



Bedhead Terminals

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
Bedhead Terminal	DS-KHH9530X-H

Contents

Chapter 1 Main Interface Description	1
Chapter 2 Typical Applications	3
Chapter 3 Activation	4
3.1 Activate via Device	4
Chapter 4 Local Configuration and Operation	5
4.1 Local Operation	5
4.1.1 Messages	5
4.1.2 Health Education	5
4.1.3 Admission and Discharge Guide	5
4.1.4 Hospital/Ward/Department/Physician/Nurse Introduction	5
4.1.5 Trigger Alarms	6
4.1.6 Call Nurse Station	6
4.2 Local Configuration of the Device	6
4.2.1 Activate the Device	6
4.2.2 Quick Operation	7
4.2.3 Device Information	7
4.2.4 Basic Settings	8
4.2.5 Advanced Settings	9
Chapter 5 Quick Operation via Web Browser	11
5.1 Change Password	11
5.2 Select Language	11
5.3 Time Settings	11
5.4 Administrator Settings	13
5.5 No. and System Network	13
Chapter 6 Operation via Web Browser	15
6.1 Login	15

6.2 Overview	15
6.3 Person Management	16
6.4 Search Event	16
6.5 Configuration	17
6.5.1 View Device Information	17
6.5.2 Set Time	17
6.5.3 Change Administrator's Password on PC Web	18
6.5.4 View Device Arming/Disarming Information on PC Web	18
6.5.5 View Online User	18
6.5.6 Network Settings	19
6.5.7 Set Video and Audio Parameters	21
6.5.8 Call Settings	22
6.5.9 Add Broadcast Materials	23
6.5.10 Broadcast Plans	23
6.5.11 Privacy Settings	25
6.5.12 Set Card Security	26
6.5.13 Set Preference	27
6.5.14 Upgrade and Maintenance	27
6.5.15 Device Debugging	28
6.5.16 Security Audit Log	29
6.5.17 Set Protocol Testing	29
6.5.18 Set Network Penetration Service via PC Web	30
6.5.19 Security Mode Settings	30
6.5.20 Certificate Management	30
Chapter 7 Other Platforms to Configure	32

Chapter 1 Main Interface Description

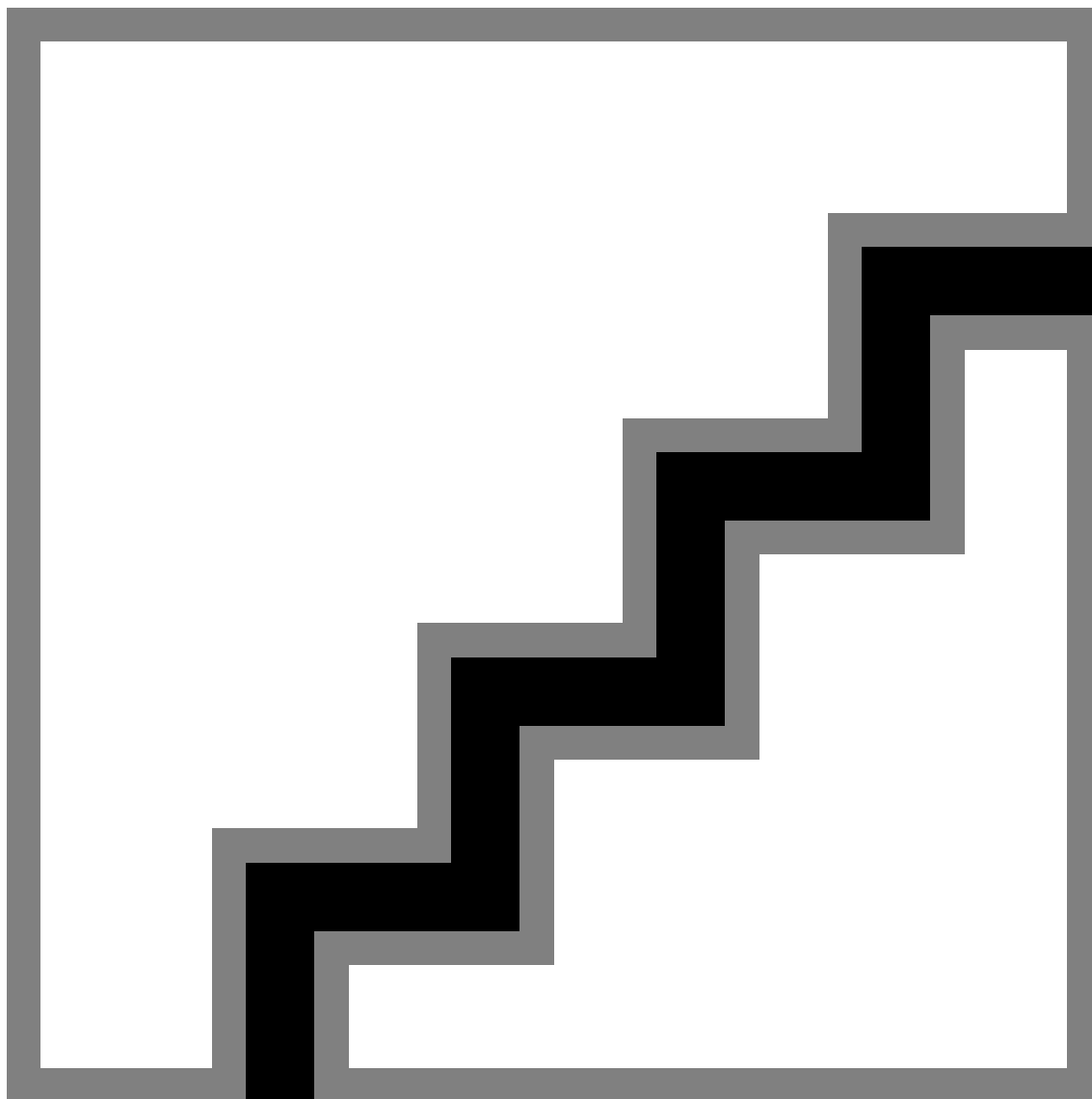


Figure 1-1 Bedhead Terminal Main Interface Description

Bed Information

Displays the bed location and patient care level of the bedhead terminal.

Patient Information

Includes patient name, ID No., patient No., gender, date of birth.

Admission Information

Shows admission date, attending doctor., nurse, and discharge date.

Risk Alert

Displays patient risk alerts.

Messages

Tap to enter the message interface and view historical messages.

Call/ Change Dressing

Tap to call the nurse station host.

Chapter 2 Typical Applications

Typical Application 1: Call/ Dressing Change

You can call or send medication reminders from the bedside terminal to the nurse station host.

1. Complete device wiring and installation. Refer to the Quick Start Guide for details.
2. Add devices in **HikCentral Professional**, then link them to the nurse station host, or link in batch to the nurse station host.
3. Call the nurse station host. Refer to Call Nurse Station Host for details.

Typical Application 2: Applying Patient Information

You can edit patient information in **HikCentral Professional** and applying it to the corresponding bedhead terminal.

Please refer to Adding Patient for details.

Chapter 3 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

3.1 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 be 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).
-

Chapter 4 Local Configuration and Operation

4.1 Local Operation

4.1.1 Messages

You can view medicine reminders, test reminders, examination reminders, allergy reminders and surgery reminders in the Message interface.

Steps

1. On the device main interface, swipe left and tap **Message**.
 - When you have new messages, the home screen displays **New Messages** with the quantity. You can tap **New Messages** to enter the Message interface.
 - When you have no new messages, the home screen displays **No New Message**. You can tap **No New Message** to enter the Message interface.
2. Tap **Medicine Reminders**, **Test Reminders**, **Examination Reminders**, **Surgery Reminders** or **Allergy Reminders** to view corresponding messages.

4.1.2 Health Education

You can view health education information.

Steps

1. On the device main interface, swipe left and tap **Health Education**.
2. Tap the document name to read the full content.

4.1.3 Admission and Discharge Guide

You can view the admission and discharge guide.

Steps

1. On the device main interface, swipe left and tap **Admission and Discharge Guide**.
2. Tap the document name to read the full content.

4.1.4 Hospital/Ward/Department/Physician/Nurse Introduction

You can view hospital introduction, ward introduction, department introduction, doctor introduction, and nurse introduction.

Steps

1. On the device main interface, swipe left to enter the menu page.

2. As needed, tap **Hospital Introduction**, **Ward Introduction**, **Department Introduction**, **Physician Introduction**, or **Nurse Introduction** to view corresponding information.
Swipe left twice to access the second menu page where you can see **Nurse Introduction**.

4.1.5 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.

4.1.6 Call Nurse Station

Describes how to make emergency calls from the Bedhead Terminal to the Nurse Station.

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



Note

Ensure the device is linked to the corresponding host first.

Steps

1. Calling from Bedhead Terminal

Press the call button on the terminal to automatically call the Nurse Station host.

2. Calling via Handset

- Press the call button on the handset to call the Nurse Station.
- Press the dressing change button on the handset to send a dressing change reminder to the nurse station host.



Note

After triggering a call or dressing change reminder:

- Press the button on the handset again to cancel the call.
 - Long press to cancel the dressing change reminder.
-

4.2 Local Configuration of the Device

4.2.1 Activate the Device

You can only configure and operate the device after creating a password for the device activation.

Steps

1. Power on the device. It will enter the activation page automatically.

2. Create a password and confirm it.
3. Tap **OK**. The device will automatically go to the Quick Setup interface.



Note

We highly recommend you to create a strong 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.

4.2.2 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.

4.2.3 Device Information

View the device information, including the version information, model, serial No. etc..

Steps

1. On the device main interface, swipe left twice and tap **Settings → About this product** to view current device version and other information.
2. View the device information, user manual and open source software license.
3. **Optional:** Tap **Open Source Software License** to view the OSS statement.
4. **Optional:** Tap **Device Restart** to restart the device.

5. Optional: Tap **User Manual**. Use your phone to scan the pop-up QR code to view the user manual.

4.2.4 Basic Settings

Call Settings

You can set the device call volume.

Steps

1. Tap **Settings** → **Call Settings** to enter the call settings page.
2. Set corresponding parameters.

Call Volume

Drag the slider to adjust the call volume. Range: 1-10.

General Settings

You can view the device's date, time, timezone, and configure screen brightness and screen-off time.

Click **Settings** → **General Settings** to enter the page.

View the device's date, time, and timezone.



Note

Device time can be configured on the web client. For details, refer to Set Device Time.

Slide the slider to adjust screen brightness.

Click **Screen-off Time**, select the desired duration based on actual needs, then click **OK** to save settings.

Set Basic Settings for Broadcast

You can select audio file for broadcasting or click to do a real-time broadcast.

On main the page, click **Broadcast** to enter the setting page.

Select the devices for broadcast playback, or click **Select All** in the upper-right corner of the interface to choose all devices.

Start broadcasting.

- For real-time broadcast: click the microphone icon to begin.
- For audio file broadcast: select the audio file to play before starting.

4.2.5 Advanced Settings

Steps

1. Click **Settings** → **Advanced Settings** , then enter admin password to enter the page.
2. You can modify the local IP address, subnet mask, gateway, server IP, port number, department/ward, and usage mode, and view the SIP service address.

ID Configuration

Configure ID No. for medical intercom system.

Steps

1. On the device main interface, swipe left twice and tap **Settings**.
2. Tap **Advanced Settings** → **ID Configuration** , and enter the engineering password to enter the setting page.
The engineering password is created by the platform.
3. Configure the hospital No., ward No., floor No., room No., and bed No. where the device is located.
4. Tap **OK** to save the settings.

SIP Settings

Devices in the medical intercom system must be registered to a unified SIP server for normal call functionality.

Steps

1. On the device main interface, swipe left twice and tap **Settings**.
2. Tap **Advanced Settings** and enter the engineering password.
The engineering password is created by the platform.
3. Enter the IP address and port number of the nurse station host to be used as the server in **Server IP** and **Port No.**.
4. Tap **OK** to save the configuration.

Local Network Configuration

After device activation, modify the network parameters of the device. The device IP address must be in the same network segment as other devices in the intercom system for normal communication.

Steps

1. On the device main interface, swipe left twice and tap **Settings**.
2. Tap **Advanced Settings**, enter the engineering password to access the advanced settings page.

The engineering password is created by the platform.

3. Configure network parameters. Manually enter the local IP address, subnet mask, and gateway.

4. Click **Save**.

Chapter 5 Quick Operation via Web Browser

5.1 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.

5.2 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.

5.3 Time Settings

Time Sync

Device Time 2024-05-08 14:00:58

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

Time Synchronization mode ☒ NTP ☐ Manual

* Server IP Address 0.0.0.0

* NTP Port 123

* Interval 60 min ▲▼

[Previous](#) [Next](#) [Skip](#)

Figure 5-1 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.

5.4 Administrator Settings

Steps

1. Click  in the top right of the web page to enter the wizard page. After setting previous parameters, you can click **Next** to enter the **Administrator Settings** page. Or you can click **Skip** to enter the **Administrator Settings** page directly.
2. Enter the employee ID and name of the administrator.
3. Select a credential to add.
 - 1) Click **Add Card** to enter the Card No. and select the property of the card.



Note

Up to 5 cards can be supported.

4. Click **Complete** to complete the settings.

5.5 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**.

Device No.

No.	Formerly known as	Custom Name	No.
Community No.	Hospital No.		44
Building No.	Floor No.		1
Unit No.	Ward No.		1
Room No.	Room No.		1
Door Station No.	Bed No.		2

Video Intercom Network

*Registration Password

*Main Station IP

*Private Server IP

Figure 5-2 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 99.

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 6 Operation via Web Browser

6.1 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.

6.2 Overview

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

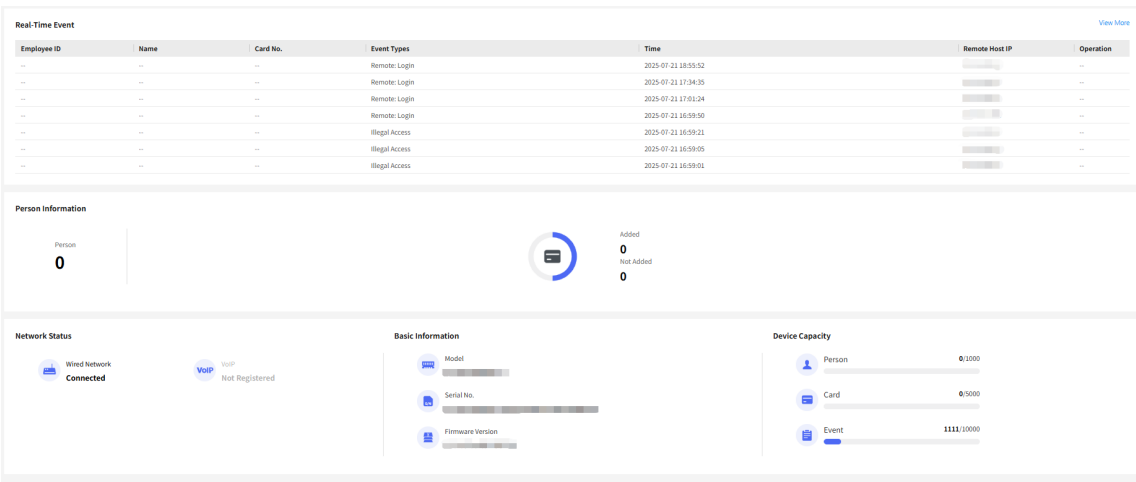


Figure 6-1 Overview Page

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**.

6.3 Person Management

Click **Person Management** at the main page to enter the configuration page.

Click **+ Add** to add the person's information, including the basic information, certificate, 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.

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.



Note

Up to 5 cards can be supported.

Click **Save** to save the settings.

6.4 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.

6.5 Configuration

6.5.1 View Device Information

View the device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, 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, IO input, IO output, local RS-485, alarm input and alarm output number.

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

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

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

6.5.2 Set Time

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

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

Device Time 2015-01-02 19:39:07

Time Zone (GMT+00:00) Dublin, Edinburgh, London

Time Synchronization mode ☐ NTP ☒ Manual

Set Time 2015-01-02 19:38:43 Sync With Comp...

Save

Figure 6-2 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.

6.5.3 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.)
-

6.5.4 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.

6.5.5 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.

6.5.6 Network Settings

Set Basic Network Parameters via PC Web

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

DHCP ☐

*IPv4 Address

*IPv4 Subnet Mask

*IPv4 Default Gateway

Mac Address

MTU

* Alarm Center IP

* Alarm Host Port

DNS Server

Preferred DNS Server

Alternate DNS Server

Save

Figure 6-3 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.

VoIP Account Settings

You can realize voice call by network.

Steps

1. Go to **Configuration → Network → Device Access → VoIP**.
2. Slide 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. Slide 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.

6.5.7 Set Video and Audio Parameters

Set the image quality and resolution.

Set Audio Parameters

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

The screenshot shows the 'Audio' settings page. At the top, 'Stream Type' is set to 'Main Stream'. Below it, 'Audio Encoding' is set to 'G.711ulaw'. 'Audio Input Type' is set to 'External Handle Microphone' with a dropdown arrow, and a 'Custom' checkbox is checked. There are three volume sliders: 'Input Volume', 'Output Volume', and 'Speak Volume', each with a red progress bar and a numeric input field set to '7'. At the bottom, there is a red 'Save' button.

Figure 6-4 Audio Settings Page

Set the audio input volume, output volume, speak volume and audio input type.

Check **Custom**, then you can select audio input type according to your actual needs .

Click **Save** to save the settings.

6.5.8 Call Settings

Device No. Settings

Steps

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

No.	Original Name	Custom Name	No.
	Community No.	Hospital No.	1
	Building No.	Floor No.	1
	Unit No.	Ward No.	1
	Room No.	Room No.	1
	Door Station No.	Bed No.	1

Save

Figure 6-5 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

Slide 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 devices.

Set Ringtone on PC Web

Steps

1. Click **Configuration → Intercom → Ringbacktone Settings** to enter the settings page.
 2. Click  to import new ringtone.
-

Note

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

6.5.9 Add Broadcast Materials

You can add and delete broadcast materials in.

Steps

1. Click **Configuration → Broadcast Settings → Dtabase** 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.

6.5.10 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.

6.5.11 Privacy Settings

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

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

Event Storage Settings

Event Storage Type ☐ Delete Old Events Periodically
☐ Delete Old Events by Specified Time
☒ Overwrite

Patient Information Desensitization Display

Patient Name Desensitization Display ☒

Patient No. Desensitized Display ☒

Patient's Date of Birth Desensitized ... ☐

Patient ID No. Desensitization Display ☒

Patient's Attending Physician Name ... ☒

Patient's Care Nurse Name Desensi... ☒

Save

Figure 6-6 Privacy Settings

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 physician's name and care nurse's name.

6.5.12 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.

CPU Card Read Content

After enabling CPU card and CPU card read content, the device support CPU card recognition and data reading .

6.5.13 Set Preference

You can set the sleep time for the device.

Set Theme

Click **Configuration** → **Preference** .

Custom Screen Saver ☒

Screen Saver Picture Duration s

Sleep ☒

Sleep after s

Start Time

End Time

Save

Figure 6-7 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.

6.5.14 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 slide 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.

6.5.15 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: 30 to 300s.

Capture Packet Size Range: 1 to 100MB.

3. Click **Save**.

6.5.16 Security Audit Log

Steps

1. Click **Maintenance → Security Audit Log** to enter the page.
2. You can slide to enable **Log Upload Server**, **Encrypt Transmission** 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.

6.5.17 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.

6.5.18 Set Network Penetration Service via PC Web

When the device 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 **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.

6.5.19 Security Mode Settings

Set the security mode for logging in the client software.

On the Device for Management page, click **Maintenance and Security → Security → Security Service**.

Select a security mode, and click **Save**.

Security Mode

High security level for user information verification when logging in the client software.

Compatible Mode

The user information verification is compatible with the old client software version when logging in.

6.5.20 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 7 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