



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. m²

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.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

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.....	6
1.1 Product Introduction.....	6
1.2 Key Feature.....	6
Chapter 2 Activation and Login	7
2.1 Activate Device.....	7
2.1.1 Default Information.....	7
2.1.2 Activate via SADP	7
2.1.3 Activate via Web Browser	8
2.2 Log in	9
2.3 Log out.....	10
Chapter 3 Live View Operation	11
Chapter 4 Basic Operation	12
4.1 Configure Entrance & Exit Parameters.....	12
4.1.1 Configure Basic Parameters	12
4.1.2 Configure Ticket	12
4.1.3 Configure Audio	13
4.1.4 Configure Media.....	14
4.1.5 Configure Screen Display	15
4.1.6 View Entrance & Exit Status.....	16
4.2 Configure Two-Way Audio.....	18
4.2.1 Two-Way Audio with Computer	18
4.2.2 Two-Way Audio with Software.....	18
Chapter 5 Network Configuration.....	19
5.1 Configure TCP/IP.....	19
5.2 Connect to Platform	20
5.3 Configure Port	21
Chapter 6 Safety Management	22
6.1 Manage User	22
6.1.1 Add User.....	22
6.1.2 Edit User	23
6.1.3 Delete User.....	24

6.2 Configure Security	25
Chapter 7 Maintenance	26
7.1 Configure Basic Information.....	26
7.2 Configure Time.....	26
7.3 Configure DST.....	27
7.4 Configure RS-232.....	28
7.5 Reboot	28
7.6 Restore Default Settings.....	29
7.7 Format Database	29
7.8 Export Configuration File	29
7.9 Import Configuration File.....	30
7.10 Upgrade	30
7.11 Configure and Export Log.....	31

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.



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.
- 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.

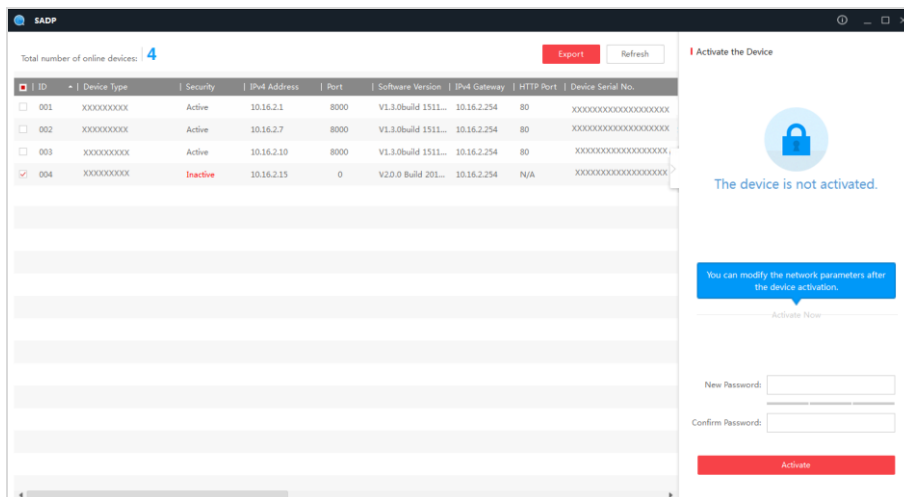


Figure 2-1 SADP Interface

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**.

Modify Network Parameters

Enable DHCP

Device Serial No.: XXXXXXXXXXXX

IP Address: 10.16.2.15

Port: 0

Subnet Mask: 255.255.255.0

Gateway: 10.16.2.254

IPv6 Address:

IPv6 Gateway:

IPv6 Prefix Length: 0

HTTP Port: 0

Security Verification

Admin Password: ●●●●●●●●

Modify

[Forgot Password](#)

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.

 A screenshot of a web browser's activation interface. The title bar at the top says "Activation". There are three input fields: "User Name" with the value "admin", "Password" (empty), and "Confirm" (empty). A red "X" icon is next to the Password field. Below the Password field, there is a text box with the following text: "Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained." An "OK" button is located at the bottom right of the form.

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 Operation

Click **Live View** to enter the Live View interface. You can control the connected barrier on the interface.

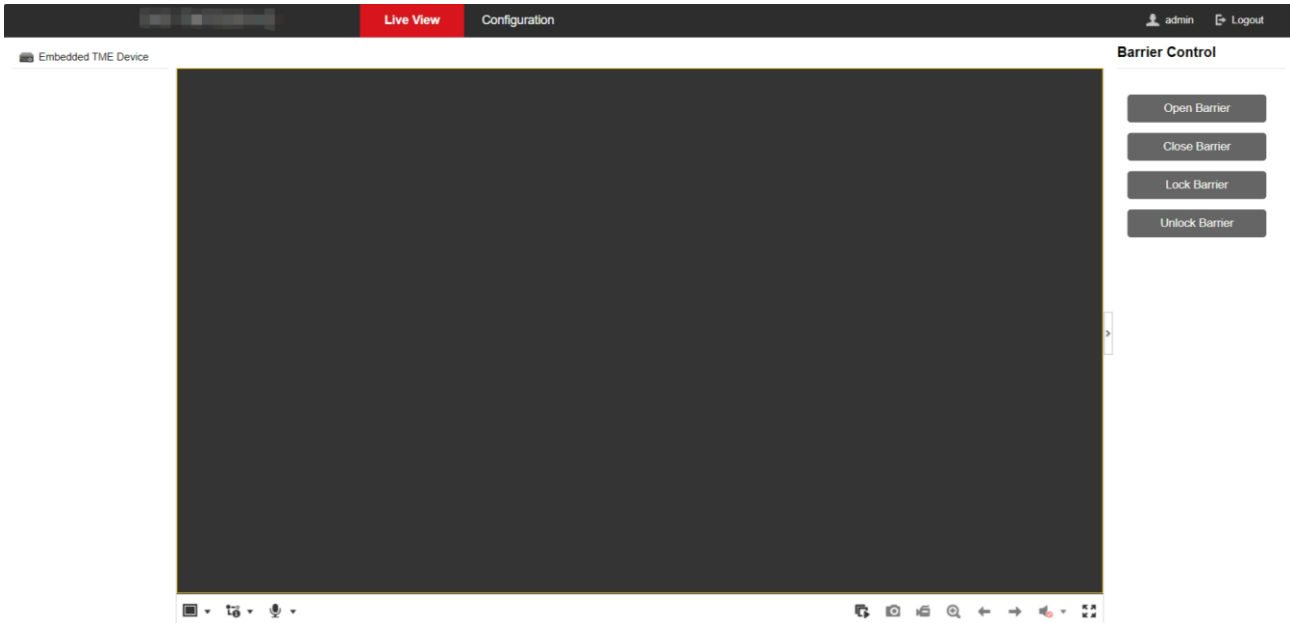


Figure 3-1 Live View

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

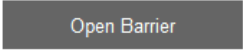
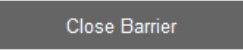
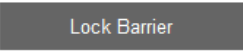
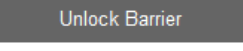
Icon	Description
	Open barrier.
	Close barrier.
	Lock barrier.
	Unlock barrier.

Table 3-1 Live View Icon Description

 **NOTE**

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

Chapter 4 Basic Operation

4.1 Configure Entrance & Exit Parameters

4.1.1 Configure Basic Parameters

You can configure the basic parameters for entrance and exit.

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

QR code display time	<input type="text" value="10"/>	s
Check Card Validity	<input type="checkbox"/>	
Get Card/ticket for Vehicle Without License Plate	<input type="checkbox"/>	

Figure 4-1 Basic Parameters

Step 2 Configure the following parameters according to your needs.

- **QR Code Display Time:** The display time of the QR code on the screen.
- **Check Card Validity:** If it is checked, the station will check whether the card is valid.
- **Get Card/Ticket for Vehicle Without License Plate:** For the vehicle without license plate, the station will play the voice prompt to remind the driver to take card or ticket.

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

4.1.2 Configure Ticket

You can configure the content on the ticket.



This function is only available to Entrance Station.

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



Title	<input type="text"/>
Contact No.	<input type="text"/>
Custom	<input type="text"/> 
Code Type	<input type="text" value="QR Code"/> 
Print License Plate Number	<input checked="" type="checkbox"/>
Print Entering Time	<input checked="" type="checkbox"/>
Print ticket number	<input checked="" type="checkbox"/>
	<input type="button" value="Print Test"/>

Figure 4-2 Ticket Configuration

Step 2 Enter **Title**, **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) Check **Print Ticket Number** to print the ticket number on the ticket.

Step 7 (Optional) Click **Print Test** to print the configured ticket to view the effect. The ticket format is shown below.



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

4.1.3 Configure Audio

You can configure the voice prompt.

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

Default Voice Prompt of Entrance/Exit

Select Voice

Volume

Start Time1

End Time1

Volume1

Start Time2

End Time2

Volume2

Start Time3

End Time3

Volume3

Content

Figure 4-3 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.

4.1.4 Configure Media

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

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

Video

Enable

File Upload (Note: Files support mp4/jpg format. after the import file need to restart to take effect)

ID	File Name	File Type	File Size	Operation

Figure 4-4 Media Configuration

Step 2 Check **Enable**.

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

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



- 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.

Result:

LCD will play the imported video automatically.

4.1.5 Configure Screen Display

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

Display Configuration		
Start Time1	00:00:00	
End Time1	05:59:59	
Passing Brightness1		2
Idle Brightness1		2
Start Time2	06:00:00	
End Time2	13:59:59	
Passing Brightness2		7
Idle Brightness2		7
Start Time3	14:00:00	
End Time3	17:59:59	
Passing Brightness3		7
Idle Brightness3		7
Start Time4	18:00:00	
End Time4	23:59:59	
Passing Brightness4		1
Idle Brightness4		1
Enable Loop Play	<input type="checkbox"/>	
Loop Interval (s)	<input type="text" value="0"/>	
Image Display Duration (s)	<input type="text" value="0"/>	

Figure 4-5 Display Configuration

Step 2 Set the display period on the screen, and set **Passing Brightness** and **Idle Brightness** 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 **Image Display Duration**.

Step 4 Click **Save**.

4.1.6 View Entrance & Exit Status

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



After the station is added to the 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.

Card Status

View card number, swiping card time, source, card status, card type, upload time, and upload result.

No.	Card No.	Swiping Card Time	Source	Card Status	Card Type	Upload Time	Upload Result
1	8443702842233	2023-11-07 15:52:46.275	Entrance Ticket		Ticket		
2	8443702837628	2023-11-07 15:51:59.966	Entrance Ticket		Ticket		

Synchronization Status

View synchronization mode, synchronization status, synchronization center, start time, and end time.

Synchronization Mode	Synchronization Status	Start Time	End Time	Synchronization Center

Passing Status

View mode, passing result, and passing time.

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

Peripheral Status

View the name and status of the peripheral devices.

Device Name	Device 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

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%

Induction

View the name and status of induction devices.


Device Name	Device Status
Sense Coil	No Vehicles

4.2 Configure Two-Way Audio

4.2.1 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.

4.2.2 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 4-6 Two-Way Audio

Step 2 Adjust the value.

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

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

Chapter 5 Network Configuration

5.1 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**.

The screenshot displays the configuration page for the network interface 'Lan1'. The 'NIC Type' is set to 'Auto'. The 'DHCP' checkbox is unchecked. The 'IPv4 Address', 'IPv4 Subnet Mask', and 'IPv4 Default Gateway' fields are empty. The 'IPv6 Address' field contains the value 'fe80::200:33ff:fea3:7559'. The 'IPv6 Default Gateway' field is empty. The 'MAC Address' field contains '00:00:33:a3:75:59'. The 'MTU' field contains '1500'. Below these fields is a 'DNS Server' section with 'Preferred DNS Server' set to '8.8.8.8' and 'Alternate DNS Server' empty. A red 'Save' button is located at the bottom of the configuration area.

Figure 5-1 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**.



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

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

5.2 Connect to Platform

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**.

<input type="checkbox"/> Enable	
Platform Access Mode	ISUP5.0
Server IP	0.0.0.0
Server Port	0
Device ID	@
Register Status	Offline

Figure 5-2 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**.



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**.

5.3 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**.

HTTP Port	<input type="text" value="80"/>
RTSP Port	<input type="text" value="554"/>
Server Port	<input type="text" value="8000"/>

Figure 5-3 Port Configuration

Step 2 View the port parameters.

Chapter 6 Safety Management

6.1 Manage User

6.1.1 Add User

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



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**.

The screenshot shows a web interface titled "User Management". At the top, there is a "User List" header with three buttons: "Add", "Modify", and "Delete". Below the header is a table with three columns: "No.", "User Name", and "Level". The table contains one row with the following data: "1" in the "No." column, "admin" in the "User Name" column, and "Administrator" in the "Level" column.

No.	User Name	Level
1	admin	Administrator

Figure 6-1 User Management

Step 2 Click **Add**.

Figure 6-2 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.

6.1.2 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**.

Modify User [X]

User Name: admin

Admin Password: []

Level: Administrator

Password: [] Strong

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Confirm: []

- Select All
- Local: Upgrade/Format
- Local: Shutdown/Reboot
- Local: Parameters Settings
- Local: Manual Operation
- Remote: Parameters Settings
- Remote: Upgrade / Format
- Remote: Two-Way Audio
- Remote: Shutdown / Reboot
- Remote: Notify Surveillance Center / Trig...
- Remote: Serial Port Control
- Remote: Manual Record

OK Cancel

Figure 6-3 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.

6.1.3 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.

6.2 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**.

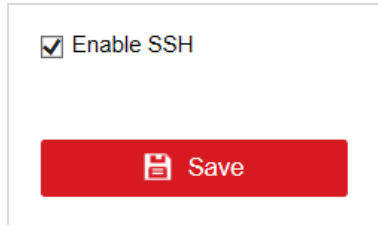


Figure 6-4 Security Configuration

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

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

Chapter 7 Maintenance

7.1 Configure Basic Information

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

Device Name	<input type="text"/>
Device No.	<input type="text" value="255"/>
Model	<input type="text"/>
Serial No.	<input type="text"/>
Firmware Version	<input type="text"/>
Encoding Version	<input type="text"/>
Web Version	<input type="text"/>
Plugin Version	<input type="text"/>
Number of Channels	<input type="text" value="1"/>
Number of HDDs	<input type="text" value="0"/>
Number of Alarm Input	<input type="text" value="4"/>
Number of Alarm Output	<input type="text" value="4"/>

Figure 7-1 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.

7.2 Configure Time

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

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore ▾

NTP

NTP

Server Address

NTP Port

Interval minute(s)

Manual Time Sync.

Manual Time Sync.

Device Time



Set Time  Sync. with computer time

Figure 7-2 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.

7.3 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**.

7.4 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**.

Baud Rate	115200	▼
Data Bit	8	▼
Stop Bit	1	▼
Parity	None	▼
Flow Ctrl	None	▼
Usage	Console	▼

Figure 7-3 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**.

7.5 Reboot

You can reboot the station.

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

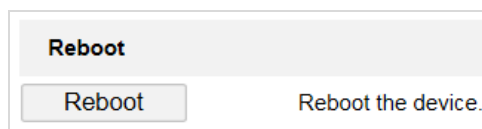


Figure 7-4 Reboot

Step 2 Click **Reboot**.

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

7.6 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**.

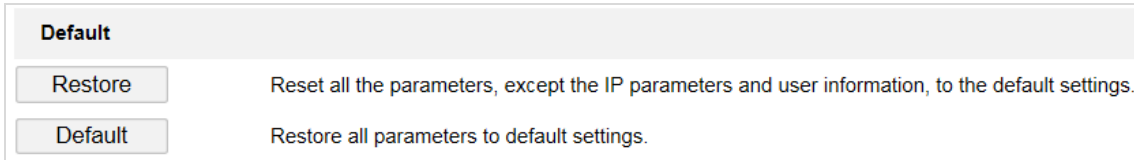


Figure 7-5 Restore Default Settings

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.

7.7 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**.

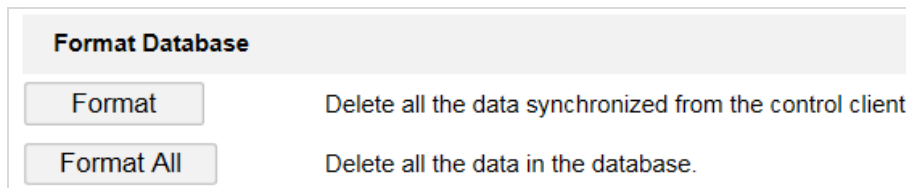


Figure 7-6 Format Database

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.

7.8 Export Configuration File

You can export the configuration file of the station.

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

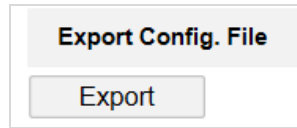


Figure 7-7 Export Configuration File

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.

7.9 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 7-8 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.

7.10 Upgrade

You can upgrade the station.

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



Figure 7-9 Upgrade

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

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



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

7.11 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**.

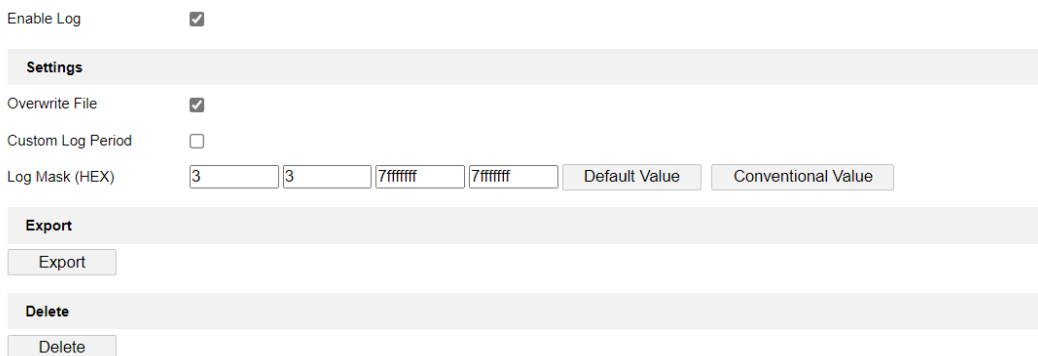


Figure 7-10 Log Configuration

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.



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.

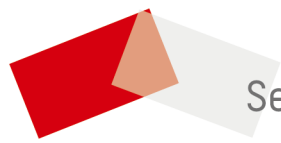
Step 5 (Optional) Click **Delete** to delete the log file.



NOTE

Back up the data before deleting the log file.

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



See Far, Go Further