



Card Reader Intercom Station

User Manual

Legal Information

About this Document

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

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- 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
 Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Contents

Chapter 1 Activation and Login	1
1.1 Activation.....	1
1.1.1 Default Information	1
1.1.2 Activate via HiTools Delivery	1
1.1.3 Activate via Web Browser.....	3
1.2 Login.....	3
1.3 Download Plug-in	4
Chapter 2 Network Configuration	5
2.1 Set IP Address	5
2.2 Set Port	6
2.3 Set DDNS.....	7
2.4 Set QoS.....	8
2.5 Data Connection	9
2.5.1 Set ISAPI Listening	9
2.5.2 Set Arming Upload	9
2.5.3 Set SDK Listening	9
2.5.4 Connect to ISUP Platform	10
2.5.5 Connect to OTAP	11
2.5.6 Connect to Hik-Connect	13
2.5.7 Connect to SIP Platform	15
Chapter 3 Capture Configuration	17
3.1 Set Barrier Gate Parameters	17
3.2 Set Voice Prompt.....	19
3.3 Set Card Reader Event.....	20
3.4 View Alarm Input Status	22
3.5 Advanced Configuration.....	22
3.5.1 System Service.....	22
Chapter 4 Data	23
4.1 Manage Card No. List	23

4.2 Search Card Records	24
Chapter 5 Exception Alarm	26
Chapter 6 Safety Management	27
6.1 Manage User	27
6.2 Enable User Lock	28
6.3 Set SSH	28
6.4 Prohibit PING	29
6.5 Set Timeout Logout	29
6.6 Set Password Validity Period	29
6.7 Set IP Address Filtering	30
6.8 Set HTTPS	30
6.8.1 Create and Install Self-signed Certificate	30
6.8.2 Install Authorized Certificate	30
Chapter 7 Maintenance	32
7.1 View Device Information	32
7.2 Synchronize Time	33
7.3 Set DST	34
7.4 Set RS-232	34
7.5 Download Debug Data	35
7.6 Enable System Log Service	35
7.7 Reboot	36
7.8 Restore Parameters	36
7.9 Export Parameters	36
7.10 Import Configuration File	37
7.11 Upgrade	37

Chapter 1 Activation and Login

1.1 Activation

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. The device supports multiple activation methods, such as activation via HiTools Delivery, web browser, and iVMS-4200 Client.



Note

Refer to the user manual of iVMS-4200 Client for the activation via client software.

1.1.1 Default Information

The device default information is shown as below.

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

1.1.2 Activate via HiTools Delivery

HiTools Delivery aims to streamline and enhance the activation, networking, and batch configuration for various devices. You can use the software to detect, activate, and modify the IP addresses of multiple devices over the LAN.

Before You Start

- Set the device and the computer that runs the software to the same network segment.
- Access the official website (<https://www.hikvision.com/en>) and enter **Support** → **Download** → **Software** → **HiTools** → **HiTools Delivery** to download HiTools Delivery and install it according to the prompts.

Steps

1. Run the software.
2. Click **Home Page** → **Search** → **Current Subnet**. Click **Refresh**, and the list will display all the online devices in the same network segment.
3. Select the inactive device(s) in the list. Set a new password according to the popup requirements and confirm the password.
4. Click **Activation**. The device activation status will change to **Activated** after successful activation.

Card Reader Intercom Station User Manual

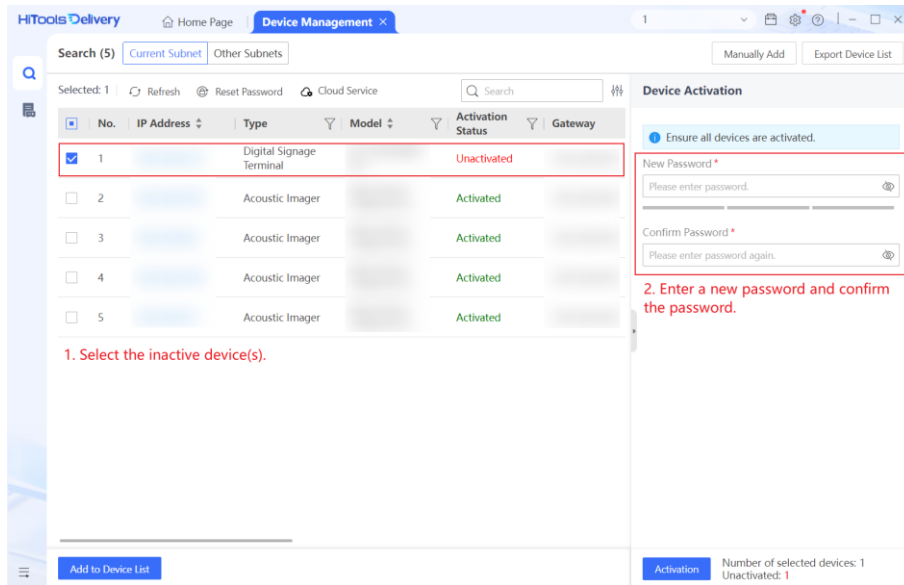


Figure 1-1 Activation

5. Optional: Change the IP address of the device.

- 1) On **Current Subnet** interface, select multiple devices that need to change the IP addresses.
- 2) On the right **Network Parameter** window, set the start IP address, port No., IPv4 subnet mask, IPv4 gateway, etc., and the selected devices will be automatically assigned to increasing IP addresses. Or check **Enable DHCP** to assign dynamic IP addresses.
- 3) Enter the admin password and click **OK**.

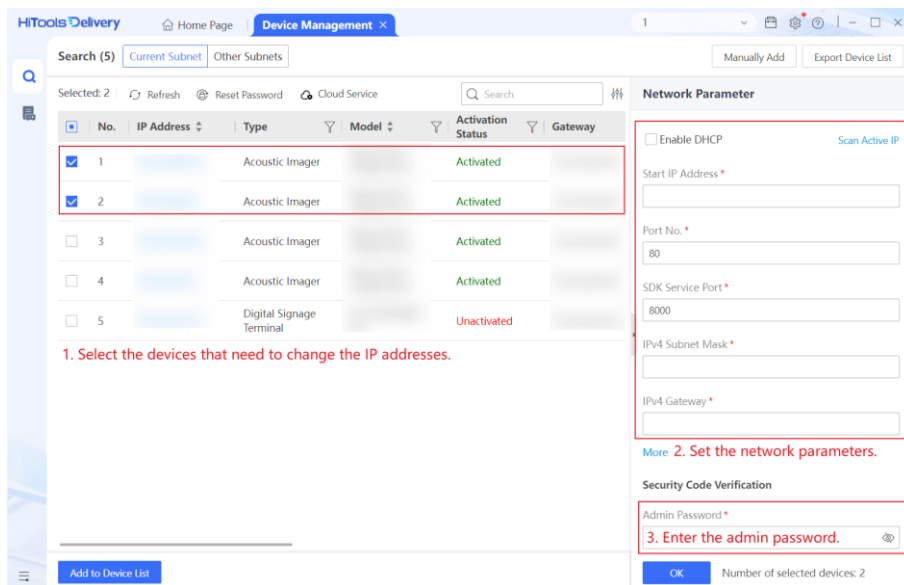


Figure 1-2 Modify Network Parameters

Note

- Set the device IP address to the same network segment with that of your computer.
- You can click **Scan Active IP** to detect and view the available IP addresses. Refer to the help of

HiTools Delivery for details.

- You can also click **Home Page** → **Maintenance** → **Change IP** to change the IP addresses in batch by exporting and importing the template. Refer to the help of HiTools Delivery for details.
-

1.1.3 Activate via Web Browser

Use web browser to activate the device. For the device with the DHCP enabled by default, use SADP software or client software to activate the device.

Before You Start

Ensure the device and the computer are in the LAN with the same network segment.

Steps

1. Change the IP address of your computer to the same network segment as the device.
 2. Open the web browser, and enter the default IP address of the device to enter the activation interface.
 3. Create and confirm the admin password.
-



Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click **OK** to complete activation.
5. Go to the network settings interface to modify IP address of the device.

1.2 Login

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

Before You Start

Connect the device to the network directly, or via a switch or a router.

Steps

1. Open the web browser, and enter the IP address of the device to enter the login interface.
 2. Optional: Select the language.
 3. Enter **User Name** and **Password**.
 4. Click **Login**.
-

Note

- If live view failed, click  on the upper right corner of the interface to download the plug-in and install it.
 - Close the web browser to install the plug-in, or the installation may fail. If you still cannot realize live view after installing the plug-in, try to uninstall the plug-in and reinstall.
-

5. Reopen the web browser after the installation of the plug-in and repeat steps 1 to 4 to login.
6. Optional: Click  on the upper right corner of the interface to log out of the device.

1.3 Download Plug-in

No plug-in mode is enabled by default. In no-plug in mode, "No Plug-in Mode" prompt will appear on the upper right corner of the interface. You can click  to download the plug-in. Close the browser to install the plug-in to the computer. Then access to the IP address of the device again, and the "No Plug-in Mode" prompt will disappear from the upper right corner of the interface.

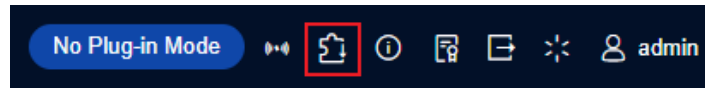


Figure 1-3 Download Plug-in

Chapter 2 Network Configuration

2.1 Set IP Address

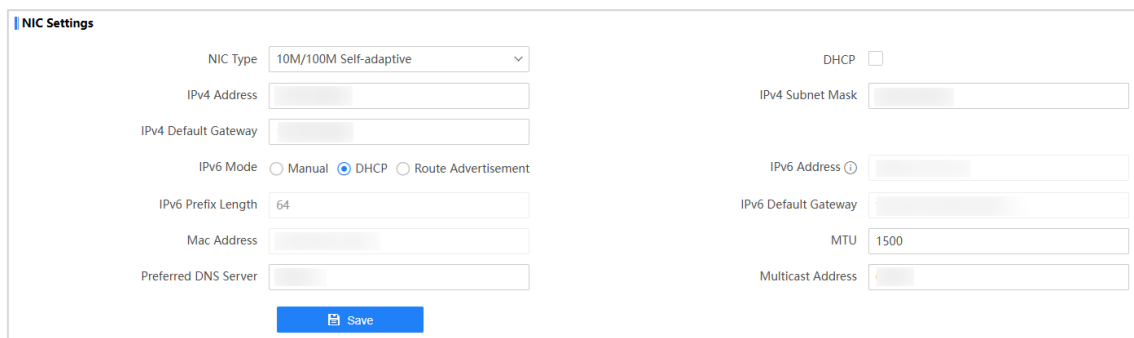
IP address must be properly configured before you operate the device over network. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.

Steps



The supported parameters vary with different models. The actual device prevails.

1. Go to **Configuration** → **Network** → **Network Parameters** → **Network Interface**.



The image shows a 'NIC Settings' configuration window. It contains two columns of settings. The left column includes: 'NIC Type' (a dropdown menu set to '10M/100M Self-adaptive'), 'IPv4 Address' (a text input field), 'IPv4 Default Gateway' (a text input field), 'IPv6 Mode' (radio buttons for 'Manual', 'DHCP' (which is selected), and 'Route Advertisement'), 'IPv6 Prefix Length' (a text input field set to '64'), 'Mac Address' (a text input field), and 'Preferred DNS Server' (a text input field). The right column includes: 'DHCP' (a checkbox), 'IPv4 Subnet Mask' (a text input field), 'IPv6 Address' (a text input field with a circular icon to its left), 'IPv6 Default Gateway' (a text input field), 'MTU' (a text input field set to '1500'), and 'Multicast Address' (a text input field). At the bottom center is a blue 'Save' button with a floppy disk icon.

Figure 2-1 Set IP Address

2. Set network parameters.

NIC Type

Select a NIC (Network Interface Card) type according to your network condition.

IPv4

Two modes are available.

DHCP

The device automatically gets the IP parameters from the network if you check **DHCP**. The device IP address is changed after enabling the function. You can use SADP to get the device IP address.



The network that the device is connected to should support DHCP (Dynamic Host Configuration Protocol).

Manual

You can set the device IP parameters manually. Enter **IPv4 Address**, **IPv4 Subnet Mask**, and **IPv4 Default Gateway**.

IPv6

Three IPv6 modes are available.

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.



Note

Route advertisement mode requires the support from the router that the device is connected to.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Enter **IPv6 Address**, **IPv6 Prefix Length**, and **IPv6 Default Gateway**. Consult the network administrator for required information.

MTU

It stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.

The valid value range of MTU is 1280 to 1500.

Multicast Address

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneously. After setting the IP address of the multicast host, you can send the source data efficiently to multiple receivers.

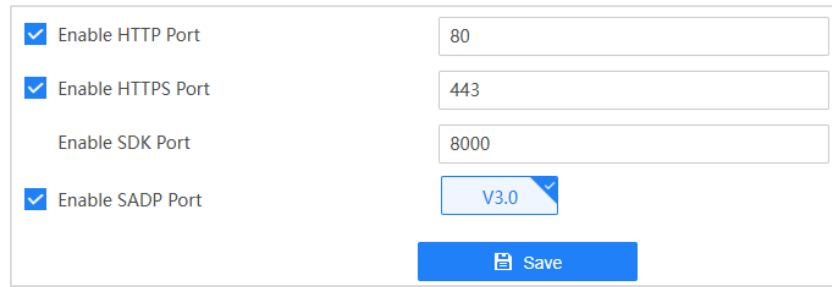
DNS

It stands for domain name server. It is required if you need to visit the device with domain name. And it is also required for some applications (e.g., sending email). Set **Preferred DNS Address** properly if needed.

3. Click **Save**.

2.2 Set Port

The device port can be modified when the device cannot access the network due to port conflicts. Go to **Configuration** → **Network** → **Network Parameters** → **Port** for port settings.



☒ Enable HTTP Port	80
☒ Enable HTTPS Port	443
☐ Enable SDK Port	8000
☒ Enable SADP Port	V3.0

Save

Figure 2-2 Set Port

Enable HTTP Port

It refers to the port through which the browser accesses the device. For example, when the HTTP port is modified to 81, you need to enter ***http://192.168.1.64:81*** in the browser address bar for login.

Enable HTTPS Port

It refers to the port through which the browser accesses the device, but certificate verification is needed.

Enable SDK Port

It refers to the port through which the client adds the device.

Enable SADP Port

It refers to the port through which the SADP software searches the device. Select the SADP version.

Note

- After editing the port, access to the device via the new port.
 - Reboot the device to bring the new settings into effect.
 - The supported ports vary with different models. The actual device prevails.
-

2.3 Set DDNS

You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

Before You Start

- Register the domain name on the DDNS server.
- Set the LAN IP address, subnet mask, gateway, and DNS server parameters. Refer to **[Set IP Address](#)** for details.
- Complete port mapping. The default ports are 80, 8000, and 554.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **DDNS**.

2. Enable DDNS.

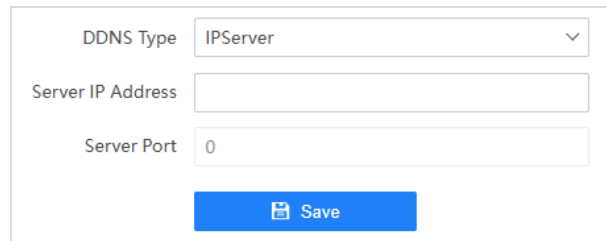


Figure 2-3 Set DDNS

3. Enter the server address and other information.

Note

You can select **IPServer**, **DynDNS**, and **NO-IP** for the DDNS type.

4. Click **Save**.

5. Access the device.

By Browsers

Enter the domain name in the browser address bar to access the device.

By Client Software

Add domain name to the client software. Refer to the client software manual for specific adding methods.

2.4 Set QoS

QoS (Quality of Service) can help improve the network delay and network congestion by setting the priority of data sending.

Note

QoS needs support from network devices such as routers and switches.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **QoS**.
 2. Enable DSCP according to the actual needs and set the value.
-

Note

Network can identify the priority of data transmission. The bigger the DSCP value is, the higher the priority is. Same settings need to be set in the router for configuration.

3. Click **Save**.

2.5 Data Connection

2.5.1 Set ISAPI Listening

ISAPI listening and SDK listening are mutually exclusive protocols. If you enable the picture uploading listening, the device will transmit images via the SDK listening. If not, the device will upload images via ISAPI protocol after the ISAPI parameters are set.

Before You Start

The listening service has been enabled for the ISAPI host, and the network communication with the device is normal.

Steps

1. Go to **Configuration** → **Network** → **Data Connection** → **ISAPI Listening**.
2. Enable **ISAPI**.

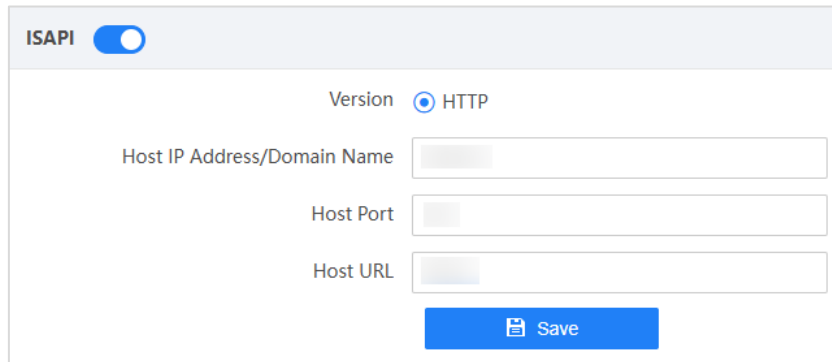


Figure 2-4 Set ISAPI Listening

3. Select **Version**.
4. Set **Host IP Address/Domain Name**, **Host Port**, and **Host URL**.
5. Click **Save**.

2.5.2 Set Arming Upload

Go to **Configuration** → **Network** → **Data Connection** → **Arm Upload**. The other platforms can arm and connect the device via the SDK protocol.

2.5.3 Set SDK Listening

The SDK listening can be used to receive the uploaded information and pictures of the device arming alarm.

Before You Start

The listening service has been enabled for the SDK listening, and the network communication with the device is normal.

Steps

1. Go to **Configuration** → **Network** → **Data Connection** → **SDK Listening**.
2. Enable SDK listening.

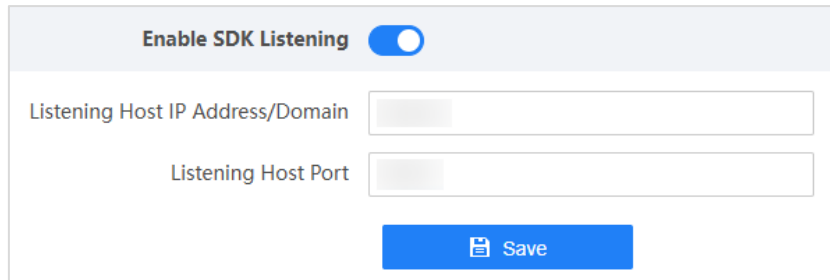
The screenshot shows a configuration window titled 'Enable SDK Listening' with a toggle switch turned on. Below the title, there are two input fields: 'Listening Host IP Address/Domain' and 'Listening Host Port'. At the bottom right of the window is a blue button with a floppy disk icon and the text 'Save'.

Figure 2-5 Set SDK Listening

3. Set **Listening Host IP Address/Domain** and **Listening Host Port** if you need to upload the alarm information and pictures.
4. Click **Save**.

2.5.4 Connect to ISUP Platform

ISUP is a platform access protocol. The device can be remotely accessed via this platform.

Before You Start

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

Steps

1. Go to **Configuration** → **Network** → **Data Connection** → **ISUP**.
2. Enable **ISUP Platform Index**.

ISUP Platform Index ☒

Protocol Version v5.0

Address Type IP Address

Server Port

Device ID

Encryption Key

8 to 32 letters or digits, case sensitive. You are recommended to use a combination of letters or digits.

Registration Status Offline

	Server Type	Server IP Address	Server Port	Upload Type
Platform Status Alarm Ser...			1	Upload D
Picture Se...			1	Upload D

Save

Figure 2-6 Connect to ISUP Platform

3. Select **Protocol Version**.
4. Select **Address Type** and enter IP address or domain name of the platform.
5. Enter **Server Port**, **Device ID**, and **Encryption Key**.

 Note

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

6. Click **Save**.

What to do next

When the registration status shows online, you can add or manage the device via the platform software.

2.5.5 Connect to OTAP

The device can be accessed to the maintenance platform via OTAP protocol, in order to search and acquire device information.

Before You Start

- Set the network parameters including device IP address, gateway, DNS, etc. to get access to the network.
- Disable the other platform accesses conflicting with OTAP.

Steps

1. Go to **Configuration** → **Network** → **Data Connection** → **OTAP**.
2. Select **Platform Access Mode** as **Private Deployment**.
3. Enable **OTAP Server**.

OTAP Server ☒

Address Type: Domain Name

Server Port:

Device ID:

Key:

Warning:

- 1. 8 to 16 characters allowed.
- 2. At least 2 types of the following characters should be contained: uppercase letters, lowercase letters, numbers, and special characters.
- 3. The password cannot contain the user name itself, 123, or admin.
- 4. The password cannot contain continuous increasing or descending numbers of 4 characters or above, or the same symbols.
- 5. The password cannot contain the following phrases connected by letters: hik, hkws, hikvision (case-insensitive).

Registration Status: Offline

Figure 2-7 Connect to OTAP

4. Set corresponding parameters.

Address Type

Select the address type of the connected platform or server, and enter the IP address or domain name.

Server Port

The port of the connected platform or server.

Device ID

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

Key

Set a custom key to encrypt the data connection between the device and the platform or server.

5. Click **Save**.

What to do next

When the registration status is online, you can add or manage the device via the platform software.

2.5.6 Connect to Hik-Connect

The device can be remotely accessed via Hik-Connect.

Before You Start

- Set the network parameters including device IP address, gateway, DNS, etc. to get access to the network.
- OTAP connection is disabled.

Steps

1. Enable Hik-Connect in two ways.
 - Get access to Hik-Connect V2.0. Go to **Configuration** → **Network** → **Data Connection** → **OTAP**, and select **Platform Access Mode** as **Hik-Connect**. Enable the function.

Enable ☒

Server Domain Name ☐ Custom

Registration Status Offline

Offline Reason Unknown

Offline Code 0

Binding Status Unknown

Verification Code

Enable Video Encryption ☒

Video Encryption Password

8 to 32 letters or digits, case sensitive. You are recommended to use a combination of letters or digits.

Confirm Video Encryption Password

Figure 2-8 Connect to Hik-Connect (V2.0)

- Get access to Hik-Connect V3.0. Go to **Configuration** → **Network** → **Data Connection** → **Hik-Connect Platform**. Enable **Hik-Connect Platform**.

Server Domain Name ☐ Custom

Registration Status **Offline**

Offline Reason Unknown

Offline Code 0

Binding Status Unknown

Verification Code

Enable Video Encryption ☒

Video Encryption Password

Confirm Video Encryption Password

! 8 to 32 letters or digits, case sensitive. You are recommended to use a combination of letters or digits.

! You need to set the network parameters including device IP address, gateway, DNS, etc. to get access to the network.

Figure 2-9 Connect to Hik-Connect (V3.0)

- Optional: If you have allocated a custom server, check **Custom** and enter the custom **Server Domain Name**.
- Enter a custom **Verification Code** used to add the device via **Hik-Connect**.

 Caution

The verification code should be 6 letters or digits, case sensitive. You are recommended to use a combination of letters or digits.

- Optional: Check **Enable Video Encryption** and set **Video Encryption Password** to encrypt the videos transmission. Confirm the password.
- Click **Save**.
- Add the device to Hik-Connect.
 - Get and install Hik-Connect application by the following ways.
 - Visit <https://appstore.hikvision.com> to download the application according to your mobile phone system.
 - Visit the official site of our company. Then go to **Support** → **Tools** → **Installation & Maintenance Tools** → **Hikvision APP Store**.
 - Scan the QR code below to download the application.



Figure 2-10 Hik-Connect

 Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit <https://appstore.hikvision.com/static/help/index.html> to refer to the troubleshooting.
- Visit <https://appstore.hikvision.com/>, and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

-
- 2) Start the application and register a user account to log in.
 - 3) Add device by the serial No. on the device body and the verification code.

 Note

Refer to the user manual of Hik-Connect application for details.

2.5.7 Connect to SIP Platform

You can connect the device to SIP platform to realize intercom.

Before You Start

Ensure the device can communicate normally with the platform.

Steps

1. Go to **Configuration** → **Network** → **Data Connection** → **SIP**.
2. Enable **SIP**.

Enable SIP ☒

Local SIP Port

SIP Server ID

SIP Server Domain

SIP Server IP Address

SIP Server Port

SIP Authentication ID

Registration Expiration (s)

3600

Heartbeat Period(s)

60

Max. Times of Heartbeat Timeout

3

Registration Status

Not Registered

 Save

Figure 2-11 Connect to SIP Platform

3. Set SIP server parameters according to the SIP protocol.
4. Click **Save**.

Chapter 3 Capture Configuration

3.1 Set Barrier Gate Parameters

Set the barrier gate control mode, alarm output, linked I/O, linked Wiegand, and time period of keeping the barrier gate open.

Steps

1. Go to **Configuration** → **Capture** → **Entrance and Exit** → **Barrier Gate**.

The screenshot shows the 'Barrier Gate' configuration page. At the top, there's a 'Control Mode' section with three radio buttons: 'Device Control Mode' (unselected), 'Platform Control Mode' (selected), and 'Device Control Mode' (unselected). Below this is the 'Barrier Gate Remote Control' section, which includes four 'Alarm Output' dropdown menus (Alarm Output1 to Alarm Output4) and three buttons: 'Rise', 'Lock Barrier', and 'Unlock Barrier'. The 'Barrier Gate Linked I/O' section has four dropdown menus for 'Barrier Gate Linked I/O No.1' through 'No.4'. The 'Barrier Gate Linked Wiegand' section includes a 'Filter Invalid Card' checkbox, a 'Filter Time(s)' input field (set to 3), a 'Remote Card Wiegand Access Mode' dropdown (set to 'Wiegand 34'), a 'Card No. Filter Mode' dropdown (set to 'Card Reader Filter Mode'), a 'Card Mode (Hexadecimal and Decimal)' dropdown (set to 'Decimal'), and a 'Write card encryption enable' checkbox. The 'Barrier Setting' section at the bottom has a 'Barrier Period' label and a 'Set Time Period' button.

Figure 3-1 Set Barrier Gate Parameters

2. Select **Control Mode**.

Device Control Mode

Vehicle passing is controlled by the device.

Platform Control Mode

All the cards read by the card reader will be reported to the platform.

3. Set **Barrier Gate Remote Control**.

- 1) Select the barrier gate control mode from the drop-down list according to the actual wiring of the device's alarm output interfaces and barrier gates.
 - 2) Click the buttons behind the drop-down boxes to control the barrier gates.
 - If the control signal is **Rise**, you can rise, lock, or unlock the barrier gate.
- Lock Barrier:** The barrier gate remains open, and cannot be closed.

Unlock Barrier: The barrier gate is unlocked, and can be closed.

- If the control signal is **Fall**, you can only fall the barrier gate.

4. Select **Barrier Gate Linked I/O** from the drop-down list according to the actual wiring of the device's alarm input interfaces.
5. Set **Barrier Gate Linked Wiegand** parameters.

Filter Invalid Card

In device control mode, check it to filter invalid cards.

Card No. Filter Mode

Select the mode for filtering the same card No. within the set **Filter Time**. **Card Reader Filter Mode** filters the same card No. by the connected card reader, while **Control Station Filter Mode** filters the same card No. of all card readers.

Card Mode:

Decimal and Hexadecimal are selectable.

Remote Card Wiegand Access Mode

Wiegand 26 and Wiegand 34 are selectable.



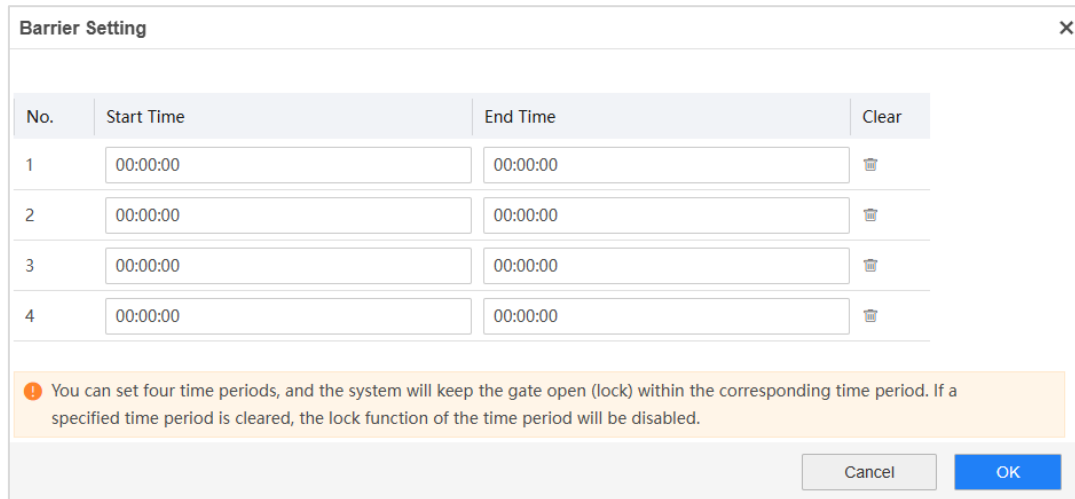
Note

- In decimal card mode, if Wiegand 26 is selected, the card No. should be an 8-digit decimal number. If Wiegand 34 is selected, the card No. should be a 10-digit decimal number.
 - In hexadecimal card mode, if Wiegand 26 is selected, the card No. should be a 6-digit hexadecimal number. If Wiegand 34 is selected, the card No. should be an 8-digit hexadecimal number.
 - The Wiegand access mode settings take effect after you reboot the device.
-

Write card encryption enable

Enable the function and set the key to write encrypted card numbers.

6. Click **Set Time Period** to set time periods to control barrier gate.



Barrier Setting

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

You can set four time periods, and the system will keep the gate open (lock) within the corresponding time period. If a specified time period is cleared, the lock function of the time period will be disabled.

Cancel OK

Figure 3-2 Set Time Periods to Control Barrier Gate

- 1) Set the start time and end time, and the system will keep the barrier gate open within the set time period.
- 2) (Optional) Click to clear the specified time period, and the barrier gate lock function of the time period will be disabled.

Note

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

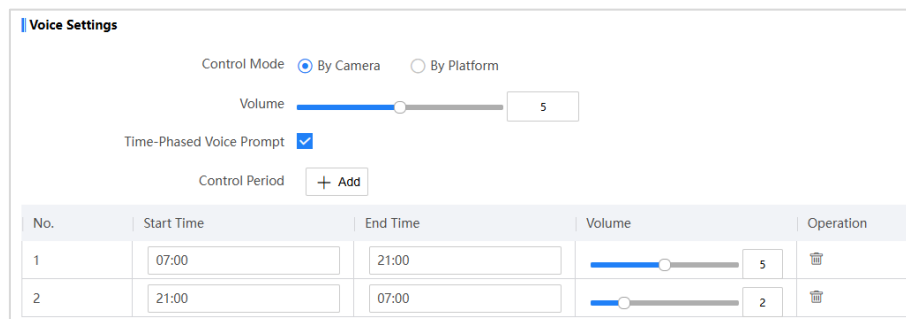
7. Click **Save**.

3.2 Set Voice Prompt

The device is equipped with the loudspeaker. You can set the voice prompt.

Steps

1. Go to **Configuration** → **Capture** → **Entrance and Exit** → **Voice Prompt**.
2. Set voice prompt parameters.



Voice Settings

Control Mode ☒ By Camera ☐ By Platform

Volume 5

Time-Phased Voice Prompt ☒

Control Period Add

No.	Start Time	End Time	Volume	Operation
1	07:00	21:00	5	
2	21:00	07:00	2	

Figure 3-3 Set Voice Prompt Parameters

Control Mode

- **By Platform:** Select this mode in the scene in which the entry permissions are controlled by the software.
- **By Camera:** Select this mode in standalone scene (no control software) and allowlist scene in which the device controls the barrier gate.

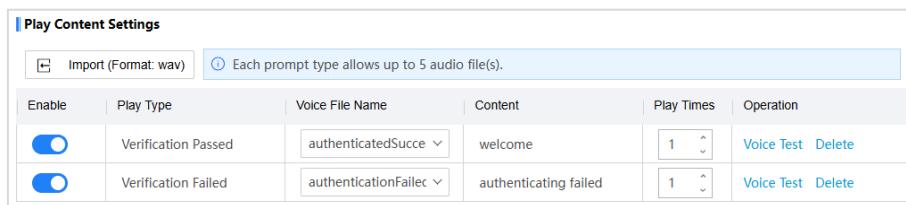
Volume

Adjust the voice volume.

Time-Phased Voice Prompt

Enable the function to play the voice prompt at fixed time period. Click **Add** to add a time period. Set **Start Time** and **End Time** of the time period, and adjust **Volume**. You can click  to delete the time period.

3. Import the voice prompt files.



Enable	Play Type	Voice File Name	Content	Play Times	Operation
☒	Verification Passed	authenticatedSucce	welcome	1	Voice Test Delete
☒	Verification Failed	authenticationFalle	authenticating failed	1	Voice Test Delete

Figure 3-4 Import Voice Prompt Files

- 1) Click **Import**.
- 2) Enter **Content**.
- 3) Select **Play Type** for the play content.
- 4) Click **Browse** to select the voice prompt file from the computer, and click **Import** to import it to the device.
- 5) Repeat the steps above to import more voice prompt files.
- 6) Enable the voice prompt(s).
- 7) Optional: Click **Voice Test** to test the actual voice prompt effect. Click **Delete** to delete it.

Note

- Each prompt type allows up to 5 audio file(s).
- Mono audio files in .wav format with 16-bit depth and 8 kHz sampling rate allowed.

4. Click **Save**.

3.3 Set Card Reader Event

Set the card reader event to control barrier gates via card readers or platform.

Steps

1. Go to **Configuration** → **Capture** → **Entrance and Exit** → **Card Reader Event**.

Reader1

Reader2

Reader3

Reader4

Card Reader Name

Reader1

Enable Card Reader

☒

Alarm Input Linkage

NO	1	2	3	4
Alarm Input Control	None	None	None	None
Enable	☐	☐	☐	☐

Linkage Target

Registered Card

Temporary Card

Invalid Card

Unregistered Card

NO	1	2	3	4
Card Status	Rise	None	None	None
Normal	☐	☐	☐	☐
Expired	☐	☐	☐	☐
Report Card Loss	☐	☐	☐	☐
Logout	☐	☐	☐	☐

Platform Management

Alarm Output No.	1	2	3	4
Alarm Output	Rise Lock Unlock	None	None	None
Enable	☒	☐	☐	☐

Figure 3-5 Card Reader Event

- Click the corresponding card reader No, set **Card Reader Name**, and check **Enable Card Reader**.
- Select the function of the corresponding alarm input No. Enable corresponding alarm input No. to trigger card reading. If the corresponding alarm input linked I/O is detected, the card reader can be triggered to read cards. For example, if you enable alarm input No.2 and its linked I/O is closing limit, the card reader can read cards only when the barrier gate is in closing limit.
- Click corresponding card type and enable the card status for the corresponding alarm output No. For example, if you select registered card type and normal card status for alarm output No.1, and the barrier gate remote control for alarm output No. 1 is **Rise**, the barrier gate will be triggered to rise when normal registered cards are read.
- To control the barrier gates from the platform, enable corresponding Alarm Output No. for Platform Management. You can also select **Lock** or **Unlock** if the barrier gate remote control for the corresponding alarm output No. is **Rise**. For example, if you enable alarm output No. 1 and its barrier gate remote control is **Rise**, and select **Lock** and **Unlock** next to **Rise**, and then you can rise, lock, and unlock the barrier gate via the platform.
- Click **Save**.

Note

- The alarm input No. for each card reader cannot conflict.
- Up to four card readers are supported.
- The settings take effect after you reboot the device.

3.4 View Alarm Input Status

View the device name and device status of the corresponding alarm input No.

Steps

1. Go to **Configuration** → **Capture** → **Entrance and Exit** → **AlarmIn Status**.
2. View the device name and device status of the corresponding alarm input No.

Note

The device name refers to the selected function for each alarm input No. in **Configuration** → **Capture** → **Entrance and Exit** → **Card Reader Event** → **Alarm Input Linkage**. Refer to step 3 of **3.3 Set Card Reader Event** for details.

Alarm Input	Device Name	Device Status
1	NONE	NONE
2	NONE	NONE
3	NONE	NONE
4	NONE	NONE

Figure 3-6 Alarm Input Status

3.5 Advanced Configuration

Note

The advanced configurations below are only provided to debug the device by the professionals.

3.5.1 System Service

The onsite technicians can enter debug commands to debug device.

Steps

1. Go to **Configuration** → **Capture** → **Advanced** → **System Service**.
2. Enter **cmdIndex** and **cmdValue**.
3. Click **Save**.

Chapter 4 Data

4.1 Manage Card No. List

You can add, import, export, and delete cards.

Steps

1. Go to **Data** → **Card No. List**.
2. Click **Add**.

The screenshot shows a software window titled "Add" with a close button (X) in the top right corner. Inside the window, there is a section labeled "Basic Information". This section contains several input fields and buttons:

- Card No.:** A text input field.
- Card Type:** A dropdown menu currently showing "Registered Card".
- Card Status:** A dropdown menu currently showing "Normal".
- Effective Date:** A date and time input field showing "2026-03-24 00:00:00".
- Expiry Date:** A date and time input field showing "2027-03-24 23:59:59".
- Action Buttons:** Two buttons are located to the right of the Card No. field: "Read Card No. and Sto..." and "Write to Card and Store...".
- Validity Period Buttons:** Four buttons are located below the Expiry Date field: "One Month", "Three Months", "Half a Year", and "One Year".
- Footer Buttons:** At the bottom right of the window are "Cancel" and "OK" buttons.

Figure 4-1 Add Card

3. Set the basic information for the card.

Card No.

Enter the card No. manually, or click **Write to Card and Store Card** to write a card No. automatically. 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.

Card Type

Registered Card, Temporary Card, and Invalid Card are selectable.

Effective Date

Set the start time of the effective date.

Expiry Date

Set the expiry date, or select the validity period.

Note

- To write card No., connect a card enrollment station to your computer first, and then click  on the upper right corner of the interface to download the plug-in of the card reader.
- When writing card No. automatically, the card No. cannot be modified.
- It is recommended to enable write card encryption in **Configuration** → **Capture** → **Entrance and Exit** → **Barrier Gate**, otherwise the card No. will be generated in ascending order.

- Click **OK** to add the card.
- (Optional) Other operations.
 - Click  under the **Operation** column to edit the card information.
 - Click  under the **Operation** column to delete the corresponding card.
 - Select the card(s) to be deleted, and click **Delete** to delete in batch.
 - Set the search conditions and click **Search** to search the cards. The cards satisfying the search conditions will be listed below.

Card No.

Card Type

ALL

Card Status

ALL

Search

Add

Import

Export

Delete

☐	No.	Card No.	Card Type	Card Status	Effective Date	Expiry Date	Operation
☐	1		Registered Card	Expired	2026-01-08 00:00:00	2026-02-07 23:59:59	 
☐	2		Registered Card	Expired	2026-01-13 00:00:00	2026-02-12 23:59:59	 
☐	3		Registered Card	Normal	2026-01-13 00:00:00	2026-03-28 00:00:00	 
☐	4		Registered Card	Expired	2026-01-13 00:00:00	2026-02-12 23:59:59	 
☐	5		Registered Card	Normal	2024-06-15 10:00:00	2027-07-15 10:00:00	 
☐	6		Temporary Card	Report Card Loss	2024-06-15 10:00:00	2027-07-15 10:00:00	 
☐	7		Registered Card	Normal	2024-06-15 10:00:00	2027-07-15 10:00:00	 
☐	8		Registered Card	Normal	2024-06-15 10:00:00	2027-07-15 10:00:00	 
☐	9		Temporary Card	Report Card Loss	2024-06-15 10:00:00	2027-07-15 10:00:00	 
☐	10		Registered Card	Normal	2024-06-15 10:00:00	2027-07-15 10:00:00	 
☐	11		Registered Card	Normal	2024-06-15 10:00:00	2027-07-15 10:00:00	 
☐	12		Temporary Card	Report Card Loss	2024-06-15 10:00:00	2027-07-15 10:00:00	 
☐	13		Registered Card	Normal	2024-06-15 10:00:00	2027-07-15 10:00:00	 
☐	14		Registered Card	Normal	2024-06-15 10:00:00	2027-07-15 10:00:00	 

100

Total 50000 Items

<<

>>

1/500

Figure 4-2 Card No. List

- Click **Import** to import the cards in batch. Click **Download Template** to download the template, and then edit and save the template file. Click **Browse** to select the file from the computer. Click **Import** to import the selected file to the device.

Note

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

- Click **Export** to export the searched card No. List in batch. Click **Export**. Click **Export** on the pop-up window. The card No. list will be downloaded to your computer.

4.2 Search Card Records

You can search card swiping records by searching conditions.

- Go to **Data** → **Card No. Record**.

Card Reader Intercom Station User Manual

- 2. Set the start time and end time, and the other search conditions.
- 3. Click **Search** to search the card records. The search results will be listed below.

Start Time

2026-03-01 00:00:00

End Time

2026-03-24 23:59:59

Card No.

Card Type

ALL

Card Status

ALL

Card Reader

ALL

Local Release by Device

ALL

Platform Report Result

ALL

Search

Export

☐	No.	Swiping Card Time	Card No.	Card Type	Card Status	Card Reader	Local Release by Device	Platform Report Time	Platform Report Result
☐	1	2026-03-19 14:36:41		Unregistered Card	Normal	Wiegand1	Not Released		Reporting failed.
☐	2	2026-03-19 14:36:41		Unregistered Card	Normal	Wiegand4	Not Released		Reporting failed.
☐	3	2026-03-19 14:36:41		Unregistered Card	Normal	Wiegand2	Not Released		Reporting failed.
☐	4	2026-03-19 14:36:41		Unregistered Card	Normal	Wiegand3	Not Released		Reporting failed.
☐	5	2026-03-19 14:36:38		Unregistered Card	Normal	Wiegand3	Not Released		Reporting failed.
☐	6	2026-03-19 14:36:38		Unregistered Card	Normal	Wiegand2	Not Released		Reporting failed.
☐	7	2026-03-19 14:36:38		Unregistered Card	Normal	Wiegand1	Not Released		Reporting failed.
☐	8	2026-03-19 14:36:38		Unregistered Card	Normal	Wiegand4	Not Released		Reporting failed.
☐	9	2026-03-19 14:36:34		Unregistered Card	Normal	Wiegand1	Not Released		Reporting failed.
☐	10	2026-03-19 14:36:34		Unregistered Card	Normal	Wiegand3	Not Released		Reporting failed.
☐	11	2026-03-19 14:36:34		Unregistered Card	Normal	Wiegand4	Not Released		Reporting failed.
☐	12	2026-03-19 14:36:34		Unregistered Card	Normal	Wiegand2	Not Released		Reporting failed.
☐	13	2026-03-19 14:36:31		Unregistered Card	Normal	Wiegand1	Not Released		Reporting failed.

100

Total 49976 Items

1/500

Figure 4-3 Card No. Record

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

Chapter 5 Exception Alarm

Set exception alarm when the network is disconnected, the IP address is conflicted, etc.

Steps



Note

The supported exception types vary with different models. The actual device prevails.

1. Go to **Configuration** → **Event** → **Alarm Linkage** → **Exception**.
2. Select the exception type(s) and the linkage method.
3. Click **Save**.

Chapter 6 Safety Management

6.1 Manage User

The administrator can add, modify, or delete other accounts, and grant different permissions to different user levels.

Steps

1. Go to **Configuration** → **System** → **User Management** → **User List**.
2. Add a user.

Add

User Name

User Type ☒ Operator ☐ User

Password Level ☒ Medium Level ☐ Strong Level

Admin Password

New Password

Confirm Password

Basic Permission

- ☐ Remote: Parameters Settings
- ☒ Remote: Log Search/Interrogat...
- ☐ Remote: Upgrade/Format
- ☐ Remote: Shutdown/Reboot
- ☐ Remote: Notify Surveillance C...
- ☐ Remote: Serial Port Control

1. 8 to 16 characters allowed.

2. At least 2 types of the following characters should be contained: uppercase letters, lowercase letters, numbers, and special characters.

3. The password cannot contain the user name itself, 123, or admin.

4. The password cannot contain continuous increasing or descending numbers of 4 characters or above, or the same symbols.

5. The password cannot contain the following phrases connected by letters: hik, hkws, hikvision (case-insensitive).

Cancel OK

Figure 6-1 Add User

- 1) Click **Add**.
- 2) Enter **User Name** and select **User Type**.
- 3) Select **Password Level**. The password level of the added user should conform to the selected level.
- 4) Enter **Admin Password**, **New Password**, and confirm the password.

Caution

To increase security of using the device on the network, please change the password of your account regularly. Changing the password every 3 months is recommended. If the device is used in high-risk environment, it is recommended that the password should be changed every month or week.

5) Assign remote permissions to users based on needs.

User

Users can be assigned permissions of remote log search/interrogate working status and changing their own passwords, but no permissions for other operations.

Operator

Operators can be assigned all permissions except for operations on the administrator and creating accounts.

6) Click **OK**.

3. Optional: You can do the following operations.

Edit the user information Click  to edit the user information.

Delete the user Click  to delete the user.

6.2 Enable User Lock

To raise the data security, you are recommended to lock the current IP address.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service** → **Software**.
2. Enable user lock.
3. Click **Save**.

Result

When the times you entered incorrect passwords have reached the limit, the current IP address will be locked automatically.

6.3 Set SSH

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

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service** → **Software**.

2. Enable or disable **SSH Service**, and set **SSH Port** if you enable the function.
3. Click **Save**.

6.4 Prohibit PING

You can prohibit the external devices to operate network connection volume test to the current device.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service** → **Software**.
2. Enable **Prohibit PING**.
3. Click **Save**.

6.5 Set Timeout Logout

You can improve network access security by setting timeout logout.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service** → **Login Management**.
2. Enable timeout logout for static page.
3. Set **Max. Timeout**.
4. Click **Save**.

Result

When the page static time exceeds the set time, the device will automatically log out.

6.6 Set Password Validity Period

You can improve network access security by setting password validity period.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service** → **Login Management**.
2. Select **Password Validity Period**.
 - Select **Permanent**. The password will be permanently valid.
 - Select **Daily** and set **Password Expiry Time**. It will prompt you that the password is expired according to the set password expiry time, and you need to set the new password.
3. Click **Save**.

6.7 Set IP Address Filtering

You can set the IP addresses allowable and not allowable to access the device.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Settings**.
2. Enable IP address filtering.
3. Set **Filtering Mode**.

Blocklist Mode

The added IP addresses are not allowed to access the device.

Allowlist Mode

The added IP addresses are allowed to access the device.

4. Click **Add**, enter the IP address, and click **OK**.



Note

The IP address only refers to the IPv4 address.

5. Optional: Edit, delete, or clear the added IP addresses.
6. Click **Save**.

6.8 Set HTTPS

6.8.1 Create and Install Self-signed Certificate

HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **HTTPS**.
2. Select **Create Self-signed Certificate**.
3. Click **Create**.
4. Follow the prompt to enter **Country/Region**, **Domain/IP**, **Validity**, and other parameters.
5. Click **OK**.

Result

The device will install the self-signed certificate by default.

6.8.2 Install Authorized Certificate

If the demand for external access security is high, you can create and install authorized certificate

via HTTPS protocol to ensure the data transmission security.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **HTTPS**.
2. Select **Create certificate request first and continue the installation**.
3. Click **Create**.
4. Follow the prompt to enter **Country/Region**, **Domain/IP**, **Validity**, and other parameters.
5. Click **Download** to download the certificate request and submit it to the trusted authority for signature.
6. Import certificate to the device.
 - Select **Signed certificate is available, start the installation directly**. Click **Browse** and **Install** to import the certificate to the device.
 - Select **Create the certificate request first and continue the installation**. Click **Browse** and **Install** to import the certificate to the device.
7. Click **Save**.

Chapter 7 Maintenance

7.1 View Device Information

Basic Information and Algorithms Library Version

Go to **Configuration** → **System** → **System Settings** → **Basic Information** to view the basic information and algorithms version of the device.

You can edit **Device Name** and **Device No.** The device No. is used to control the device. It is recommended to reserve the default value.

Device Status

Go to **Configuration** → **System** → **System Settings** → **Device Status** to view the device status and data upload monitoring.

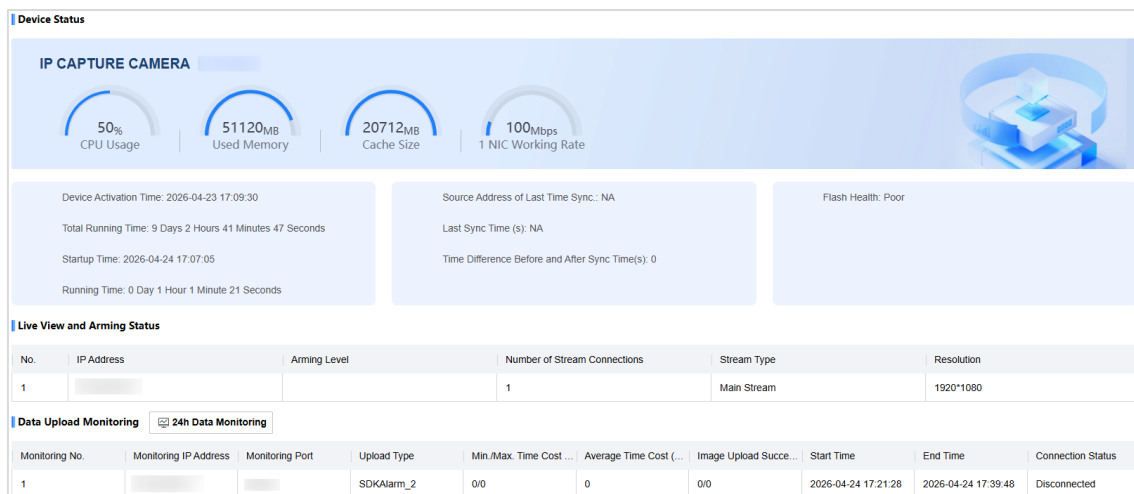


Figure 7-1 Device Status

You can click **24h Data Monitoring**, and select the IP address of the picture upload server to view the data upload statistics in 24 hours. The statistics data will be cleared if the device is rebooted by default. You can enable **Flash Storage** and set **Flash Storage Days** to keep the statistics data not to be cleared when the device is rebooted within the set time.

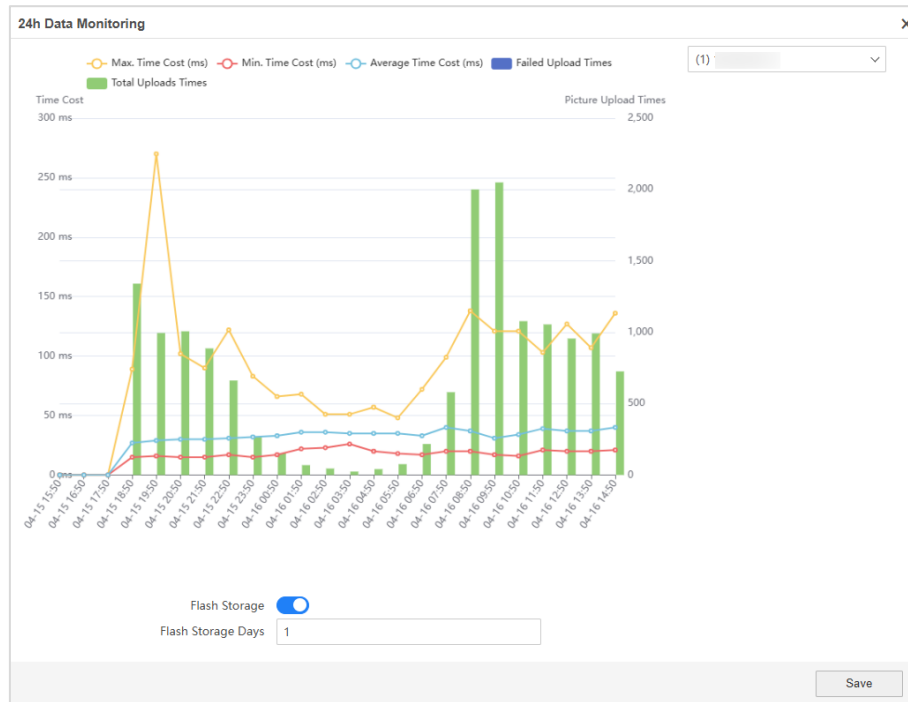


Figure 7-2 24h Data Monitoring

7.2 Synchronize Time

Synchronize the device time when it is inconsistent with the actual time.

Steps

1. Go to **Configuration** → **System** → **System Settings** → **Time Settings**.
2. Select **Time Zone**.
3. Select **Sync Mode**.

NTP Time Sync.

Select it to synchronize the device time with that of the NTP server. Set **Server IP**, **NTP Port**, and **Interval**. Click **NTP Test** to test if the connection between the device and the server is normal.

Manual Time Sync.

Select it to synchronize the device time with that of the computer. Set time manually, or check **Sync. with computer time**.

SDK

If the remote host has been set for the device, select it to synchronize time via the remote host.

No

Select it to disable time synchronization.

All

Select it, and you can select any mode above.

4. Click **Save**.

7.3 Set DST

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

Steps

1. Go to **Configuration** → **System** → **System Settings** → **DST**.
2. Enable **DST**.
3. Set **Start Time**, **End Time**, and **DST Bias**.
4. Click **Save**.

7.4 Set RS-232

Set RS-232 parameters if you need to debug the device via RS-232 serial port.

Before You Start

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

Steps

1. Go to **Configuration** → **System** → **System Settings** → **Serial Port** → **RS-232**.
2. Set **Baud Rate**, **Data Bit**, **Stop Bit**, etc.



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

3. Select **Work Mode**.



- The supported work modes vary with different models. The actual device prevails.
 - You need to reboot the device after editing the work mode to take effect.
-

Console

Select it when you need to debug the device via RS-232 serial port.

Transparent Channel

Select it, and the network command can be transmitted to RS-232 control command via the RS-232 serial port.

Narrow Bandwidth Transmission

Reserved.

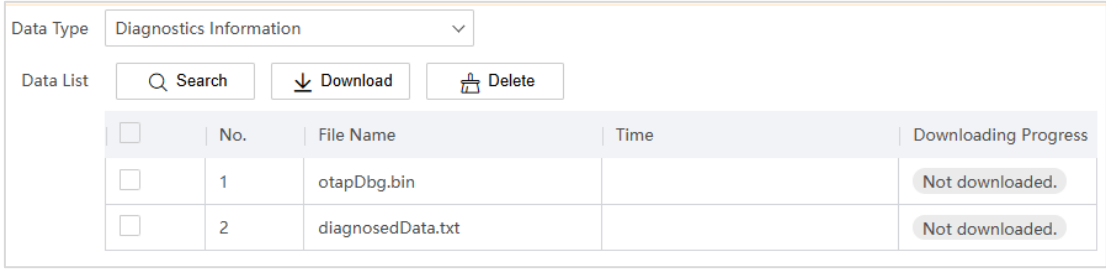
4. Click **Save**.

7.5 Download Debug Data

You can search and download the diagnostics information of the device to debug the device.

Steps

1. Go to **Configuration → System → Maintenance → Debug Data Download**.



Data Type		Diagnostics Information		
Data List		Search	Download	Delete
	No.	File Name	Time	Downloading Progress
☐	1	otapDbg.bin		Not downloaded.
☐	2	diagnosedData.txt		Not downloaded.

Figure 7-3 Download Debug Data

2. Select **Data Type**.

Diagnostics Information

The diagnostics information includes kernel, status, version information, etc.

3. Click **Search** to search the data list.

4. Select the file(s) to be downloaded, and click **Download** to download the file(s). You can view the downloading progress.

5. Optional: Select the file(s) to be deleted, and click **Delete** to delete the file(s).

7.6 Enable System Log Service

The security logs refer to the security operation logs. Enable system log service to analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events. You are recommended to save the logs on a log server.

Steps

1. Go to **Configuration → System → Maintenance → Log Search**.

2. Click **Configuration** to enable system log service.

3. Enter **IP Address** and **Port** of the log server.

4. Click **OK**.



Note

For the device not supporting TF card, other functions on this interface are not supported.

7.7 Reboot

When the device needs to be rebooted, reboot it via the software instead of cutting off the power directly.

Steps

1. Go to **Configuration** → **Upgrade** → **Device Maintenance**.
2. Click **Reboot**.
3. Click **OK** to reboot the device.



You can also click  on the upper right corner of the interface to reboot the device.

7.8 Restore Parameters

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

Steps

1. Go to **Configuration** → **Upgrade** → **Device Maintenance**.
2. Select the restoration mode.
 - Click **Restore** and click **OK**. Then the parameters except the IP parameters and user parameters will be restored to the default settings.
 - Click **Restore Factory Settings** and click **OK**. Enter the admin password to restore all the parameters to the factory settings.
3. Click **OK**.

7.9 Export Parameters

You can export the parameters of one device, and import them to another device to set the two devices with the same parameters.

Steps

1. Go to **Configuration** → **Upgrade** → **Backup and Import Parameters**.
2. Click **Export** after **Configuration Parameters**.
3. Set an encryption password, confirm the password, and click **OK**.



The password is used for importing the configuration file of the current device to other devices.

4. Select the saving path, and enter the file name.
5. Click **Save**.

7.10 Import Configuration File

Import the configuration file of another device to the current device to set the same parameters.

Before You Start

Save the configuration file to the computer.

Steps



Caution

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

1. Go to **Configuration** → **Upgrade** → **Backup and Import Parameters**.
2. Select **Importing Method**.
3. Click **Browse** to select the configuration file.
4. Click **Import**.
5. Enter the password which is set when the configuration file is exported, and click **OK**.
6. Click **OK** on the popup window.

Result

The parameters will be imported, and the device will reboot.

7.11 Upgrade

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

Before You Start

- Update the plugin before upgrade.
- Prepare the upgrade file in .dav format.

Steps

1. Go to **Configuration** → **Upgrade** → **Import Upgrade File**.
2. Click **Browse** to select the upgrade file.
3. Click **Upgrade**.
4. Click **OK** in the popup window.



Note

The upgrading process will take minutes. Do not power off the device. The device will restart automatically after upgrading. If the network condition is poor, it may take more time.

Result

The device will reboot automatically after upgrade.



See Far, Go Further