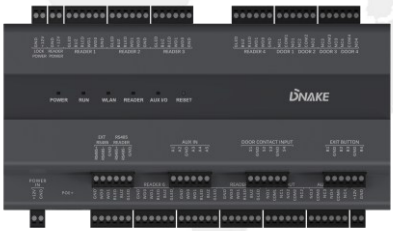
DNAKE



User Manual

DNAKE Access Controller



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

TECHNICAL PARAMETER 1

PACKAGE CONTENT 2

OVERVIEW 3

WEB SETTING 6

SYSTEM DIAGRAM 36

DEVICE WIRING 37

INSTALLATION 42

TROUBLESHOOTING 43

SAFETY INSTRUCTION 44

PRODUCT FEATURE

1. Support up to 100,000 users, 300,000 cards and 300,000 logs
2. Support OSDP protocol (2.2)
3. Support QR Code, Card, PIN, APP Unlock
4. Support advanced access features such as multi-door interlocking, anti-passback, first person in etc.
5. Work with DNAKE Cloud server and CMS

TECHNICAL PARAMETER

Power Supply: PoE+ or 12V DC

Outputs: 8 (4 Relay for Locks, 4 Relays for AUX Outputs)

Inputs: 13 (4 Exit Devices, 4 Door Contacts and 5 AUX Inputs)

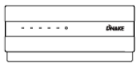
Working Humidity: 10 to 90% no condensing

Operating Temperature: -10℃to +55℃

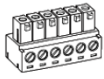
Storage Temperature: -40℃to +70℃

PACKAGE CONTENT

Model: AC-4D-MW



AC-4D-MW



6-Pin Terminal Block



2-Pin Terminal Block



Resistor



Wi-Fi Antenna

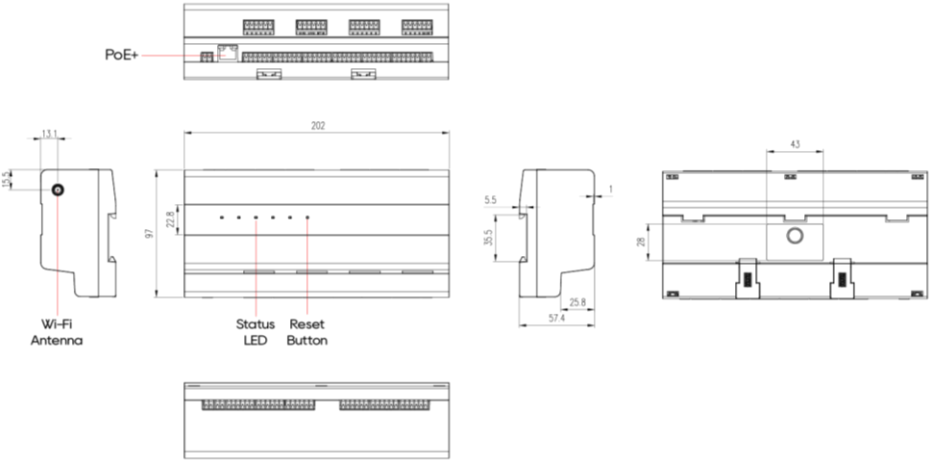


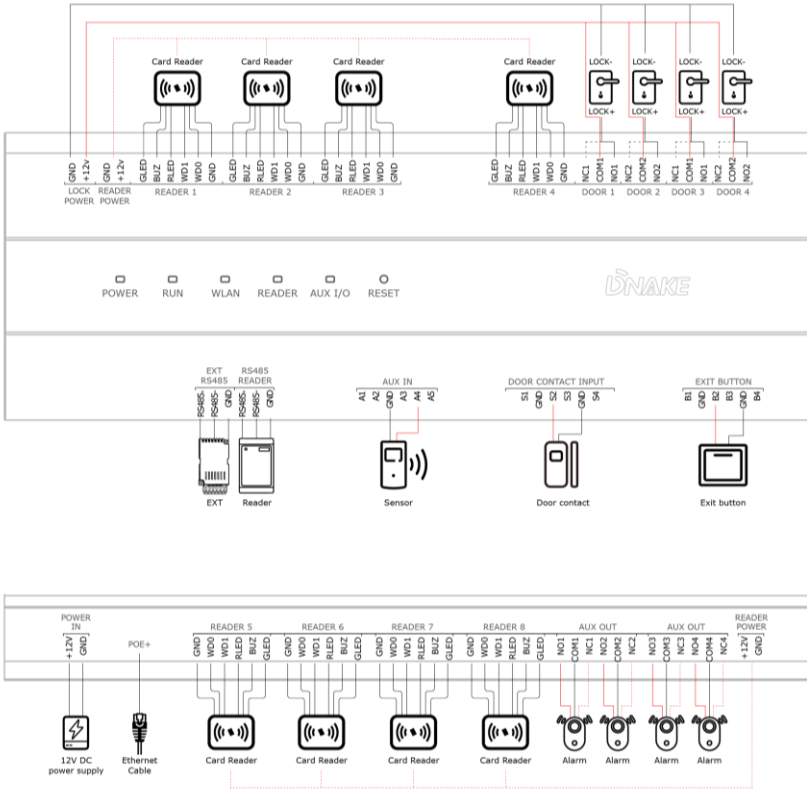
Antenna Connector



Quick Start Guide

OVERVIEW


PoE+
13.1
202
97
22.8
Wi-Fi
Antenna
Status
LED
Reset
Button
5.5
35.5
1
25.8
57.4
43
28



1. Status LED

Type	Status	Description
POWER	ON	The device is power on.
RUN	Flashing	The device completed startup and is operating normally.
WLAN	ON	The device connects to Wi-Fi network
READER	Flashing	The device receives signals from the READER interface
AUX I/O	ON	The device receives signals from the AUX I/O interface

2. Interface

Type	Function	Type	Function
Power In	12V DC Power Supply	Exit Button	Used to connect to the exit button.
RJ45 (PoE +)	Network Port for Communication and PoE Power Supply	Door Relay	Used to connect the relay to open or close door
RS485 for Reader	Used to connect the card reader	Wiegand Reader	Used to connect the Wiegand card reader
RS485 for Extension	Connect to the Security Relay Module and Elevator Control Module.	Reader Power	Provides 12 V DC power to the reader.
Auxiliary Input	Auxiliary input interface for connecting alarm sensors	Lock Power	Provides 12 V DC power to the reader.
Auxiliary Output	Auxiliary output interface for connecting audible and visual alarm devices.	Door Sensor	Used to connect the door sensor.

Note:

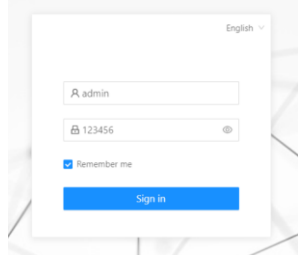
LED Light: Indicates the status of the device power, operation, WLAN, readers, and auxiliary interfaces.

Reset Button: Press the Reset button for 5s to reset the device.

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.

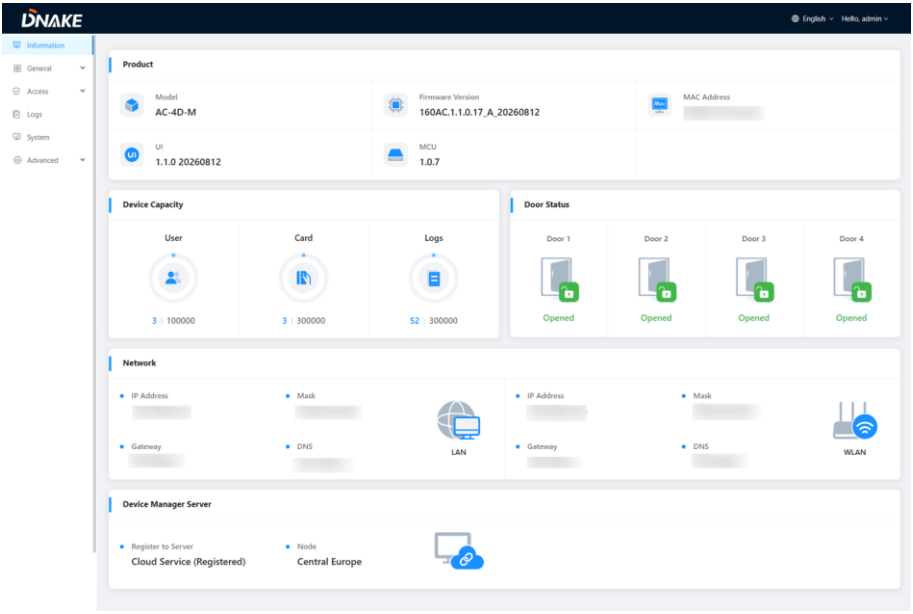
To get the IP address, you can search by DNAKE Remote Upgrade Tool installed in the same LAN with the devices.



3. Information

3.1. Information

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

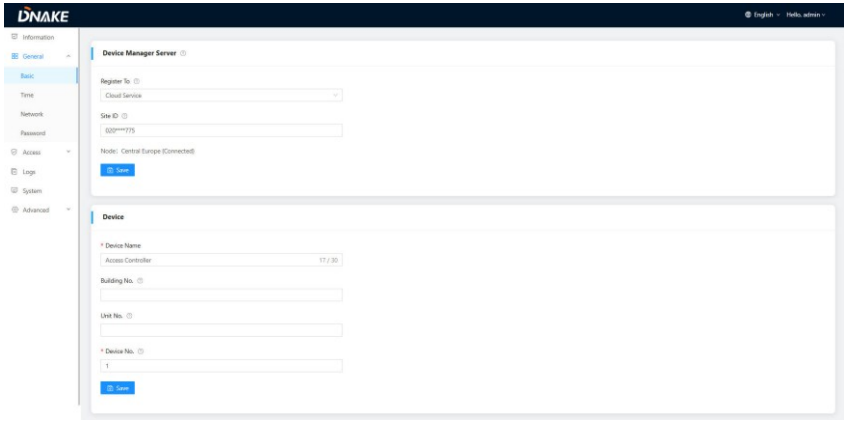


Category	Parameter	Description
Product	Model:	Model of the device;
	Firmware Version:	Firmware version of the device;
	MAC Address:	MAC address of the device;
	Framework:	Framework of the device;
	UI:	UI of the device;
	MCU:	MCU of the device;
Device Capacity	Device Capacity:	You can check the remaining capacity of the User Card and Logs;
Door Status	Door Status:	Status of Door;
Network	LAN:	Displays the LAN network information.
	WLAN:	Display the WLAN network information
	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;
Register to Server	Register To	Displays the selected cloud service type and its current status.
	Node	Node information of the management server to which the device is connected.

4. General

4.1. General > Basic

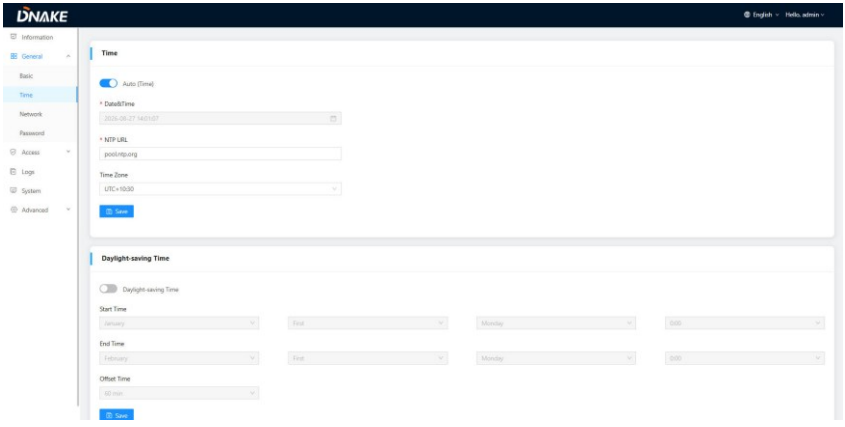


Category	Parameter	Description
Device Manager Server	Register to	Configure CMS or Cloud Platform device management server the device registers with
	Site ID / CMS IP	When Cloud Platform Service is selected, enter the corresponding Site ID in this field. When CMS service is selected, enter the corresponding CMS IP in this field.

	Node	Node information of the management server to which the device is connected.
Device	Building No.:	Number of the Building (Range: 1-999);
	Unit No.:	Number of the Unit (Range: 1-99);
	Device No.	Number of the Device (Range: 1-99);

4.2. General > Time

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

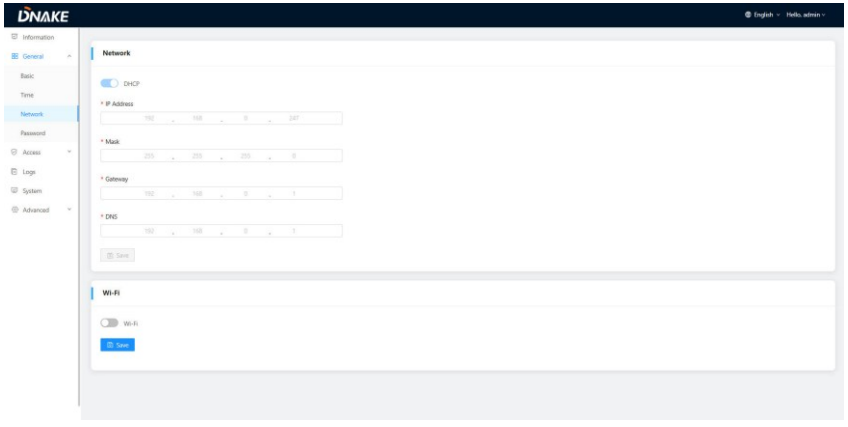


Category	Parameter	Description
Time	Auto (Time):	Enable to synchronize computer time;
	Date & Time:	Date and time can be set manually;
	NTP URL:	Network Time Protocol (NTP) is a protocol used to synchronize computer time;
	Time Zone:	A region that observes a uniform standard time;
Daylight-saving Time	Daylight-saving Time:	Enable or disable to set DST;

	Start Time:	The beginning of DST;
	End Time:	The ending of DST;
	Offset Time:	The default value is 60 minutes;

4.3. General > Network

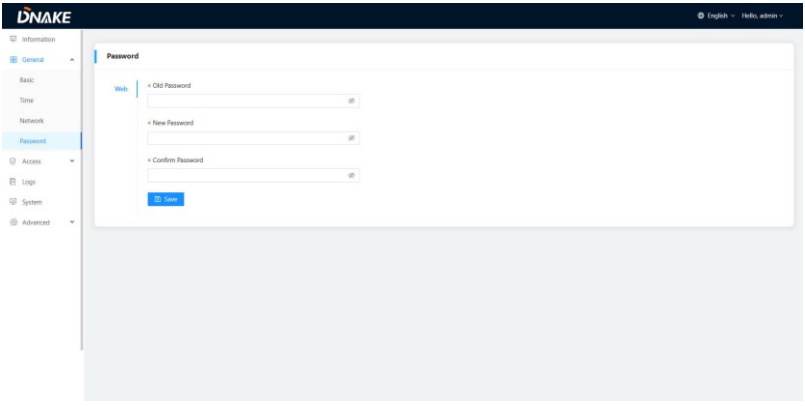
The device network can be set to either DHCP or a static IP address.



Category	Parameter	Description
Network	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;
Wi-Fi	Wi-Fi	Enable or disable the Wi-Fi function of device

4.4. General > Password

The Web password is for the administrator to log in settings on the web. The default password is 123456.

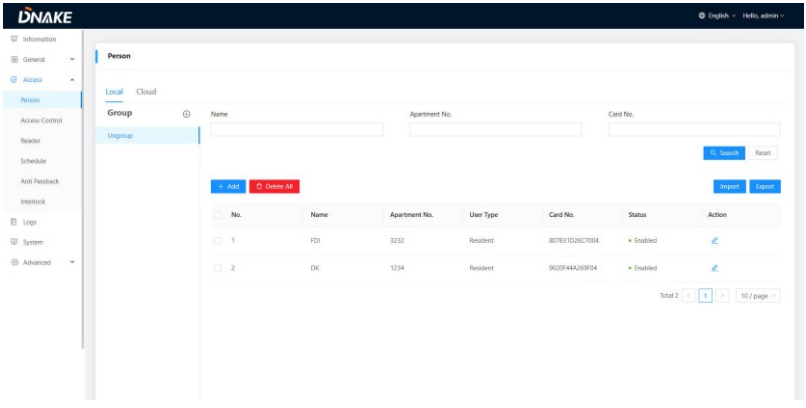


Category	Parameter	Description
Web	Web Old Password:	Current administrator password of the web (Default 123456);
	Web New Password:	New administrator password of the web;
	Web Confirm Password:	Confirm administrator password of the web;

5. Access

3.1. Access > Person

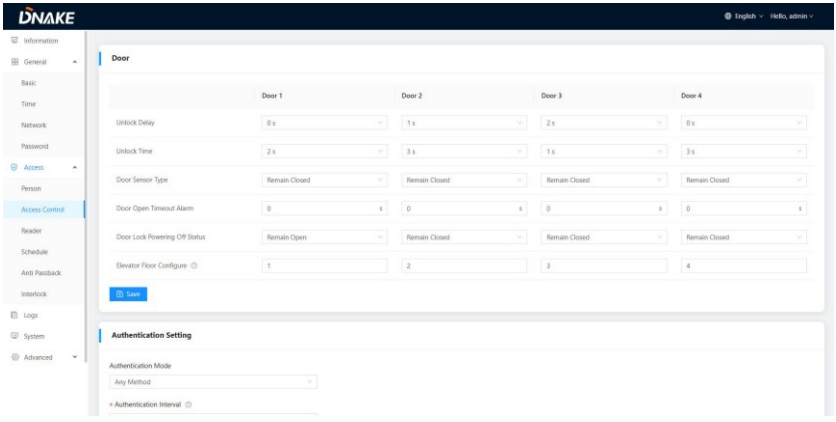
User column is for access authorization.



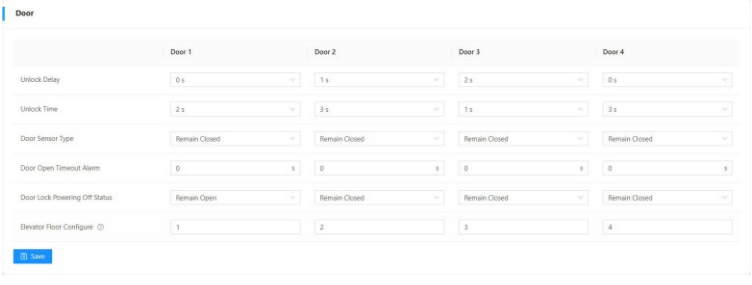
Category	Parameter	Description
Person	Search:	Fill in text inputs to search;
	Reset:	Click reset to clear words in text inputs;
	Add:	Add users to device;
	Delete All:	Delete all data on the chart;
	Export:	Export all data on the chart;

3.2. Access > Access Control

Door, Authentication Setting, Card, Public PIN Code and Logs Storage can be configured here.

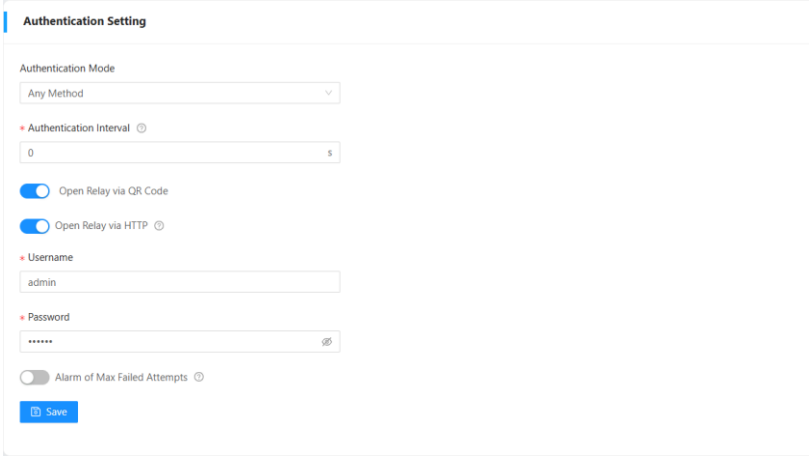


3.2.1. Access Control > Door



Category	Parameter	Description
Door	Unlock Delay:	The length of unlock delay time (0-9s);
	Unlock Time:	The length of unlock time (1-9s);
	Door Sensor Type:	4 types of door sensor are supported (NO (With EOL), NC (With EOL), NO (Without EOL), NC (Without EOL))
	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)

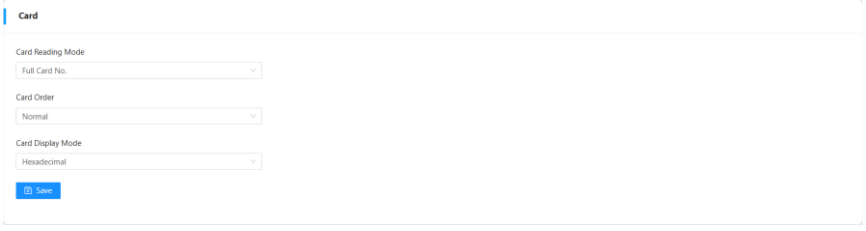
3.2.2. Access Control > Authentication Setting



Category	Parameter	Description
Authentication Setting	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 or disable device open relay by QR code function
	Open Relay via HTTP	Configure whether third-party devices can use http to unlock. If enabled, third parties can use http commands to unlock.
	Username	The username of HTTP open relay function
	Password	The password of HTTP open relay function

	Alarm of Max Failed Attempts:	Device will trigger a 10s alert after max times of failed verification (1-10);

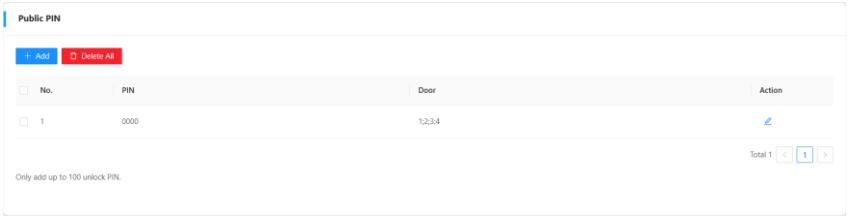
3.2.3. Access Control > Card



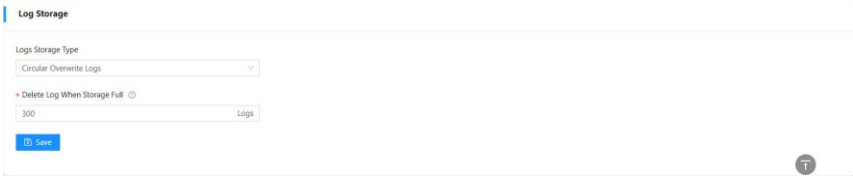
Category	Parameter	Description
Card	Card Reading Mode:	When reading the card, the card information will display different data according to different modes (Default Mode or Full Card No.);
	Card Order:	Select the reading order, which affects how the card data is displayed (Normal or Reversed);
	Card Display Mode:	Select the card information display format (Hexadecimal or Decimal);

3.2.4. Access Control > Public PIN

Configure the public PIN code of the device. You can unlock the corresponding relay by using this PIN



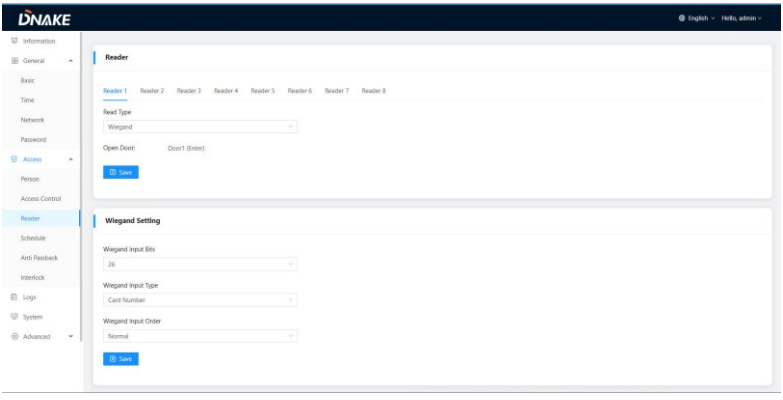
3.2.5. Access Control > Log Storage



Category	Parameter	Description
Log Storage	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 S torage 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

3.3. Access > Reader

Configures the parameters of the controller's external Wiegand readers and RS-485 (OSDP) readers.



3.3.1. Reader >Reader

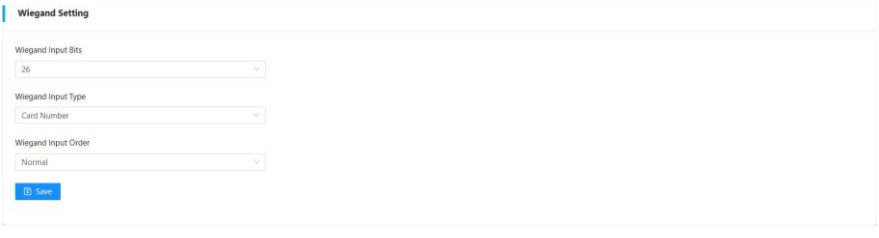
The controller supports up to 8 external readers, with each reader assigned to a corresponding door (relay).



Category	Parameter	Description
Reader	Reader Type	Sets the communication type for Reader 1–Reader 8. The available options are Wiegand, RS-485, and OSDP, with Wiegand as the default. When set to Wiegand, the controller receives input data from the corresponding Wiegand reader port

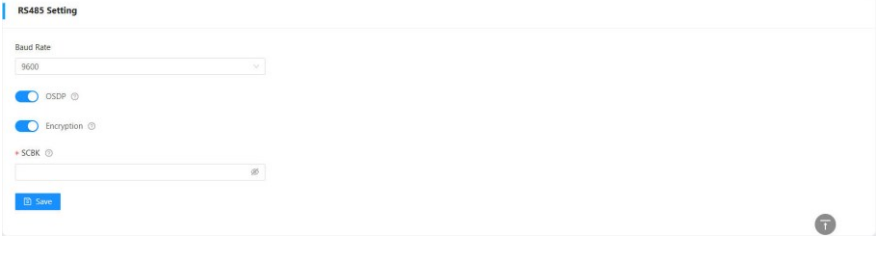
		for access verification and door unlocking.
		When set to RS-485 or OSDP, the controller receives input data from the RS-485 reader port for access verification and door unlocking.
	Open Door	Readers 1–8 are assigned to Doors 1–4 in pairs for entry and exit.

3.3.2. Reader > Wiegand Setting



Category	Parameter	Description
Wiegand Setting	Wiegand Input Bits:	Select Input Bits (26,34 or 58)
	Wiegand Input Type:	Select Input Type;
	Wiegand Input Data Order	Select Input Data Order of Wiegand port (Normal or Reversed)

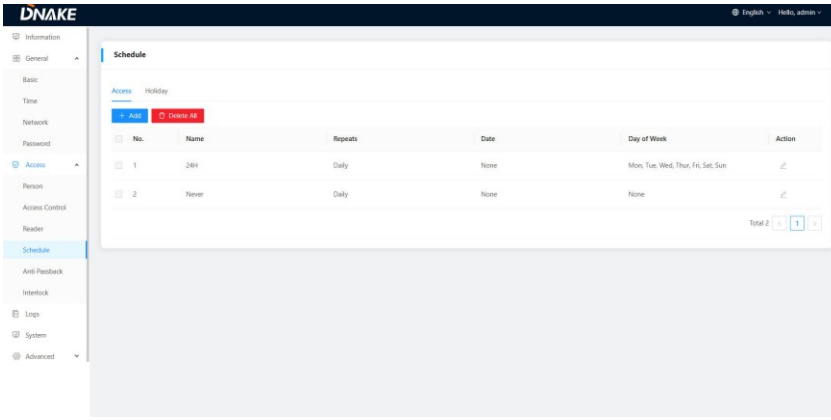
3.3.3. Reader > RS485 Setting



Category	Parameter	Description
RS485 Setting	Baud Rate	The baud rate of RS485 interface
	OSDP	Enable or disable the OSDP protocol. When disabled, the RS485 port uses the standard RS485 protocol and functions as an RS485 reader. When enabled, the RS485 port uses the OSDP protocol and functions as an OSDP reader.
	Encryption	Enable or disable OSDP encryption. This feature is supported only by OSDP v2.x devices.
	SCBK	when OSDP encryption is enabled. Enter the OSDP encryption key manually. The key must be exactly 16 bytes in length.

3.4. Access > Schedule

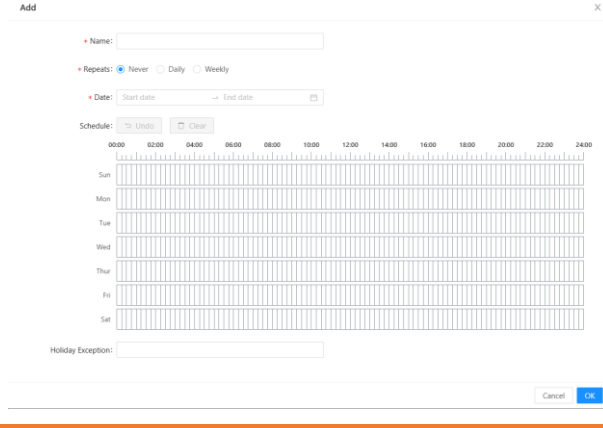
The Schedule function enables the device to automatically enter Always Open mode after the first authorized unlock within a specified time period. The device remains unlocked until the configured end time and then automatically returns to normal operation. This function is available when the Anti-Passback function is enabled.



3.4.1. Schedule > Access

On the Access page, you can configure access time templates, which can be associated with Always Open schedules or used to define access permissions for specific users.

The 24H and Never access rules are default rules and cannot be edited or deleted.

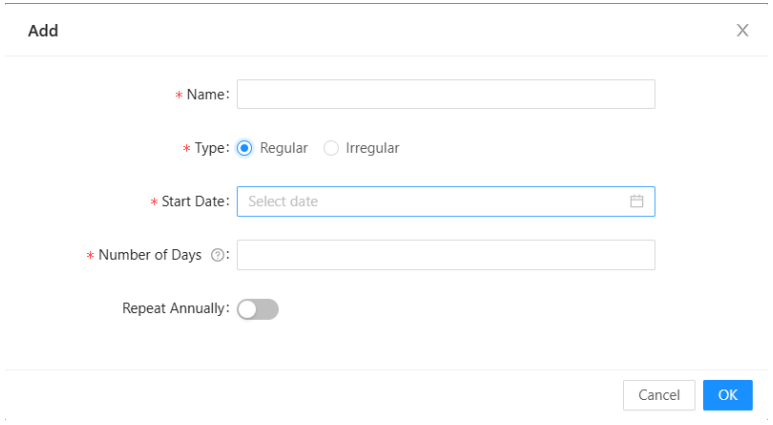


Category	Parameter	Description

Access	Name:	The name of access rule, support up to 30 characters and cannot duplicate name with any existing access rule;
	Repeats:	Select the recurrence type for the access rule: Never: Configure a one-time access rule within a specified time period.
	Date:	When the repeats set to "Never", the Start Date and End Date must be configured. The Start Date can be the same as the End Date.
	Schedule:	When the repeats set to "Never" or "Weekly", the time periods for each day from Monday to Sunday in the schedule can be configured;
		When the repeats set to "Daily", the schedule defines the time period that repeats every day;
		Multiple time periods can be configured. Use the mouse to drag across the schedule grid to set the desired time periods. Each grid cell represents 15 minutes.
	Undo:	Click Undo to revert changes. Each click reverses one operation until all previous operations have been undone.
	Clear:	Click Clear to remove all configured time periods from the schedule.
	Holiday Exception:	Use the drop-down multi-select menu to configure holiday rules. After selecting the holidays, set the corresponding time periods in the schedule.

3.4.2. Schedule > Holiday

Configure holidays, which can be associated with access time templates to define access rules during holiday periods.

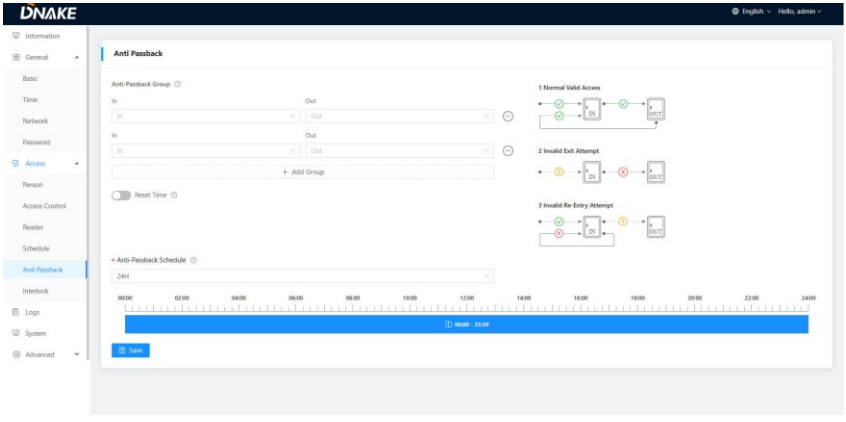


Category	Parameter	Description
Holiday	Name:	The name of holiday, support up to 30 characters and cannot duplicate name with any existing holiday;
	Type:	Type can be set to Regular or Irregular;
	Date:	When the repeats set to "Never", the Start Date and End Date must be configured. The Start Date can be the same as the End Date.
	Type:	When Type is set to Regular, select a specific date as the start date.
		When Type is set to Irregular, select a specific day of the week as the start date. 1.Select the Year from the drop-down list. The available range is from the current year to the current year + 10 years.

		2.Select the Month from the drop-down list. The available range is January to December. 3.Select the Week Number from the drop-down list: First, Second, Third, Fourth, or Last week. 4.Select the Day of the Week from the drop-down list: Monday to Sunday.
	Number of Days:	Enter the number of holiday days. Only integers from 1 to 366 are supported.
	Repeat Annually:	When selected, the holiday will repeat every year.

3.5. Access > Anti-Passback

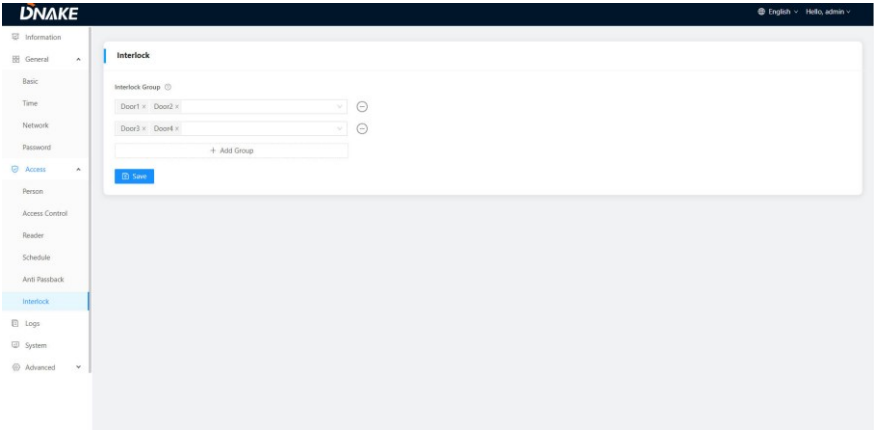
Verification is required for both entry and exit. If a user enters after successful verification but exits without verification, an alarm is triggered and the user is denied entry on the next attempt. Similarly, if a user enters without verification, an alarm is triggered and exit is denied when the user attempts to verify for exit.



Category	Parameter	Description
Anti-Passback	Anti-Passback Group:	Supports configuring verification points (readers) for anti-passback rules. Up to 4 groups can be added, and each group must include at least one entry reader and one exit reader.
		Entry: Select one or more readers as entry readers from Reader 1–8.
		Exit: Select one or more readers as exit readers. Readers assigned to Entry cannot be selected again.
		Anti-passback Logic: The system checks the user's previous access direction during verification. If no previous record exists, the first verification at an Entry reader is allowed
	Reset Time	Sets whether to enable the anti-passback reset time. When enabled, the system checks whether the reset time has elapsed since the last valid unlock. If not, access is denied and an anti-passback event is generated.
	Anti-passback Schedule	Select a time schedule template from the available schedules. Anti-passback rules apply only during the scheduled periods. No anti-passback verification or events are triggered outside the scheduled periods.

3.6. Interlock

Sets the doors to be included in the interlock group



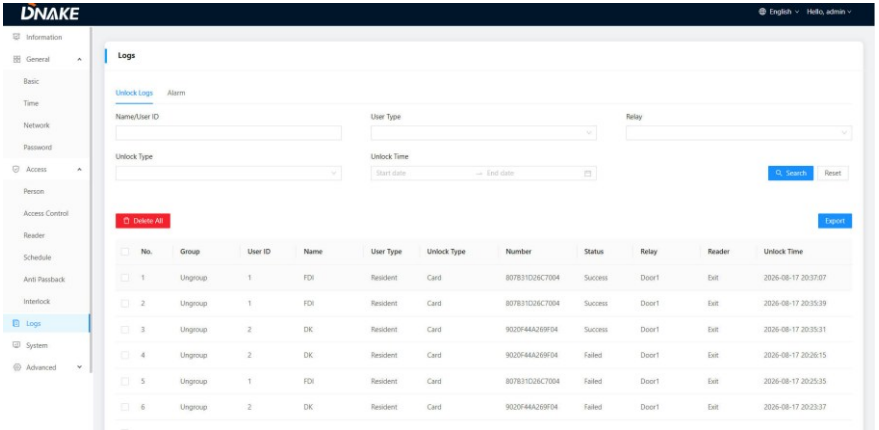
Category	Parameter	Description
Interlock	Interlock Group	Adds doors to the interlock group. Select Door 1–Door 4 from the dropdown list.
	Interlock Logic	When one door in the same group is open, as indicated by the door sensor status, verification on other doors is denied and an interlock event is generated.

6. Logs

It can support 300000 logs at most. If the logs are more than 300000, the previous logs will be covered;

4.1. Unlock Logs

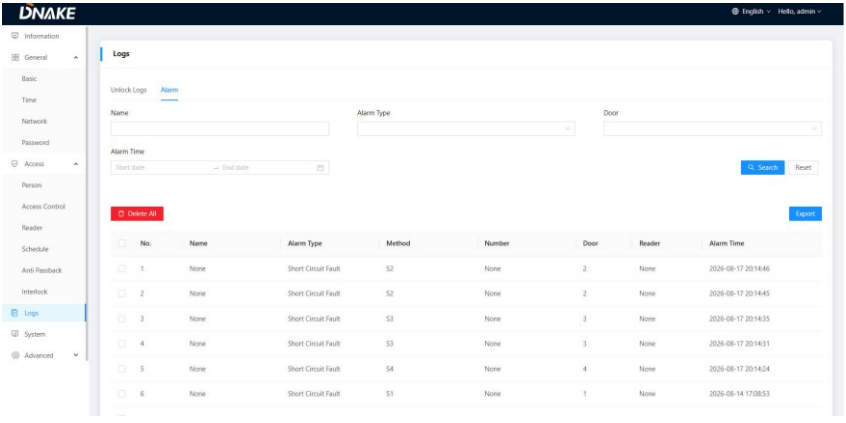
Unlock logs by the Access Control are recorded here.



Category	Parameter	Description
Unlock Logs	Name:	The name of the person you add;
	User ID:	The User ID you set on user column.
	User Type	The User Type set in the column
	Unlock Type:	The type of Unlock Logs;
	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.

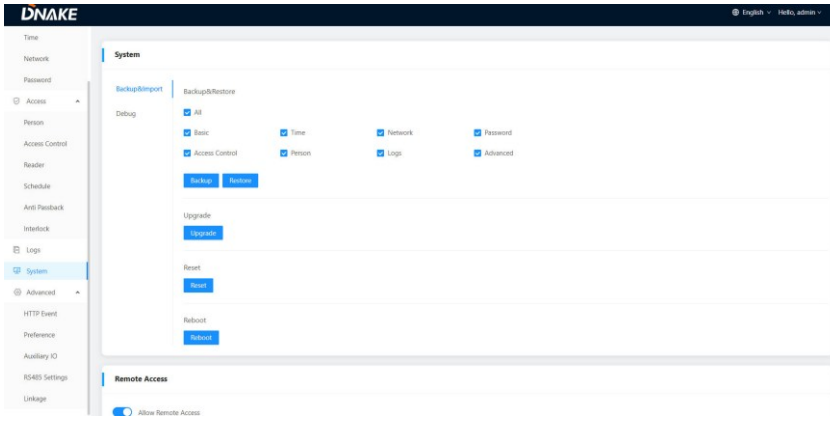


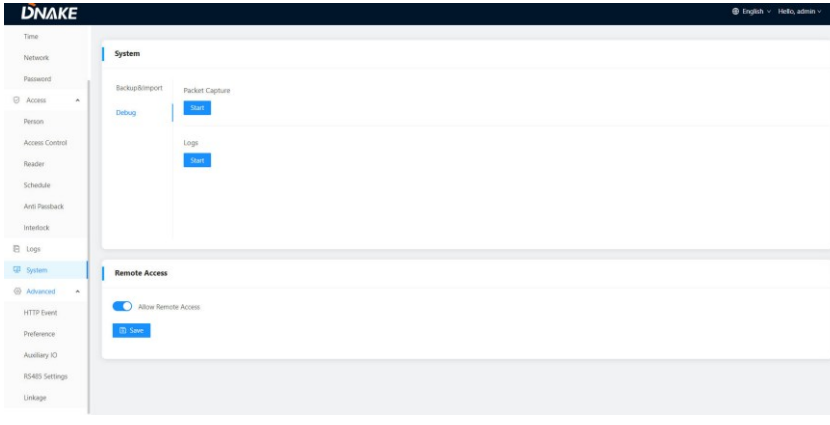
Category	Parameter	Description
Alarm	Name:	The name of the person you add;
	Alarm Type:	The type of Alarm Logs
	Door	Select the door that triggered the alarm event to filter the alarm information.
	Alarm Time:	The Alarm Logs will be filtered by the Date &Time you set;
	Search:	Fill in text inputs to 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;

7. System

7.1. System

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





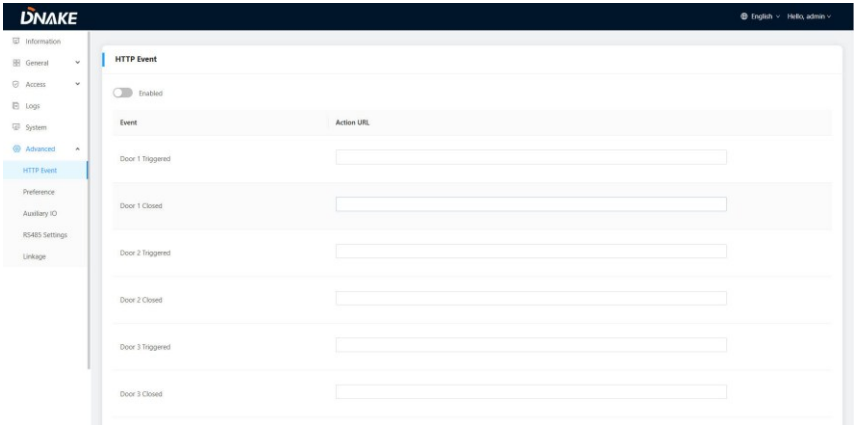
Category	Parameter	Description
Backup & Import	Backup & Restore:	Backup all setting and restore settings;
	Upgrade:	Upgrade equipment;
	Reset:	Reset to factory settings;
	Reboot:	Reboot the device;
Debug	Packet Capture:	Capturing packets can help developers reproduce positioning problems;
	Logs:	Device logs;

	Screenshot:	Screenshot device interface;
Remote Access	Allow Remote Access	Configure whether the device allows the cloud platform remote Web UI

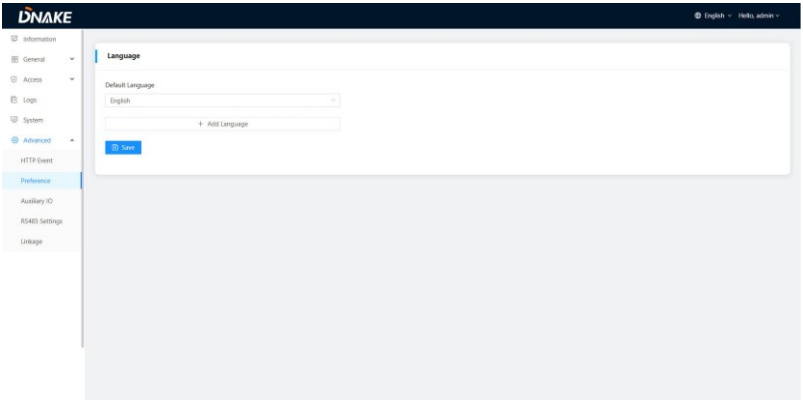
8. Advanced

8.1. HTTP Event

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



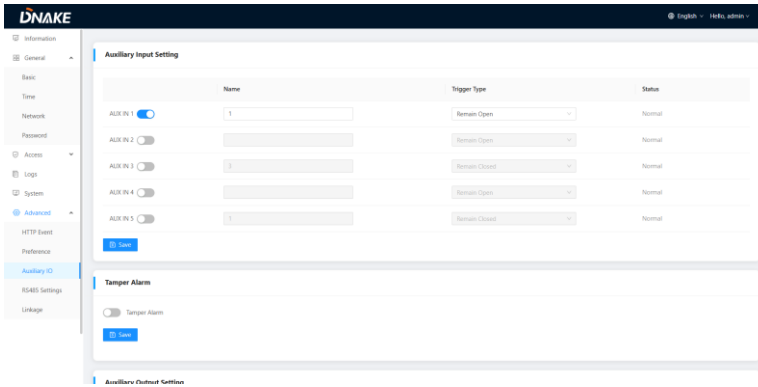
8.2. Preference



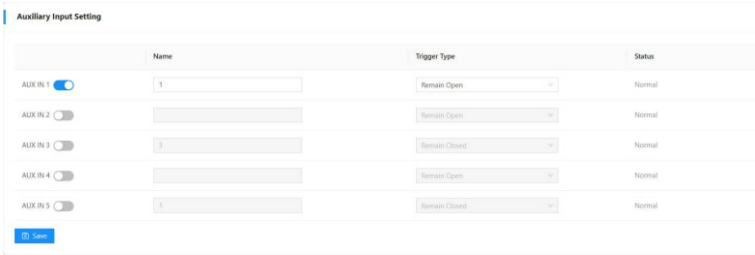
Category	Parameter	Description
Language	Default Language:	Language setup and import;

8.3. Auxiliary IO

Configures the parameters of the device's 5 dry-contact inputs and 4 auxiliary relay outputs, typically used for sensor alarms and audible/visual alarm devices.



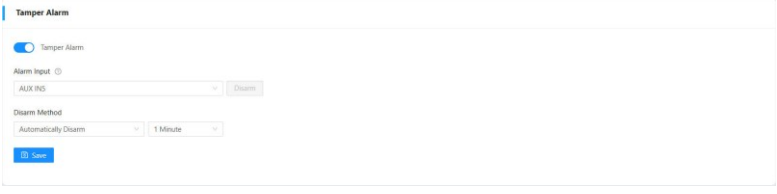
8.3.1. Auxiliary Input Setting



Category	Parameter	Description
Auxiliary Input Setting	Enable/Disable:	Enables or disables the five dry-contact inputs: AUX IN1–AUX IN5. When enabled, a change in input status triggers the associated logic

		actions and generates an alarm event record.
		When disabled, status changes do not trigger any actions or events, and the Name and Trigger Type settings are disabled.
	Name	Sets the name of the auxiliary input event. The name is displayed as the Alarm Type in alarm event records.
	Trigger Type	Selects the trigger type for the dry-contact input

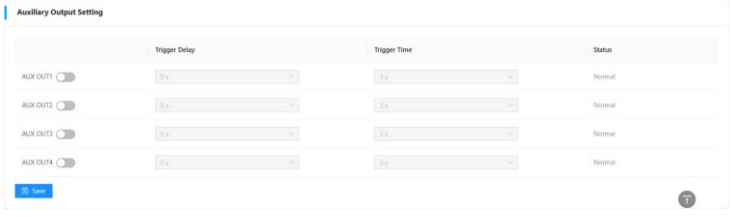
8.3.2. Tamper Alarm



Category	Parameter	Description
Tamper Alarm	Alarm Switch	Enables or disables the tamper alarm function.
		When enabled, a change in the selected auxiliary input triggers a tamper alarm event and activates the device buzzer.
		When disabled, no tamper alarm is triggered and the related settings are hidden. Disabled by default.
	Alarm Input	Selects an auxiliary input as the tamper alarm trigger point. This setting is required when the alarm is enabled.

	Disarm Method	Sets the method for canceling the alarm sound after a tamper alarm is triggered
		Auto Disarm: Select 1/5/10/30 minutes. The alarm sound is automatically canceled after the selected time has elapsed.
		Card/Password Twice: Present the same registered card twice or enter the same password twice at the same reader within 1 minute to cancel the alarm sound.

8.3.3. Auxiliary Output Setting

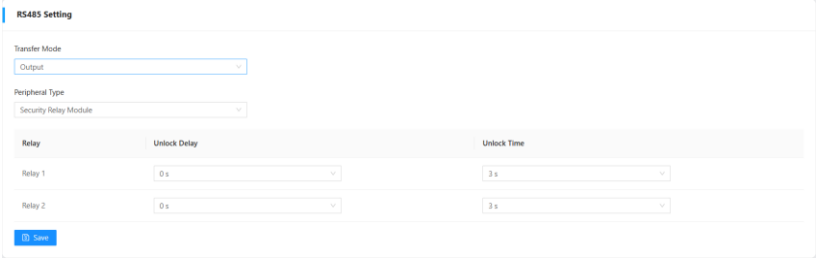


Category	Parameter	Description
Language	Enable/Disable	Enables or disables the auxiliary relay output.
		When enabled, the relay can be triggered as a linked action.
		When disabled, the relay cannot be triggered and the related settings are disabled. Disabled by default.
	Trigger Delay	Sets the delay before the relay is triggered. Range: 0–9 s. Default: 0 s.
	Trigger Duration	Sets how long the relay remains triggered. Range: 1–9 s. Default: 3 s.

	Status	Displays Triggered when the relay is activated and Normal when the relay returns to its normal state.

8.4. RS485 Setting

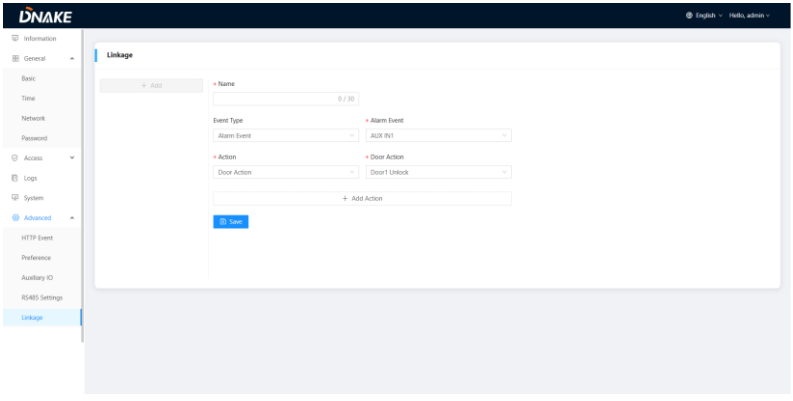
Supports configuring the device's RS-485 expansion interface to connect to an elevator control module for linked elevator control actions, or to a relay module to expand the number of relay outputs.



Category	Parameter	Description
RS485 Setting	Transfer Mode	Sets the RS-485 transfer mode. Currently, only Output mode is supported, in which the controller outputs data via RS-485 to control external modules.
	Peripheral Type	Selects the type of connected peripheral device: Security Relay Module or Elevator Control Module.
		Security Relay Module: Connects to the UM5-F19 relay module to control relay unlocking. The unlock delay and duration can be configured separately for Relay 1 and Relay 2.
		Elevator Control Module: When the output type is set to Elevator Floor,

		the controller outputs the floor and resident information via RS-485 after successful access verification.

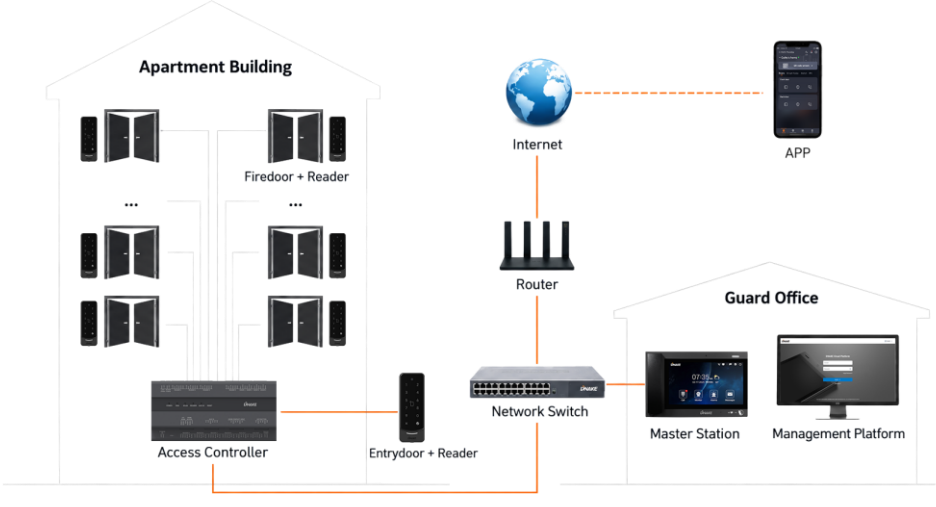
8.5. Linkage



Category	Parameter	Description
Linkage	Name	Required. Enter up to 30 characters as the linkage name.
	Event Type	Select the event type used as the linkage condition
	Event Parameter	Select the event parameter used as the linkage condition
	Action	Select the action to be performed when the linkage condition is set
	Action Parameter	Select the action parameter used as the action condition
	Action Parameters	Door Action: Select one or more doors to unlock.
		Auxiliary Output: Select one or more auxiliary output relays to trigger.
		HTTP URL: Enter the URL to be sent when the linkage condition is met.

		Security Relay Module: Select one or more relays (Relay 1 or Relay 2) to trigger.

SYSTEM DIAGRAM



DEVICE WIRING

1. Controller Power Input

The power input interface of the device. Connect to a 12V 7A DC power supply.



1.1. 12V DC Power Supply

When the access controller powered by a 12 V DC power supply:

- LOCK POWER provides 12 V/4 A to power the locks. The current for a single lock must not exceed 3 A.
- READER POWER provides 12 V/1 A to power the readers. The current for a single reader must not exceed 500 mA.

1.2. PoE +

When the access controller is powered by PoE+:

- LOCK POWER provides no power output. The locks must be powered by an external power supply, and the power supply ground must be connected to the access controller ground.

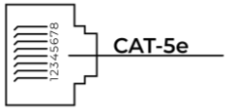


- READER POWER provides 12 V/0.8 A to power the readers. The current for a single reader must not exceed 500 mA.



2. Network Interface

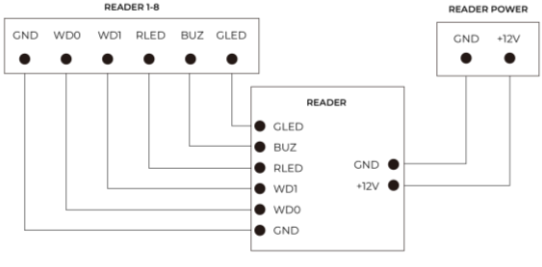
Standard RJ45 interface for connecting the device to other network device through a switch. The interface support PoE+, allowing a PoE+ switch to power the access controller



3. Wiegand Reader Interface

Used to connect external Wiegand readers. The reader are powered by the access controller through the READER POWER interface.

- When the access controller is powered by 12 V DC, READER POWER provides 12 V/1 A.
- When the access controller is powered by PoE+, READER POWER provides 12 V/0.8 A.
- The maximum Wiegand signal cable length is 80 m.
- Reader interfaces 1-8 have the same connection method.



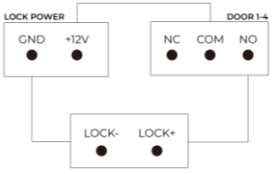
4. Relay Unlock Interface

The electric lock interfaces are shown below. The supported lock types include cathode locks and anode locks/magnetic locks.

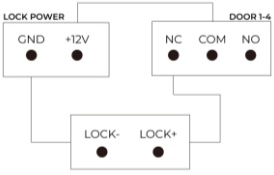
The relay terminals support a maximum load of 3.5 A at 24 V DC for a purely resistive load.

When the lock power cable is less than 100 m, the lock can be powered by the access controller through LOCK POWER, which provides 12 V/4 A. The current for a single lock must not exceed 3 A.

When the lock power cable is longer than 100 m, a external power supply must be used. The external power ground must be connected to the access controller ground.



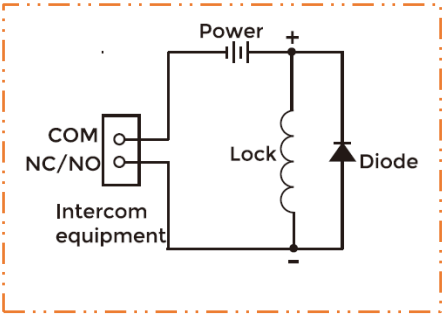
Cathode Lock



Anode 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.

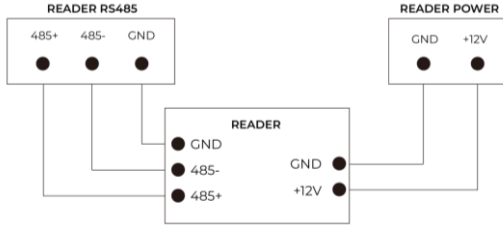


5. RS485 Interface

The RS485 interface include EXT RS485 and READER RS485

5.1. EXT RS485

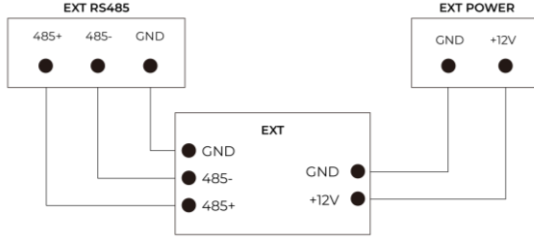
Connects to external expansion modules. The expansion module must be powered by an external power supply, and the power supply ground must be connected to the access controller ground.



5.2. READER S485

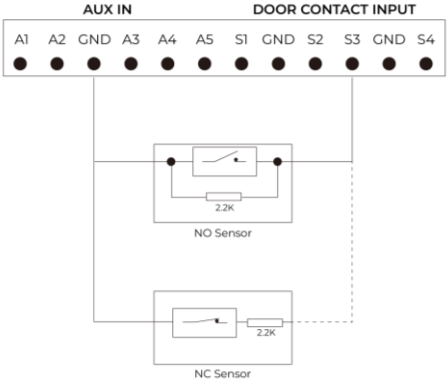
Connects to RS485 reader. The readers are powered by the access controller through the READER POWER interface.

- When the access controller is powered by 12 V DC, READER POWER provides 12 V/ 1 A.
- When the access controller is powered by PoE+, READER POWER provides 12 V/0.8 A.



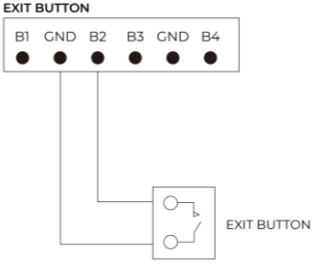
6. Auxiliary Input/Door Contact Interface

The auxiliary input door contact interfaces provide 9 inputs in total. Each input support a normally open (NO) or normally closed (NC) sensor switch.



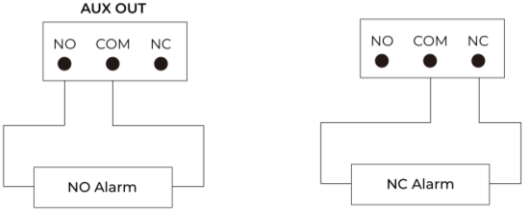
7. Exit Button Interface

The EXIT BUTTON interface supports up to 4 exit buttons.

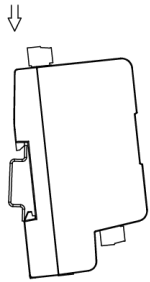


8. Auxiliary Output Interface

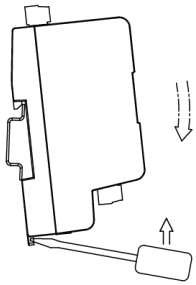
The auxiliary output interfaces provide switching outputs for connecting normally open (NO) or normally closed (NC) alarm devices.



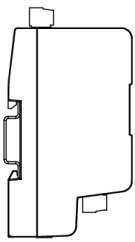
INSTALLATION



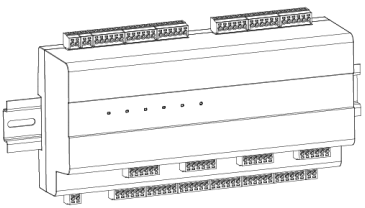
Step1:
Hook the upper clip onto the DIN rail.



Step2:
Lift the spring clip with a flat-head screwdriver and snap the module onto the DIN rail.



Step3:
Installation complete.



TROUBLESHOOTING

The Access Controller cannot start up or power off automatically.

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

The Access Controller did not get IP address.

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

---

The OSDP reader cannot be used.

- Check whether the wiring is correct;
- Check whether OSDP is enabled in the RS485 settings;
- Check whether encryption needs to be enabled;
- If encryption is enabled, check whether the SCBK is entered correctly.

Lock cannot open

- Check lock relay wiring for correct connection.
- Confirm valid user access permission and time schedule.
- Check power supply and hardware status of the lock.

Network failure, cannot access web portal

- Check network cable and RJ45 interface.
- Ensure PC and controller are in the same LAN. Confirm DHCP/IP settings.
- For Wi-Fi-optional model: check Wi-Fi parameters and signal strength.
- Make sure relevant network protocols are not blocked by firewall.

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.

V1.0

EASY & SMART
INTERCOM SOLUTIONS

DNAKE