DNAKE

User Manual

DNAKE AC02C

REMARK

Please follow the user manual for correct installation and testing. If there is any doubt please call our tech-supporting and customer center.

Our company applies ourselves to reformation and innovation of our products. No extra notice for any change. The illustration shown here is only for reference. If there is any difference, please take the actual product as the standard.

The product and batteries must be handled separately from household waste. When the product reaches the end of service life and needs to be discarded, please contact the local administrative department and put it in the designated collection points in order to avoid the damage to the environment and human health caused by any disposal. We encourage recycling and reusing the material resources.

CATALOG

PRODUCT FEATURE

1. 50mm width slim design, suitable for narrow installation scenario
2. Multiple unlock method includes: RFID, NFC, Bluetooth, App remotely unlock
3. Support Wiegand & RS485
4. Flush mounted & surface mounted
5. IP65 & IK08

TECHNICAL PARAMETER

Power Supply: PoE or DC 12V/2A

RFID Reader:13.56MHz and 125kHz

Working Temperature: -40℃ to +55℃

Storage Temperature: -40℃ to +70℃

Working Humidity: 10% to 90% (non-condensing)

PACKAGE CONTENT

MODEL: AC02C(Surface mounting)


AC02C


Outlet Seal Plug

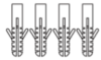

Junction Pressing Plate


Screw(FM2*6,4 pcs)


Screw(TM3*4)

Torx Screwdriver(T10)


Screw(FA4*25,4 PCS)


Screw Fixing Seat(4 pcs)


Rear Cover

MODEL: AC02C(Flush mounting)


AC02C


Outlet Seal Plug

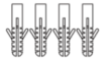

Junction Pressing Plate


Screw(FM2*6,4 pcs)


Screw(TM3*4)

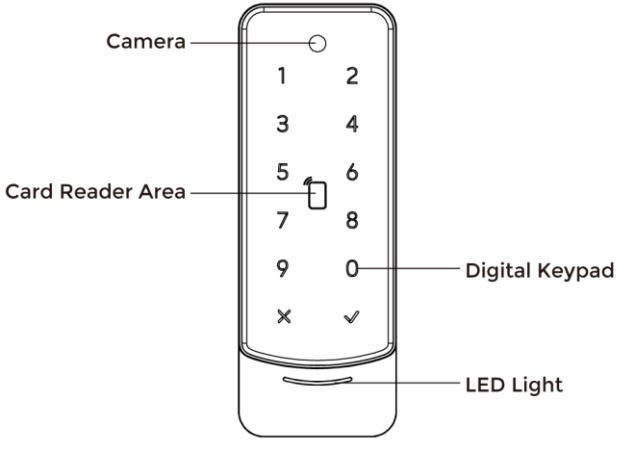
Torx Screwdriver(T10)


Screw(FA4*25,4 PCS)


Screw Fixing Seat(4 pcs)


Flush Mounting Box

OVERVIEW



Note:

LED light: The light is used to display the running status of the device and the unlocking status

Relay Outputs: Supports 1 relay output.

Camera :It is used for QR Code unlock

BASIC OPERATION

1. Add Cards by Admin Card

1.1. Add other cards

Step 1: Tap the admin card once;

Step 2: And then tap other cards immediately. Other cards you have tapped can be used to open the door;

Step 3: Tap the admin card again to finish.

1.2. Delete other cards one by one

Step 1: Tap the admin card twice;

Step 2: And then tap other cards immediately. Other cards you have tapped will be deleted;

Step 3: Tap the admin card again to finish.

1.3. Delete all other cards

Tap the admin card five times. All the other cards will be deleted.

Tips: The admin card can only be used to manage cards. It cannot be used to open the door.

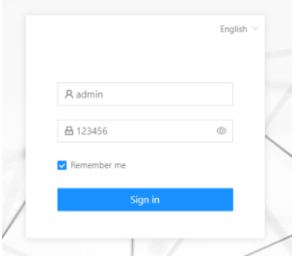
2. IP Broadcasting

If you want to check the IP address of the device, you can short press the RESET button of the device or press and hold the "✓" button on the device screen for 5 seconds, and the device will broadcast the current IP address.

WEB SETTING

Connect Access Control and PC to a network switch in the same LAN. You can enter the IP address of Access Control in the web browser search bar and log in with the default account (admin) and password (123456). This is where you can configure the device.

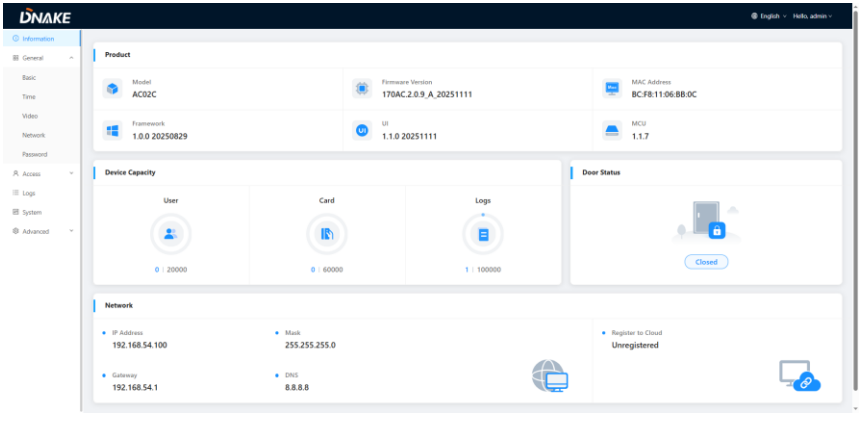
To get the IP address, you can search by DNAKE Remote Upgrade Tool installed in the same LAN with the devices.



1. Information

1.1. Information

When you first log in to the web interface, you can find basic information displayed in this dashboard.

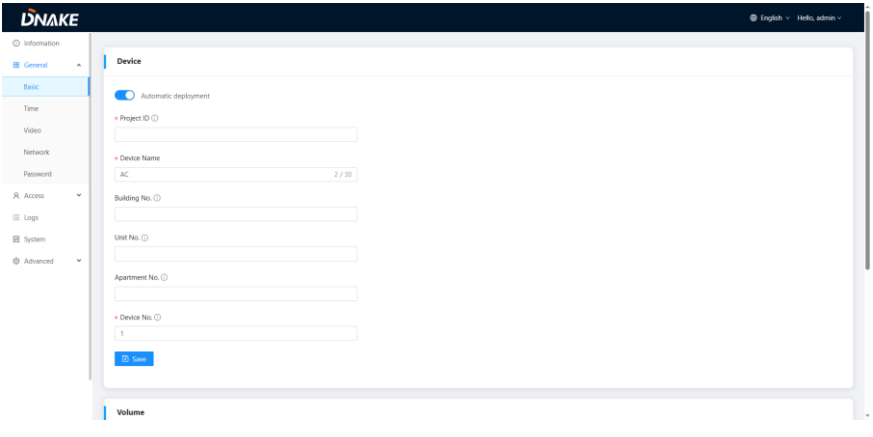


Model:	Model of the device;
Firmware Version:	Firmware version of the device;
MAC Address:	MAC address of the device;
Framework:	Framework of the device;
UI:	UI of the device;
MCU:	MCU of the device;
Device Capacity:	You can check the remaining capacity of the User Card and Logs;
Door Status:	Status of Door;
IP Address:	Current IP address of the device;
Mask:	Subnet mask of the device;
Gateway:	Gateway of the device;
DNS:	Domain Name Server of the device;
Status:	Status of Cloud registration of the device;

2. General

2.1. General > Basic

Device, Volume and Tamper of the device can be configured in this column.

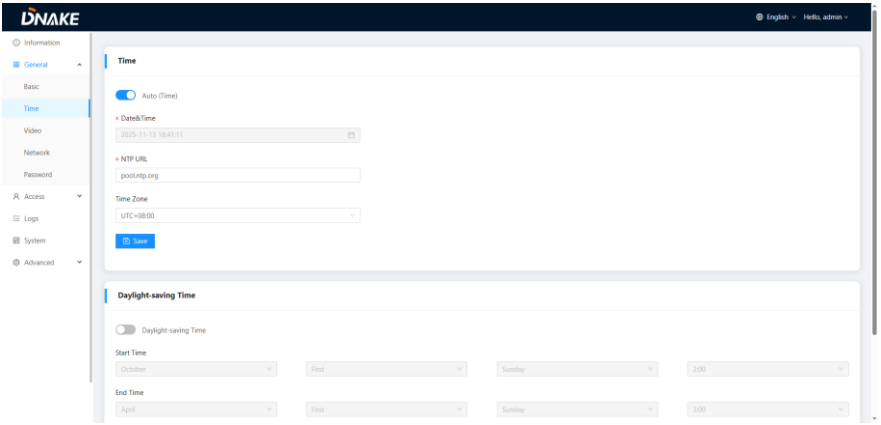


Automatic Deployment:	Turn on or off Automatic deployment;

Project ID:	It is used to configure the automatic deployment function of the device. After creating a project on the cloud platform, fill in the Project ID here and the device will be automatically added to the project;
Building No.:	Number of the Building (Range: 1-999);
Unit No.:	Number of the Unit (Range: 1-99);
Apartment No.:	Number of the Apartment (Range: 1-9899);
Device No.	Number of the Device (Range: 1-99);
Volume:	Volume of system can be set from 1 to 6;
Tamper:	Enable to use Tamper alarm on the back of the device;

2.2. General > Time

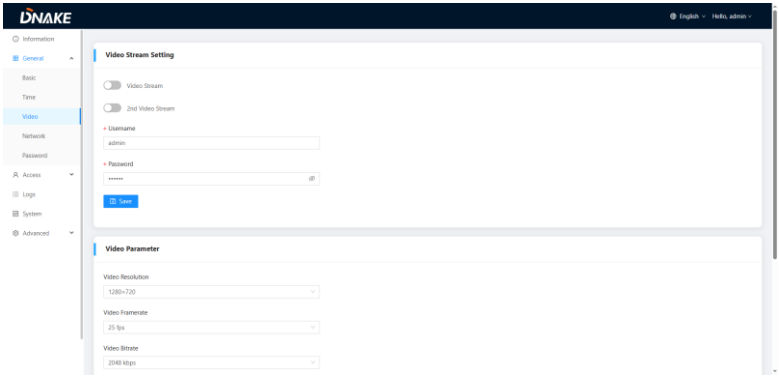
Time of the device can be configured. Daylight Saving Time is also supported.



Auto (Time):	Enable to synchronize computer time;
Date &Time:	Date and time can be set manually;
NTP URL:	Network Time Protocol (NTP) is a protocol used to synchronize computer time;
Time Zone:	A region that observes a uniform standard time;
Daylight-saving Time:	Enable to set DST;
Start Time:	The beginning of DST;
End Time:	The ending of DST;

Offset Time:	The default value is 60 minutes;

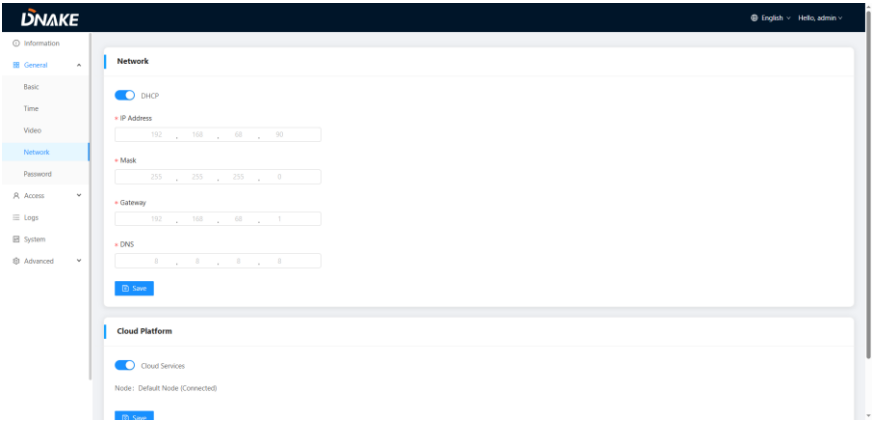
2.3. General > Video



Video Stream:	Enable main video stream for RTSP or Onvif; Format :rtsp://admin:123456@**ip address**:8554/ch01
2nd Video Stream:	Enable sub video stream for RTSP or Onvif; Format :rtsp://admin:123456@**ip address**:8554/ch01/sub
Username:	Set the username for video stream URL;
Password:	Set the password for video stream URL;
Video Resolution:	Set the resolution for main video stream;
Video Framerate:	Set the framerate for main video stream;
Video Bitrate:	Set the bitrate for main video stream;
2nd Video Resolution:	Set the resolution for sub video stream;
2nd Video Framerate:	Set the framerate for sub video stream;
2nd Video Bitrate:	Set the bitrate for sub video stream;

2.4. General > Network

The device network can be set to either DHCP or a static IP address.

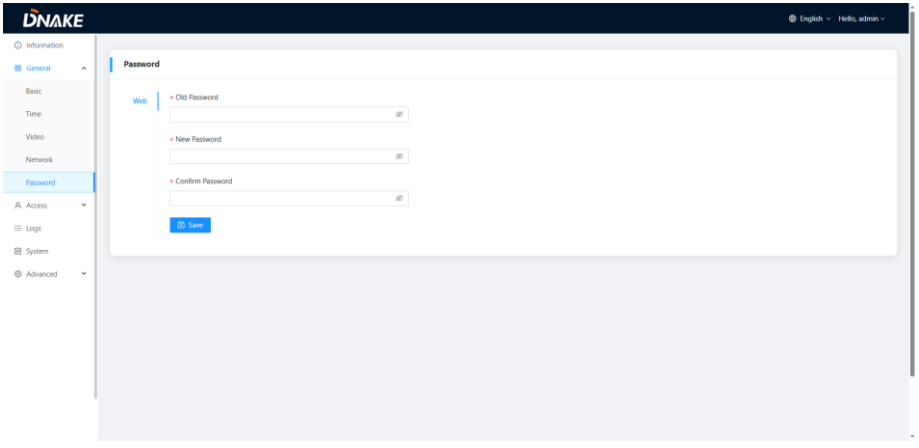


DHCP:	Enable DHCP (Dynamic Host Configuration Protocol) to dynamically distribute network configuration parameters;
IP Address:	Configure Static IP address to manually distribute network configuration parameters;
Mask:	Subnet mask;
Gateway:	A component that is part of two networks, which use different protocols;
DNS:	Domain Name Server of the device;
Cloud Platform:	Turn on or off the cloud platform connection

2.5. General > Password

The Web password is for the administrator to log in settings on the web.

The default password is 123456.

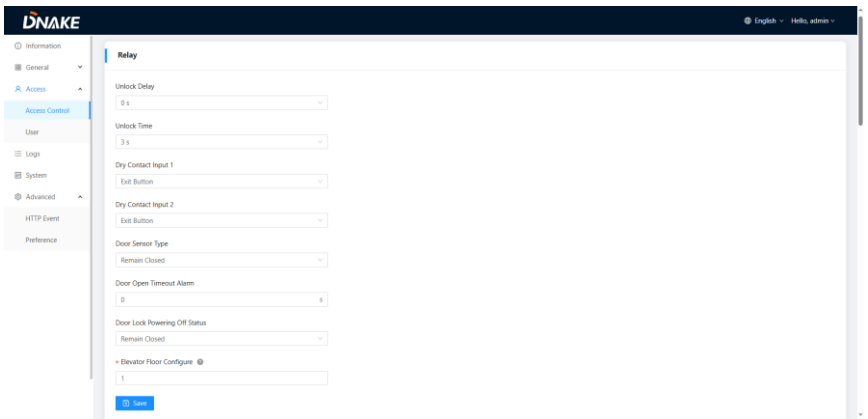


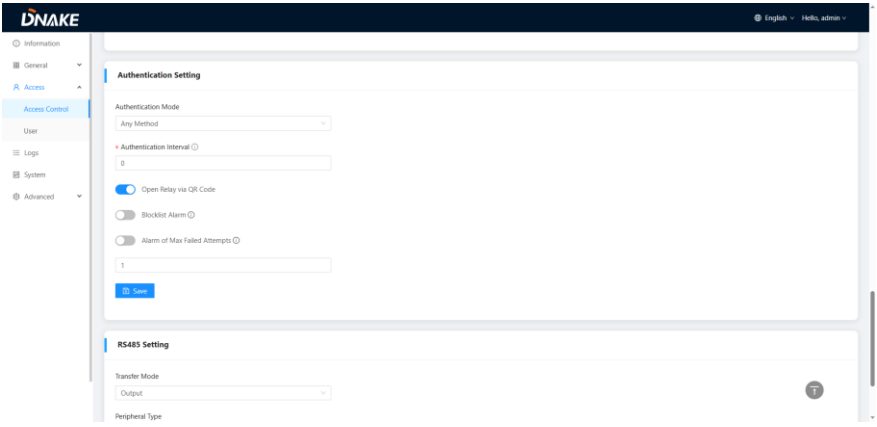
Web Old Password:	Current administrator password of the web (Default 123456);
Web New Password:	New administrator password of the web;
Web Confirm Password:	Confirm administrator password of the web;

3. Access

3.1. Access > Access Control

Relays, Access Cards, Wiegand Transfer Mode and Event Storage can be configured here.





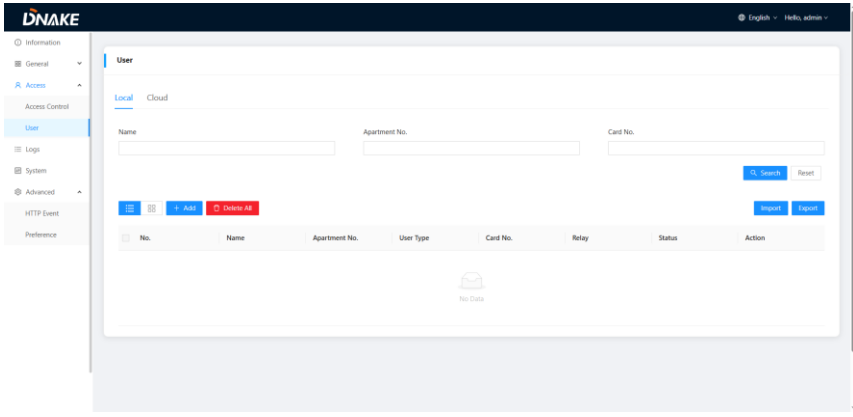
Unlock Delay:	The length of unlock delay time (0-9s);
Unlock Time:	The length of unlock time (1-9s);
Dry Contact Input 1-2:	3 modes of dry contact inputs are supported (Exit Button, Door Sensor, Fire Linkage);
Door Sensor Type:	2 types of door sensor are supported (Remain Closed ,Remain Open)
Door open Timeout Alarm:	Set the door open timeout (0-255s)
Door Lock Powering Off Status:	2 types of door lock powering off status are supported (Remain Closed ,Remain Open)
Elevator Floor Configure:	You can set the AC to the current floor (-9-99)
Master Card:	Click read to add Master card to manage cards;
Card Reading Mode:	When reading the card, the card information will display different data according to different modes (Default Mode or Full Card No.);
Card Order:	Select the reading order, which affects how the card data is displayed (Normal or Reversed);
Card Display Mode:	Select the card information display format (Hexadecimal or Decimal);

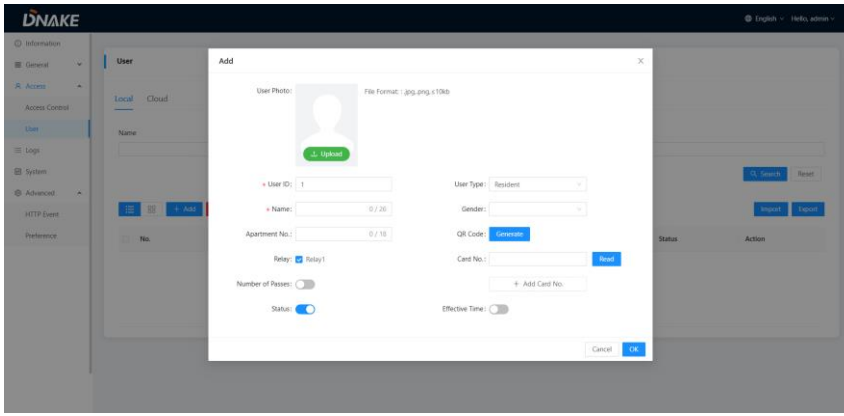
Mifare Card Encryption:	Enable or disable the Mifare Card Encryption;
Sector:	Select the sector to read the Mifare card (0~15);
Block:	Select the block of sector to read the Mifare card (0~3);
Block Key:	You can enter the Mifare card's encryption key here;
Wiegand Transfer Mode:	Select Transfer Mode of Wiegand port (Input or Output);
Wigand Output Bits:	Select Output Bits (26,34 or 58);
Wiegand Output Type:	Select Output Type;
Wiegand Input Bits:	Select Input Bits (26,34 or 58)
Wiegand Input Type:	Select Input Type;
Logs Storage Type:	You can set different storage method (Circular overwrite logs,Delete old logs periodically,Delete old logs by specified time;)
Delete Log When Storage Full:	When the unlocking record is full, if you want to store a new unlocking record, the device will delete the entry from beginning. You can set the specific quantity (0~999, Default is 300);
Duration:	Set the duration of deleting old logs periodically (10-86400 mins);
Specified Time:	System will delete logs within the specified time immediately after save
Authentication Mode:	Any Mode:you can use card or password to unlock Card+Password:you need to use card and password together to unlock;
Authentication Interval:	Each user can only unlock once successfully per configured period (0-65535);
Open Relay via QR code:	Enable it to allow QR code unlock;
Blocklist Alarm:	Device will trigger a 30s alert after identify a blocklist user;
Alarm of Max Failed Attempts:	Device will trigger a 10s alert after max times of failed verification (1-10);

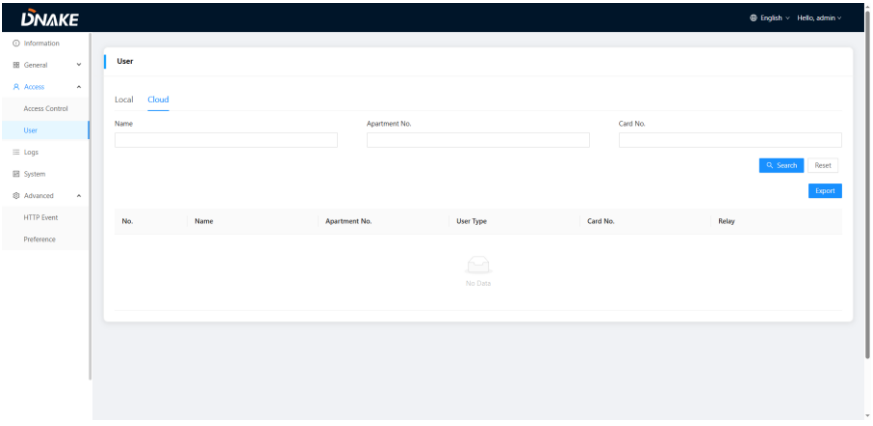
Transfer Mode:	You can set the transfer mode of RS485 interface (Input,Ouput);
Peripheral Type:	Set the peripheral type ,you can set it according to the device you want to connect (Security Relay Module,Elevator Control Module);
Elevator Mode:	Card Number:Access control will send card number to elevator module ,if you set this mode , you need to connect Access control to 485-1 interface of elevator module Elevator Floor:Access control will send current floor to elevator module ,if you set this mode , you need to connect Access control to 485-2 interface of elevator module

3.2. Access > User

Person column is for access authorization. You can add users to the device and relate them with relays or cards.


DNAKE
English
Hello, admin
Information
General
Access
Access Control
User
Logs
System
Advanced
HTTP Event
Preference
User
Local
Cloud
Name
Apartment No.
Card No.
Search
Reset
Add
Delete All
Import
Export
No.
Name
Apartment No.
User Type
Card No.
Relay
Status
Action
No Data


DNAKE
English
Hello, admin
Add
User Photo:
File Format: .jpg,.png,≤10kb
Upload
User ID:
User Type:
Resident
Name:
Gender:
Apartment No.:
QR Code:
Generate
Relay:
Relay1
Card No.:
Read
Number of Passes:
Add Card No.
Status:
Effective Time:
Cancel
OK



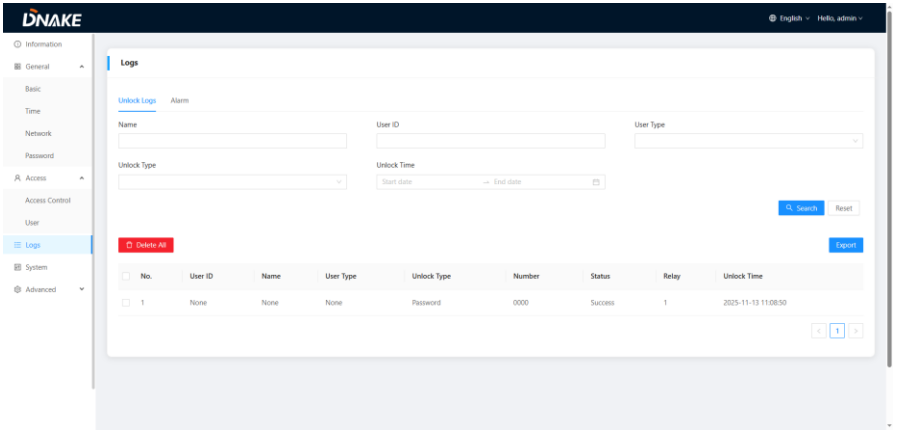
Search:	Fill in text inputs to search;
Reset:	Click reset to clear words in text inputs;
Delete All:	Delete all data on the chart;
Import:	Import all data to the chart;
Export:	Export all data on the chart;
Add:	Add users to Access Control; Fill in the User ID, Name, Apartment No, Number of Passes, choose the Relay, User Type, Gender, QR Code, Card No and Effective Time to add users.
Cloud:	The cloud platform will sync user information to the local device, you can check it in the Cloud column

4. Logs

It can support 100000 logs at most. If the logs are more than 100000, the previous logs will be covered;

4.1. Unlock Logs

Unlock logs by the Access Control are recorded here ,



Name:	The name of the person you add;
User ID:	The User ID you set on user column.
Unlock Type:	The type of Unlock Logs, including Card, Exit button, BLE , Card+Password, NFC, QR Code and APP;
Unlock Time:	The Unlock Logs will be filtered by the Date &Time you set;
Search:	Fill in text inputs to search;
Reset:	Click reset to clear words in text inputs;
Delete All:	Delete all data on the chart;
Export:	Export all data on the chart;

4.2. Alarm

Alarm triggered by the Access Control are recorded here ,

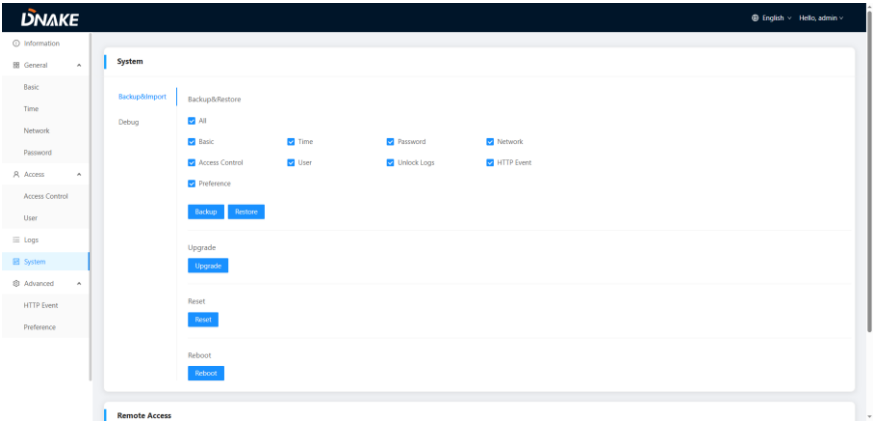
Name:	The name of the person you add;
Alarm Type:	The type of Alarm Logs, including Blocklist, Tamper, Fire, Door Open Timeout, Max Failed Attempt
Alarm Time:	The Alarm Logs will be filtered by the Date &Time you set;
Search:	Fill in text inputs to search;
Reset:	Click reset to clear words in text inputs;

Delete All:	Delete all data on the chart;
Export:	Export all data on the chart;

5. System

5.1. System

The system column is designed for data backup and restore, firmware upgrade, factory default, device reboot, packet capture and logs capture.



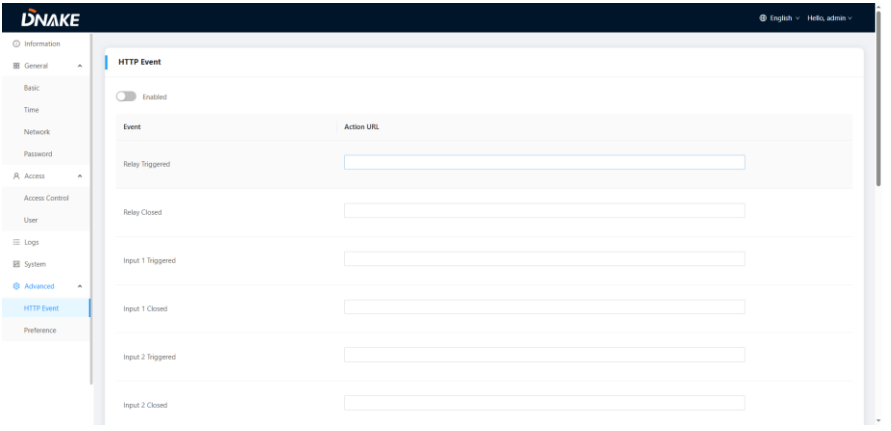
5.2. Remote access

Allow Remote access :After you enable it , you are able to access the device web interface from Cloud platform

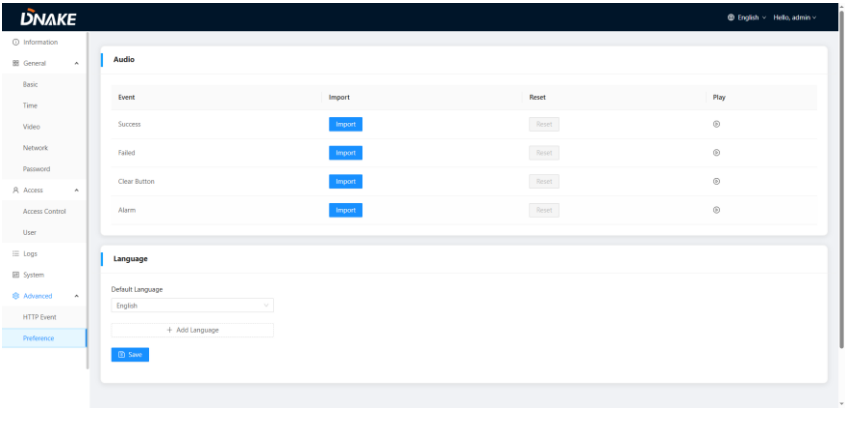
6. Advanced

6.1. Http Event

The device will send the corresponding URL when any of the following events is triggered

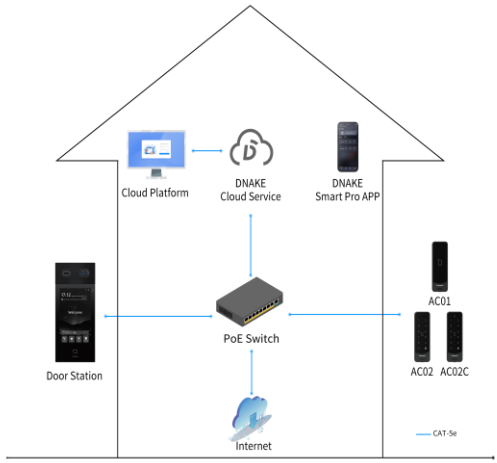


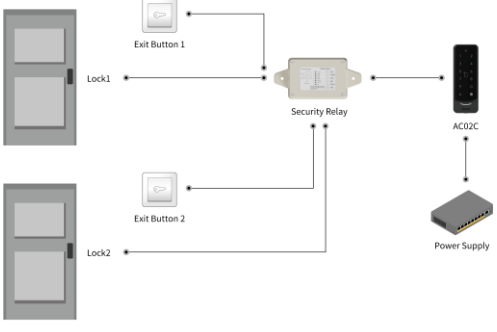
6.2. Preference



Audio:	You can customize the device's notification sound (Success.Failed,Alarm and clear button);
Language:	Language setup and import;

SYSTEM DIAGRAM




Exit Button 1
Lock1
Security Relay
AC02C
Exit Button 2
Power Supply
Lock2

DEVICE WIRING

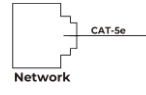
1	+12V
2	GND
3	NO
4	COM
5	NC

1	INPUT1
2	INPUT2
3	+5V
4	WD0
5	WD1
6	GND
7	485-
8	485+

1. Network (PoE)

Standard RJ45 interface is for the connection with PoE switch or other network switch.

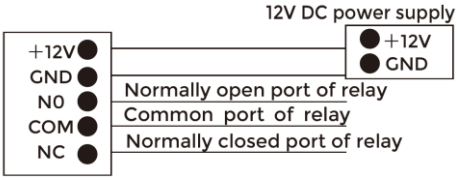
PSE shall comply with IEEE 802.3af (PoE) and its output power not less than 15.4W and its output voltage not be less than 50V.



2. Power/Switching Value Output

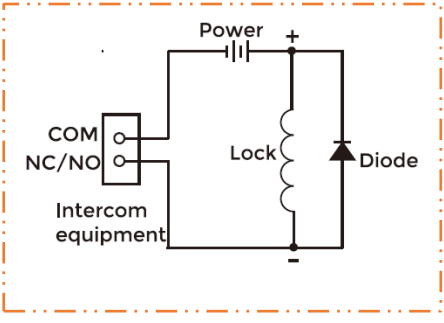
The power interface of Access Control connects to 12V DC power.

Connect to the lock module (an independent power supply is necessary for the lock).



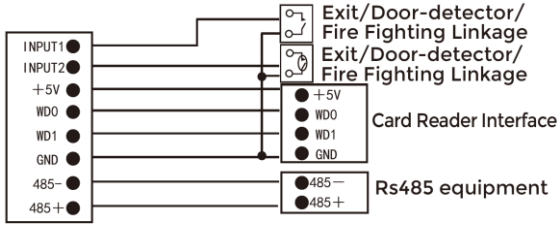
⚠ Warning!

1. When connecting to an inductive load device such as a relay or electromagnetic lock, you are recommended to use a diode 1A/400V (included in the accessories) in anti-parallel with the load device to absorb inductive load voltage peaks. The access control will be better protected in this way.
2. The load current of the relay cannot be greater than 2A. See attached picture for more details.



3. Custom input configuration interface/Wiegand/RS485

- The input interface can be configured with various functions, such as the exit button, door status sensor, and fire linkage interface.
- The interface can be connected to one IC/ID card reader or be used for reading the information of built-in card reader. Card swiping device connected to Weigand interface.
- +5V can power the Wiegand card swiping device, note that the current must not exceed100mA.
- Enable to connect equipment with RS485 interface. Connect to the lock module(independent power supply is necessary for the lock).

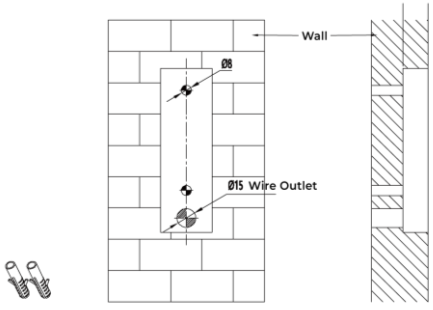


INPUT/Weigand/RS485

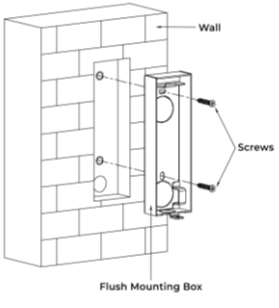
Note: Access Control can only be connected to one card reader or management device at a time.

INSTALLATION

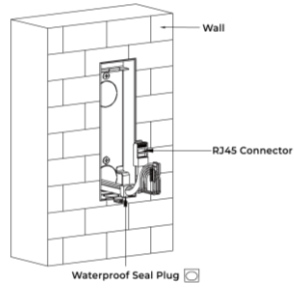
Installation of Flush Mounting



1. Choose the suitable height , and put the label sticker on the wall.
2. According to the sticker, drill three 8 x 45mm for screws and one 5mm for wire outlet.
3. Remove the sticker after drilling.



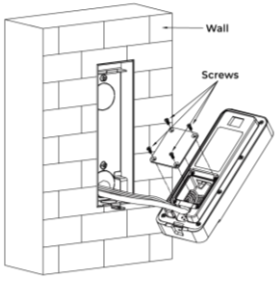
4. Lock the Flush Mounting Box with 2 screws.



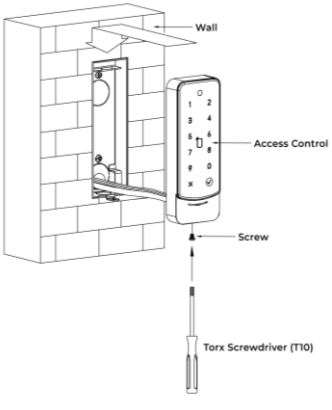
5. Let wires(included) and network cable without RJ-45 plug go through flush mounting box and waterproof seal plug.

6. Connect RJ-45 Plug.

7. Plug waterproof seal plug into the cover groove at the bottom.

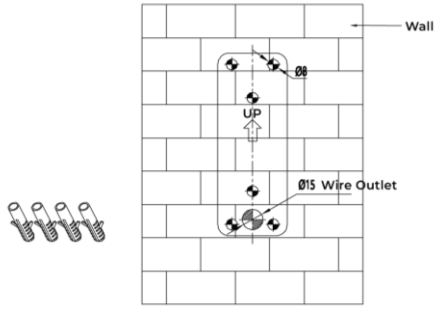


8. Fix interface clamp to the device with 4 screws.

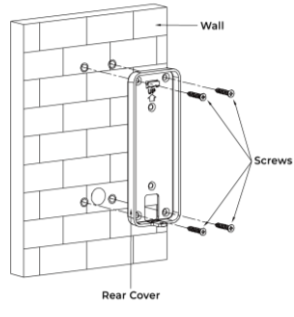


9. Use screwdriver to lock the bottom of the device with 1 screw

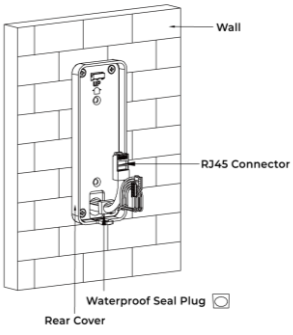
Installation of Surface mounting



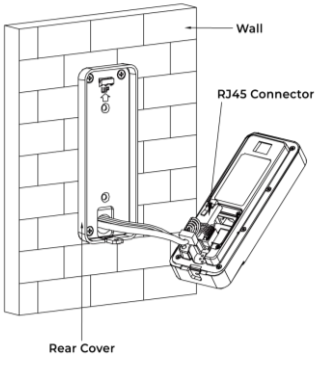
1. Choose the suitable height , and put the label sticker on the wall.
2. According to the sticker, drill three 8 x 45mm for screws and one 5mm for wire outlet.
3. Insert 4 screw fixing seats into the screw holes.
4. Remove the sticker after drilling.



5. Lock the rear cover with 4 screws.

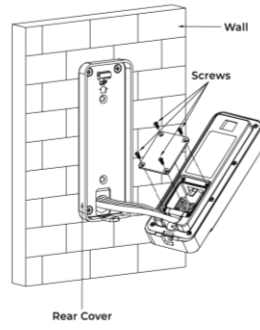


6. Let wires(included) and network cable without RJ-45 plug go through rear cover and waterproof seal plug.

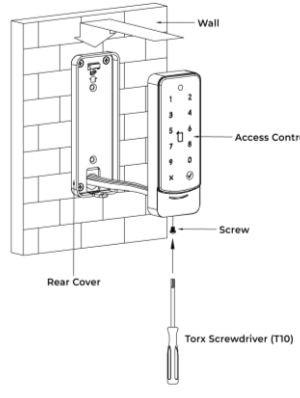


7. Connect RJ-45 Plug.

8. Plug waterproof seal plug into the cover groove at the bottom.



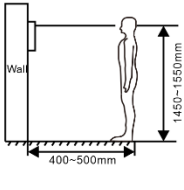
9. Fix interface clamp to the device with 4 screws.



10. Hang up device with rear cover.

11. Use screwdriver to lock the bottom of the device with 1 screw

Tips:



The camera should be 1450~1550mm above the ground.

TROUBLESHOOTING

The Access Control cannot start up or power off automatically.

- Check whether it has power-failure, and power it on again

The Access Control did not get IP address.

- Check if the DHCP is enabled on Access Control.
- Check whether the router can provide the IP address normally

---

No sound during the communication.

- Check whether the volume is set to the lowest.

Multimedia files cannot be played normally.

- Check whether the system supports the file format. Please refer to the multimedia setting for details.

Mifare SL3 card cannot be read in Access Control.

- The card reading mode needs to be 'Full Card No.'
- Block Key needs to be entered correctly;
- Select the correct sectors and blocks.

The temperature of device is too high.

- Long-term use leads to high temperature. It's normal and will not affect the device's use life and performance.

SAFETY INSTRUCTION

In order to protect you and others from harm or your device from damage, please read the following information before using the device.

- Do not install the device in the following places:
- Do not install the device in high-temperature and moist environment or the area close to magnetic field, such as the electric generator, transformer or magnet.
- Do not place the device near the heating products such as electric heater or the fluid container.
- Do not place the device in the sun or near the heat source, which might cause discoloration or deformation of the device.
- Do not install the device in an unstable position to avoid the property losses or personal injury caused by the falling of device.

Guard against electric shock, fire and explosion:

- Do not use damaged power cord, plug or loose outlet.
- Do not touch the power cord with wet hand or unplug the power cord by pulling.
- Do not bend or damage the power cord.
- Do not touch the device with wet hand.
- Do not make the power supply slip or cause the impact.
- Do not use the power supply without the manufacturer's approval.
- Do not have the liquids such as water go into the device.

Clean Device Surface

- Clean the device surfaces with soft cloth dipped in some water, and then rub the surface with dry cloth.

Other Tips

- In order to prevent damage to the paint layer or the case, please do not expose the device to chemical products, such as the diluent, gasoline, alcohol, insect-resist agents, opacifying agent and insecticide.
- Do not knock on the device with hard objects.

- Do not press the screen surface. Overexertion might cause flopover or damage to the device.
- Please be careful when standing up from the area under the device.
- Do not disassemble, repair or modify the device at your own discretion.
- The arbitrary modification is not covered under warranty. When any repair required, please contact the customer service center.
- If there is abnormal sound, smell or fume in the device, please unplug the power cord immediately and contact the customer service center.
- When the device isn't used for a long time, the adaptor can be removed and placed in dry environment.
- When moving, please hand over the manual to new tenant for proper usage of the device.

FCC Warning

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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE 1: 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.

NOTE 2: Any changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

RF exposure statement

This equipment complies with the FCC radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

V2.0

EASY & SMART
INTERCOM SOLUTIONS

DNAKE