

Four Door Two-way Access Controller

User Manual

Revision 1.0

Four Door Two-way Access Controller User Manual

Preface

This manual introduces the functions and operations of the access controller. Please read it carefully before using the controller, and keep the manual in a safe place for future reference.

Privacy Notice

As a device user or data controller, you may collect personal data from others, such as their facial images, audio, fingerprints, and license plate numbers. You are required to comply with local privacy protection laws and regulations by implementing measures to protect the legitimate rights and interests of others, including but not limited to the following: providing clear and visible identification to inform individuals of the presence of monitoring areas and offering the necessary contact information.

Safety Instruction

The following signal words may appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which may result in death or serious injury if not avoided.
 WARNING	Indicates a moderate or low potential hazard which may result in minor or moderate injury if not avoided.
 CAUTION	Indicates potential risks that, if not mitigated, may lead to property loss, data loss, performance degradation, or unpredictable outcomes.
 TIPS	Provides ways to help you solve problems or save time.
 NOTE	Provides additional information as a text supplement.

Revision History

Version	Revision Content
V1.0	First release.

About the Manual

- This manual is for reference only. There may be slight differences between the manual and the product.
- We do not accept responsibility for losses caused by operating the product in a manner that does not comply with the manual.
- This manual will be updated in accordance with the latest laws and regulations of the

relevant jurisdictions. For detailed information, please refer to the printed user manual, use our CD, scan the QR code, or visit our official website. This manual is for reference only.

There may be slight differences between the electronic version and the printed version.

- All designs and software are subject to change without prior written notice. Product updates may result in some discrepancies between the actual product and the manual. Please contact customer service for the latest Process and supplementary documentation.
- There may be errors in printing, or deviations in the descriptions of functions, operations, and technical data. In case of any questions or disputes, we reserve the right to make the final interpretation.
- If you are unable to open the manual (PDF format), please upgrade your reader software or try other mainstream reader software.
- All trademarks, registered trademarks, and company names in the manual are the property of their respective owners.
- If you encounter any issues while using the equipment, please visit our website to contact the supplier or customer service.
- In case of any uncertainties or disputes, we reserve the right of final interpretation.

Important Safety Instruction and Warning

Transportation Requirement

Transport, use, and store the access controller under permitted humidity and temperature conditions.

Storage Requirement

Store the access controller under permissible humidity and temperature conditions.

Installation Requirements

- Shut off the circuit breaker before connecting AC power cables.
- Strictly follow to local electrical safety regulations and standards. Ensure that the environmental voltage is stable and meets the power requirements for the access controller.
- Do not connect the access controller to two or more power sources to avoid damage to the access controller.
- Improper use of batteries may result in fire or explosion.
- Please follow the electrical requirements to power the access controller.

AC Power Cable Requirements

- The AC power cable must comply with all local electrical safety codes.
- Only copper conductors are allowed. Minimum cross-section: 0.75 mm² (18 AWG).
Insulation rating: at least 300V and 75°C.
- The cable must contain three wires: Line (brown), Neutral (blue), and Ground (green/yellow).
- The cable must be provided and installed by a qualified electrician.

Four Door Two-way Access Controller User Manual

- Ensure proper grounding of the device. Do not operate the product without a ground connection.
- Personnel working at heights must take all necessary measures to ensure personal safety, including wearing safety helmets and safety harnesses.
- Do not place the access controller in direct sunlight or near heat sources.
- Keep the access controller away from moisture, dust, and smoke.
- Install the access controller on a stable surface to prevent it from falling.
- Install the access controller in a well-ventilated area and do not block its ventilation openings.

Operation Requirements

- Before powering on, ground the device to the protective ground.
- Operate the access controller within the rated input and output power range.
- Use the access controller under permitted humidity and temperature conditions.
- Do not spill or splash liquids onto the access control unit, and ensure that there are no items containing liquids on the access control unit to prevent liquids from entering it.
- Do not disassemble the access controller without professional instruction.
- This product is a professional device.
- This access controller is not suitable for use in areas where children may be present.

Four Door Two-way Access Controller User Manual

Contents

Preface	I	Configuring Anti-passback	18
Introduction.....	1	Configuring Multi-door Interlock.....	19
Hardware Overview	2	Configuring Unlock Methods	19
Dimensions and Appearance.....	2	Configuring Card Settings.....	20
Installation.....	2	Configuring Back-end Comparison.....	20
Components and Wiring.....	3	Configuring Access Card Rule Settings.....	20
Components	3	Access Monitoring	21
Door Control Port Wiring	4	Event information	22
Unlock Button or Door Detector	4	Details	22
Magnetic Lock	4	Configuring System Settings	22
Cable Specification.....	5	Configuring Alarm Linkage.....	22
Web Operations	6	Configuring Alarm Input Channel.....	22
Initialization	6	Configuring Alarm Output Channel	23
Logging In.....	6	Configuring Alarm Settings	24
Resetting the Password.....	6	Account Management.....	24
Home Page	7	Adding Administrators.....	24
User Management	7	Resetting the Password	25
Adding User	7	Adding ONVIF Users	25
Authentication	9	Viewing Online Account.....	26
Passwords	9	Configuring Time Settings	26
Cards.....	9	Network Settings.....	27
Fingerprints	10	Configuring TCP/IP.....	27
Fingerprint Registration Notes	10	Configuring Port	27
Fingers Recommended	10	Configuring Basic Service	28
How to Scan Your Fingerprint	10	Configuring Cloud Service	29
Bluetooth Cards	11	System Information	29
Configuring Access Rules	13	Viewing Version Information	29
Configuring Weekly Schedule	13	Viewing Legal Information	29
Configuring Holiday Schedule	14	Maintenance Center	29
Configuring Door Parameters.....	14	System Capacity	29
Configuring Advanced Settings	17	Viewing Logs.....	29
Configuring First-person Unlock	17	System Logs.....	29
		Unlock Records	30
		Alarm Logs.....	30
		Maintenance Management	30

Four Door Two-way Access Controller User Manual

- Exporting and Importing Configuration Files 30
- Configuring the Card Reader 31
- Configuring the Fingerprint Similarity Threshold 31
- Restoring Default Settings 31
- Restarting the controller 32
- Updating the System 32
 - Controller Update 32
 - File Update..... 32
 - Online Update 32
 - Card Reader Update..... 32
- Advanced Maintenance..... 33
 - Exporting..... 33
 - Packet Capture..... 33
 - Network Test 33
- Security Settings 33
 - Configuring System Service 33
- Attack Defense 34
 - Configuring Firewall..... 34
 - Configuring Account Lockout 34
 - Configuring Anti-DoS Attack..... 35
- Installing Device Certificate..... 35
 - Creating Certificate 35
 - Applying for and Importing CA Certificate..... 36
 - Installing Existing Certificate 37
 - Installing the Trusted CA Certificate 37
- Cybersecurity Recommendations..... 38

Four Door Two-way Access Controller User Manual

Introduction

The flexible and convenient access controller is equipped with a user-friendly system that allows you to manage access permissions on the web page via the controller's IP address, and it is compatible with various card readers. Functionally, it supports first-person unlock, anti-passback and multi-person unlock. It is widely applicable in communities, commercial complexes, group properties, and office buildings.

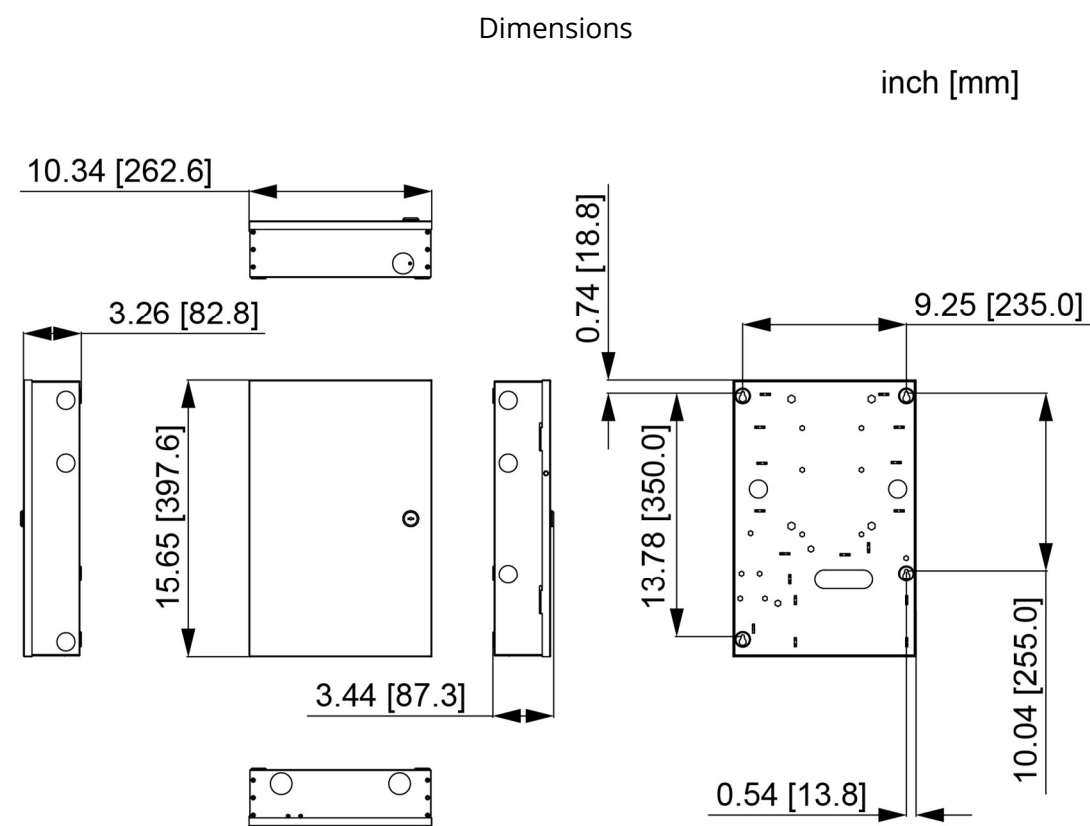


The web page is subject to periodic updates; please refer to the actual web page for the latest information.

Four Door Two-way Access Controller User Manual

Hardware Overview

Dimensions and Appearance



Panel



Panel description

No.	Description
1	Cable entry knockout
2	Door lock

Installation

The controller supports two installation methods: concealed wiring and exposed wiring.

Process

1. Mark the wall screw hole positions per the controller's screw holes, drill 4 holes, then tap the wall anchors into the holes until flush.
2. Install 4 Phillips screws into the wall anchors, leaving at least 1.5 mm gap between each screw head and anchor.
3. Remove the metal sheet according to the actual wiring situation.
4. Wire the controller.

Four Door Two-way Access Controller User Manual

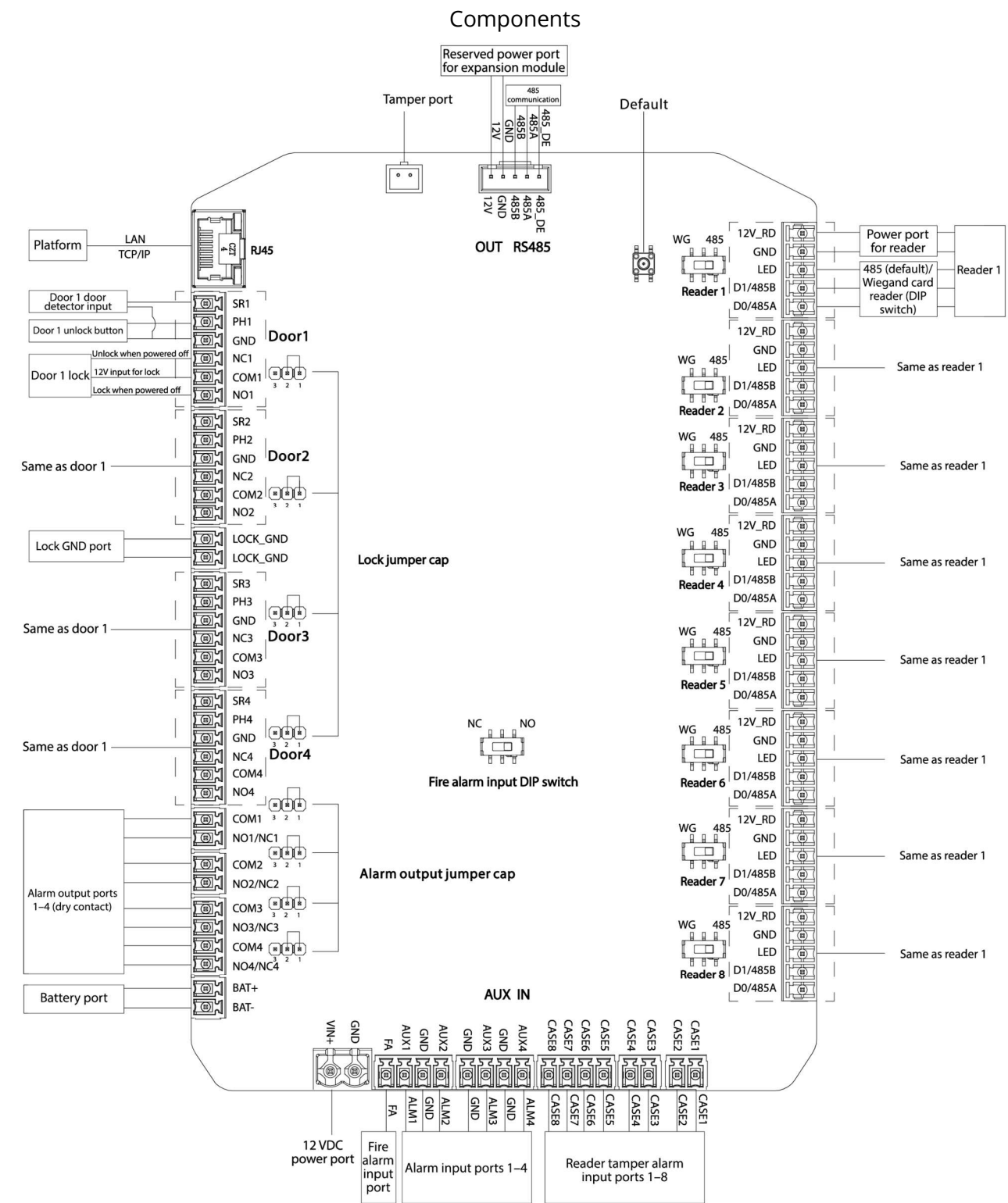


Please shut off the circuit breaker before connecting AC power cables.

- For concealed wiring installation
 - Feed the cable through the pre-punched hole(s).
 - Hang the device onto the Phillips head screws.
 - Connect AC power cables and all other cables to the corresponding internal interfaces. For more details, please refer to "**Components and Wiring**".
 - For exposed wiring installation
 - Hang the device onto the Phillips head screws.
 - Feed the cables through the pre-punched hole(s).
 - Feed the cables through the pre-punched hole(s). Then connect AC power cables and all other cables to the corresponding internal interfaces. For more details, please refer to "**Components and Wiring**".
5. Turn on the circuit breaker after wiring is completed, then press the "I" side of the switch to power on the device.
6. Use the key to lock the cover of the controller.

Components and Wiring

Components



Components description

Component	Description
Tamper port	Tamper alarm use.
OUT	Power output port. The OUT port adjacent to the RS-485 port supports a maximum current of 500 mA

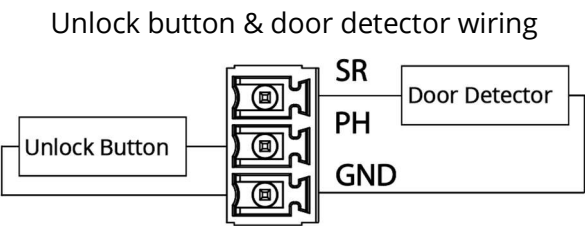
Four Door Two-way Access Controller User Manual

Component	Description
RS485	Connect to external alarm module to expand 8-channel alarm input or 8-channel alarm output.
Default	Restore the controller to default settings. NOTE This operation can only be performed within 5 minutes after the controller is powered on. - Factory Defaults: Press and hold the Default button for more than 5 seconds, and the controller beeps for 3 seconds. During restoration, the controller beeps continuously. When the beeping stops, the controller is restored to factory settings and restarts automatically. - Restore to Default (Keep User Info and Logs): Short press the Default button, and the controller beeps for 0.3 seconds. During restoration, the controller beeps continuously. When the beeping stops, the controller is restored to default settings and restarts automatically.
Reader 1 – Reader 8	Access reader port. - The 8 ports use the same connection method. - One access reader port can only connect to the access readers of the same type. - The reader supports a 12 VDC power supply with 1 A current. - The DIP switch defaults to the 485 position. To connect to an external Wiegand access reader, set the DIP switch to the WG position.
AUX IN	Alarm input port. Connects to smoke detector and IR detector.
12 VDC power port	Power input port. Converts input power to 12 VDC.
Battery port	Connects to the battery.
Alarm output jumper cap	The alarm output jumper cap is connected to ports 1 and 2 by default. - Connect 1 and 2: NO acts as the dry contact output terminal, for normally open alarm devices. - Connect 2 and 3: NC acts as the dry contact output terminal, for normally closed alarm devices.
Fire alarm input DIP switch	Use DIP switches to switch between normally open and normally closed alarm device connections.

Component	Description
Door1 – Door4	Door control port. The 4 ports use the same connection method. - By default, the door lock jumper cap connects ports 1 and 2. - Connecting ports 1 and 2: COM port is unpowered. The lock uses an external power supply. COM acts as the common terminal. - Connecting ports 2 and 3: COM port functions as a 12 V (1 A) output terminal, supplying power to the lock. NOTE Wire according to the actual lock type. For more details about wiring, please refer to “Door Control Port Wiring”.
RJ45	Network port.

Door Control Port Wiring

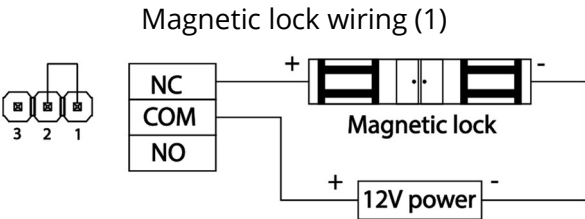
Unlock Button or Door Detector



Magnetic Lock

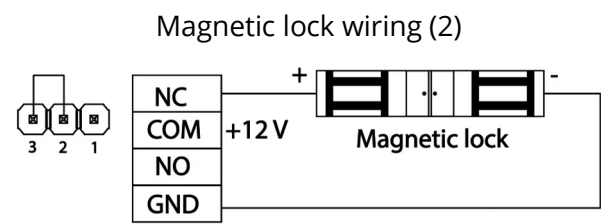
The wiring method should be selected based on the type of lock. Magnetic locks can be powered either via the access controller (using its COM port) or an external power supply.

- Powered by External Power Supply



- Powered by Controller
Connecting 2 and 3 means COM serves as a 12 VDC output terminal.

Four Door Two-way Access Controller User Manual



Cable Specification

The access controller provides power to the access reader and lock.

Cable specification description

Device Connection	Recommended Cable	Max Power Supply Distance
Controller to Reader	RVV 2 × 1.0, RVV 4 × 1.0 or Cat5e - RVV 0.5: ≤ 39.0 Ω/km - RVV 1.0: ≤ 19.5 Ω/km - RVV 1.5: ≤ 13.3 Ω/km - Cat5e: ≤ 9 Ω/100 m	- RVV 0.5 - RS-485: < 200 m - Wiegand: < 120 m - Cat5e - RS-485: < 120 m - Wiegand: < 50 m

Device Connection	Recommended Cable	Max Power Supply Distance
Controller to Lock		- RVV 0.5 - Magnetic Lock (280 kg) 1 Door: ≤ 60 m 2 Doors: ≤ 25 m - Magnetic Lock (500 kg) 1 Door: ≤ 50 m 2 Doors: ≤ 20 m - RVV 1.0 - Magnetic Lock (280 kg) 1 Door: ≤ 100 m 2 Doors: ≤ 40 m - Magnetic Lock (500 kg) 1 Door: ≤ 100 m 2 Doors: ≤ 40 m - RVV 1.5 - Magnetic Lock (280 kg) 1 Door: ≤ 140 m 2 Doors: ≤ 80 m - Magnetic Lock (500 kg) 1 Door: ≤ 140 m 2 Doors: ≤ 60 m
- Wiring distance depends on power supply voltage and cable specifications. Ensure voltage at the device meets the minimum operating requirements for the controller, reader, and lock. Do not use the same wire for Controller-to-Reader and Controller-to-Lock connections. - If the access reader is powered by the controller, use a reader with max current ≤ 200 mA. The reader must support wide voltage operation and operate down to 9 V minimum. - If the lock is powered by the controller, use a lock with max current ≤ 1,200 mA. The lock must support wide voltage operation and operate down to 10 V minimum. - If using Cat5e for power, distribute unused wires evenly between power lines to reduce voltage loss. - The data above is measured under laboratory conditions and may differ from actual field performance. For reference only.		

Four Door Two-way Access Controller User Manual

Web Operations

On the web page, you can configure and operate the controller, including configuring network parameters, access parameters, and other operations. You can also maintain and update the controller.

Initialization

Initialize the controller after your first login to the web page or after restoring it to factory default settings.

Precondition

Ensure that the computer used to log in to the web page is on the same LAN as the controller.

Process

1. Open the browser and visit the IP address of the controller (the default IP address is 192.168.1.101).



NOTE

We recommend that you use the latest version of the Chrome or Firefox browser.

2. Select a language.
3. Configure the time zone.
4. Set the password and email address according to the screen instructions.



NOTE

- The password must consist of 8 to 32 non-empty characters and must include at least two of the following types of characters: uppercase letters, lowercase letters, numbers, and special characters (excluding ' ' ; : &). Please set a high-security password according to the password strength prompts.
- Please keep the password safe after initialization and change it regularly to enhance security.
- To reset your password, an email address is required. You will receive a security code via this email address.

5. (Optional) Select **Auto Check for Updates**.
After you select the function, the system automatically checks for available updates. It notifies you when a new version is available.
6. Click **Completed** to finish the initialization process.

Logging In

Process

1. Open the browser and visit the IP address of the controller, and press the Enter key.
2. Enter the username and password on the login page.



NOTE

- If you forget the administrator login password, click **Forgot password?**.
- The default administrator name is admin, and the password is the one you set during initialization. We recommend that you regularly change the administrator password to enhance the security.

3. Click **Login**.

Resetting the Password

If you forget the admin password, reset it using the linked email address.

Process

1. Click **Forgot password?** on the login page.
2. Read the on-screen prompt carefully, then click **OK**.
3. Scan the QR code. You will receive a security code.



NOTE

- Scanning the same QR code generates up to two security codes.
- If the security code expires, refresh the QR code and scan again.
- After scanning the QR code, you will receive a security code via your linked email. Use it within 24 hours. Otherwise, it expires.
- Entering the wrong security code 5 times consecutively freezes the admin account for 5 minutes.

4. Enter the security code.
5. Click **Next**.
6. Reset and confirm the password.

Four Door Two-way Access Controller User Manual

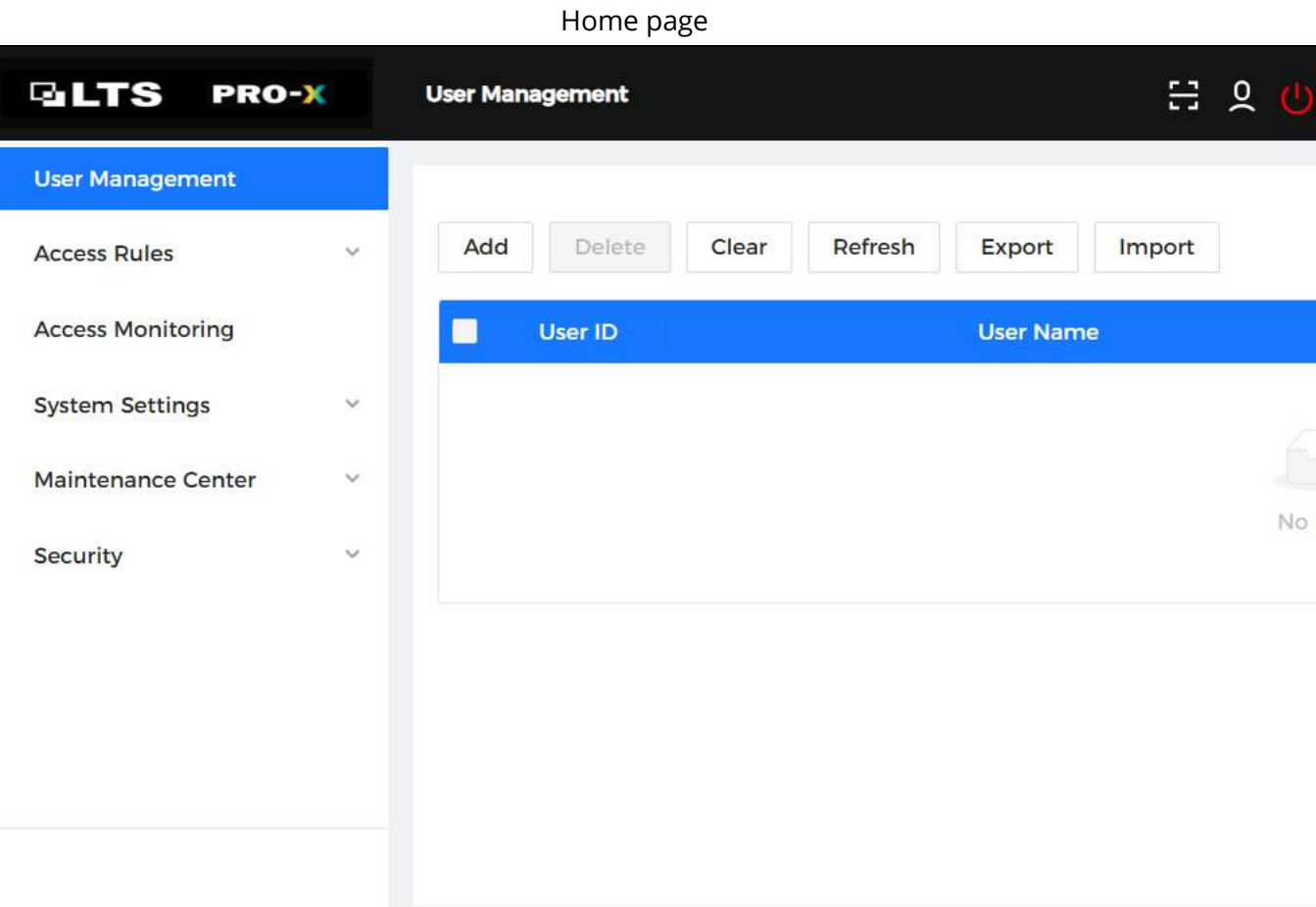
 NOTE

The password must consist of 8 to 32 non-empty characters and must include at least two of the following types of characters: uppercase letters, lowercase letters, numbers, and special characters (excluding ' " ; : &).

7. Click **OK**.

Home Page

After you successfully log in, the home page of the controller will be displayed.



Home page description

No.	Description
1	: Display the username of the currently logged-in user. : Log out or restart the controller. : Product QR-code

User Management

Adding User

Process

1. Select **User Management** on the home page, then click **Add**.
2. Configure user information.

Four Door Two-way Access Controller User Manual

Add user

Basic Info

User ID

1

User Name

Valid from05-12-2026 12:00:00 AM

Valid to12-31-2037 11:59:59 PM

User TypeGeneral

* Times UsedUnlimited

mail

Authentication

▼ Password

Not Added

Add

> Card

Not Added

> Fingerprint

Not Added

> Bluetooth Card

Not Added

Permission

type

Use the Same Time Template for All Doors

Door Permissions

1

2

3

4

Weekly Schedule

255-Full Day x

* Holiday Schedule

255-No Plan x

Add

Add More

Cancel

Parameters description

Parameter		Description
Basic Info	User ID	The User ID functions like an employee ID; it can consist of numbers, letters, or a combination of both, with a maximum length of 30 characters.
	User Name	The name can contain up to 32 characters, including numbers, symbols, and letters.
	Valid from	Set the period that the access permissions of the person are effective.
	Valid to	

Parameter		Description	
	User Type	The user types. • General: General users can unlock the door. • VIP: If the door is in "Normal" status, VIP users can open it at any time, regardless of other rules. • Guest: Guests can unlock the door within the specified time or the specified number of times. Once the specified time expires or the number of unlocks is exhausted, they will no longer be able to unlock the door. • Staff: The permissions of staff users will be recognized, but they do not have the authority to unlock the door. • Blocklist: When users in the blocklist unlock the door, service personnel will receive a notification. • Manager: Manager users have the highest privileges, which are not affected by the unlock mode or door status. • Other: When they unlock the door, the door will remain unlocked for 5 seconds.	
		Times Used	Set an unlock limit for guest users. After the unlock times run out, they cannot unlock the door.
		Email	The email address must be the same as the one used to register for Pro-X Next App.
	Authentication	Password Card Fingerprint Bluetooth Card	For more details, please refer to " Authentication ".
Permission	Type		• Use the Same Time Template for All Doors: Configure the same weekly schedule and holiday plan for all the channels. • Use Different Time Templates for Different Doors: Configure different weekly schedule and holiday for different channels.
		Door Permissions	The number corresponds to a specific door (e.g., 1 refers to Door 1). Select a door to assign its access permissions.
		Weekly Schedule	People can unlock the door during the defined time period.
		Holiday Schedule	People can unlock the door during the defined holiday. There is no holiday by default.

3. Click **Add**.

8

Four Door Two-way Access Controller User Manual

Related Operations

- Import user information: Click **Export**, and download the template and enter user information in it. Place face images and the template in the same file path, then click **Import** to import the folder.



NOTE

Up to 10,000 users can be imported at a time.

- Clear: Clear all users.
- Refresh: Refresh the user list.
-  : Search by user name or user ID.

Authentication

Passwords

Add a password for users so that they can gain access by entering the password.

The duress password is the unlock password + 1. For example, if the user password is 12345, the duress password will be 12346. A duress alarm will be triggered when a duress password is used to unlock the door.

Process

1. Click **Add**.
2. Enter the password and confirm the password.
The maximum length of the password is 8 digits.
3. Click **OK**.



NOTE

- If PIN code authentication is not enabled, you can unlock the door by entering the unlock password in the format of **user ID#password#**. For example, if the user ID is 123 and the password you set is 12345, you must enter 123#12345# to unlock the door. For more details about PIN code authentication, please refer to "**Configuring Unlock Methods**".
- If PIN code authentication is enabled, you can unlock the door by entering the unlock password in the format of **password#**. For example, if the user ID is 123 and the password you set is 12345, you must enter **12345#** to unlock the door.

Cards

Add IC cards or DESFire cards to users to enable card swipe access. A user can register up to 5

cards.

Process

Collect the card information through the external devices or enter the card number manually.

- Enter the card number manually.
 1. Click **Add**.
 2. Enter the card number, then click **Add**.
- Read the card number automatically through the enrollment readers (IC card).
 1. Click **Add**, then go to **Modify > Enrollment Reader** to select **IC Card** that is connected to the access controller.
 2. Swipe cards on the enrollment reader, then click **Add**.
A 60-second countdown is displayed to remind you to swipe the card. The system reads the card number automatically. If the countdown times out, click **Read Card** again to start a new countdown.
 3. Click **Add**.
- Read the number automatically through the enrollment readers (DESFire card).
 1. Click **Add**, then go to **Modify > Enrollment Reader** to select **DESFire Card** that is connected to the access controller.
 2. Place the card on the enrollment reader, then click **Read Card**.
If the DESFire card has been written with the card number, it will be read and displayed here. If the card is empty, then the card number needs to be written first. The card number will be automatically generated on the computer, and be written to the card.
 3. Click **Add**.
- Read the card number automatically through the card reader connected to the controller.
 1. Click **Add**, then go to **Modify > Device** to select a card reader connected to the access controller.
 2. Swipe the card on the selected card reader, then click **Add**.
A 60-second countdown is displayed to remind you to swipe the card. The system reads the card number automatically. If the countdown times out, click **Read Card** again to start a new countdown.
 3. Click **Add**.

You can enable the **Duress Card** function. An alarm will be triggered if a duress card is used to unlock the door.

- : Set duress card.
- : Change card number.
- : Delete the added card.



NOTE

One user can only set one duress card.

Four Door Two-way Access Controller User Manual

Fingerprints

Background Information

- A user can register up to 3 fingerprints. One fingerprint can be set as the duress fingerprint, which triggers an alarm when used to unlock the door.
- Fingerprints can be enrolled via the enrollment reader connected to the computer or the external card reader connected to the access controller.

Process

1. Click **Add**, then go to **Modify > Enrollment Reader** to select an enrollment reader or go to **Modify > Device** to select the card reader that is connected to the access controller.
2. Press finger on the scanner according to the on-screen instructions.
3. Click **Add**.

NOTE

- We do not recommend you set the first fingerprint as the duress fingerprint.
- One user can only set one duress fingerprint.

Fingerprint Registration Notes

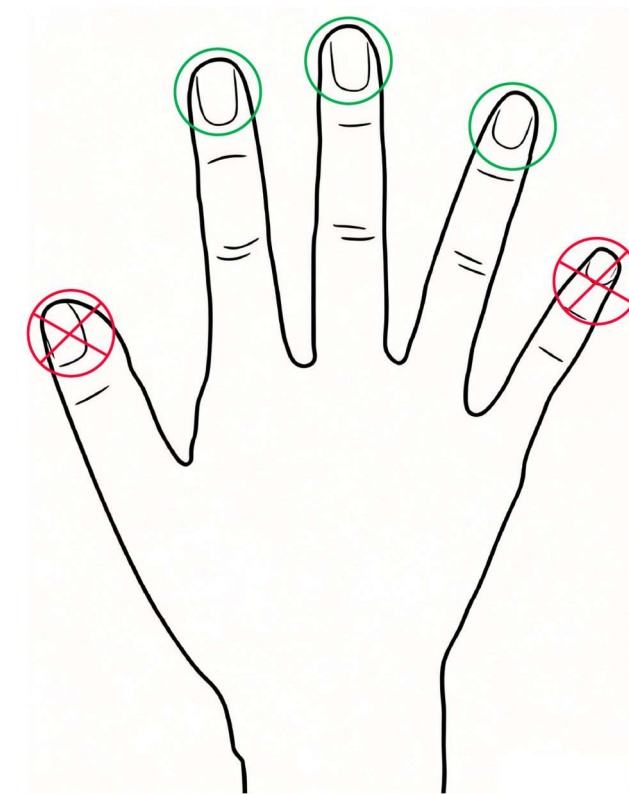
When you register the fingerprint, pay attention to the following points:

- Make sure that your fingers and the scanner surface are clean and dry.
- Press your finger on the center of the fingerprint scanner.
- Do not put the fingerprint sensor in a place with intense light, high temperature, and high humidity.
- If your fingerprints are unclear, use other unlocking methods.

Fingers Recommended

Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

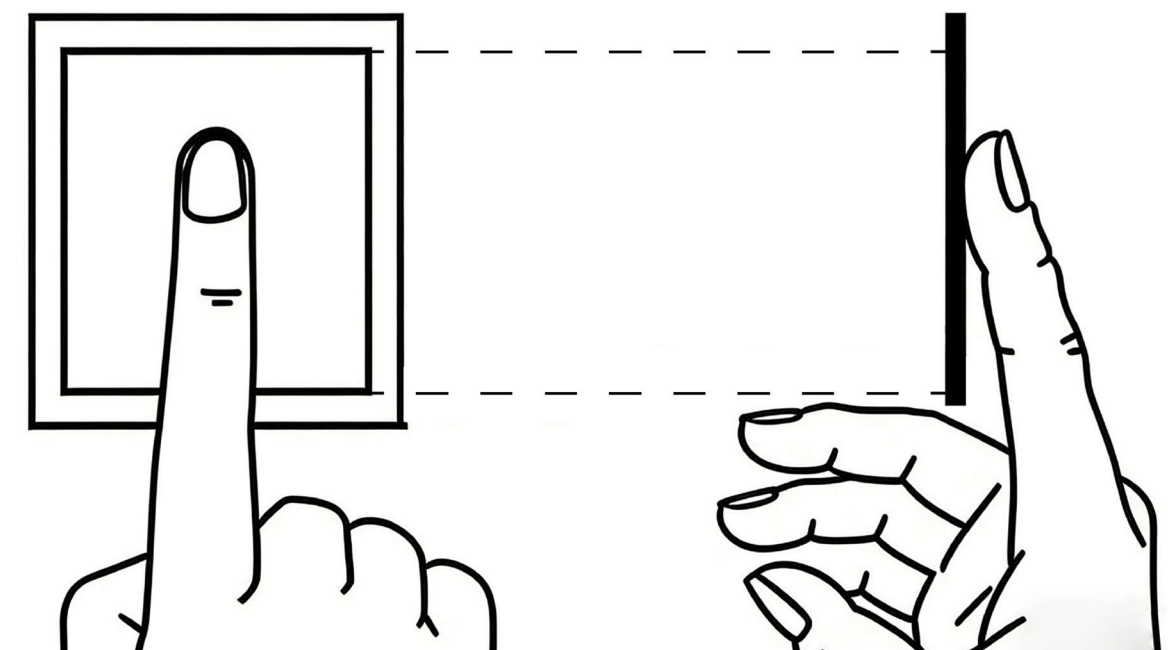
Recommended fingers



How to Scan Your Fingerprint

Place the pad of your finger flat and centered on the fingerprint scanner, apply gentle, steady pressure, and hold it still until the scan is confirmed.

Correct placement



Four Door Two-way Access Controller User Manual

Bluetooth Cards

Add a Bluetooth card for users so that they can gain access through the Bluetooth card.

Precondition

- The Bluetooth unlocking function has been enabled. For more details, please refer to **"Configuring Door Parameters"**.
- The access controller has been added to Pro-X Next App. For more details, please refer to **"Configuring Cloud Service"**.
- The user has been added to the access controller platform.
- General users, such as company employees, have installed and signed up for Pro-X Next App with their email.



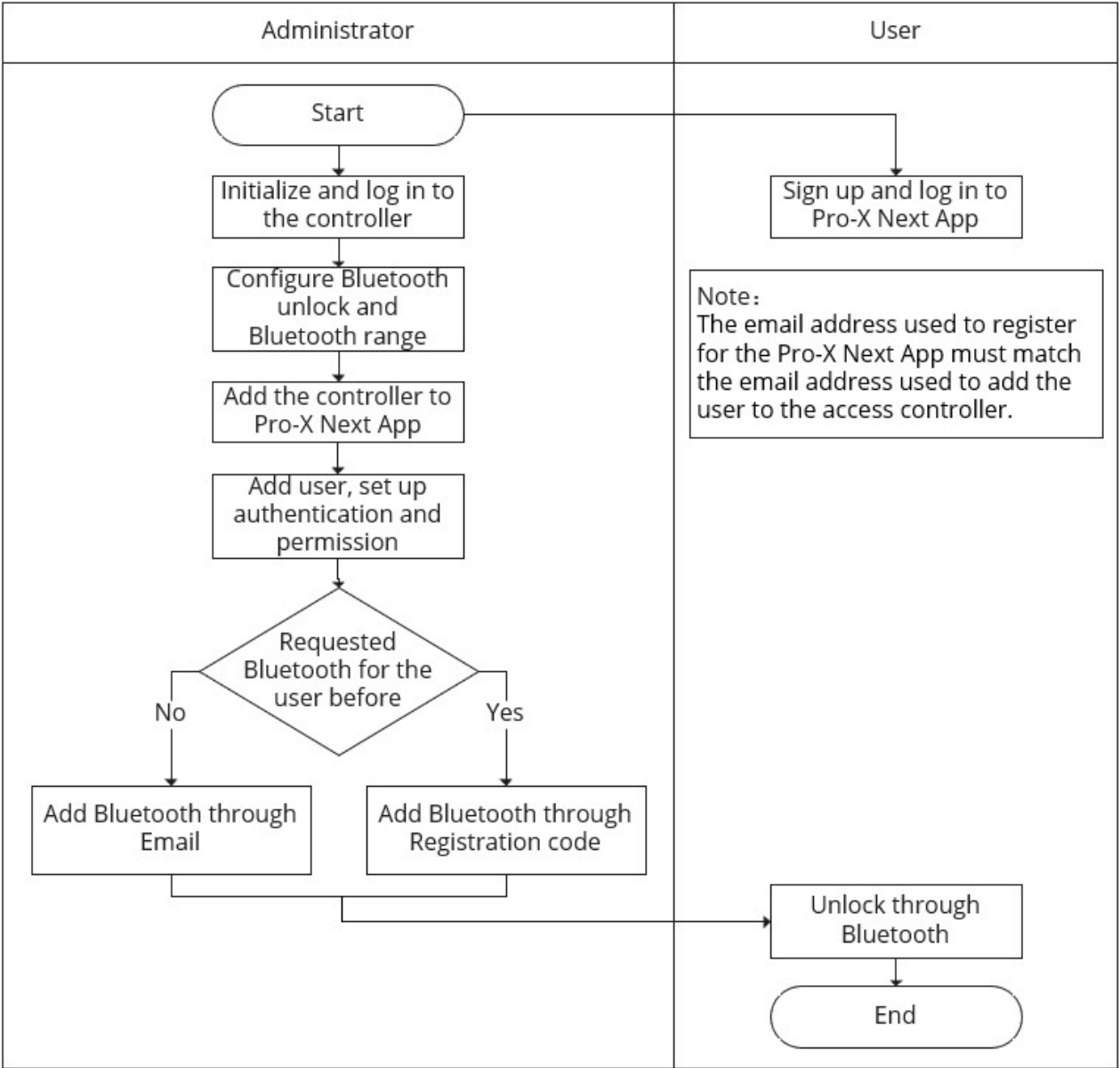
NOTE

The email address used to register for the Pro-X Next App must match the email address used to add the user to the access controller.

Background Information

Please refer to the flowchart for configuring Bluetooth unlocking. Administrators and regular users need to perform different actions to complete the process. Regular users, such as company employees, only need to register and log in to Pro-X Next App using their email to unlock the door with the Bluetooth card sent to them.

Flowchart for configuring Bluetooth unlock

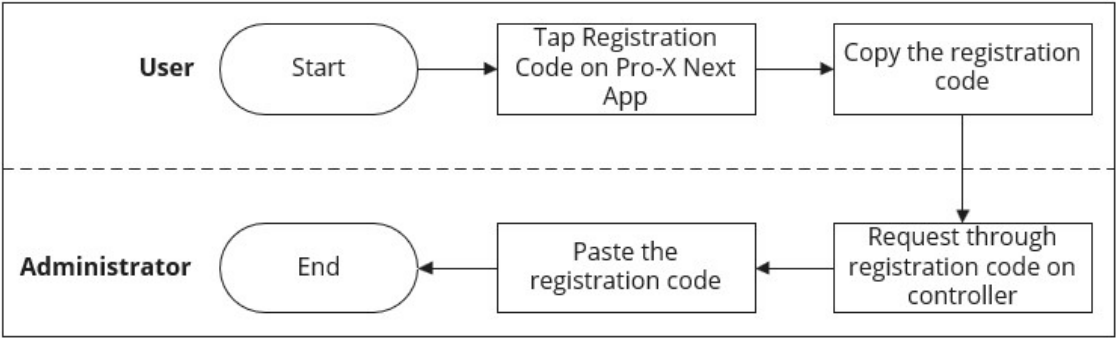


Process

1. Click Bluetooth Card in the Authentication section.
There are two methods to add a Bluetooth card.
 - Request through email one by one: Click **Request through Email**.
Bluetooth cards will be generated automatically. Each user can generate a maximum of 5 cards.
 - If you have previously requested a Bluetooth card for the user, you can add the Bluetooth card by registering the code.

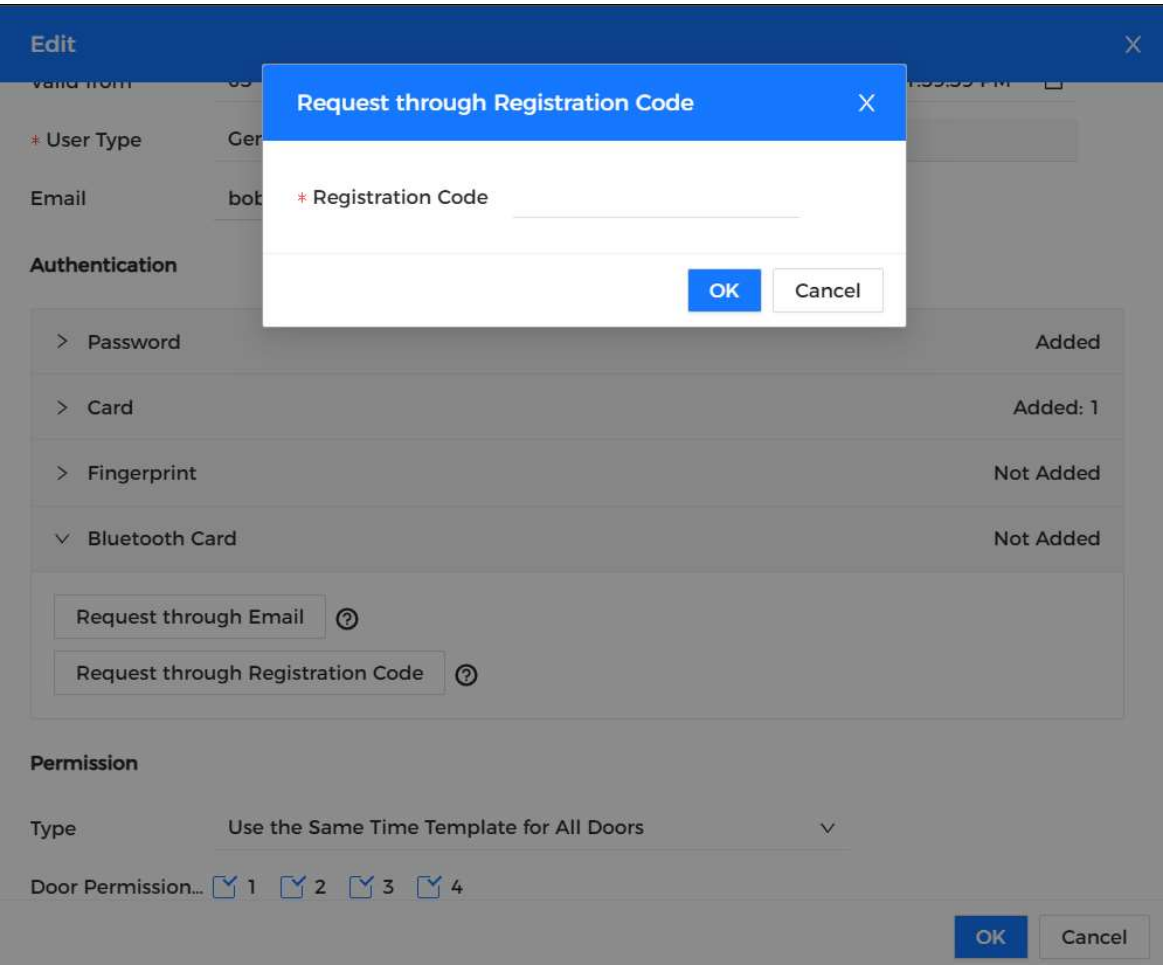
Four Door Two-way Access Controller User Manual

Flowchart for adding Bluetooth card via registration code



- 1) Tap **Registration Code** of a Bluetooth card on Pro-X Next App.
The registration code is automatically generated by Pro-X Next App.
- 2) Copy the registration code.
- 3) Click **Request through Registration Code** in the **Bluetooth Card** section, paste the registration code, then click **OK**.

Request through registration code



- 4) Click **OK** and the Bluetooth card will be added.
2. Click **OK**.

Result

After users register and log in to Pro-X Next App using their email address, they can open Pro-X Next App and unlock the door using the Bluetooth card. For more details, please refer to the Pro-X Next App user manual.

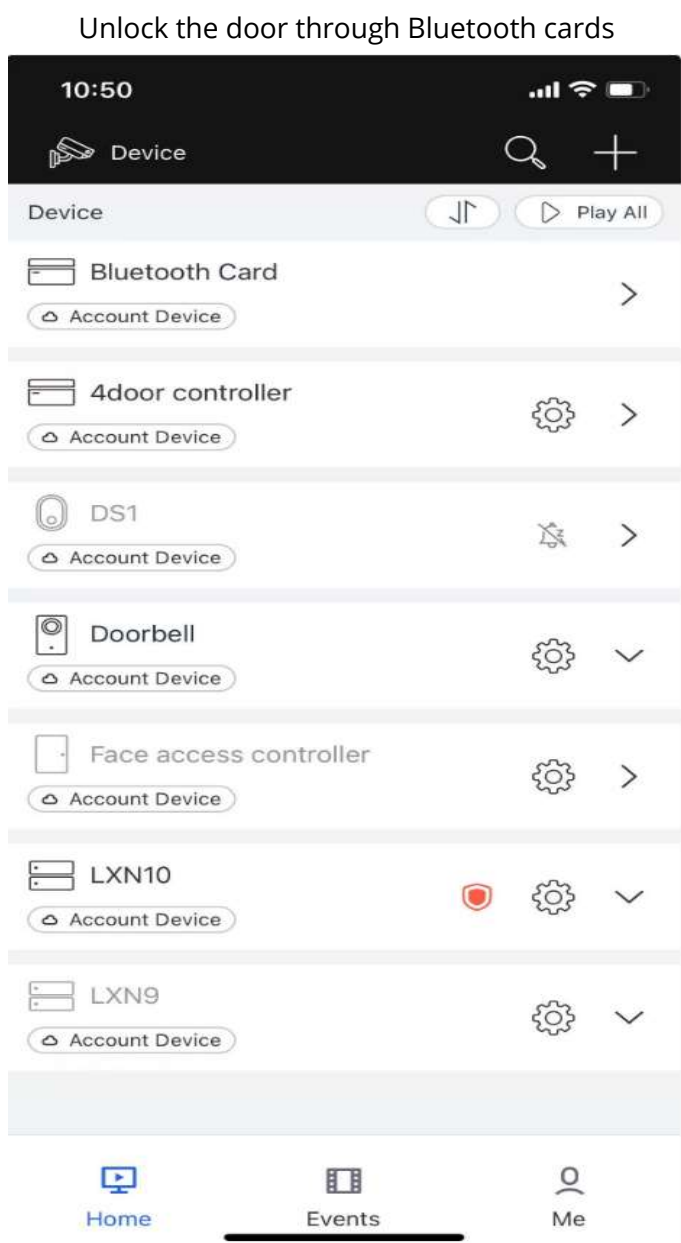
- **Auto Unlock:** The door will automatically unlock when you are within the defined Bluetooth range, allowing the Bluetooth card to transmit signals to the reader.

CAUTION

In auto unlock mode, the Bluetooth card might continuously unlock the door when you are within the Bluetooth range for a long time until a failure occurs. Please turn off Bluetooth on the phone and then turn it on again.

- **Shake to unlock:** When you shake your phone, the door will unlock, allowing the Bluetooth card to transmit a signal to the reader.

Four Door Two-way Access Controller User Manual



Related Operations

Users can manage Bluetooth cards on Pro-X Next App.

- **Move to the Top:** If multiple Bluetooth cards have been added, you can move the currently used card to the top.
- **Rename:** Rename the Bluetooth card.
- **Delete:** Delete the Bluetooth card.

Configuring Access Rules

Configuring Weekly Schedule

You can configure up to 128 weekly schedule periods (No. 0 to No. 127); each period requires setting door access schedules for the entire week, and door access is only permitted during the scheduled time.

Process

1. Log in to the web page.
2. Go to **Access Rules > Weekly Schedule**.
3. Click **+**.
 - 1) Configure the plan name and the plan number.
 - 2) Drag the time slider to configure time for each day.
 - 3) (Optional) Click Copy to copy the configuration to the rest of days.

Configure weekly schedule

Edit

Name

Weekly Schedule 1

No.

0

Time Plan

0123456789101112131415161718192021222324

Sun

Copy

Mon

Copy

Tue

Copy

Wed

Copy

Thu

Copy

Fri

Copy

Sat

Copy

4. Click **Apply**.

Four Door Two-way Access Controller User Manual

Configuring Holiday Schedule

You can configure up to 128 holiday groups (No. 0 to No. 127); each group allows adding up to 16 holidays, then assign the configured holiday groups to a holiday plan, and door access is only permitted during the time defined in the holiday plan.

Process

1. Log in to the web page.
2. Go to **Access Rules > Holiday Schedule**.
3. Click **+**.
 - 1) Configure the plan name and the plan number.

Add a holiday schedule

Edit

Details

* Name

Holiday Schedule 1

No.

0

Time Plan

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Holiday List

Add

No.	Holiday Name	Start Time	End Time	Operation
No Data				

Apply

Cancel

- 2) Drag the time slider to configure time for the holiday.
You can configure up to 4 periods.
- 3) Click Add, configure the name and the period, then click OK to add a holiday to the holiday list.

Add a holiday

Add

* Holiday Name

* Period

Start date

→

End date

OK

Cancel

- 4) Click **OK**.
4. Click **Apply**.

Related Operations

Copy the configured holiday to other holiday schedules.

Holiday list

Holiday List

Add

No.	Holiday Name	Start Time	End Time	Operation
1	A	05-03-2026	06-09-2026	

1. Click , select the added holiday schedule, then click **OK**.

Copy the holiday

Copy to

Holiday Sche...

Select All

Holiday Schedule 1

OK

Cancel

2. Click **Apply**.

Configuring Door Parameters

Four Door Two-way Access Controller User Manual

Configure door status, unlock methods and other door parameters.

Process

1. Log in to the web page.
2. Go to **Access Rules > Door Parameters**.
3. Configure basic parameters for the access rules in the **Basic Settings** section.

Basic parameters

Basic Settings

Name

Door1

Door Status

☒ Normal ☐ Always Locked ☐ Always Unlocked

Keep Door Unlocked for

Weekly Schedule Disabled ▾

Holiday Schedule Disabled ▾

Keep Door Locked for

Weekly Schedule Disabled ▾

Holiday Schedule Disabled ▾

Holiday Plan Authentication

Disabled ▾

Admin Unlock Password

☐

Basic parameters description

Parameter	Description
Name	The door name.
Door Status	Set the door status. • Normal: The door unlocks and locks as per your settings. • Always Locked: The door stays locked at all times. • Always Unlocked: The door stays unlocked at all times.
Keep Door Unlocked for	When select Normal, you can choose a time template from the drop-down list. The door will stay open or closed during the defined time period. Note that you must configure the weekly schedule and holiday schedule in advance. NOTE • If the normally open period conflicts with the normally closed period, the normally open period takes priority. • If a period conflicts with the holiday schedule, the holiday schedule takes priority.
Keep Door Locked for	
Holiday Plan Authentication	Authorized access is permitted for normally closed doors during the defined holiday plan.

Parameter	Description
Admin Unlock Password	Once enabled, you can unlock the door by entering the admin password directly. No need to input a user ID. This works regardless of user type, unlock method, weekly schedule, holiday plan, or anti-passback permissions. NOTE The admin password cannot unlock the door only when the door is in normally closed status.

4. In **Unlock Settings**, configure unlock method and corresponding parameters.

- Combination unlock
 - 1) Select **Combination Unlock** from the **Unlock Method** list.
 - 2) Select **Or** or **And**.
 - **Or**: Use one of the selected unlock methods to open the door.
 - **And**: Use all the selected unlock methods to open the door.
 - 3) Select unlock methods, then configure other parameters.

Unlock settings

Unlock Settings

Unlock Method

Combination Unlock ▾

Combination Method

☒ Or ☐ And

Unlock Method (Multi-select)

☒ Card ☒ Fingerprint ☒ Password

Door Unlocked Duration

3.0

s (0.2-600)

Unlock Timeout

60

s (1-9999)

Remote Verification

☐

Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	Supports unlocking through card, fingerprint, password or Bluetooth card. All unlock methods are enabled by default.

Four Door Two-way Access Controller User Manual

Parameter	Description
Bluetooth Range	The Bluetooth card must maintain a certain distance from the access control device in order to exchange data and unlock the door. Below is the most suitable range of distances. • Short (<0.2m): The Bluetooth unlock range is less than 0.66 ft (0.2 meters). • (Default) Medium (<2m): The Bluetooth unlock range is less than 6.56 ft (2 meters). • Long (<10m): The Bluetooth unlock range is less than 32.81 ft (10 meters). ⚠ CAUTION The Bluetooth unlocking range may vary depending on the mobile phone model and the environment.
Door Unlocked Duration	Once a person is granted access, the door will remain unlocked to allow them to pass through, with a duration ranging from 0.2 seconds to 600 seconds.
Unlock Timeout	When the door remains unlocked for longer than the set time, a timeout alarm will be triggered.
Remote Verification	Open the door remotely.

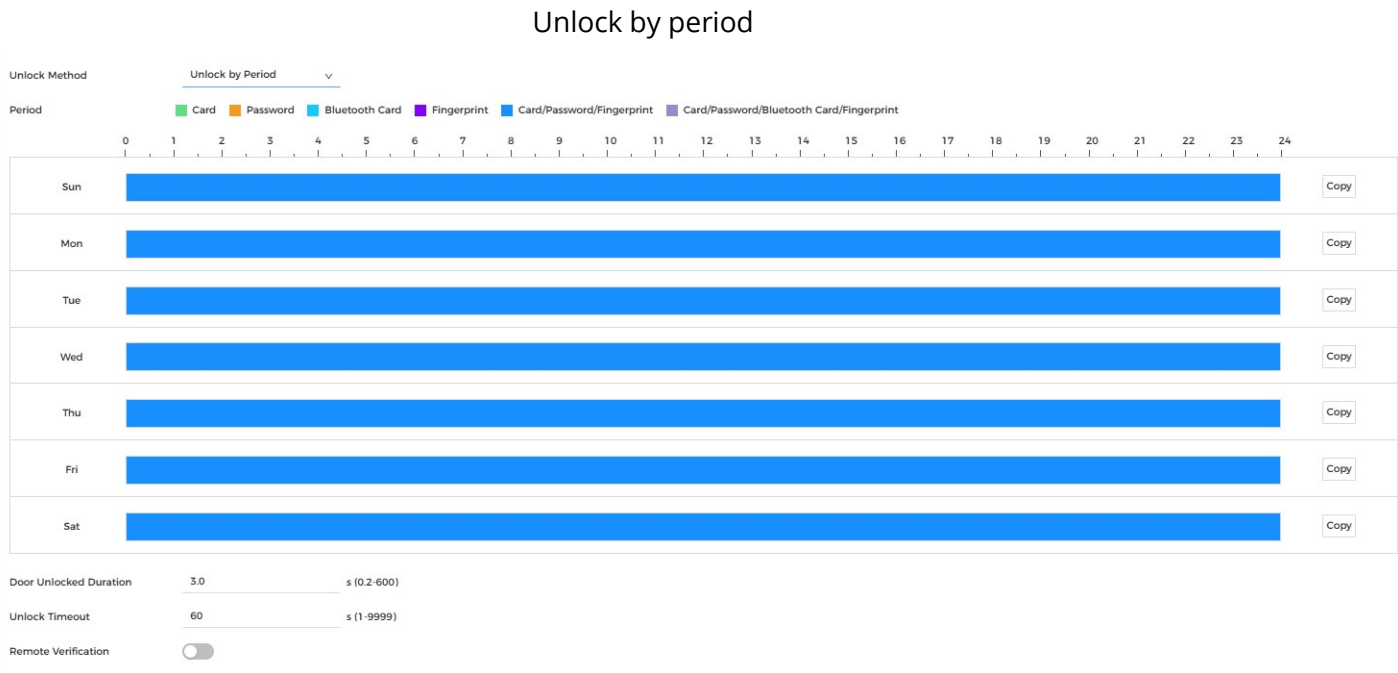
- Unlock by period
 - 1) Select Unlock by Period in the Unlock Method list.
 - 2) Drag the slider to adjust time period for each day.



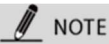
NOTE

You can also click **Copy** to apply the configured time period to other days.

- 3) Select the combination method and the unlock method for the time period.



- Unlock by multiple users.
 - 1) Select Unlock by Multiple Users in the Unlock Method list.
 - 2) Click Add to add groups.
 - 3) Select unlock method, valid number and users.
 - If only one group is added, the door unlocks only when the number of access-granting members in the group matches the defined valid number.
 - If more than one group is added, the door unlocks only when the number of access-granting members in each group matches the defined valid number.
 - 4) Configure the verification of multi-person unlock timeout duration.



NOTE

- Maximum 4 groups can be added. The valid number refers to the count of group members required to verify their identity on the controller for door unlock. For example, if a group's valid number is set to 2, any 2 members of the group must verify their identity to unlock the door.
- If first-card unlock is configured and the first-card user belongs to the user group, the first-card user must verify their identity first.

5. Configure alarm parameters in the **Alarm Settings** section.

Four Door Two-way Access Controller User Manual

Alarm settings

Alarm Settings

Door Sensor

Normally Open Normally Closed

Intrusion Alarm

Link Local Buzzer

Duration

 15

s (1-1800)

Unlock Timeout Alarm

Link Local Buzzer

Controller Buzzer Mode

Custom Time

Duration

 15

s (1-1800)

Link Buzzer of Card Reader Bou...

Card Reader Buzzer Mode

Custom Time

Duration

 15

s (1-255)

Duress Alarm

Description of alarm parameters

Parameter	Description
Door Sensor	When the door sensor is wired to the device, an alarm triggers if the door is opened or closed abnormally. The door sensor has two types: Normally Open and Normally Closed . • Normally Open: The circuit is open when the door is closed. • Normally Closed: The circuit is shorted when the door is closed.
Intrusion Alarm	When both the door sensor and intrusion alarm are enabled, an intrusion alarm triggers and lasts for a defined duration if the door is opened abnormally.

Parameter	Description
Unlock Timeout Alarm	When both the door sensor and unlock timeout alarm are enabled, a door timeout alarm triggers and lasts for a defined duration if the door remains unlocked beyond the set timeout. • Link Local Buzzer: When the alarm triggers, the controller beeps. You can configure the buzzing mode and duration. • Link Buzzer of Card Reader Bound to This Channel: When the alarm triggers, the RS-485 card reader bound to this channel beeps. You can configure the buzzing mode and duration. Buzzing mode supports 2 methods: ◦ Custom Time: The controller stops beeping when the configured duration is exceeded. ◦ Until the Door Locks: The controller stops beeping when the door closes.
Duress Alarm	An alarm triggers when a duress card, duress password, or duress fingerprint is used to unlock the door.

6. Click **Apply**.

Configuring Advanced Settings

Configuring First-person Unlock

Designate specific users as first-card holders. Other users can only unlock the door by identity verification after a first-card holder has completed identity verification.

Process

1. Log in to the web page.
2. Go to **Access Rules > Advanced Settings > First-person Unlock**.
3. Select the door, then click [✎](#).
4. Click .

Four Door Two-way Access Controller User Manual

Assign first-card permission to users

Edit

Enable

Status

Normal

▼

Weekly Schedule

255-Full Day

▼

Holiday Schedule

255-No Plan

▼

Person List

Remove

+

5. Select the weekly schedule and the holiday schedule.
The first-card rule applies only within the defined time period; during each period of the plan, after a first-card holder completes identity verification, other users can perform identity verification to unlock the door.
6. Select the door status.
 - **Normal:** Non-first cards users must verify their identities to unlock the door after first-card users grant access on the Access Controller.
 - **Always Unlocked:** The door stays open after first-card users grant access on the Access Controller.
7. Click

+

 to add first-card users, then click **OK**.

NOTE

- You can only select the user whose user type is **General User**.
- Up to 100 users can be configured as the first-card user.

Add first-card users

Add User

Select Person

User ID/Name

Q

Selected People

Clear

No.	User ID	Name
-----	---------	------

>

No.	User ID	Name	Operation
No Data			

8. Click **Apply**.

Configuring Anti-passback

Users must verify their identity for both entry and exit; otherwise, an anti-passback alarm triggers. It prevents card holders from passing their access card to others for entry. When anti-passback is enabled, card holders must exit the secure area before the system allows another entry.

Background Information

- If an authorized person exits without identity verification, an alarm triggers and access is denied when they attempt to enter again.
- If a person enters by tailgating without identity verification, an alarm triggers and access is denied when they attempt to exit.

Process

1. Log in to the web page.
2. Go to **Access Rules > Advanced Settings > Anti-passback**.
3. Click **+**, configure the parameters, then click **Apply**.

Four Door Two-way Access Controller User Manual

Anti-passback

Add

Reset Time30min (1-1440)

Weekly Schedule255-Full Day▼Holiday Schedule255-No Plan▼

Anti-passback?

Entry Group(2/8)

+ AddClear

Door1/Reader 1
Remove

Door1/Reader 2
Remove

Exit Group(2/8)

+ AddClear

Door2/Reader 3
Remove

Door2/Reader 4
Remove

Description of anti-passback group parameters

Parameter	Description
Reset Time	Set a time period during which the anti-passback alarm is triggered. For example, if the reset time is set to 60 minutes, when a person enters with authorization and exits without authorization, if they attempt to enter again within 60 minutes, the reverse passage alarm will be triggered.
Weekly Schedule	Select weekly schedule and holiday schedule. Anti-passback function takes effect during the specified time periods.
Holiday Schedule	
Entry Group	Click Add , then select card readers for entry and exit.
Exit Group	NOTE At least 2 groups must be added.

4. Click ☐ to enable the function.

Result

Group number indicates card swiping sequence. Cards must be used in the specified group order. For example: swipe at a Group 1 reader first, then a Group 2 reader, then a Group 3 reader, etc. The system operates normally as long as card swiping follows the preset sequence.

Configuring Multi-door Interlock

Multi-door interlock controls the locking status of two or more doors. When one door is unlocked, access to the remaining doors is prohibited. A single device supports configuration of 2 doors. The two doors operate independently without mutual interference.

NOTE
Unstable network during multi-door interlock use may cause door opening after identity verification and time-out alarm on the card reader. Ensure network stability.

Process

1. Log in to the web page.
2. Go to **Access Rules > Advanced Settings > Interlock**.
3. Click ☐ to enable the function, then click **+ Add**.

Interlock

Advanced Settings

Add

Enable☐

+ Add

1 record(s)

NameInterlock 1

Device Group

+ AddClear

Door2
Remove

4. Click **+Add**, select the door, then click **OK**.
5. Click **Apply**.

Configuring Unlock Methods

Process

1. Log in to the web page.
2. Go to **Access Rules > PIN Code Unlock**.
3. Turn on or turn off **PIN Code Authentication**.
When PIN code authentication is enabled, the door can be opened using only the password.

Four Door Two-way Access Controller User Manual

PIN code authentication

PIN Code (password without User ID) Unlock

When PIN code authentication is enabled, doors can be unlocked by inputting only password number without User ID. Additionally, Unlock Records will not record and display detailed user information.

PIN Code Authentication ☐

Apply Refresh Default

4. Click **Apply**.

Configuring Card Settings

Process

1. Log in to the web page.
2. Go to **Access Rules > Card Settings**.
3. Configure the card parameters.

Card parameters

Card Encryption Type

After the number system is changed, the card numbers will become invalid.

Card Encryption Type ☒ Hexadecimal ☐ Decimal

Apply Refresh Default

DESFire Card Write

Acquisition Device Enrollment Reader

Please place the card on the swiping area of the device.

Card Number **Write**

Card parameters description

Item	Parameter	Description
Card Encryption Type	Card Encryption Type	When a Wiegand card reader is connected, select decimal or hexadecimal format for the card number. The card encryption type applies to both card number input and output.

Item	Parameter	Description
DESFire Card Write	Card Number	Place the card on the reader, enter the card number, then click Write to write card number to the card. NOTE • Only supports hexadecimal format. • Supports up to 8 characters.

Configuring Back-end Comparison

Directly pass data such as card number to the third-party platform for data validation rather than validating data on the controller.

Process

1. Go to **Access Rules > Back-end Comparison**.
2. Click ☐ to enable the function, then click **Apply**.

Back-end comparison

Card No. Pass-through ☐

Apply Refresh Default

Configuring Access Card Rule Settings

The platform supports 5 default Wiegand formats. You can also add custom Wiegand formats.

Process

1. Log in to the web page.
2. Go to **Access Rules > Access Card Rule Settings**.
3. Click **Add**, then configure new Wiegand formats.

Four Door Two-way Access Controller User Manual

Add new Wiegand formats

Add

X

Wiegand Format

Total Bits

(1-128)

Facility Code

Add

No.	Start Bit	End Bit	Total Bits	Operation
No Data				

Card Number

Add

No.	Start Bit	End Bit	Total Bits	Operation
No Data				

Parity Code

Add

Parity Code	Type	Start Bit	End Bit	Total Bits	Operation
No Data					

Apply

Cancel

Wiegand format description

Parameter	Description
Wiegand format	The name of the Wiegand format.
Total bits	Enter the total number of bits.
Facility Code	Click Add , then enter the start bit and the end bit for the facility code.
Card number	Click Add , then enter the start bit and the end bit for the card number.

Parameter	Description
Parity Code	1. Click Add. 2. Enter the parity bit, the parity bit type, the parity start bit, and the parity end bit.

4. Click **Apply**.

Related Operations

- You can also click **Add Protocol** to import a Wiegand file to the platform.
- Facility Code:
 - (Default) **Off**: Card numbers converted from hexadecimal to decimal do not distinguish between the "facility code bits" and the "card number bits".
 - On**: Card numbers converted from hexadecimal to decimal distinguish between the "facility code bits" and the "card number bits".When the Facility Code is enabled, HID26 will be activated simultaneously.
- HID26: If the function is turned on:
 - Only Wiegand 26 is supported.
 - The platform only supports displaying card in decimal format.
 - The card number must have 5 characters and the facility code must has 3 characters at most. When you manually entering card, the system will automatically add leading zero to fixed number length. For example, if the card number you enter is less than 5 characters, like 123, leading zero is added to fix the number length to 5 characters, like 00123, and another 0 is added to function as a facility code. Therefore, the final card No. will be 000123.

Access Monitoring

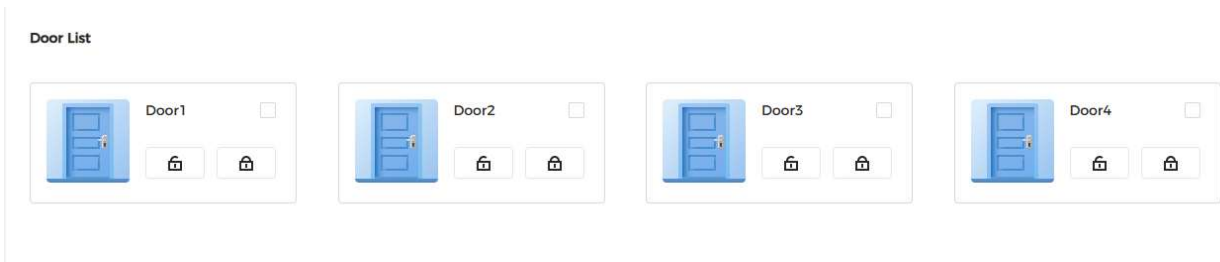
Log in to the web page, select **Access Monitoring**, and all the connected doors are displayed.

Operations to control the door

- Click  or  next to the door to remotely control the door.
 -  : Open.
 -  : Close.
- Select the door, then click **Always Unlocked** or **Always Locked** to remotely control the door. The door will remain open or closed all the time. You can select the door, then click **Normal** to restore access control to its normal status, and the door will be open or closed based on the configured verification methods.

Four Door Two-way Access Controller User Manual

Operations to control the door



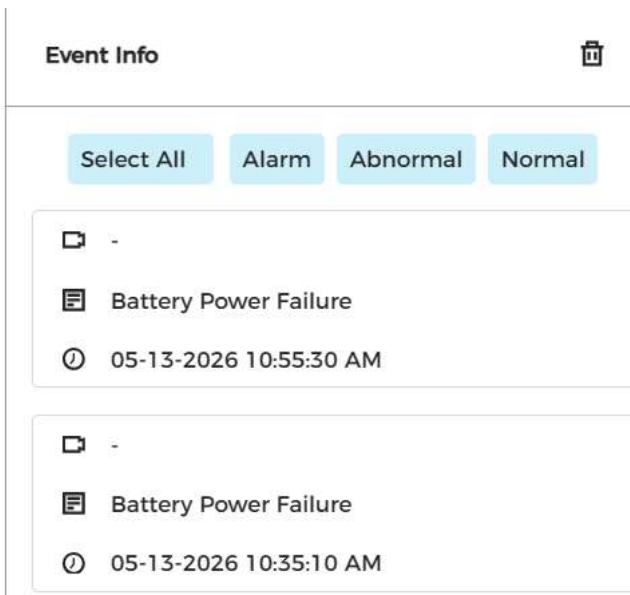
NOTE

If the controller is added to a management platform, the alarm settings will be synchronized to the platform.

Event information

Select the event type to view the events in the **Event Info** section. Click to clear all the events.

Event information



Configuring Alarm Input Channel

You can configure alarm linkages.

Process

1. Log in to the web page.
2. Go to **System Settings > Alarm Linkage Setting > Alarm**.
3. Click next to the alarm input channel to configure the parameters.

Alarm linkage

Edit

Enable

Alarm Input Channel

1

Alarm Input Name

Zone1

Alarm Input Type

Normally Open

Link Fire Safety Control

Number of EOLs

0EOL

Resistance

OK

Module Type

Local

Address

--

Channel No.

--

Alarm-out Port

Duration

30

s (1-300)

Alarm Output Channel

1

2

3

4

5

6

7

8

9

10

11

12

Access Control Linkage

Link Local Buzzer

OK

Refresh

Cancel

Details

Click events to display the details of the controller. You can view the IP address, device type and the device model here.

Configuring System Settings

Configuring Alarm Linkage

Four Door Two-way Access Controller User Manual

Description of alarm input

Parameter	Description
Alarm Input Name	Customize the name.
Alarm Input Type	Select Normally Open or Normally Closed based on the external alarm input device type. • Normally Open: The alarm input device is in an open circuit state when no alarm is triggered. Closing the circuit activates the alarm. • Normally Closed: The alarm input device is in a closed-circuit state when no alarm is triggered. Opening the circuit activates the alarm.
Link Fire Safety Control	When this function is enabled, all alarm output channels and access control channels open by default.
Number of EOLs	• Local alarm input: Select from 0EOL (alarm, normal), 1EOL (alarm, normal, open circuit) and 2EOL (alarm, normal, open circuit, short circuit). • External expansion module: Select from 0EOL (alarm, normal), 1EOL NC (alarm, normal, short circuit), 1EOL NO (alarm, normal, open circuit) and 2EOL (alarm, normal, open circuit, short circuit). When connecting external alarm input devices: • 0EOL requires no resistor configuration. • 1EOL and 2EOL require 1 and 2 resistors respectively.  NOTE • The access controller supports polymorphic alarm only for the first two alarm input channels. • Voltage values for each alarm state vary with resistor quantity and resistance combinations. Choose flexibly based on the actual external alarm devices used.
Resistance	• No configuration of this parameter is required for local alarm input. • Select the resistance based on the actual connected alarm device.
Module Type	• Supports connection of RS-708 and RS-808 modules. • Select type, address and channel number based on the actual connected modules (-- indicates an invalid channel number)
Address	 NOTE No configuration of this parameter is required for local alarm input.
Channel No.	
Alarm-out Port	Enable the alarm-out port, then select alarm output channels. When an alarm is triggered, the selected alarm output will activate. The default activation duration is 30 seconds.
Duration	
Alarm Output Channel	

Parameter	Description
Access Control Linkage	When enabled, the door switches to the configured status upon alarm trigger. • Auto: The door retains its pre-alarm status. If the door was in normal (authorized unlocked) status before the alarm, it remains normal after the alarm. • Normally Open: The door opens automatically when a fire alarm is triggered. • Normally Closed: The door closes automatically when a fire alarm is triggered. When Normally Open or Normally Closed is selected as the door status, configure the linkage mode. ◦ Strong Execution: The door stays in its current status after the fire alarm signal ends. Manually restore the previous status if needed. ◦ Weak Execution: The door automatically returns to its pre-alarm status after the fire alarm signal ends.
Link Local Buzzer	When enabled, the controller beeps upon alarm trigger. The default beep duration is 15 seconds.

4. Click **OK**.

Configuring Alarm Output Channel

Configure address, channel number and other parameters when connecting external alarm output expansion modules.

Process

1. Log in to the web page.
2. Go to **System Settings > Alarm Linkage Setting > Alarm Output Channel**.
3. Click  next to the alarm output channel to configure the parameters.

Four Door Two-way Access Controller User Manual

Alarm output channel

Edit

×

Enable

☒

Module Type

Local

▼

Address

0

▼

Channel No.

--

▼

OK

Cancel

4. Click **OK**.

Configuring Alarm Settings

Process

1. Log in to the web page.
2. Go to **System Settings > Alarm Settings**.

Alarm Settings

Battery Undervoltage Alarm

☒

Link Local Buzzer

☐

Utility Power Failure Alarm

☒

Link Local Buzzer

☐

Fire Signal Input Type

☒ Normally Open ☐ Normally Closed

Please make sure that the DIP switch for the fire alarm cable on the mainboard is set to NO.

Apply

Refresh

Default

3. Configure the alarm and the linkage as needed.
Turn on or off the battery undervoltage alarm and utility power failure alarm. Enable the **Link Local Buzzer** and configure its duration. When the alarm is triggered, the controller beeps for the configured period.
4. Configure the fire signal input type.
Ensure the fire switch on the controller is set to **Normally Open**. Select **Normally Open** and **Normally Closed** as the fire signal input type.
5. Click **Apply**.

Account Management

You can add or delete users, change users' passwords. Enter an email address for password reset when the password is forgotten.

Adding Administrators

You can add new administrator accounts, then they can log in to the web page of the controller.

Process

1. Select **System Settings > Account Management** on the home page.
2. Click **Add**, and enter the user information.

NOTE

- The username cannot be the same with existing account. The username consists of up to 31 characters and only allows for numbers, letters, underscores, midlines, dots, or @.
- The password must consist of 8 to 32 non-empty characters and must include at least two of the following types of characters: uppercase letters, lowercase letters, numbers, and special characters (excluding ' " ; : &). Please set a high-security password according to the password strength prompts.

Four Door Two-way Access Controller User Manual

Add administrators

Add

X

* Username

* Password

* Confirm Password

Remarks

OK

Cancel

3. Click **OK**.

 NOTE

Only the admin account can change passwords. The admin account cannot be deleted.

Resetting the Password

Reset the password via the linked email if you forget it.

Process

1. Go to **System Settings > Password Reset**.
2. Enter the email address, and set the password expiration time.
3. Turn on the password reset function.

Reset Password

Account

ONVIF User

Password Reset

Enable

If you forgot the password, you can receive security codes through the email address left in advance to reset the password.

Email Address

@gmail.com

Password Expires in

Never

Days

Apply

Refresh

Default

 NOTE

If you forget the password, you can receive a security code via the linked email address to reset it.

4. Click **Apply**.

Adding ONVIF Users

Open Network Video Interface Forum (ONVIF) is a global, open industry forum. It develops global open standards for interfaces of physical IP-based security products. These standards enable compatibility between products from different manufacturers. ONVIF users are authenticated via the ONVIF protocol. The default ONVIF user is admin.

Process

1. Go to **System Settings > Account Management > ONVIF User** on the home page.
2. Click **Add**, then configure parameters.

Four Door Two-way Access Controller User Manual

Add ONVIF user

ONVIF user description

Parameter	Description
Username	The username cannot be the same as an existing account. The username consists of up to 31 characters and may only include numbers, letters, underscores, hyphens, periods, or the @ symbol.
Password	The password must consist of 8 to 32 non-empty characters and must include at least two types of the following characters: uppercase letters, lowercase letters, numbers, and special characters (excluding ' " ; : &).
Group	There are three permission groups, representing different levels of access. Admin: You can access user management on the ONVIF Device Manager. Operator: You cannot access user management on the ONVIF Device Manager. User: You cannot access user management and system logs on the ONVIF Device Manager.

3. Click **OK**.

Viewing Online Account

Go to **System Settings > Online Account** on the home page. You can view the online users currently logged in to the web page.

Configuring Time Settings

Process

1. Go to **System Settings > Time Settings** on the home page.
2. Configure the time of the Platform.

Date settings

Time settings description

Parameter	Description
System Time	Manually enter the time or you can click Synchronize PC to synchronize time with your PC.
Time Zone	Select the time zone, date format, and time format.
Date Format	
Time Format	
NTP Settings	The access controller will automatically synchronize the time with the NTP server. Enable NTP Settings , set the NTP server, the NTP server port, and the synchronization interval.
NTP Server	
Port	
Interval	
Daylight Saving Time	1. Enable Daylight Saving Time. 2. Set the start time and end time.

3. Click **Apply**.

Four Door Two-way Access Controller User Manual

Network Settings

Configuring TCP/IP

You need to configure the IP address of the access controller to ensure that it can communicate with other devices.

Process

1. Go to **System Settings > Network Settings > TCP/IP**.
2. Configure the parameters.

TCP/IP

NIC

NIC 1

▼

Mode

☒ DHCP

☐ Static

MAC Address

IP Version

IPv4

▼

IP Address

192 . 168 . 1 . 168

Subnet Mask

255 . 255 . 255 . 0

Default Gateway

192 . 168 . 1 . 1

Preferred DNS

Alternate DNS

MTU

1500

Apply

Refresh

Default

Description of TCP/IP

Parameter	Description
Mode	• Static: Manually enter IP address, subnet mask, and gateway. • DHCP: When DHCP is enabled, the access controller will automatically assign IP addresses, subnet masks, and gateways.
MAC Address	MAC address of the controller.

Parameter	Description
IP Version	IPv4 or IPv6.
IP Address	If you select static mode, configure the IP address, subnet mask and gateway. NOTE • IPv6 addresses are represented in hexadecimal. Subnet masks are not required for IPv6. • The IP address and default gateway must be in the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.
MTU	MTU (Maximum Transmission Unit) is the maximum data size transmittable in a single network packet. A larger MTU boosts transmission efficiency by reducing packet count and network overhead. If a network device cannot handle the packet size, fragmentation or transmission errors may occur. Ethernet networks commonly use an MTU of 1500 bytes. Smaller values may be needed for PPPoE, VPN, or other specific protocols/services. Recommended MTU values: • 1500: Default and maximum for Ethernet. Used for connections without PPPoE/VPN (e.g., routers, adapters, switches). • 1492: Optimal for PPPoE. • 1468: Optimal for DHCP. • 1450: Optimal for VPN.

3. Click **Apply**.

Configuring Port

You can limit access to the controller at the same time through web page, desktop client and mobile client.

Process

1. Go to **System Settings > Network Settings > Port**.
2. Configure the ports.

Four Door Two-way Access Controller User Manual

Configure ports

Max Connection

50

(1-50)

HTTP Port

80

HTTPS Port

443

Apply

Refresh

Default

NOTE

Except for **Max Connection**, you need to restart the controller to make the configurations effective after you change other parameters.

Description of ports

Parameter	Description
Max Connection	Set the maximum number of clients that can simultaneously access the access controller, such as web pages, desktop clients, and mobile phones.
HTTP Port	The default is 80. If you wish to change the port number, please add the new port number after the IP address when logging into the web page.
HTTPS Port	The default value is 443.

3. Click **Apply**.

Configuring Basic Service

When you want to connect the controller to a third-party platform, turn on the CGI and ONVIF functions.

Process

1. Go to **System Settings > Network Settings > Basic Services**.
2. Configure the basic service.

Basic service

SSH

☐

Multicast/Broadcast Search

☒

CGI

☒

ONVIF

☒

Private Protocol Authentication Mode

Security Mode (Recommen... ▾)

Private Protocol

☒ ?

TLSv1.1

☐

Apply

Refresh

Default

Basic service parameter description

Parameter	Description
SSH	SSH (Secure Shell Protocol) is a remote administration protocol. It lets users access, control, and modify remote servers over the internet.
Mutlicast/Broadcast Search	Search for devices via multicast or broadcast protocols.
CGI	The Common Gateway Interface (CGI) is an interface for web servers. It enables standardized data exchange between external applications and servers.
ONVIF	ONVIF stands for Open Network Video Interface Forum. It aims to standardize interfaces between IP-based security devices. These specifications act as a common communication language for devices.
Private Protocol Authentication Mode	Set the authentication mode. Options include Security Mode and Compatibility Mode. Security Mode is recommended. Security Mode (Recommended): Does not support Digest, DES, or plaintext authentication for controller access. Improves device security. Compatibility Mode: Supports Digest, DES, and plaintext authentication for controller access. Security is reduced.
Private Protocol	The platform adds devices using the private protocol.

Four Door Two-way Access Controller User Manual

Parameter	Description
TLSv1.1	TLSv1.1 refers to Transport Layer Security version 1.1. TLS is a cryptographic protocol. It provides secure and authenticated communication over computer networks. NOTE Enabling TLSv1.1 may introduce security risks. Please note this.

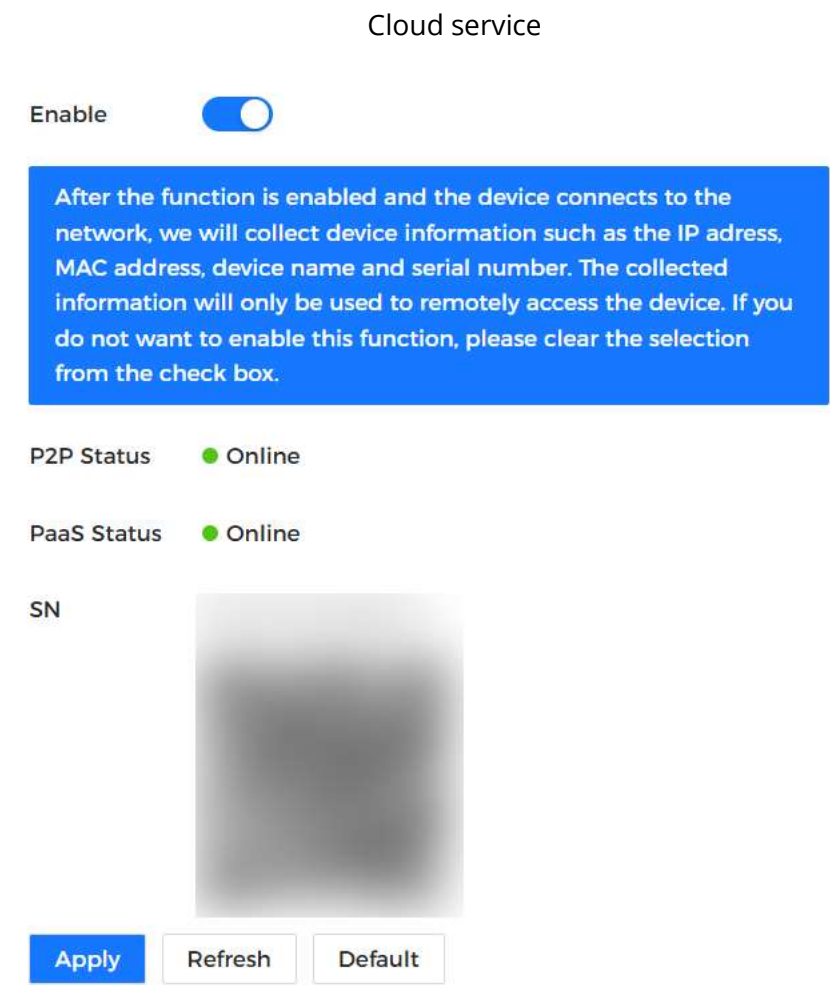
3. Click **Apply**.

Configuring Cloud Service

The cloud service offers NAT traversal. Users can manage multiple devices via Pro-X Next App. No need to apply for a dynamic domain name, configure port mapping, or deploy a server.

Process

1. Go to **System Settings > Network Settings > Cloud Service** on the home page.
2. Turn on the cloud service function.
The cloud service is online when P2P and PaaS are online.



3. Click **Apply**.
4. Scan the QR code with Pro-X Next App to add the controller.

System Information

Viewing Version Information

Go to **System Settings > System Info > Version** on the web page, and you can view version information of the controller.

Viewing Legal Information

Go to **System Settings > System Info > Legal Info** on the home page, and you can view the software license agreement, privacy policy and open source software notice.

Maintenance Center

System Capacity

You can view the storage capacity of the controller for users, cards, fingerprints, alarm logs, and unlock records.
Go to **Maintenance Center > System Capacity** on the web page.

Viewing Logs

View logs including system logs, alarm logs, and unlock records.

System Logs

View and search for system logs.

Process

1. Log in to the web page.
2. Go to **Maintenance Center > Log > Log**.

Four Door Two-way Access Controller User Manual

System Logs

Please keep unencrypted files secure to avoid data leaks.

Time Range 05-13-2026 12:00:00 AM → 05-14-2026 12:00:00 AM Type All Search Reset

☐ Encrypt Log Backup Export

No.	Time	Type	Log Content
1	05-13-2026 10:38:28 AM	Save Config	
2	05-13-2026 10:38:26 AM	Logout	
3	05-13-2026 10:38:26 AM	Login	
4	05-13-2026 10:36:41 AM	Save Config	
5	05-13-2026 10:36:41 AM	Save Config	

3. Select the time range and the log type, then click **Search**.

Related Operations

- click **Export** to export the searched logs to your local computer.
- Click **Encrypt Log Backup**, then enter a password. The exported file can be opened only after entering the password.
- Click  to view details of a log.

Unlock Records

Search for unlock records and export them.

Process

1. Log in to the web page.
2. Go to Maintenance Center > Log > Unlock Records.

Unlock records

Door Channel All Type All Time Range 03-13-2026 00:00:00 → 03-14-2026 00:00:00 Search

Export

No.	Unlock Method	User ID	User Name	Status	Time	Door Channel
1	Remote Unlock			Succeed	03-13-2026 16:11:38	Door1

3. Select the time range and the type, then click **Search**.
You can click **Export** to download the log.

Alarm Logs

View alarm logs.

Process

1. Log in to the web page.

2. Go to **Maintenance Center > Log > Alarm Logs**.

Alarm Logs

Door Channel All Type All Time Range 05-13-2026 12:00:00 AM → 05-14-2026 12:00:00 AM Search

Export

No.	Unlock Method	User ID	User Name	Status	Time	Door Channel
1	Remote Unlock			Succeed	05-13-2026 11:14:31 AM	Door1
2	Card			Failed	05-13-2026 10:36:41 AM	Door4

2 records < 1 >

3. Select the type and the time range.
4. Enter the admin ID, then click **Search**.

Maintenance Management

When multiple devices require the same configuration, you can set their parameters by importing or exporting configuration files.

Exporting and Importing Configuration Files

You can import and export the controller's configuration file. To apply the same configuration to multiple devices, import the configuration file to them.

Background Information

- The controller supports exporting and importing the following configurations:
 - Access control functions
 - Alarm linkage/alarm settings
 - Bluetooth unlocking function
 - Time settings
- Network settings and security settings do not support export or import.

Process

1. Log in to the web page.
2. Go to **Maintenance Center > Maintenance > Config**.

Configuration management

Config

Config Export Export

File Browse Import File

Imported configuration will overwrite previous configuration.

Four Door Two-way Access Controller User Manual

3. Export or import configuration files.
- Export the configuration file.
Click **Export** to download the file to the local computer.

• Import the configuration file.

1) Click **Browse** to select the configuration file.

2) Click **Import File**.

NOTE

Configuration files can only be imported to devices of the same model.

Configuring the Card Reader

Process

1. Log in to the web page.
2. Go to **Maintenance Center > Maintenance > Config**.
3. Configure the card reader parameters in the **Card Reader Settings** section, then click **Apply**.

1) Select the door channel, then enable or close **Card No. Inversion**.

2) Select the reader device, then select the protocol and the baud rate.

Card reader settings

Card Reader Settings

Door Channel

1

▼

Card No. Inversion

☐ Enable

☒ Close

Reader

Reader 1

▼

Card Reader Protocol

☒ RS-485

☐ OSDP

Baud Rate

☒ 9600

☐ 115200

Apply

Refresh

Default

Configuring the Fingerprint Similarity Threshold

Configure the fingerprint similarity threshold. A higher value means higher accuracy but lower pass rate.

Process

1. Log in to the web page.
2. Go to **Maintenance Center > Maintenance > Config**.
3. Enter the similarity threshold in the **Fingerprint** section, then click **Apply**.

NOTE

• The parameter is available on the modular access controller with the fingerprint module.

• The parameter is available on the access controller with fingerprint function.

Fingerprint similarity threshold

Fingerprint

Fingerprint Similarity Threshold

3

(1-10)

Apply

Refresh

Default

Restoring Default Settings

Process

1. Log in to the web page.
2. Go to **Maintenance Center > Maintenance > Config**.

CAUTION

Restoring the controller to its default configurations will result in data loss.

Restoring the controller

Default

Factory Defaults

Restore to Default (Except for User Info and Logs)

3. Restore to default settings if necessary.
- **Factory Defaults:** Resets all the configurations of the controller and deletes all the data.

Four Door Two-way Access Controller User Manual

- 1) Click **Factory Defaults** in the **Default** section.
- 2) Enter the administrator password, then click **OK**.
During restoration, the controller beeps continuously. When the beeping stops, the controller is restored to factory settings and restarts automatically.
- **Restore to Default (Except for User Info and Logs)**: Resets the configurations of the controller and deletes all the data except for user information and logs.
 - 1) Click **Restore to Default (Except for User Info and Logs)** in the **Default** section.
 - 2) Click **OK**.
During restoration, the controller beeps continuously. When the beeping stops, the controller is restored to default settings and restarts automatically.



You can also use the "Default" button on the controller to restore default settings. For more details, please refer to "**Components description**".

Restarting the controller

You can periodically restart the access controller during its idle time to improve its performance. By default, it is set to **Never**, and we recommend changing it to once a week.

Process

1. Log in to the web page.
2. Go to **Maintenance Center > Maintenance > Restart**.

Restarting the controller

Restart System	
Restart Time	Never ▼
Manual Operation	<button>Restart</button>
<button>Apply</button><button>Refresh</button>	

3. Set the restart time, then click **Apply**.
The controller will restart at the scheduled time.
4. (Optional) Click **Restart**, and the access controller will restart immediately.

Updating the System



CAUTION

- Use the correct update file. Make sure that you get the correct update file from technical support.
- Do not disconnect the power supply or network, and do not restart or shutdown the controller during the update.

Controller Update

File Update

Process

1. Go to **Maintenance Center > Update** on the home page.
2. Click **Browse** in the **Controller Update > File Update** section, then upload the update file.



The update file should be a .bin file.

3. Click **Update**.
The controller will restart after the update finishes.

Online Update

Process

1. Go to **Maintenance Center > Update** on the home page.
2. Select an update method in the **Controller Update > Online Update** section.
 - Select **Auto Check for Updates**, and the controller will automatically check for the latest version update.
 - Select **Manual Check**, and you can immediately check if the latest version is available.
3. (Optional) Click **Update Now** to update the controller immediately.

Card Reader Update

Process

1. Go to **Maintenance Center > Update** on the home page.
2. Select card readers to update in the **Card Reader Update** section.
3. Click **Browse**, then upload the update file.

Four Door Two-way Access Controller User Manual

 NOTE

The update file must be a .bin file.

4. Click **Update**.
- The controller will restart after the update finishes.

Advanced Maintenance

Acquire device information and capture packets. This helps maintenance personnel troubleshoot more easily.

Exporting

Process

1. Go to **Maintenance Center > Advanced Maintenance** on the home page.
2. Click **Export** to export the serial number, firmware version, device operation logs and configuration information.

Packet Capture

Process

1. Go to **Maintenance Center > Advanced Maintenance** on the home page.

Packet Capture						
Packet Capture						
NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Capture D...
eth0	192.168.1.168	Optional	Optional	Optional	Optional	0.00MB
lo	127.0.0.1	127.0.0.1	Optional	Optional	Optional	0.00MB

2. Enter the IP address and port number in the **Packet Capture** section, click ▶ .
- ▶ changes to || .
3. After you acquired enough data, click || .
- Captured packets are automatically downloaded to your local computer.

Network Test

Process

1. Go to **Maintenance Center > Advanced Maintenance** on the home page.
2. Enter the destination address in the **Network Test** section, then configure data packet size.

Network test

Network Test

Destination Address192.168.1.128TestStop

Data Packet Size64Byte (64-4096)

Test Result

timeout
72 bytes from 192.168.1.28: icmp_seq = 5 ttl = 64 time = 5 ms
72 bytes from 192.168.1.28: icmp_seq = 6 ttl = 64 time = 2 ms
72 bytes from 192.168.1.28: icmp_seq = 7 ttl = 64 time = 2 ms
72 bytes from 192.168.1.28: icmp_seq = 8 ttl = 64 time = 2 ms
72 bytes from 192.168.1.28: icmp_seq = 9 ttl = 64 time = 2 ms

Copy

3. Click **Test**.
- The result is displayed in the **Test Result** area. You can copy the result.

Security Settings

 NOTE

Users can enable or configure these features based on their actual security needs.

Configuring System Service

Create a certificate or upload an authenticated certificate. Then you can log in to the webpage via HTTPS on your computer. HTTPS secures network communication.

Process

1. Go to **Security > System Service**.
2. Click  to enable the HTTPS service.

 CAUTION

Enabling compatibility with TLS v1.1 and earlier versions may introduce security risks. Please note this.

3. Select the certificate.
- When Auto Redirect to HTTPS is enabled, logging in via HTTP will automatically redirect to the HTTPS login page.

Four Door Two-way Access Controller User Manual

 NOTE

If no certificates are in the list, click **Certificate Management** to upload a certificate.

HTTPS

Enable ☒

HTTPS is a service entry based on Transport Layer Security (TLS). HTTPS provides web service, ONVIF access service and RTSP access service.

Auto Redirect to HTTPS ☐

*Select a device certificate

Certificate Management

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
1		343037616134613637666...	05-07-2056 10:24:00 AM	BM12C53YA3B6919	BSC	HTTPS, RTSP over TLS

Apply Refresh Default Download Root Certificate

4. Click **Apply**.
- Enter “https://IP address: https port” in a web browser. If the certificate is installed, you can log in to the web page successfully, and if not, the web page will show the certificate as invalid or untrusted.

Attack Defense

Configuring Firewall

Configure the firewall to restrict access to the controller.

Process

1. Go to **Security > Attack Defense > Firewall**.
2. Click ☐ to enable the firewall function.

Firewall

Enable ☒

Mode ☒ Allowlist ☐ Blocklist

Only source hosts whose IP/MAC are in the following list are allowed to access corresponding ports of the device.

Add Delete

No.	Host IP/MAC	Port	Operation
No Data			

Apply Refresh Default

3. Select the mode: **Allowlist** and **Blocklist**.
- Allowlist**: Only IP/MAC addresses on the allowlist can access the controller.
 - Blocklist**: IP/MAC addresses on the blocklist cannot access the controller.
4. Click **Add** to enter the IP information.

Add IP information

Add

Add Mode IP

IP Version IPv4

IP Address 192 . 168 . 1 . 111

All Device Po... ☒

OK Cancel

5. Click **OK**.

Configuring Account Lockout

If an incorrect password is entered a specified number of times, the account will be locked.

Process

1. Go to **Security > Attack Defense > Account Lockout**.
2. Enter the number of allowed login attempts and the lockout duration for the administrator account and ONVIF users.

Four Door Two-way Access Controller User Manual

Account lockout

Device Account

Login Attempt

5time(s)

▼

Lock Time

5

min

ONVIF User

Login Attempt

30time(s)

▼

Lock Time

5

min

Apply

Refresh

Default

- **Login Attempt:** The maximum number of login attempts allowed. If an incorrect password is entered the specified number of times, the account will be locked.
- **Lock Time:** The duration during which the account cannot be logged into after being locked.

3. Click **Apply**.

Configuring Anti-DoS Attack

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to protect the controller against DoS attacks.

Process

1. Go to **Security > Attack Defense > Anti-DoS Attack**.
2. Turn on **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** to protect the controller against Dos attack.

Anti-DoS attack

SYN Flood Attack Defense

An attacker might send out repeated SYN messages to the device, leaving many half-open TCP connections on the device, which will make the device crash. When hit by an SYN flood attack, the device will defend itself by discarding the first message.

ICMP Flood Attack Defense

An attacker might send out an abnormally large number of ICMP packets to the device, which will use up all computing resources and thus make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.

Apply

Refresh

Default

3. Click **Apply**.

Installing Device Certificate

Create a certificate or upload a trusted certificate. Then you can log in to the controller via HTTPS on your computer.

Creating Certificate

Create a certificate for the controller.

Process

1. Go to **Security > CA Certificate > Device Certificate**.
2. Select **Install Device Certificate**.
3. Select **Create Certificate**, and click **Next**.

Create Certificate

Four Door Two-way Access Controller User Manual

Step 1: Select installation mode. X

Create Certificate

Apply for CA Certificate and Import (Recommended)

Install Existing Certificate

NextCancel

4. Enter the certificate information.

Certificate information (1)

Step 2: Fill in certificate information. X

Custom Name

* IP/Domain Name192.168.1.168

Organization Unit

Organization

* Validity PeriodDays (1-5000)

* Region

Province

City Name

BackCreate and install certificateCancel



NOTE

The region name must not exceed 2 characters. We recommend using the region's abbreviation.

5. Click **Create and install certificate**.

After the certificate is installed successfully, the newly installed certificate will be displayed on the **Device Certificate** page.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

Applying for and Importing CA Certificate

Import the third-party CA certificate into the access controller.

Process

- Go to **Security > CA Certificate > Device Certificate**.
- Click **Install Device Certificate**.
- Select **Apply for CA Certificate and Import (Recommended)**, and click **Next**.
- Enter the certificate information.
 - IP/Domain name**: The IP address or domain name of the controller.
 - Region**: The region name must not exceed 3 characters. We recommend using the region's abbreviation.

Certificate information (2)

Step 2: Fill in certificate information. X

* IP/Domain Name192.168.1.168

Organization Unit

Organization

* Region

Province

City Name

BackCreate and DownloadCancel

5. Click **Create and Download** to save the request file to your computer.

6. Apply to a third-party CA authority for the certificate by using the request file.

7. Import the signed CA certificate.

- Save the CA certificate to your computer.
- Click **Installing Device Certificate**.
- Click **Browse** to select the CA certificate.
- Click **Import and Install**.

After the certificate is installed successfully, the newly installed certificate will be displayed on the **Device Certificate** page.

- Click **Recreate** to regenerate the request file.
- Click **Import Later** to import the certificate at another time.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the certificate name.

Four Door Two-way Access Controller User Manual

- Click  to download the certificate.
- Click  to delete the certificate.

Installing Existing Certificate

If you already have a certificate and private key file, import them.

Process

1. Go to **Security > CA Certificate > Device Certificate**.
2. Click **Install Device Certificate**.
3. Select **Install Existing Certificate**, and click **Next**.
4. Click **Browse** to select the certificate and private key file, and enter the private key password.

Certificate and private key

Step 2: Select certificate and private key.

Custom Name

Certificate Path

Private Key

Private Key Passwor...

Browse

Browse

Back

Import and Install

Cancel

5. Click **Import and Install**.
After the certificate is installed successfully, the newly installed certificate will be displayed on the **Device Certificate** page.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click  to download the certificate.
- Click  to delete the certificate.

Installing the Trusted CA Certificate

A trusted CA certificate is a digital certificate. It validates the identities of websites and servers. For example, when using the 802.1x protocol, a CA certificate for switches is required. It authenticates the switch's identity.

NOTE

802.1X is a network authentication protocol. It opens network access ports. This happens after the organization authenticates the user's identity and authorizes their network access.

Process

1. Go to **Security > CA Certificate > Trusted CA Certificates**.
2. Select **Install Trusted Certificate**.
3. Click **Browse** to select the trusted certificate.

Install the trusted certificate

Install Trusted Certificate

Custom Name

Certificate Path

Browse

OK

Cancel

4. Click **OK**.
After the certificate is installed successfully, the newly installed certificate will be displayed on the **Trusted CA Certificates** page.

Related Operations

- Click **Enter Edit Mode** on the **Trusted CA Certificates** page to edit the name of the certificate.
- Click  to download the certificate.
- Click  to delete the certificate.

Four Door Two-way Access Controller User Manual

Cybersecurity Recommendations

Account Management

1. Use complex passwords

Please refer to the following suggestions for setting a password:

- The length must not be less than 8 characters;
- Include at least two types of characters: uppercase letters and lowercase letters, numbers, and symbols;
- Do not include the account name or the reverse order of the account name;
- Do not use consecutive characters, such as 123, abc, etc.;
- Do not use repeated characters, such as 111, aaa, etc.

2. Change passwords Regularly

It is recommended to regularly change device passwords to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Add users appropriately according to service and management requirements, and assign the minimum set of permissions to the users.

4. Enable account lockout function

The account lockout function is enabled by default. It is recommended that you keep this feature enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

The controller supports a password reset function. To reduce the risk of this function being exploited by malicious actors, please make timely modifications if there are any changes to the information. When setting security questions, it is recommended not to use easily guessable answers.

Service Configuration

1. Enable HTTPS

We recommend that you enable HTTPS to access network services through a secure channel.

2. Encrypted transmission of audio and video

If your audio and video data content is very important or sensitive, it is recommended to use encryption transmission features to reduce the risk of audio and video data being intercepted during transmission.

3. Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

If necessary, it is strongly recommended to select safe mode, including but not limited to the following services:

- SNMP: Select SNMP v3 and set strong encryption and authentication passwords.
- SMTP: Select TLS to access the mailbox server.
- FTP: Select SFTP and set a complex password.
- AP hotspot: Select WPA2-PSK encryption mode and set a complex password.

4. Change HTTP and other default service ports

It is recommended that you change the default ports for HTTP and other services to any port between 1024 and 65535 to reduce the risk of being targeted by threat actors.

Network Configuration

1. Enable Allow list

We recommend that you enable the allowlist feature, allowing only the IP addresses on the allowlist to access the controller. Therefore, be sure to add your computer's IP address and the IP addresses of supported devices to the allowlist.

2. MAC address binding

We recommended to bind the gateway's IP address to the controller's MAC address to reduce the risk of ARP spoofing.

3. Build a secure network environment

To better ensure the safety of the equipment and reduce potential network risks, it is recommended to take the following measures

- Disable the port mapping function of the router to prevent external networks from directly accessing internal network devices;
- Based on actual network requirements, the network should be segmented: If there is no communication requirement between two subnets, it is recommended to use methods such as VLANs and gateways to segment the network for isolation purposes;
- Establish an 802.1x access authentication system to reduce the risk of unauthorized terminal access to the private network.

Security Auditing

1. Check online users

We recommended to regularly check online users to identify unauthorized users.

2. Check device log

By reviewing the logs, you can understand the IP address of the device attempting to log in and the key actions of the logged-in user.

3. Configure network log

Four Door Two-way Access Controller User Manual

Due to the limited storage capacity of the controller, the number of logs stored is also restricted. If you need to retain logs for an extended period, it is recommended to enable the network logging feature to ensure that critical logs can be synchronized to the network log server for tracking.

Software Security

1. Update firmware in time

According to industry standard operating procedures, the firmware of the equipment needs to be updated to the latest version in a timely manner to ensure that the controller has the latest features and security. If the controller is connected to a public network, it is recommended to enable the automatic detection feature for online upgrades to promptly receive firmware update information released by the manufacturer.

2. Update client software in time

We recommended to download and use the latest client software.

Physical Protection

We recommended that you implement physical protection for the equipment (especially storage devices), such as placing the devices in dedicated server rooms and cabinets, and implementing access control and key management to prevent unauthorized personnel from damaging hardware and other external devices (such as USB flash drives and serial ports).