Doorway Terminal

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.

Data Protection

- To protect data, the development of Hikvision Products incorporates privacy by design principles. For example, for Products with facial recognition features, biometrics data is stored in your Products with encryption method; for fingerprint Products, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
- As a data controller/processor, you may process personal data, including collection, storage, use, processing, disclosure, deletion, etc. You are advised to pay attention to and comply with applicable laws and regulations related to the protection of personal data, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and the assessments of the effectiveness of your security controls.

© 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.

Regulatory Information

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.
This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. this device may not cause interference, and
2. this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.
Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.
Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

About this Manual

Get the manual and related software from or the official website (http://www.hikvision.com).

Product	Model
Doorway Terminal	DS-KHD9800X-W

Contents

Chapter 1 Activation 1
1.1 Activate via Device 1
1.2 Activate via SADP 1
Chapter 2 Local Configuration and Operation 3
2.1 Local Configuration of the Device 3
2.1.1 Activate the Device 3
2.1.2 Quick Operation 3
2.1.3 Basic Settings 4
2.2 Local Operation 4
2.2.1 Trigger Alarms 4
2.2.2 Call Nurse Station 4
Chapter 3 Quick Operation via Web Browser 5
3.1 Change Password 5
3.2 Select Language 5
3.3 Time Settings 5
3.4 Administrator Settings 6
3.5 No. and System Network 7
Chapter 4 Operation via Web Browser 9
4.1 Login 9
4.2 Overview 9
4.3 Person Management 10
4.4 Search Event 11
4.5 Device Management 11
4.6 Configuration 11
4.6.1 Local 11
4.6.2 View Device Information 13

4.6.3 Set Time 13
4.6.4 Change Administrator's Password on PC Web 14
4.6.5 View Device Arming/Disarming Information on PC Web 15
4.6.6 View Online User 15
4.6.7 Network Settings 15
4.6.8 Set Video and Audio Parameters 18
4.6.9 Set OSD Parameters via PC Web 21
4.6.10 Event 21
4.6.11 Access Control Settings 22
4.6.12 Call Settings 23
4.6.13 Add Broadcast Materials 25
4.6.14 Broadcast Plans 26
4.6.15 Privacy Settings 27
4.6.16 Set Biometric Parameters 27
4.6.17 Set Card Security 28
4.6.18 Preference Settings 28
4.6.19 Set Preference 29
4.6.20 Upgrade and Maintenance 30
4.6.21 Device Debugging 31
4.6.22 Security Audit Log 32
4.6.23 Set Protocol Testing 32
4.6.24 Set Network Penetration Service via PC Web 32
4.6.25 Certificate Management 33
Chapter 5 Other Platforms to Configure 34

Chapter 1 Activation

You should activate the device before the first login. After powering on the device, the system will switch to Device Activation page.

Activation via the device, SADP tool and the client software are supported.

The default values of the device are as follows:

- The default IP address: 192.0.0.64
- The default port No.: 8000
- The default user name: admin

1.1 Activate via Device

If the device is not activated, you can activate the device after it is powered on.

On the Activate Device page, create a password and confirm the password. Tap **Activate** and the device will activated.

Caution

- The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of 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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
- Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
- Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
- Password cannot contain words such as hik, hkws, and hikvision (case insensitive).

1.2 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website ***http://www.hikvision.com/en/*** , and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

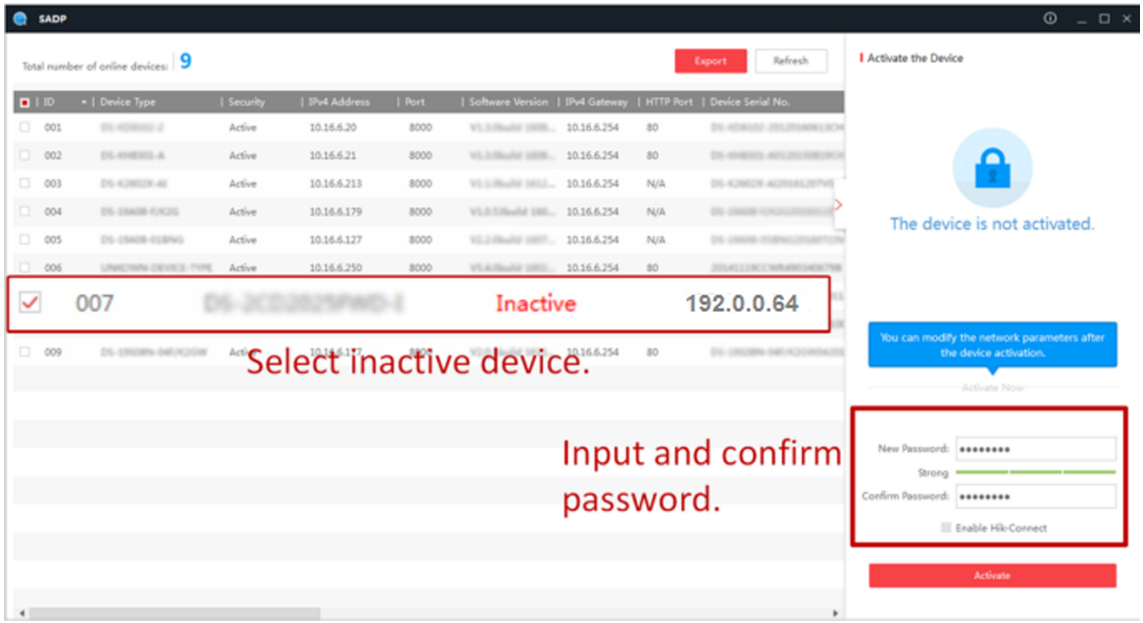
Caution

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.

Note

Characters containing admin and nimda are not supported to be set as activation password.

4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
   3) Input the admin password and click **Modify** to activate your IP address modification.

Chapter 2 Local Configuration and Operation

2.1 Local Configuration of the Device

2.1.1 Activate the Device

You can only configure and operate the device after creating a secret key and finishing activation.

Steps

1. Power on the device. It will enter the activation page automatically.
2. Enter the secret key for activation and tap **Next**.
3. Tap **OK**. The device will automatically go to the Quick Setup interface.

Note

Interfaces may vary depending on the device model. Please refer to the actual interface.

2.1.2 Quick Operation

After device activation, the system will automatically enter the configuration wizard. You need to select the usage mode, configure Server Settings and Service Settings.

Steps

1. At Mode Selection, please select usage mode then tap **Next**.

   Note

   Demo mode is typically used by manufacturers to demonstrate device operation to users. For regular device usage, please select normal mode.
2. Configure the local IP address. Enter **Local IP**, **Subnet Mask** and **Gateway**, then click **Next**.
3. Configure the server.
   1) Enter the server address, port number and admin password.
   2) Tap **Next**.

   Note

   The admin password can be viewed and modified in HikCentral Professional.
   After server configuration is completed, the device will connect to HikCentral Professional.
4. Select department/ ward to complete the configuration.
5. Tap **Finish** to save the settings.

2.1.3 Basic Settings

On the device main interface, press and hold the hospital name in the upper left corner and enter the admin password to access the settings interface.

You can edit the server IP, port No., department/ward, room, and mode.

Note

The admin password can be viewed and set in the **HikCentral Professional** Platform.

2.2 Local Operation

2.2.1 Trigger Alarms

You can trigger an alarm by pressing the alarm button connected to the device.

After connecting the bathroom alarm button to the device, press the button to trigger a bathroom alarm. The alarm information will be reported to the nurse station host.

Long press the button to cancel the alarm.

2.2.2 Call Nurse Station

In case of emergency, you can call from the Doorway Terminal to the Nurse Station.

Before You Start

Ensure the device is linked to the corresponding host first.

Steps

1. Press the call button, the device will call the nurse station automatically.

Chapter 3 Quick Operation via Web Browser

3.1 Change Password

You can change the device password.

Click on the top right of the web page to enter the **Change Password** page. You can set security questions from the drop-down list and fill in the answers.

Click **Next** to complete the settings. Or click **Skip** to skip the step.

3.2 Select Language

You can select a language for the device system.

Click in the top right of the web page to enter the **Device Language Settings** page. You can select a language for the device system from the drop-down list.

By default, the system language is English.

Note

After you change the system language, the device will reboot automatically.

3.3 Time Settings

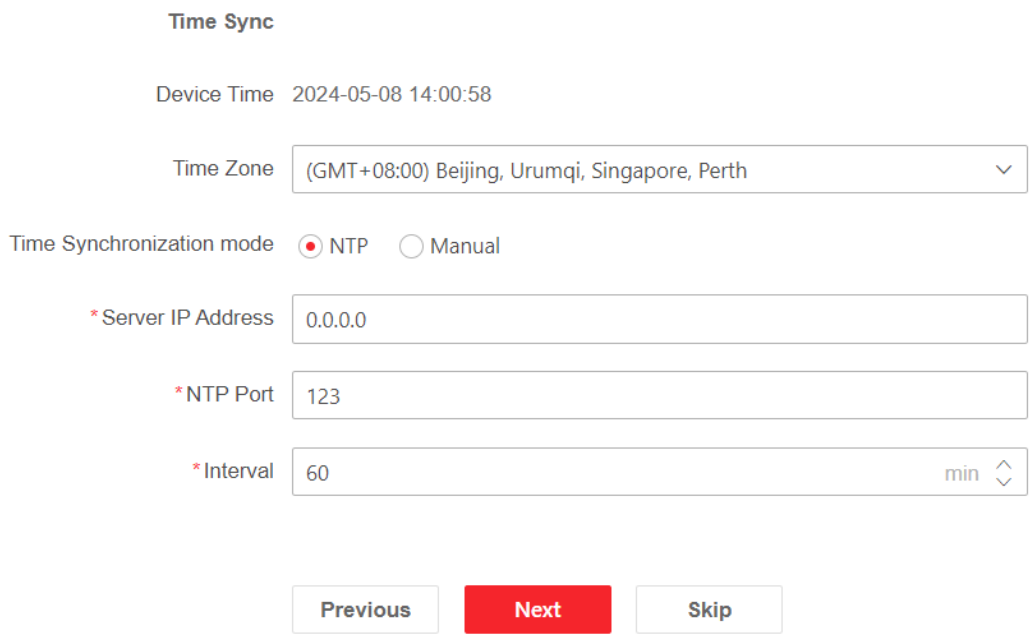


Figure 3-1 Set Time and DST

Click in the top right of the web page to enter the wizard page. After setting device language, you can click **Next** to enter the **Time Settings** page.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address/NTP Port/Interval

You can set the server address, NTP port, and interval.

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip time settings.

3.4 Administrator Settings

Steps

1. Click in the top right of the web page to enter the wizard page.

2. Enter the employee ID and name of the administrator.
3. Select a credential to add.

Note

You should select at least one credential.

1) Click **Add Face** to upload a face picture from local storage.

Note

The uploaded picture should be within 200 K, in JPG、JPEG、PNG format.

2) Click **Add Card** to enter the Card No. and select the property of the card.

Note

Up to 5 cards can be supported.

3.5 No. and System Network

Steps

1. Click in the top right of the web page to enter the wizard page. After previous settings, you can click **Next** to enter the **No. and Network System Network** settings page.
2. You can edit **No.** or **Custom Name**.

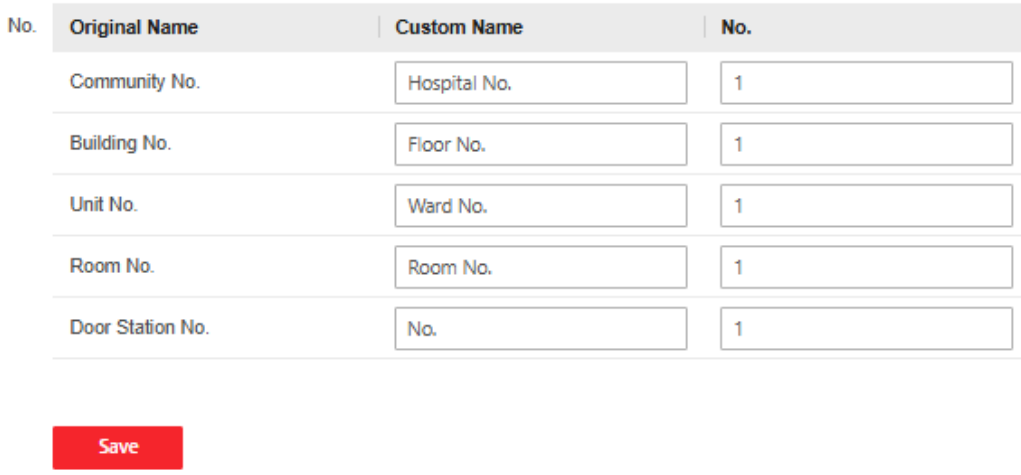


Figure 3-2 Device No.

Community No.

Range: 1 to 999.

Building No.

Range: 1 to 999.

Unit No.

Range: 1 to 999.

Room No.

Range: 1 to 999.

Door Station No.

Range: 1 to 999.

3. Set the video intercom network parameters.

Registration Password

Set the registration password of the main station for communication.

Main Station IP

Set the IP of the main station for communication.

Private Server IP

Refers to the SIP server IP. Enter the main station' s IP address that used for communication. At this time the main station is used as a SIP server. Other intercom devices should registered to this server address to realize communication.

4. Click **Complete** to save the settings after the configuration.

Chapter 4 Operation via Web Browser

4.1 Login

You can login via the web browser or the remote configuration of the client software.

Note

Make sure the device is activated. For detailed information about activation, see .

Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.

Enter the device user name and the password. Click **Login**.

Note

5 failed password enterings will lock the device. You should try again after 30 min.

4.2 Overview

You can view linked devices, network status and basic information etc..

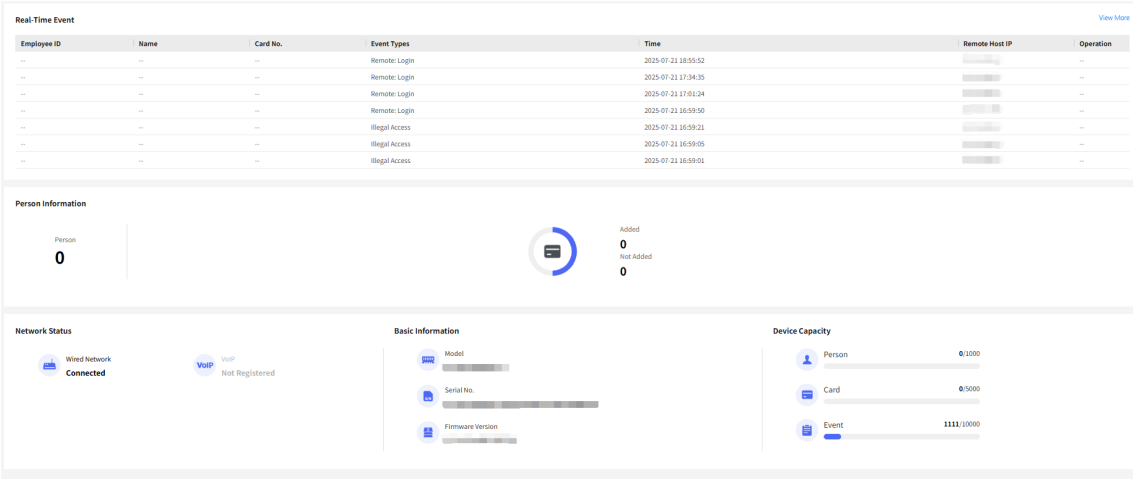


Figure 4-1 Overview Page

Function Descriptions:

Linked Device

You can view linked devices and their online status.

Network Status

You can view the connected and registered status of wired network and VoIP.

Basic Information

You can view the model, serial No. and firmware version.

Device Capacity

You can view person, card and event capacity.

Person Information

You can view the added and not added information of person.

View More

You can click **View More** to enter the page of **Device Management**.

4.3 Person Management

You can add the person's information, including the basic information, credentials, authentication and settings.

Add Basic Information

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, and person type.
If you select **Visitor** as the person type, you can set the visit times.
Click **Save** to save the settings.

Set Permission Time

Click **Person Management → Add** to enter the Add Person page.
Enable **Long-Term Effective User**, or set **Start Time** and **End Time** and the person can only has the permission within the configured time period according to your actual needs.
Click **Save** to save the settings.

Add Card

Click **Person Management → Add** to enter the Add Person page.
Click **Add Card**, enter the **Card No.** and select the **Property**, and click **Save** to add the card.
Click **Save** to save the settings.

No. Settings

Click **Person Management → Add** to enter the Add Person page.
You can link a ward No. for the person to realize elevator calling function after the person passing through the turnstile.
Click **Add**, enter the **Ward No.** and **Floor No.**
You can also click 🗑 to delete the ward No.
Click **Save** to save the settings.

4.4 Search Event

Click **Event Search** to enter the Search page.

Enter the search conditions, including the event type, the employee ID, the name, the card No., the start time, and the end time, and click **Search**.

The results will be displayed on the right panel.

4.5 Device Management

You can manage the linked device on the page.

Click **Device Management** to enter the settings page.

Add Device

- Click **+Add** to add camera. Enter the parameters (including IP Address, Channel No., Port, User and Password) and click **Save** to add.
- You can view information including IP Address, Channel No., Port, User, Protocol in the added device's list.

Delete

Select the device and click **Delete** to remove the selected device from the list.

Optional: Set Device Information.

- Click to edit device information.
- Click to delete device information from the list.

4.6 Configuration

4.6.1 Local

You can check and configure the live view parameters, record file settings, and picture and clip settings on this page.

Click **Configuration → Local** to enter this page.

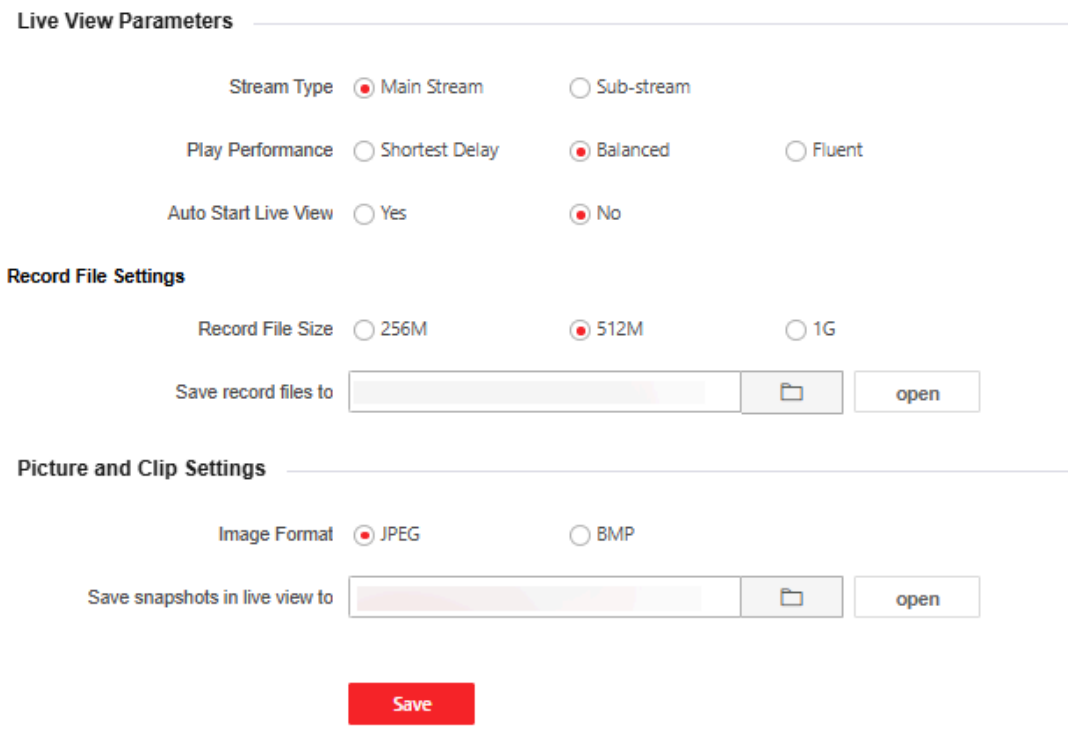


Figure 4-2 Local

Live View Parameters

Stream Type

Choose between Main Stream or Sub-stream.

Note

The main stream provides higher resolution and quality, while the sub-stream is optimized for lower bandwidth usage.

Play Performance

- Select one of the following options:

- **Shortest Delay**: Minimizes latency but may reduce video quality.
- **Balanced**: Balances latency and video quality (selected by default).
- **Fluent**: Prioritizes smooth playback over latency.

Auto Start Live View

If choose **Yes**, the live view interface will automatically play the live view image upon opening; if disabled.

If choose **No**, the user must manually click the play button to start live view.

Record File Settings

- **Record File Size**: Select the package size for recording files as 256 MB, 512 MB, or 1 GB based on requirements.
- The local path where recording files are stored. Click **Open** to access the folder in the storage path.
- Click 🗀 to select where your files will be stored.

Picture and Clip Settings

- You can select image format as **JPEG** or **BMP** according to your actual needs.
- The local path where snapshots files are stored. Click **Open** to access the folder in the storage path.
- Click 🗀 to select where your snapshots files will be stored.

4.6.2 View Device Information

View the device name, device No., language, model, serial No., version, number of channels, alarm input, alarm output, and device capacity, etc.

Click **Configuration → System → System Settings → Basic Information** to enter the configuration page.

You can view the language, model, serial No., version, local RS-485, alarm input and alarm output number etc..

You can change **Device Name** and click **Save**.

Click **Upgrade** to upgrade the firmware version.

You can view the device capacity, including person, card, face and event.

4.6.3 Set Time

Set the device's time zone, synchronization mode, server address, NTP port, and interval.

Click **Configuration → System → System Settings → Time Settings** .

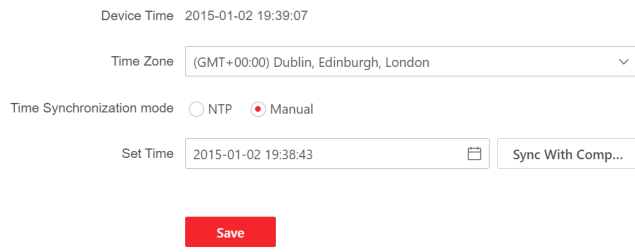


Figure 4-3 Time Settings

Click **Save** to save the settings after the configuration.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

4.6.4 Change Administrator's Password on PC Web

Steps

1. Click **Configuration → System → User Management** .
2. Click .
3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **Save**.

Note

- The password should be 8 to 16 characters.
- The password should contain at least 2 of the following types: digits, lowercase letters, uppercase letters and special characters.
- The username cannot be the same as the password. Password cannot be inverted write of user name.
- The password strength of the device can be automatically checked. In order to increase the security of your product, we highly recommend you change the password of your own choosing. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

- (If the device supports AP mode, after the admin password is changed, the password of AP hotspot will be changed simultaneously.)

4.6.5 View Device Arming/Disarming Information on PC Web

View device arming type and arming IP address.

Go to **Configuration → User Management → Arming/Disarming Information** .

You can view the device arming/disarming information. Click **Refresh** to refresh the page.

4.6.6 View Online User

You can view online users.

Click **Configuration → System → User Management → Online User** .

You can view online users' information including name, type, IP Address and operation time. Click **Refresh** to refresh the page.

4.6.7 Network Settings

Set Basic Network Parameters via PC Web

Click **Configuration → Network → Network Settings → TCP/IP** .

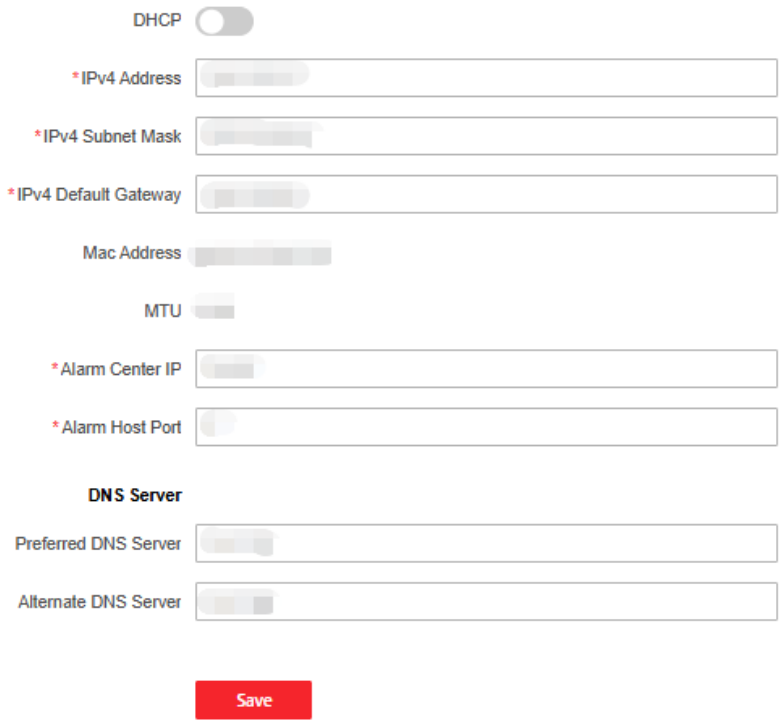


Figure 4-4 TCP/IP Settings Page

Set the parameters and click **Save** to save the settings.

DHCP

If uncheck the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, Mac address, MTU, Alarm Center IP and Alarm Host Port.

If you check the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway automatically.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Note

If you check DHCP, the system will allocate preferred DNS server and the Alternate DNS server automatically.

Configure Wi-Fi

Steps

1. Click **Configuration → Network → Network Settings → Wi-Fi** to enter this page.

2. Slide to enable the Wi-Fi function.
3. Enter the SSID name and password or you can select a network from the Wi-Fi list.
4. Set the Wi-Fi **Security Mode** from the drop-down list.
5. **Optional:** Click **Refresh** to refresh the network status.
6. **Optional:** Set WLAN parameters.
   1) On the **Wi-Fi Settings** page, after enabling **Wi-Fi**, **WLAN** information will be shown automatically.
   2) Uncheck **DHCP** and set the Device IPv4 Address, Device IPv4 Subnet Mask, Device IPv4 Default Gateway, Preferred DNS Server, and Alternate DNS Server.
7. Click **Save**.

VoIP Account Settings

You can realize voice call by network.

Steps
1. Go to **Configuration → Network → Device Access → VoIP** .
2. Silde to **Enable VoIP Gateway**.
3. Set **Register User Name**、**Registration Password**、**Server IP Address**、**Server Port**、**Expiry Time**、**Register Status**、**Number** and**Display User Name.**.
4. Click **Save**.

Set FTP

Before You Start
Get the FTP server address first.

Steps
1. Go to **Configuration → Network → Network Service → FTP** .
2. Silide to enable **FTP**.
3. Select Server Type, enter Server IP Address, Port, User Name and Password.
4. Check **Anonymous**, you do not need to configure the user name and password.
5. You can save the configuration file in Root Directory, Parent Directory or Child Directory.
   - You can set device name, device IP, time, building No. and unit No. in parent directory.
   - You can set building No., unit No. and door station number in parent directory.
6. You can set the delimiter, named item, and named element according to your needs.
7. Click **Save**.

Set Port Parameters

Set the HTTP, HTTPS, RTSP and Server port parameters.

Click **Configuration → Network → Network Service → HTTP(S)** .

HTTP

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://192.0.0.65:81*** in the browser for login.

HTTPS

Set the HTTPS for accessing the browser. Certificate is required when accessing.

Click **Configuration → Network → Network Service → RTSP** .

RTSP

It refers to the port of real-time streaming protocol.

Click **Configuration → Network → Device Access → SDK Server** .

SDK Server

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

4.6.8 Set Video and Audio Parameters

Set the image quality and resolution.

Set Video Parameters

Click **Configuration → Video/Audio → Video** .

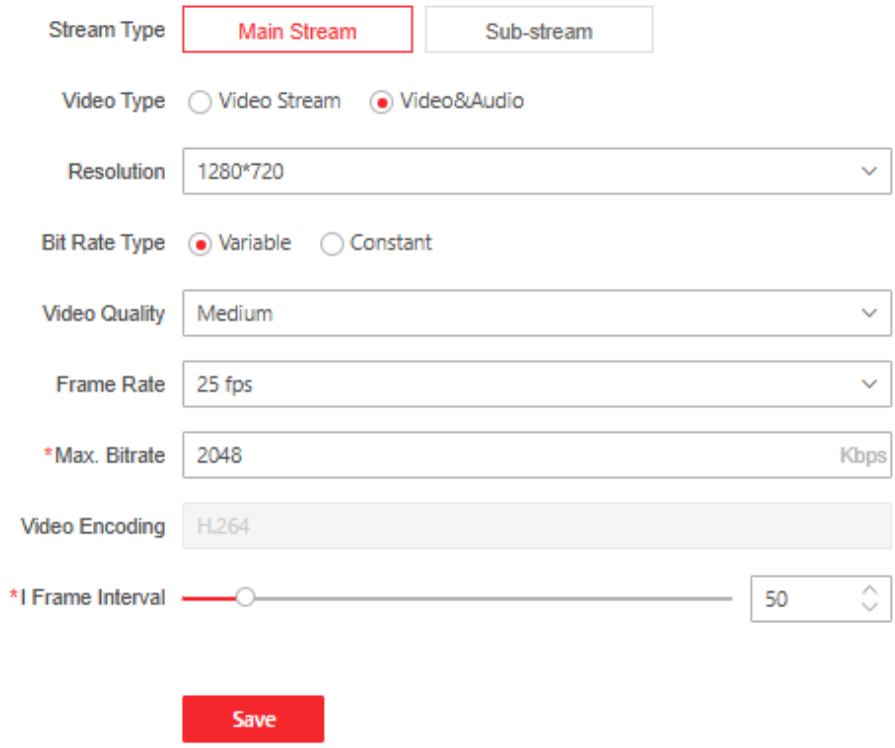


Figure 4-5 Video Settings Page

Set the stream type, the video type, the resolution, the Bit Rate type, the video quality, the frame rate, the Max. bitrate, the video encoding, and I Frame Interval.

Stream Type

Set video parameters for main stream or sub-stream.

Video Type

Set video type to composite stream (including video and audio) or video stream only.

Resolution

Main stream resolution options: 1280×720P or 1920×1080P. Sub-stream resolution options: 640×480P or 1280×720P. Select according to actual requirements.

Bitrate Type

Select variable bitrate (VBR) or constant bitrate (CBR). CBR transmits at a fixed bitrate. Bitrate upper limit range: 32 to 16384.

Image Quality

Set the image quality level.

Video Frame Rate

Set the number of frames per second (FPS) based on actual conditions.

Bitrate Upper Limit

Configurable range: 32 to 16384.

Video Encoding

Set stream encoding to H.264. Actual encoding types depend on specific models.

I-frame Interval

Number of frames between two keyframes. Configurable range: 1 to 400.

Click **Save** to save the settings.

Note

The functions vary according to different models. Refers to the actual device for details.

Set Audio Parameters

Click **Configuration → Video/Audio → Audio** .

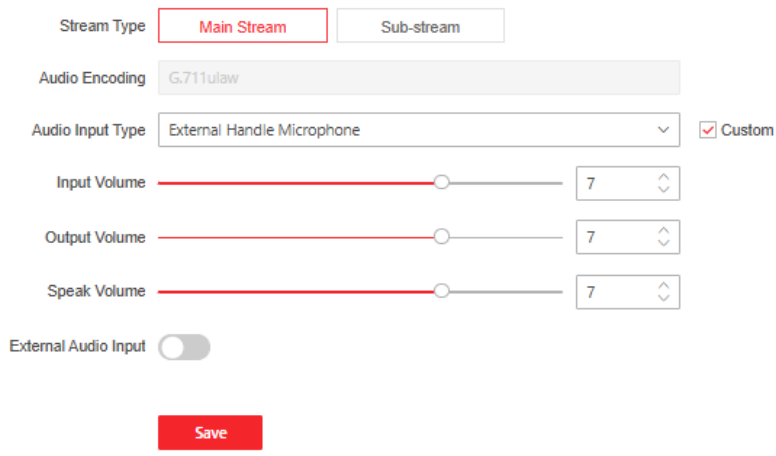


Figure 4-6 Audio Settings Page

If you check **Custom**, the system will automatically change to the appropriate **Audio Input Type**.
Set input volume, output volume and speak volume.
Slide to enable audio input according to your actual needs.

Note

If enabled, the device can connect to external microphone.

Stream Type

Set audio parameters for main stream or sub-stream.

Audio Encoding

Currently supports only G.711ulaw audio bitrate type.

Input Volume

Microphone input volume. Adjustable range: 0 to 10.

Output Volume

Device volume during audio playback. Adjustable range: 0 to 10.

Intercom Volume

Device volume during call. Adjustable range: 0 to 10.

Click **Save** to save the settings.

4.6.9 Set OSD Parameters via PC Web

You can customize the camera name, time/date format, display mode, and OSD size displayed on the live view.

Steps

1. Click **Configuration → Image → OSD Configuration** to enter the settings page.
2. Enable **OSD**.
3. Check the corresponding checkbox to select the display of camera name, date or week if required.
4. Enter **Camera Name**.
5. Select from the drop-down list to set the **Time Format** and **Date Format**.
6. Click **Add** to enter the characters in the textbox, and adjust the OSD position and alignment.

4.6.10 Event

Set Motion Detection

After enable the function of motion detection, people or stuff enter the configured area will trigger alarm.

Steps

1. Click **Configuration → Event → Event Detection → Motion Detection** .
2. Enable **Motion Detection**.

   Note

   If motion detection is not enabled, you cannot draw detection areas or adjust sensitivity.

3. Drag the process bar to adjust the **Sensitivity** parameter.
4. Click and drag the left mouse button on the screen to draw a detection area. Release the mouse button to complete drawing. Click **Stop Drawing** when finished.

   Clear Drawn Areas

Click **Clear All** to remove all drawn areas.

Set Motion Detection Sensitivity

Drag the progress bar to set area sensitivity. Higher numbers indicate higher sensitivity.

Note

When sensitivity is set to 0, motion detection will not function.

5. You can also click **Modify** to change arming schedule. The device is armed all day by default. Click on the arming time period to display and adjust motion detection arming time.

Note

- To set the same arming time for other periods, click the green copy button on the right side of the timeline.
- You can configure start and end times for up to 8 time periods per day.

6. Enable **Notify Surveillance Center** according to your actual needs. After enabled, the alarm information is uploaded to the surveillance center when an alarm event is detected.
7. Click **Save**.

Note

The arming schedule is defaulted as all-day.

Linkage Settings

Configure the linkage parameters when an event is triggered, including regular linkage and upload to center.

Steps

1. Go to **Configuration → Event → Event Detection → Linkage Settings** .
2. Set the linkage method.

   Tampering Alarm

   Silde to enable. It's the basic form of alarm.

   Notify Surveillance Center

   Slide to enable. When an alarm occurs, upload the alarm information to the center platform.
3. Click **Save** to complete the configuration.

4.6.11 Access Control Settings

Set Authentication Interval

Set the device's authentication interval of the same person when authenticating.

Steps

1. Click **Configuration → Access Control → Authentication Settings** .

Note

The functions vary according to different models. Refers to the actual device for details.

2. Set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed.
3. Click **Save**.

RS-485 Settings

Steps

1. Click **Access Control → RS-485** to enter the settings page.
2. The **Peripheral Type** is set as disable by default.
3. Click **Save** to enable the settings.

Password Settings

Click **Configurationo → Access Control → Password Settings** to enter the page.

Click **+Add** to add password.

Set password and remarks and click to enable electric lock.

Click **Save** to save the settings.

4.6.12 Call Settings

Device No. Settings

Steps

1. Click Click **Configuration → Intercom → Device No.** to enter the settings page.

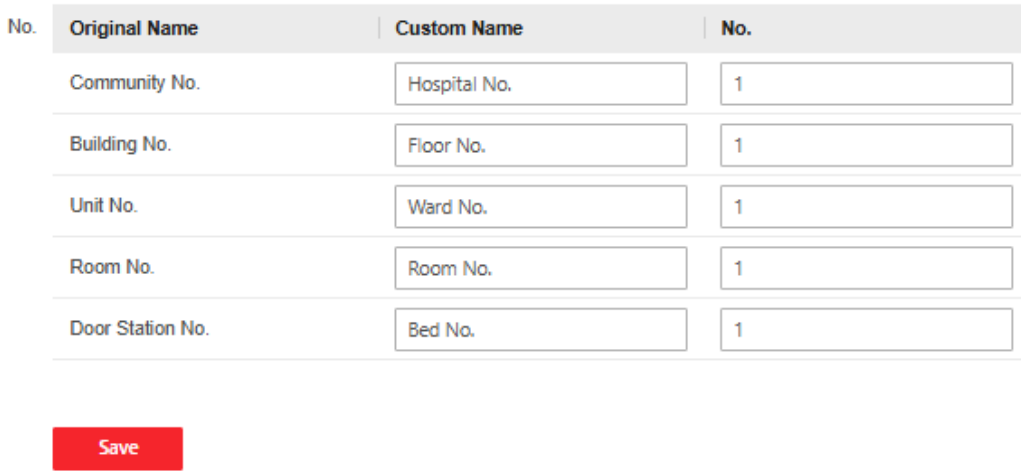


Figure 4-7 Device No. Settings

2. You can set Custom Name and No. of **Building No.**, **Door Station No.**, **Room No.**, **Community No.** and **Unit No.**
3. Click **Save** to enable the device number configuration.

Video Intercom Network

Steps

1. Click **Configuration → Intercom → Video Intercom Network** to enter the settings page.
2. Set the main station IP address and private server IP.
3. Enter the registration password.
4. Click **Save** to enable the settings.

Set Call Parameters

Set Call Duration

Go to **Configuration → Intercom → Call Settings** .
Set **Max. Intercom Duration**, **Max. Ring Duration** and **Max. Message Duration**. Click **Save**.

Note

- The max. intercom duration range is 90 s to 1800 s.
- The max. ring duration range is 30 s to 90 s.
- The max. message duration range is 30 s to 60 s.

Auto Answer

Silde to enable **Auto Answer**.

Note

After enabling the auto-answer function, the other party can leave the voice message to the bedside terminal from nurse station or other deivces.

Press Button to Call

Steps

1. Click **Configuration → Intercom → Press Button to Call** .
2. Select **Device Button Settings**
   - Rgular Call: Press the button to call management center.
   - Alarm Call: Press the button to call the management center and trigger an SOS alarm.

     After triggering the SOS alarm, press and hold the call button to cancel it.
3. Click **Save**.

Set Ringtone on PC Web

Steps

1. Click **Configuration → Intercom → Ringbac Settings** to enter the settings page.
2. Slide to enable ringtone.
3. Click to import new ringtone.

Note

The supported audio file type for importing is .wav. The file should be less than 800 KB.

4.6.13 Add Broadcast Materials

You can add and delete broadcast materials in.

Steps

1. Click **Configuration → Broadcast Settings → Database** to enter the configuration interface.
2. Click **Batch Import** to select multiple broadcast materials from local storage.

   Note

   Each material should be less than 20 MB in MP3 or WAV format.
3. **Optional:** Click **Import More** to keep adding materials that need to be imported.
4. Click **OK**.
5. **Optional:** Check the broadcast materials that need to be deleted and click **Delete** to remove them.

4.6.14 Broadcast Plans

Add scheduled broadcast tasks to make devices broadcast according to the schedule.

Steps

1. Click **Configuration → Broadcast Settings → Broadcast Plans** to enter the broadcast schedule configuration interface.
2. Click **+ Add** to create a broadcast task.
3. Enter the task name.
4. Select the task type as Daily Schedule or Weekly Schedule.

   Daily Schedule

   The broadcast task will be played at fixed time every day.

   Weekly Schedule

   Specify the days of the week when the broadcast task needs to be played.
5. **Optional:** If there are existing plans that can be reused, click **Copy From** to select the plan to be copied.
6. Configure the validity period of the broadcast schedule. The broadcast will be played within the validity period.
7. Configure broadcast rules in **Play Schedule**.

   1) Add terminal devices for broadcasting. Click **+ Add**, check the devices that need to play the broadcast, then click **OK**.

   Note

   If needed, you can click to delete a single device or check multiple devices and click **Delete** to batch delete devices.

   2) Add play time and broadcast content. Click **+ Add**, select broadcast start time, configure audio source, select or add audio, configure broadcast level and play mode.

   Start Time

   Configure the time to start broadcasting.

   Audio Source

   Audio File

   If materials have been added to the broadcast material database, audio files from the database will appear directly in the audio file list.

   If there are no materials in the database, click **+ Add** → **+ Add Material**, select audio from local computer, then click **Add**.

   Check audio files from the list as broadcast materials.

   Broadcast Ratings

   Drag the slider to configure the playback priority of this broadcast. 0 is the highest priority and 15 is the lowest.

   Play Mode

Play Once

Play in the order of the audio list, each audio is played only once.

Loop

Note

When selecting Weekly Plan as the task type, you need to select the **Cycle** period.

Play in order and loop.

8. Click **Save** to complete the configuration.

4.6.15 Privacy Settings

You should set the privacy parameters, including the event storage.

Click **Configuration → Security → Privacy Settings** to enter this page.

Event Storage Settings

Select a method to delete the event. You can select from **Delete Old Events Periodically**, **Delete Old Events by Specified Time**, or **Overwrite**.

Delete Old Events Periodically

Drag the block or enter number to set the period for event deleting. All events will be deleted according to the configured time duration.

Delete Old Events by Specified Time

Set a time and all events will be deleted on the configured time.

Overwrite

The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

Patient Information Desensitization Display

You can choose to enable desensitization display of six types of patient's information including name, No., date of birth, ID No., attending physicianis name and care nurse's name.

4.6.16 Set Biometric Parameters

Set Basic Parameters

Click **Configuration → Smart → Smart** .

Note

The functions vary according to different models. Refers to the actual device for details.

Click **Save** to save the settings after the configuration.

Recognition Distance

Select the distance between the authenticating user and the device camera.

Face 1:N Matching Threshold

Set the matching threshold when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.

Face Recognition Timeout Value

Set the timeout value when face recognizing. If the face recognition time is longer than the configured value, the system will pop up a prompt.

Set Recognition Area

Click **Configuration → Smart → Area Configuration** .
Drag the yellow frame in the live video to adjust the recognition area. Only the face within the area can be recognized by the system.
Click **Save** to save the settings.
Click or to record videos or capture pictures.

4.6.17 Set Card Security

Click **Configuration → Card Settings → Card Type** to enter the settings page.

Set the parameters and click **Save**.

Enable NFC Card

In order to prevent the mobile phone from getting the data of the access control, you can enable NFC card to increase the security level of the data.

Enable M1 Card

Enable M1 card and authenticating by presenting M1 card is available.

M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Sector

Enable the function and set the encryption sector. By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.

Enable CPU Card

Enable CPU card and authenticating by presenting CPU card is available.

4.6.18 Preference Settings

Configure screen display, information publishing, tone schedule, custom tones, authentication result text, and voice assistant.

Customize Prompt Voice via PC Web

You can customize prompt voices for the device.

Steps

1. Go to **System and Maintenance → Preference → Custom Prompt** .
2. Slide to enable prompt schedule.
3. Add time periods for authentication success and failure.
4. Click **Save** to save your settings.

Audio Service

Steps

1. Click **Configuration → Preference → Audio Service** to enter the configuration page.
2. Slide to enable voice recognition function.

Note

This function is a reserved feature.

4.6.19 Set Preference

You can set the sleep time for the device.

Set Theme

Click **Configuration → Preference** .

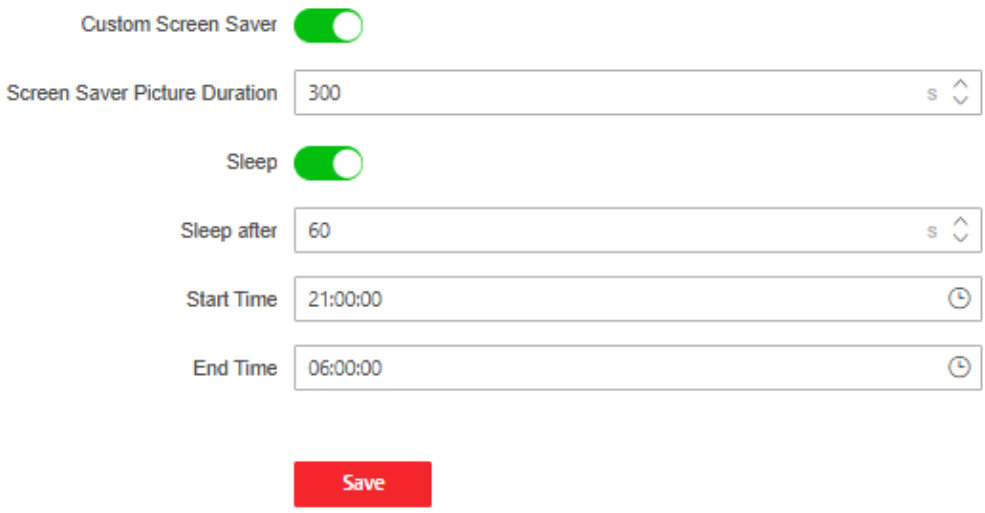


Figure 4-8 Screen Display

Custom Screen Saver

Enable **Custom Screen Saver**, then you can edit screen saver picture duration.

Note

Range: 30 to 3600s.

Sleep

Enable **Sleep**, then you can configure start time and end time for sleep mode.

You can also configure the device to **sleep after** a set time. Range from 10 to 3600 s.

4.6.20 Upgrade and Maintenance

Reboot device, restore device parameters, and upgrade device version.

Reboot Device

Click **Maintenance and Security → Maintenance → Restart** .
If you want to manually reboot the device, you can click **Restart** to reboot the device.
If you want to reboot the device automatically, you can silde to enable **Reboot Automatically** and choose the rebooting time.

Upgrade

Click **Maintenance and Security → Maintenance → Upgrade** .

Select upgrade settings from the drop-down list. Click and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.
If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can click **Upgrade** after Online Update to upgrade the device system.

Note

The upgrading process will last 3 to 10 minutes. Do not power off during the process. The device will reboot automatically after upgrading.

Restore Parameters

Click **Maintenance and Security → Maintenance → Backup and Reset** .

Restore All

All parameters will be restored to the factory settings. You should activate the device before usage.

Restore

The device will restore to the default settings, except for the device IP address and the user information.

Import and Export Parameters

Click **Maintenance and Security → Maintenance → Backup and Reset** .

Export

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

Note

You can import the exported device parameters to another device.

Import

Click and select the file to import. Click **Import** to start import configuration file.

4.6.21 Device Debugging

You can set device debugging parameters.

Steps

1. Click **Maintenance and Security → Maintenance → Device Debugging** .
2. You can set the following parameters.

   Enable SSH

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

   ADB

Enable **ADB Remote Control** for actual needs.

Print Log

You can click **Export** to export log.

Capture Network Packet

You can set the **Capture Packet Duration**, **Capture Packet Size** and click **Start Capture** to capture network data.

Note

Capture Packet Duration Range: 3o to 300s.
Capture Packet Size Range: 1 to 100MB.

3. Click **Save**.

4.6.22 Security Audit Log

Steps

1. Click **Maintenance → Security Audit Log** to enter the page.
2. You can slide to enable **Log Upload Server**, **Encrypt Tramsmission** or **Verify Certificate**.
3. In **Server Configuration**, you can edit **Log Server Address**, **Log Server Port** and **Uploading Cycle**.

Note

Log Server Port Range: 1 to 65535.
Uploading Cycle Range: 1 to 24 Hours.

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

4.6.23 Set Protocol Testing

Select a protocol address, and enter the protocol to test. You can debug the device according to the response header and returned value.

Go to **Maintenance and Security → Maintenance → Protocol Testing** .

Select a protocol address, and enter the protocol. Click **Execute**.

Debug the device according to the response header and returned value.

4.6.24 Set Network Penetration Service via PC Web

When the devcie is deployed in the LAN, you can enable the penetration service to realize device remote management.

Steps

1. Go to **Maintenance → Network Penetration Service** .
2. Slide to **Enable Penetration Service**.

3. Set **Server IP Address** and **Server Port**. Create **User Name** and **Password**.
4. **Optional:** You can set **Heartbeat Timeout**. The value range is 1 to 6000.
5. **Optional:** You can view the status of the penetration service. Click **Refresh** to refresh the status.
6. Click **Save**.

Note

The penetration service will auto disabled after 48 h.

4.6.25 Certificate Management

It helps to manage the server/client certificates and CA certificate.

Note

The function is only supported by certain device models.

Import Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Before You Start

You should send the asking file to a certification authority for signature. Then save the authorized certificate locally.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **Import Key** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. Click **Import**.

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Create an ID in the **CA Certificate ID** area.

   Note

   The input certificate ID cannot be the same as the existing ones.
3. Upload a certificate file from the local.
4. Click **Import**.

Chapter 5 Other Platforms to Configure

You can also configure the device via HikCentral Professional Mobile Client. For details, see the platforms' user manual.

HikCentral Professional Mobile Client (HCP)

Click/tap the link to view the HCP's user manual.

http://enpinfodata.hikvision.com/analysisQR/showQR/24cb4850

See Far, Go Further

UD44497B