Video Intercom Villa Door Station

User Manual

Legal Information

©2022 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***).
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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 MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

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.

Safety Instruction

Warning

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

Caution

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.

- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Input voltage should meet both the SELV and the Limited Power Source according to 60950-1 standard.
- The power supply must conform to LPS. The recommended adaptor models and manufacturers are shown as below. Use the attached adapter, and do not change the adaptor randomly.

Model	Manufacturer	Standard
ADS-24S-12 1224GPCN	SHENZHEN HONOR ELECTRONIC CO.,LTD	CEE
G0549-240-050	SHENZHEN GOSPELL DIGITAL TECHNOLOGY CO.,LTD	CEE
TS-A018-120015Ec	SHENZHEN TRANSIN TECHNOLOGIES CO., LTD	CEE

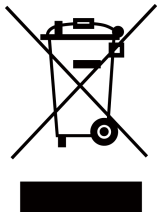
Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help
FCC Conditions
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see:www.recyclethis.info

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.

Contents

Chapter 1 Appearance 1

Chapter 2 Terminal and Wiring Description 3

2.1 Terminal Description 3

Chapter 3 Installation 5

3.1 Accessory Introduction 5

3.2 Surface Mounting 6

3.3 Flush Mounting 8

Chapter 4 Activation 10

4.1 Activate Device Locally 10

4.2 Activate Device via Web 10

4.3 Activate Device via Client Software 11

Chapter 5 Local Configuration 12

5.1 Quick Configuration 12

5.2 Authentication via Admin 18

5.3 Forget Admin Password 20

5.4 User Management 22

5.5 Network Parameters Settings 24

5.5.1 Edit Wired Network Parameters 24

5.5.2 Connect to Wi-Fi 26

5.5.3 Cloud Service Settings 27

5.5.4 Device Hotspot 28

5.6 Local Settings 30

5.7 System Maintenance 31

Chapter 6 Local Operation 34

6.1 Call from the Device 34

6.1.1 Call Resident 34

6.1.2 Call Center 37
6.2 Unlock Door 37
6.2.1 Unlock by Password 37
6.2.2 Unlock by Face 37
6.2.3 Unlock by Presenting Card 37
6.2.4 Unlock by QR Code 37
Chapter 7 Quick Operation via Web Browser 39
7.1 Change Password 39
7.2 Select Language 39
7.3 Time Settings 39
7.4 Environment Settings 40
7.5 Administrator Settings 40
7.6 No. and System Network 41
Chapter 8 Operation via Web Browser 42
8.1 Login 42
8.2 Forget Password 42
8.3 Overview 42
8.4 Person Management 44
8.5 Device Management 46
8.6 Configuration 47
8.6.1 Set Local Parameters 47
8.6.2 View Device Information 47
8.6.3 Set Time 47
8.6.4 Set DST 48
8.6.5 Change Administrator's Password 48
8.6.6 Online Users 48
8.6.7 View Device Arming/Disarming Information 49
8.6.8 Network Settings 49

8.6.9 Set Video and Audio Parameters 53
8.6.10 Set Image Parameters 54
8.6.11 Motion Detection 55
8.6.12 Event Linkage 56
8.6.13 Access Control Settings 57
8.6.14 Intercom Settings 60
8.6.15 Set Card Security 63
8.6.16 Set Biometric Parameters 63
8.6.17 Set Screen Display 65
8.6.18 Upgrade and Maintenance 66
8.6.19 Device Debugging 67
8.6.20 Certificate Management 67
Appendix A. Communication Matrix and Device Command 69

Chapter 1 Appearance

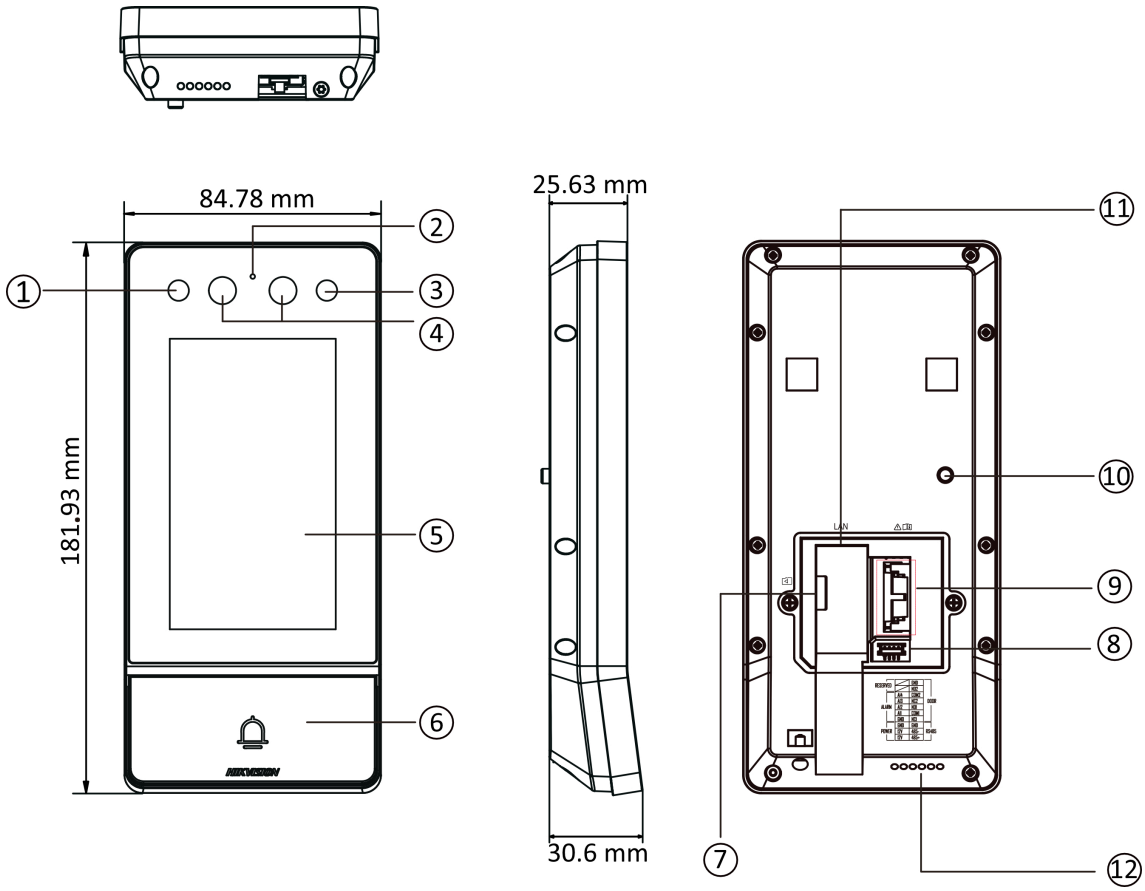


Figure 1-1 Device Appearance

Table 1-1 Description

No.	Description
1	IR Light
2	Microphone
3	IR Light
4	Camera
5	Touch Screen
6	Button
7	TF Card Slot

No.	Description
8	Debugging Port
9	TAMPER
10	Terminals
11	Network Interface
12	Loudspeaker

Chapter 2 Terminal and Wiring Description

2.1 Terminal Description

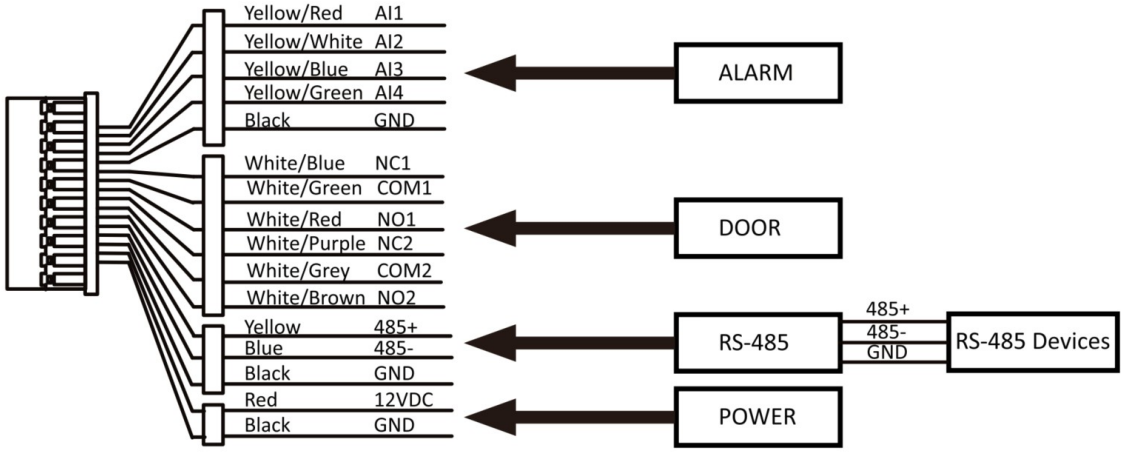


Figure 2-1 Terminal Description

Table 2-1 Description of Terminal and Interfaces

Name	Interface	Description
DOOR	NC2	Door Lock Relay Output 2 (NC)
	COM2	Common Interface
	NO2	Door Lock Relay Output 2 (NO)
	NC1	Door Lock Relay Output 1 (NO)
	COM1	Common Interface
	NO1	Door Lock Relay Output 1 (NO)
ALARM IN	AI1	Alarm Input 1 (For the access of Door Contact)
	AI2	Alarm Input 2 (For the access of Door Contact) **Note** Before accessing to the Door Contact, select **Input** as **Door Status** in **I/O Settings** page first.
	AI3	Alarm Input 3 (For the access of Exit Button)

Name	Interface	Description
	AI4	Alarm Input 4 (For the access of Exit Button) **Note** Before accessing to the Exit Button, select **Input** as **Exit Button** in **I/O Settings** page first.
	GND	Grounding
RS-485	485+	RS-485 Communication Interface
	485-	
Power Input	GND	12 VDC Input

Chapter 3 Installation

Note

- Make sure the device in the package is in good condition and all the assembly parts are included.
- Make sure your power supply matches your door station.
- Make sure all the related equipment is power-off during the installation.
- Check the product specification for the installation environment.

3.1 Accessory Introduction

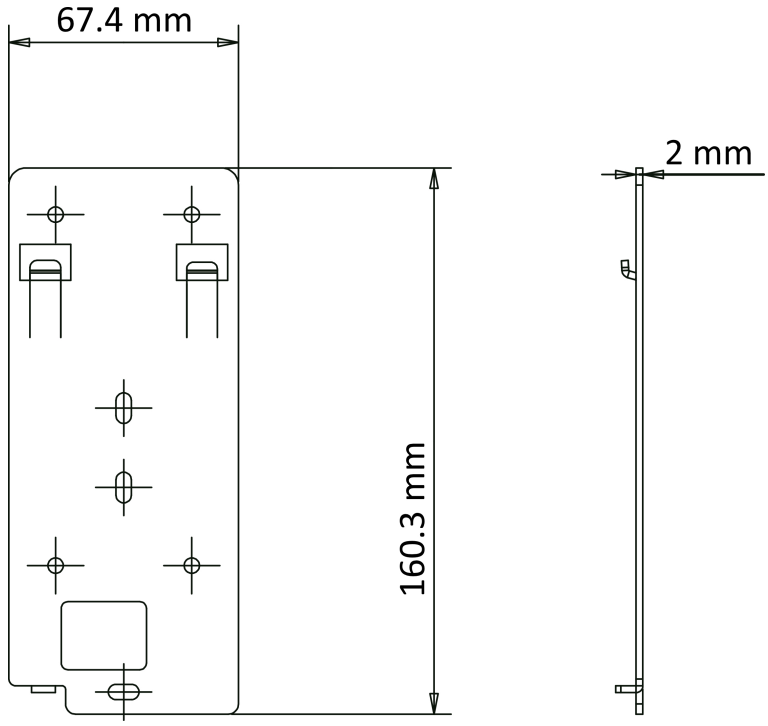


Figure 3-1 Installation Plate

Note

The dimension of plate for door station is: 160.3 mm × 86 mm.

3.2 Surface Mounting

Steps

1. Stick the mounting template on the wall. Drill screw holes according to the mounting template. Remove the template from the wall.

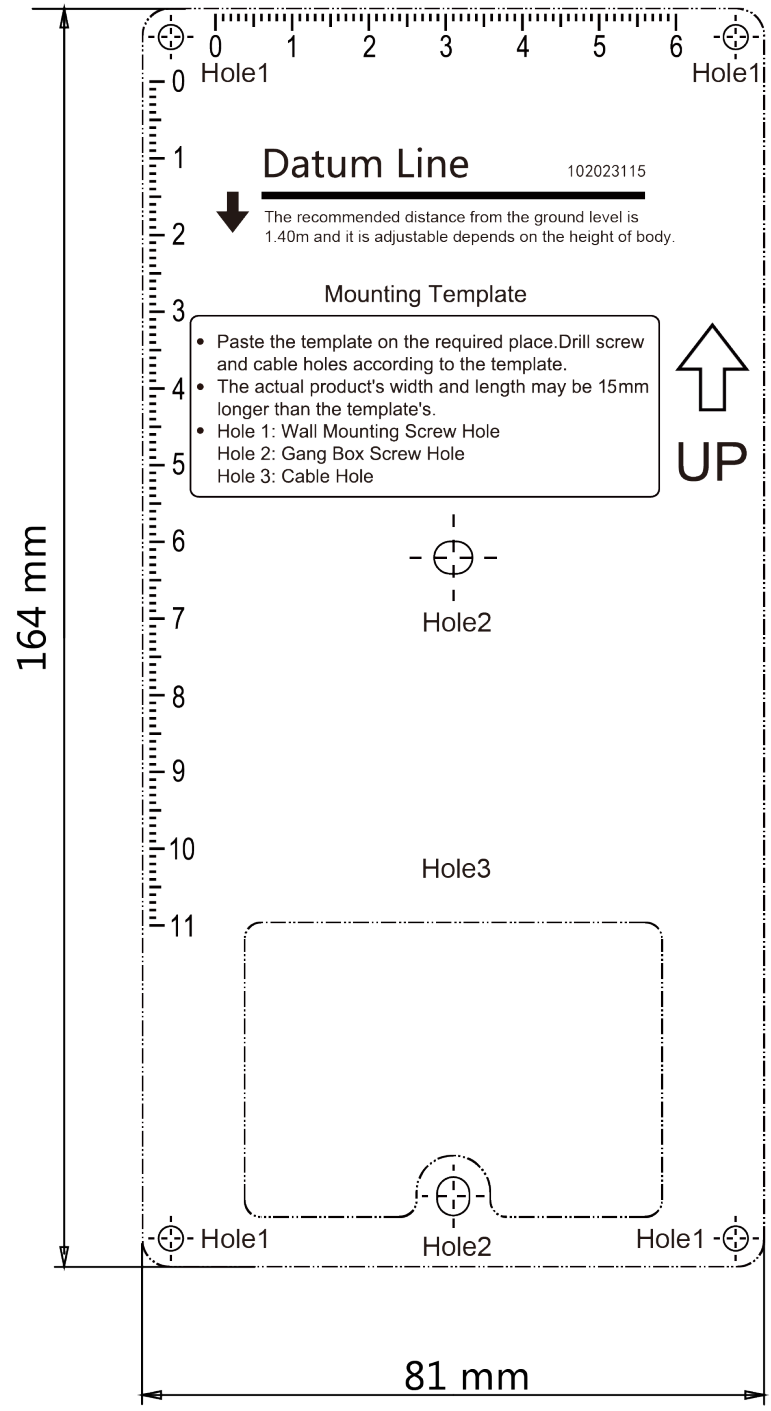


Figure 3-2 Mounting Template

2. Secure the mounting plate on the gang box with the 4 supplied screws (SC-KA4X25). Remove the back cover and route the cable through the cable hole, wire the cables and insert the cables in the gang box.

3. Align the device with the mounting plate, and secure the device on the mounting plate with 1 supplied screw (SC-M3X8NL-SUS316L-GB78).

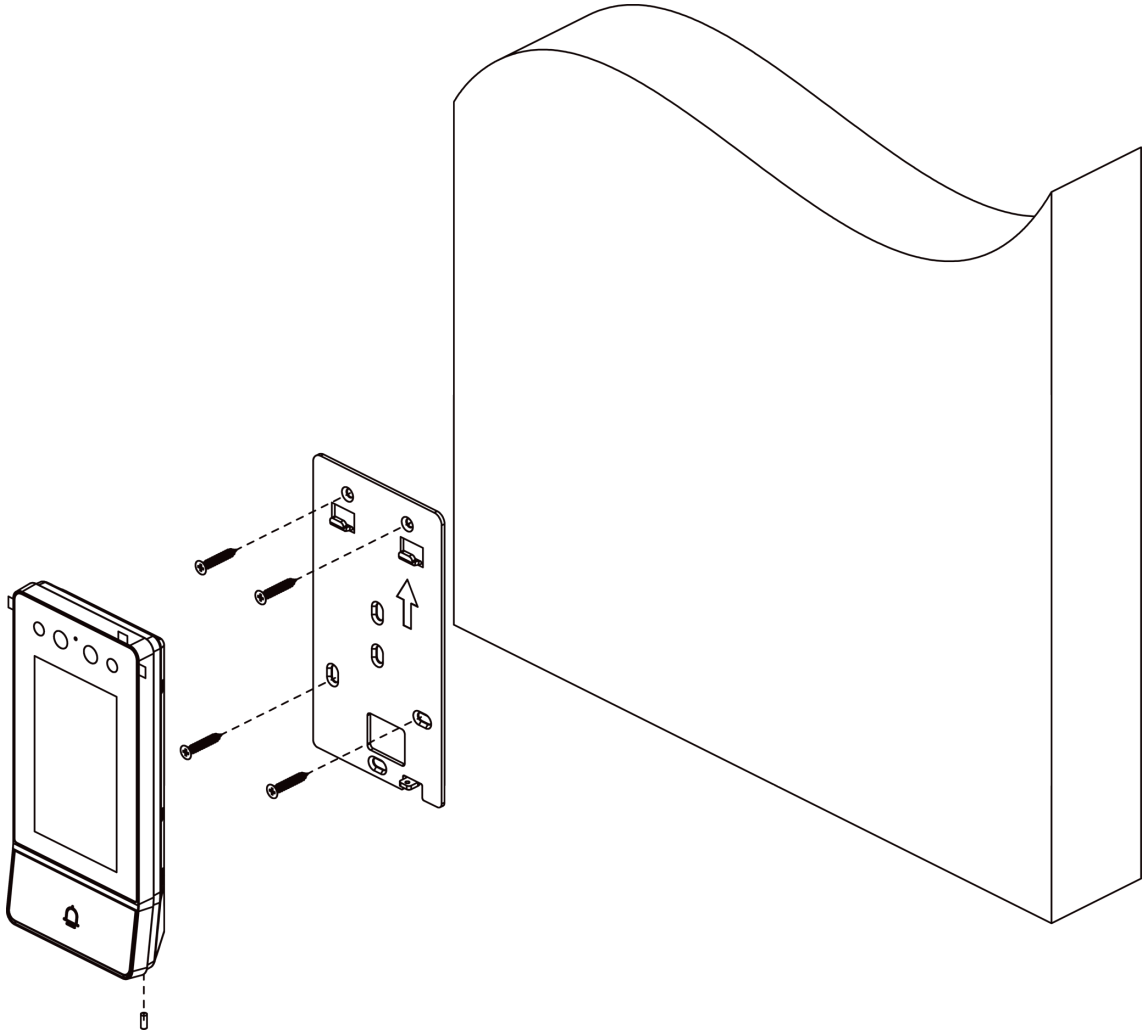


Figure 3-3 Surface Mounting

3.3 Flush Mounting

Steps

1. Make sure the gang box is installed on the wall.
2. Secure the mounting plate on the gang box with the four supplied screws (SC-KA4X25).
3. Remove the back cover and route the cable through the cable hole, wire the cables and insert the cables in the gang box.
4. Align the device with the mounting plate, and secure the device on the mounting plate with 1 supplied screw (SC-M3X8NL-SUS316L-GB78).

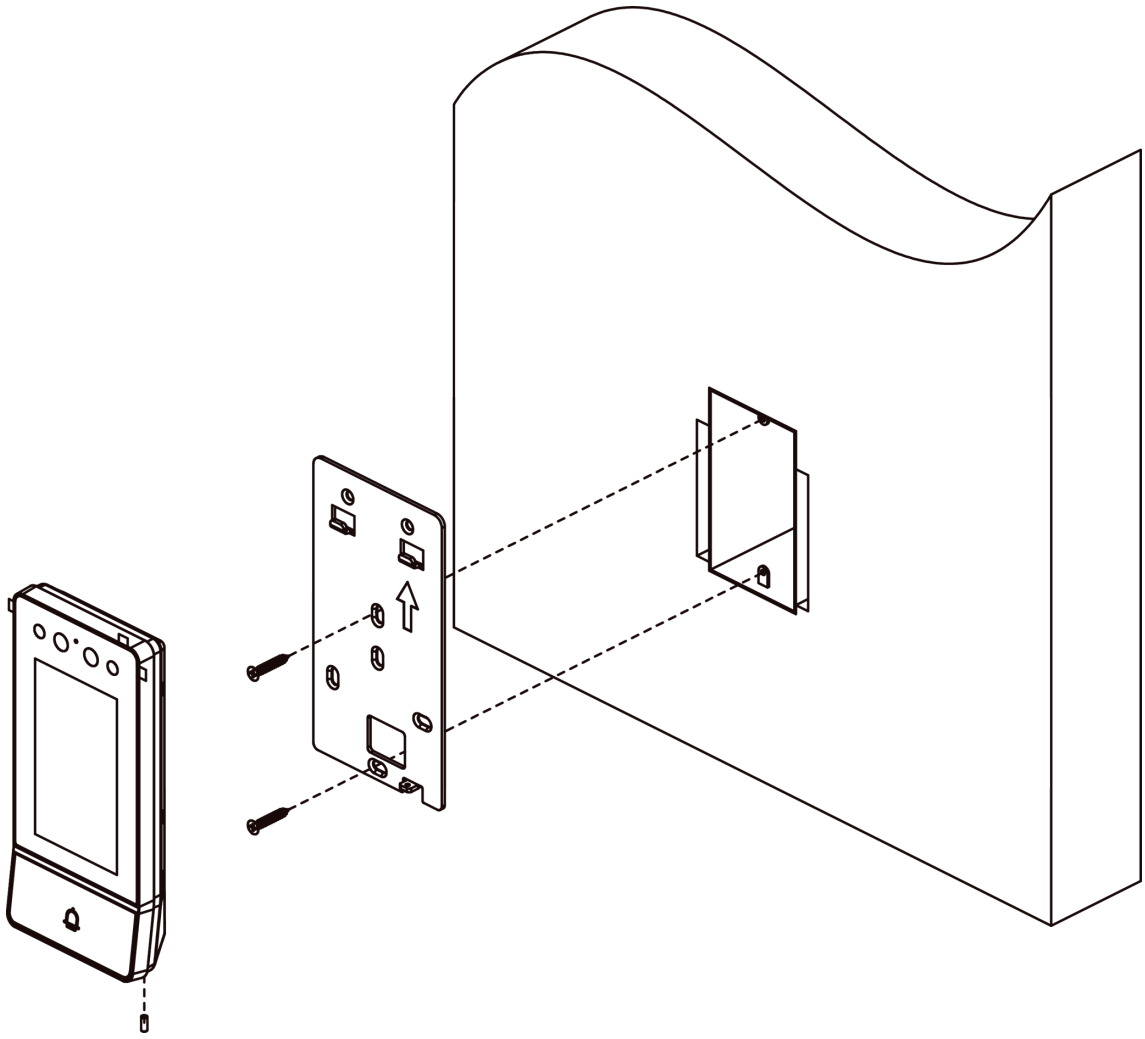


Figure 3-4 Flush Mounting

Chapter 4 Activation

4.1 Activate Device Locally

You are required to activate the device first by settings a strong password for it before you can use the device.

Steps

1. Power on the device to enter the activation page automatically.
2. Create a password and confirm it.

   Note

   You can tap to enable or disable password reveal.
3. Tap **Next** to finish activation.

   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.

What to do next

After activating the device, the quick configuration page will pop-up automatically. Refers to ***Quick Configuration*** for details.

4.2 Activate Device via Web

You are required to activate the device first by setting a strong password for it before you can use the device.

Default parameters of the door station are as follows:

- Default IP Address: 192.0.0.65.
- Default Port No.: 8000.
- Default User Name: admin

Steps

1. Power on the device, and connect the device to the network.
2. Enter the IP address into the address bar of the web browser, and click **Enter** to enter the activation page.

Note

The computer and the device should belong to the same subnet.

3. Create and enter a password into the password field.
4. Confirm the password.
5. Click **OK** to activate the device.

4.3 Activate Device via Client Software

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

Default parameters of door station are as follows:

- Default IP Address: 192.0.0.65.
- Default Port No.: 8000.
- Default User Name: admin.

Steps

1. Run the client software, click **Maintenance and Management → Device Management → Device** to enter the page.
2. Click **Online Device**.
3. Select an inactivated device and click **Activate**.
4. Create a password, and confirm the password.

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.

5. Click **OK** to activate the device.

Note

- When the device is not activated, the basic operation and remote operation of device cannot be performed.
- You can hold the **Ctrl** or **Shift** key to select multiple devices in the online devices, and click the **Activate** button to activate devices in batch.

Chapter 5 Local Configuration

5.1 Quick Configuration

After activating the device, the quick configuration page will pop up automatically.

Steps

1. Select the system language and tap **NEXT**.

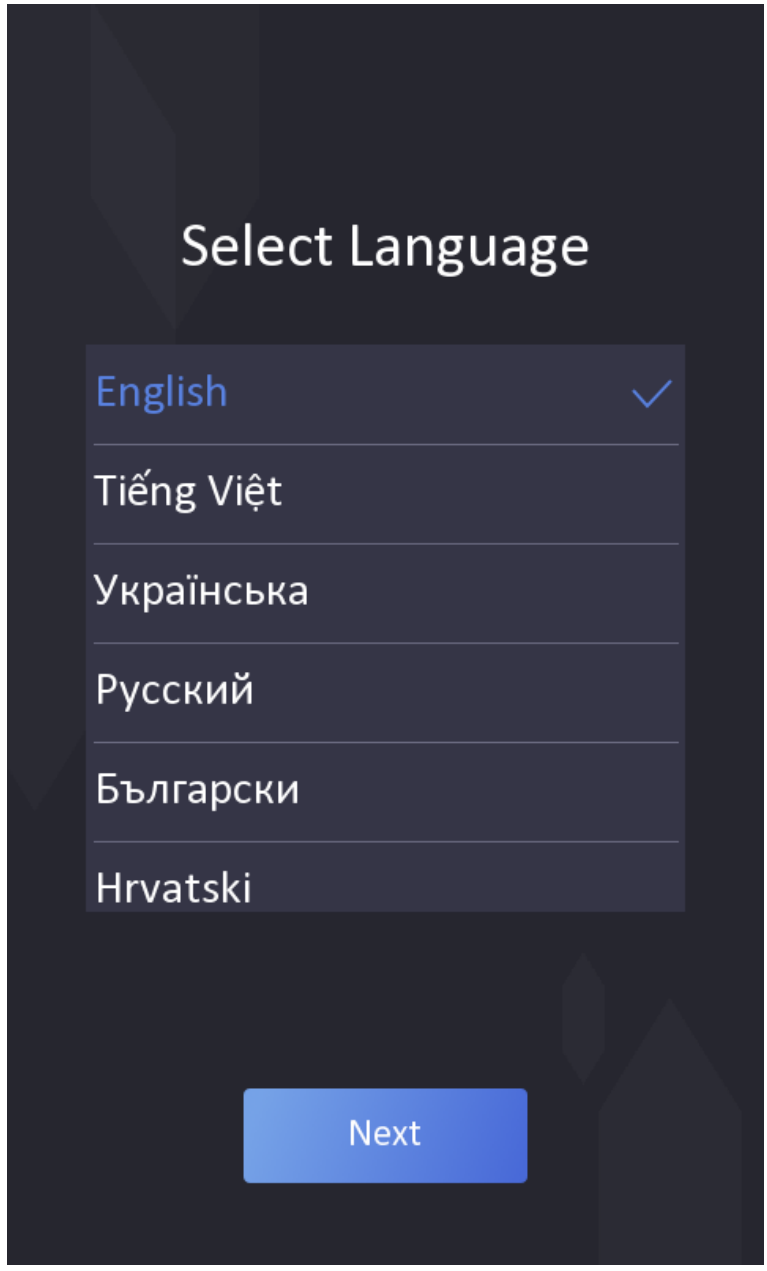


Figure 5-1 Select Language

2. Set password reset method and tap **NEXT**.

- Enter the Reserved Email address, then you can reset the admin password by email.

Note

On the security questions settings page, you can tap **Change to Reserved Email** to modify the password reset method.

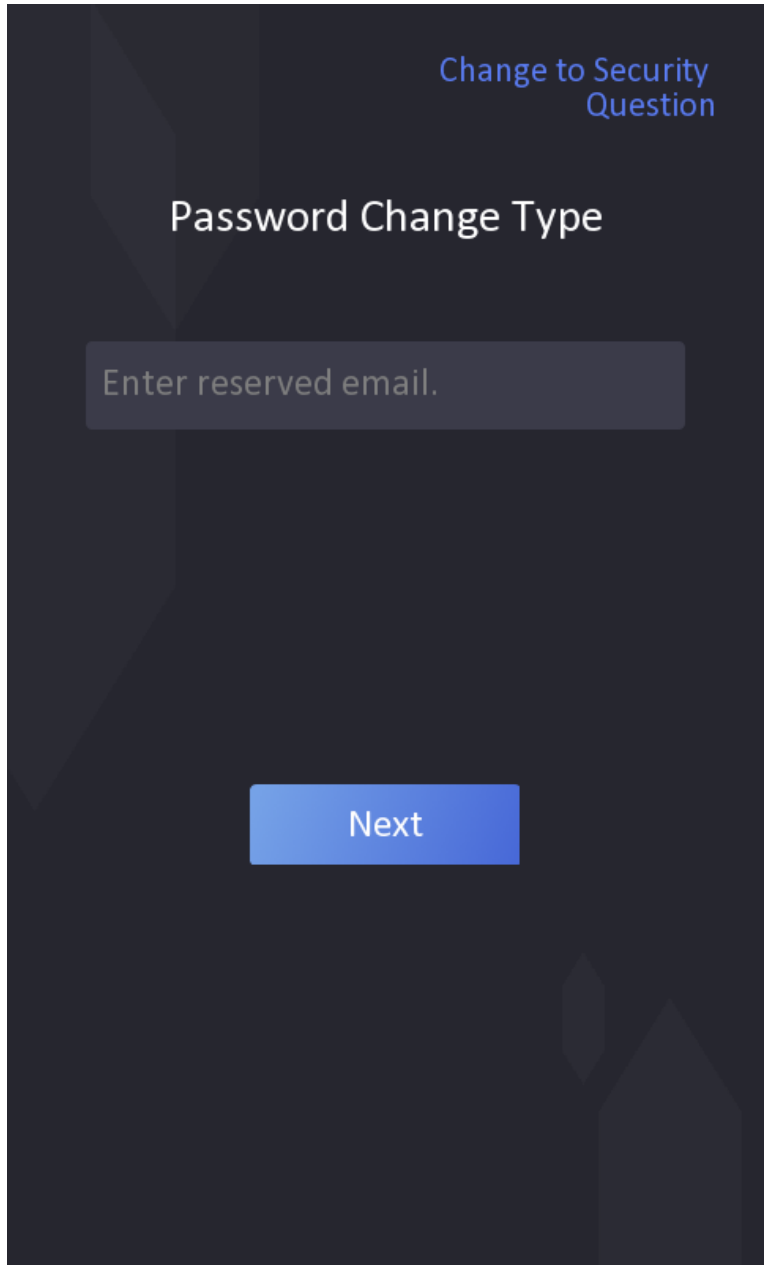


Figure 5-2 Password Reset by Setting Reserved Email Address

- Tap **Change to Security Question**. Select 3 security questions from deficiency list and enter the answers of the questions, then you can reset the password by answering security questions.

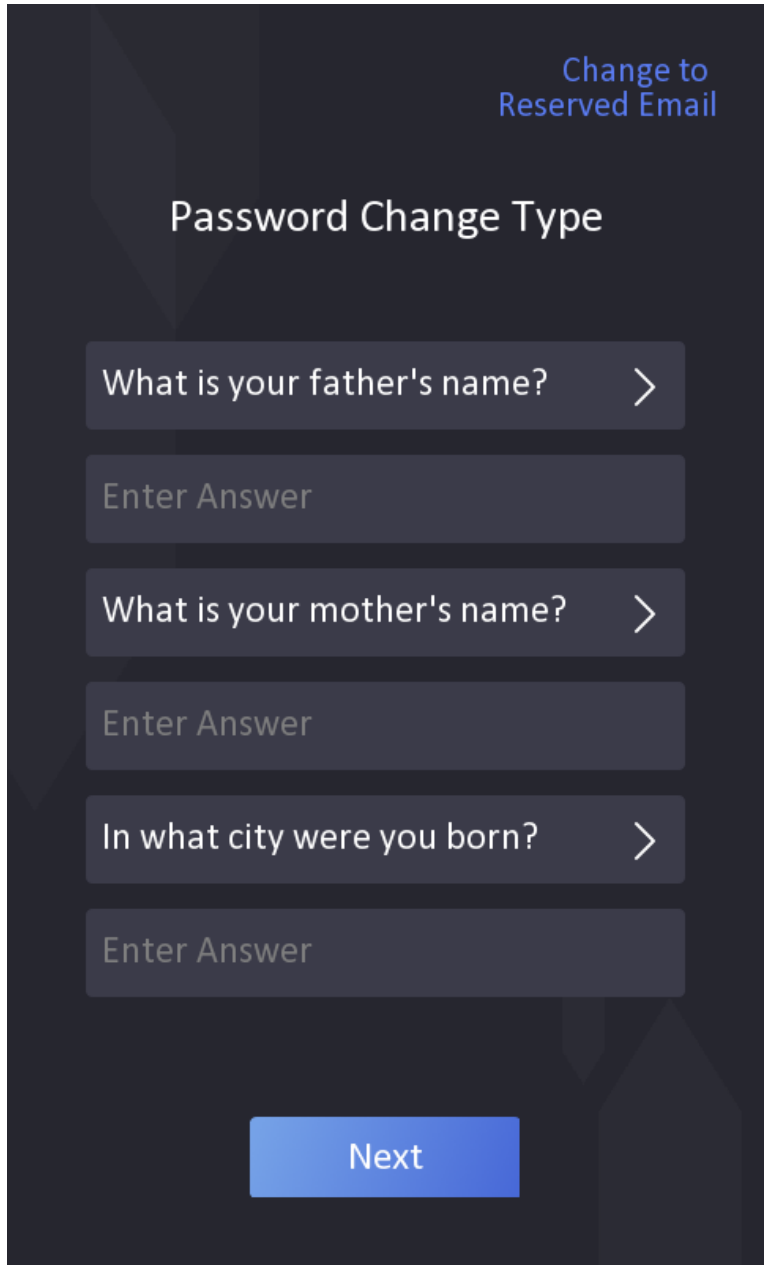


Figure 5-3 Password Reset by Setting Security Questions

3. Set network parameters and tap **NEXT**.

-

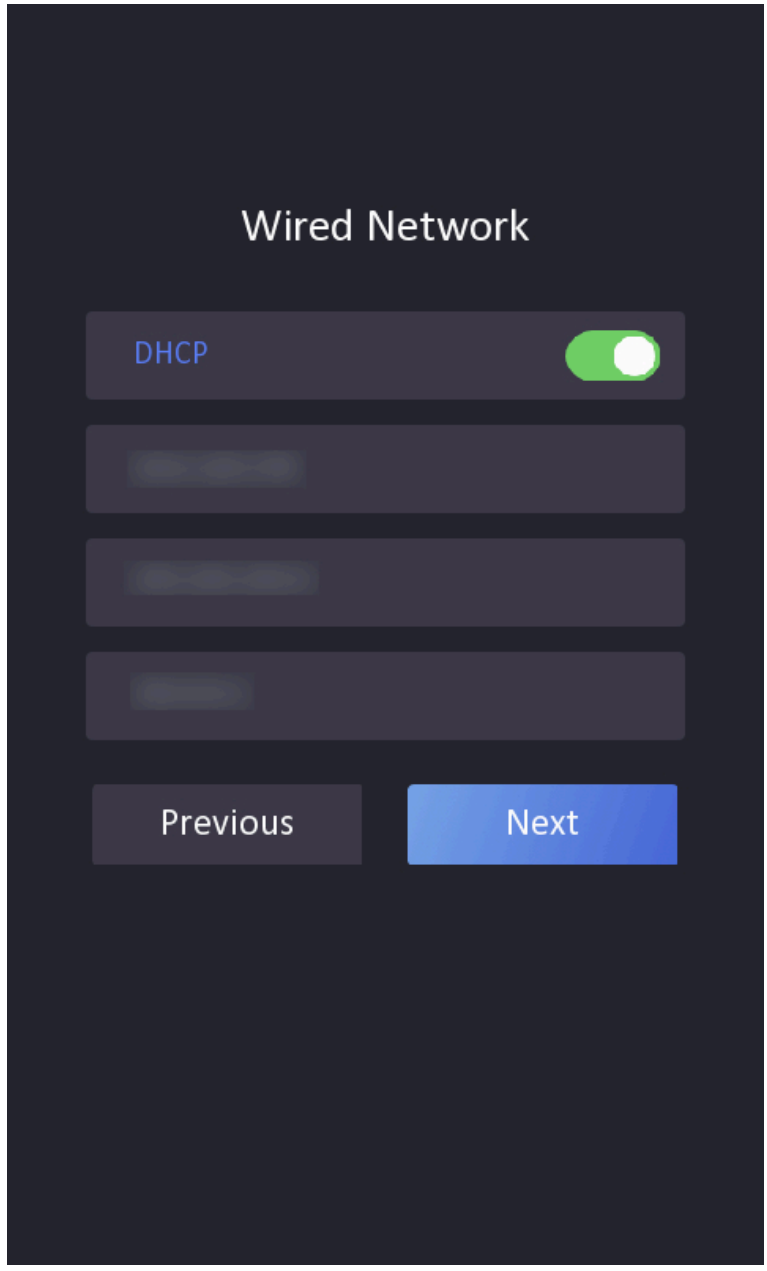


Figure 5-4 Wired Network

Set the **IP address**, **Subnet Mask** and **Gateway** manually.

Enable **DHCP**, the device will get network parameters automatically.

-

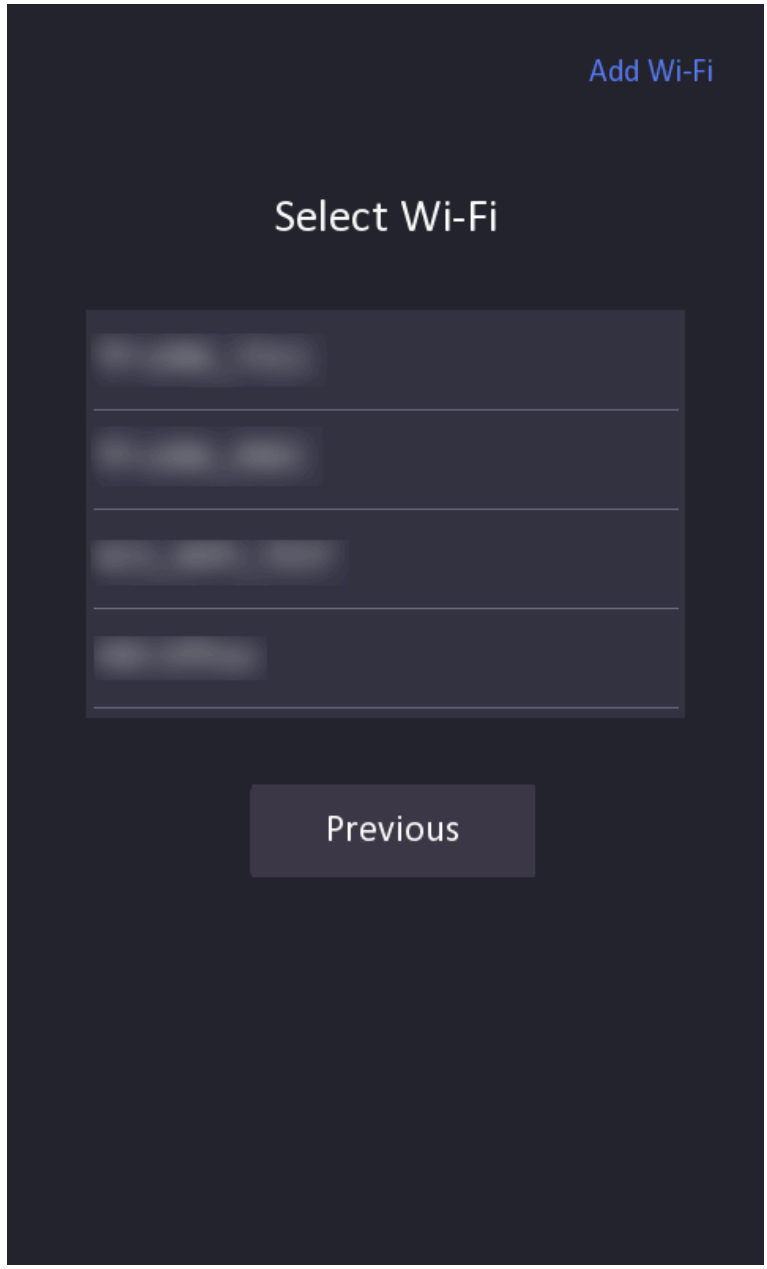


Figure 5-5 Wireless Network

4. Enable the cloud service functions and create a verification code. Tap **NEXT**.

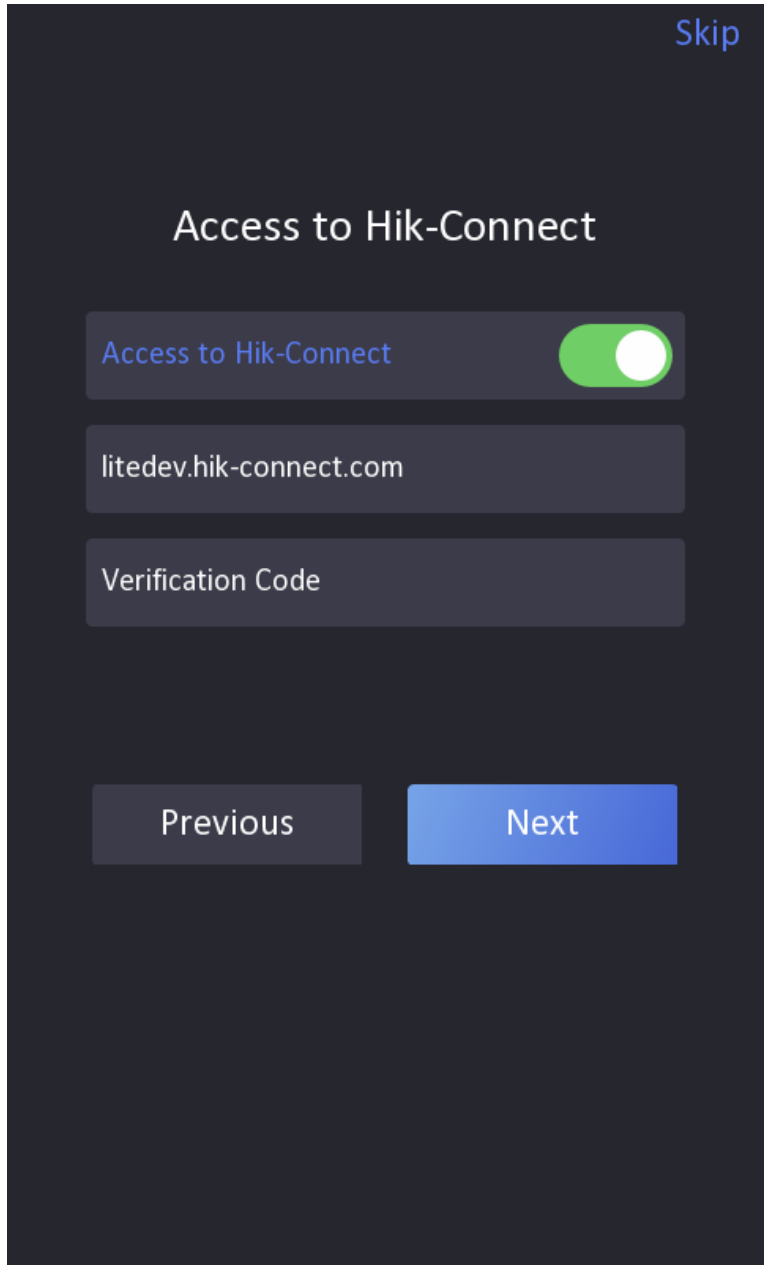


Figure 5-6 Cloud Service

5. Tap **Next** to finish wizard.

5.2 Authentication via Admin

You can configure the parameters of the device on the menu page. You should authenticate to enter the menu.

If you want to authenticate via face or card, you should add administrator first. Refers to ***User Management*** for details.

Steps

1. Hold the screen to enter the authentication page.
2. You can enter the admin password or authentication via face or card to enter the menu.

Note

Admin password is set as activation password.

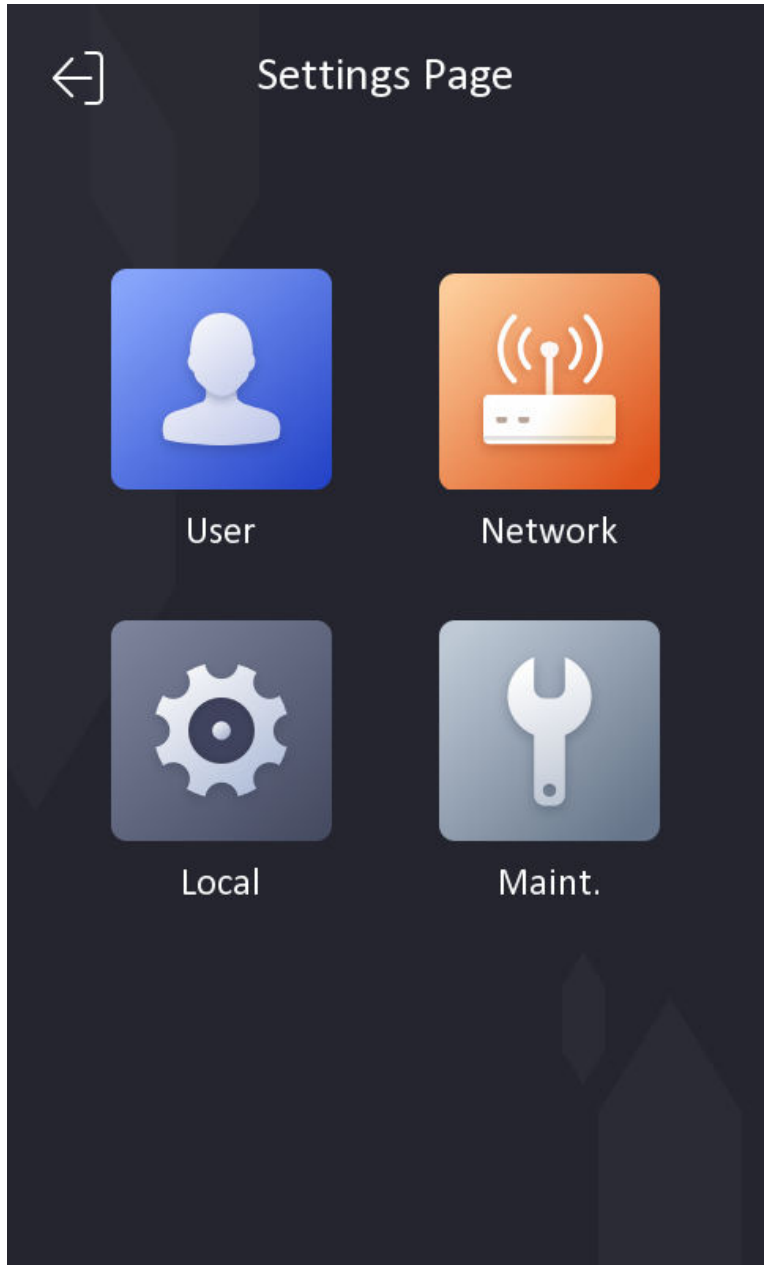


Figure 5-7 Menu Page

5.3 Forget Admin Password

Admin password is used for authenticating to enter the local configuration menu. If you forget the password, you can change it by entering security questions' answers.

Steps

1. Hold the main page to enter the authentication page.

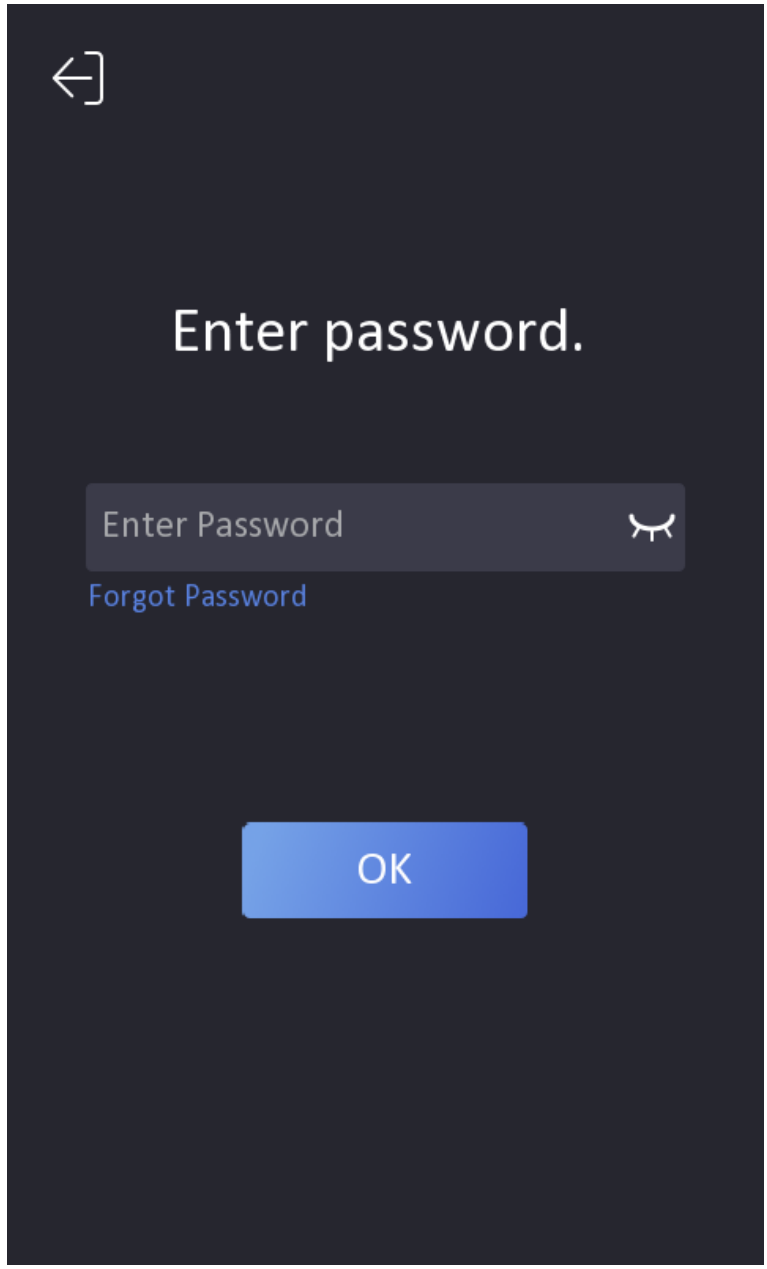


Figure 5-8 Authentication Page

2. Tap **Forgot Password**.
3. Change the admin password via entering answers of security questions or email address.
4. Create and confirm a new password.

5.4 User Management

On the user management page, you can add new users, configure the user's room information, card information, and face information.

Before You Start

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

Steps

1. On the menu, tap **User** to enter the settings page.

Figure 5-9 User Management

2. Tap **+** to enter the add user page.
3. Set **Employee No.**, **Name**, **Room No.** and **Floor No.**.
4. Add **Face**.
   1) Tap **Face Picture**, and point the face at the camera.
   2) Tap to add the face.
   3) Tap to enable the settings.
5. Add **Card**.
   1) Tap **Card**, and tap **+** to enter the add card page.

2) Enter the card No. manually or present the card in the card presenting area to obtain the card No.
3) Tap **OK** to enable the settings.

6. Set **User Role** as **Normal User** or **Administrator**.
7. Exit the settings page.

5.5 Network Parameters Settings

The device support wired network, wireless network, cloud service settings and hotspot.

5.5.1 Edit Wired Network Parameters

The device should be connected to the network.

Before You Start
Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

Steps
1. On the menu, tap **Network → Wired Network** to enter the settings page.

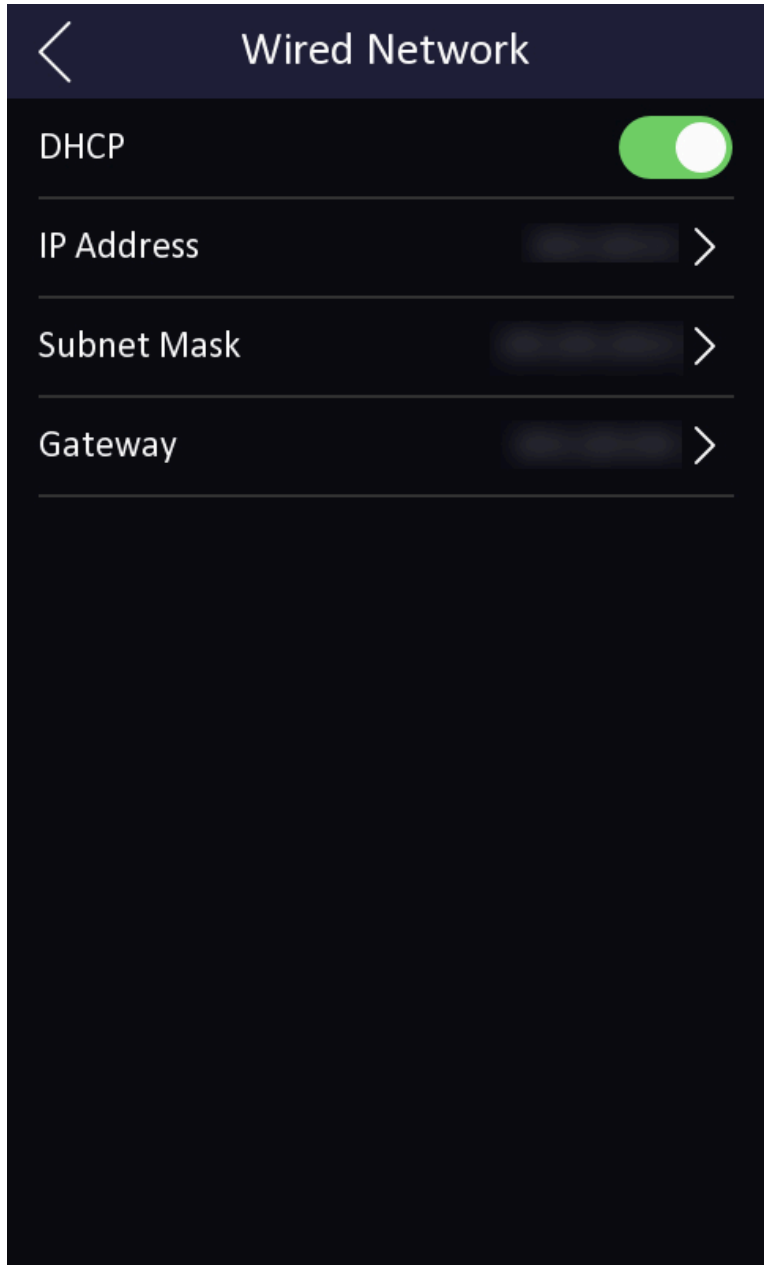


Figure 5-10 Wired Network Settings

2. Edit the wired network parameters.

- Edit the wired network parameters manually.
- Enable **DHCP**, and the system will get the parameters automatically.

5.5.2 Connect to Wi-Fi

Before You Start

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

Steps

1. On the menu, tap **Network → Wi-Fi** to enter the settings page.

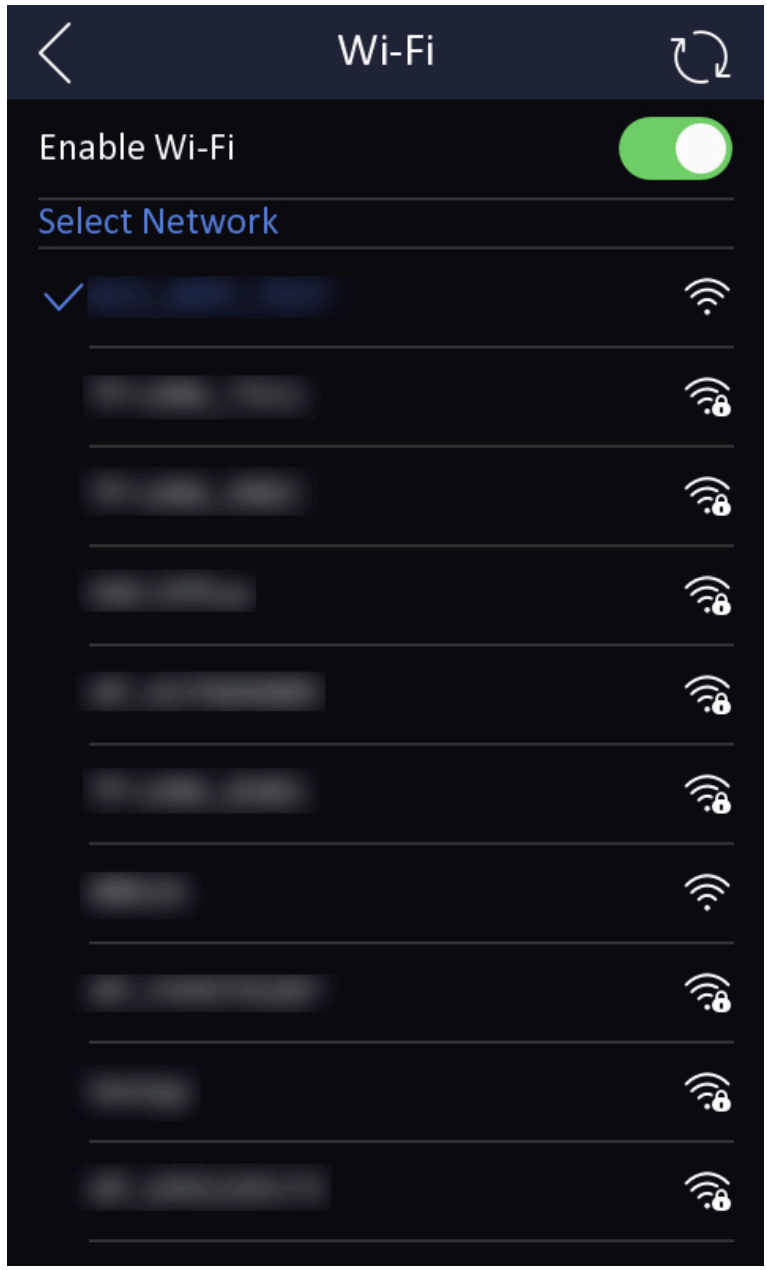


Figure 5-11 Wi-Fi Settings

2. Slide to enable the function.

3. Select a Wi-Fi and enter the password to connect.

5.5.3 Cloud Service Settings

Enable the function, you can configure the device via mobile client remotely.

Before You Start
Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

Steps
1. On the menu, tap **Network → Cloud Service** to enter the settings page.

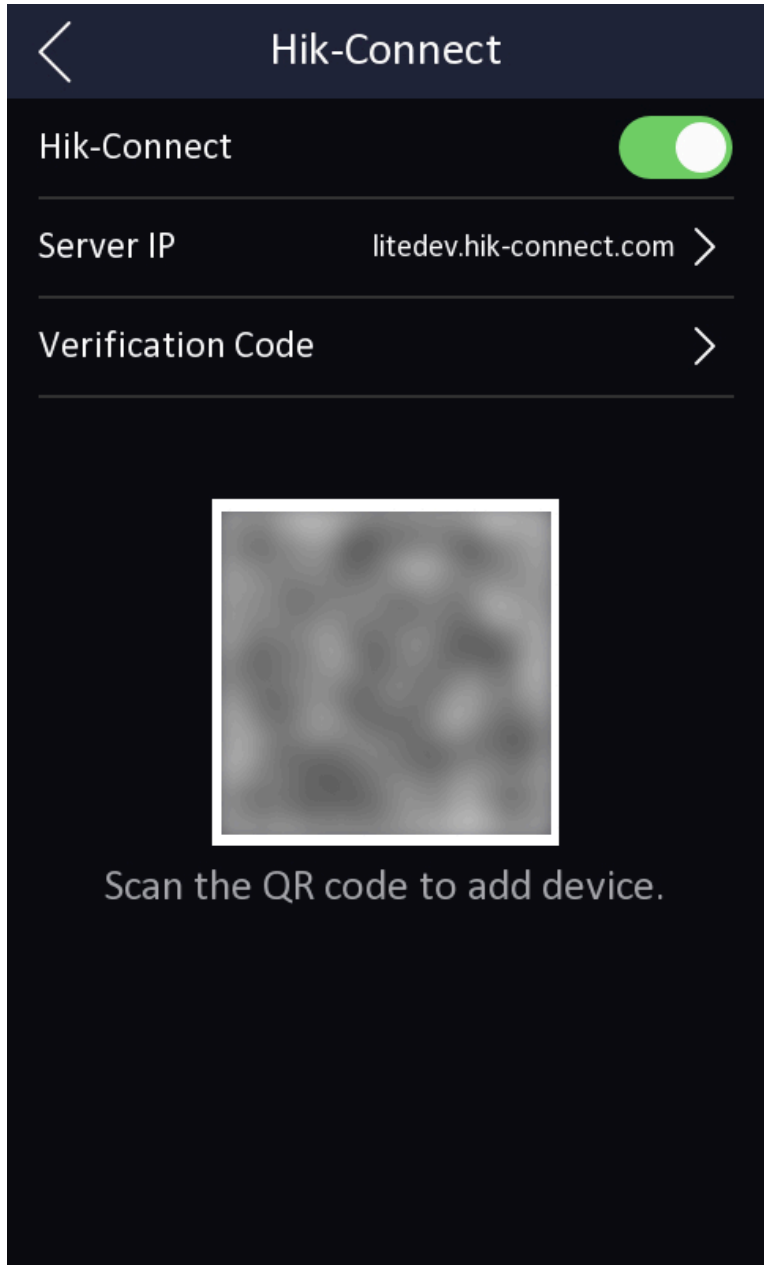


Figure 5-12 Cloud Service Settings

2. Slide to enable the function.
3. Edit the **Cloud Service Address** and create a **Verification Code**.
4. Tap **√** to save the settings.

5.5.4 Device Hotspot

Set the device hotspot.

On the menu, tap **Network → Hotspot** to enter the settings page.

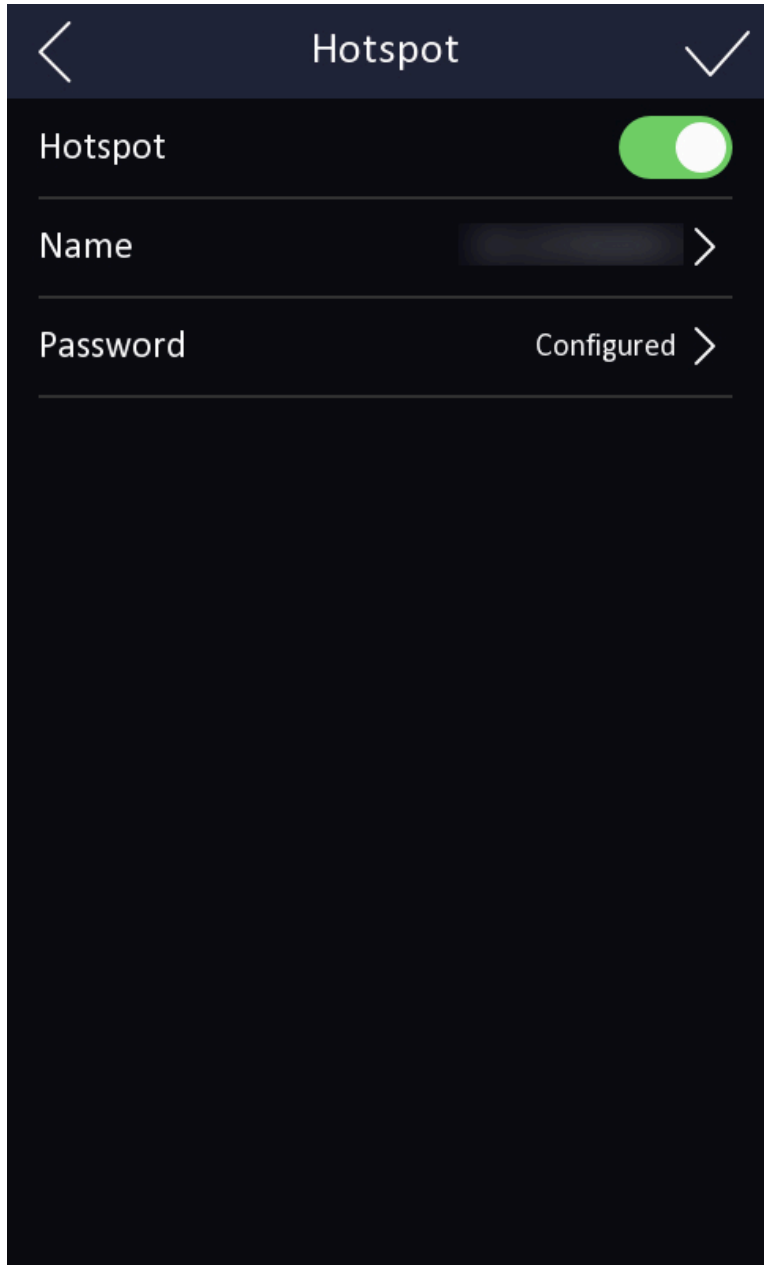


Figure 5-13 Hotspot Settings

Click to enable **Hotspot**. Set hotspot **Name** and **Password**.

Click **Save**.

5.6 Local Settings

Steps

1. Tap **Local** on the settings page.

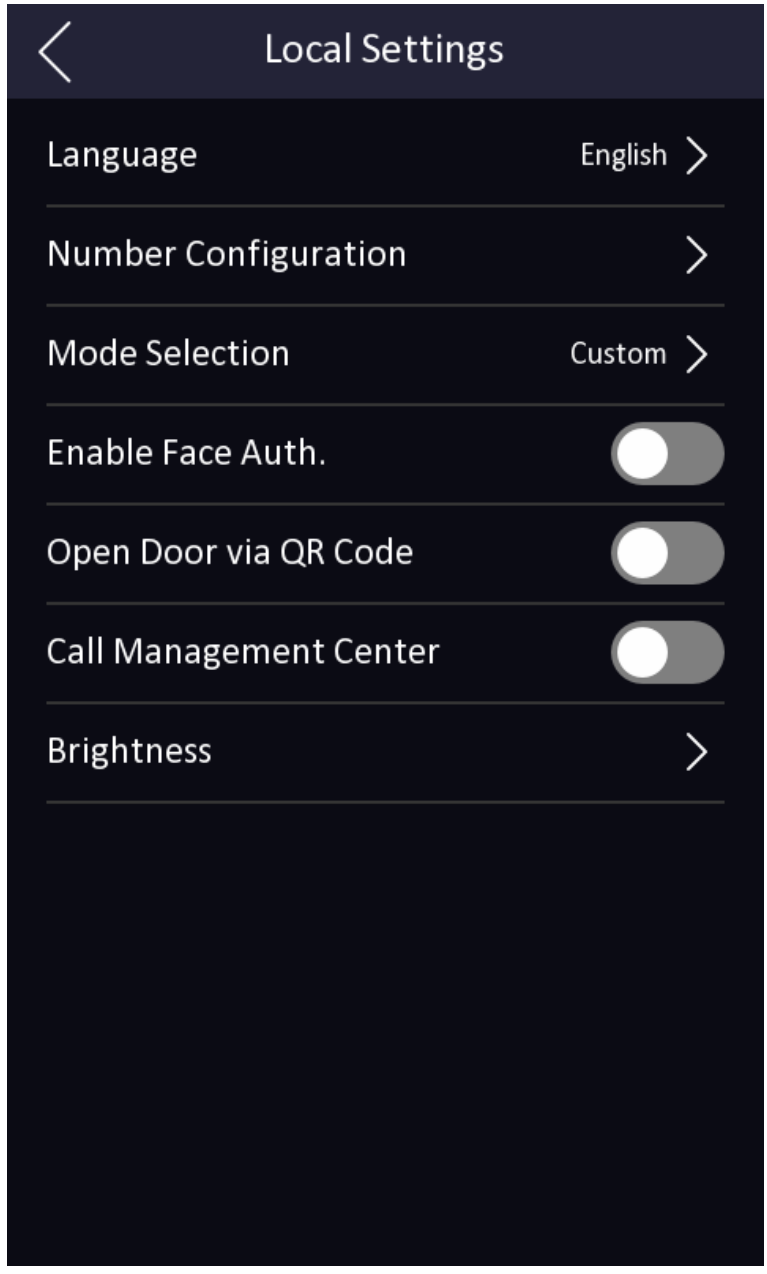


Figure 5-14 Local Settings

2. Tap **Language** and select a language at your needs.
3. Tap **Number Configuration** and set the building No., floor No., room No., project No., and unit No. Tap **<** to save the settings.

4. Tap **Mode Selection** to choose live view or custom theme.
5. Tap to **Enable Face Auth.**, **Open Door via QR Code** and **Call Management Center**at your needs.
6. Tap **Brightness** and drag the block to adjust the screen light.

5.7 System Maintenance

You can restore the device, upgrade system, reboot device or view device information, capacity and user manual on the system maintenance page.

Tap **Maint.** on the settings page to enter the system maintenance page.

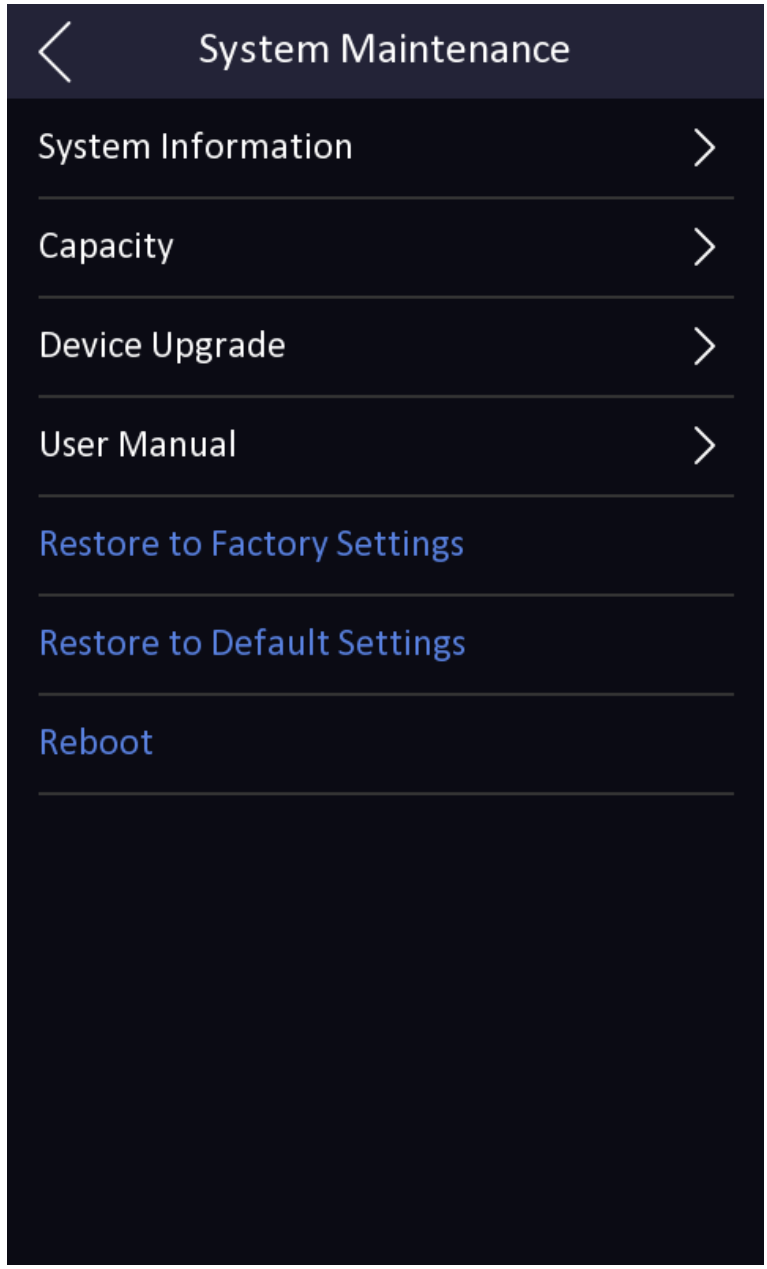


Figure 5-15 System Maintenance

System Information

You can view the device model, serial No., APP version and disclaimer.

Capacity

You can view the used and total capacity of user, face and card.

Device Upgrade

Tap **Upgrade** to get the upgrade package online.

User Manual

You can scan the QR code to get the user manual.

Restore to Factory Settings

Tap **Restore to Factory Settings** to restore all parameters and reboot the system.

Restore to Default Settings

Tap **Restore to Default Settings** to restore the default settings and reboot the system.

Reboot

Tap to reboot the device.

Chapter 6 Local Operation

6.1 Call from the Device

Door station supports calling users or management center.

6.1.1 Call Resident

Call Resident from Door Station

On the main page, tap to enter the calling page.

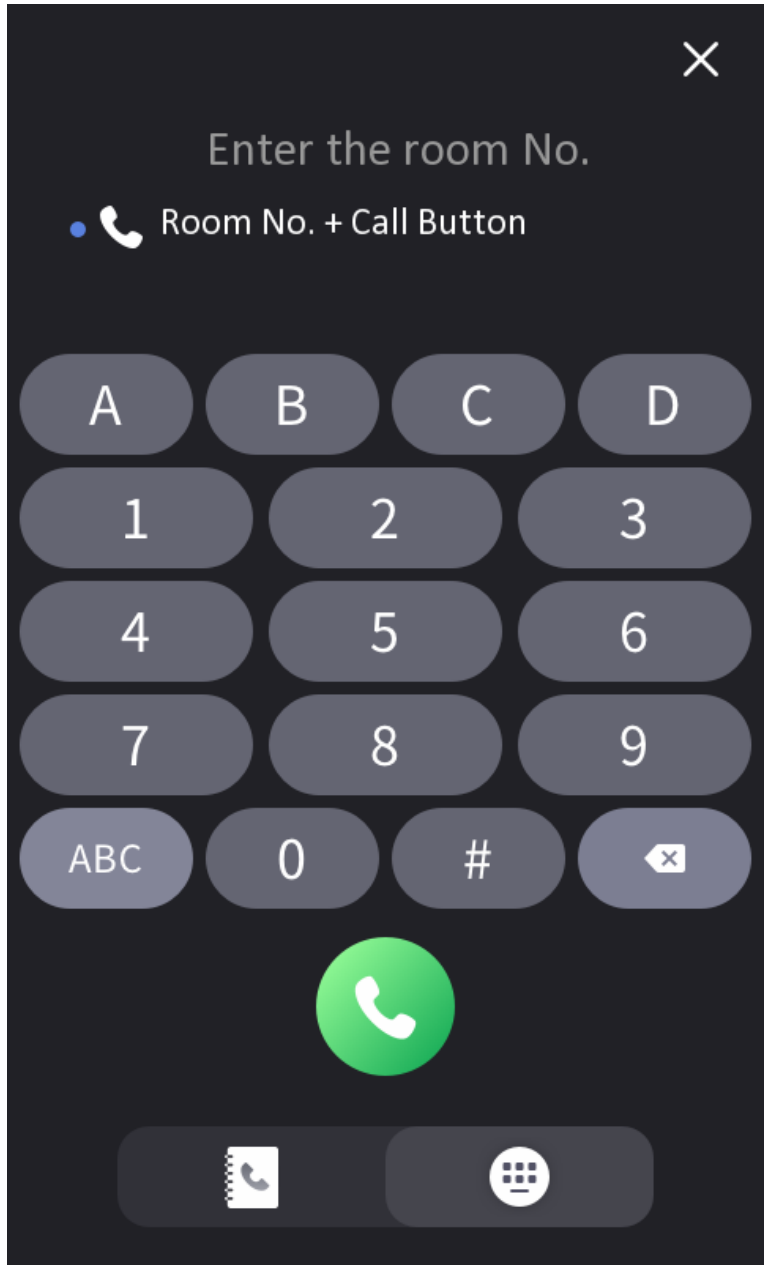


Figure 6-1 Calling

Enter the **Room No.**, and tap to call residents.
Tap contact button to enter the contact list. Select a contact from the list to call.

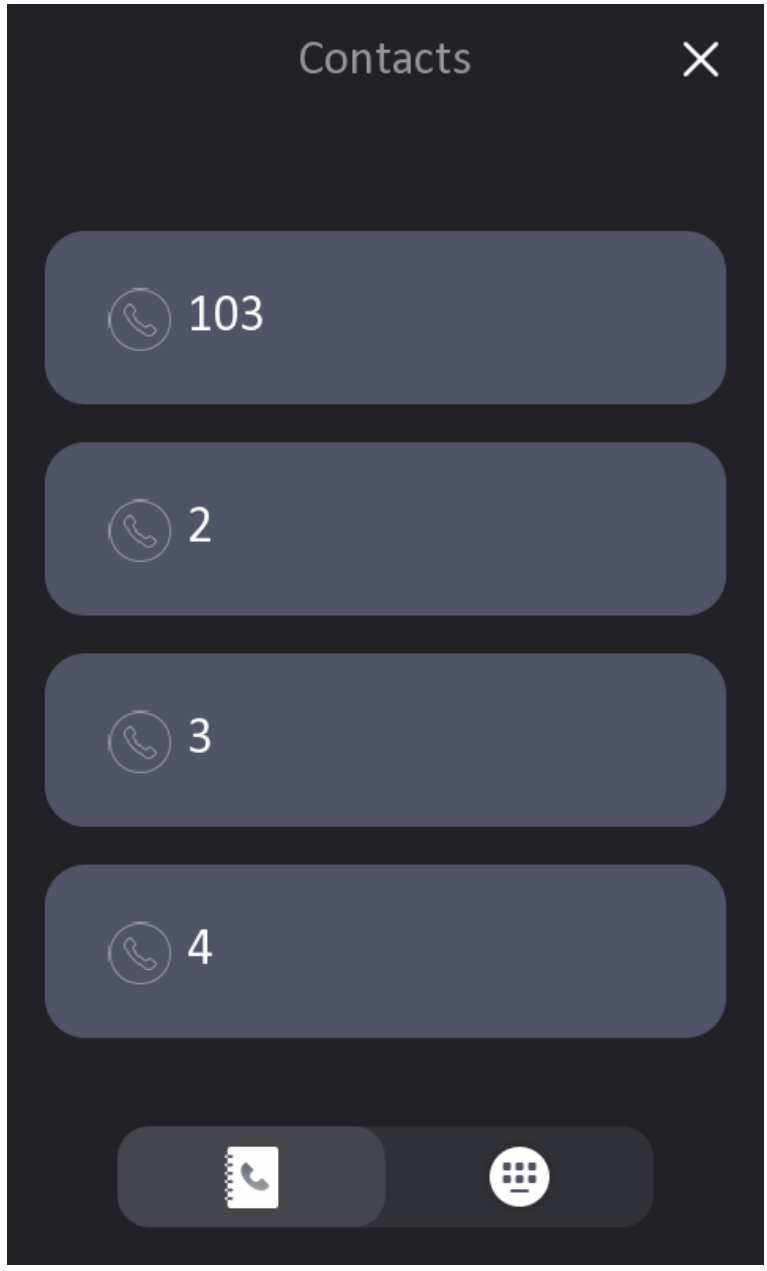


Figure 6-2 Contacts

Call Resident from Outer Door Station

On the main page of the outer door station, tap Call to enter the calling page.
Enter **Phase No.** + **#** + **Building No.** + **#** + **Unit No.** + **#** + **Room No.**, and tap Call again to call residents.
Enter **Phase No.** + **#** + **Building No.** + **#** + **Unit No.** + **#** + **Room No.**, and tap Call again to call residents.
Enter **Phase No.** + **#** + **Room No.**, and tap Call again to call residents.

6.1.2 Call Center

On the settings page, tap **Local** and enable **Call Management Center** to set the calling shortcut key.

Tap on the main page to call management center administrator. Tap cancel button to cancel during calling management center.

6.2 Unlock Door

You can unlock door station in following methods: Unlock by password, unlock by card, unlock by face, and unlock by QR code.

6.2.1 Unlock by Password

Tap call button on the main page to enter the calling page.

Enter 【# + Public Password】, and tap unlock button.

6.2.2 Unlock by Face

Note

Make sure that you have added your face picture to the device. Refers to the *User Management* for details.

Face forward at the camera to unlock.

Note

- Face recognition distance: 0.3 m to 2 m
- Face recognition duration: ＜ 0.2 s per person

6.2.3 Unlock by Presenting Card

Note

Make sure you have issued the card to the device. Refers to User Management for details.

Present the card on the card reading area to unlock.

6.2.4 Unlock by QR Code

Door station supports unlock by QR code. You can generate a QR code through the mobile phone client, and use the door station camera to scan the mobile phone QR code to open the door.

Steps

Note

- Make sure that the door station IP has been added to the indoor station, and the indoor station and the door station can communicate normally.
- Make sure that the door station is connected to the network.
- QR code is for visitors only.

1. Installing Hik-Central Pro on your PC.
2. Register user accounts according to the prompts, and log in.
3. Follow the prompts to add the indoor station by scanning the QR code/barcode or manually entering the serial number.
4. Enter unlock by QR code page and generate the QR code.
5. On the main page of door station, tap down button to enter the unlock by QR code page.
6. Aim the QR code generated by the phone at the camera and scan the code to open the door.

Note

- It is recommended that when installing the door station, try to select a location that does not cause reflections, otherwise it may affect the QR code scanning. If it is acrylic door station, make sure that the membrane on the surface of the door machine has been torn off.
- It is recommended to align the mobile phone's QR code with the door station camera horizontally when scanning the QR code.
- QR code recognition is not supported at night.

Chapter 7 Quick Operation via Web Browser

7.1 Change Password

You can change the device password.

Click in 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.

You can set the reserved E-mail address for password reset.

Click **Next** to complete the settings.

7.2 Select Language

You can select a language for the device system.

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

Click **Next** on the change password 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.

Click **Next** to complete the settings.

7.3 Time Settings

Set Time and DST

Click → **Time Settings** .

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 Type/Server Address/NTP Port/Interval

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

DST Settings

Enable **DST**.

Set the DST start time, end time and bias time.

Click **Next** to complete the settings.

7.4 Environment Settings

After activating the device, you should select an application mode for better device application.

Steps

1. Click → **Environment Settings**.
2. Select **Indoor** or **Other**.

Note

- If you install the device indoors near the window or the face recognition function is not working well, select **Others**.
- If you do not configure the application mode and tap **Next**, the system will select **Indoor** by default.
- If you activate the device via other tools remotely, the system will select **Indoor** as the application mode by default.

Click **Next** to complete the settings.

7.5 Administrator Settings

Steps

1. Click in the top right of the web page to enter the wizard page. After setting device language, time, environment and privacy, you can click **Next** to enter the **Administrator Settings** 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 KB, 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.

Click **Next** to save the settings and go to the next paramater. Or click **Skip** to skip administrator settings.

7.6 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 System Network** settings page.
2. Set the device type.

   If set the device type as **Door Station** or **Outer Door Station**, you can set the **Community No.**, **Building No.**, **Unit No.**, **Floor No.**, and **Door Station No.**

   If set the device type as **Outer Door Station**, you can set outer door station No., and community No.
3. Set **Registration Password**, **Main Station IP** and **Private Server IP**.
4. **Optional:** Click to **Enable Protocol 1.0**.
5. Click **Complete** to save the settings after the configuration.

Chapter 8 Operation via Web Browser

8.1 Login

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

Note

Make sure the device is activated.

Login via Web Browser

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**.

Login via Remote Configuration of Client Software

Download and open the client software. After adding the device, click to enter the Configuration page.

8.2 Forget Password

If you forget the password when logging in, you can change the password by email address or security questions.

On the login page, click **Forget Password**.

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

1. Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.
2. You will receive a verification code within 5 minutes in your reserved email.
3. Enter the verification code into the verification code field to verify your identification.

Click **Next**, create a new password and confirm it.

8.3 Overview

You can view the live video of the device, linked device, person information, network status, basic information, and device capacity.

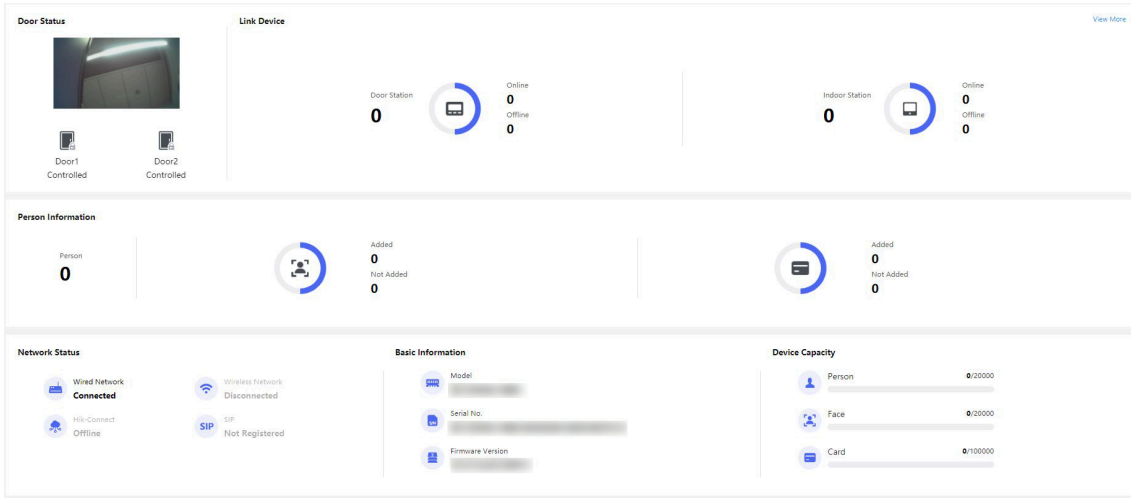


Figure 8-1 Overview Page

Function Descriptions:

Door Status

Click to view the device live view.

Set the volume when starting live view.

Note

If you adjust the volume when starting two-way audio, you may hear a repeated sounds.

You can capture image when starting live view.

Select the streaming type when starting live view. You can select from the main stream, sub stream or third stream.

Full screen view.

/ / /

The door status is open/closed/remaining open/remaining closed.

Controlled Status

You can control the door1 or door2 to be opened, closed, remaining open or remaining closed according to your actual needs.

Link Device

You can view the quantity and status of linked devices.

Person Information

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

Network Status

You can view the connected and registered status of wired network, wireless network, cloud service and SIP.

Basic Information

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

Device Capacity

You can view the person, face, and card capacity.

View More

You can click **View More** to ***Device Management*** .

8.4 Person Management

Click **Add** to add the person's information, including the basic information, certificate, authentication and settings.

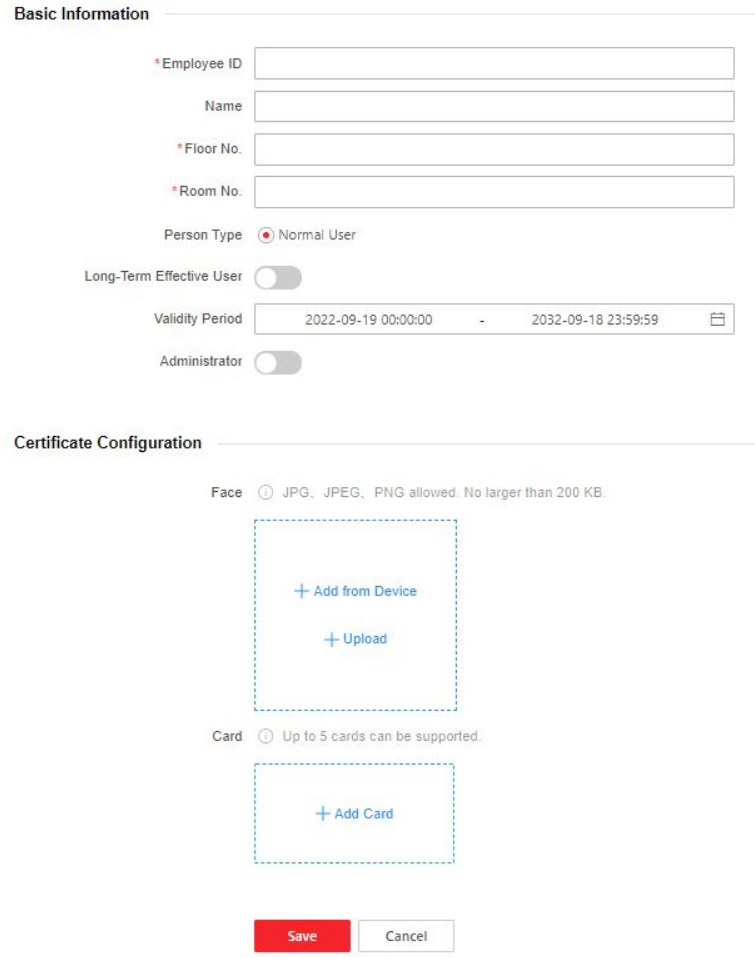


Figure 8-2 Add Person

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, floor No., and room No.
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 **Validity Period** 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 Face Picture

Click **Person Management → Add** to enter the Add Person page.
Click **+** on the right to upload a face picture from the local PC.

Note

The picture format should be JPG or JPEG or PNG, and the size should be less than 200 KB.

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 **OK** to add the card.

Note

Up to 5 cards can be added.

Click **Save** to save the settings.

8.5 Device Management

You can manage the linked device on the page.

Steps

1. Click **Device Management** to enter the settings page.
2. Click **Search Online Device** to search for the online devices automatically.
3. Click **Add** to add the indoor station or sub door station. Enter the parameters and click **OK** to add.
4. Click **Import**. Enter the information of the device in the template to import devices in batch.
5. Click **Export** to export the information to the PC.
6. Select the device and click **Delete** to remove the selected device from the list.
7. Click **Device Upgrade** and import upgrading package to install the latest version.
8. Click **Upgrade Status** to view the upgrading process.
9. Click to enable **Synchronization Settings**.

   Note

   If enabled, the current device's settings will be synchronized to other devices.
10. Click **Refresh** to get the device information.
11. **Optional:** Set Device Information.

Edit Device Information	Click to edit device information.
Delete Device Information	Click to delete device information from the list.
Search Devices	Select **Status** and **Device Type** to search devices.

8.6 Configuration

8.6.1 Set Local Parameters

Set the live view parameters, picture and clip settings.

Set Live View Parameters

Click **Configuration → Local** to enter the Local page. Configure the stream type, the play performance and click **Save**.

Picture and Clip Settings

Click **Configuration → Local** to enter the Local page. Select image format, saving path and click **Save**.
You can also click **Open** to open the file folder to view details.

8.6.2 View Device Information

View the device name, device No., system type, language, model, serial No., version, number of channels, IO input, RS-485, register number, alarm input, alarm output, and device capacity, etc.

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

You can view the device name, device No., system type, language, model, serial No., version, number of channels, IO input, RS-485, register number, alarm input, alarm output, and device capacity, etc.

8.6.3 Set Time

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

Click **Configuration → System → System Settings → 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.

Server Address Type/Server Address/NTP Port/Interval

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

8.6.4 Set DST

Steps

1. Click **Configuration → System → System Settings → Time Settings** .
2. Enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

8.6.5 Change Administrator's Password

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**.

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 installer and/or end-user.

8.6.6 Online Users

The information of users logging into the device is shown.

Go to **Configuration → System → User Management → Online Users** to view the list of online users.

8.6.7 View Device Arming/Disarming Information

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.

8.6.8 Network Settings

Set TCP/IP, Wi-Fi parameters, and device hotspot.

Set Basic Network Parameters

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

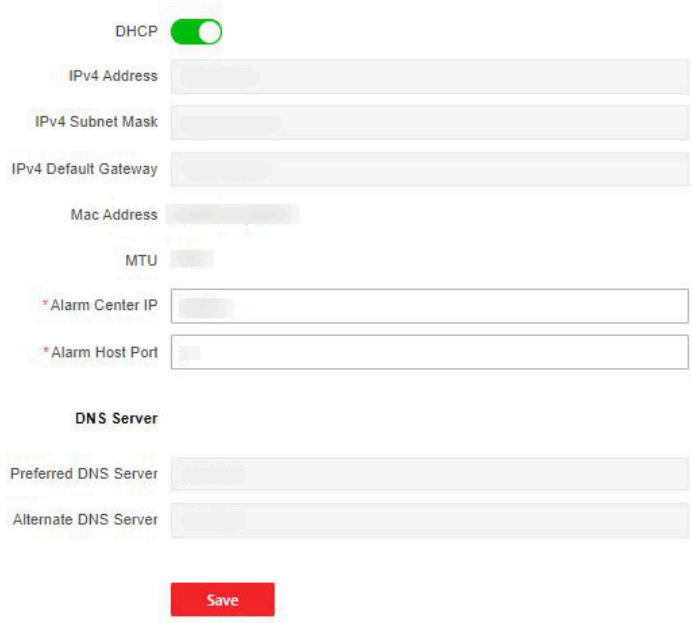


Figure 8-3 TCP/IP Settings

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

DHCP

If disable the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, preferred DNS server and the Alternate DNS server.

If you check the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway, preferred DNS server and the Alternate DNS server automatically.

DNS Server

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

Set Wi-Fi Parameters

Set the Wi-Fi parameters for device wireless connection.

Steps

Note

The function should be supported by the device.

1. Click **Configuration → Network → Network Settings → Wi-Fi** .
2. Check **Wi-Fi**.
3. Select a Wi-Fi
   - Click **Connect** of a Wi-Fi in the list and enter the Wi-Fi password.
   - Click **Manual Add** and enter a Wi-Fi's SSID, working mode, security mode, and password. Click **OK**.
4. Set the WLAN parameters.
   1) Set the IP address, subnet mask, and default gateway. Or enable **DHCP** and the system will allocate the IP address, subnet mask, and default gateway automatically.
5. Set the DNS server. Set the preferred DNS server and alternate DNS server. Or enable **DHCP** and the system will allocate the preferred DNS server and alternate DNS server automatically.
6. Click **Save**.

Device Hotspot

Set the device hotspot.

On the menu, tap **Network → Hotspot** to enter the settings page.

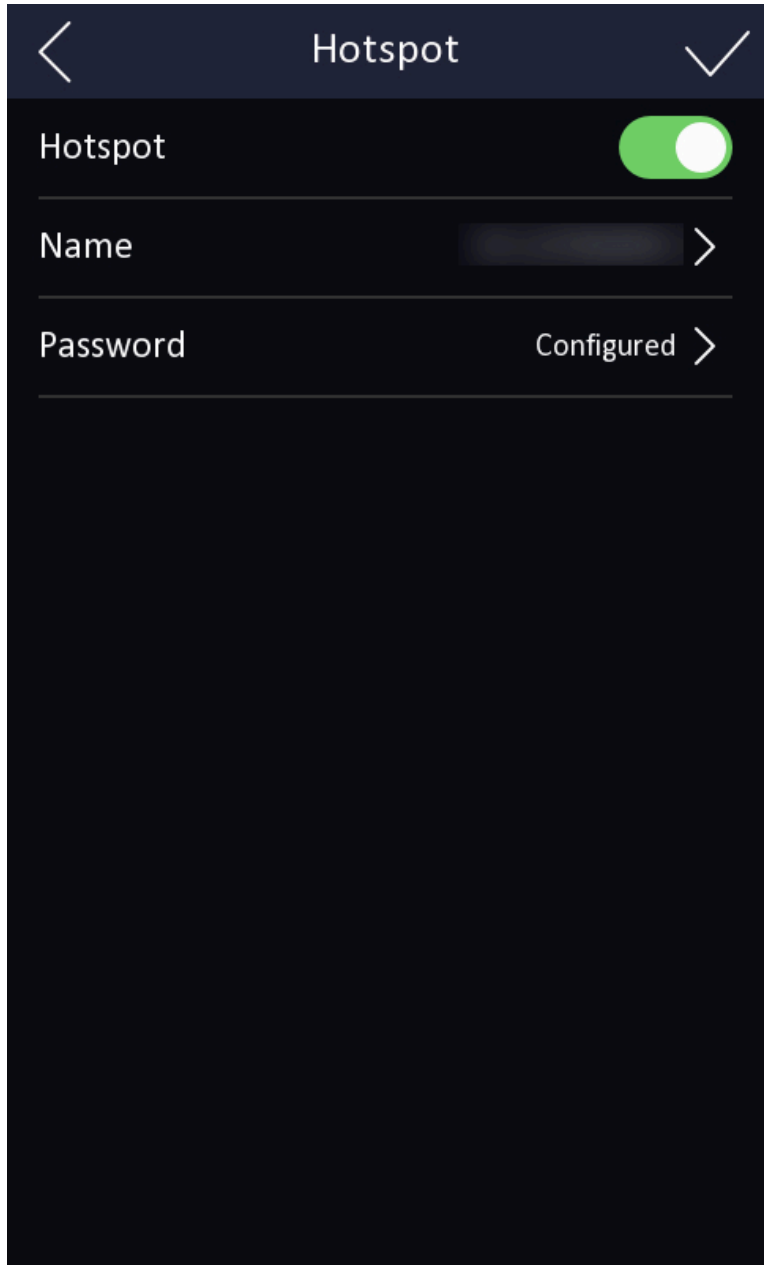


Figure 8-4 Hotspot Settings

Click to enable **Hotspot**. Set hotspot **Name** and **Password**.

Click **Save**.

Network Service

Set the HTTP, HTTPS, HTTP Listening, RTSP and FTP 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.

HTTP Listening

The device can send alarm information to the event alarm IP address or domain name via HTTP protocol/HTTPS protocol. Edit the event alarm IP address or domain name, URL, port, and protocol.

Note

The event alarm IP address or domain name should support the HTTP protocol/HTTPS protocol to receive the alarm information.

RTSP

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

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

FTP

Click **Configuration → Network → Network Service → FTP** .

Check to **Enable FTP**.

Select **Server Type**. Input the **Server IP Address** and **Port**. Configure the user name and password server login. Set the **Directory Structure**, **Parent Directory** and **Child Directory**. Set the **Delimiter** and select **Named Item** and **Named Element**.

Note

If you enable **Anonymous**, you will not need to set user name or password.

Platform Access

Platform access provides you an option to manage the devices via platform.

Steps

1. Click **Configuration → Network → Device Access → Hik-Connect** to enter the settings page.

Note

Hik-Connect is an application for mobile devices. With the App, you can view live image of the device, receive alarm notification and so on.

2. Check **Enable** to enable the function.
3. **Optional:** Check the checkbox of **Custom**, and you can set the server address by yourself.
4. Enter the server IP address, and verification code.

Note

6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

5. Click **Save** to enable the settings.

Device Access Setting

Steps

1. Click **Configuration → Network → Device Access → SIP** to enter the settings page.
2. Check **Enable VOIP Gateway**.
3. Configure the SIP parameters.
4. Click **Save** to enable the settings.
5. Click **Configuration → Network → Device Access → SDK Server** to enter the settings page.
6. Set the **Server Port**. It refers to the port through which the client adds the device.

8.6.9 Set Video and Audio Parameters

Set the image quality and resolution.

Set Video Parameters

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

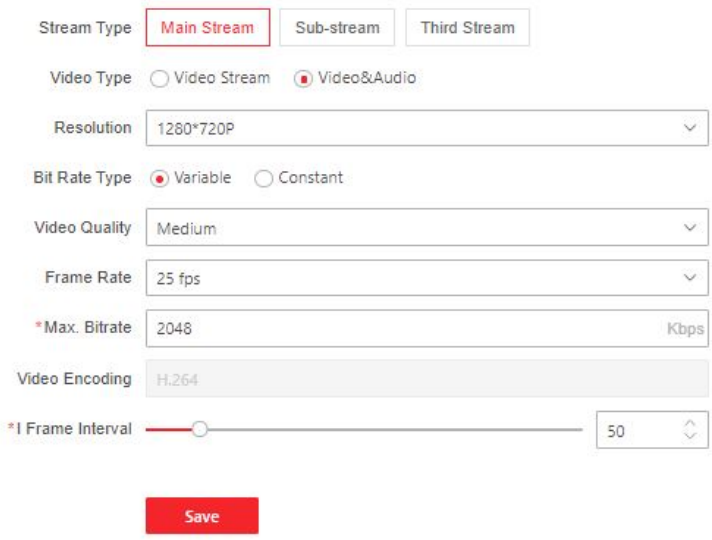


Figure 8-5 Video Settings Page

Set the stream type, the video type, the resolution, the bitrate type, the video quality, the frame rate, the Max. bitrate, the video encoding, and I Frame Interval.
Click **Save** to save the settings after the configuration.

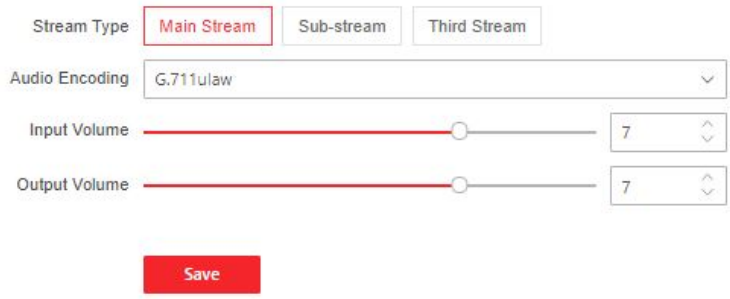


Figure 8-6 Audio Settings

Set the stream type, audio encoding, input volume, and output volume according to your actual needs.
Click **Save** to save the settings.

8.6.10 Set Image Parameters

You can adjust the image parameters, video parameters, supplement parameters and capture interval.

Steps

1. Click **Configuration → Image** .

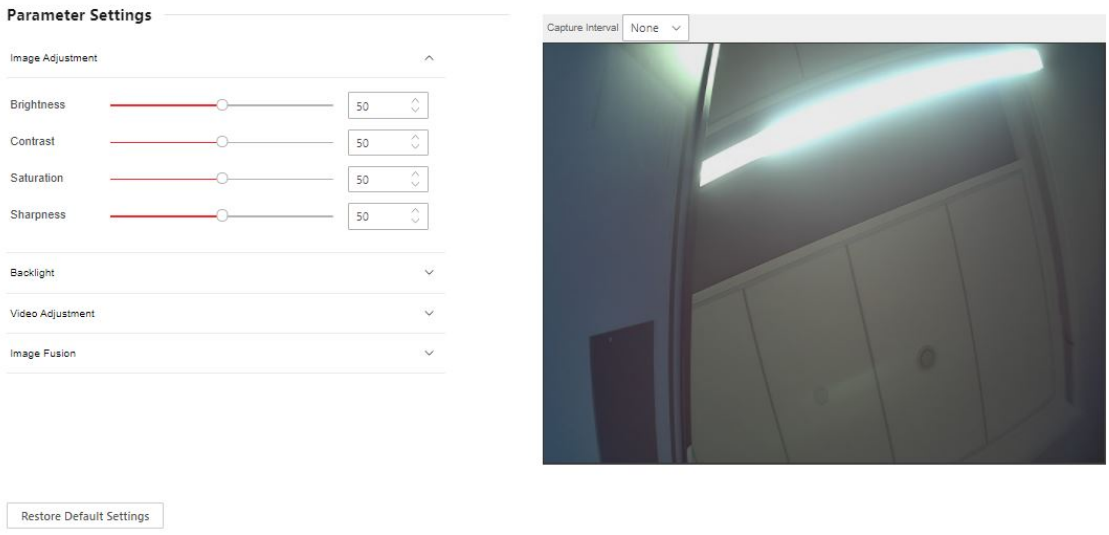


Figure 8-7 Image Settings

2. Configure the parameters to adjust the image.

Image Adjustment

Drag the block or enter the value to adjust the live video's brightness, contrast, saturation, and sharpness.

Video Adjust

Set the video frame rate when performing live view remotely. After changing the standard, you should reboot the device to take effect.

PAL

25 frames per second. Suitable for mainland China, Hong Kong (China), the Middle East countries, Europe countries, etc.

NTSC

30 frames per second. Suitable for the USA, Canada, Japan, Taiwan (China), Korea, the Philippines, etc.

Backlight

Enable or disable **WDR**.

When there are both very bright and very dark areas simultaneously in the view, WDR balances the brightness level of the whole image and provide clear images with details.

Image Fusion

Wen the environment is dark, you can select **Auto** to enable the image fusion function. The live view page will display the fusion image. And you can also set the sensitivity.

Select **Disable** to disable the function.

3. Click **Restore Default Settings** to restore the parameters to the default settings.

8.6.11 Motion Detection

Motion detection detects the moving objects in the configured security area, and a series of actions can be taken when the alarm is triggered.

Steps

1. Click **Configuration → Event → Event Detection → Motion** to enter the settings page.

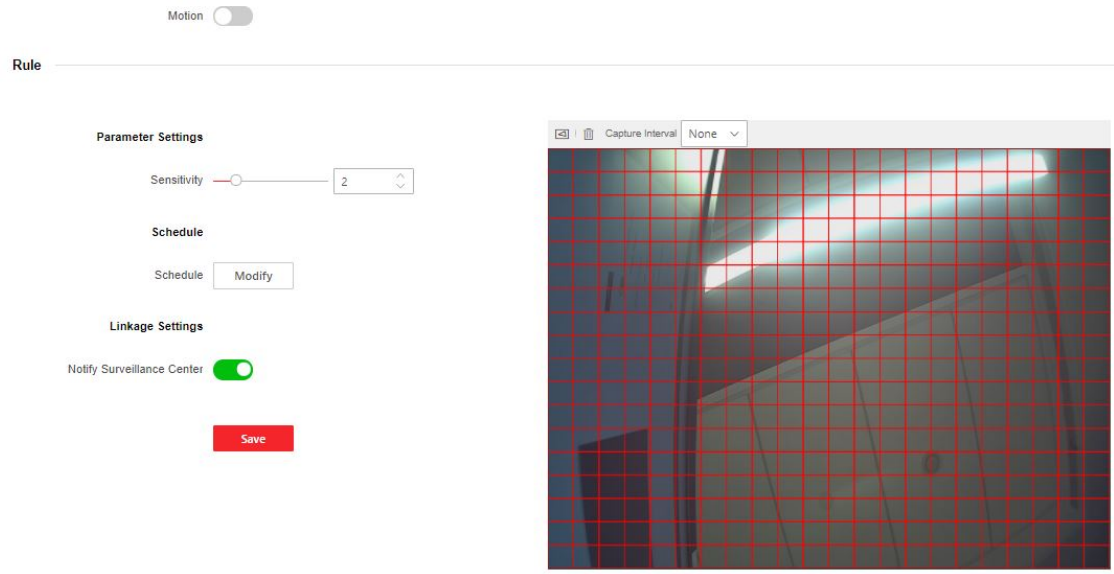


Figure 8-8 Motion Detection

2. Drag the block or set value to adjust sensitivity.
3. Click **Modify** to edit the arming schedule.
4. Click on the time bar and drag to select the time period. Click **Save** to save the settings.
5. Click to enable **Notify Security Center**.

Note

Send an exception or alarm signal to the remote management software when an event occurs.

6. Click **Save** to enable the settings.

8.6.12 Event Linkage

Set linked actions for events.

Steps

1. Click **Configuration → Event → Event Detection → Linkage Settings** to enter the page.

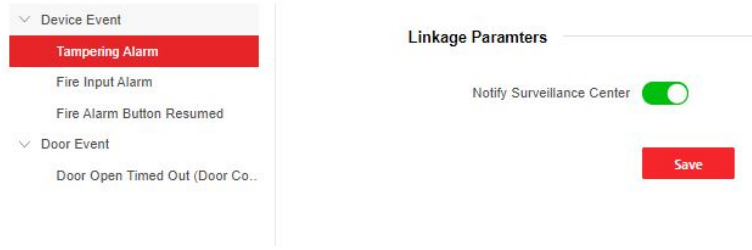


Figure 8-9 Event Linkage

2. Select device event or door event.
3. Click to enable or disable **Notify Security Center** for event.

Note

Send an exception or alarm signal to the remote management software when an event occurs.

8.6.13 Access Control Settings

Set Authentication Parameters

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

Note

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

Figure 8-10 Set Authentication Parameters

Terminal

Terminal description is read-only.

Continuous Face Recognition Interval

You can set the interval between 2 continuous recognition of a same person during the authentication. In the configured interval, Person A can only recognized once. If another person (Person B) has recognized during the interval, Person A can recognized again.

Note

The interval ranges from 1 s to 10 s.

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

Set Door Parameters

Click **Configuration → Access Control → Door Parameters** .

Door No.

Select the device corresponded door No.

Door Name

You can create a name for the door.

Open Duration

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Relay Reverse

Click to enable or disable relay reverse.

Enable QR Code Auth.

Click to enable or disable QR Code Authentication.

Enable Face Auth.

Click to enable or disable face Authentication.

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

Elevator Control

Steps

1. Click **Configuration → Access Control → Elevator Control Parameters** .

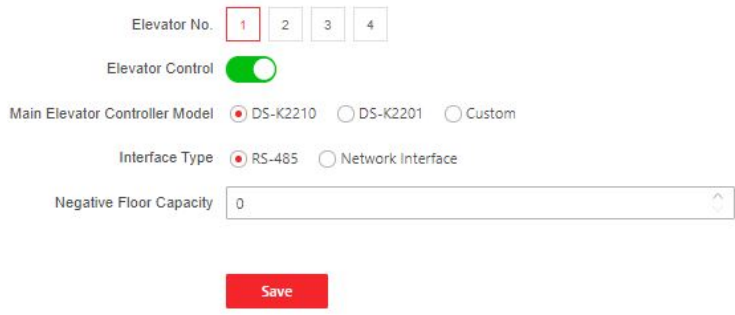


Figure 8-11 Access Control and Elevator Control

2. Click to enable **Elevator Control**.
3. Set the elevator parameters.

Elevator No.

Select an elevator No.

Main Elevator Controller Model

Select an elevator controller.

Interface Type

If you select **RS-485**, make sure you have connected the device to the elevator controller with RS-485 wire.

If you select **Network Interface**, enter the elevator controller's IP address, port No., user name, and password for communication.

Negative Floor Capacity

Set the negative floor number.

Note

- Up to 4 elevator controllers can be connected to 1 device.
- Up to 10 negative floors can be added.
- Make sure the interface types of elevator controllers, which are connected to the same device, are consistent.

RS-485 Settings

Set the working mode to linked device.

Steps

1. Click **Access Control → RS485** to enter the settings page.
2. Select the working mode.
3. Click **Save** to enable the settings.

Password Settings

Set public password.

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

Click **Add** to add password.

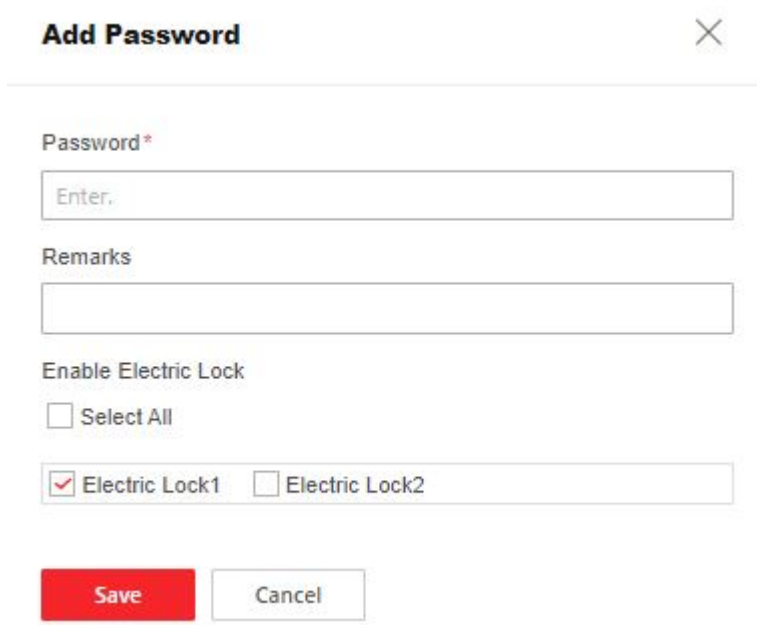


Figure 8-12 Add Password

Set password and remarks and click to enable electric lock.

Click **Save** to save the settings.

8.6.14 Intercom Settings

Device No. Settings

Steps

1. Click **Device No.** to enter the page.

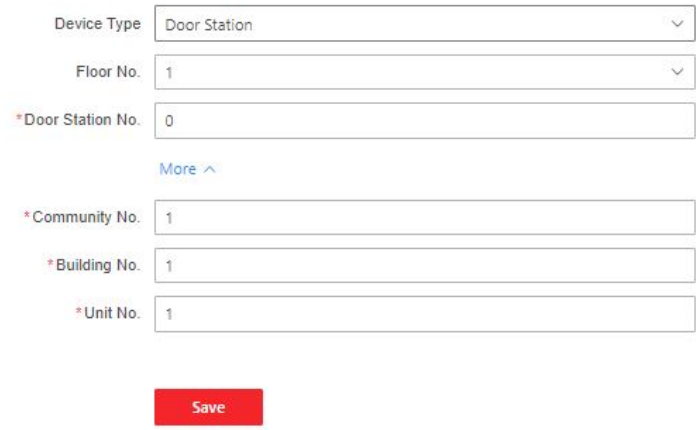


Figure 8-13 Villa Door Station No. Settings

2. Select the device type from the drop-down list, and set the corresponding information including **Building No.**, **Floor No.**, **Door Station No.**, **Community No.** and **Unit No.**

Note

When you select **Outer Door Station** as **Device Type**, only **Community No.** and **Outer Door No.** can be set.

3. Click **Save** to enable the device number configuration.

Linked Network Settings

Steps

1. Click **Intercom → Session Settings** to enter the settings page.

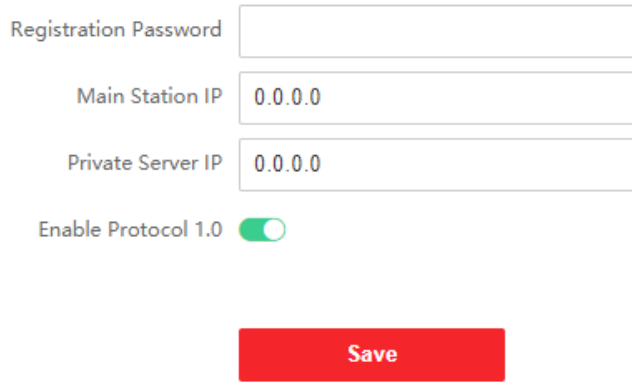


Figure 8-14 Session Settings

2. Set **Registration Password**.
3. Set **Main Station IP** and **VideoIntercom Server IP**.

4. Enable Protocol 1.0.
5. Click **Save** to enable the settings.

Time Parameters

Go to **Intercom → Call Settings** to enter the page.

Configure **Max. Communication Time** and **Max. Message Duration**, and click **Save**.

Note

- Max. communication time between the module indoor station and client ranges from 90 s to 120 s. The call will end automatically when the actual calling duration is longer than the configured one.
- Max. message duration ranges from 30 s to 60 s. The message will end automatically when the actual message duration is longer than the configured one.

Press Button to Call

Steps

1. Click **Intercom → Press Button to Call** to enter the settings page.
2. Click **Call Schedule Settings** to create a new template plan.
   1) Set **Schedule Name**.
   2) drag to set weekly schedule for indoor station and center.
   3) Click **Add**, set specific **Start Time** and **End Time**, and drag to set schedule for indoor station and center.
   4) Click **Save**.
3. Click to configure **Button Settings** and select a call schedule.
4. Click **Save**.

Number Settings

Link the room No. and SIP numbers.

Click **Number Settings** to enter the page.

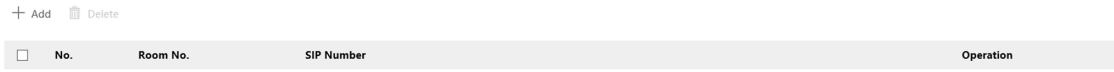


Figure 8-15 Number Settings

Click **Add**, set the **Room No.** and SIP numbers in the pop-up dialog box.

8.6.15 Set Card Security

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

Click to **Enable Card Encryption Parameters** and set the encryption sector. By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.

Click **Save**.

8.6.16 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.

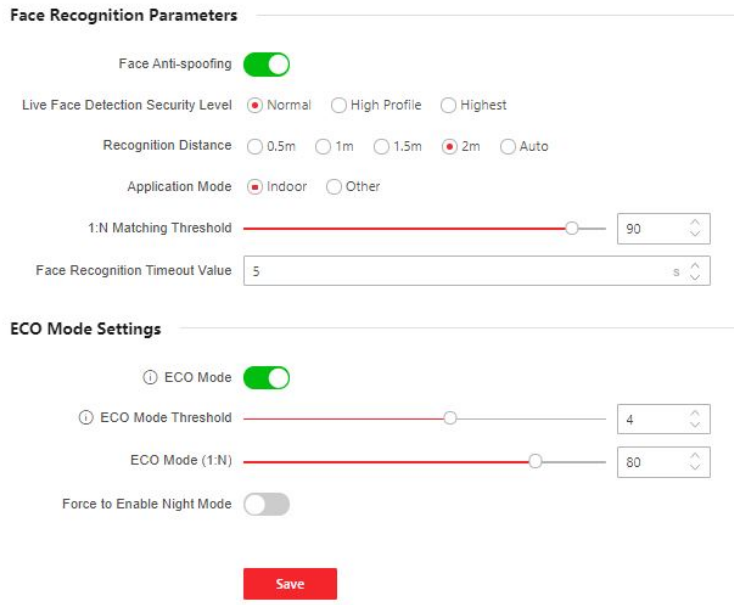


Figure 8-16 Smart Settings Page

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

Face Anti-spoofing

Enable or disable the live face detection function. If enabling the function, the device can recognize whether the person is a live one or not.

Note

Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

Live Face Detection Security Level

After enabling the face anti-spoofing function, you can set the matching security level when performing live face authentication.

Recognition Distance

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

Application Mode

Select either others or indoor according to actual environment.

1:1 Matching Threshold

Set the matching threshold when authenticating via 1:1 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.

ECO Mode

After enabling the ECO mode, the device will use the IR camera to authenticate faces in the low light or dark environment. You can set the ECO mode threshold and ECO mode (1: N).

ECO Mode (1:N)

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

Force to Enable Night Mode

You can click to enable forced night mode when the ECO mode is enabled.

Set Recognition Area

Click **Configuration → Smart → Area Configuration** .
Drag the yellow frame in the live video, drag the block or set value to adjust the recognition area. Only the face within the area can be recognized by the system.
Select **Capture Interval** from the dropdown list.
Click **Save** to save the settings.

8.6.17 Set Screen Display

You can set the display theme for the device.

Click **Configuration → Preference → Screen Display** .

You can select display theme for device authentication. You can select **Theme Mode** as **Authentication** or **Advertisement**.

Click **Save**.

Notice Publication

You can set the notice publication for the device.

Click **Configuration → Preference → Notice Publication** .

Theme Management

Click **Media Library Management → +** to upload the picture from the local PC.

You can click **+**, and set **Name** and **Type** to create a theme. After creating the theme, click **+** in the **Theme Management** panel to select pictures in the media library. Click **OK** to add pictures to the theme.

Schedule Management

After you have created a theme, you can select the theme and draw a schedule on the time line.

Select the drawn schedule, and you can edit the exact start and end time.

Select the drawn schedule and you can click **Clear** or **Clear All** to delete the schedule.

Slide Show Interval

Enter a number to set the slide show interval. The picture will be changed according to the interval.

8.6.18 Upgrade and Maintenance

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

Reboot Device

Click **Maintenance and Security → Maintenance → Restart** .
Click **Restart** to reboot the device.

Upgrade

Click **Maintenance and Security → Maintenance → Upgrade** .
Select an upgrade type 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

Do not power off during the 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.

8.6.19 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.

   Capture Network Packet

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

8.6.20 Certificate Management

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

Note

The function is only supported by certain device models.

Create and Install Self-signed Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **Certificate Files** area, select a **Certificate Type** from the drop-down list.
3. Click **Create**.
4. Input certificate information.
5. Click **OK** to save and install the certificate.

   The created certificate is displayed in the **Certificate Details** area.

   The certificate will be saved automatically.
6. Download the certificate and save it to an asking file in the local computer.
7. Send the asking file to a certification authority for signature.
8. Import the signed certificate.
   1) Select a certificate type in the **Import Passwords** area, and select a certificate from the local, and click **Install**.
   2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Install**.

Install Other Authorized Certificate

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

Steps

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

Install 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 **Import CA Certificate** area.

   Note

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

Appendix A. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.
Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.

Figure A-1 QR Code of Communication Matrix

Device Command

Scan the following QR code to get the device common serial port commands.
Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.

Figure A-2 Device Command

See Far, Go Further