkbox.
7. Draw parking spaces.

   According to the number of spaces you set, the quadrilaterals appear in the image.

   1) Click a quadrilateral, and drag corner of the quadrilateral to adjust the shape of it, or drag the quadrilateral to adjust the location of it.

2) Repeat step 1) to configure other quadrilaterals.

8. (Optional) Click **Copy to…** to copy the settings to other cameras.

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

Configure Parking Space Indicator

The indicator displays the status of parking spaces, different colors stand for different status. You can select the indicator and the color of different status.

Steps:

1. Go to **Configuration > Remote Configuration > Camera Settings > Parking Space Indicator**.
2. Select **Channel No.**
3. Select **Channel Mode** or **Multi-Parking Space Mode** to set the indicators.

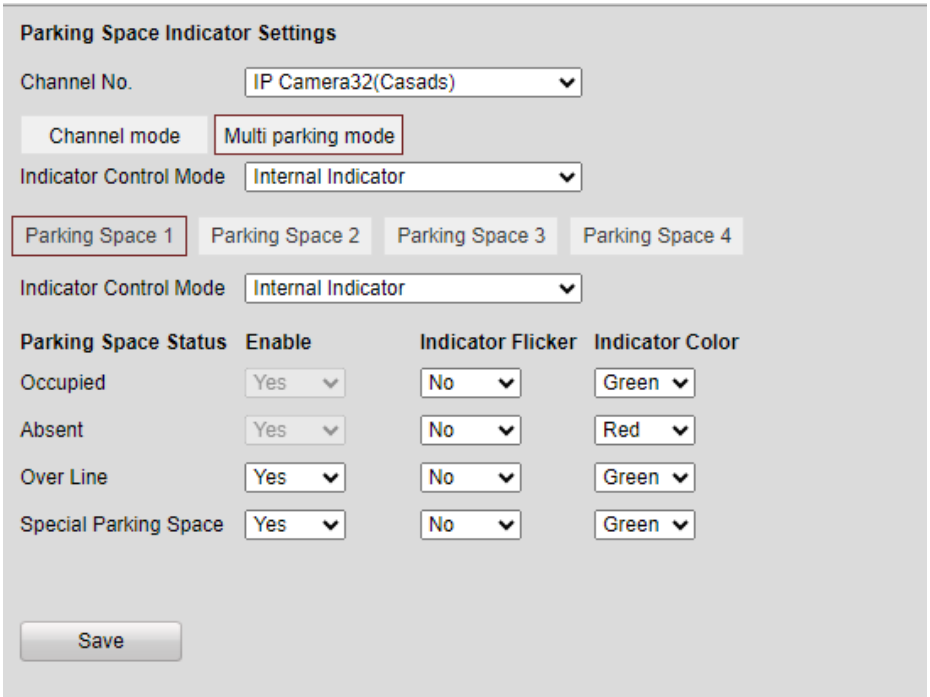


Figure 3-14 Select Mode

NOTE

- In channel mode, the set parking space status is effective to all the parking spaces under the channel. In multi-parking space mode, you can set the indicators for each parking space.
- Multi-parking space mode is only available to certain cameras. Please refer to the actual device.

4. Select the indicator in the drop-down list of **Indicator Control Mode** on your demand, including **Internal Indicator**, **External Indicator**, and **Internal and External Indicator**.

- If you select the **Internal Indicator** or **External Indicator**, and when all the detected parking spaces are occupied, the indicator turns to the occupied color; when the detected parking spaces are not all occupied, the indicator remains the unoccupied color.
- If you select the **Internal and External Indicator**, the indicators work at the same time, you can respectively configure the indicator to display the status of each parking space.

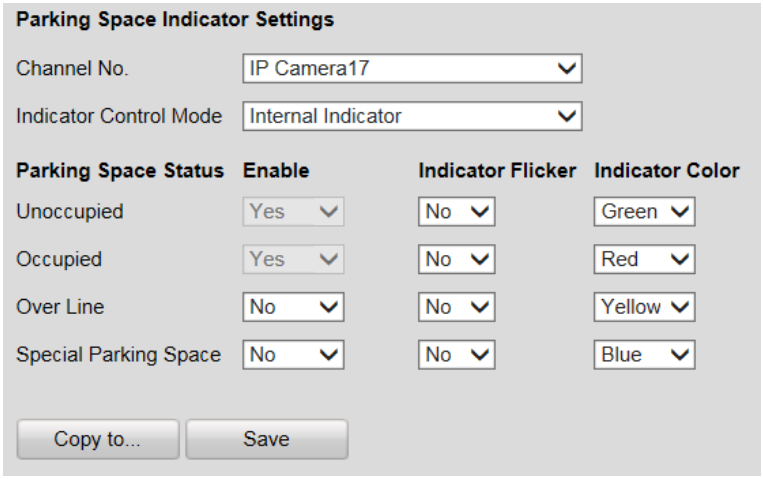


Figure 3-15 Configure Internal Indicator

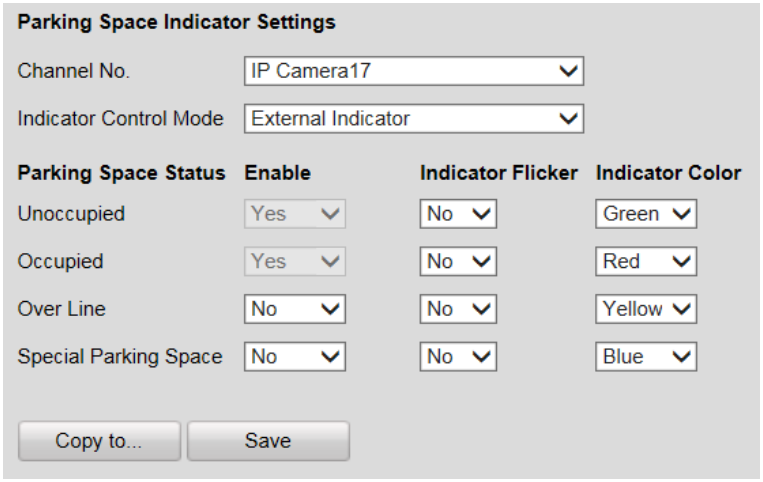


Figure 3-16 Configure External Indicator

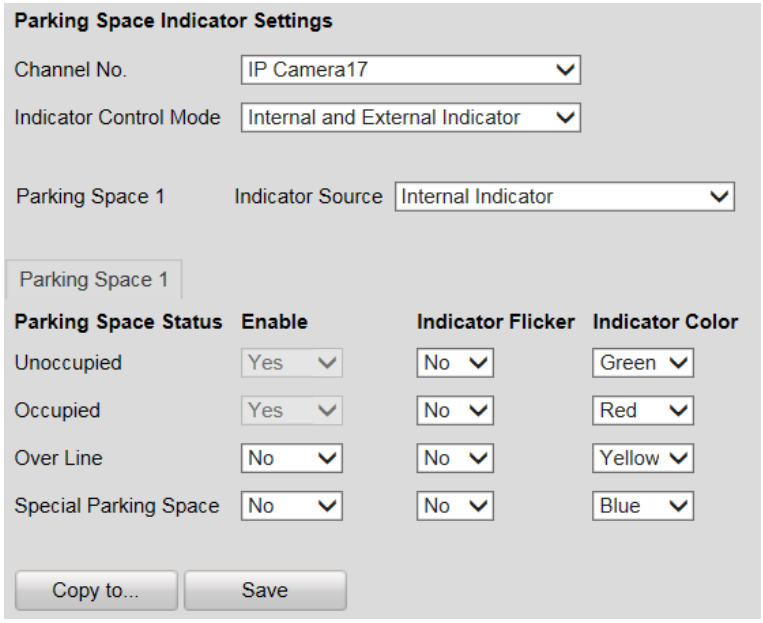


Figure 3-17 Configure Internal and External Indicator

5. Set the indicator parameters for different parking space status.

   The description of different status is shown below:

   Unoccupied: The space is free.

   Occupied: The space is occupied by a vehicle.

   Over Line: A vehicle occupied two parking spaces.

   Special Parking Space: The space is specified to a certain vehicle.

   1) If you choose **Internal and External Indicator**, click the tab of the parking space No. (e.g. Parking Space 1) and select the indicator in the **Indicator Source** drop-down list.
   2) Configure the following parameters on your demand.

      Enable: Select **Yes** or **No** to enable or disable the indication for the corresponding status.

      Indicator Flicker: Set the indicator flicker or not for the corresponding status.

      Indicator Color: Choose the color of the indicator for the corresponding status.
6. (Optional) Click **Copy to…** to copy the settings to other cameras.
7. Click **Save** to save the settings.

Configure Bluetooth

If Bluetooth parking camera is connected, you can configure the Bluetooth parameters.

Steps:

1. Go to **Configuration > Remote Configuration > Camera Settings > Bluetooth Settings**.

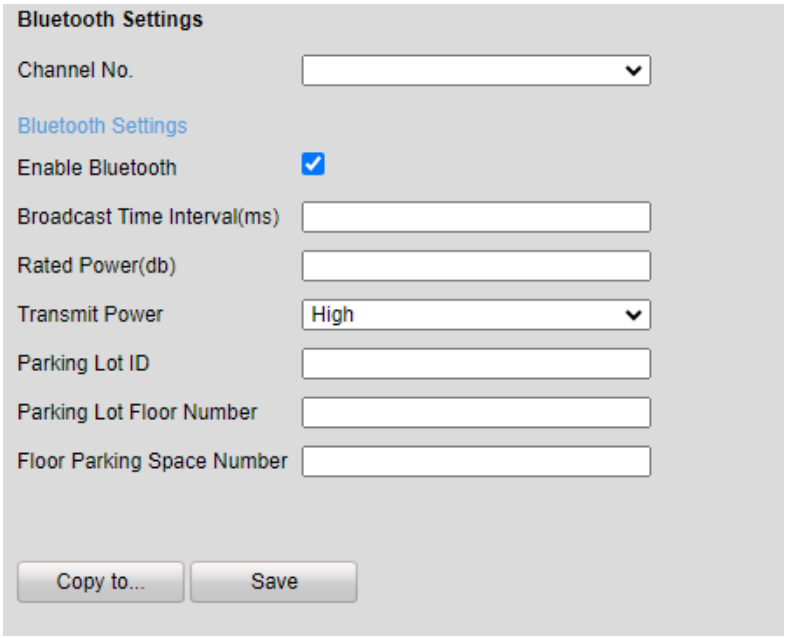


Figure 3-18 Bluetooth Configuration

2. Select **Channel No.**
3. Check **Enable Bluetooth**.
4. Configure the Bluetooth parameters.
   - **Broadcast Time Interval**: the frequency of sending broadcast frame by Bluetooth module.
   - **Rated Power**: the signal strength received by mobile client which is 1 meter away from the parking camera.
   - **Transmit Power**: Three levels are selectable. The stronger the transmit power, the further the receivable distance.
   - **Parking Lot ID**: Hex number can be entered (0 - F).
   - **Parking Lot Floor Number**: Configure according to the actual conditions.
   - **Floor Parking Space Number**: Configure according to the actual conditions.

Configure Video

Configuration > Remote Configuration > Camera Settings > Video Settings, you can set the video parameters including stream type, video type, resolution, etc.

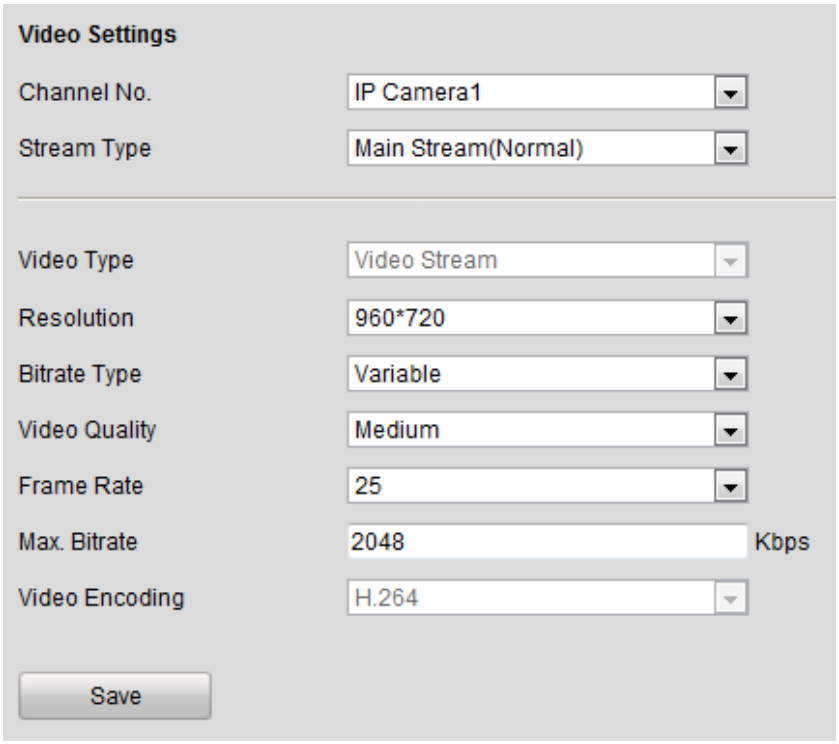


Figure 3-19 Video Settings

Parameters	Description
Channel No.	Up to 32 channels.
Stream Type	Select video stream. Main Stream (Normal)/Sub Stream/Main Stream (Event) are selectable.
Video Type	Video stream.
Resolution	The higher the resolution is, the clearer the image will be. Meanwhile, the network bandwidth requirement is higher.
Bitrate Type	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.
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.
Frame Rate	The higher the frame rate, the larger bandwidth it needs, and the larger storage space it needs.
Max. Bitrate	The maximum bitrate.
Video Encoding	H.264.

Configure Schedule

You can set the record schedule in the Schedule Settings interface as follows.

Steps:

1. Go to **Configuration > Remote Configuration > Camera Settings > Schedule Settings**.

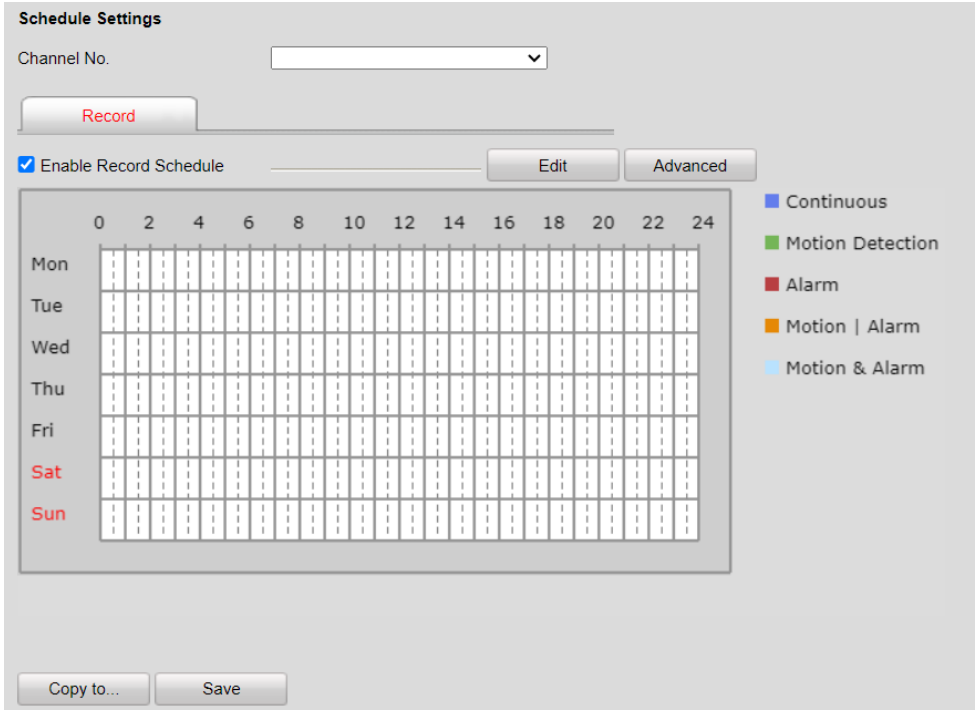


Figure 3-20 Schedule Settings

2. Select the channel No. from the drop-down list.
3. Check **Enable Record Schedule**.
4. Click **Edit** to set the schedule as follows.

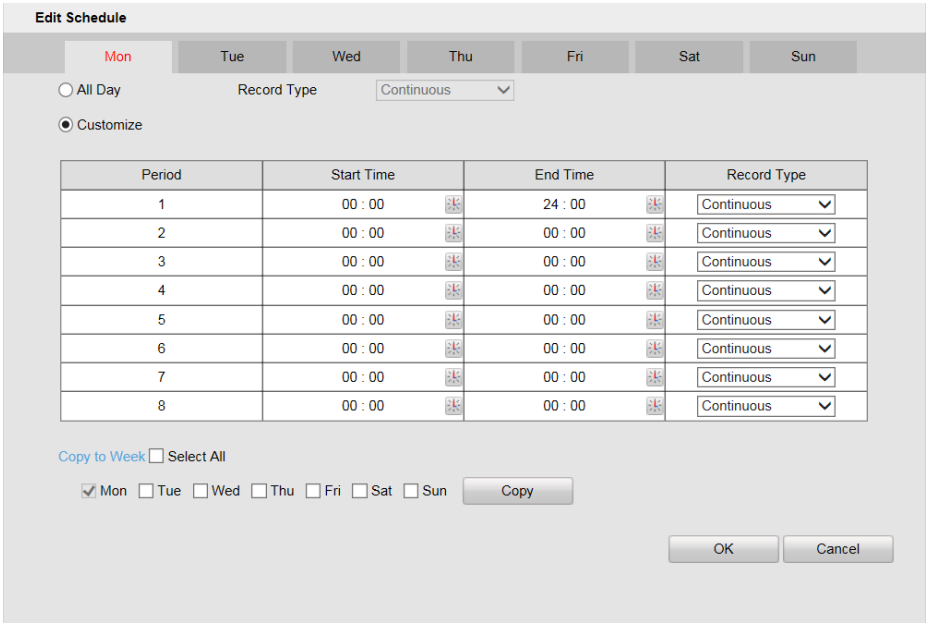


Figure 3-21 Edit Schedule

1) Select **All Day** or **Customize** to edit the schedule.
2) Select the **Record Type**. Continuous, Motion Detection, Alarm, Motion or Alarm and Motion & Alarm are selectable.
3) If you select **Customize**, click to set the start time and end time.
4) (Optional) If you want to copy the settings to other days, check the checkbox and click **Copy**.
5) Click **OK** to save the settings.

5. Click **Advanced** in the Schedule Settings interface to configure advanced settings as follows.

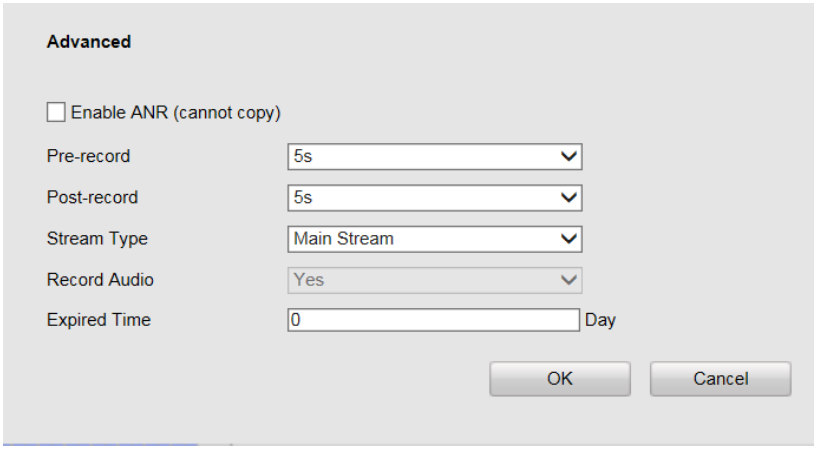


Figure 3-22 Advanced Settings

Enable ANR

ANR (Automatic Network Replenishment) can automatically save the videos in the local

storage of the connected camera in the condition of network disconnection, and can synchronize data after the network is recovered.

Pre-record

Set the time to record before the recording start time.

Post-record

Set the time to record after the recording end time.

Stream Type

Select Main Stream to get the high-quality image when the network condition is good. Select Sub-Stream to get the fluent image when the network condition is not good enough.

Expired Time

Set Expired Time for the recorded videos stored in the local storage. Beyond the time, the files will be overwritten.

6. (Optional) If you want to copy all the settings to other channels, click **Copy to…** and select channels, and then click **OK**.
7. Click **Save** to save the settings.

Configure Motion Detection

It can detect the moving objects in the detection region and trigger the linkage actions.

Steps

1. Go to **Configuration > Remote Configuration > Camera Settings > Motion Detection**.
2. Select **Channel No.**
3. Check **Enable Motion Detection**, and **Enable Dynamic Analysis for Motion** to mark the detected objects with green rectangles on the live view window.
4. Draw the motion detection areas.
   1) Click **Area Settings** and **Draw Area**.
   2) Draw areas in the live view window, and then click **Stop Drawing**.
   3) (Optional) To clear all detection areas, click **Clear All**.
   4) Set the detection sensitivity. The higher the value, the more accurate the detection.
   5) To copy the area settings to other channels, click **Copy to**, and select the channel(s).

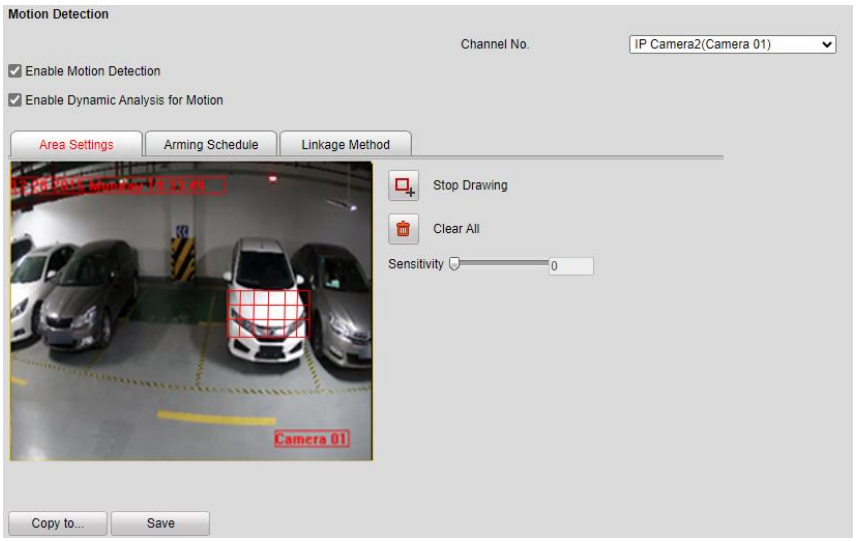


Figure 3-23 Configure Motion Detection

5. Set the arming schedule.

1) Click **Arming Schedule**, and click **Edit** to edit the arming schedule time. You can refer to Configure Schedule for details.

2) To copy the schedule to other days, select the day(s) or check **Select All**, and then click **Copy**.

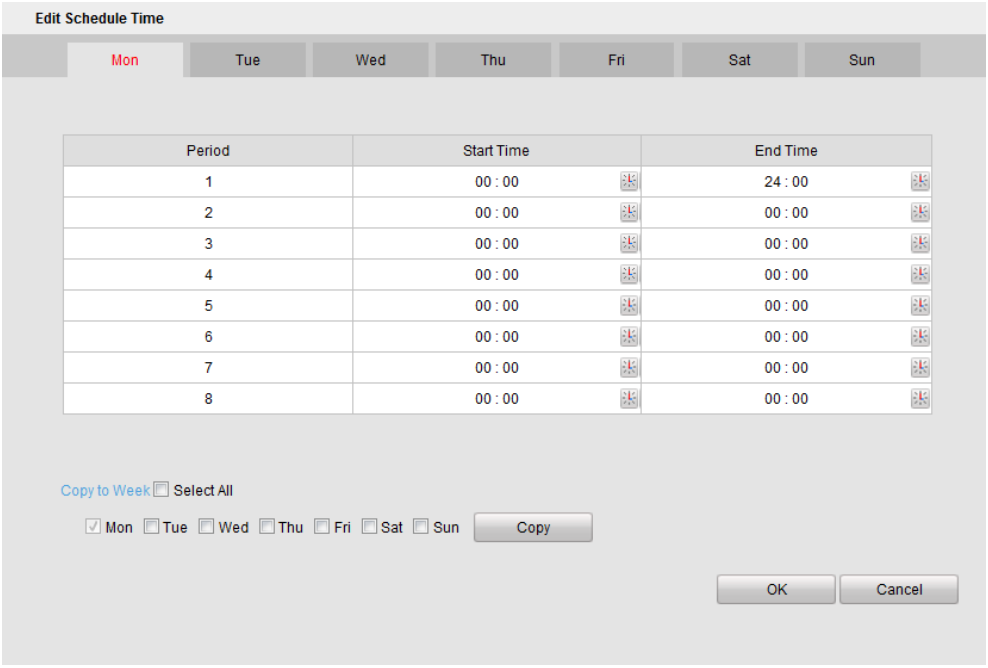


Figure 3-24 Edit Schedule Time

6. Click **Linkage Method**.

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

2) Check **Notify Surveillance Center** to upload the alarm information to the surveillance

center when an alarm event is detected.

7. Click **Save**.

3.2.4 Configure Network

The guidance terminal is equipped with two network interface cards and you can configure extranet and intranet parameters respectively.

Configure TCP/IP

Go to **Configuration > Remote Configuration > Network Settings > TCP/IP**. Set the IP address before you operate the device over network, and the default IP address is 192.168.1.64. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.

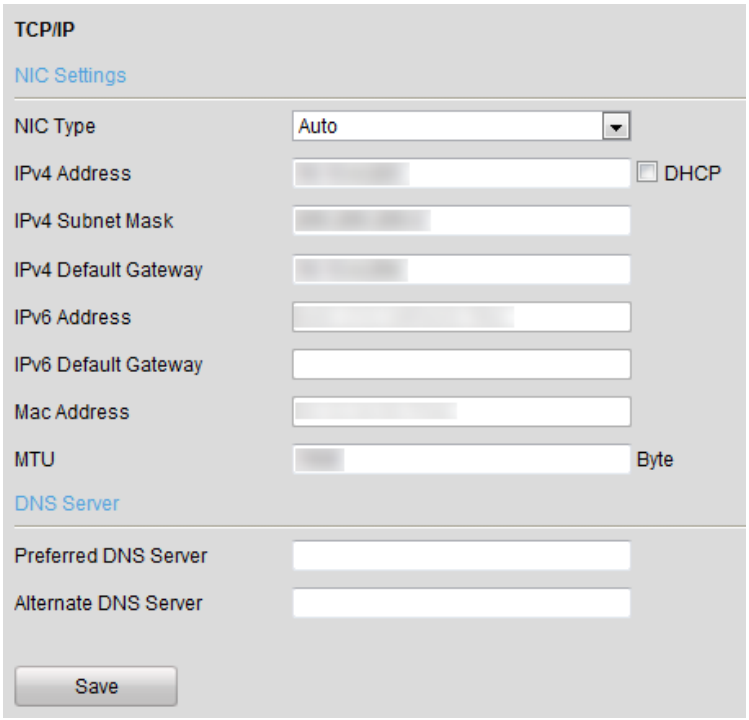


Figure 3-25 TCP/IP Settings

NIC Type

Select a NIC (Network Interface Card) type according to your network condition. Auto, 10 M Half-dup, 10 M Full-dup, 100 M Half-dup and 100 M Full-dup is selectable.

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

Enter **IPv6 Address**, **IPv6 Subnet Mask**, and **IPv6 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 Address** properly if needed.

NOTE

You are required to reboot the guidance terminal after modifying the IP address.

Configure Internal Net

Go to **Configuration > Remote Configuration > Network Settings > Internal Net**. You can view IP address and modify subnet mask and gateway of the 16 100 M network interface cards in the following interface.

Figure 3-26 Internal Net Settings

The default IP address is 192.168.254.1. The 16 network interface cards are in the same network segment, which can interact with cameras and up to 32 parking cameras can be accessed.

NOTE

Network segment: 192.168.254.2 ~ 192.168.254.33. Other IP address cannot access to the guidance terminal.

Configure HTTPS

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** > **Remote Configuration > Network Settings > HTTPS**.

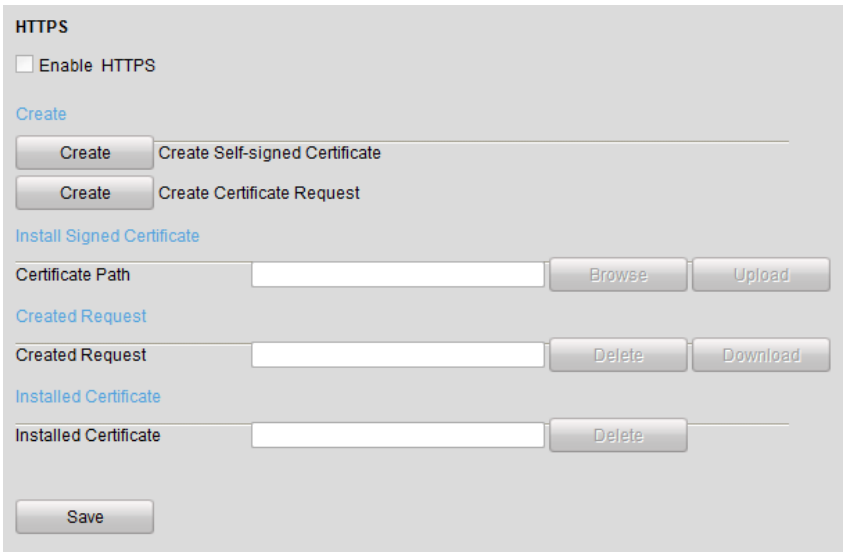


Figure 3-27 HTTP Settings

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.

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**.
3. Click **Create**.
4. Follow the prompt to enter **Country/Region**, **Hostname/IP**, **Validity**, and other parameters.
5. Click **Download** to download the certificate request and submit it to the trusted authority for signature.
6. Click **Browse** and **Install** to import the certificate to the device.
7. Click **Save**.

Configure Remote Access

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.

Steps:

1. Go to **Configuration** > **Remote Configuration > Network Settings > Remote Access.**

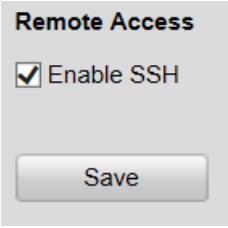


Figure 3-28 Remote Access Settings

2. Disable **SSH Service**.
3. Click **Save**.

3.2.5 Configure Serial Port

Configure RS-232 Serial Port

Go to **Configuration > Remote Configuration > Serial Port Settings > 232 Serial Port**. RS-232 serial port parameters are for the RS-232 interface. Please keep the settings as default.

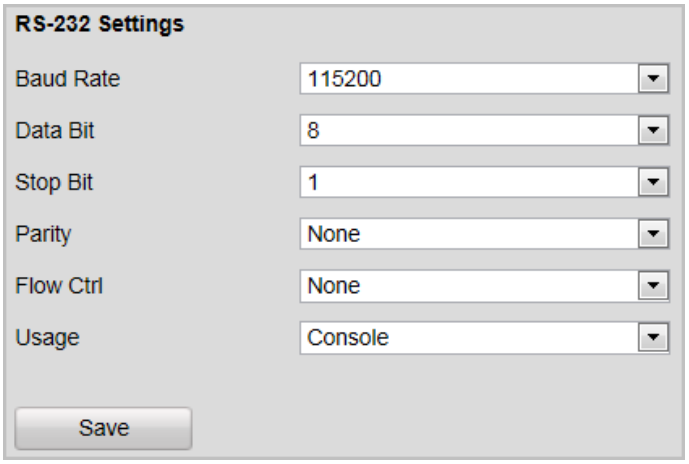


Figure 3-29 RS-232 Settings

Configure RS-485 Serial Port

Go to **Configuration > Remote Configuration > Serial Port Settings > 485 Serial Port**. RS-485 serial port is used for connecting to LED display units, which shows the available parking spaces and the direction of the parking area.

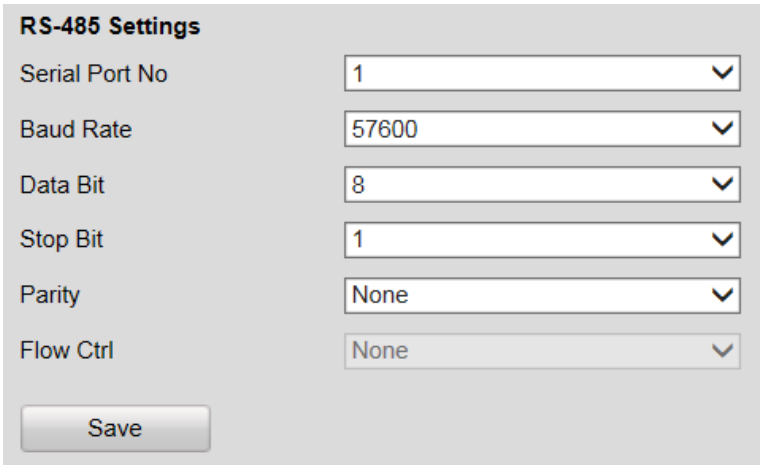


Figure 3-30 RS-485 Settings

3.2.6 Configure Alarm

Configure Alarm Input

Steps:

1. Go to **Configuration > Remote Configuration > Alarm Settings > Alarm Input**.

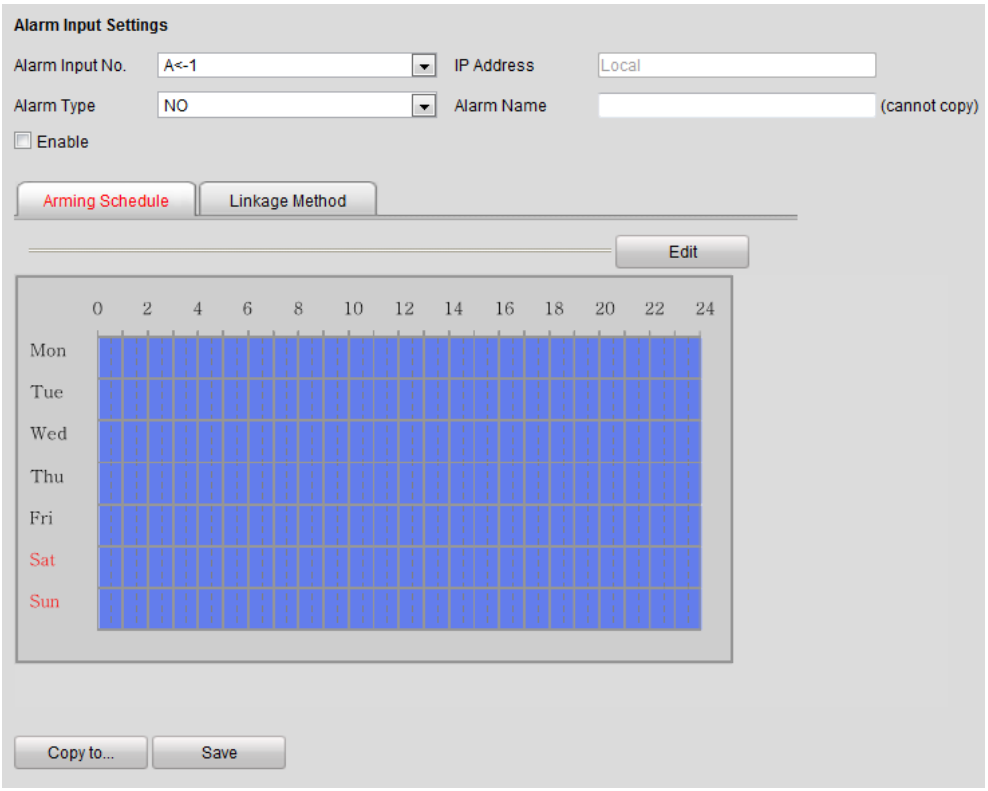


Figure 3-31 Alarm Input

2. Select the **Alarm Input No.** from the drop-down list.
3. Select **Alarm Type** as **NO** (Normally Open) or **NC** (Normally Closed).
4. Enter the **Alarm Name**.
5. Check **Enable** to enable the alarm input.
6. Click **Arming Schedule** to set the schedule.
7. Click **Edit** to edit the arming schedule time. You can refer to Configure Schedule for details.

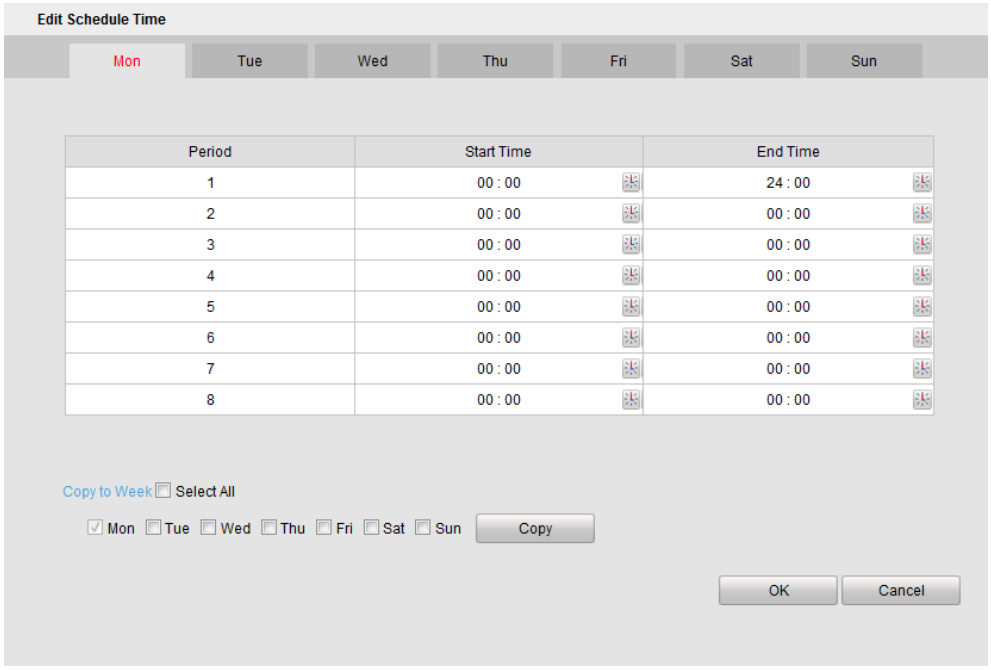


Figure 3-32 Edit Schedule Time

8. Click **Linkage Method** to select the alarm output No. according to the alarm interface connected to the external alarm device, select the channel(s) to trigger when the alarm occurs, and select the linkage method.

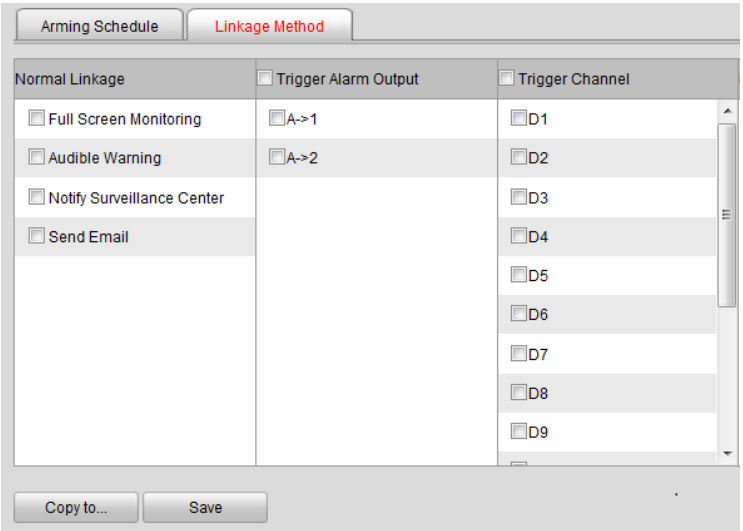


Figure 3-33 Linkage Method

Configure Alarm Output

Go to **Configuration > Remote Configuration > Alarm Settings > Alarm Output**. When the device generates alarm signal, it will trigger alarm output. The configuration of alarm output is similar

with that of alarm input. Refer to Configure Alarm Input for details

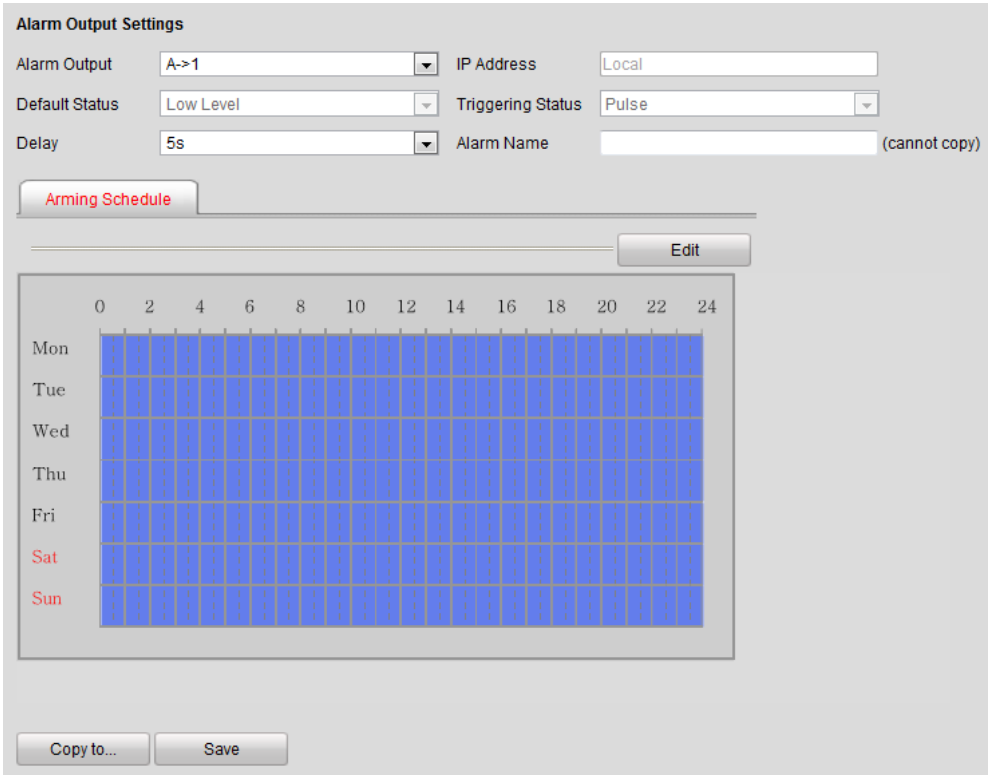


Figure 3-34 Alarm Output

3.2.7 Control Indicator

Configure Opposite Space Detection

The opposite space detection is applicable to the parking lot that the aisle between the opposite parking spaces is very narrow. After you configure the function, the indicator of the current parking camera displays the status of opposite space, and vice versa.

NOTE

The parking space indicator configuration of two cameras for opposite space detection must be the same.

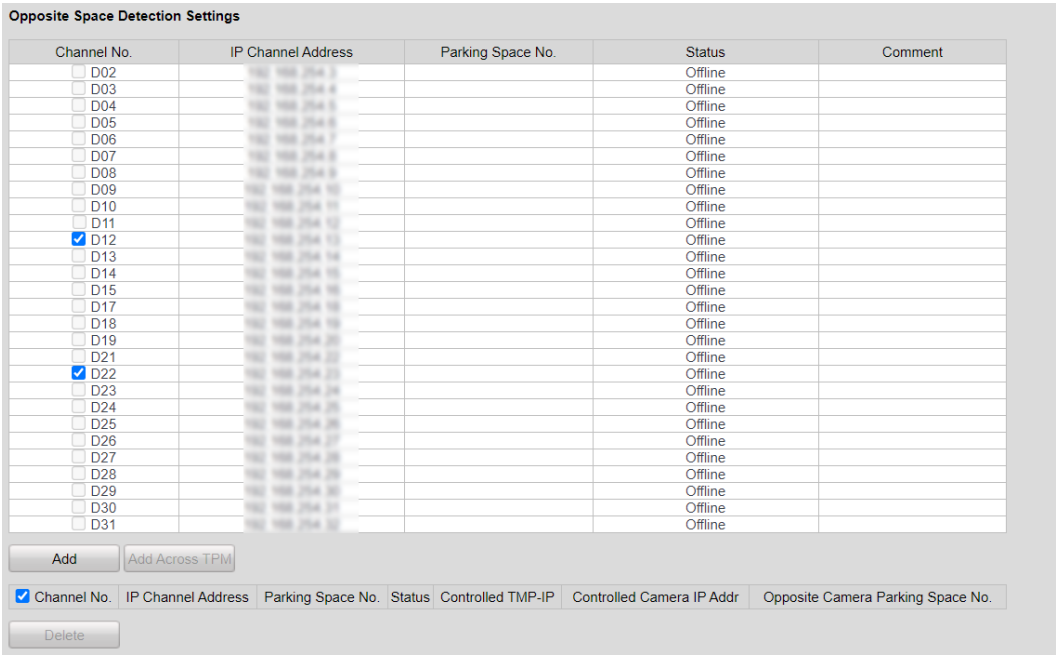


Figure 3-35 Opposite Space Detection Settings

Steps:

1. Go to **Configuration > Remote Configuration > Indicator Control Settings > Opposite Space Detection**.

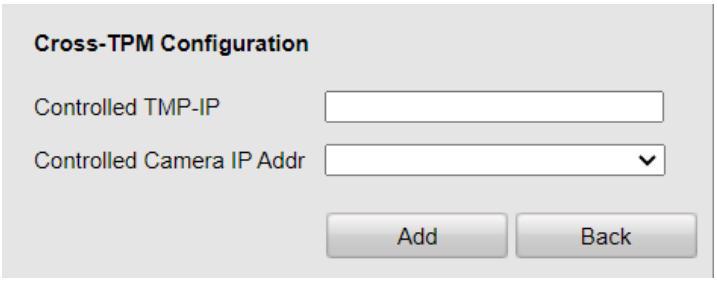


Figure 3-36 Add Across TPM

2. Check two cameras for opposite space detection.
3. Click **Add** to set the selected two cameras to detect the opposite parking space.
4. If the camera needs to detect the parking space of another camera under other guidance terminal, select the camera and click **Add Across TPM**.
   1) Enter **Controlled TMP-IP** and select **Controlled Camera IP Addr**.
   - Controlled TPM is another guidance terminal which needs to be controlled.
   - Controlled camera is another parking camera which needs to be controlled.

   2) Click **Add** to save the settings.

3.2.8 Configure Exception

Go to **Configuration > Remote Configuration > Exception** to set the alarm output method when exception happens. You can select the alarm output No. according to the alarm interface connected to the external alarm device, and select the linkage method when the selected exception occurs.

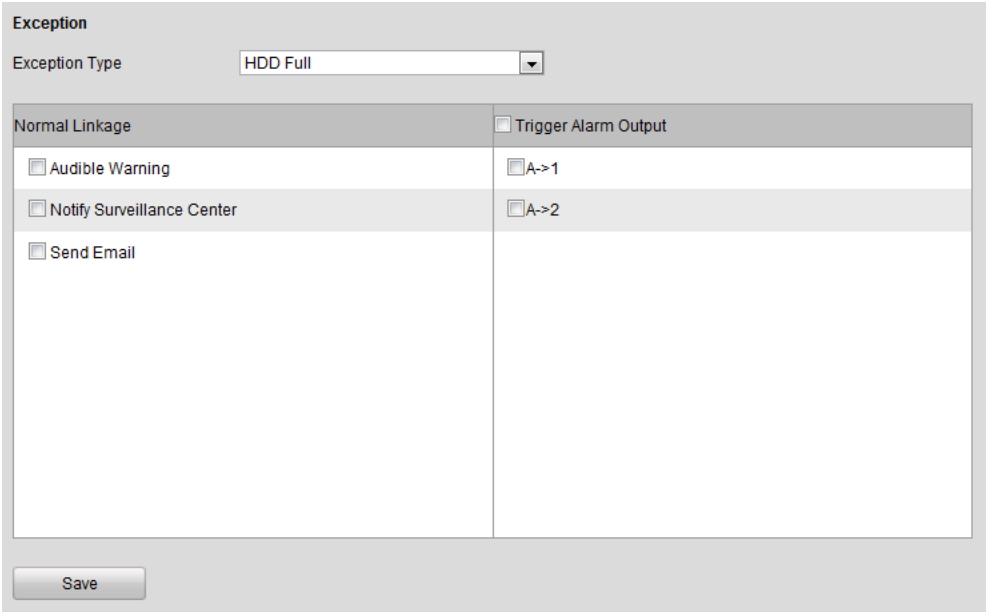


Figure 3-37 Exception

Refer to the following descriptions of Exception Type.

Exception Type	Description
HDD Full	All the HDD space is full.
HDD Error	Error when writing in the HDD or the HDD is not initialize.
Network Disconnected	The network is not connected.
IP Address Conflicted	IP addresses are conflicted.
Illegal Login	Wrong password.
Record/Capture Exception	Exception of record or capture.

3.2.9 Manage User

Go to **Configuration > Remote Configuration > User Management**. You can add, modify and delete users and set user permission in User Management interface.

By default, there is only one user account **admin** and the level is Administrator.

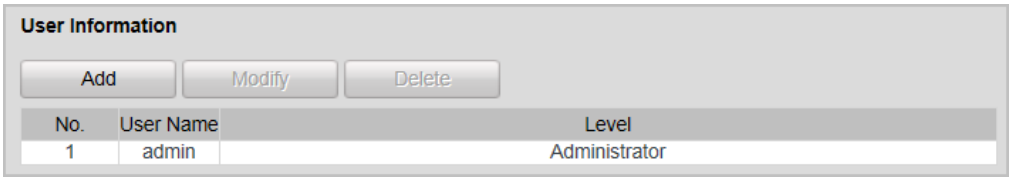


Figure 3-38 User Management

Add a User

Steps:

1. Click **Add** in the User Management interface.
2. Enter the **User Name** and **Password** as desired.

   WARNING

   STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, and contains at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.
3. Select the level as **Operator** or **User**.
4. Confirm the password.
5. Select the user permission including **Basic Permission** and **Camera Configuration** Permission by checking the checkbox.

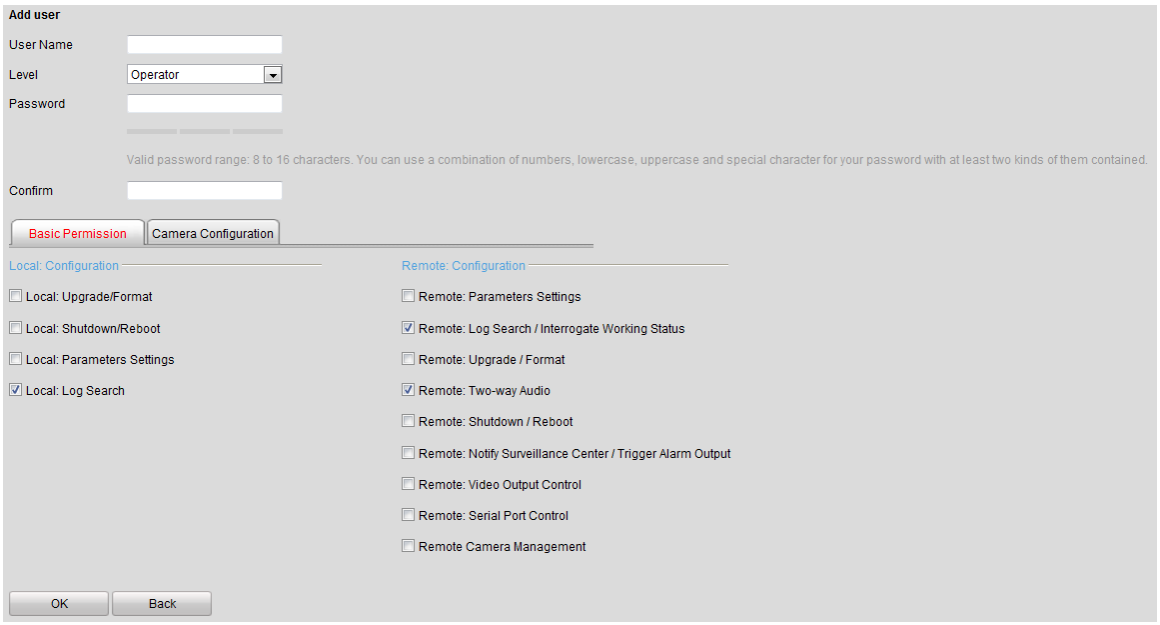


Figure 3-39 Add a User

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

Modify a User

Steps:

1. Select the user account for modifying and click **Modify**.
2. You can modify the user name, password, level and permission.

   NOTE

   - For **admin** account, you can only modify the password.
   - We recommend you to use strong password for security purpose.
3. Click **OK** to save the settings.

Delete a User

Select the user account for deleting and click **Delete**.

NOTE

You cannot delete the **admin** account.

3.2.10 Manage HDD

The device supports HDD management for the purpose of stable and reliable storage.

Configure Basic Settings

Steps:

1. Go to **Configuration > Remote Configuration > HDD Management > Basic Settings**.
2. You can select the HDD No. and set the property as R/W, Read-only or Redundancy.
3. Click **Set** to save the settings.
4. (Optional) Select the HDD in the list and click **Format** to initialize the selected HDD.

NOTE

Initialization removes all the data saved in the HDD.

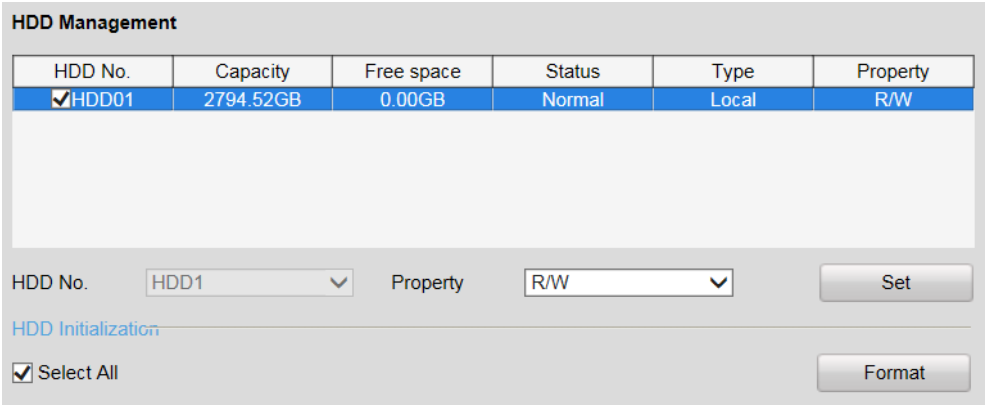


Figure 3-40 HDD Management

Configure Picture Quota

Go to **Configuration > Remote Configuration > HDD Management > Picture Quota**. You can set the space of the picture by setting **Picture Quota**, and the rest space will be used to save the record files.

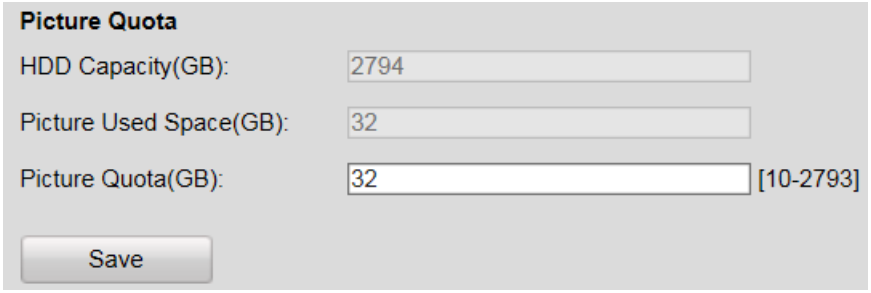


Figure 3-41 Quota Allocation

3.2.11 Debug Log

Running log is used for the research and development personnel to debug the device.

Steps:

1. Go to **Configuration > Remote Configuration > Debug Log**.
2. Check **Save Log**.
3. Set the log saving time, and select the log type. Logs are automatically saved within the set time at the set interval.
4. Select the log mask. The default log mask is to print error information.
5. Set the start time and end time.
6. Click **Save** to save the settings.
7. (Optional) Click **Export** to export the log.

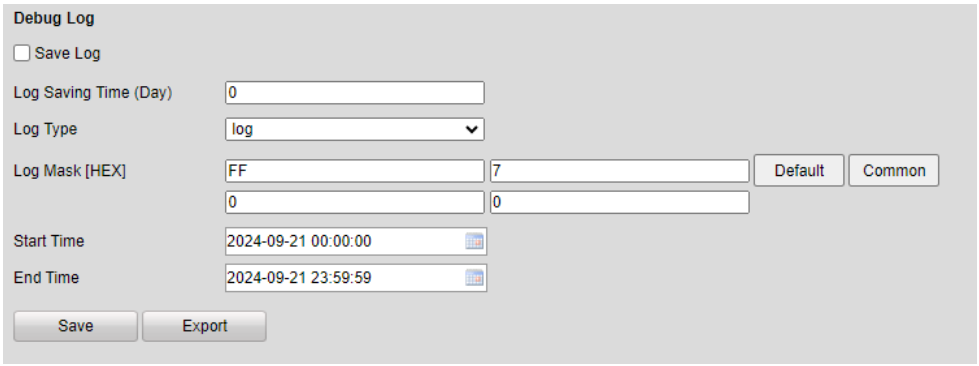


Figure 3-42 Debug Log

3.2.12 Maintenance

You can operate some maintenance functions in Maintenance interface including Reboot, Reset, etc.

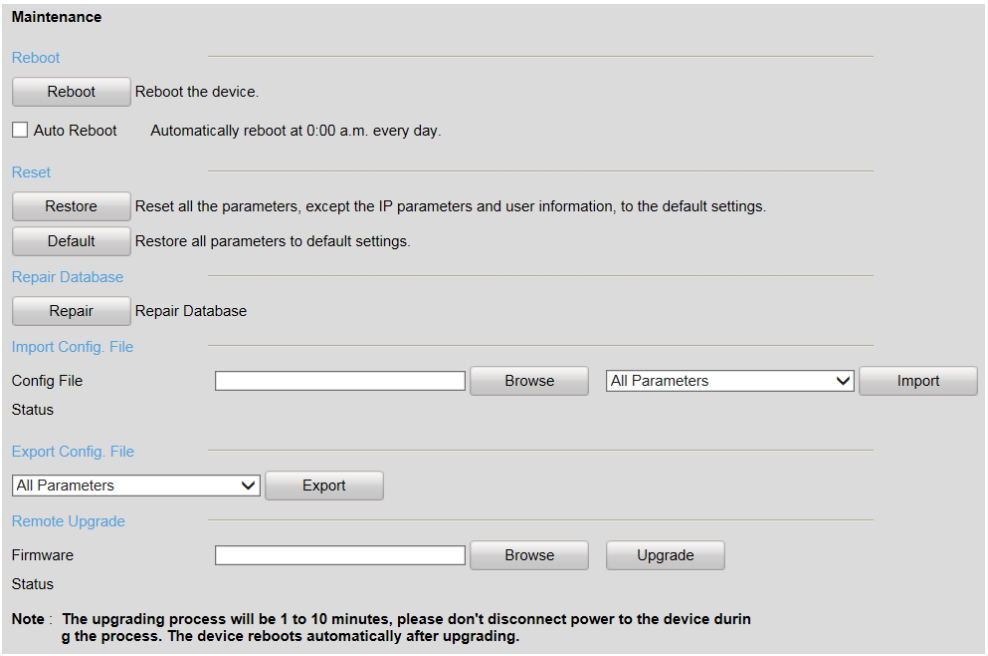


Figure 3-43 Maintenance

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 > Remote Configuration > Maintenance > Reboot**.
2. Click **Reboot**.
3. (Optional) Check **Auto Reboot** as needed. The device will reboot automatically every day.
4. Click **OK** to reboot the device.

Reset Parameters

When the device is abnormal caused by the incorrect set parameters, you can restore the parameters.

Steps:

1. Go to **Configuration > Remote Configuration > Maintenance > Restore**.
2. Select the restoration mode.
   – Click **Restore** to restore the parameters except the IP address, subnet mask, gateway, and port No. to the default settings.
   – Click **Default** to restore all the parameters to the factory settings.
3. Click **OK**.

Repair Database

When the database is abnormal, you can repair the parameters.

Steps:

1. Go to **Configuration > Remote Configuration > Maintenance > Repair**.
2. Click **Repair** to repair the database.
3. Click **OK**.

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:

NOTE

Importing configuration file is only available to the devices of the same model and same version.

1. Go to **Configuration** > **Remote Configuration** > **Maintenance** > **Import Config. File**.
2. Select the import method.
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.

Export Configuration File

Export the configuration file to the computer.

Steps:

1. Go to **Configuration** > **Remote Configuration** > **Maintenance** > **Export Config. File**.
2. Select the export method.
3. Click **Export** to export the configuration file.

Result:

The parameters will be exported.

Upgrade

Upgrade the system when you need to update the device version.

Before You Start:

- Update the plugin before upgrade.
- Prepare the upgrade file. If the upgrade file is a compressed package, it needs to be decompressed into the .dav format.

Steps

1. Go to **Configuration** > **Remote Configuration** > **Maintenance** > **Remote Upgrade**.
2. Click **Browse** to select the upgrade file.
3. Click **Upgrade**.
4. Click **OK** in the popup window.

NOTE

- The upgrade process will take 1 to 10 minutes. Do not cut off the power supply.
- The device will reboot automatically after upgrading.

3.2.13 Connect to Hik-Connect

The guidance terminal can connect to Hik-Connect.

Access to Hik-Connect

Hik-Connect is a micro-video service platform. The guidance terminal can connect to Hik-Connect to realize video/audio on demand, playback, etc.

Steps:

1. Go to **Configuration > Remote Configuration > Platform Settings**.
2. Check the **Enable** checkbox.
3. Select the **Platform Access Mode** as **Hik-Connect**.

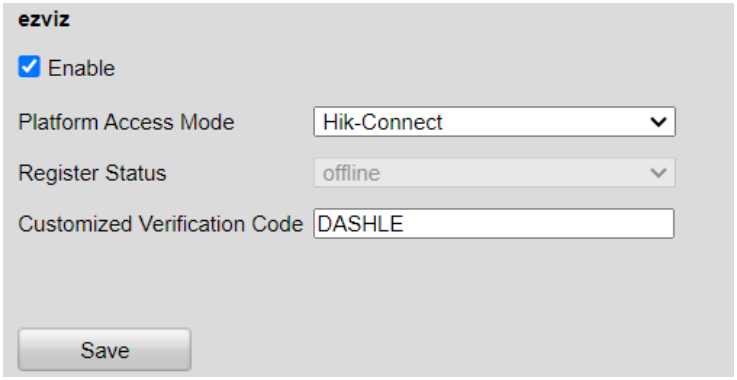


Figure 3-44 Get Access to Hik-Connect

4. Customize a verification code for security.
5. Click **Save** to save the settings.
6. Reboot the guidance terminal to take the settings into effect. Then you can view the **Register Status** to see if the terminal is accessed to Hik-Connect successfully. If the status is online, register the Hik-Connect account, and add the terminal to Hik-Connect.

3.2.14 Configure Remote Host

You can set the remote host parameters for the data uploading in the Remote Host interface.

Steps:

1. Set the remote host parameters.
   1) Go to **Configuration > Remote Configuration > Remote Host**.
   2) Select the remote host from the drop-down list.
   3) Enter the **IP Address**, **Port**, and **Upload Timeout Interval**. If the set time is exceeded, it means that the data upload to the remote host is timed out.
   4) Click **Save** to save the settings.

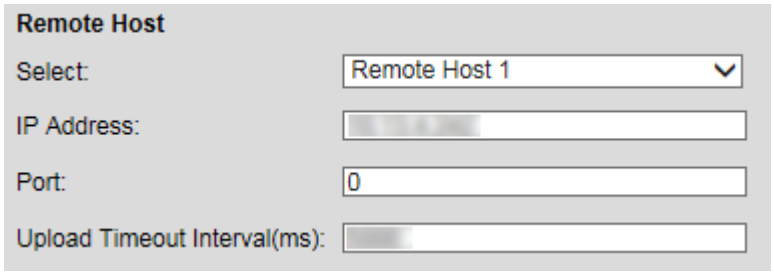


Figure 3-45 Remote Host

2. Set remote host parameters for data upload via HTTP.
   1) Select the remote host from the drop-down list.
   2) Select **Address Format Type** to enter the domain name or IP address.
   3) Enter **Port**, **URL**, **Heartbeat Interval**.
   4) Set the upload interval for the channel status.
   5) Enable **Upload Image**.
3. Click **Save** to save the settings.

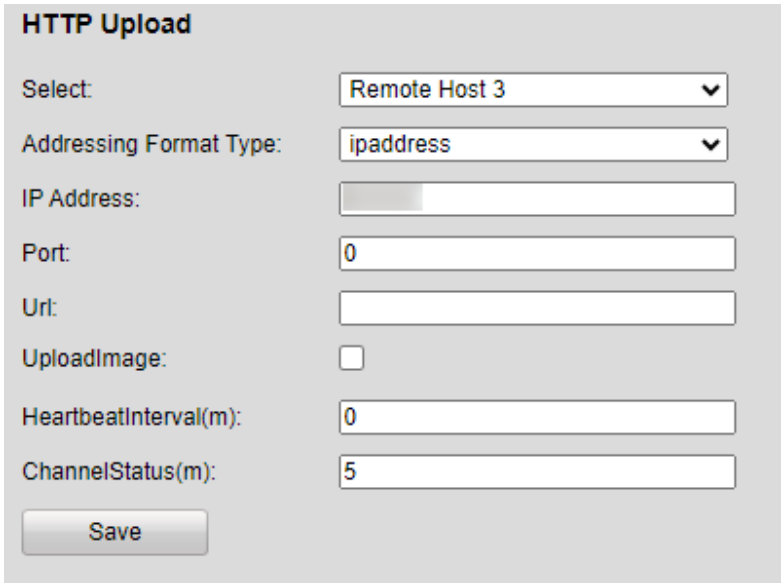


Figure 3-46 HTTP Upload

3.2.15 View Status

You can view the system status in the Status interface.

View Network Uploading Status

Go to **Configuration > Remote Configuration > Status > Network Uploading Status**. You can view the network uploading status to find out if the remote host is enabled. If the status is **Disable**, you should check if the IP address and other parameters are correctly configured in Remote Host interface.

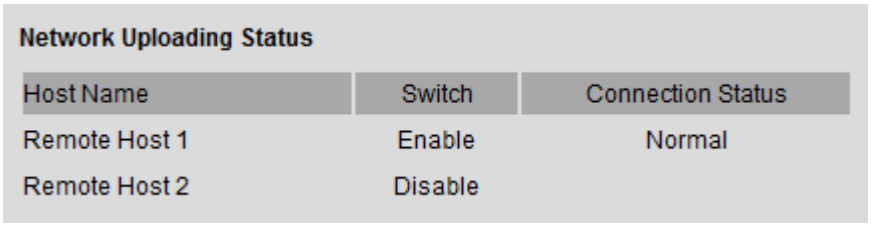


Figure 3-47 Network Uploading Status

View Working Status

Go to **Configuration > Remote Configuration > Status > Working Status**, you can view the system time and working time.

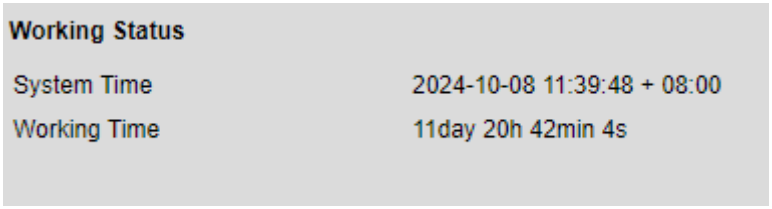


Figure 3-48 Working Status

View Serial Port Status

Go to **Configuration > Remote Configuration > Status > Serial Port Status**, you can view the serial port information.

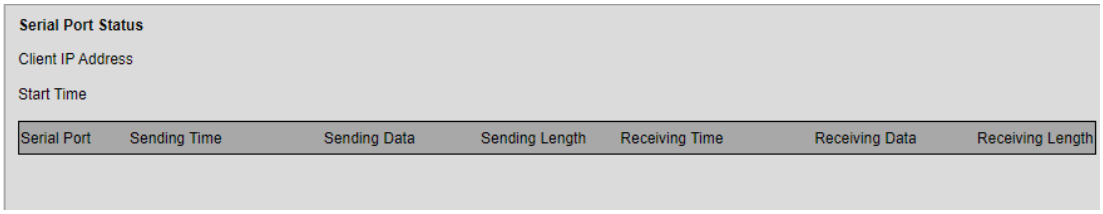


Figure 3-49 Serial Port Status

Chapter 4 Live View

Steps:

1. Open the Live View page.
2. (Optional) Click the icon in the live view toolbar, and select the screen layout mode.
3. Double-click the camera name after selecting the display window to start the live view.
   Or you can click before the camera name to start the live view.
4. (Optional) Click before the camera name to select the main stream or sub stream.

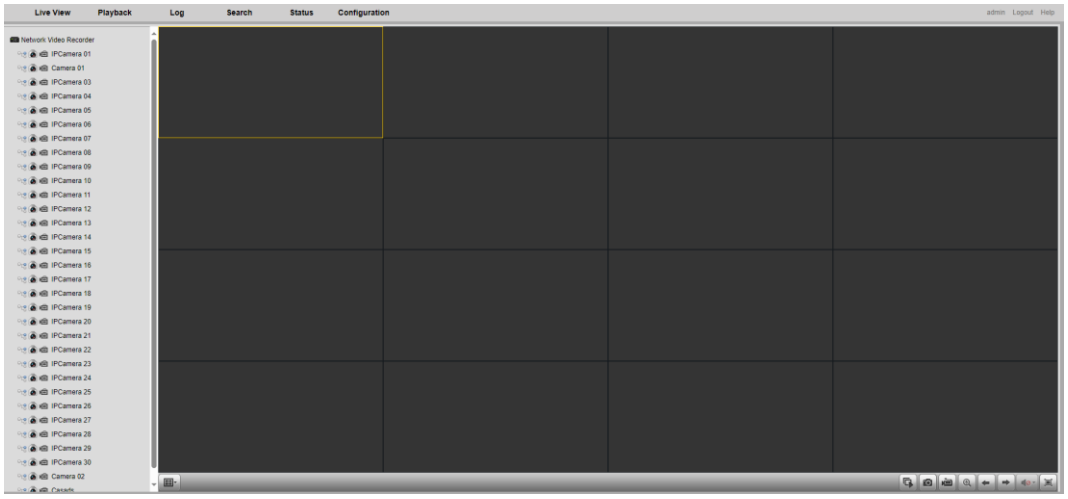


Figure 4-1 Live View Interface

Live View Toolbar:

Figure 4-2 Toolbar

On the Live View page, the following toolbar buttons are available:

Icon	Name	Description
	Set View	Set the screen layout mode. 4 types of screen layout modes are selectable: 1-Screen, 4-Screen, 9-Screen and 16-Screen.
	Start All Live View	Start the live view of all cameras.
	Capture	Capture the picture in the live view process.
	Start All Recording	Start the recording of all cameras.

	Enable e-PTZ	Enable digital zoom. 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.
	Prev Page	Go for live view of the previous page.
	Next Page	Go for live view of the next page.
	Audio On/Audio Off	Turn on/off the audio in live view
	Full Screen	Display the live view in full screen mode. Press **ESC** to exit.

Chapter 5 Playback

Purpose:

The record files stored on the HDDs on the local device can be searched and played back remotely through the web browser.

Click the **Playback** tab to enter the Playback interface. The Playback interface is shown as follows.

Figure 5-1 Playback Interface

Playback Toolbar:

Figure 5-2 Playback Toolbar

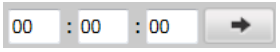
On the Playback page, the following toolbar buttons are available:

Icon	Name	Description
	Set View	Set the screen layout mode. 4 types of screen layout modes are selectable: 1-Screen, 4-Screen, 9-Screen, and 16-Screen.
	Reverse	Go back to the beginning of the current record file.
	Play	Play the record files.
	Stop Playback	Stop the playback of the record files.
	Slow Forward	Decrease the playback speed of the record files.

Icon	Name	Description
	Fast Forward	Increase the playback speed of the record files.
	Single Frame	Play back the record files frame by frame.
	Stop All Playback	Stop the playback of all the cameras.
	Capture	Capture the picture in the playback process.
	Download	Download the record file for backup.
	Start/Stop Clipping	Start/Stop clipping the record files.
	Audio On/Audio Off	Turn on/off the audio in live view
	Full Screen	Display the playback in full screen mode. Press **ESC** to exit.

Steps:

1. Open the Playback page.
2. Select the cameras to be searched from the list.
3. Select the date on the calendar for the search.
4. Click **Search**.
5. Click on the timeline to select the time and play the record. You can click  to zoom out or zoom in on the timeline.

   Or you can input the time in the  and click  to go to the specified time to view the record.

Chapter 6 Log

Purpose:

You can view and export the log files at any time, including operation, alarm, exception and information of device.

Before you start:

The Log function can be realized only when the device is connected with HDD or network disk.

Click **Log** tab to entre the Log interface.

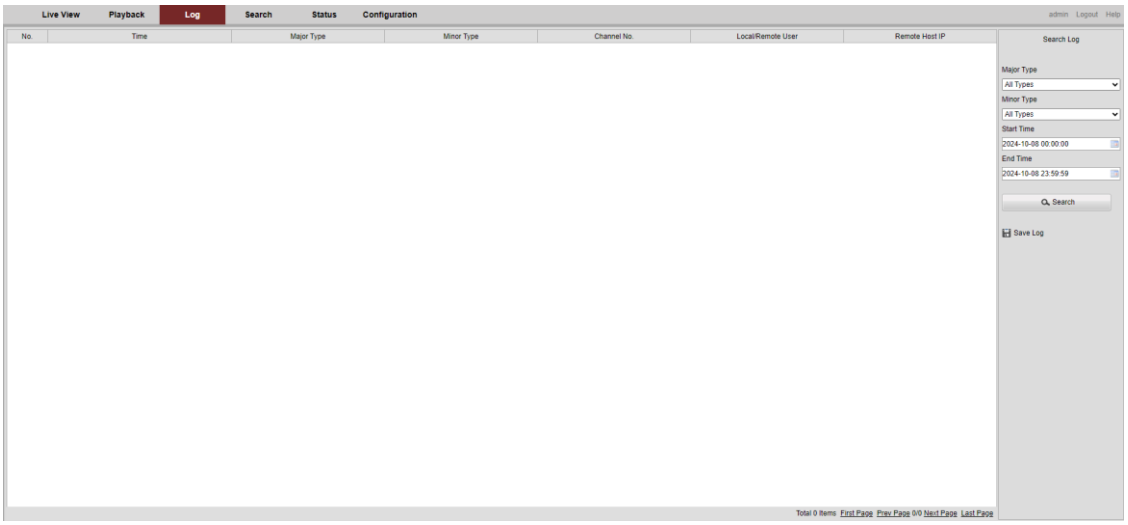


Figure 6-1 Log Interface

Steps:

1. Open the Log Search page.
2. Select the **Major Type**. There are four major types, including **Alarm**, **Exception**, **Operation**, and **Information**. You can also select **All Types** to search all types of the log.
3. Select the **Minor Type**.
4. Click to specify the **Start Time** and **End Time**.
5. Click **Search**. The log files between the start time and end time will be displayed on the list.
6. (Optional) You can click **Save Log** to save the searched logs.

NOTE

Please narrow the time range or filter the log type for search if there are too many log files.

Chapter 7 Data Search

Purpose:

You can search the data such as the license plate number, parking space number, etc. by specifying the search condition in Search interface.

Click the **Search** tab to enter the Search interface.

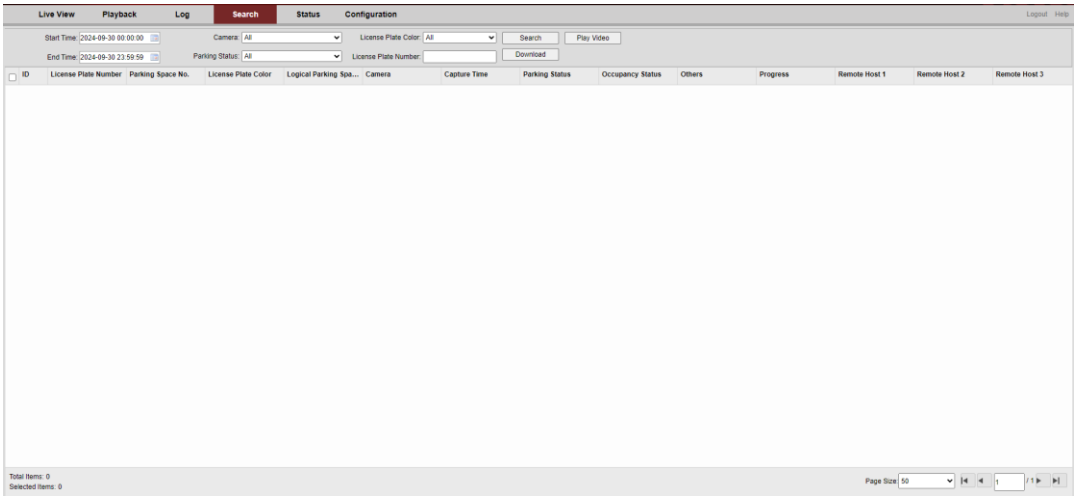


Figure 7-1 Search Interface

Steps:

1. Click to specify the **Start Time** and **End Time**.

   NOTE

   - When inputting the time, you can click for quick selection.
   - Time range cannot exceed 7 days.
2. Select the **Camera** from the drop-down list.
3. Select **Parking Status** from the drop-down list.
4. Select **License Plate Color** from the drop-down list.
5. (Optional) You can enter the **License Plate Number** for detailed search.
6. Click **Search**.

Chapter 8 Status

Purpose:

You can view the status of the current working cameras as well as the parking space status.

Click **Status** tab to enter the Status interface.

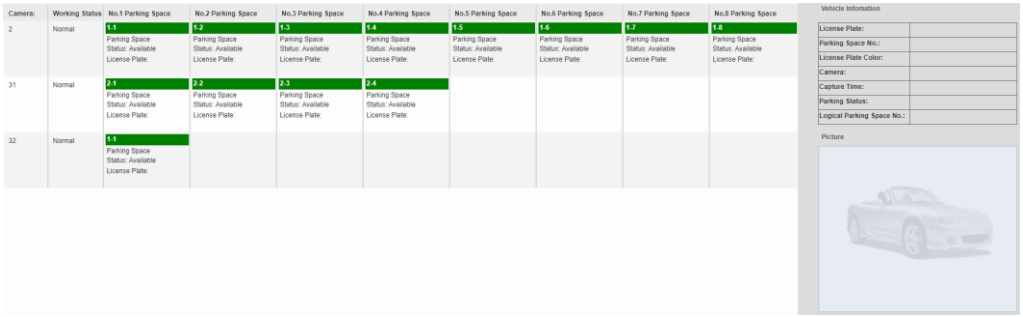


Figure 8-1 Status Interface

You can view the camera working status, and the parking space information including parking space status, liscence plate, etc.

NOTE

- If the colour of parking space box on the interface and the colour of the parking space indicator is the same, the parking space is occupied by a vehicle.
- If the parking space box on the interface is coloured, click it and you can view vehicle information and picture on the right part of the interface as follows.

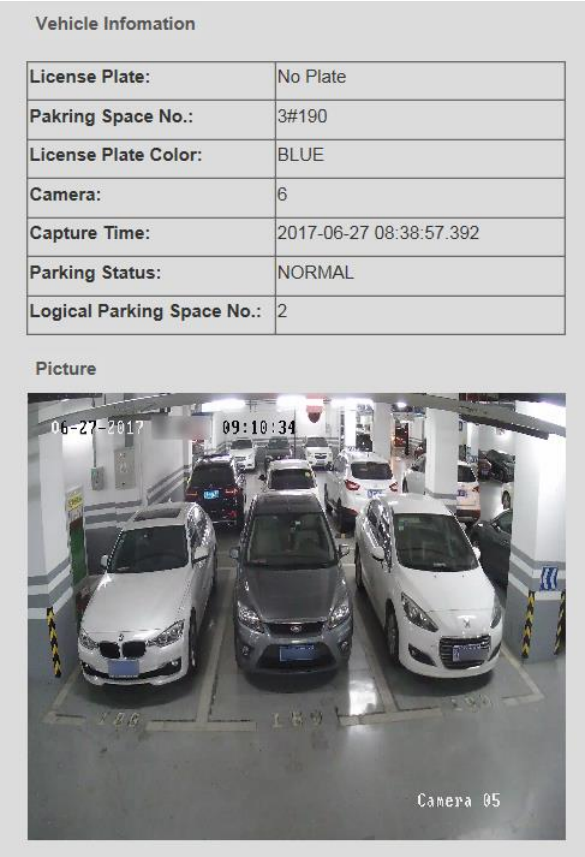


Figure 8-2 Vehicle Information


See Far, Go Further