Entrance/Exit Station

User Manual

About this Manual

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

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

Trademarks Acknowledgement

- 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 MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED “AS IS” AND “WITH ALL FAULTS AND ERRORS”. HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF 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 INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU

ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE 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 Instruction

Laws and Regulations

Use of the product must be in strict compliance with the local laws and regulations. Please shut down the device in prohibited area.

Power Supply

- Use of the product must be in strict compliance with the local electrical safety regulations.
- Use the power adapter provided by qualified manufacturer. Refer to the product specification for detailed power requirements.
- It is recommended to provide independent power adapter for each device as adapter overload may cause over-heating or a fire hazard.
- Make sure that the power has been disconnected before you wire, install, or disassemble the device.
- DO NOT directly touch exposed contacts and components once the device is powered up to avoid electric shock.
- DO NOT use damaged power supply devices (e.g., cable, power adapter, etc.) to avoid electric shock, fire hazard, and explosion.
- DO NOT directly cut the power supply to shut down the device. Please shut down the device normally and then unplug the power cord to avoid data loss.
- DO NOT block the power supply equipment to plug and unplug conveniently.
- Make sure the power supply has been disconnected if the power adapter is idle.
- Make sure the device is connected to the ground firmly.

Transportation, Use, and Storage

- To avoid heat accumulation, good ventilation is required for a proper operating environment.
- Store the device in dry, well-ventilated, corrosive-gas-free, no direct sunlight, and no heating source environment.
- Avoid fire, water, and explosive environment when using the device.
- Avoid lightning strike for device installation. Install a lightning arrester if necessary.
- Keep the device away from magnetic interference.
- Avoid device installation on vibratory surface or places, and avoid equipment installation on vibratory surface or places subject to shock (ignorance may cause device damage).
- DO NOT touch the heat dissipation component to avoid burns.
- DO NOT expose the device to extremely hot, cold, or humidity environments. For temperature and humidity requirements, see device specification.

Maintenance

- If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.
- If the device is abnormal, contact the store you purchased it or the nearest service center. DO NOT disassemble or modify the device in any way (For the problems caused by unauthorized modification or maintenance, the company shall not take any responsibility).
- Keep all wrappers after unpacking them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage to the device and the company shall not take any responsibility.

Network

- Please enforce the protection for the personal information and the data security as the device may be confronted with the network security problems when it is connected to the Internet. Please contact us when the device might exist network security risks.
- Please understand that you have the responsibility to configure all the passwords and other security settings about the device, and keep your user name and password.

Data

DO NOT disconnect the power during formatting, uploading, and downloading. Or files may be damaged.

Table of Contents

Chapter 1 Introduction

1.1 Product Overview

Entrance/Exit Station (hereinafter referred to as station) is used for data collection and management of entrance, exit, and parking lot. Through interaction with the software, the station can control the entrance/exit, manage the parking lot effectively, and charge parking fee.

Peripheral devices such as capture camera, barrier gate, remote card reader, alarm device, etc. can be connected to the station to realize vehicle passing, charging, and management.

The station must be used with the matched control terminal software or platform.

1.2 Key Feature

- Strong processing performance to realize vehicle management of large traffic flow easily.
- Supporting QR code payment, satisfying the vehicle to enter and exit normally in unattended station scene.
- Embedded Linux operating system and modular design to guarantee long-time and stable operation of the system.
- Diversified charging standards configuration to distinguish charging standards for different vehicles.
- Flexible vehicle entering and exiting management strategy. Multiple release rules configurable to satisfy the requirements of different scenes.
- Supporting card reading and writing. Offline charging is possible even when the network is disconnected.
- Voice prompt to notice the charging fees, reducing the manual labor.
- Integrated with vehicle detection module, detecting and controlling vehicle after connecting loops.
- Abundant peripheral interfaces to connect multiple peripheral devices, satisfying various scenes.
- Backup and restoration to avoid repeated configuration for many times.

Chapter 2 Activation and Login

2.1 Activate Device

You need to activate the station and set the password for first-time login. You can activate the station via multiple methods. Here we take example of activation via SADP and web browser.

NOTE

For activation via client software, refer to the software user manual for details.

2.1.1 Default Information

- IP Address: 192.168.1.64
- User name: admin

2.1.2 Activate via SADP

You can activate the station via SADP software.

NOTE

Ensure your station and computer are in the same network segment.

Step 1 Run the SADP software to search the online devices.

Step 2 Check the device status from the device list, and select an inactive device.

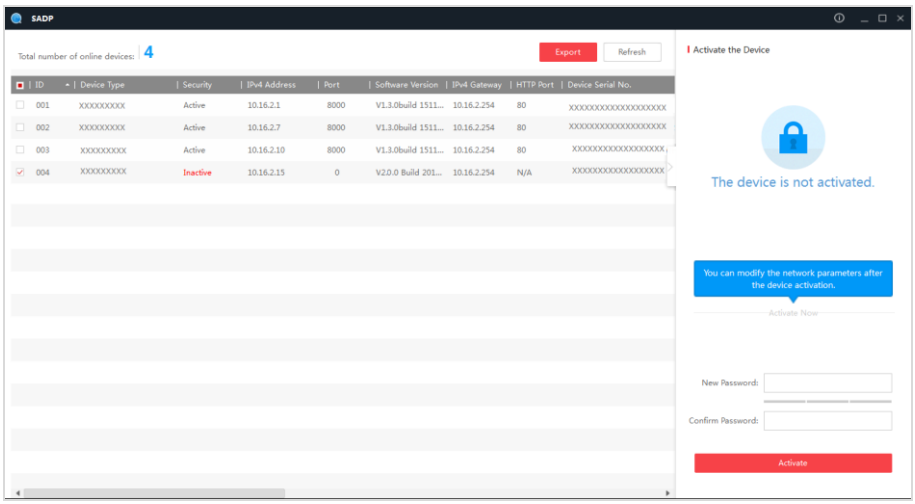


Figure 2-1 SADP Interface

Step 3 Create a password and input the password in the password field, 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 4 Click **Activate** to activate the device.

Step 5 Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking **Enable DHCP**.

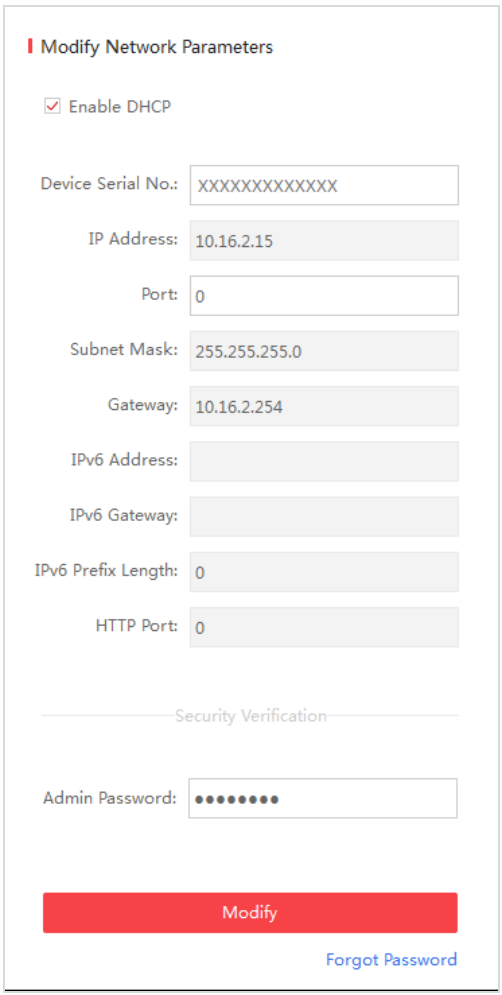


Figure 2-2 Modify IP Address

Step 6 Input the password and click **Modify** to activate your IP address modification.

2.1.3 Activate via Web Browser

You can activate the station via web browser.

NOTE

Ensure your station and computer are in the same network segment.

Step 1 Enter the default IP address of the station in the address bar of the web browser and press the **Enter** key to enter the activation interface.

Step 2 Enter a new password and confirm it.

Step 3 Click **OK** to activate the station.

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.

2.2 Log in

You can log in to the station via web browser for further operations such as live view and local configuration.

Step 1 Open the web browser.

Step 2 Enter the IP address of the station in the address bar, and press the **Enter** key to enter the login interface.

Step 3 Enter **User Name** and **Password**.

Step 4 Click **Login**.

Figure 2-3 Login Interface

NOTE

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

Step 5 Install the plug-in before other operations. Please follow the installation prompts to install the plug-in.

NOTE

Close the web browser to install the plug-in. Please reopen the web browser and log in again after installing the plug-in.

2.3 Log out

After login, click **Logout** to log out of the station.

Chapter 3 Live View

3.1 Live View Operation

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

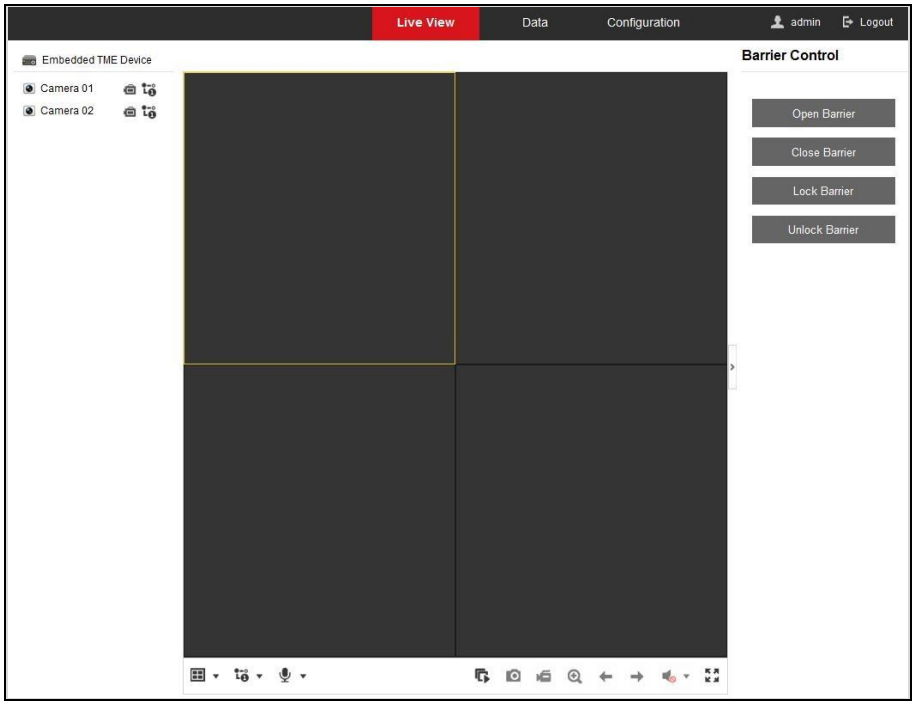
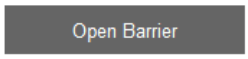
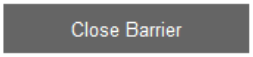
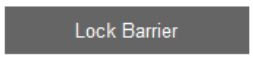
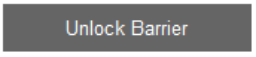


Figure 3-1 Live View

On the Live View interface, see Table 3-1 for the functions of the icons.

Table 3-1 Live View Icon Description

Icon	Description
/	Start/Stop live view of the selected camera.
	Select the window division mode. 1, 4, 9 and 16 window division modes are selectable.
	Main Stream and Sub-Stream are selectable.
	Start two-way audio.
/	Start/Stop live view of all the cameras.

	Capture picture in live view.
	Start/Stop recording of all the cameras.
	Enable/Disable e-PTZ function.
	Go for live view of the previous page.
	Go for live view of the next page.
	Turn on/off the audio in live view.
	Slide the bar to adjust the volume.
	Display the live view of the selected camera in full screen. Press **ESC** to exit.
	Open barrier.
	Close barrier.
	Lock barrier.
	Unlock barrier.

NOTE

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

3.2 Configure Local Live View Parameters

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

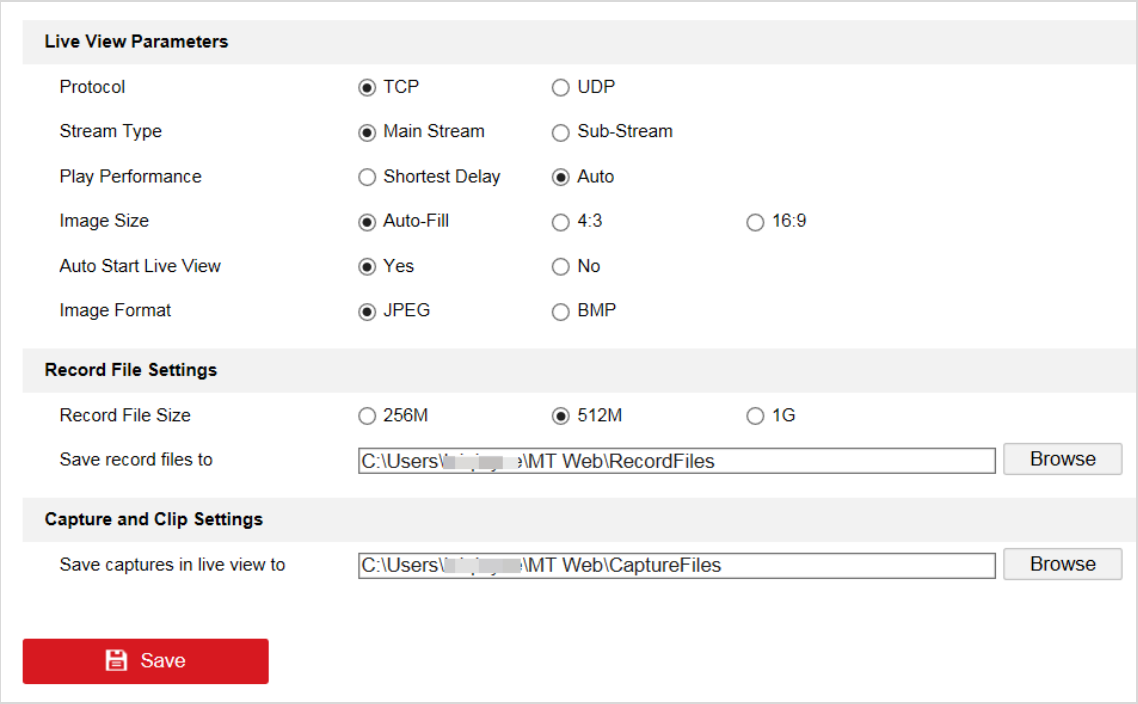


Figure 3-2 Local Configuration

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

- **Live View Parameters**
  - **Protocol**: TCP is selected by default. Select UDP when high requirement of video stream is not needed and the network is not stable.
  - **Stream Type**: Select main stream for HD live view. Select sub-stream for SD live view.
  - **Play Performance**: Auto is selected by default. In auto mode, the play performance will adjust automatically according to the network conditions. It takes both real time and fluency into consideration. While shortest delay mode has good real-time performance but it may influence the fluency.
  - **Image Size**: Select the image size according to the actual requirements.
  - **Auto Start Live View**: If you select Yes, live view will automatically start after the station is accessed.
  - **Image Format**: Select the captured picture format.
- **Record File Settings**
  - **Record File Size**: Select the size of record file saved locally.
  - **Save record files to**: Click **Browse** to set the local path to save the record files.
- **Capture and Clip Settings**

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

Chapter 4 Data Search

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

4.1 Search Card

You can search card according to the card type and card status, or you can enter the card No. to search the specific card.

Step 1 Click **Card Search**.

Step 2 Set search conditions such as **Card Type**, **Card Status**, and **Card No.**

Step 3 Click **Search** to search the card. The search results will be displayed on the right. You can view the information.

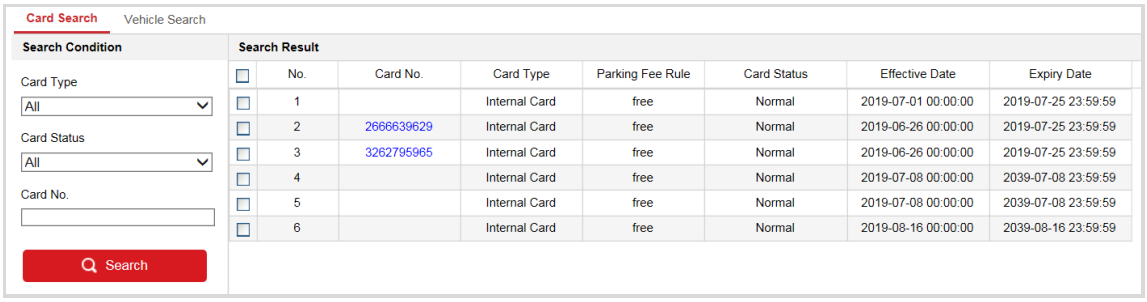


Figure 4-1 Search Card

4.2 Search Vehicle

You can search vehicle according to the vehicle type and license plate color, or you can enter the license plate number to search the specific vehicle.

Step 1 Click **Vehicle Search**.

Step 2 Set search conditions such as **Vehicle Type**, **License Plate Color**, and **License Plate Number**.

Step 3 Click **Search** to search the vehicle. The search results will be displayed on the right. You can view the information.

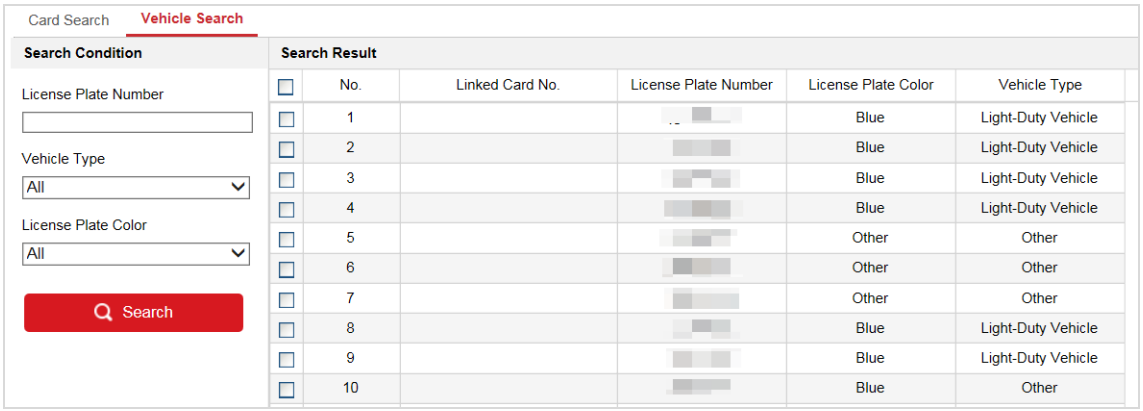


Figure 4-2 Search Vehicle

Chapter 5 Basic Operation

5.1 Manage IP Camera

5.1.1 Add IP Camera Manually

Connect capture unit to the station manually if the passwords of them are different.

Before you start

- The capture unit can communicate normally with the station.
- The capture unit has been activated.

Step 1 Go to **Configuration > System > Camera Management > IP Camera**.

Step 2 Click **Add**.

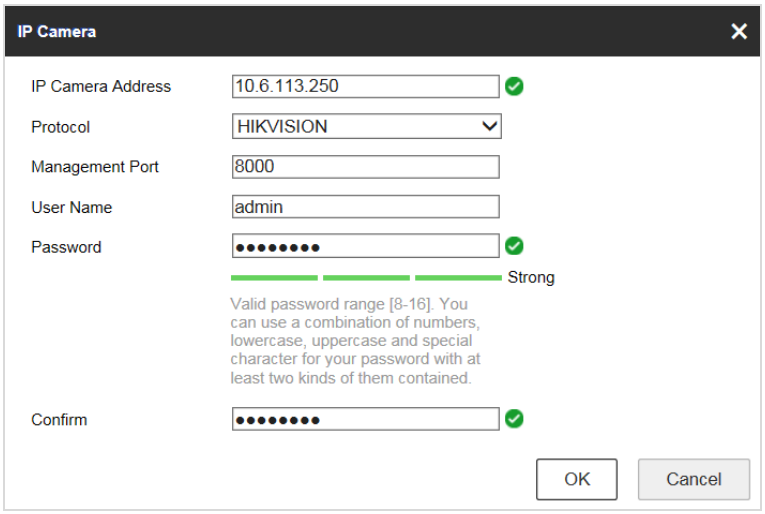


Figure 5-1 Add IP camera

Step 3 Enter **IP Camera Address**, **Management Port**, **User Name**, and **Password** of the IP camera.

Step 4 Confirm the password.

Step 5 Click **OK** to add it.

5.1.2 Add IP Camera Quickly

You can search the IP camera in the same network segment with the station and add it quickly if the passwords of them are the same.

Step 1 Go to **Configuration > System > Camera Management > IP Camera**.

Step 2 Click **Quick Add** and the interface will show the online IP cameras in the same network segment with the station.

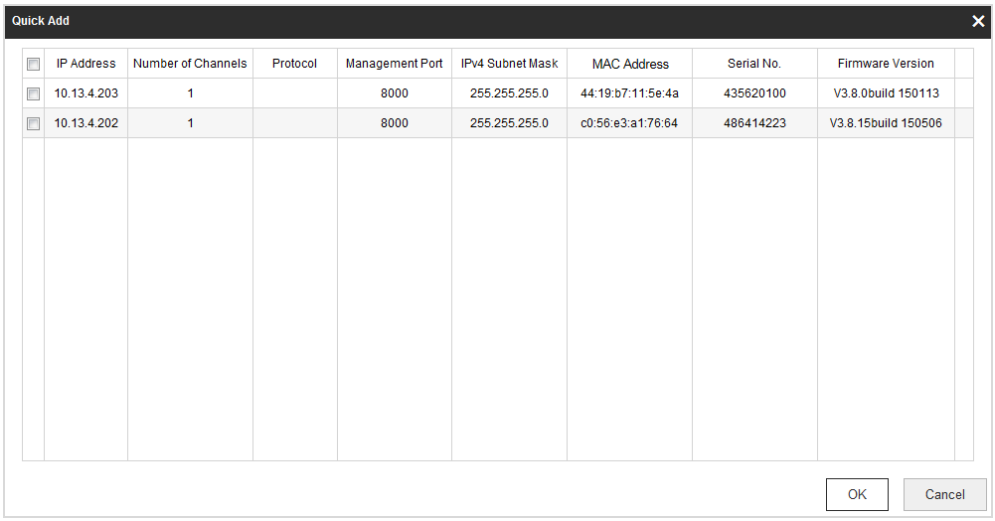


Figure 5-2 Quick Add

Step 3 Check the IP camera.

Step 4 Click **OK** to add it.

5.1.3 Edit IP Camera

You can edit the added IP camera parameters.

Step 1 Go to **Configuration > System > Camera Management > IP Camera**.

Step 2 Check the camera to edit.

Step 3 Click **Modify**.

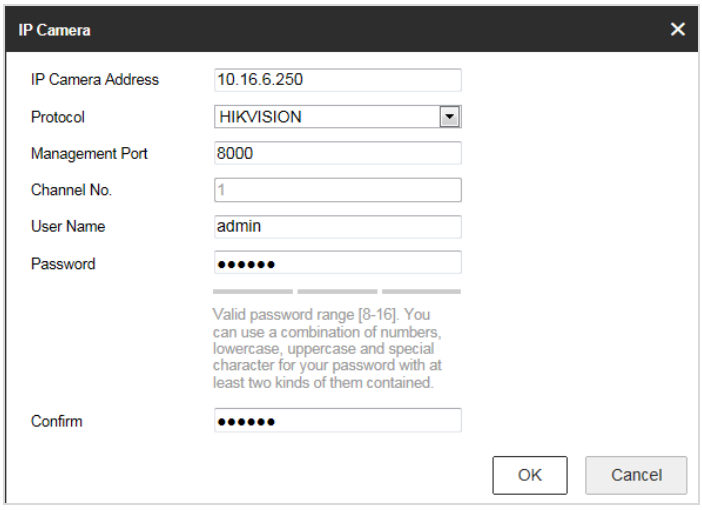


Figure 5-3 Modify IP Camera

Step 4 Edit the parameters of the IP camera.

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

5.1.4 Delete IP Camera

You can delete the added IP camera.

Step 1 Go to **Configuration > System > Camera Management > IP Camera**.

Step 2 Check the camera to delete.

Step 3 Click **Delete** to delete it.

5.2 Configure Entrance & Exit Parameters

5.2.1 Configure Basic Parameters

You can configure the basic parameters for entrance and exit.

Step 1 Go to **Configuration > Entrance and Exit > Settings > Basic Parameters**.

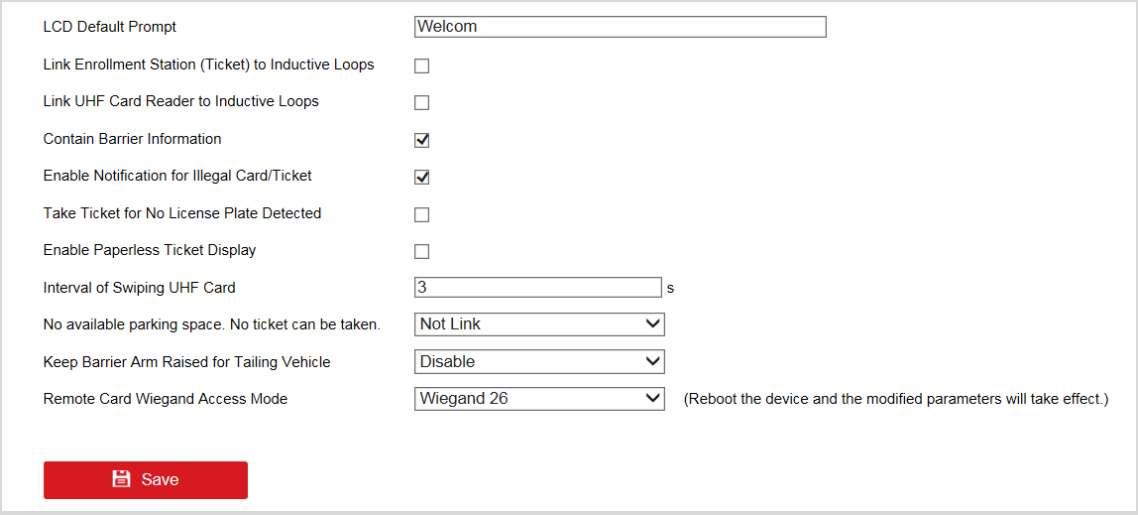


Figure 5-4 Basic Parameters

Step 2 Configure the following parameters according to your needs.

- **LCD Default Prompt**: Enter the information to show on LCD of the station.
- **Link Enrollment Station (Ticket) to Inductive Loops**: If it is checked, when the inductive loops detect the passing vehicle and the signal is triggered, the ticket will be printed. If it is unchecked, the ticket can be printed and taken at any time.
- **Link UHF Card Reader to Inductive Loops**: If it is checked, when the inductive loops detect the passing vehicle, the UHF card reader will read the card. If it is unchecked, the card reader will read card continuously.
- **Contain Barrier Information**: Check it to get the barrier status information if signal lines are connected to the barrier.

- **Enable Notification for Illegal Card/Ticket**: If it is checked, 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 unchecked, the platform will judge whether the card information is legal or not.
- **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.
- **Interval of Swiping UHF Card**: The interval ranges from 1 to 300. The station will detect the UHF card every configured interval.
- **No available parking space. No ticket can be taken.**: If you select **Link**, when there is no available parking space, the vehicle cannot enter.
- **Keep Barrier Arm Raised for Tailing Vehicle**: If you enable the function, the barrier arm will not fall when vehicles enter one by one continuously.
- **Remote Card Wiegand Access Mode**: Select the Wiegand protocol type for remote card access according to the actual conditions.

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

5.2.2 Configure Ticket

You can configure the content on the ticket.

Step 1 Go to **Configuration > Entrance and Exit > Settings > Ticket Configuration**.

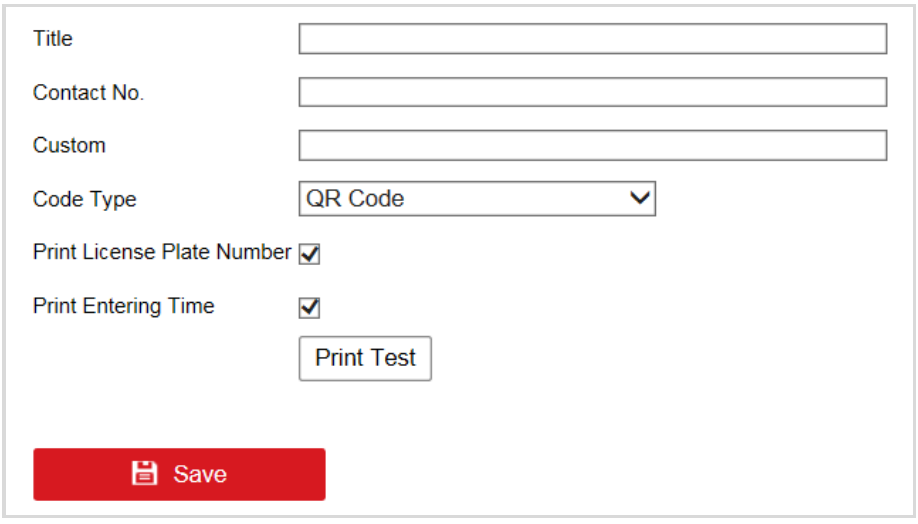


Figure 5-5 Ticket Configuration

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

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

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

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

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

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

5.2.3 Configure Audio

You can configure the voice prompt.

Step 1 Go to **Configuration > Entrance and Exit > Settings > Audio Configuration**.

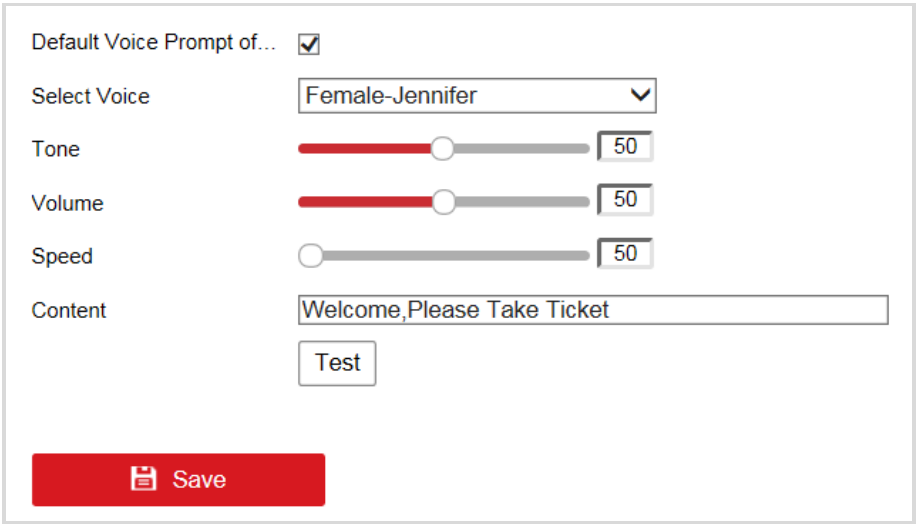


Figure 5-6 Audio Configuration

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

Step 3 Select the voice.

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

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

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

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

5.2.4 Configure Media

You can configure the video to be played on the LCD.

Step 1 Go to **Configuration > Entrance and Exit > Settings > Media Configuration**.

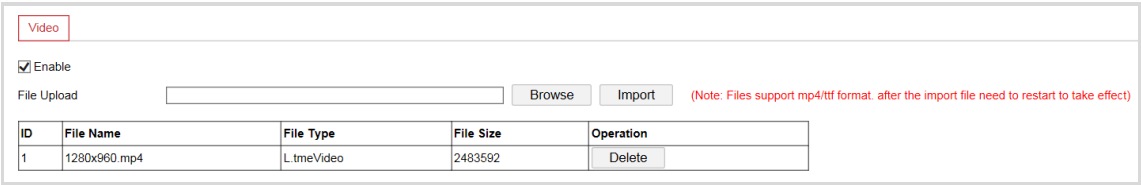


Figure 5-7 Media Configuration

Step 2 Check **Enable**.

Step 3 Click **Browse** to select the video file.

Step 4 Click **Import** to import it.

NOTE

The video file should be in the format of MP4, and the size should be less than 100 M.

Result:

LCD will play the imported video automatically.

5.2.5 Configure Multi-Channel Capture

If multiple capture units are installed for one lane, you can enable multi-channel capture. The clearest captured picture will be uploaded to the platform automatically according to the effects of different pictures captured by the capture units.

Step 1 Go to **Configuration > Entrance and Exit > Settings > Multi-Channel Capture**.

Figure 5-8 Multi-Channel Capture

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

Step 3 Enter **Matching Time**.

NOTE

Matching time is the longest matching waiting time for multi-channel capture. The value ranges from 0 to 1000, and 300 is recommended.

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

5.2.6 Configure Barrier

If barrier gate is connected to the station, the barrier gate can be controlled via the station.

Step 1 Go to **Configuration > Entrance and Exit > Settings > Barrier Settings**.

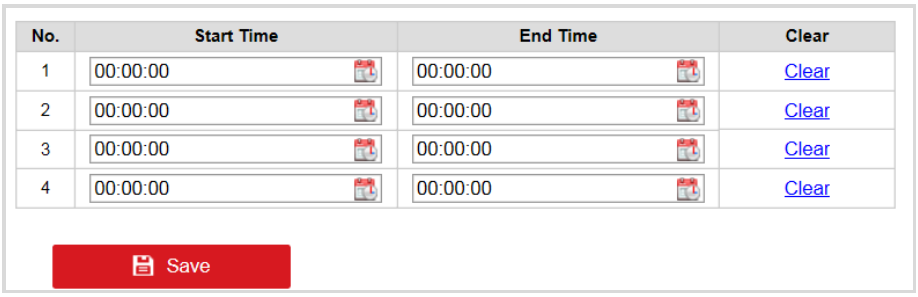


Figure 5-9 Barrier Settings

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.

5.2.7 Configure Brightness

You can configure the brightness of LCD.

Step 1 Go to **Configuration > Entrance and Exit > Settings > Brightness Settings**.

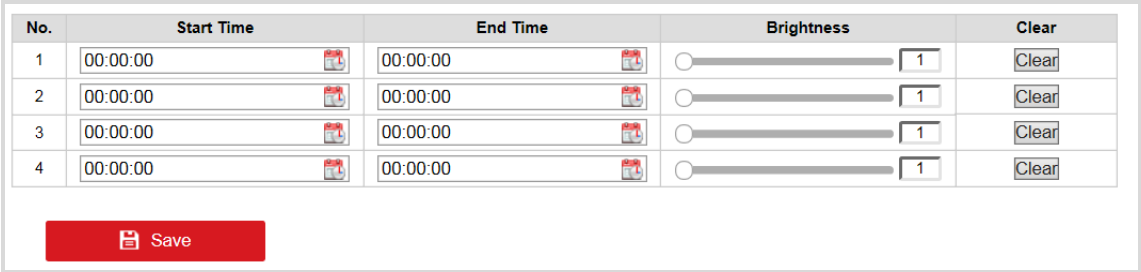


Figure 5-10 Brightness Settings

Step 2 Set **Start Time** and **End Time**.

Step 3 Slide the bar to set the brightness of LCD during the time period.

Step 4 (Optional) Click **Clear** to clear the settings.

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

5.2.8 View Entrance & Exit Status

Go to **Configuration > Entrance and Exit > Status** to view vehicle status, card status, synchronization status, etc.

NOTE

After the station is added to dedicated software, the functions such as license plate recognition of capture unit, vehicle passing of barrier gate, fee charging, etc. can be realized. Refer to the software user manual for details.

5.3 Configure Two-Way Audio

5.3.1 Two-Way Audio with Computer

On the live view interface, you can start two-way audio between the controller and the station.

Step 1 On the live view interface, select the image to start two-way audio.

Step 2 Click  to start two-way audio.

5.3.2 Two-Way Audio with Software

The controller can connect to dedicated software to realize two-way audio with the software.

Step 1 Go to **Configuration > Network > Advanced Settings > Two-way Audio**.

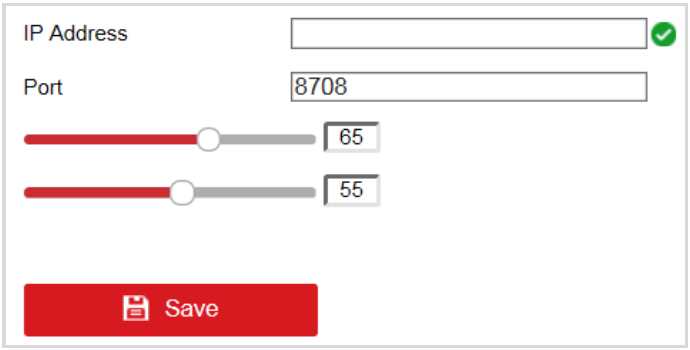


Figure 5-11 Two-Way Audio

Step 2 Enter **IP Address** of the device installed the software, and keep the default **Port**.

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

Step 4 Press Help button on the controller front panel to start two-way audio.

Chapter 6 Image Configuration

6.1 Configure Display

You can configure the image parameters of the camera.

Step 1 Go to **Configuration > Image > Display Settings**.

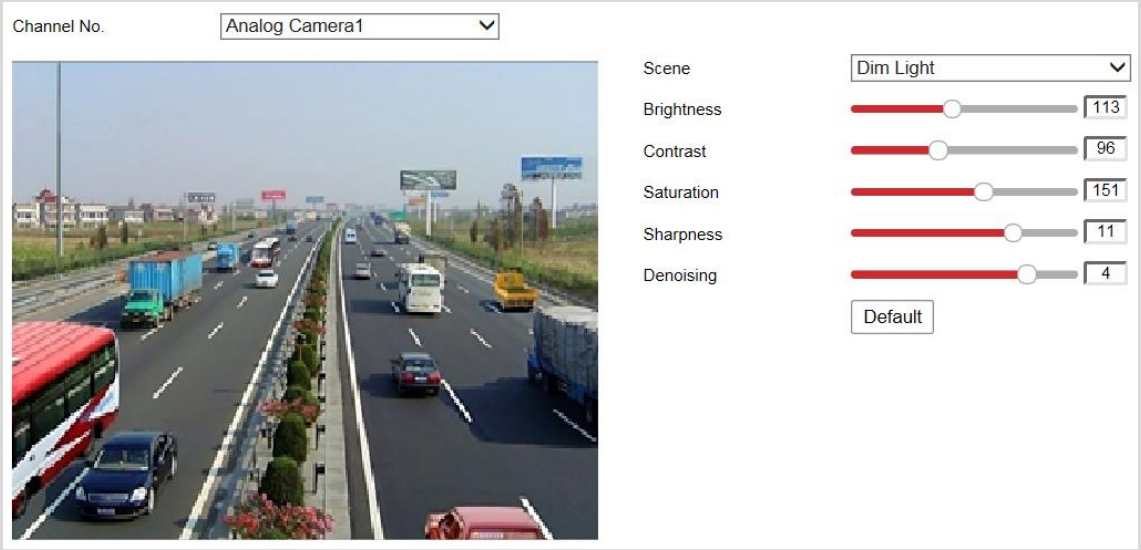


Figure 6-1 Display Settings

Step 2 Select **Channel No.**

Step 3 Configure the image display of the selected camera.

- **Scene:** Select the scene type from the drop-down list according to the real scene.
- **Brightness:** Slide the bar to adjust brightness of the image. The value ranges from 0 to 255.
- **Contrast:** Slide the bar to adjust contrast of the image. The value ranges from 0 to 255.
- **Saturation:** Slide the bar to adjust color saturation of the image. The value ranges from 0 to 255.
- **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.
- **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.

6.2 Configure OSD

You can configure the on-screen display of the live view image.

Step 1 Go to **Configuration > Image > OSD Settings**.

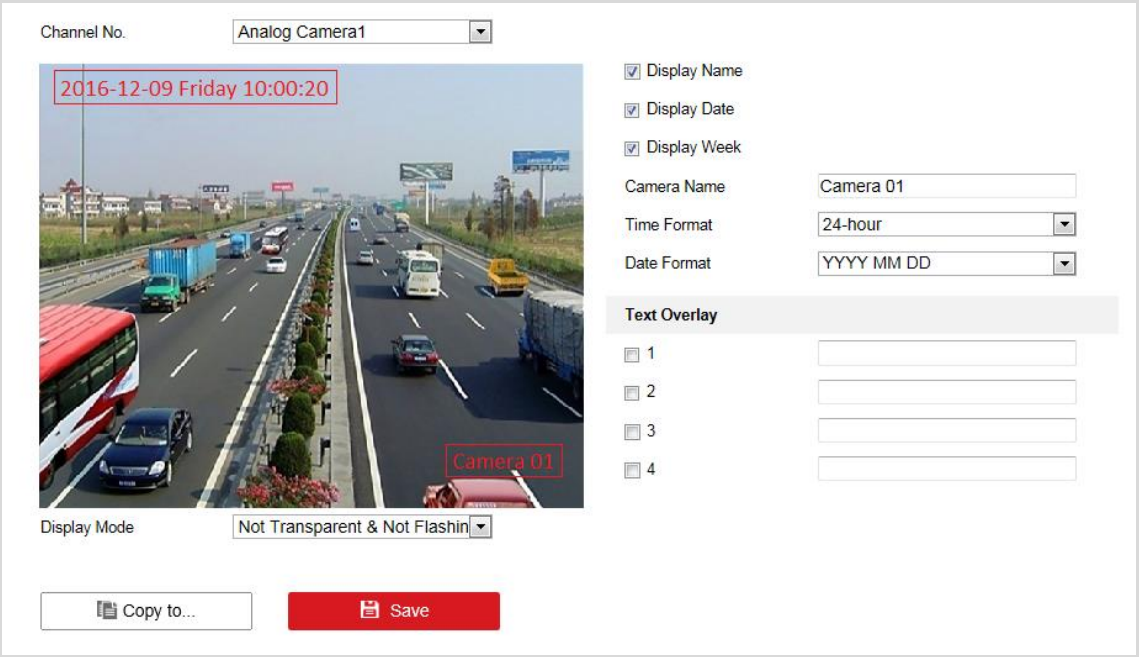


Figure 6-2 OSD Settings

Step 2 Select **Channel No.**

Step 3 Configure OSD of the selected camera.

- Check the corresponding checkbox(es) to display name, date, or week.
- Edit **Camera Name**.
- Select **Time Format** and **Date Format**.
- Drag the text frame in the live view window to adjust the OSD position.
- Edit **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 **Display Mode**.

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

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

Chapter 7 Event Configuration

7.1 Configure Alarm Input

You can configure arming schedule and linkage method for alarm input.

Step 1 Go to **Configuration > Event > Basic Event > Alarm Input**.

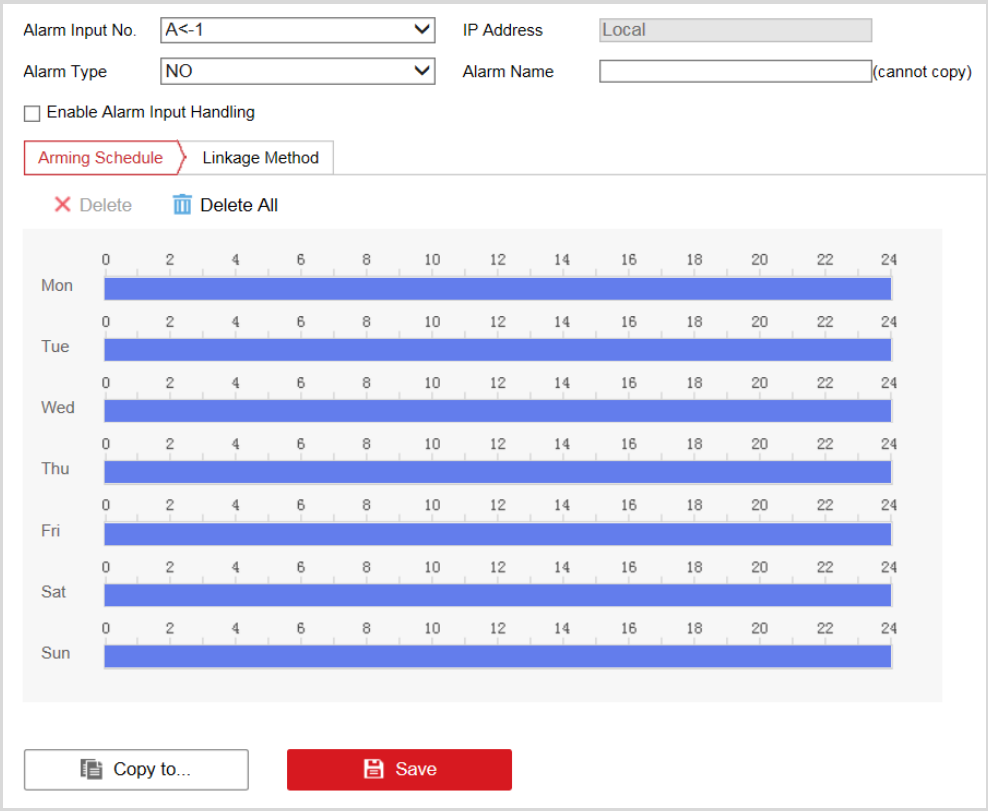


Figure 7-1 Alarm Input

Step 2 Select **Alarm Input No.** and **Alarm Type**. The alarm type can be **NO** (Normally Open) and **NC** (Normally Closed).

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

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

Step 5 Configure **Arming Schedule**.

1) Click **Arming Schedule**.

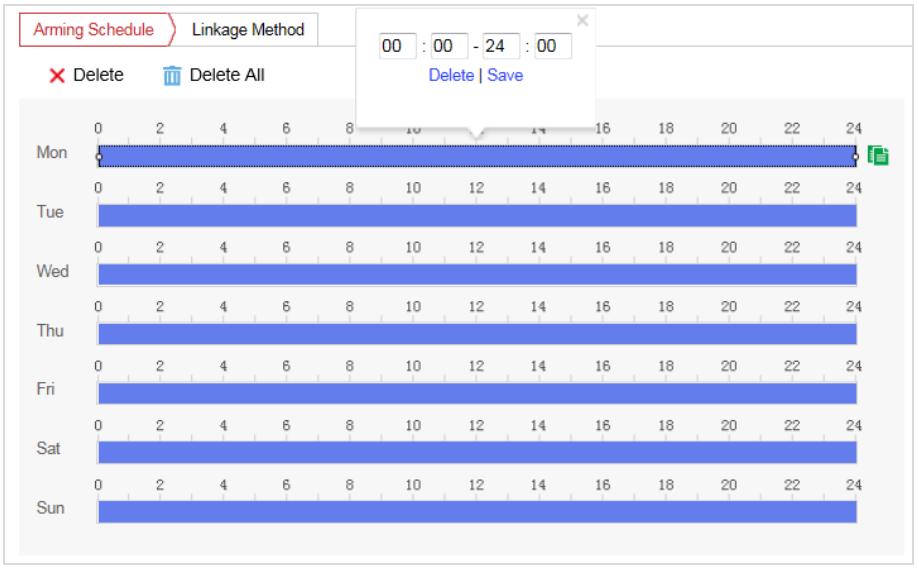


Figure 7-2 Arming Schedule

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

   You can also enter 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 on the end of a day to copy the current arming schedule to other days.

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

NOTE

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

Step 6 Configure **Linkage Method**.

1) Click **Linkage Method**.

2) Configure normal linkage, triggered alarm output, triggered channel, and PTZ linking.

NOTE

The linkage methods vary with different models.

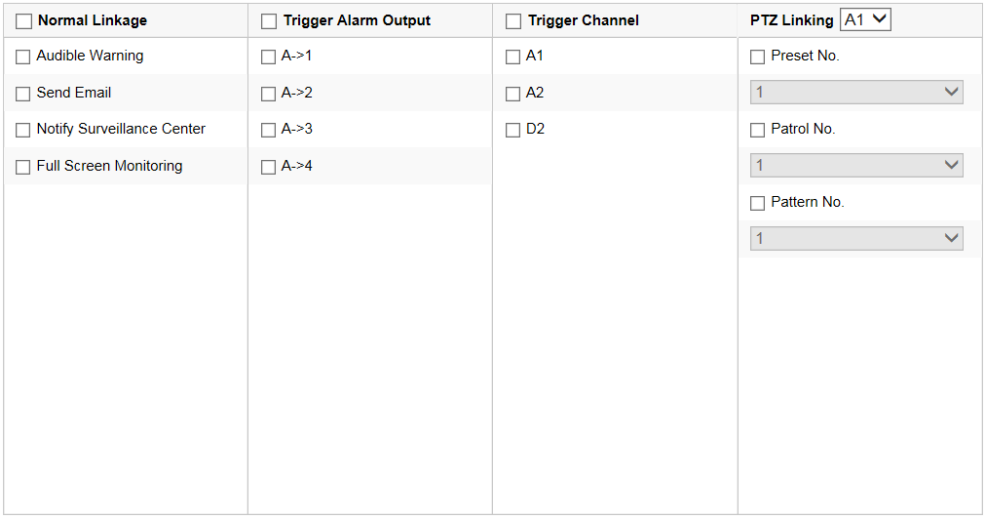


Figure 7-3 Linkage Method

Step 7 (Optional) Click **Copy to** to copy the alarm input settings to other alarm inputs.

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

NOTE

Alarm input settings vary with different models.

7.2 Configure Alarm Output

You can configure the arming schedule for the alarm output.

Step 1 Go to **Configuration > Event > Basic Event > Alarm Output**.

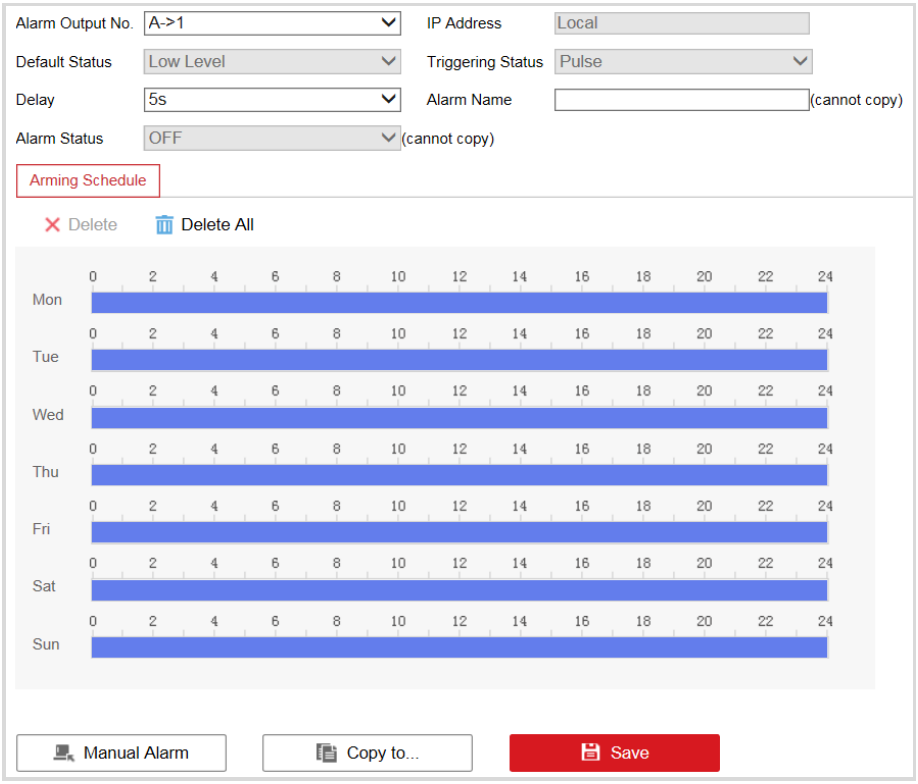


Figure 7-4 Alarm Output

Step 2 Select **Alarm Output No.**

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

Step 4 Select **Delay** time.

NOTE

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

Step 5 Configure **Arming Schedule**. Refer to 7.1 Step 5 of 7.1 Configure 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.

7.3 Configure Exception

You can configure the linkage methods and trigger alarm outputs for different exceptions.

Step 1 Go to **Configuration > Event > Basic Event > Exception**.

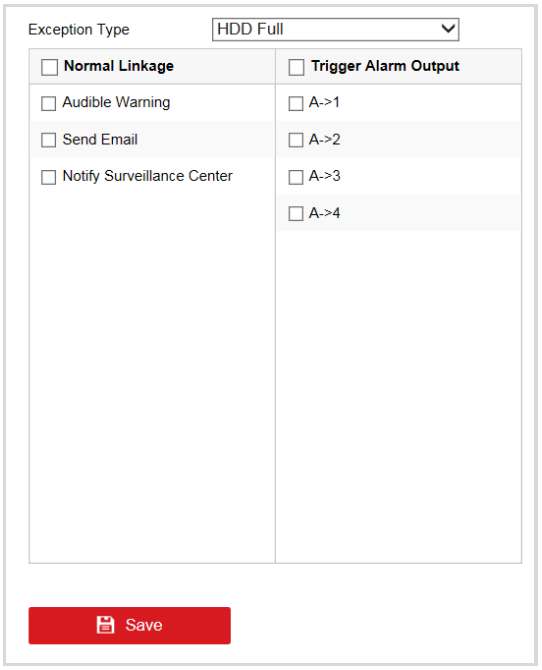


Figure 7-5 Exception Configuration

Step 2 Select **Exception Type**.

Step 3 Check the normal linkage method(s) and alarm output(s).

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

Chapter 8 Network Configuration

8.1 Configure TCP/IP

The station is connected to the network via network cables. Configure the IP address to access the network or connect capture unit.

Step 1 Go to **Configuration > Network > Basic Settings > TCP/IP**.

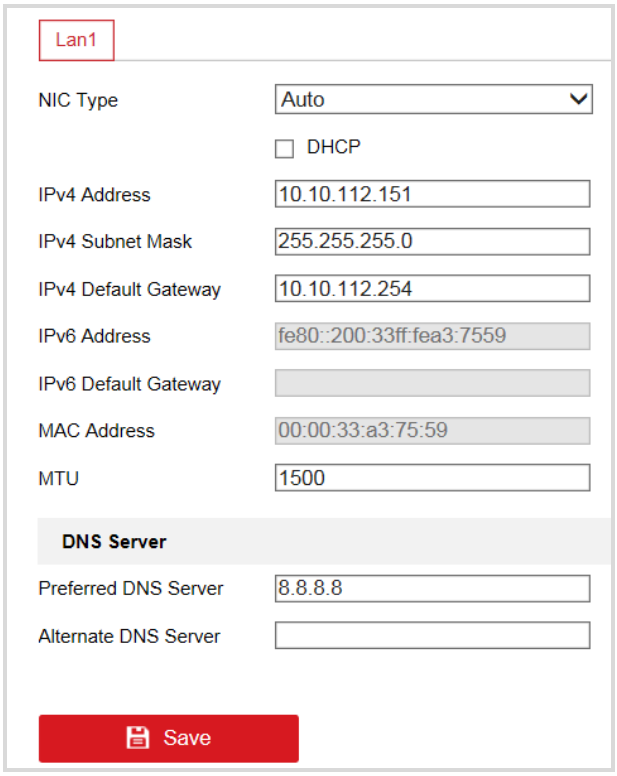


Figure 8-1 TCP/IP Configuration

Step 2 Configure the parameters, including NIC Type, IPv4/IPv6 Address, IPv4/IPv6 Subnet Mask, etc.

NOTE

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

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

Step 4 (Optional) If you need to access the station via extranet, configure **Preferred DNS Server** and **Alternate DNS server**.

NOTE

DNS server can be set according to the DNS settings of router.

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

8.2 Configure Port

HTTP port is used to access the station via web browser. RTSP port is used to get stream. Server port is used to connect to client software.

Step 1 Go to **Configuration > Network > Basic Settings > Port**.

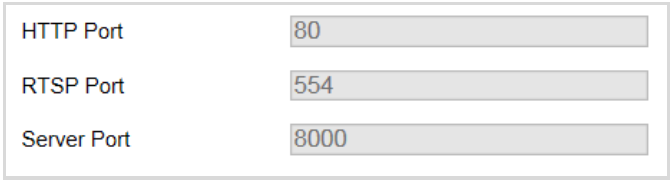


Figure 8-2 Port Configuration

Step 2 View the port parameters.

8.3 Configure Platform Access

The station can be connected to the supported platform.

Step 1 Go to **Configuration > Network > Basic Settings > Platform**.

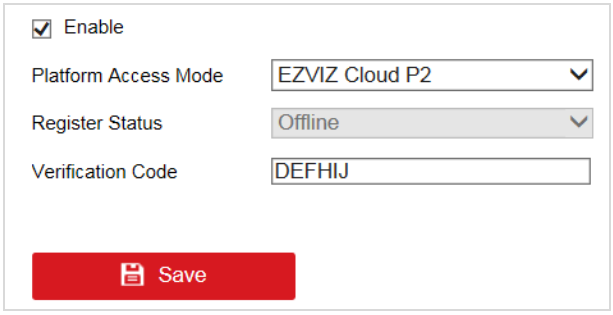


Figure 8-3 Platform Configuration

Step 2 Check **Enable**.

Step 3 Select **Platform Access Mode**.

Step 4 Enter **Verification Code** gotten from the platform.

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

Chapter 9 Safety Management

9.1 Manage User

9.1.1 Add User

You can add users and set user permissions to control the station.

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.

Step 1 Go to **Configuration > System > User Management**.

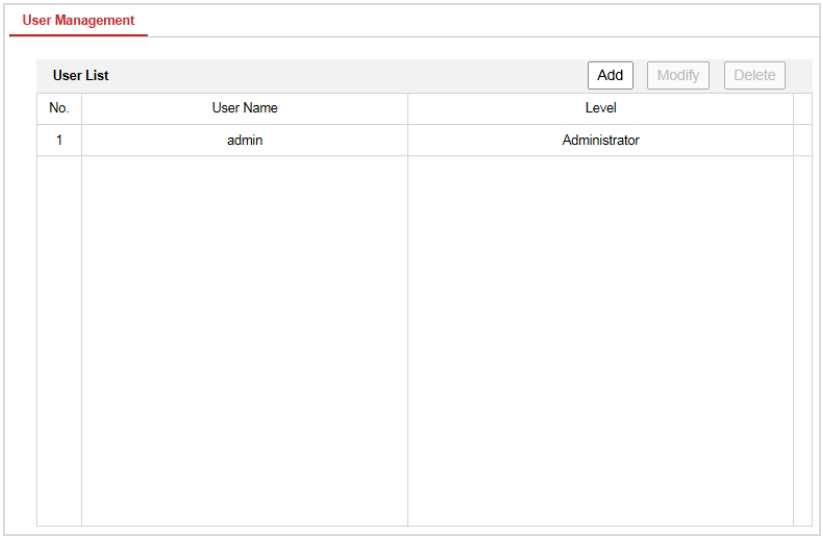


Figure 9-1 User Management

Step 2 Click **Add**.

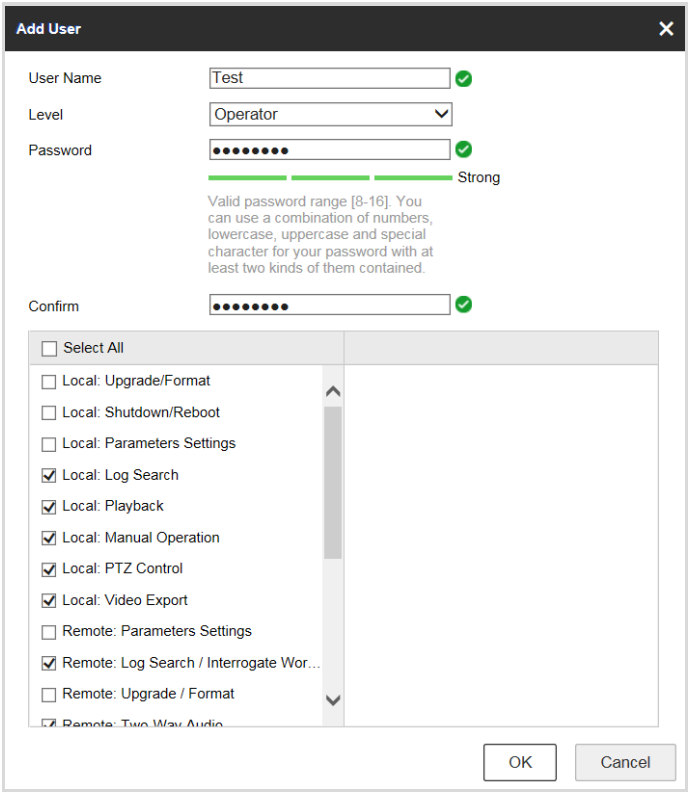


Figure 9-2 Add User

Step 3 Enter **User Name**, select **Level**, enter **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 4 Check the checkbox(es) to select the user permission(s).

Or check **Select All** to select all the permissions.

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

9.1.2 Edit User

You can edit the added user.

Step 1 Go to **Configuration > System > User Management**.

Step 2 Select the user account to edit and click **Modify**.

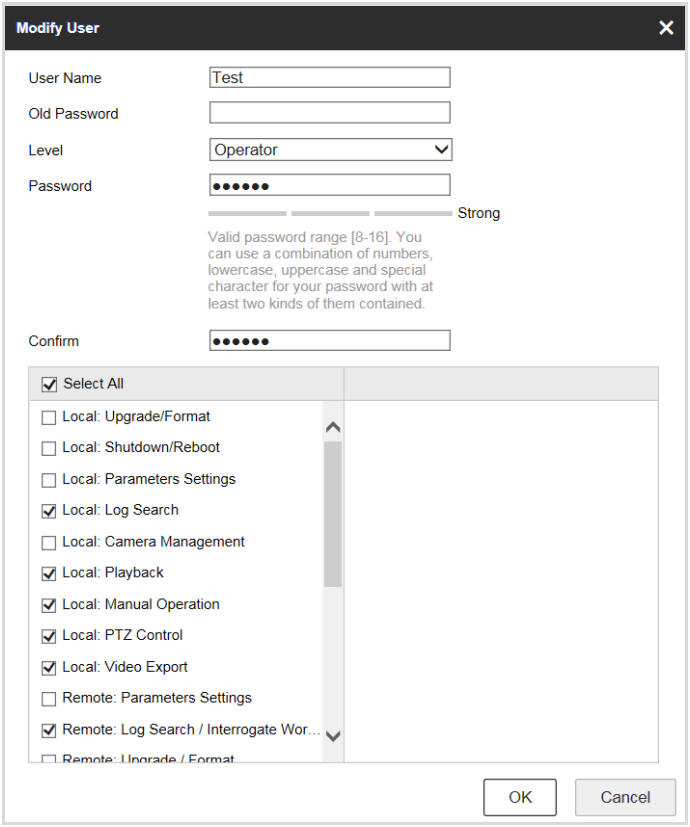


Figure 9-3 Edit User

Step 3 Edit **User Name**, **Password**, **Level**, and permissions.

NOTE

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

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

9.1.3 Delete User

You can delete the added user.

Step 1 Select the user account to delete.

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

NOTE

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

9.2 Configure Security

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

Step 1 Go to **Configuration > System > Security**.

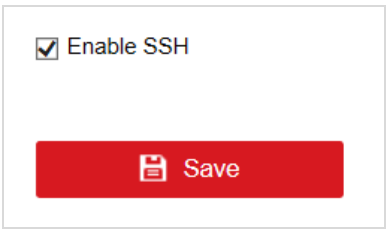


Figure 9-4 Security Configuration

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

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

Chapter 10 Maintenance

10.1 Configure Basic Information

Step 1 Go to **Configuration > System > System Settings > Basic Information**.

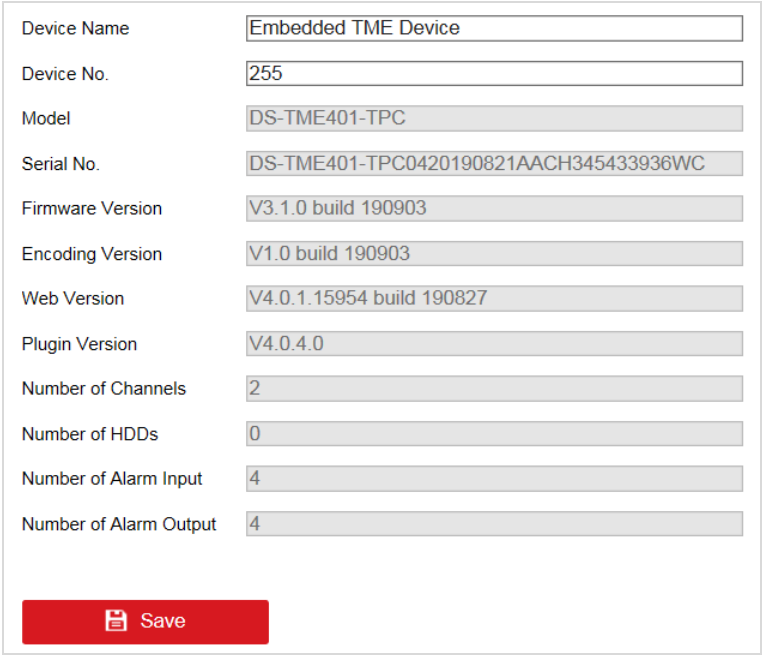


Figure 10-1 Basic Information

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

Step 3 View the other device information including **Model**, **Serial No.**, **Firmware Version**, etc.

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

10.2 Configure Time

Step 1 Go to **Configuration > System > System Settings > Time Settings**.

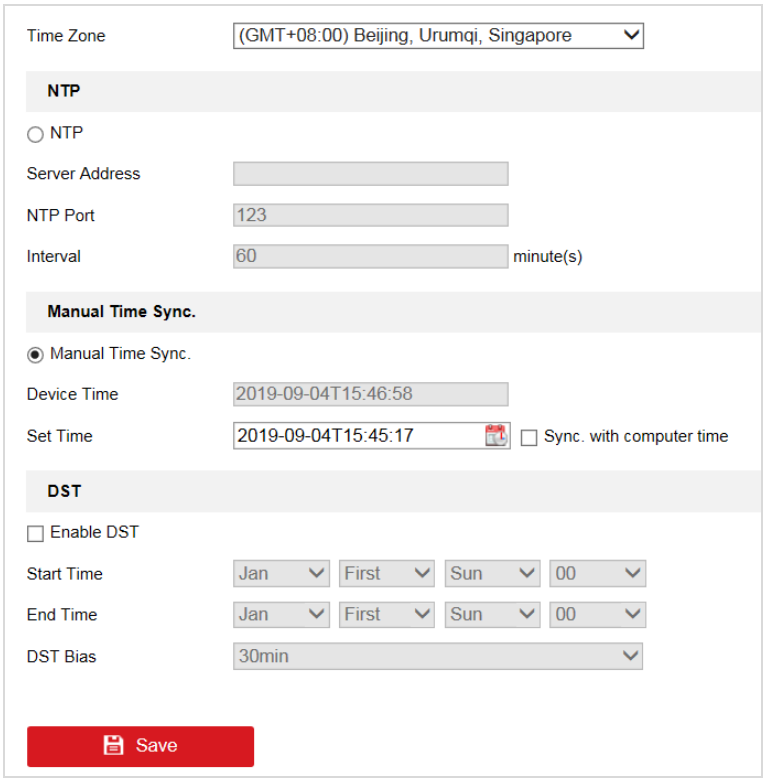


Figure 10-2 Time Settings

Step 2 Select **Time Zone**.

Step 3 Synchronize time.

- **NTP**: After enabling NTP, the NTP server will synchronize the station time at regular intervals.
  1) Select **NTP**.
  2) Enter **Server Address**, **NTP Port**, and **Interval**.
- **Manual Time Sync.**: After enabling Manual Time Synchronization, the station time can be synchronized with the set time or the computer time.
  1) Select **Manual Time Sync.**
  2) Click  to set the time.
  3) (Optional) Check **Sync. with computer time** to synchronize the station time with the computer time.

Step 4 (Optional) Configure DST.

1) Check **Enable DST**.
2) Set **Start Time**, **End Time**, and **DST Bias**.

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

10.3 Reboot

You can reboot the station.

Step 1 Go to **Configuration > System > Maintenance > Upgrade & Maintenance > Reboot**.

Figure 10-3 Reboot

Step 2 Click **Reboot**.

Step 3 Click **OK** on the popup window to reboot the station.

10.4 Restore Default Settings

You can restore the station to default settings if there are parameters errors.

Step 1 Go to **Configuration > System > Maintenance > Upgrade & Maintenance > Default**.

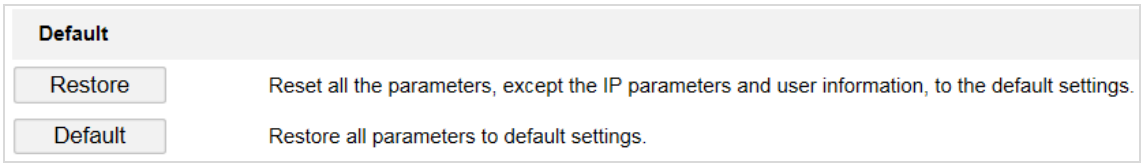


Figure 10-4 Restore Default Settings

Step 2 Select restoration mode.

- Click **Restore** to reset parameters, except the IP parameters and user information, to the default settings.
- Click **Default** to restore all parameters to default settings.

Step 3 Click **OK** on the popup window.

10.5 Format Database

If you need to clear data in the memory card, format the database.

NOTE

Formatting will clear data. Back up data first.

Step 1 Go to **Configuration > System > Maintenance > Upgrade & Maintenance > Format Database**.

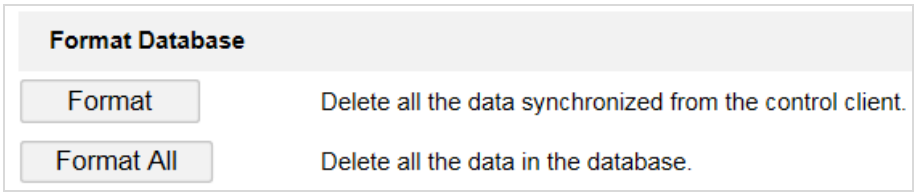


Figure 10-5 Format Database

Step 2 Select the formatting mode.

- Click **Format** to clear the captured pictures and cards data.
- Click **Format All** to clear all the data in the memory card.

Step 3 Click **OK** on the popup window.

10.6 Export Configuration File

You can export the configuration file of the station.

Step 1 Go to **Configuration > System > Maintenance > Upgrade & Maintenance > Export Config. File**.

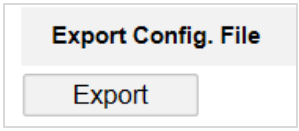


Figure 10-6 Export Configuration File

Step 2 Click **Export**.

Step 3 Select the saving path and edit the file name.

Step 4 Click **Save** to export the configuration file to the computer.

10.7 Import Configuration File

If you want to set the same parameters for stations, you can import the configuration file of one station to another station.

NOTE

The parameters can only be imported among the stations of the same model or the same version.

Before you start

The configuration file has been exported.

Step 1 Go to **Configuration > System > Maintenance > Upgrade & Maintenance > Import Config. File**.

Figure 10-7 Import Configuration File

Step 2 Click **Browse** to select the configuration file from the computer.

Step 3 Click **Import** to import the selected configuration file to the station.

10.8 Upgrade

You can upgrade the station.

Step 1 Go to **Configuration > System > Maintenance > Upgrade & Maintenance > Upgrade**.

Figure 10-8 Upgrade

Step 2 Click **Browse** to select the upgrade file from the computer.

Step 3 Click **Upgrade** to upgrade the firmware.

NOTE

The station will reboot automatically after upgrading. DO NOT disconnect power to the station during the process.

10.9 Configure and Export Log

You can configure log parameters, export log, and delete log.

Step 1 Go to **Configuration > Entrance and Exit > Log**.

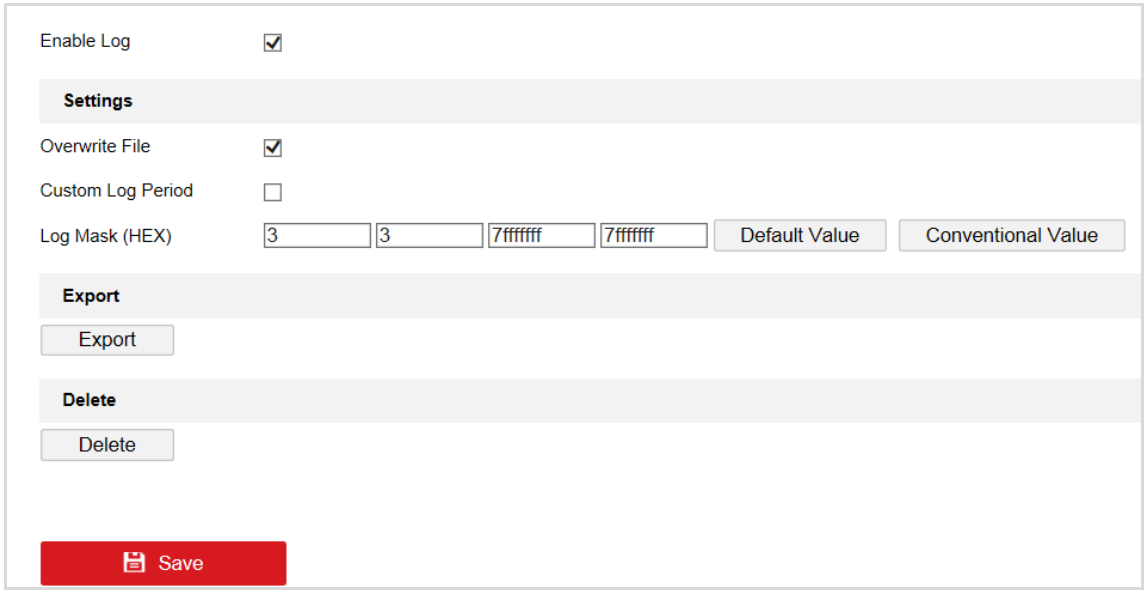


Figure 10-9 Log Configuration

Step 2 Check **Enable Log**.

Step 3 Configure log parameters.

- **Overwrite File**: Check it, and the former log will be overwritten when the log storage is full.
- **Custom Log Period**: Check it if you want to record log during custom time period. Configure the time period.
- **Log Mask (HEX)**: If you want to configure the log type, enter the log mask of the log type.

NOTE

Contact the technical supports of our company to get the log mask.

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

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

NOTE

Back up the data before deleting the log file.

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


See Far, Go Further