Entrance/Exit Ticket Station

User Manual

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product. m^2

About this Product

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

Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR

LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

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

Symbol Conventions

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

Symbol	Description
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.

Table of Contents

Chapter 1 Introduction

1.1 Product Introduction

Entrance/Exit Ticket 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.

NOTE

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

1.2 Key Features

- 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.
- Voice prompt to notice the charging fees, reducing the manual labor.
- 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.

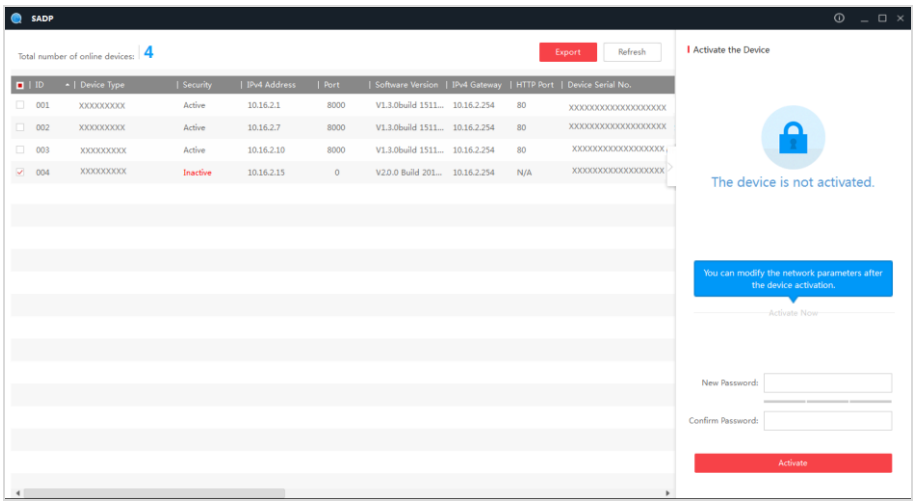


Figure 2-1 SADP Interface

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**.

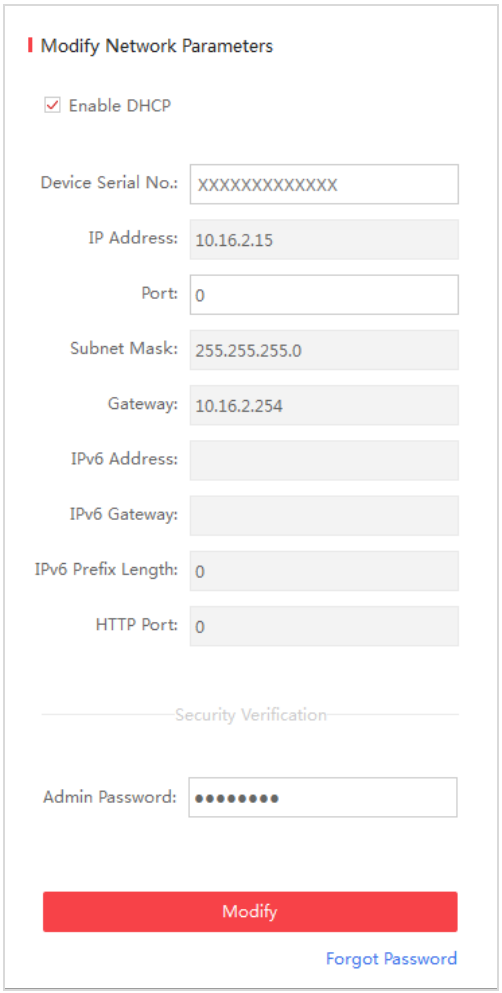


Figure 2-2 Modify IP Address

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

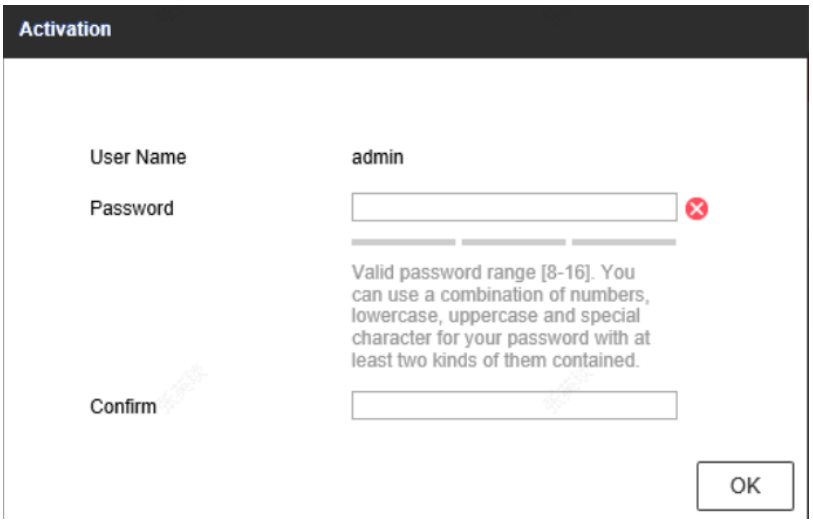
2.1.3 Activate via Web Browser

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 Basic Operation

3.1 Configure Entrance & Exit Parameters

3.1.1 Configure Basic Parameters

You can configure the basic parameters for entrance and exit.

Step 1 Go to **Configuration > Settings > Basic Parameters**.

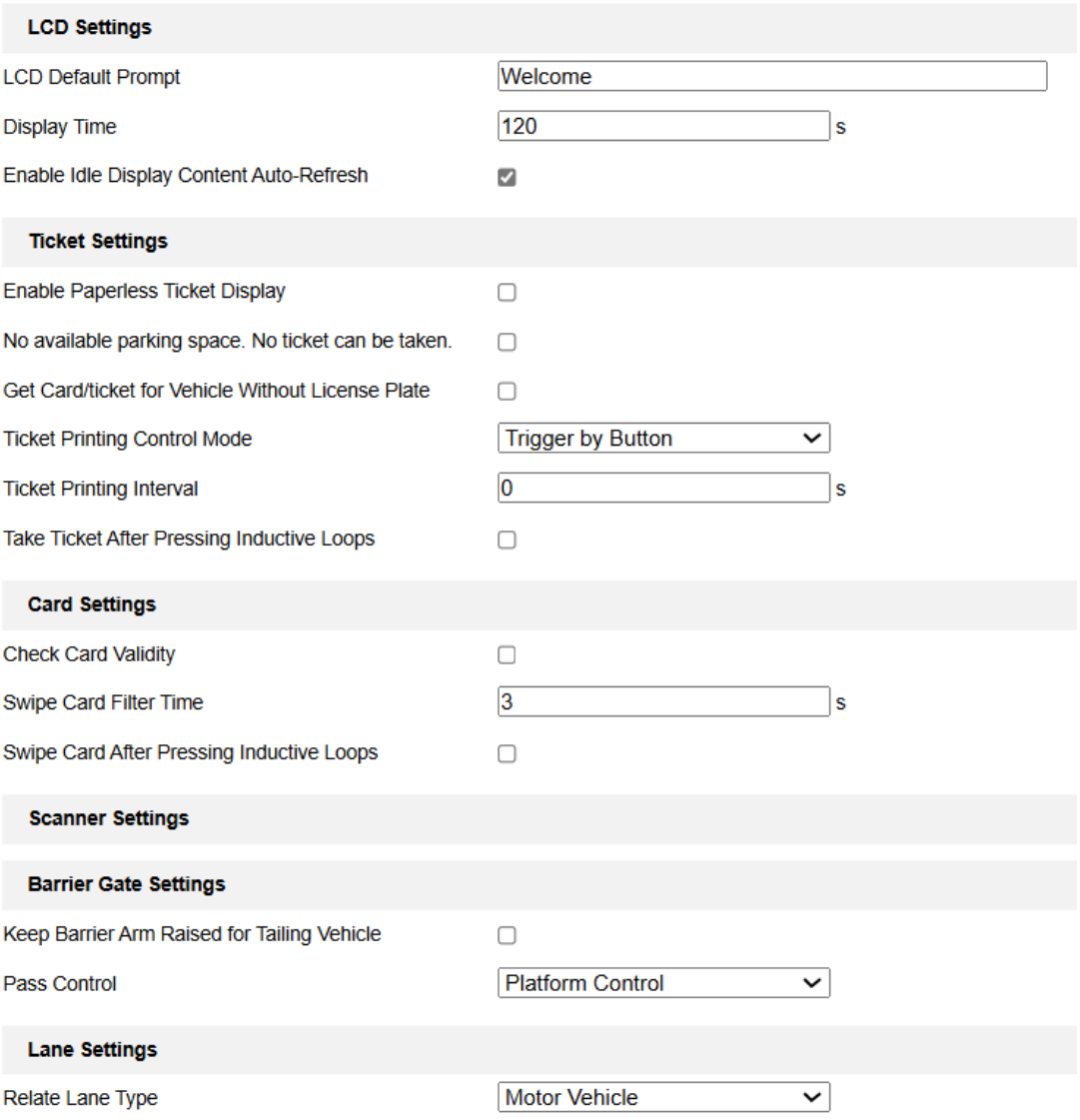


Figure 3-1 Basic Parameters

Step 2 Configure the following parameters according to your needs.

1. Set the LCD parameters.

- **LCD Default Prompt**: Enter the LCD default prompt content.
- **Display Time**: Set the display time of the LCD scene.
- **Enable Idle Display Content Auto-Refresh**: When enabled, the LCD scene will automatically refresh to the default scene after reaching the set display time. When disabled, the scene will not be refreshed automatically. This item will not affect the local device prompts.

2. Set the ticket parameters.

- **Enable Paperless Ticket Display:** When enabled, the LCD will display the paperless prompt if there is no paper ticket.
- **No available parking space. No ticket can be taken**.: When enabled, the ticket will not be available if there are no available parking spaces.
- **Get Card/ticket for Vehicle Without License Plate**: When enabled, only the vehicles without license plates can get card or ticket.
- **Ticket Printing Control Mode:** Set the ticket printing to be triggered by the platform or the device.
- **Ticket Printing Interval:** Set the ticket printing interval time.
- **Take Ticket After Pressing Inductive Loops**: When enabled, the ticket can be taken only when the vehicle is on the inductive loop.

NOTE

Ticket parameters are only available to Entrance Station.

3. Set the card parameters.

- **Check Card Validity**: When enabled, only registered cards can be reported to the platform, otherwise, all cards will be reported.
- **Swipe Card Filter Time**: Set the filter time for the same card No.
- **Swipe Card After Pressing Inductive Loops**: When enabled, swiping card is allowed only when the vehicle is on the inductive loop.

4. Set the scanner parameters.

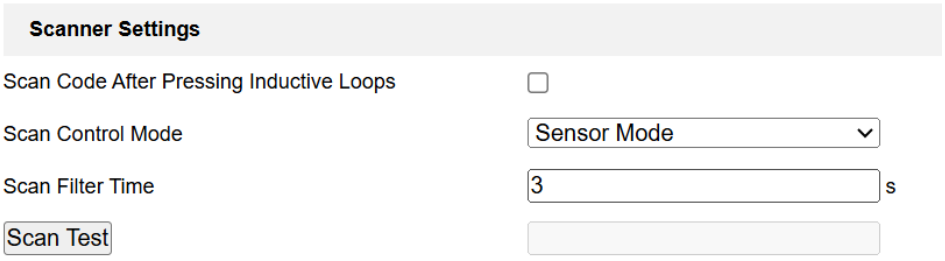


Figure 3-2 Scanner Parameters

- **Scan Code After Pressing Inductive Loops**: When enabled, scanning codes is allowed only when the vehicle is on the inductive loop.
- **Scan Control Mode**: In sensor mode, the scanner is controlled by sensor. In trigger mode, the scanner is controlled by protocol.

NOTE

After configuration, reboot the station to take the settings into effect.

- **Scan Filter Time**: Set the filter time for scanning the same ticket No.
- **Scan Test**: Click **Scan Test**, and scan the code to view the card No. in the text field.

NOTE

Scanner settings are only available to Exit Station.

5. Set the barrier gate and lane parameters.

- **Keep Barrier Arm Raised for Tailing Vehicle**: When enabled, the barrier gate keeps open when the device detects tailing vehicles are passing.
- **Pass Control**: Select **Device Control** if you want to control the barrier gate by the device, or select **Platform Control** to control the barrier gate by the platform.
- **Relate Lane Type**: Select the lane type based on the actual situation.

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

3.1.2 Configure Ticket

You can configure the content on the ticket.

NOTE

This function is only available to Entrance Station.

Step 1 Go to **Configuration > Settings > Ticket Configuration**.

Figure 3-3 Ticket Configuration

Step 2 Set the basic ticket parameters.

1. Enter **Title**, **Contact No.**, and **Custom** information to be printed on the ticket.
2. Select **Code Type**. Barcode and QR Code are selectable.
3. (Optional) Check **Print License Plate Number** to print the license plate number on the ticket.
4. (Optional) Check **Print Entering Time** to print the entering time of the vehicle on the ticket.
5. (Optional) Check **Print Ticket Number** to print the ticket number on the ticket.
6. (Optional) Click **Print Test** to print the configured ticket to view the effect. The ticket format is shown below.

Figure 3-4 Ticket Example

Step 3 Click **Advanced** to customize the ticket parameters as needed.

1. Select the type to be printed on the ticket, including title, contact information, plate No., entry time, etc., or you can customize the type.

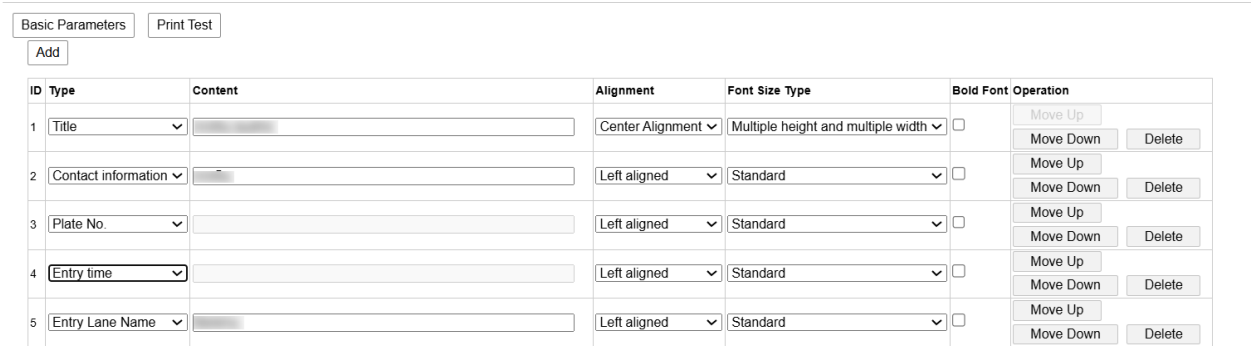


Figure 3-5 Advanced Parameters

2. Enter the content you want to print in the **Content** column.
3. (Optional) Set the text format, including alignment, font size, and bold.
4. (Optional) Click **Move Up** or **Move Down** to adjust the order of the items.
5. (Optional) To add more types, click **Add** to add a type. To delete a type, select the type, and click **Delete** in the **Operation** button.

NOTE

Up to 25 types are allowed.

6. Click **Print Test** to print the configured ticket to view the effect.

Step 4 Click **Save**.

3.1.3 Configure Audio

You can configure the voice prompt.

Step 1 Go to **Configuration > Settings > Audio Configuration**.

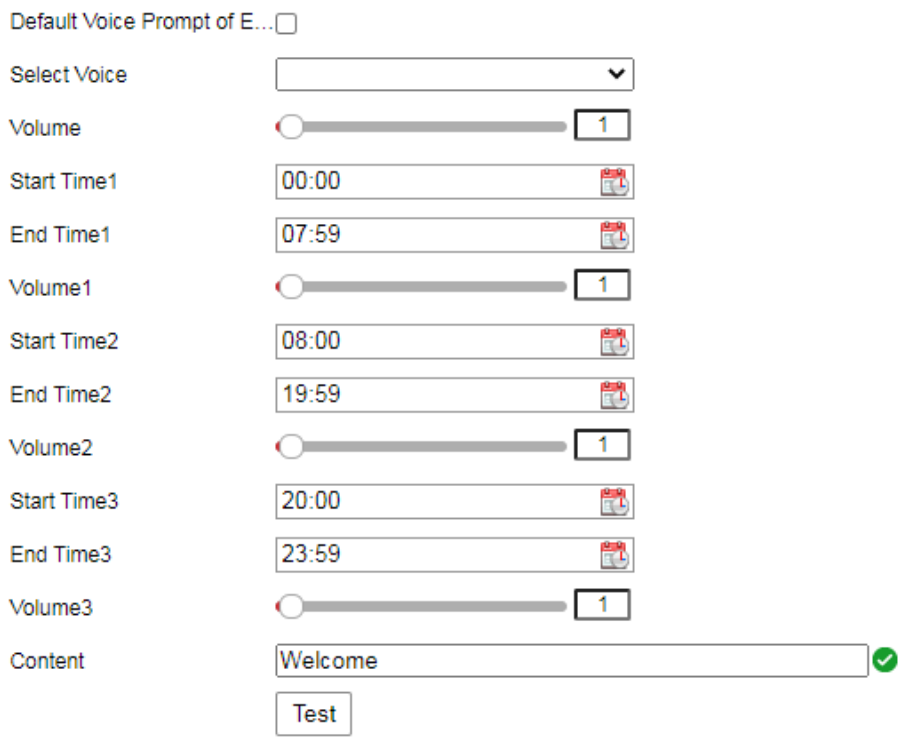


Figure 3-6 Audio Configuration

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

Step 3 Select the voice.

Step 4 Set the time period of the voice prompt, and slide the bar to adjust **Volume**. 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.

3.1.4 Configure Media

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

Step 1 Go to **Configuration > Settings > Media Configuration**.

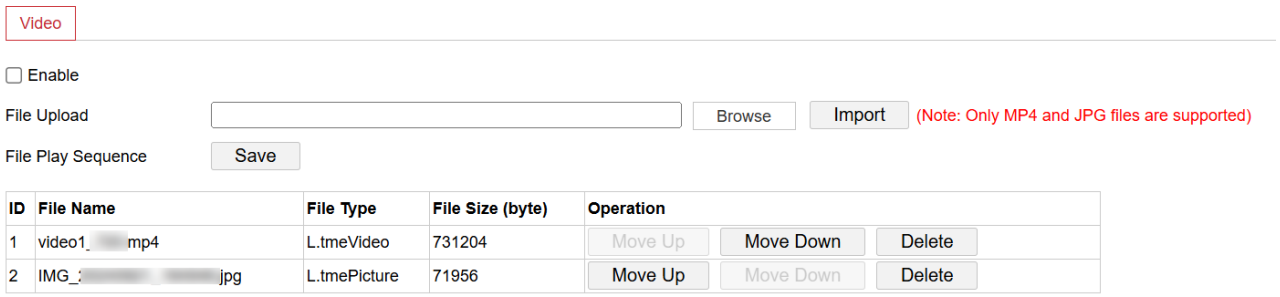


Figure 3-7 Media Configuration

Step 2 Click **Browse** to select the video file.

Step 3 Check **Enable**.

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

NOTE

- Only MP4 or JPG files are supported. The size should be less than 100 M, and the recommended resolution is 600 × 1024.
- The imported file takes effect after you reboot the device.

Step 5 (Optional) Click **Move Up** or **Move Down** to adjust the file play sequence.

Step 6 Click **Save**.

Result:

LCD will play the imported video automatically.

3.1.5 Configure Audio Prompt

You can import audio files to be played, and multi-language audio files are supported.

Step 1 Go to **Configuration > Settings > Audio Prompt**.

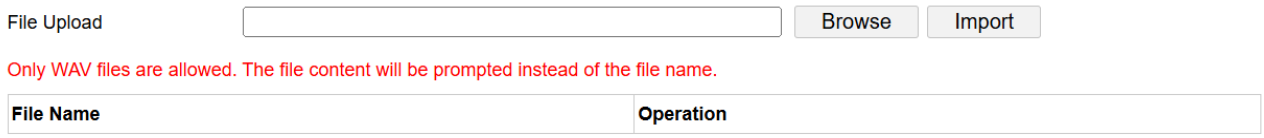


Figure 3-8 Audio Prompt

Step 2 Click **Browse** to select the audio file.

Step 3 Click **Import** to import it.

NOTE

- Only WAV files are supported, and each file cannot exceed 1 MB.

- Up to 100 files are allowed.
- After importing, the file content will be played instead of the file name.

3.1.6 Configure Barrier Gate

You can set time periods to control barrier gate.

NOTE

- This function is only available to the connected barrier gates.
- To control the barrier gate immediately, go to **Configuration** > **Entrance and Exit** > **Barrier** > **Barrier Control**.

Step 1 Go to **Configuration > Settings > Barrier Settings**.

No.	Start Time	End Time	Clear
1	00:00:00	08:20:00	Clear
2	00:00:00	00:00:00	Clear
3	00:00:00	00:00:00	Clear
4	00:00:00	00:00:00	Clear

Figure 3-9 Barrier Settings

Step 2 Set the start time and end time, and the system will keep the barrier gate open within the set time period.

Step 3 (Optional) To clear the specified time period, click **Clear**.

NOTE

- Up to four time periods are allowed.
- The set time periods are effective for all the connected barrier gates.

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

3.1.7 Configure Display

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

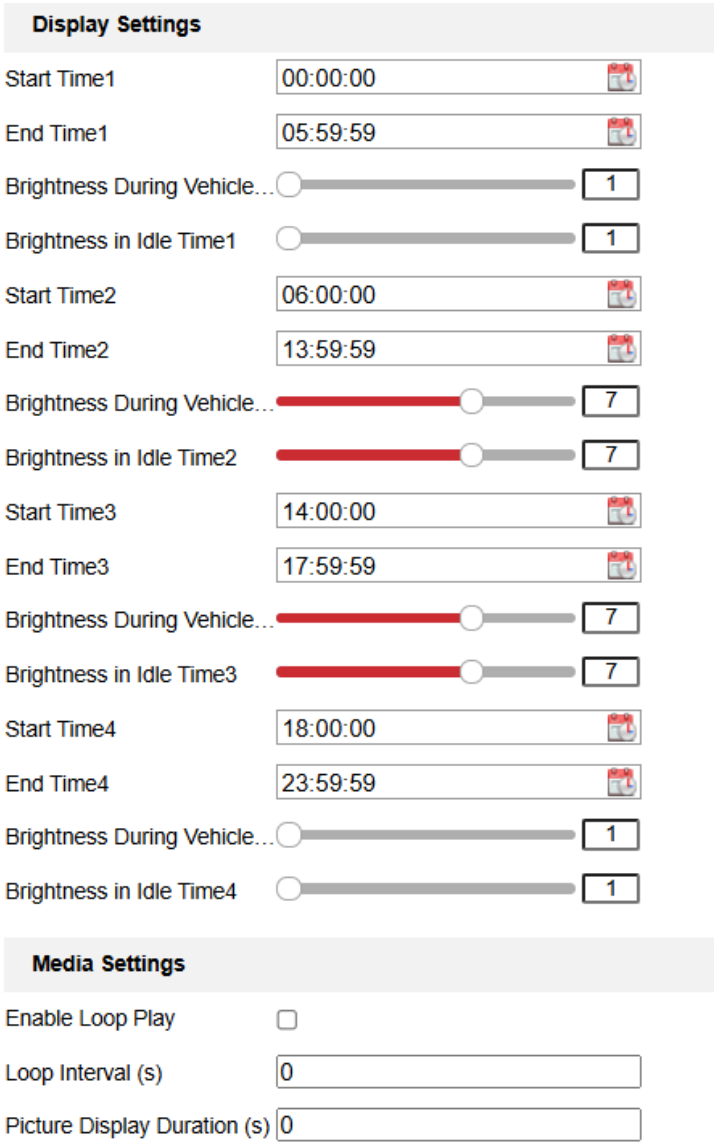


Figure 3-10 Display Settings

Step 2 Set the display period on the screen, and set **Passing Brightness During Vehicle Passing** and **Brightness in Idle Time** of each period.

Step 3 (Optional) If you want to enable loop play of the display content, check **Enable Loop Play**, and set **Loop Interval** and **Picture Display Duration**.

Step 4 Click **Save**.

3.1.8 View Entrance & Exit Status

Go to **Configuration > Entrance and Exit > Status** to view passing status, peripheral status, etc.

NOTE

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

Passing Status

View mode, passing result, and passing time.

Mode	Passing Result	Passing Time
Online Mode	Pass	2023-10-24 10:37:05.436

Figure 3-11 Passing Status

Peripheral Status

View the name and status of the peripheral devices.

Device Name	Device Status

Figure 3-12 Peripheral Status

Arming Status

View arming mode, arming host, arming time, arming state, and arming level.

Arming Mode	Arming Host	Arming Time	Arming State	Arming Level
SDK	10.184.148.227	2020-04-17 19:55:33.369	Normal	1

Figure 3-13 Arming Status

System Status

View system time, system running time, CPU utilization, and memory utilization.

System Time	System Running Time	CPU Utilization	Memory Utilization
2023-11-08 17:14:29	15D:7H:4M:56S	5%	9%

Figure 3-14 System Status

3.2 Manage Card

You can manage cards on the **Data** page.

3.2.1 Add Card

You can add cards and set the basic information.

Step 1 Go to **Data > Card No. List**.

Step 2 Click **Add**.

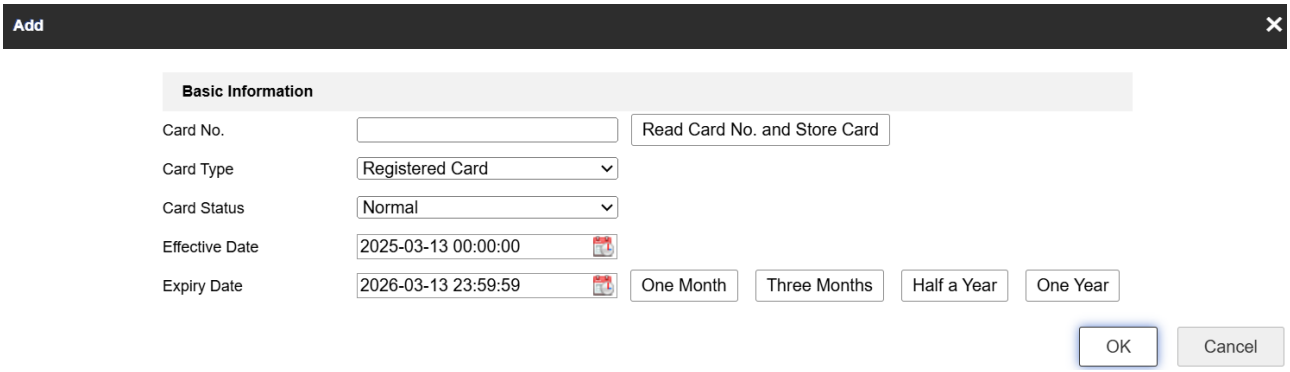


Figure 3-15 Add Card

Step 3 Set the basic information for the card.

- **Card No.**: Enter the card No. manually. You can also swipe the card on the card reader and then click **Read Card No. and Store Card**.
- **Card Type:** Registered Card, Temporary Card, and Invalid Card are selectable.
- **Card Status**: Normal, Expired, Report Card Loss, and Logout are selectable. Logout means that the card No. has been cancelled.
- **Effective Date:** Set the start time of the effective date.
- **Expiry Date**: Set the expiry date, or select the validity period.

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

Step 5 (Optional) To edit the card information, click under the **Operation** column.

3.2.2 Delete Card

You can delete the added cards one by one or in batch.

- To delete cards in batch, select the cards to delete, and click **Delete**.
- To delete a card, click under the **Operation** column to delete it.

3.2.3 Import Card

You can import a file to add cards in batch.

Step 1 Go to **Data > Card No. List**.

Step 2 Click **Import**.

Figure 3-16 Import Cards

Step 3 Click **Download Import Template** to download the template, and then complete the file according to the template.

Step 4 Click **Browse** to select the file from the computer.

Step 5 Click **Import** to import the selected file to the device.

NOTE

Up to 50,000 items can be imported one time.

3.2.4 Export Card

You can export the card No. list to your computer.

Step 1 Go to **Data > Card No. List**.

Step 2 Click **Export**.

Step 3 Click **Export** on the pop-up window. The card No. list will be downloaded locally.

3.2.5 Search Card

You can search cards by search condition.

Step 1 Go to **Data > Card No. List**.

Step 2 Enter the card No., or select the card type and card status.

Step 3 Click **Search** to search the card information.

3.3 Search Card Records

You can search card swiping records by search conditions.

Step 1 Go to **Data** > **Card No. Record**.

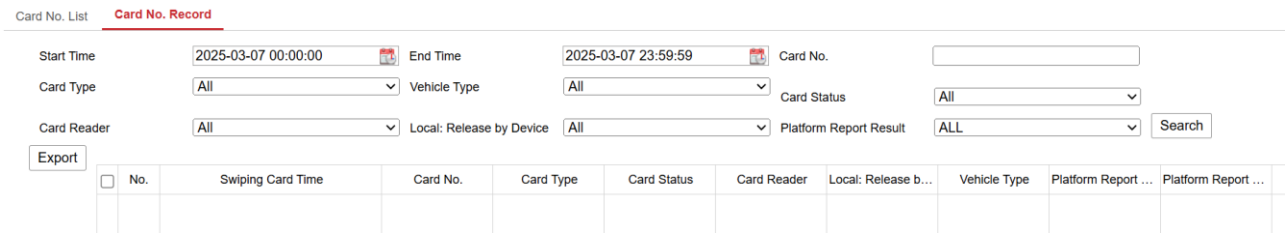


Figure 3-17 Search Card No. Records

Step 2 Set the start time and end time, and select **Card Type**, **Card Status**, **Card Reader**, and **Platform Report Result**. The default is **ALL**.

Step 3 (Optional) Enter the card No. in the field.

Step 4 Click **Search** to search the card records. The search results include the swiping card time, card No., card type, card status, card reader, etc.

Step 5 (Optional) To export the card records to your computer, select the records and click **Export**.

3.4 Configure Two-Way Audio

3.4.1 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.

3.4.2 Two-Way Audio with Software

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

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

Figure 3-18 Two-Way Audio

Step 2 Adjust the value.

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

Chapter 4 Network Configuration

4.1 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**.

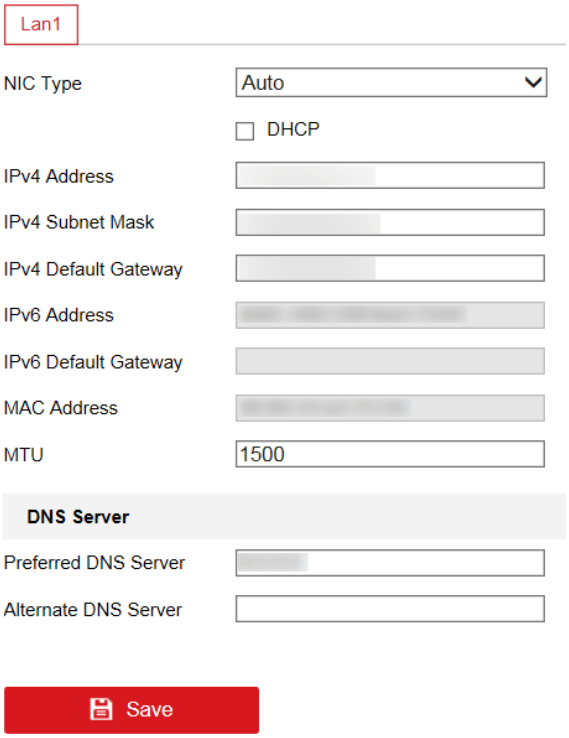


Figure 4-1 TCP/IP Configuration

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.

4.2 Connect to ISUP

The station can be remotely accessed via ISUP platform.

Before You Start

- Create the station ID on ISUP platform.
- Ensure the station can communicate with the platform normally.

Step 1 Go to **Configuration > Network > Advanced Settings > Platform Access**.

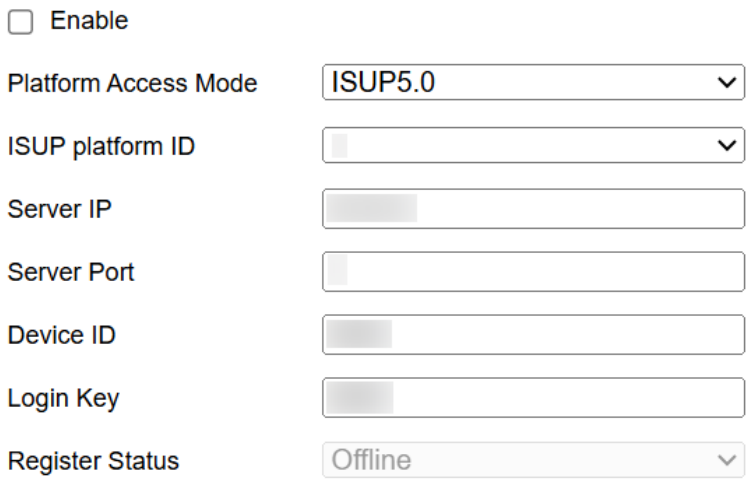


Figure 4-2 Platform Access

Step 2 Check **Enable**.

Step 3 Select **Platform Access Mode** as **ISUP5.0**.

Step 4 Enter **Server IP**, **Server Port**, and **Device ID**.

NOTE

The device ID should be the same with the added one on the ISUP platform.

Step 5 Click **Save**.

Step 6 (Optional) View **Registration Status**.

4.3 Connect to SIP

The Session Initiation Protocol (SIP) is a signaling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video and messaging applications.

Before You Start

Ensure the station can communicate with the platform normally.

Step 1 Go to **Configuration > Network > Advanced Settings > Platform Access**.

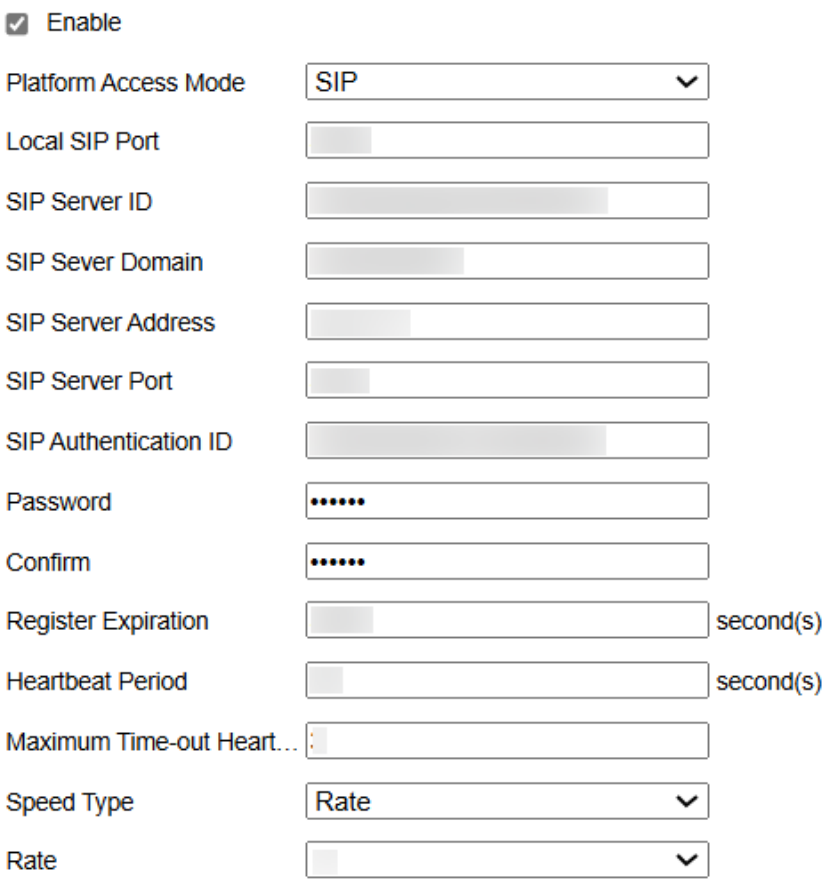


Figure 4-3 Platform Access

Step 2 Check **Enable**.

Step 3 Select **Platform Access Mode** as **SIP**.

Step 4 Set the SIP server related parameters, including address, port, and server ID.

Step 5 Create the SIP server password, and confirm the password.

Step 6 Set the register expiration, heartbeat, speed type, and rate.

Step 7 Click **Save**.

4.4 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**.

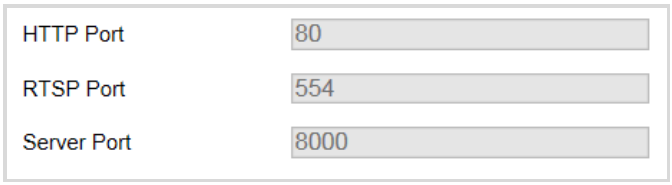


Figure 4-4 Port Configuration

Step 2 View the port parameters.

4.5 Configure HTTP

You can connect the station to HTTP platform to report events such as scanning codes and alarms to the platform.

Before You Start

The network communication between the station and the platform is normal.

Step 1 Go to **Configuration > Network > Advanced Settings > HTTP**.

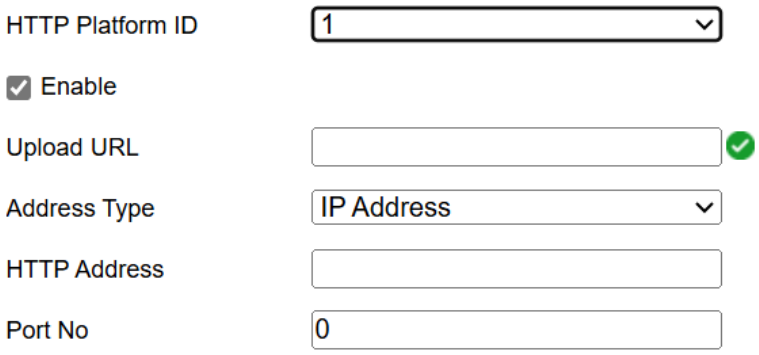


Figure 4-5 Connect to HTTP Platform

Step 2 Select **HTTP platform ID**.

Step 3 Check **Enable**.

Step 4 Set the URL of the platform.

Step 5 Select **Address Type**, and set the corresponding parameters.

Step 6 Click **Save**.

Chapter 5 Safety Management

5.1 Manage User

5.1.1 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**.

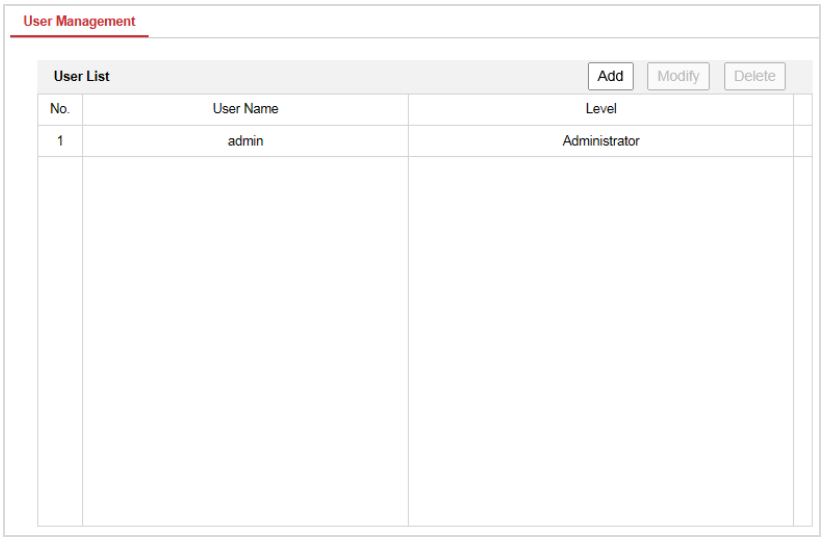


Figure 5-1 User Management

Step 2 Click **Add**.

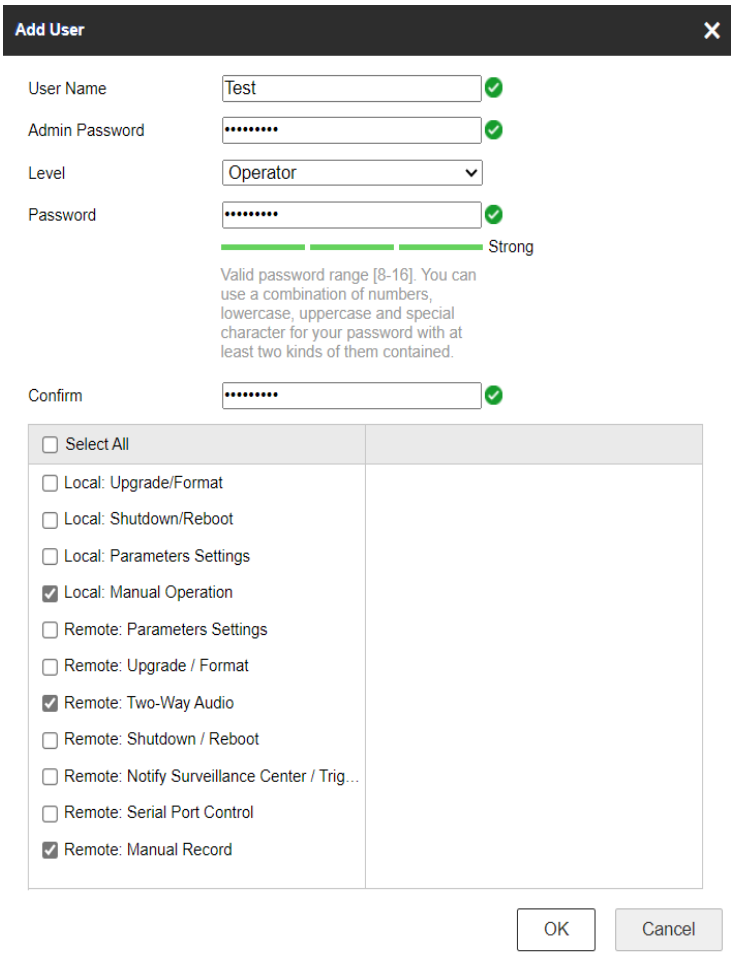


Figure 5-2 Add User

Step 3 Enter **User Name** and **Admin Password**, 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 two 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.

5.1.2 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**.

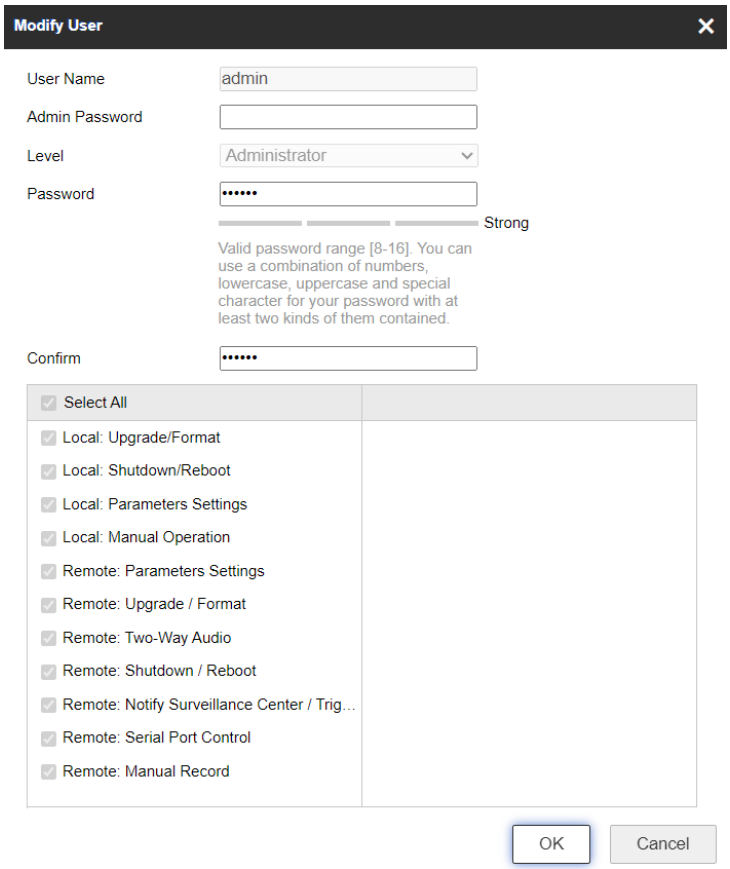


Figure 5-3 Edit User

Step 3 Edit **Admin Password**, **Password**, 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.

5.1.3 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.

5.2 Configure Security

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

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

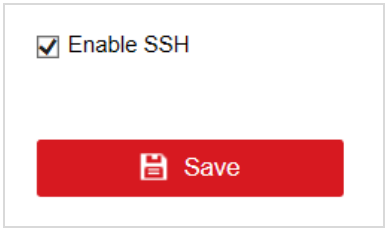


Figure 5-4 Security Configuration

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

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

Chapter 6 Maintenance

6.1 Configure Basic Information

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

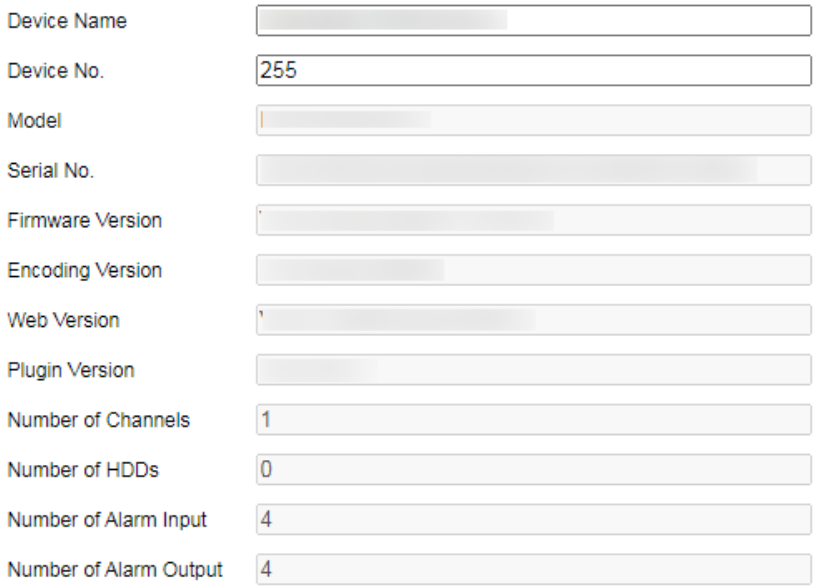


Figure 6-1 Basic Information

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.

6.2 Configure Time

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

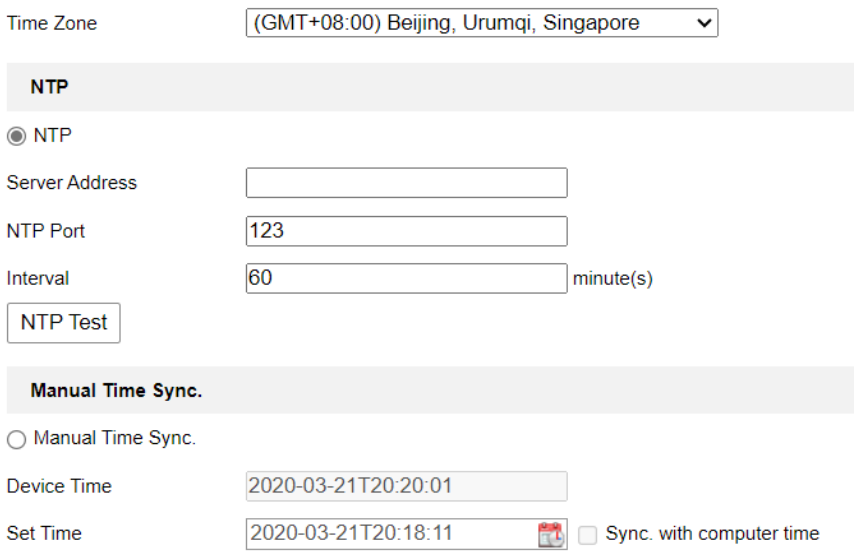


Figure 6-2 Time Settings

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 Click **Save** to save the settings.

6.3 Configure DST

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

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

Step 2 Check **Enable DST**.

Step 3 Set **Start Time**, **End Time**, and **DST Bias**.

Step 4 Click **Save**.

6.4 Configure RS-232

Set RS-232 parameters if you need to debug the device via RS-232 serial port, or peripheral devices have been connected.

Before You Start

The corresponding device has been connected via the RS-232 serial port.

Steps

Step 1 Go to **Configuration > System Settings > RS232**.

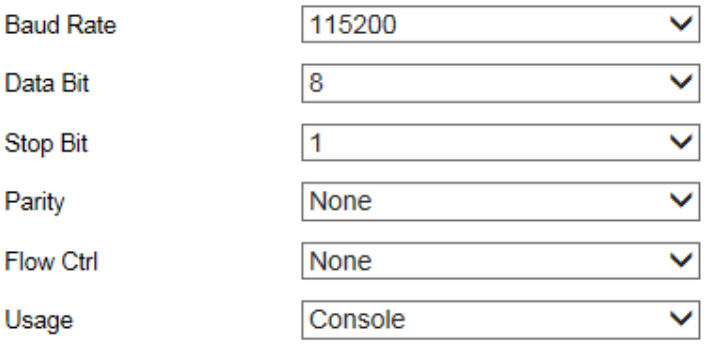


Figure 6-3 Set RS-232

Step 2 Set **Baud Rate**, **Data Bit**, **Stop Bit**, etc.

NOTE

The parameters should be same with those of the connected device.

Step 3 Click **Save**.

6.5 Reboot

You can reboot the station.

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

Figure 6-4 Reboot

Step 2 Click **Reboot**.

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

6.6 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**.

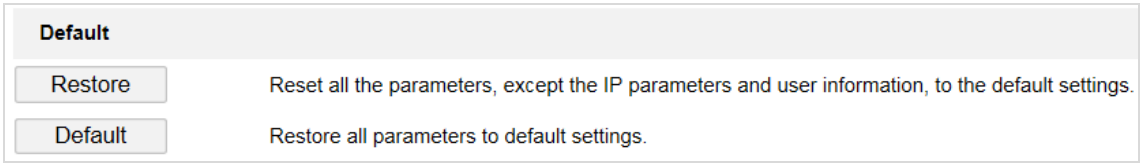


Figure 6-5 Restore Default Settings

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.

6.7 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**.

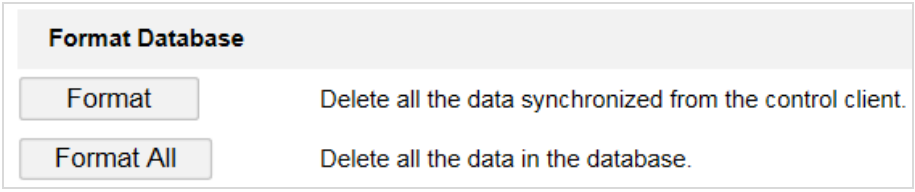


Figure 6-6 Format Database

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.

6.8 Export Configuration File

You can export the configuration file of the station.

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

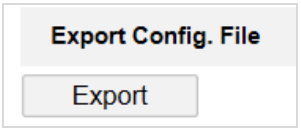


Figure 6-7 Export Configuration File

Step 2 Click **Export**.

Step 3 Enter the password on the popup window.

Step 4 Select the saving path and edit the file name.

Step 5 Click **Save** to export the configuration file to the computer.

6.9 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**.

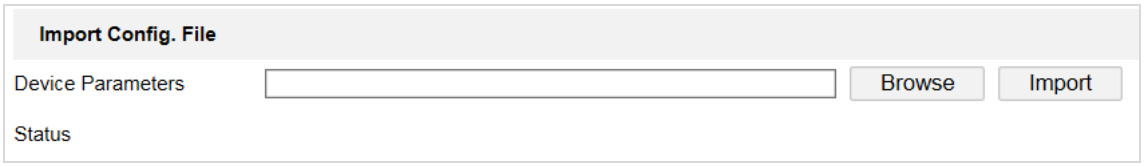


Figure 6-8 Import Configuration File

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.

6.10 Upgrade

You can upgrade the station.

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

Figure 6-9 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.

6.11 Configure and Export Log

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

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

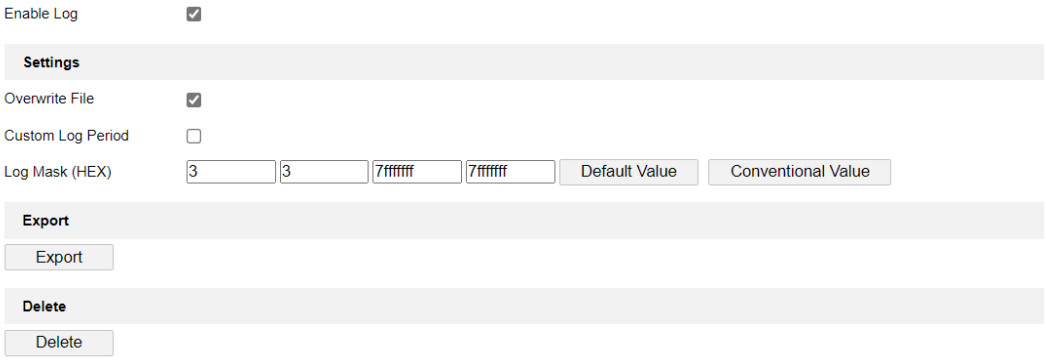


Figure 6-10 Log Configuration

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.

UD35722B-A