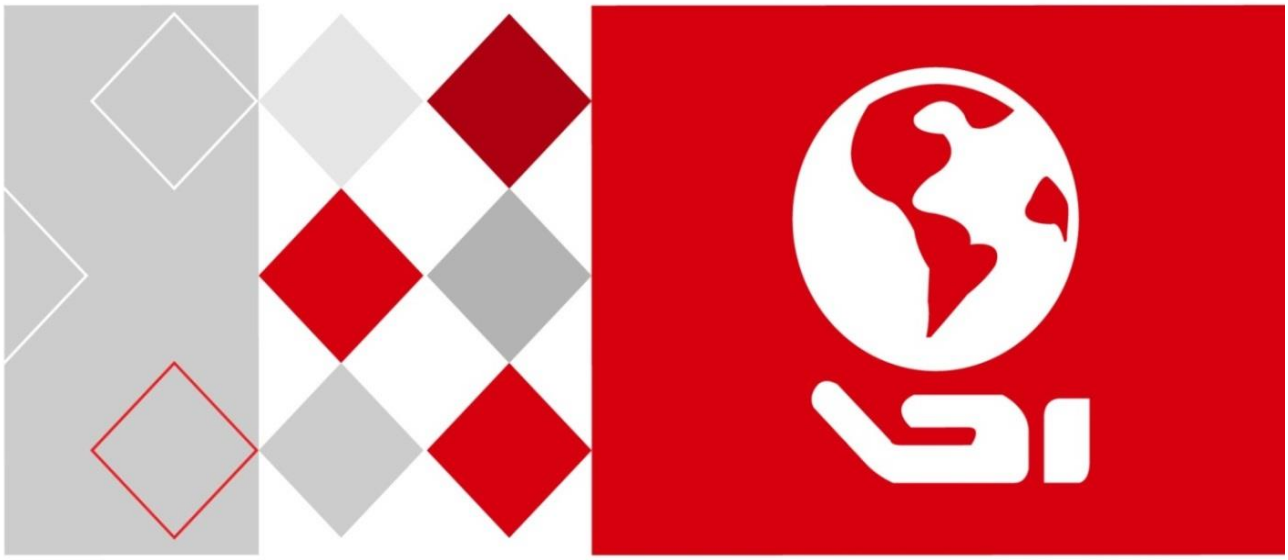
HIKVISION



# Entrance & Exit Station

User Manual

UD03949B

**User Manual**

COPYRIGHT ©2016 Hangzhou Hikvision Digital Technology Co., Ltd.
**ALL RIGHTS RESERVED.**
Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be "Hikvision"). This user manual (hereinafter referred to be "the Manual") cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

**About this Manual**

This Manual is applicable to Entrance & Exit Station.
The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (http://overseas.hikvision.com/en/).
Please use this user manual under the guidance of professionals.

**Trademarks Acknowledgement**

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

**Legal Disclaimer**

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS", WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

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

# Regulatory Information

## FCC Information

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

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

### FCC Conditions

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

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

### EU Conformity Statement

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

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

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

### Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

# Symbol Conventions

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

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

# Safety Instructions

- Please adopt the power adapter which can meet the safety extra low voltage (SELV) standard.
- To reduce the risk of fire or electrical shock, do not expose this product to rain or moisture.
- This installation should be made by a qualified service person and should conform to all the local codes.
- Please install blackouts equipment into the power supply circuit for convenient supply interruption.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

# Preventive and Cautionary Tips

- Make sure the power supply voltage is correct before using the device.
- Do not drop the device or subject it to physical shock.
- Do not place the device in extremely hot, cold temperatures (please refer to the product specification for the operating temperature), dusty or damp environment, and do not expose it to high electromagnetic radiation.
- To avoid heat accumulation, good ventilation is required for a proper operating environment.
- Keep the device away from water and any liquid.
- While shipping, the device should be packed in its original packing.

- Improper use or replacement of the battery may result in hazard of explosion. Please use the manufacturer recommended battery type.

# Table of Contents

Chapter 1 Introduction ..... 7
1.1 Product Overview ..... 7
1.2 Features and Functions ..... 7
1.3 Front Panel Introduction ..... 8
Chapter 2 Connecting Peripheral Devices ..... 10
Chapter 3 Activation and Login ..... 12
3.1 Activation ..... 12
3.1.1 Activating via SADP ..... 12
3.1.2 Activating via Web Browser ..... 15
3.2 Login via Web Browser ..... 15
Chapter 4 Live View ..... 17
Chapter 5 Searching Data ..... 19
5.1 Searching Card ..... 19
5.2 Searching Vehicle ..... 19
Chapter 6 Configuring General Parameters ..... 21
6.1 Configuring Local Settings ..... 21
6.2 Configuring System Settings ..... 22
6.2.1 Configuring Basic Information ..... 22
6.2.2 Configuring Time Settings ..... 23
6.2.3 Maintenance ..... 24
6.2.4 Configuring Security ..... 25
6.2.5 Managing Camera ..... 26
6.2.6 Managing User ..... 28
6.3 Configuring Network ..... 31
6.3.1 Configuring TCP/IP ..... 31
6.3.2 Configuring Port ..... 32
6.3.3 Configuring Two-Way Audio ..... 33
6.4 Configuring Image ..... 33
6.4.1 Configuring Display Settings ..... 33
6.4.2 Configuring OSD Settings ..... 34
6.4.3 Configuring Privacy Mask ..... 35
6.5 Configuring Event ..... 36

6.5.1 Configuring Alarm Input ..... 36
6.5.2 Configuring Alarm Output ..... 39
6.5.3 Configuring Exceptions ..... 40
Chapter 7 Configuring Entrance and Exit ..... 41
7.1 Checking Status of Entrance & Exit ..... 41
7.1.1 Checking Vehicle Status ..... 41
7.1.2 Checking Ticket/Card Status ..... 41
7.1.3 Checking Synchronization Status ..... 41
7.1.4 Checking Passing Status ..... 42
7.1.5 Checking Peripheral Status ..... 42
7.1.6 Checking Arming Status ..... 42
7.1.7 Checking System Status ..... 43
7.2 Configuring Entrance & Exit Settings ..... 43
7.2.1 Configuring Basic Parameters ..... 43
7.2.2 Configuring Ticket ..... 44
7.2.3 Configuring Audio ..... 45
7.2.4 Configuring Multi-Channel Capture ..... 45
7.2.5 Configuring Barrier Settings ..... 46
7.3 Configuring Logs ..... 47
Chapter 8 Application of Other Models ..... 48
8.1 Checking Card Status ..... 48
8.2 Configuring Offline Settings ..... 48

# Chapter 1 Introduction

## 1.1 Product Overview

DS-TME4XX series Entrance & Exit Station is used for data acquisition and management of entrance & exit and parking lot. Through interaction with the software, the station can control the entrance & exit and manage the parking lot effectively. It is composed of audio output module, LED display module, main control module, vehicle detection module and power supply module. Peripheral devices such as analog camera, capture camera, barrier gate, remote card reader, alarm device, etc. can be connected to realize the vehicle passing, charging and management.

The models and functions of the Entrance & Exit Station are shown in the following figure.

Table 1-1 Entrance & Exit Station

| Model | Functions |
|---|---|
| DS-TME401-TPL | Entrance station, supporting taking ticket, LED display, voice prompt, etc. |
| DS-TME402-TPL | Exit station, supporting barcode scan, LED display, voice prompt, etc. |
| DS-TME401-TL-S | Entrance station, supporting LED display, voice prompt, etc. |
| DS-TME402-TL-S | Exit station, supporting LED display, voice prompt, etc. |
| DS-TME401-TRL | Entrance station, supporting automatic card dispatch, LED display, voice prompt, etc. |
| DS-TME402-TRL | Exit station, supporting automatic card collection, LED display, voice prompt, etc. |

NOTE

- This user manual takes DS-TME401-TPL as an example. Refer to Chapter 4 for the details about the differences of other models.
- The Entrance & Exit Station must be used with the matched software.

## 1.2 Features and Functions

- 2-ch analog cameras and 4-ch IP cameras hybrid access
- Build-in one 1 GB SSD
- Build-in 1 100M Ethernet interface

- Access via WEB
- Alarm triggered when arming vehicle (vehicle in blacklist or owing fees) enter or illegal break-in
- Light on when the parking lot is full
- LED and voice prompt system
- Built-in multiple RS-485 serial interfaces and 1 RJ45 network interface
- License plate number recognition to permit the vehicle in and out

## 1.3 Front Panel Introduction

NOTE

The front panels vary with different models. We take the front panel of card station for example.

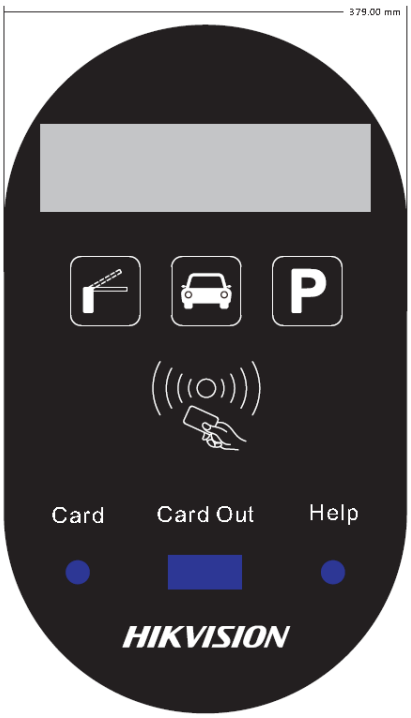
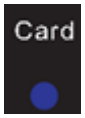
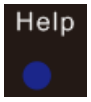



Figure 1-1 Front Panel

Table 1-2 Front Panel Description

| No. | Icon | Name | Description |
|---|---|---|---|
| 1 | | LED Display | Displays information such as prompt, parking charge, license plate number, etc. |
| 2 | | Barrier Status Indicator | Shows the open or closed status of barrier. |
| 3 | | Inductive Loops Indicator | The indicator is on when the inductive loops detect the vehicle and off when the vehicle leaves the inductive loops completely. |
| 4 | | Parking Space Indicator | The indicator is on when all the parking spaces are occupied and off when there are unoccupied parking spaces. |
| 5 | | Card Reader | Swipe card to read it. |
| 6 |   | Take Card | Press the button to take card when the vehicle enters the parking lot. |
| 7 | | Card Out | Take card here to enter the parking lot and start time-based charge. |
| 8 |   | Help | Two-way audio with the management center. |

# Chapter 2 Connecting Peripheral Devices

The internal connection has been finished before the device leaves factory. Wiring is not needed for the internal connection.

Contact the site operation personnel to connect the peripheral devices.

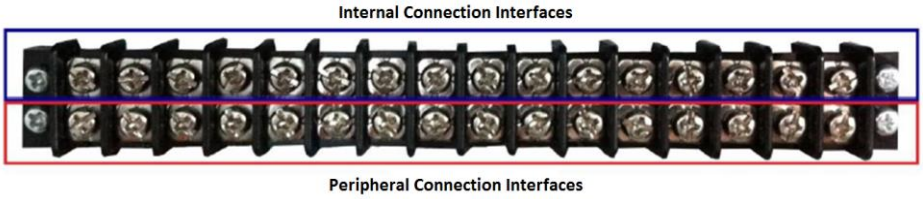



Figure 2-1 Connection Interfaces

Refer to the Figure 2-2 and Table 2-1 for the description of the interfaces.

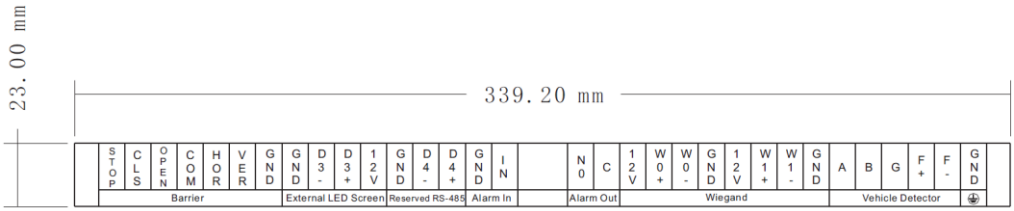



Figure 2-2 Interfaces Description

Table 2-1 Interfaces Description

| Pin | Function | Peripheral Connection | Pin | Function | Peripheral Connection |
|---|---|---|---|---|---|
| 1 | GND | Reserved RS-485 serial interfaces | 17 | N0 | Alarm output |
| 2 | D4- | | 18 | C | |
| 3 | D4+ | | 19 | 12V | Wiegand interfaces |
| 4 | GND | For external LED screen connection | 20 | W0+ | |
| 5 | D3- | | 21 | W0- | |
| 6 | D3+ | | 22 | GND | |
| 7 | 12V | | 23 | 12V | |
| 8 | STOP | Interfaces for | 24 | W1+ | |
| 9 | CLS | | 25 | W1- | |

| | | | | | |
|---|---|---|---|---|---|
| 10 | OPEN | connecting and controlling barrier | 26 | GND | |
| 11 | COM | | 27 | A | Vehicle detector inductive loops input |
| 12 | HOR | | 28 | B | |
| 13 | VER | | 29 | G | |
| 14 | GND | | 30 | F+ | Vehicle detector output |
| 15 | GND | Alarm input | 31 | F- | |
| 16 | IN | | 32 | GND | GND |

The entrance and exit station can connect other devices such as capture camera, barrier gate and entrance & exit control terminal as shown below.

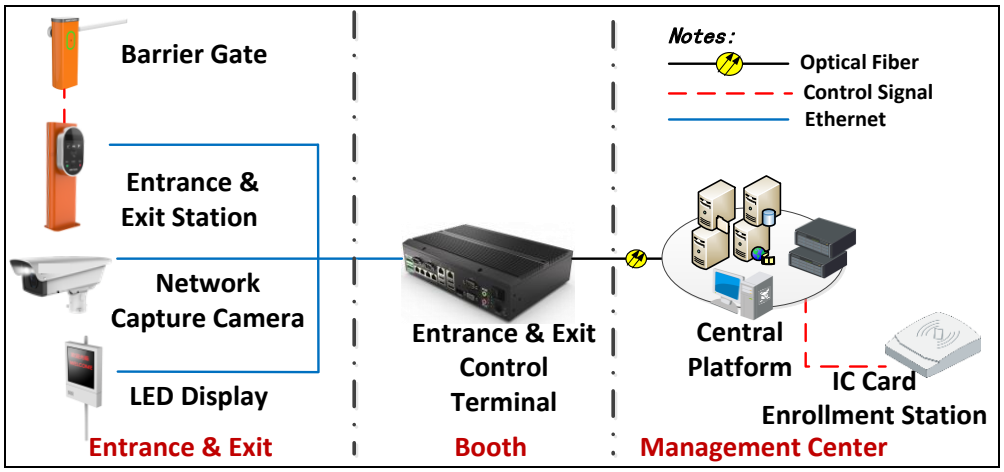



Figure 2-3 Device Connection

NOTE

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

# Chapter 3 Activation and Login

## 3.1 Activation

***Purpose***

You need to activate the device and set the password for first-time login. You can activate the device via SADP or web browser.

NOTE

- The default IP address: 192.0.0.64.
- The default port: 8000 for SDK activation, 80 for web browser activation, and 37020 for SADP activation.
- The default user account: *admin*.

### 3.1.1 Activating via SADP

NOTE

SADP software is enclosed in the disc. You can also download it from the company website.

Step 1 Install SADP software.

After running, it automatically searches the online devices every 1 minute from the subnet where your computer locates. It displays the total number and information of the searched devices in the device list. Device information includes the device type, IP address, port No., gateway, etc.

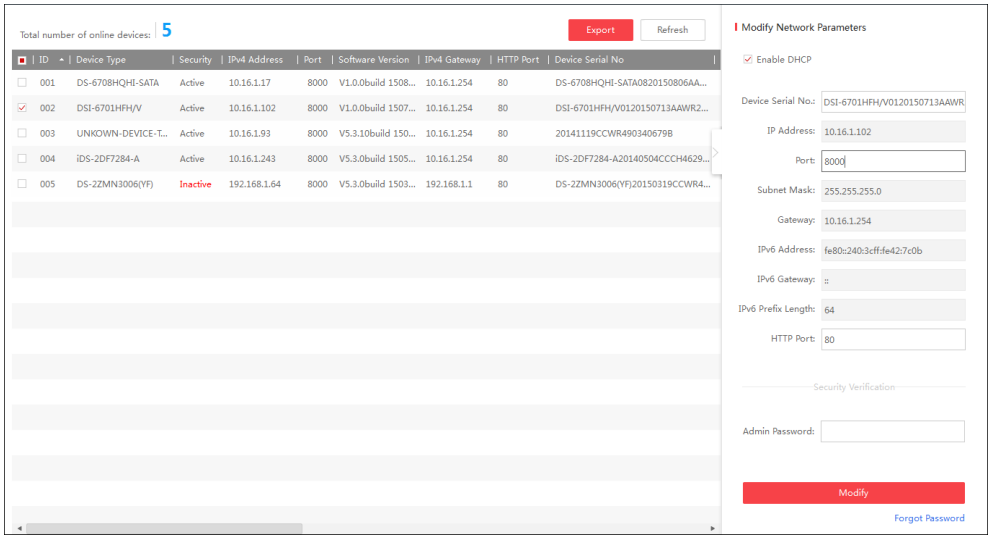



Figure 3-1 SADP Activation

Step 2 Check the checkbox of the device for activation and the device information will be displayed on the right side. On **Activate the Device** interface, create a password for the device and confirm the password. The system will judge password strength automatically, and we highly recommend you to use a strong password to ensure your data security.

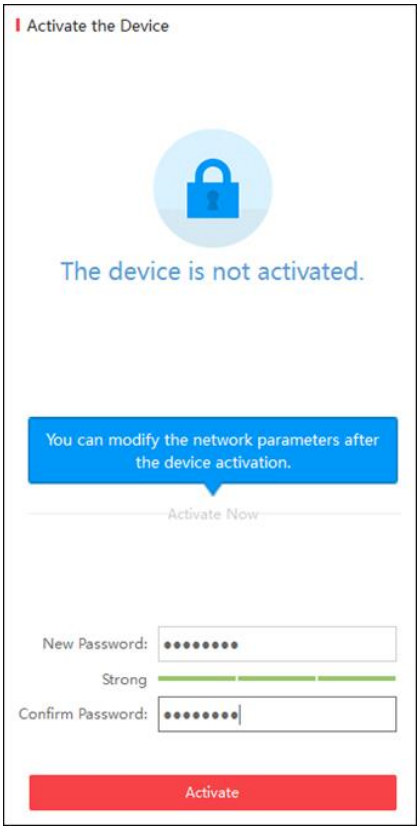



Figure 3-2 Activate the Device

**WARNING**

**STRONG PASSWORD RECOMMENDED**–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.

Step 3 Click **Activate** to activate the device. A "The device is activated." hint window pops up when the password is set successfully.

Step 4 Modify the network parameters. Select the device to be modified in the device list by checking the checkbox and the network parameters of the device will be displayed on the **Modify Network Parameters** interface on the right side. Set the network parameters including IP address, sub network mask, gateway, etc.

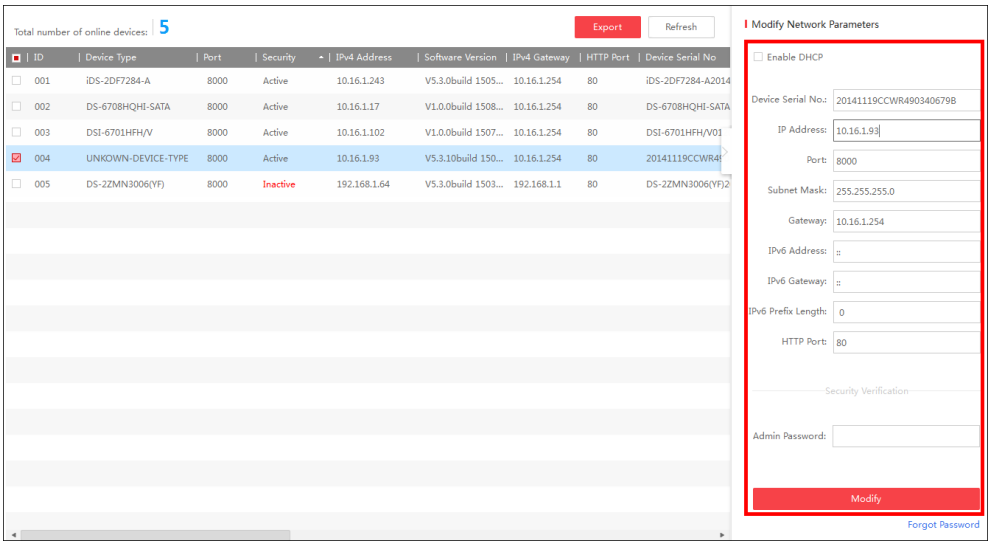



Figure 3-3 Modify Network Parameters

Step 5 Input the password of the admin account of the device in the **Admin Password** text field and click **Modify** to modify the parameters.

**NOTE**

- When setting IP address, keep the IP address of the device and the computer in the same network segment.
- "Admin" is the administrator of the device. We recommend you to create a new user to operate for protecting your data security.

### 3.1.2 Activating via Web Browser

Step 1 Modify the IP address of your computer to ensure the IP address of the computer and the device are in the same network segment.

Step 2 Input the default IP address of the entrance & exit station in the address bar of the web browser and press **Enter** to enter the activation interface.

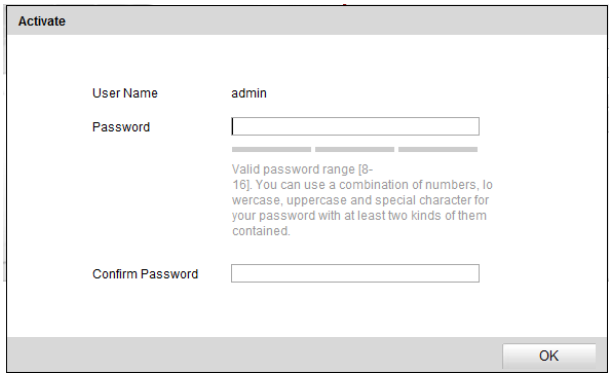



Figure 3-4 Activate via Web Browser

Step 3 Enter a new password and click **OK** to activate the device.

NOTE

- The default IP address of the entrance & exit station is 192.0.0.64.
- You are highly recommended to use a strong password to ensure your data security.

## 3.2 Login via Web Browser

***Purpose***

You can log in to the entrance & exit station via web browser for further operations such as live view, playback, local configuration, etc.

Step 1 In the address bar of the web browser, input the IP address of the entrance & exit station, and press the **Enter** key to enter the login interface.

Figure 3-5 Login Interface

NOTE

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

Step 2 Input the user name and password of the entrance & exit station.

Step 3 Click **Login**.

Step 4 For the first login, you should install the plug-in before other operations. Click **Please click here to download and install the plug-in. Close the browser when installing the plug-in.** on the live view page, run and install the plug-in according to the prompt. After the installation of plug-in, re-open the web browser and login.

NOTE

Close your web browser during the installation of the plug-in.

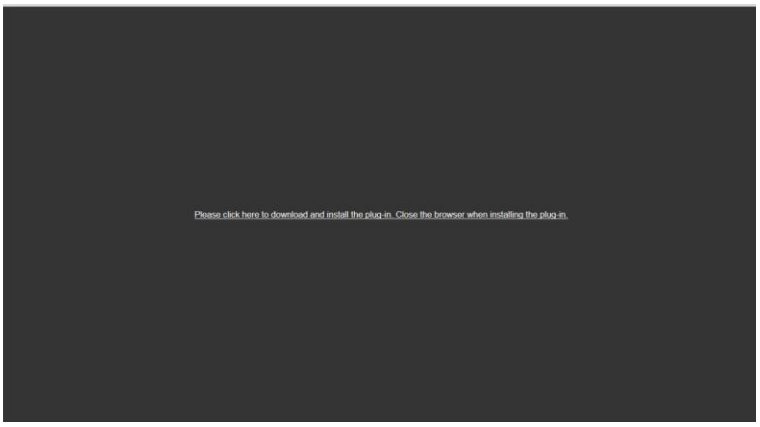



Figure 3-6 Install the Plug-in

Step 5 After login, you enter the Live View interface as below.

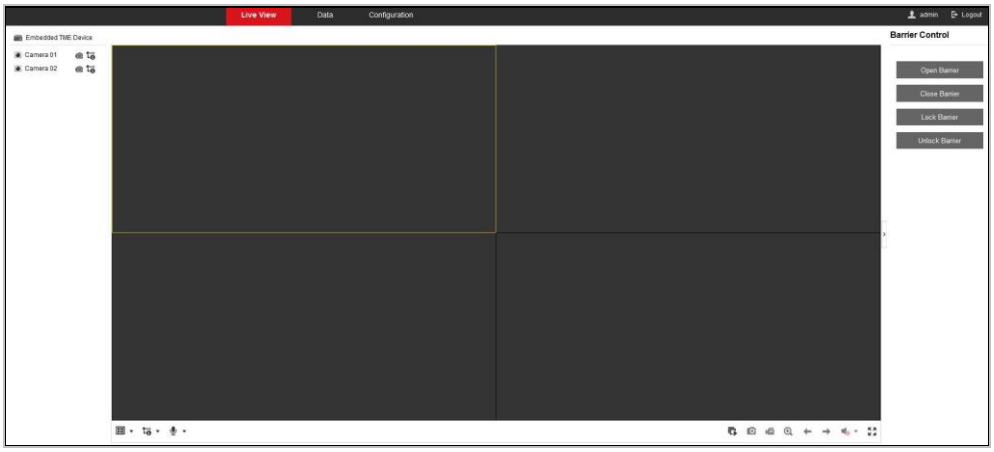



Figure 3-7 Live View Interface

# Chapter 4 Live View

***Purpose***

Click **Live View** to enter the Live View interface. You can control live view of the connected cameras and barrier on the interface.

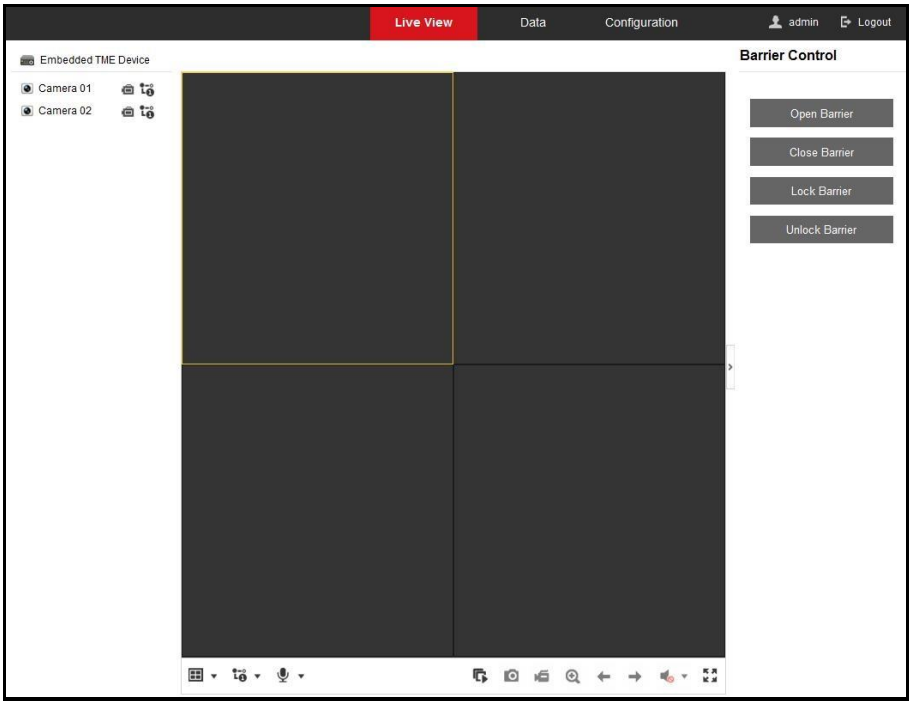



Figure 4-1 Live View

On the Live View interface, see the following table for the functions of the interface icons.

Table 4-1 Icon Description

| Icon | Name | Description |
|---|---|---|
| / | Start/Stop Live View of the Selected Camera | Start/Stop live view of the selected camera. |
| | Select Window Division Mode | Select the window division mode. 1, 4, 9 and 16 window division modes are selectable. |
| | Select Stream Type | Main Stream and Sub-Stream are selectable. |
| | Start Two-Way Audio | Start two-way audio. |

| | | |
|---|---|---|
| / | Start/Stop All Live View | Start/Stop live view of all the cameras. |
| | Capture | Capture picture in live view. |
| / | Start/Stop All Recording | Start/Stop recording of all the cameras. |
| / | Enable/Disable e-PTZ | Enable/Disable e-PTZ function. |
| | Prev. Page | Go for live view of the previous page. |
| | Next Page | Go for live view of the next page. |
| / | Audio On/Off | Turn on/off the audio in live view |
| | Adjust the Volume | Slide the bar to adjust the volume. |
| | Full Screen | Display the live view of the selected camera in full screen. Press **ESC** to exit. |
| Open Barrier | Open Barrier | Open barrier. |
| Close Barrier | Close Barrier | Close barrier. |
| Lock Barrier | Lock Barrier | Lock barrier. |
| Unlock Barrier | Unlock Barrier | Unlock barrier. |

**NOTE**

The functions of different models may differ. Refer to the actual operation interface.

# Chapter 5 Searching Data

***Purpose***

Click **Data** to enter the Search Data interface. You can search card and vehicle information via the configured search conditions.

## 5.1 Searching Card

***Purpose***

You can search card according to the Card Type and Card Status, or you can input the Card No. to search the specific card.

Step 1 Click **Card Search** tab to enter the Card Search interface.

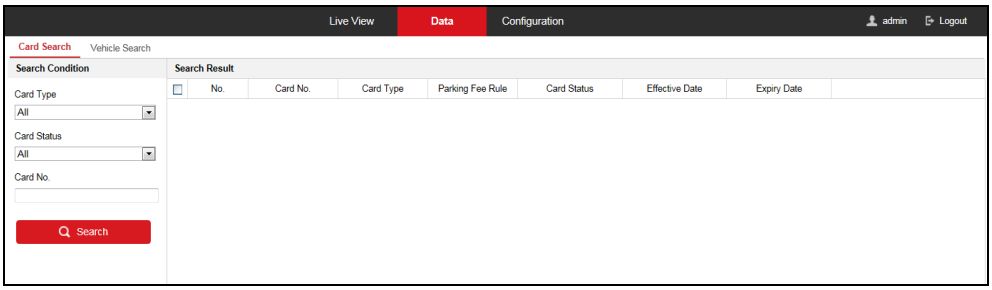



Figure 5-1 Card Search

Step 2 (Optional) On the **Search Condition** panel, select the **Card Type**. **All**, **Internal Card** and **Temporary Card** are selectable.

The default option is **All**.

Step 3 (Optional) Select the **Card Status**. **All**, **Normal**, **Lost**, **Cancelled** are selectable.

The default option is **All**.

Step 4 (Optional) Input the **Card No.** in the text field.

Step 5 Click **Search** to search the card. The search results will be displayed on the right. You can view the information of the Card No., Card Type, Parking Fee Rule, Card Status, Effective Date and Expiry Date.

## 5.2 Searching Vehicle

***Purpose***

You can search vehicle according to the Vehicle Type and License Plate Color, or you can input the License Plate Number to search the specific vehicle.

Step 1 Click **Vehicle Search** tab to enter the Vehicle Search interface.

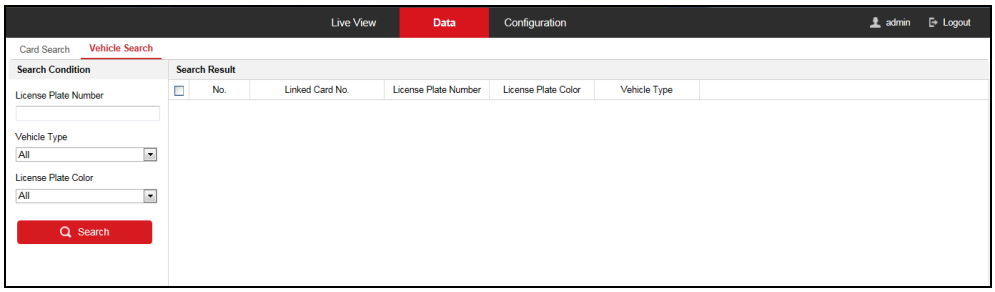



Figure 5-2 Vehicle Search

Step 2 (Optional) Input the **License Plate Number** in the text field.

Step 3 (Optional) Select the **Vehicle Type**. **All**, **Light-Duty Vehicle**, **Oversize Vehicle** and **Other** are selectable.

Step 4 (Optional) Select the **License Plate Color**. **All**, **Blue**, **Yellow**, **White**, **Black**, **Other** are selectable.

Step 5 Click **Search** to search the vehicle. The search results will be displayed on the right. You can view the information of the Linked Card No., License Plate Number, License Plate Color and Vehicle Type.

# Chapter 6 Configuring General Parameters

## 6.1 Configuring Local Settings

Step 1 Enter the Local Configuration interface.

Configuration > Local

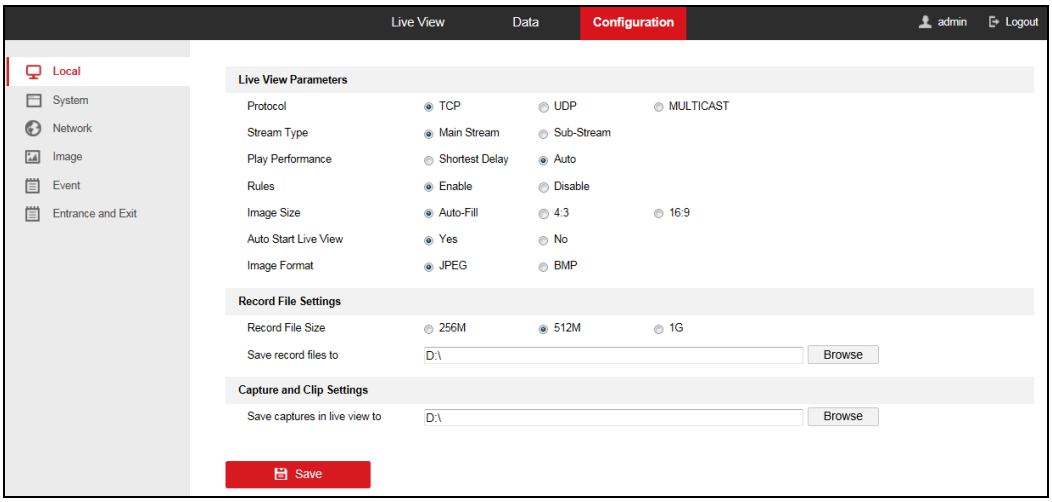



Figure 6-1 Local Configuration

Step 2 Configure the Live View Parameters, Record File Settings and Picture and Clip Settings on this interface.

- **Live View Parameters**

1) **Protocol**: TCP, UDP and MULTICAST are selectable. TCP is selected by default. Select UDP when high requirement of video stream is not needed and the network is not stable. Select MULTICAST when there are multiple users and you need to configure multicast address before you select it.

2) **Stream Type**: Main Stream and Sub-Stream are selectable.

3) **Play Performance**: Shortest Delay and Auto are selectable. Auto is selected by default. Auto mode considers both real time and fluency. While Shortest Delay mode has good real-time performance but it may influence the fluency.

4) **Rules**: Enable and Disable are selectable. If you enable rules, the live view will display the configured VCA rule lines or quadrilaterals.

5) **Image Size**: Auto-Fill, 4:3 and 16:9 are selectable.

6) **Auto Start Live View**: If you select Yes, live view will automatically starts after the device is accessed.

7) **Image Format**: Select the captured picture format. JPEG and BMP are selectable.

- **Record File Settings**

1) **Record File Size**: 256M, 512M and 1G are selectable. It is the size of single video record file saved locally.

2) **Save record files to**: Click **Browse** to set the local path to save the video record files.

- **Capture and Clip Settings**

**Save captures in live view to**: Click **Browse** to set the local path to save the captures in live view.

# 6.2 Configuring System Settings

## 6.2.1 Configuring Basic Information

Step 1 Enter the Basic Information interface.

Configuration > System > System Settings > Basic Information

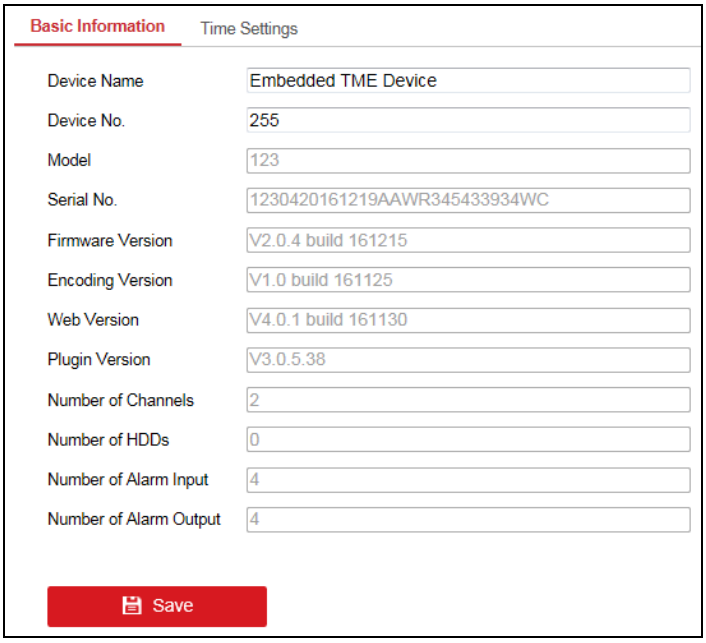



Figure 6-2 Basic Information

Step 2 (Optional) Edit the **Device Name** and **Device No.**

Step 3 View the other device information including Model, Serial No., Firmware Version, Encoding Version, Web Version, Plugin Version, Number of Channels, Number of HDDs, Number of Alarm Input and Number of Alarm Output.

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

NOTE

Number of Channels, Number of HDDs and Number of Alarm Input depend on the actual device.

### 6.2.2 Configuring Time Settings

Step 1 Enter the Time Settings interface.

Configuration > System > System Settings > Time Settings

Figure 6-3 Time Settings

Step 2 Select the **Time Zone**.

Step 3 Configure the synchronization (NTP Time Synchronization or Manual Time Synchronization).

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

1) Click the radio button before NTP to enable it.

2) Input the **Server Address**, **NTP Port** and **Interval**.

- **Manual Time Sync.**: After enabling Manual Time Synchronization, the device time can be synchronized with the set time or the computer time.

1) Click the radio button before **Manual Time Sync.** to enable it.

2) Click to set the time.

3) (Optional) Check the checkbox of **Sync. with computer time** to synchronize the device time with the computer time.

Step 4 (Optional) Configure the DST.

1) Check the checkbox of **Enable DST** to enable it.

2) Configure the **Start Time**, **End Time** and **DST Bias**.

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

### 6.2.3 Maintenance

Step 1 Enter the Maintenance interface.

Configuration > System > Maintenance > Upgrade & Maintenance

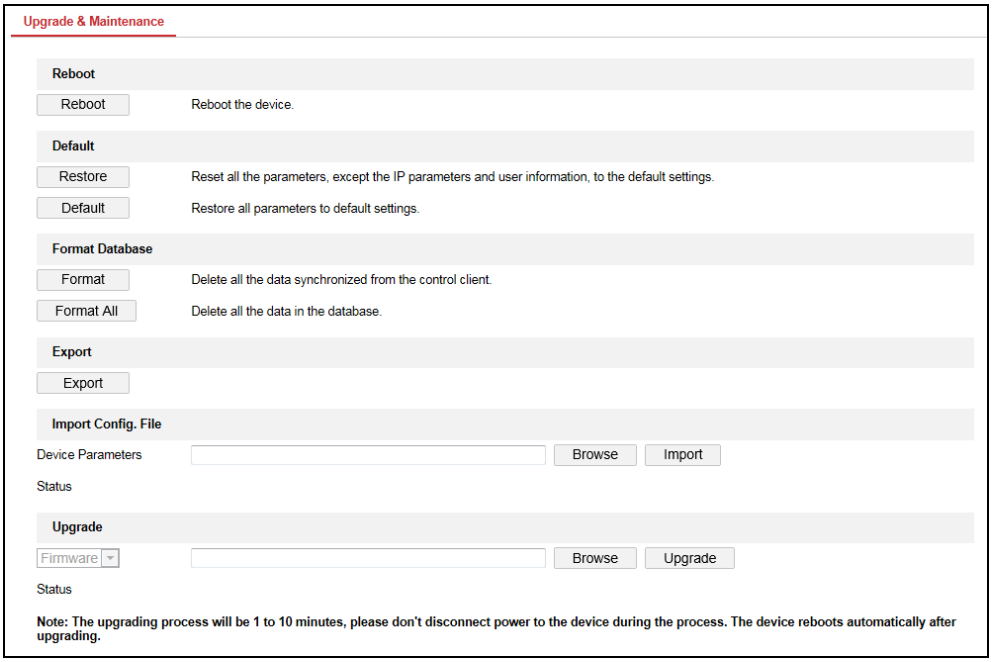



Figure 6-4 Maintenance

Step 2 Configure the following parameters.

- **Reboot**

  Click **Reboot** to reboot the device.

- **Restore**

  1) (Optional) Click **Restore** to reset parameters, except the IP parameters, user information and video standard, to the default settings.

  2) (Optional) Click **Default** to restore all parameters to default settings.

- **Format Database**

1) (Optional) Click **Format** to delete all the data synchronized from the control client.

2) (Optional) Click **Format All** to delete all the data in the database.

- **Export**

  Click **Export** to export the device parameters to the computer.

- **Import Configuration File**

1) Click **Browse** to select the configuration file from the computer.

2) Click **Import** to import the selected configuration file to the device.

- **Upgrade**

1) Click **Browse** to select the upgrade file from the computer.

2) Click **Upgrade** to upgrade the firmware.

NOTE

- The device will reboot automatically after upgrading. Don't disconnect power to the device during the process.
- The parameters can only be imported or exported among the same model and the same version of the device.

### 6.2.4 Configuring Security

Step 1 Enter the Security Service interface.

Configuration > System > Security

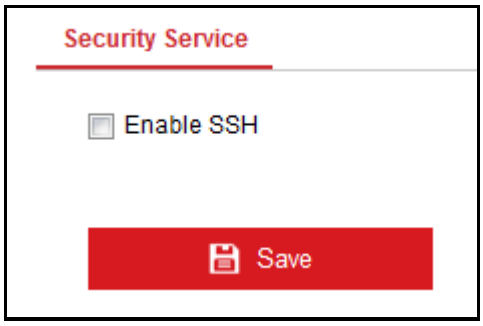



Figure 6-5 Security Configuration

Step 2 Check the checkbox of **Enable SSH** to enable the SSH function.

NOTE

Enabling SSH (Secure Shell) can encrypt and compress the data and reduce the transmission time.

### 6.2.5 Managing Camera

***Purpose***

You can view the information of analog cameras and add, modify or delete the IP cameras.

## Managing Analog Camera

Step 1 Enter the Analog Camera management interface.

Configuration > System > Camera Management > Analog Camera

Figure 6-6 Analog Camera

Step 2 View the information of the analog cameras.

## Managing IP Camera

Enter the IP Camera management interface.

Configuration > System > Camera Management > IP Camera

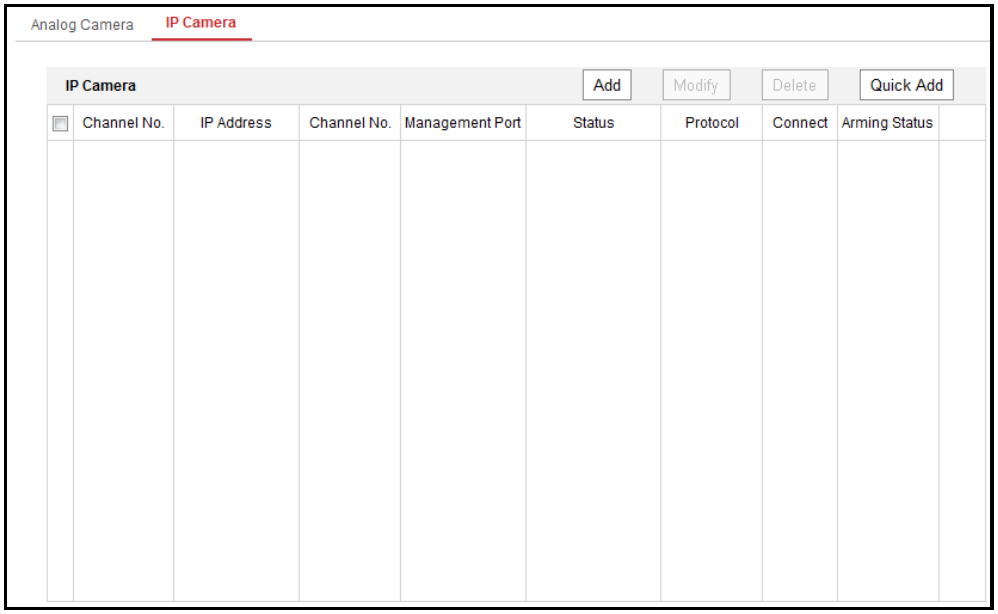



Figure 6-7 Camera Management

- **Adding IP Camera Manually**

1) Click **Add** to enter the Add IP Camera interface.

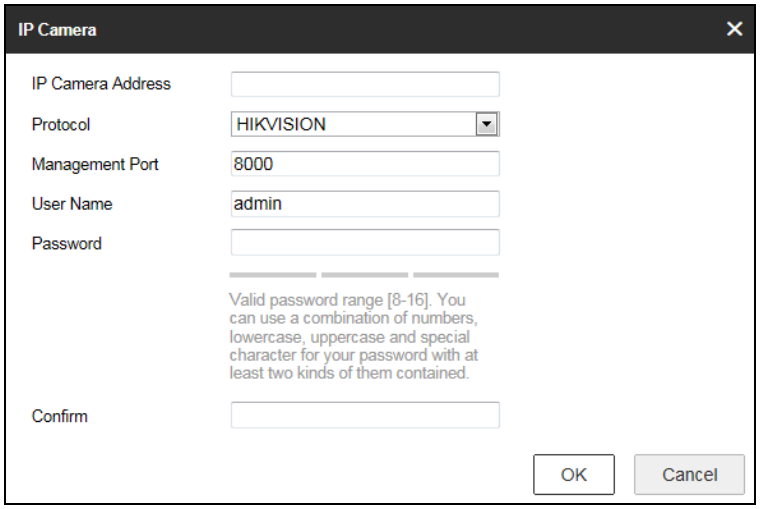



Figure 6-8 Add IP camera

2) Input the **IP Camera Address**, **Management Port**, **User Name** and **Password** of the IP camera.

3) Confirm the password.

4) Click **OK** to add it and the added camera will be displayed on the IP Camera interface.

- **Quick Add**

1) Click **Quick Add** to enter the Quick Add interface and it will show the online devices in the same network segment.

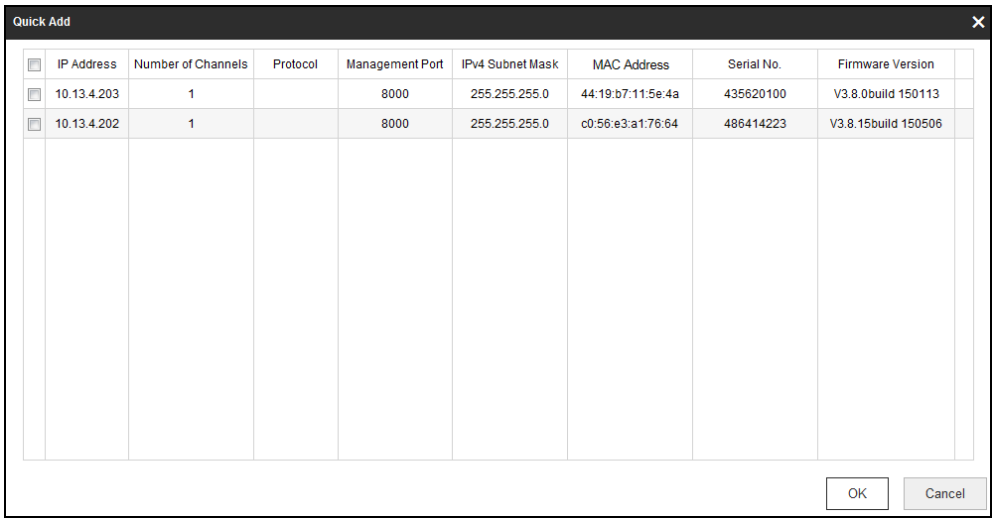



Figure 6-9 Quick Add

2) Check the checkbox of the camera for adding.

3) Click **OK** to add it.

- **Modifying the Added IP Camera**

1) On the IP Camera interface, check the checkbox of the camera for modifying.

2) Click **Modify** to enter the Modify IP Camera interface.

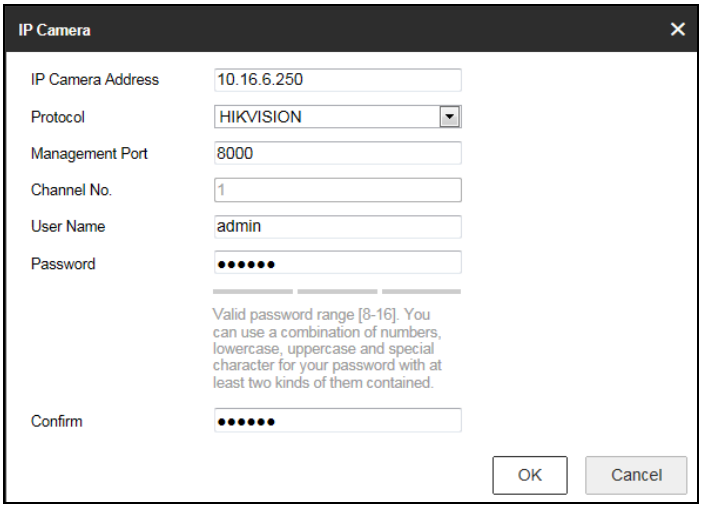



Figure 6-10 Modify IP Camera

3) Modify the parameters including the **IP Camera Address**, **Management Port**, **User Name** and **Password** of the IP camera.

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

- **Deleting the Added IP Camera**

1) On the IP Camera interface, check the checkbox of the camera for deleting.

2) Click **Delete** to delete it.

## 6.2.6 Managing User

***Purpose***

You can add, modify and delete users and set user permissions on the User Management interface.

NOTE

By default, there is only one user account ***admin*** and the level is Administrator. Up to 31 users can be created and it differs according to different models.

Enter the User Management interface.

Configuration > System > User Management

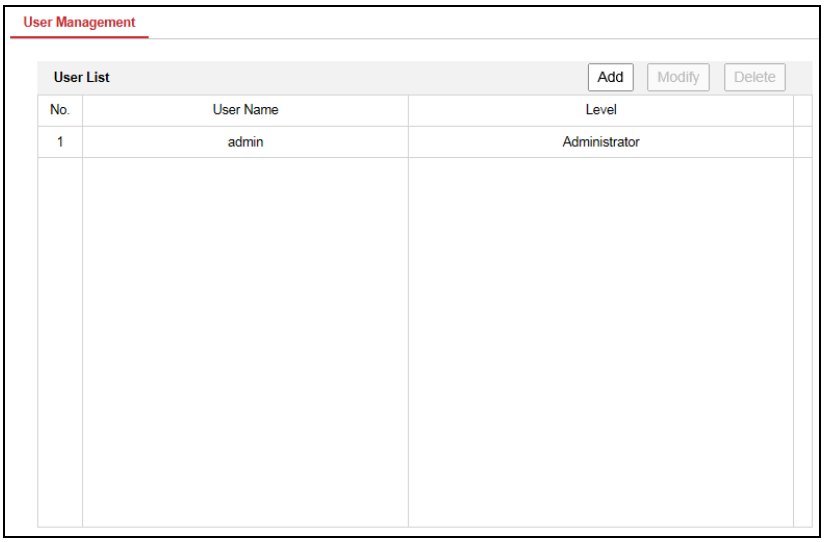



Figure 6-11 User Management

## Adding User

Step 1 Click **Add** to enter the Add User interface.

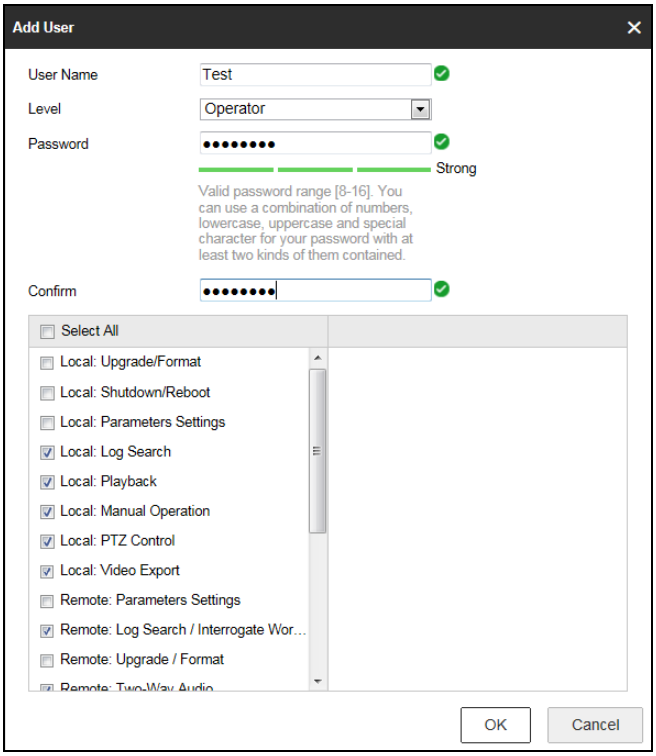



Figure 6-12 Add User

Step 2 Input the **User Name**, select the **Level** as Operator or User, input the **Password** and confirm it.

**WARNING**

**STRONG PASSWORD RECOMMENDED**–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.

Step 3 Check the checkbox(es) to select the user permission(s).

Step 4 Or you can check the checkbox of **Select All** to select all the permissions.

Step 5 Click **OK** to save the settings.

## Modifying User

Step 1 Select the user account for modifying and click **Modify**.

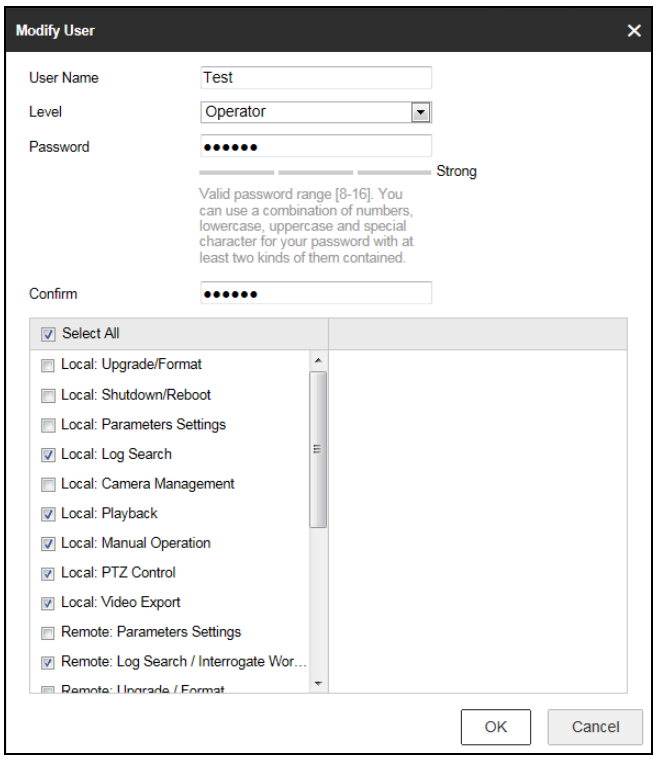



Figure 6-13 Modify User

Step 2 Modify the **User Name**, **Password**, **Level** and permissions.

**NOTE**

- For ***admin*** account, you can only modify the password.
- We highly recommend you to use strong password for security purpose.

Step 3 Click **OK** to save the settings.

### Deleting User

Step 1 Select the user account for deleting.

Step 2 Click **Delete** to delete it.

**NOTE**

You cannot delete the ***admin*** account.

## 6.3 Configuring Network

***Purpose***

You can configure TCP/IP, port and two-way audio for the network configuration.

### 6.3.1 Configuring TCP/IP

Step 1 Enter the TCP/IP interface.

Configuration > Network > Basic Settings > TCP/IP

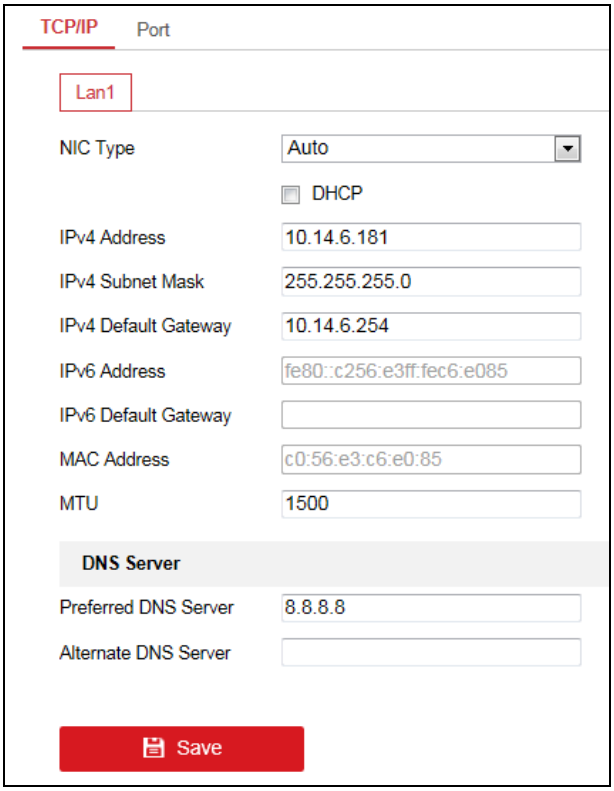



Figure 6-14 TCP/IP Configuration

Step 2 Configure the parameters, including the NIC Type, IPv4/IPv6 Address, IPv4/IPv6 Subnet Mask, IPv4/IPv6 Default Gateway, MAC Address and MTU.

NOTE

MTU refers to the maximum size of data packet in transmission.

Step 3 (Optional) If the DHCP server is available, you can check the checkbox of **DHCP** to automatically obtain an IP address and other network parameters.

Step 4 (Optional) If the DNS server settings are required for some applications (e.g., sending email), you should properly configure the **Preferred DNS Server** and **Alternate DNS server**.

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

### 6.3.2 Configuring Port

Step 1 Enter the Port configuration interface.

Configuration > Network > Basic Settings > Port

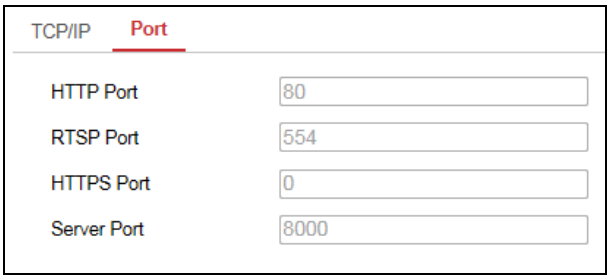



Figure 6-15 Port Configuration

Step 2 View the port parameters including **HTTP Port** (80 by default), **RTSP Port** (554 by default), **HTTPS Port** (0 by default) and **Server Port** (8000 by default).

NOTE

Do not modify the default port parameters freely. If there is port conflict and you have to modify the parameters, modify the following information.

- **HTTP Port** and **HTTPS Port**: Add the modified port to the address if you log in to the device via web browser. E.g., if you modify the HTTP Port to 81, input *http://192.168.1.64:81* in the address bar to log in to the device via web browser.
- **RTSP Port**: Ensure the modified RTSP Port is available.
- **Server Port**: If you modify the Server Port and want to log in to the device via client, you have to input the modified Server Port on the login interface.

### 6.3.3 Configuring Two-Way Audio

Step 1 Enter the Two-Way Audio interface.

Configuration > Network > Advanced Settings > Two-way Audio

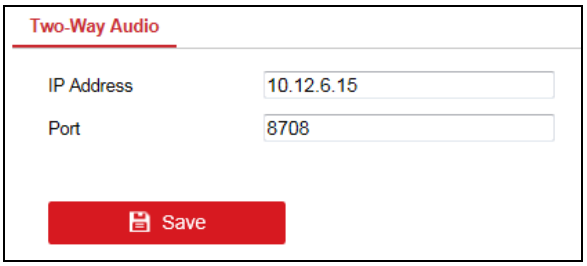



Figure 6-16 Two-Way Audio

Step 2 Input the **IP Address** and **Port**.

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

## 6.4 Configuring Image

### 6.4.1 Configuring Display Settings

Step 1 Enter the Display Settings interface.

Configuration > Image > Display Settings

Figure 6-17 Display Settings

Step 2 Select the **Channel No.** from the drop-down list.

Step 3 Configure the image display of the selected camera.

1) **Scene:** Select the scene type from the drop-down list according to the real scene. **Standard**, **Outdoor**, **Indoor** and **Dim Light** are selectable.

2) **Brightness:** Slide the bar to adjust brightness of the image. The value ranges from 0 to 255.

3) **Contrast:** Slide the bar to adjust contrast of the image. The value ranges from 0 to 255.

4) **Saturation:** Slide the bar to adjust color saturation of the image. The value ranges from 0 to 255.

**5) Hue:** Slide the bar to adjust hue of the image. It describes the degree to which a stimulus can be described as similar to or different from stimuli that are described as red, green, blue, and yellow, which ranges from 0 to 255.

6) **Sharpness:** Slide the bar to adjust sharpness of the image. It enhances the details of the image by sharpening the edges in the image. The value ranges from 0 to 255.

7) **Denoising:** Slide the bar to adjust denoising of the image. It reduces the noise in the digital image. The value ranges from 0 to 5.

Step 4 (Optional) Click **Default** to set the parameters to the defaullt value in each scene type.

## 6.4.2 Configuring OSD Settings

Step 1 Enter the OSD Settings interface.

Configuration > Image > OSD Settings

Figure 6-18 OSD Settings

Step 2 Select the **Channel No.** from the drop-down list.

Step 3 Configure the OSD settings of the selected camera.

1) Check the corresponding checkbox(es) to display name, date or week for OSD.

2) Edit the camera name in the text field of **Camera Name**.

3) Select the **Time Format** and **Date Format**.

4) (Optional) Drag the text frame in the live view window to adjust the OSD position.

5) (Optional) Edit the **Text Overlay**. Check the checkbox(es) in front of the text field(s) to enable the on-screen display and input the characters in the text field(s). You can drag the red text frame in the live view window to adjust the position.

**NOTE**

Up to 4 texts can be overlaid in live view.

Step 4 Select the Display Mode from the drop-down list. Transparent & Flashing, Transparent & Not Flashing, Not Transparent & Flashing, Not Transparent & Not Flashing are selectable.

Step 5 (Optional) Click **Copy to** to copy the settings to other cameras if required.

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

## 6.4.3 Configuring Privacy Mask

***Purpose***

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

Step 1 Enter the Privacy Mask configuration interface.

Configuration > Image > Privacy Mask

Figure 6-19 Privacy Mask

Step 2 Select the **Channel No.** from the drop-down list.

Step 3 Check the checkbox of **Enable Privacy Mask** to enable this function.

Step 4 Configure the privacy mask.

1) Click **Draw Area** to start drawing.
2) Hold and drag the mouse to draw the mask area in the live view window.
3) Click **Stop Drawing** to finish drawing.
4) (Optional) Click **Clear All** to clear all the configured privacy masks.

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

NOTE

- Privacy Mask function may not be supported by certain display modes. Refer to the actual interface for detailed information.
- Up to 4 privacy masks are configurable.

# 6.5 Configuring Event

## 6.5.1 Configuring Alarm Input

Step 1 Enter the Alarm Input interface.

Configuration > Event > Basic Event > Alarm Input

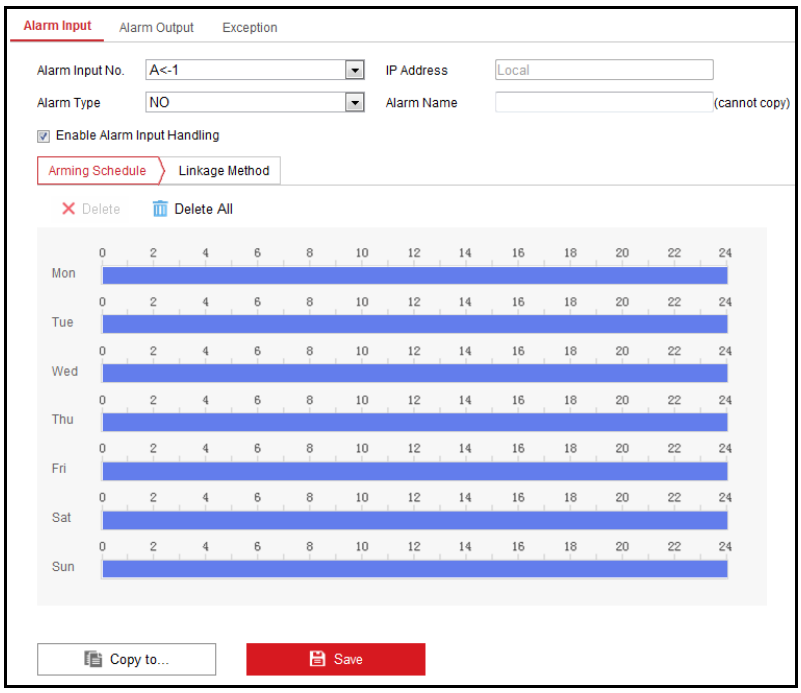



Figure 6-20 Alarm Input

Step 2 Select the **Alarm Input No.** and the **Alarm Type** from the drop-down list. The alarm type can be **NO** (Normally Open) and **NC** (Normally Closed).

Step 3 (Optional) Edit the **Alarm Name**.

Step 4 Check the checkbox of **Enable Alarm Input Handling** to enable the function.

Step 5 Configure the **Arming Schedule** and the **Linkage Method**.

- **Task 1: Configuring the Arming Schedule**

1) Click **Arming Schedule** to edit the arming schedule.

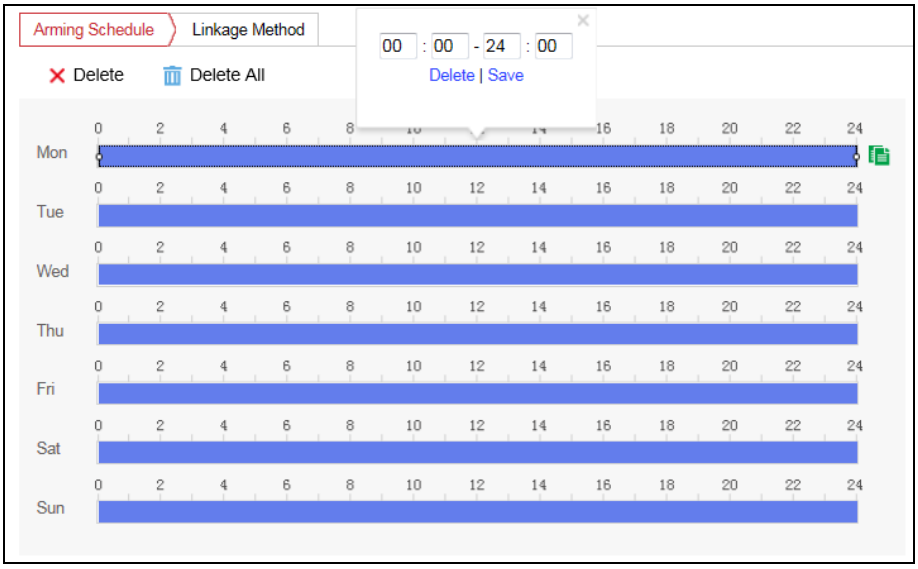



Figure 6-21 Arming Schedule Setting

2) Drag the time bar to set the time period.

You can also input the exact time period in 00 : 00 - 24 : 00 and save it.

3) (Optional) Click Delete to delete the current arming schedule, or click Delete All to delete all the arming schedule of the week.

4) (Optional) Click the icon on the end of a day to copy the current arming schedule to other days.

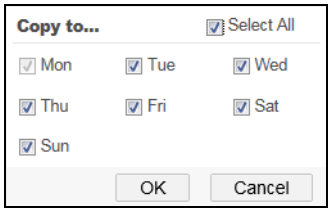



Figure 6-22 Copy Arming Schedule

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

NOTE

The time periods cannot overlap. Up to 8 periods can be configured for each day.

- **Task 2: Configuring the Linkage Method**

1) Click **Linkage Method** to enter the Linkage Method interface.

2) Configure the Normal Linkage, Triggered Alarm Output, Triggered Channel and PTZ Linking.

NOTE

The linkage methods vary with different models.

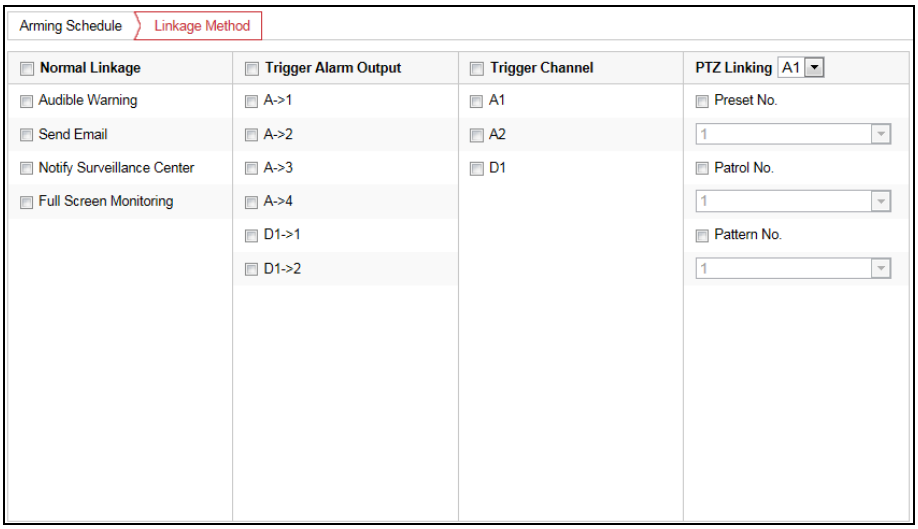



Figure 6-23 Linkage Method

Step 6 (Optional) Click Copy to... to copy the alarm input settings to other alarm inputs.

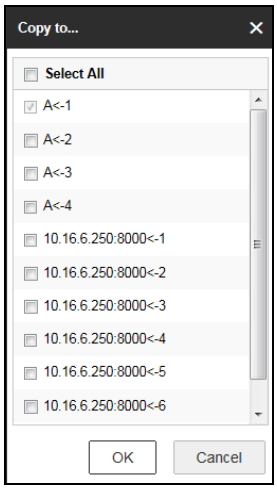



Figure 6-24 Copy to Other Alarm Inputs

Step 7 Click **Save** to save the settings.

NOTE

Alarm input settings vary with different models.

## 6.5.2 Configuring Alarm Output

Step 1 Enter the Alarm Output interface.

Configuration > Event > Basic Event > Alarm Output

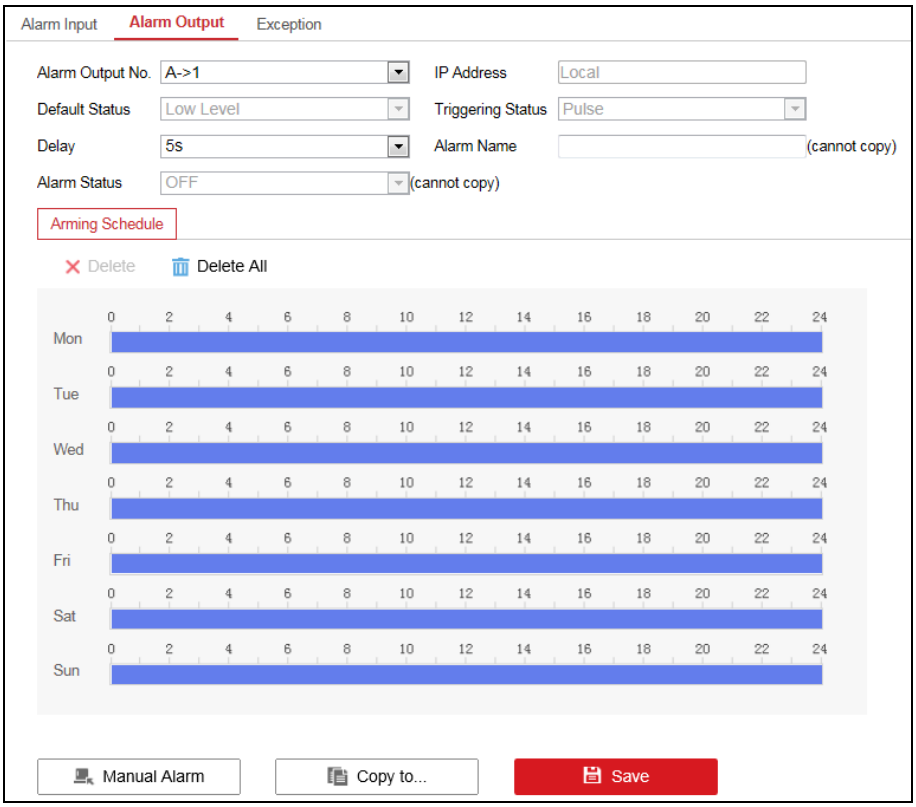



Figure 6-25 Alarm Output

Step 2 Select the **Alarm Output No.** from the drop-down list.

Step 3 (Optional) Edit the **Alarm Name**.

Step 4 Select the **Delay** time. 5 s, 10 s, 30 s, 1 min, 2 min, 5 min, 10 min and Manual are selectable.

NOTE

The delay time refers to the time duration that the alarm output remains in effect after alarm occurs.

Step 5 Configure the **Arming Schedule**. Refer to **Task 1: Configuring the Arming Schedule** in step 5 of Chapter 3.6.1 Configuring Alarm Input.

Step 6 (Optional) Click Copy to... to copy the alarm output settings to other alarm outputs.

Step 7 (Optional) Click **Manual Alarm** to trigger an alarm manually. Click **Clear Alarm** to cancel the alarm.

Step 8 Click **Save** to save the settings.

NOTE

Alarm output settings vary with different models.

### 6.5.3 Configuring Exceptions

Step 1 Enter the Exception interface.

Configuration > Event > Basic Event > Exception

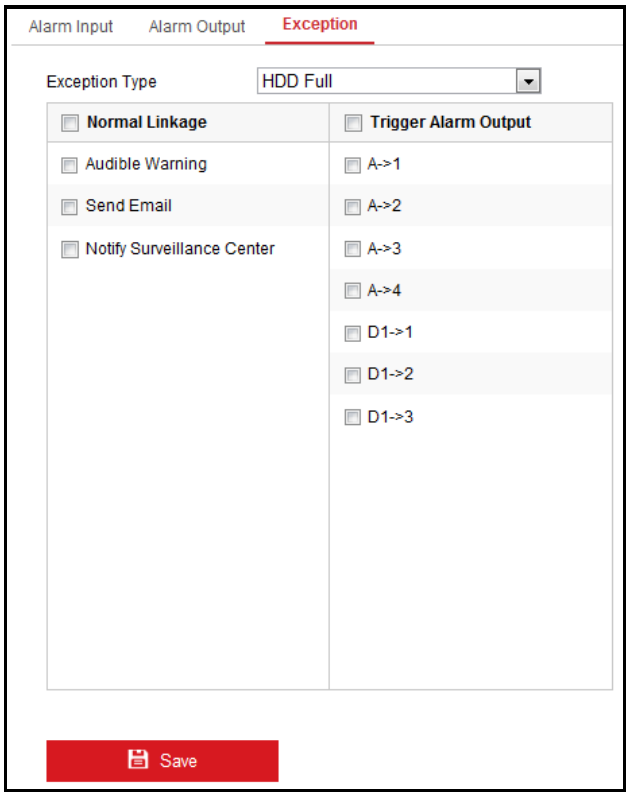



Figure 6-26 Exception Configuration

Step 2 Select the **Exception Type** from the drop-down list.

Step 3 Check the checkbox(es) to configure the actions taken for the exception alarm.

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

# Chapter 7 Configuring Entrance and Exit

## 7.1 Checking Status of Entrance & Exit

### 7.1.1 Checking Vehicle Status

Step 1 Enter the Vehicle Status interface.

Configuration > Entrance and Exit > Status > Vehicle Status

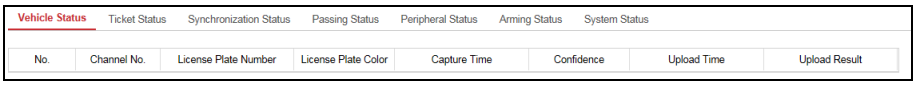



Figure 7-1 Vehicle Status

Step 2 Check the information including Channel No., License Plate Number, License Plate Color, Capture Time, Confidence, Upload Time and Upload Result.

### 7.1.2 Checking Ticket/Card Status

***Purpose***

For the Ticket Station, you can view the ticket status. For the Card Station, you can view the card status.

Step 1 Enter the Ticket/Card Status interface.

Configuration > Entrance and Exit > Status > Ticket/Card Status

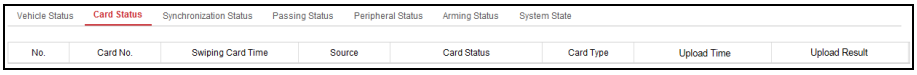



Figure 7-2 Card Status

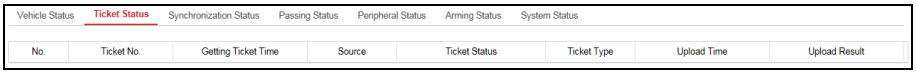



Figure 7-3 Ticket Status

Step 2 Check the information including Ticket/Card No., Getting Ticket Time/Swiping Card Time, Source, Ticket/Card Status, Ticket/Card Type, Upload Time and Upload Result.

### 7.1.3 Checking Synchronization Status

Step 1 Enter the Synchronization Status interface.

Configuration > Entrance and Exit > Status > Synchronization Status

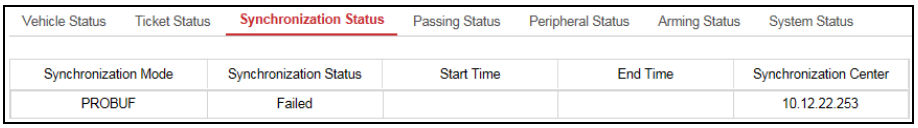



Figure 7-4 Synchronization Status

Step 2 Check the synchronization information including the Synchronization Mode, Synchronization Status, Start Time, End Time and Synchronization Center.

### 7.1.4 Checking Passing Status

Step 1 Enter the Passing Status interface.

Configuration > Entrance and Exit > Status > Passing Status

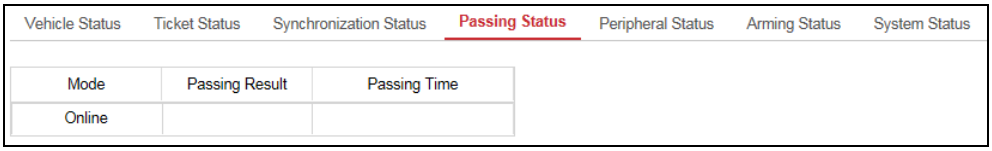



Figure 7-5 Passing Status

Step 2 Check the vehicle passing information including Mode, Passing Result and Passing Time.

### 7.1.5 Checking Peripheral Status

Step 1 Enter the Peripheral Status interface.

Configuration > Entrance and Exit > Status > Peripheral Status

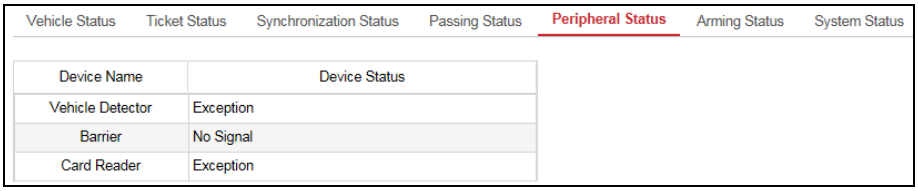



Figure 7-6 Peripheral Status

Step 2 Check the status of vehicle detector, barrier and card reader.

### 7.1.6 Checking Arming Status

Step 1 Enter the Arming Status interface.

Configuration > Entrance and Exit > Status > Arming Status

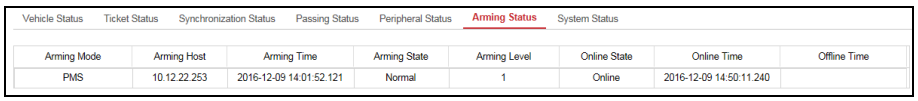



Figure 7-7 Arming Status

Step 2 Check the arming information including Arming Mode, Arming Host, Arming Time, Arming State, Arming Level, Online State, Online Time and Offline Time.

### 7.1.7 Checking System Status

Step 1 Enter the System Status interface.

Configuration > Entrance and Exit > Status > System Status

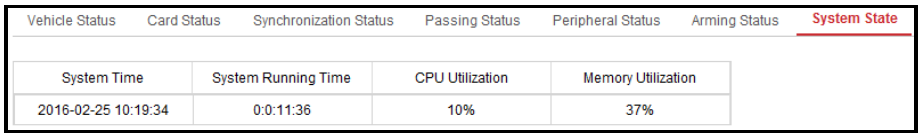



Figure 7-8 System Status

Step 2 Check the system information including System Time, System Running Time, CPU Utilization and Memory Utilization.

## 7.2 Configuring Entrance & Exit Settings

### 7.2.1 Configuring Basic Parameters

Step 1 Enter the Basic Parameters interface.

Configuration > Entrance and Exit > Settings > Basic Parameters

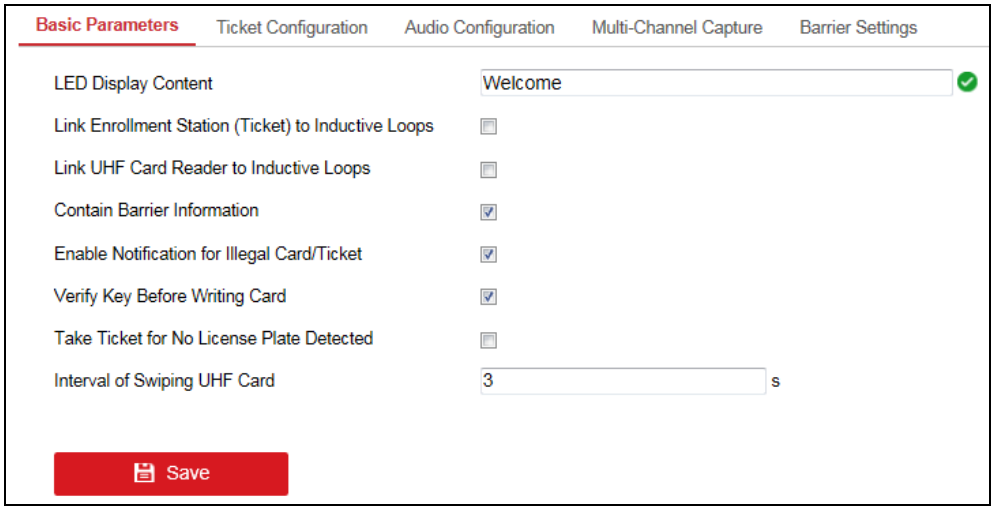



Figure 7-9 Basic Parameters

Step 2 Configure the following parameters according to your needs.

- Input the **LED Display Content** to show on the front panel of the device.
- Check the checkbox of **Link Enrollment Station (Ticket) to Inductive Loops**.

  When the inductive loops detect the passing vehicle and the signal is triggered, the ticket will be printed and there is only one ticket. If it is unchecked, the ticket can be printed and taken constantly.
- Check the checkbox of **Link UHF Card Reader to Inductive Loops**.

When the inductive loops detect the passing vehicle, the UHF card reader will read the card.

- Check the checkbox of **Contain Barrier Information** to get the barrier status information if signal lines are connected to the barrier.
- Check the checkbox of **Enable Notification for Illegal Card/Ticket**.

  If it is enabled, the station will let the vehicle pass only when the card information is legal. If illegal, the station will filter the card information and play the voice prompt of the card exception information. If it is disabled, the platform will judge whether the card information is legal or not.
- Check the checkbox of **Verify Key Before Writing Card**.

  The encrypted information of the internal card data will be verified and the card information will be updated before writing card.
- Check the checkbox of **Take Ticket for No License Plate Detected**.

  If there is no license plate detected when the vehicle passes, the station will play the voice prompt to remind the driver to take ticket.
- Input the **Interval of Swiping UHF Card** in the text field.

  The interval ranges from 1 to 300. The station will detect the UHF card every configured interval.

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

## 7.2.2 Configuring Ticket

Step 1 Enter the Ticket Configuration interface.

Configuration > Entrance and Exit > Settings > Ticket Configuration

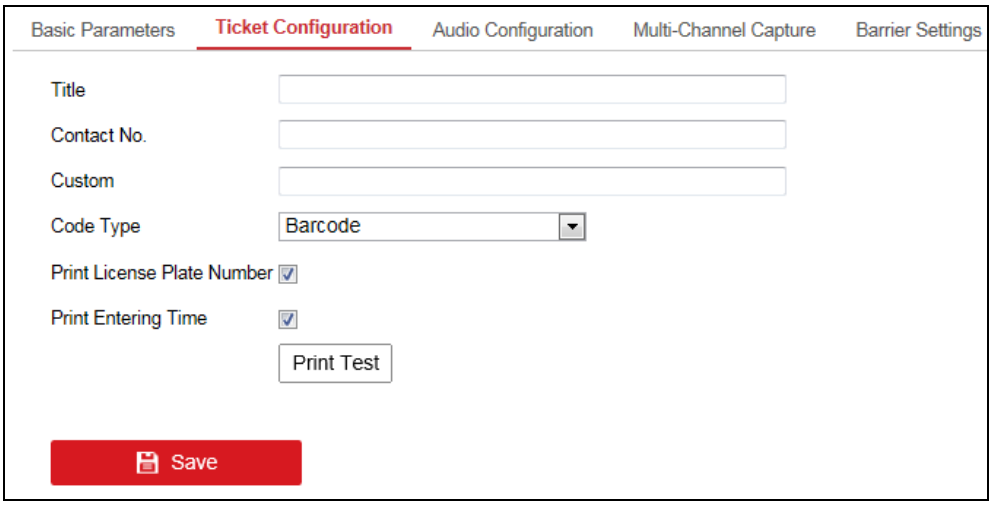



Figure 7-10 Ticket Configuration

Step 2 Input the **Tile**, **Contact No.** and **Custom** information to be printed on the ticket.

Step 3 Select the **Code Type**. Barcode and QR Code are selectable.

Step 4 (Optional) Check the checkbox of **Print License Plate Number** to print the license plate number on the ticket.

Step 5 (Optional) Check the checkbox of **Print Entering Time** to print the entering time of the vehicle on the ticket.

Step 6 (Optional) Click **Print Test** button to print the configured ticket to view the effect.

Step 7 Click **Save** to save the settings.

### 7.2.3 Configuring Audio

Step 1 Enter the Audio Configuration interface.

Configuration > Entrance and Exit > Settings > Audio Configuration

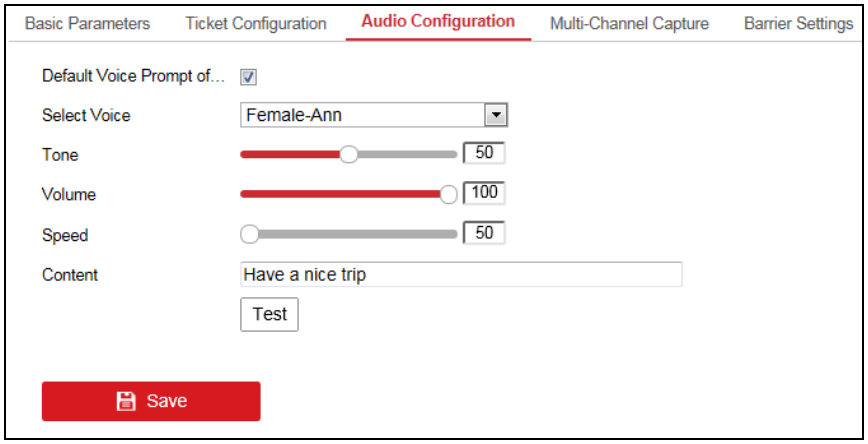



Figure 7-11 Audio Configuration

Step 2 Check the checkbox of **Default Voice Prompt of Entrance & Exit** to enable the voice prompt when the vehicle passes the entrance and exit.

Step 3 Select the voice from the **Select Voice** drop-down list. Female-Ann and Female-Jennifer are selectable.

Step 4 Slide the bar to adjust the **Tone**, **Volume** and **Speed**. The value ranges from 0 to 100.

Step 5 Input the **Content** of the voice prompt.

Step 6 (Optional) Click **Test** to test the settings.

Step 7 Click **Save** to save the settings.

### 7.2.4 Configuring Multi-Channel Capture

Step 1 Enter the Multi-Channel Capture interface.

Configuration > Entrance and Exit > Settings > Multi-Channel Capture

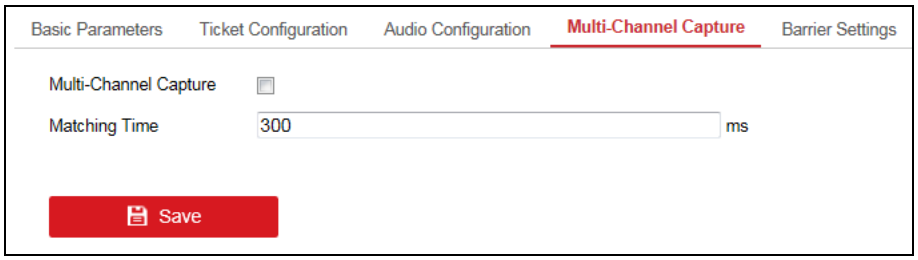



Figure 7-12 Multi-Channel Capture

Step 2 Check the checkbox of **Multi-Channel Capture** to enable the function.

The capture cameras of different angles at the entrance & exit station will capture images. After enabled, the entrance & exit station will select the captured image with the highest confidence to upload.

Step 3 Input the **Matching Time**.

The value ranges from 0 to 1000, and 300 is recommended.

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

## 7.2.5 Configuring Barrier Settings

Step 1 Enter the Barrier Settings interface.

Configuration > Entrance and Exit > Settings > Barrier Settings

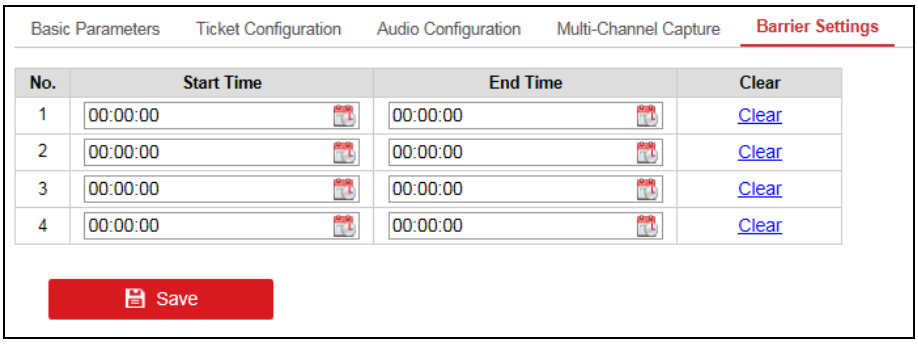



Figure 7-13 Barrier Settings

Step 2 Configure the time period and the barrier will remain open status from the configured start time to the end time.

**NOTE**

Up to 4 periods can be configured.

Step 3 (Optional) Click **Clear** to clear the settings.

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

# 7.3 Configuring Logs

Step 1 Enter the Log Configuration interface.

Configuration > Entrance and Exit > Log

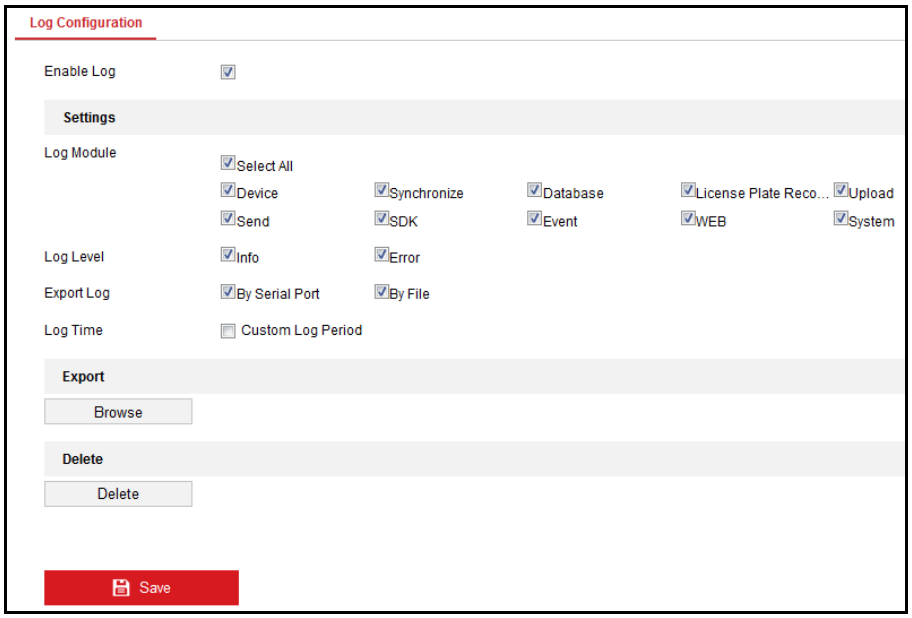



Figure 7-14 Log Configuration

Step 2 Check the checkbox of **Enable Log** to enable the function.

Step 3 Configure the **Log Module**, **Log Level**, **Export Log** and **Log Time**.

Step 4 Click **Browser** under Export to select the directory to save the log file.

Step 5 (Optional) Click **Delete** to delete the log file.

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

**NOTE**

Log Module is available for inspection by professional staff.

# Chapter 8 Application of Other Models

The DS-TME401-TRL entrance station and DS-TME402-TRL exit station are 1-layer card stations supporting automatic card dispatch at entrance and automatic card collection at exit. The web operations are similar to that of DS-TME401-TPL and DS-TME402-TPL ticket station. The differences are shown as below.

## 8.1 Checking Card Status

Step 1 Enter the Card Status interface.

Configuration > Entrance and Exit > Status > Card Status

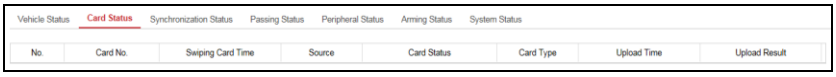



Figure 8-1 Card Status

Step 2 Check the information including Card No., Swiping Card Time, Source, Card Status, Card Type, Upload Time and Upload Result.

## 8.2 Configuring Offline Settings

***Purpose***

When the station is disconnected with the platform, you can enable the offline mode to select the card mode, vehicle passing mode, automatic vehicle passing rule, etc.

Step 1 Enter the Offline Configuration interface.

Configuration > Entrance and Exit > Settings > Offline Configuration

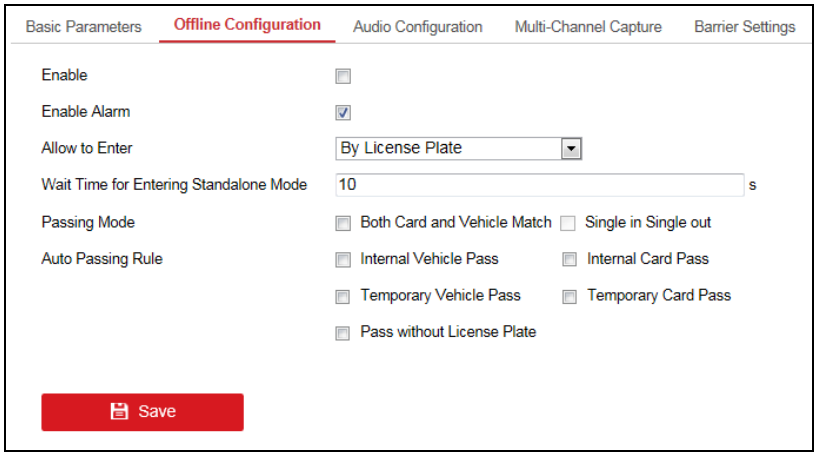



Figure 8-2 Offline Configuration

Step 2 Check the checkbox of **Enable** to enable the offline mode.

Step 3 Check the checkbox of **Enable Alarm** to enable alarm.

Step 4 Select the entering method. Allow to enter by license plate or by card.

Step 5 Input the **Wait Time for Entering Standalone Mode**.

Step 6 Select the **Passing Mode** and the **Auto Passing Rule**.

Step 7 Click **Save** to save the settings.

0200041061223

First Choice for Security Professionals

www.hikvision.com