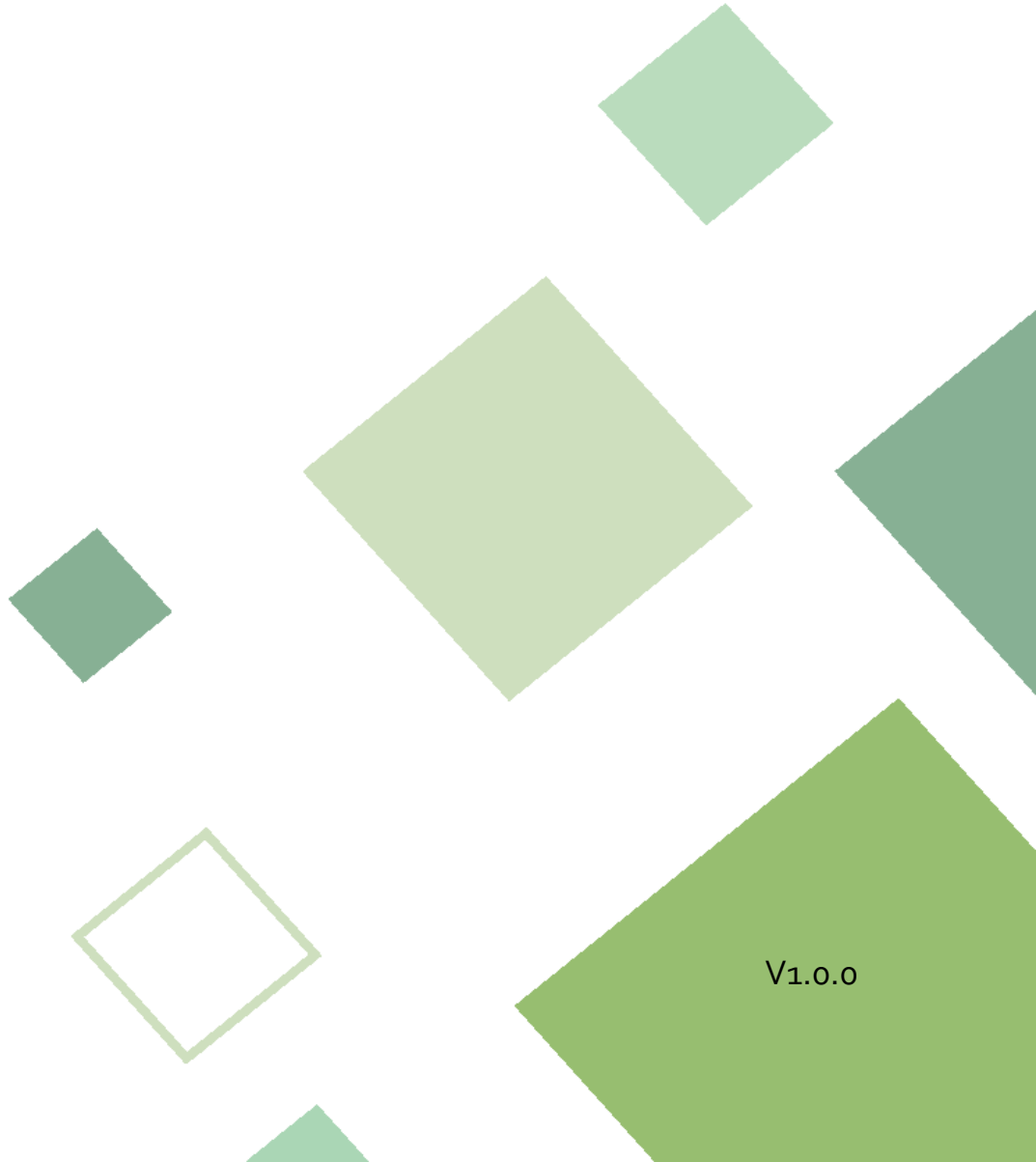


Access Controller

LXKW302-40

User's Manual



V1.0.0






Foreword

General

This manual introduces the functions and operations of the access controller. Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	December 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.

- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the access controller, hazard prevention, and prevention of property damage. Read carefully before using the access controller, and comply with the guidelines when using it.

Transportation Requirement



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

Storage Requirement



Store the access controller under allowed humidity and temperature conditions.

Installation Requirements



- Do not connect the power adapter to the access controller while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the access controller.
- Do not connect the access controller to two or more kinds of power supplies, to avoid damage to the access controller.
- Improper use of the battery might result in a fire or explosion.
- Please follow the electrical requirements to power the access controller.
 - ◇ Following are the requirements for selecting a power adapter.
 - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
 - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
 - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
 - ◇ We recommend using the power adapter provided with the access controller.
 - ◇ When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the access controller label.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the access controller in a place exposed to sunlight or near heat sources.
- Keep the access controller away from dampness, dust, and soot.
- Install the access controller on a stable surface to prevent it from falling.
- Install the access controller in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.

- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The access controller is a class I electrical appliance. Make sure that the power supply of the access controller is connected to a power socket with protective earthing.

Operation Requirements



- Check whether the power supply is correct before use.
- Ground the device to protective ground before you power it on.
- Do not unplug the power cord on the side of the access controller while the adapter is powered on.
- Operate the access controller within the rated range of power input and output.
- Use the access controller under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the access controller, and make sure that there is no object filled with liquid on the access controller to prevent liquid from flowing into it.
- Do not disassemble the access controller without professional instruction.
- This product is professional equipment.
- The access controller is not suitable for use in locations where children are likely to be present.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Product Overview	1
1.1 Product Introduction	1
1.2 Main Features	1
1.3 Application Scenarios	1
2 Main Controller-Sub Controller	3
2.1 Networking Diagram	3
2.2 Configurations of Main Controller.....	3
2.2.1 Configuration Flowchart.....	3
2.2.2 Initialization	4
2.2.3 Logging In	5
2.2.4 Home Page.....	11
2.2.5 Device Management.....	11
2.2.5.1 Adding Devices One by One	12
2.2.5.2 Adding Devices in Batches.....	13
2.2.6 User Management.....	14
2.2.6.1 Adding Group.....	14
2.2.6.2 Configuring Basic User Information.....	15
2.2.6.3 Adding Authentication Methods	17
2.2.6.3.1 Adding Passwords.....	17
2.2.6.3.2 Adding Cards.....	18
2.2.6.3.3 Adding Fingerprints.....	20
2.2.6.3.4 Adding Bluetooth Cards.....	21
2.2.7 Access Rules	26
2.2.7.1 Adding Weekly Plans.....	26
2.2.7.2 Adding Holiday Plans (Optional).....	27
2.2.7.3 Adding Zone.....	29
2.2.7.4 Adding Permission Rules	30
2.2.7.5 Viewing Data Synchronization Progress.....	31
2.2.7.6 Configuring Access Control (Optional).....	31
2.2.7.6.1 Configuring Basic Parameters	31
2.2.7.6.2 Configuring Unlock Methods.....	32
2.2.7.6.3 Configuring Alarms	34
2.2.7.7 Configuring the Password Unlock.....	35
2.2.7.8 Configuring Global Alarm linkages (Optional)	36

2.2.7.9	Configuring First-Person Unlock	39
2.2.7.10	Configuring Multi-Person Unlock	40
2.2.7.11	Configuring Anti-Passback	42
2.2.7.12	Configuring Multi-Door Interlock	44
2.2.7.12.1	Configuring Interlock within a Group	45
2.2.7.12.2	Configuring Interlock between Groups	46
2.2.8	Access Monitoring	47
2.2.8.1	Remotely Locking and Unlocking Doors	47
2.2.8.2	Setting Always Locked and Always Unlocked	48
2.2.9	Reports	49
2.2.9.1	Viewing Alarm Records	49
2.2.9.2	Viewing Unlock Records	49
2.2.10	System Settings	50
2.2.10.1	Configuring Time	50
2.2.10.2	Configuring Network	51
2.2.10.2.1	Configuring TCP/IP	51
2.2.10.2.2	Configuring Ports	52
2.2.10.2.3	Configuring Cloud Service	52
2.2.10.2.4	Configuring Automatic Registration	53
2.2.10.2.5	Configuring Basic Service	54
2.2.10.3	Updating the System	55
2.2.10.3.1	File Update	55
2.2.10.3.2	Online Update	55
2.2.10.4	Advanced Settings	56
2.2.10.4.1	Exporting and Importing Configuration Files	56
2.2.10.4.2	Configuring the Card reader	57
2.2.10.4.3	Configuring RS-485 Expansion	57
2.2.10.4.4	Restoring the Factory Default Settings	58
2.2.10.5	Configuring Card Rules	58
2.2.10.6	Restart	60
2.2.10.7	Backing up System Logs	60
2.2.10.8	Configure Local Alarm Linkages	60
2.2.10.9	Account Management	62
2.2.10.9.1	Adding Administrator Accounts	62
2.2.10.9.2	Resetting the Password	63
2.2.10.9.3	Adding ONVIF Users	63
2.2.10.10	Configuring Hardware	64
2.2.10.11	Viewing Legal Information	65
2.2.10.12	Viewing Version Information	65

2.2.11 Maintenance Center.....	65
2.2.11.1 Packet Capture	65
2.2.11.2 Running Log	66
2.2.12 Security	66
2.2.12.1 Configuring HTTPS	66
2.2.12.2 Attack Defense	67
2.2.12.2.1 Configuring Firewall.....	67
2.2.12.2.2 Configuring Account Lockout	67
2.2.12.2.3 Configuring Anti-DoS Attack	68
2.2.12.3 Installing Device Certificate	68
2.2.12.3.1 Creating Certificate.....	69
2.2.12.3.2 Applying for and Importing CA Certificate	69
2.2.12.3.3 Installing Existing Certificate	70
2.2.12.4 Installing the Trusted CA Certificate	71
2.3 Configurations of Sub Controller.....	72
2.3.1 Initialization	72
2.3.2 Logging In	72
3 X Station-Sub Controllers	73
3.1 Networking Diagram	73
3.2 Configurations on X Station.....	73
3.3 Configurations on Sub Controller.....	73
Appendix 1 Security Recommendation.....	74

1 Product Overview

1.1 Product Introduction

Flexible and convenient, the access controller has a user friendly system that allows you to access controllers on the webpage through IP address. It comes with a professional access management system, and makes the networking of main and sub control modes quick and easy, meeting the needs of small and advanced systems.

1.2 Main Features


- Built of flame-retardant PC and ABS material, it is both sturdy and elegant with an IKo6 rating.
- Supports TCP and IP connection, and standard PoE.
- Accesses card readers through Wiegand and RS-485 protocols.
- Supplies power to the lock through its 12 VDC output power supply, which has a maximum output current of 1000 mA.
- Supports 1,000 users, 5,000 cards, 5,000 Bluetooth cards, 3,000 fingerprints, and 300,000 records.
- Multiple unlock methods including card, password, fingerprint and more. You can also combine these methods to create your own personal unlock methods.
- Multiple types of alarms events are supported, such as duress, tampering, intrusion, unlock timeout, and illegal card.
- Supports a wide range of users including general, manager, VIP, guest, blocklist, and more users.
- Manual and automatic time synchronization.
- Retains stored data even while powered off.
- Offers a variety of functions and the system can be configured. Devices can also be updated through the webpage.
- Features main and sub control modes. The main control mode offers user management, access control device management and configuration, and more options. Devices under sub-control modes can be added to multiple platforms.
- A main controller can connect with and manage up to 14 sub controllers.
- Watchdog protects the system to allow the device to be stable and perform efficiently.
- Sub controllers can be added to X Station.

1.3 Application Scenarios

It is widely used in parks, communities, business centers and factories, and ideal for places such as office buildings, government buildings, schools and stadiums.

The access controller can be set to the main access controller (herein referred to as "main controller") or the Sub access controller (herein referred to as "sub controller"). 2 different networking methods are available for the access controller. You can select a networking method based on your needs.

Table 1-1 Networking methods of access controller

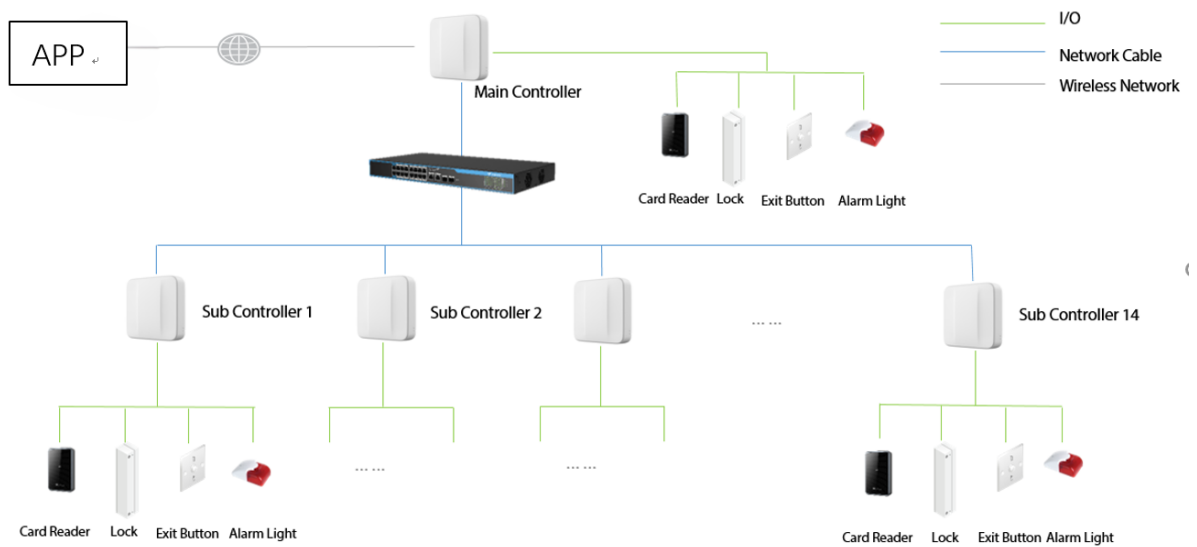
Networking Method	Description
Main Controller—Sub Controller	<p>The main controller comes with a management platform (herein referred to as the "platform"). Sub controllers must be added to the Platform of the main controller. The main controller can manage up to 14 sub controllers. For details, see "2 Main Controller-Sub Controller".</p>  <p>We do not recommend you add other management platforms in this networking method.</p>
X Station—Sub Controller	<p>Sub controllers needs to be added to a standalone management platform, such as X Station. The platform can manage up to 64 doors if each sub controller connects 2 doors. For details, see "3 X Station -Sub Controllers".</p>

2 Main Controller-Sub Controller

2.1 Networking Diagram

The main controller comes with a management platform (herein referred as the "platform"). Sub controller needs to be added to the platform of the main controller. The main controller can manage up to 14 sub controllers.

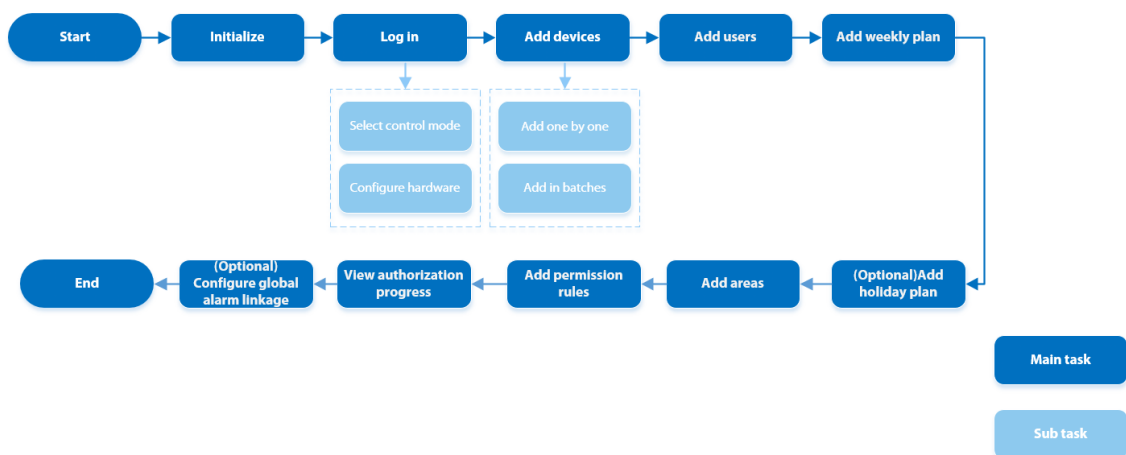
Figure 2-1 Networking diagram



2.2 Configurations of Main Controller

2.2.1 Configuration Flowchart

Figure 2-2 Configuration flowchart



2.2.2 Initialization

Initialize the main controller when you log in to the webpage for the first time or after it is restored to its factory defaults.

Prerequisites


Make sure that the computer used to log in to the webpage is on the same LAN as the main controller.

Procedure

Step 1 Open a browser, go to the IP address (the IP address is 192.168.1.101 by default) of the main controller.



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

Step 2 Set the password and email address, and then click .



- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: upper case and lower case letters, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.
- Keep the password safe after initialization and change the password regularly to improve security.

Figure 2-3 Password settings

The screenshot shows a web interface for 'Password Settings'. The header has three tabs: 'Password Settings' (active), 'Time Zone Setting', and 'Auto Check for Updates'. The main content area contains the following fields:

- Username:** admin
- Password:** A text input field with a strength indicator below it showing approximately 75% completion (yellow and orange bars).
- Confirm Password:** A text input field.
- Email Address:** A text input field with a checkbox labeled 'Email Address' to its right.


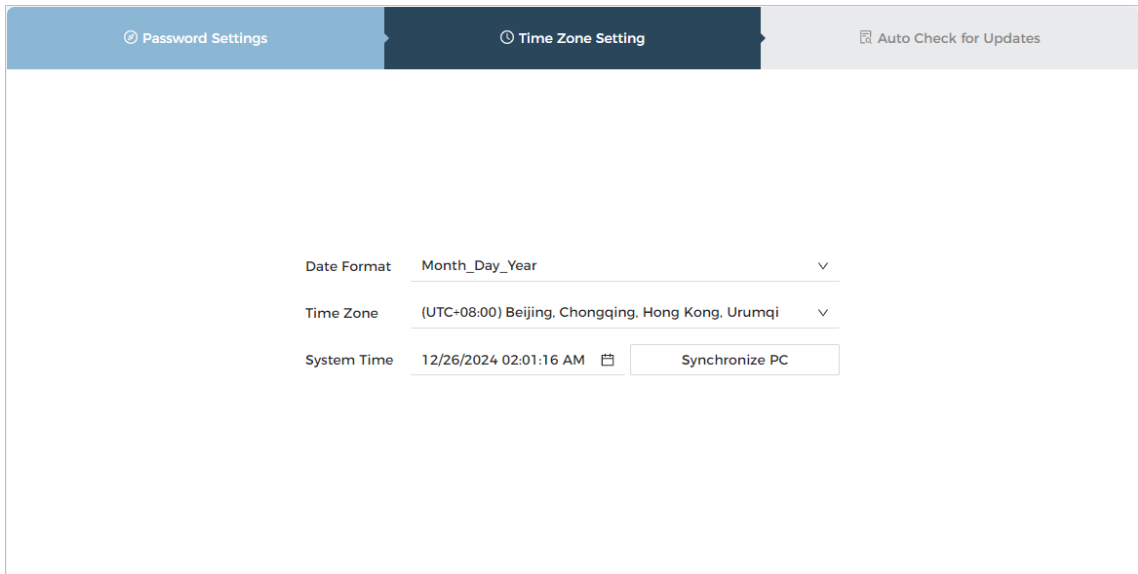
Step 3 Configure the system time, and then click .

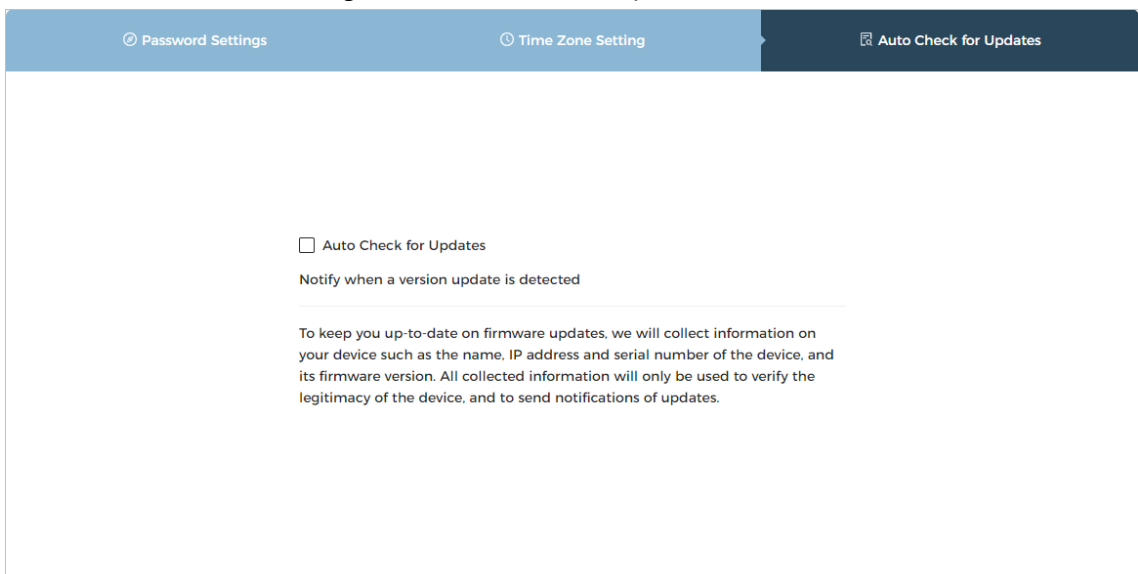
Figure 2-4 Time zone setting




Step 4 (Optional) Select **Auto Check for Updates**.

The system automatically check is there any higher version available, and inform the user to update the system. The system automatically checks for new updates, and informs you when a new update is available.

Figure 2-5 Auto check for updates



Step 5 Click . Login to the system, then it goes to the **Setup Wizard** page.

2.2.3 Logging In

For first-time login during initialization, you need to follow the login wizard to configure the type of main controller and its hardware.

Procedure

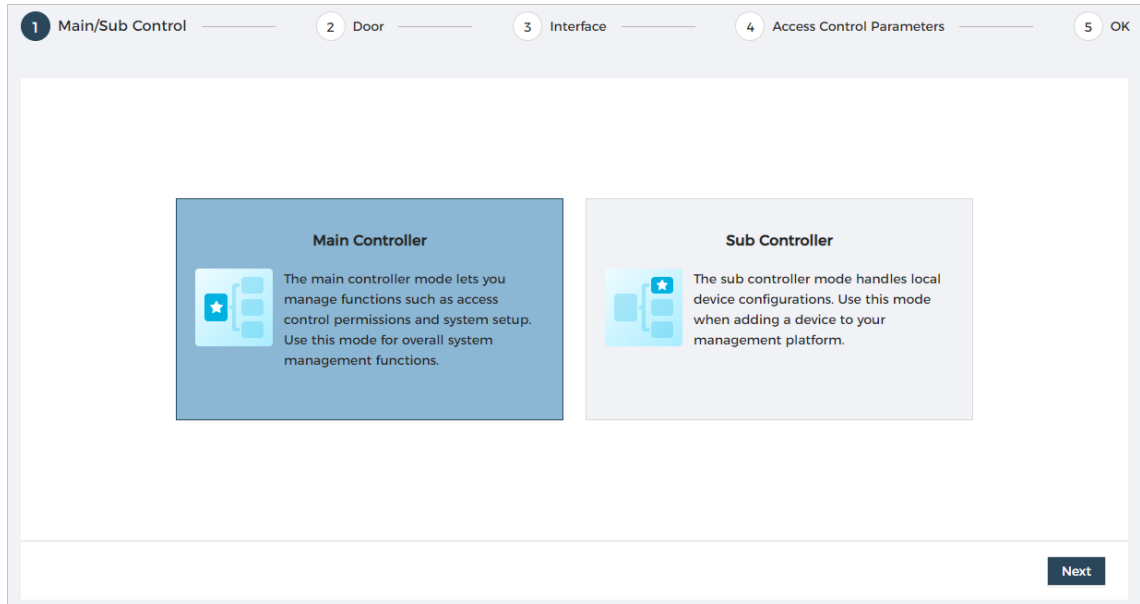
Step 1 On the login page, enter the username and password.



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

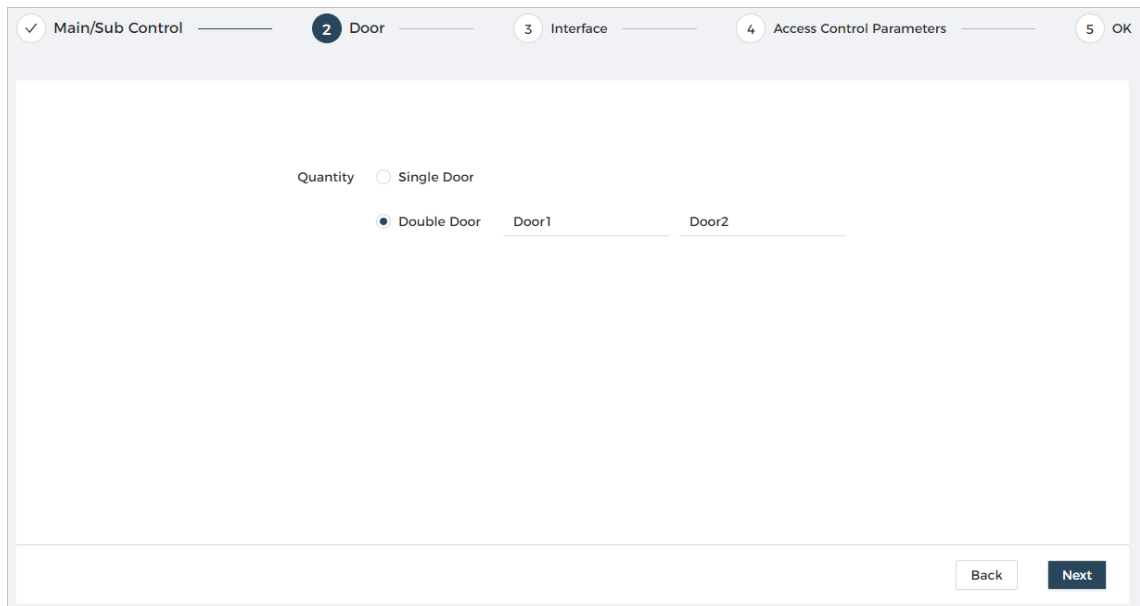
Step 2 Select **Main Control**, and then click **Next**.

Figure 2-6 Main/Sub control



Step 3 Select the number of doors, enter the name of the door, and then click **Next**.

Figure 2-7 Door





Step 4 Configure the parameters of the doors, and then click **Next**.

Figure 2-8 Configure door parameters

The screenshot shows a configuration window with a breadcrumb trail: Main/Sub Control > Door > **3** Interface > 4 Access Control Parameters > 5 OK. The main content is divided into two sections, Door1 and Door2. Each section has a 'Power Supply of Locks' header. Under 'Entry Card Reader', there are radio buttons for 'Wiegand', 'OSDP', and 'RS-485'. A dropdown menu shows 'Single' selected, with 'LED' to its right. Under 'Exit Button', there is a checkbox. Under 'Door Sensor', there is a checkbox. The 'Power Supply of Locks' section has radio buttons for '12V' and 'Relay'. To the right, there are dropdown menus for 'Fail Secure' and 'Relay Open = Locked', each with a help icon. At the bottom right, there are 'Back' and 'Next' buttons.

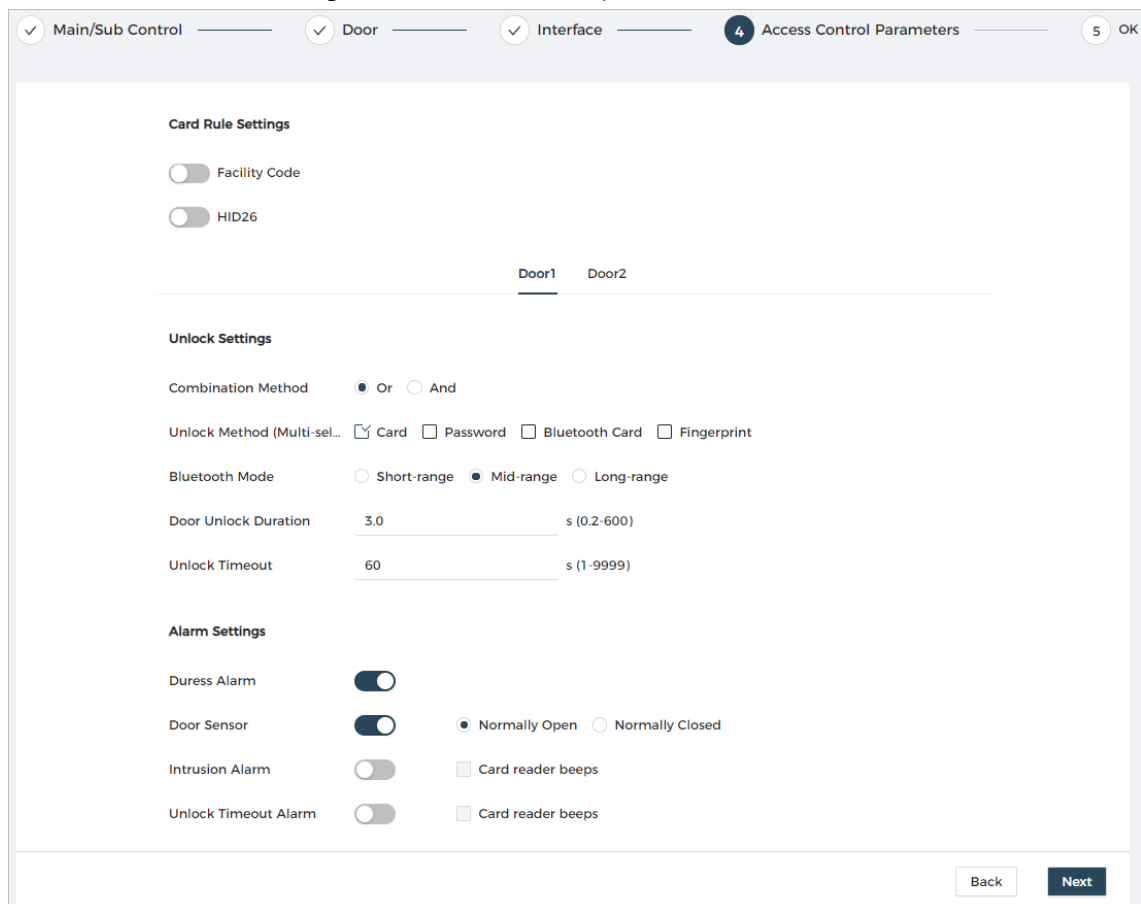
Table 2-1 Parameter description

Parameter	Description
Entry Card Reader	Select the card reader protocol.
Exit Card Reader	<ul style="list-style-type: none"> • Wiegand: Connects to a Wiegand reader. You can connect the LED wire to the LED port of the controller, and the reader will beep and flash when the door unlocks. • OSDP: Connects to an OSDP reader. • RS-485: Connects to a RS-485 reader.
Exit Button	<p>Connects to an exit button.</p> <p> Exit button is not available when Single Door is selected in the previous step.</p>
Door Sensor	Connects to a door detector.

Parameter	Description
Power Supply of Locks	<ul style="list-style-type: none"> ● 12 V: The controller provides power to the lock. <ul style="list-style-type: none"> ◇ Fail secure: When the power is interrupted or fails, the door stays locked. ◇ Fail safe: When the power is interrupted or fails, the door automatically unlocks to let people leave. ● Relay: The relay supplies power for the lock. <ul style="list-style-type: none"> ◇ Relay open = locked: Sets the lock to remain locked when the relay is open. ◇ Relay open = unlocked: Sets the lock to unlock when the relay is open. <p> The electromagnetic lock unlocks in an instant and locks again immediately when the access controller is in the soft reboot.</p>

Step 5 Configure access control parameters.

Figure 2-9 Access control parameters



Step 6 In **Unlock Settings**, select **Or** or **And** from **Combination Method**.


- Or: Use one of the selected unlock methods to authorize opening the door.
- And: Use all of the selected unlock methods to authorize opening the door.



Bluetooth card cannot be selected when you set the combination method to **And**.

Step 7 Select the unlock methods, and then configure the other parameters.

Table 2-2 Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	Supports unlocking through card, fingerprint, password or Bluetooth card. The Bluetooth card function is turned off by default.
Bluetooth Mode	<p>The Bluetooth card must be a certain distance away from the access control device to exchange data and unlock the door. Following are the ranges that are most suitable for it.</p> <ul style="list-style-type: none"> • Short-range: The Bluetooth unlock range is less than 0.66 ft (0.2 m). • Mid-range: The Bluetooth unlock range is less than 6.56 ft (2 m). • Long-range: The Bluetooth unlock range is less than 32.81 ft (10 m). <p> The Bluetooth unlock range might differ depending on models of your phone and the environment.</p>
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through. It ranges from 0.2 seconds to 600 seconds.
Unlock Timeout	A timeout alarm is triggered when the door remains unlocked for longer than the defined value.

Step 8 In **Alarm Settings**, configure the alarm parameters.

Table 2-3 Description of alarm parameters

Parameter	Description
Duress Alarm	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Door Sensor	Select the type of door detector.
Intrusion Alarm	<ul style="list-style-type: none"> • When the door detector is enabled, an intrusion alarm will be triggered if the door is opened abnormally. • A timeout alarm will be triggered when the door remains unlocked for longer than the defined unlock time. • When Card reader beeps is enabled, the card reader beeps when the intrusion alarm or timeout alarm is triggered.
Unlock Timeout Alarm	

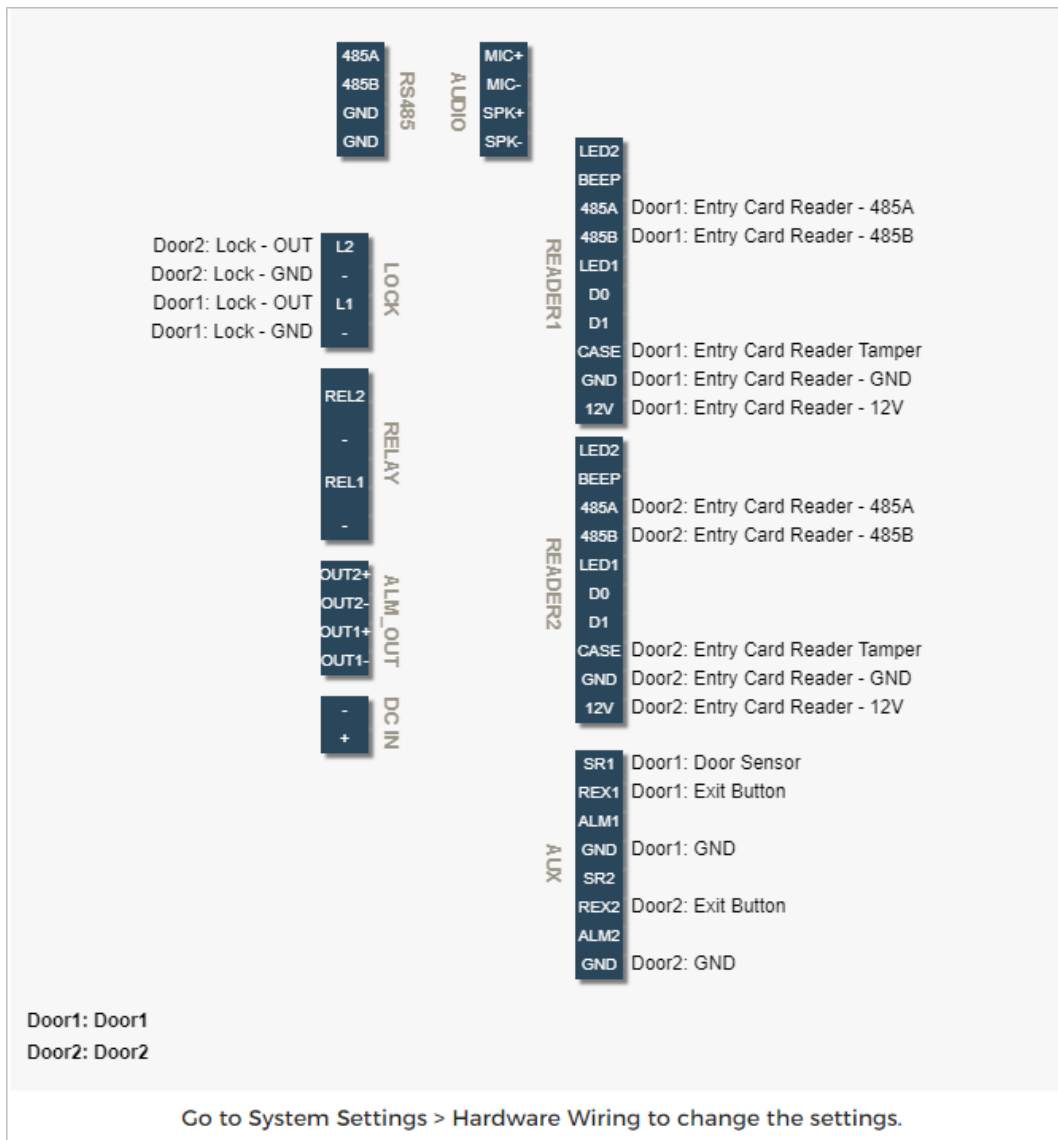
Step 9 Click **Next**.

A wiring diagram is generated based on your configurations. You can wire the device according to the diagram.



The image below is for reference only.

Figure 2-10 Wiring diagram



Step 10 Click **Apply**.

- You can go to **System Settings > Hardware Wiring** to change the settings after you successfully log in to the platform.
- Click **Download Image** to download the diagram to your computer.

Related Operations

If you want to change the settings of the hardware, go to **System Settings > Hardware Wiring**.

2.2.4 Home Page

After you successfully log in, the home page of the main controller is displayed.

Figure 2-11 Home page

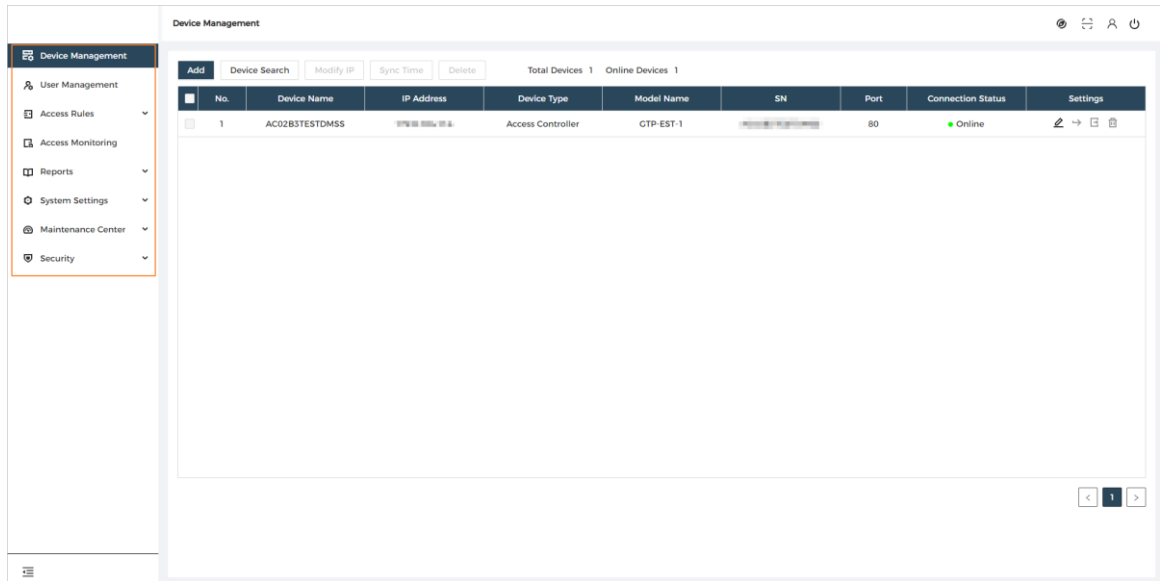


Table 2-4 Home page description

Menu	Description
Device Management	Add devices to the platform of the main controller.
User Management	Add personnel and assign area permissions to them.
Access Rules	Add time templates, create and assign area permissions, configure door parameters and global alarm linkages, and view the permission authorization progress.
Access Monitoring	Remotely control the doors and view event logs.
Reports	View and export alarm records and unlock records.
System Settings	Configure parameters for the local device, such as network and local alarm linkage.
Maintenance Center	Configure packet capturing and run log.
Security	Configure system service, attack defense and CA certificate.

2.2.5 Device Management

You can add devices to the management platform of the main controller in batches or one by one. If the controller was set to the main controller while you were going through the login wizard, you can add and manage sub controllers through the Platform.



Only the main controller comes with a management platform.

2.2.5.1 Adding Devices One by One

You can add sub controllers to the main controller one by one.

Procedure

Step 1 Click **Device Management**, and then click **Add**.

Step 2 Enter the device information.

Figure 2-12 Device information

Table 2-5 Device parameters Description

Parameter	Description
Device Name	Enter the name of the access controller. We recommend you name it after its installation area.
Add Mode	Select IP to add the access controller by entering its IP address.
IP Address	Enter the IP address of the controller.
Port	The port number is 80 by default.
Username	Enter the username and password of the access controller.
Password	

Step 3 Click **OK**.

The added controllers are displayed on the **Device Management** page.

Figure 2-13 Successfully added devices



If the controller was set as the main controller while you were going through the login wizard, the controller will be added to the management platform automatically and function as both the main controller and sub controller.

Related Operations

- : Edit the information on the device.



Only sub controllers support the below operations.

- : Go to the webpage of the sub controller.
- : Log out of the device.
- : Delete the device.

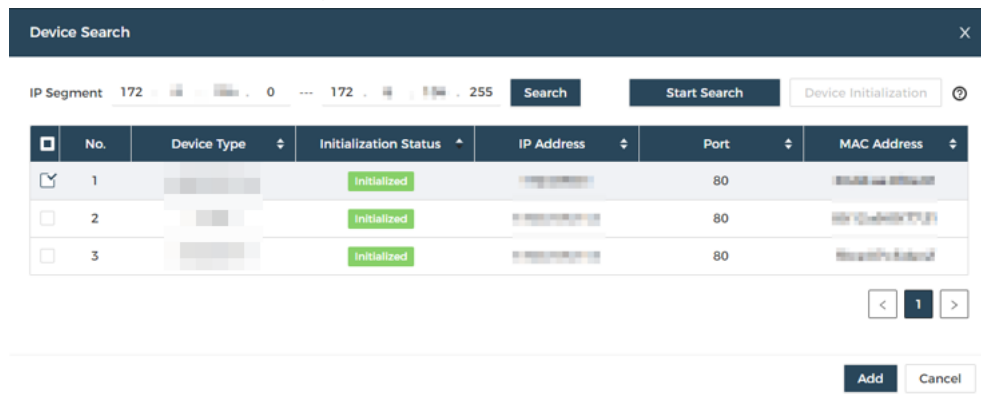
2.2.5.2 Adding Devices in Batches

We recommend you use the auto-search function when you add sub controllers in batches. Make sure the sub controllers you want to add are on the same network segment.

Procedure

- Step 1** Click **Device Management**, and then click **Search Device**.

Figure 2-14 Device search



- Click **Start Search** to search for devices on the same LAN.
- Enter a range for the IP segment, and then click **Search**.

All devices that were searched for will be displayed.



You can select devices from the list, and click **Device Initialization** to initialize them in batches.

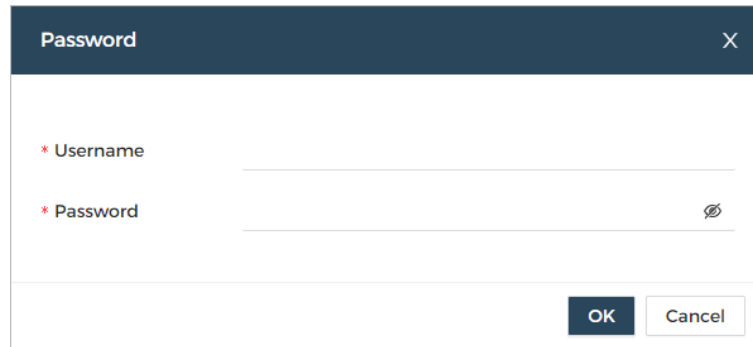


To ensure the security of devices, initialization is not supported for devices on different segments.

- Step 2** Select the access controllers that you want to add to the platform, and then click **Add**.

- Step 3** Enter the username and password of the sub controller, and then click **OK**. The added sub controllers are displayed on the **Device Management** page.

Figure 2-15 Password



Related Operations

- **Modify IP:** Select added devices, and then click **Modify IP** to change their IP addresses.
- **Sync Time:** Select added devices, and then click **Sync Time** to sync the time of the devices with the NTP server.
- **Delete:** Select the devices, and then click **Delete** to delete them.

2.2.6 User Management

Add users to groups. Enter basic information for users and set verification methods to verify their identities.

Related Operations

- **Export all the users to Excel:** On the **User Management** page, click **Export** to export all users. You can also import the exported user information to other controllers.



To prevent data loss caused by force majeure damage to the equipment, it is recommended to regularly export user data for backup purposes.

- **Import users:** On the **User Management** page, click **Import > Download Template**, enter user information in the template, and then click **Import > Import** to import all users.
- **Extract all the users:** On the **User Management** page, click **More > Extract Person Info**, and select a device to extract all the users from the sub controller and send them to them the Platform of the main controller.

2.2.6.1 Adding Group

- Step 1 Select **User Management**.
- Step 2 Click **+**.
- Step 3 Enter the name of the group, and then click **Add**.



The default group cannot be deleted.

Figure 2-16 Add group

2.2.6.2 Configuring Basic User Information

Procedure

Step 1 Select **User Management**.

Step 2 Add users.

- Add users one by one.
 1. Select user group from the left, click **Add**, and then enter the basic information for the user.

Figure 2-17 Basic information on the user

Table 2-6 Parameter description

Parameter	Description
User ID	The ID of the user.
User Name	The name of the user.
Group	The group that the user belongs to. For details on how to create groups, see "2.2.6.1 Adding Group".

Parameter	Description
User Type	<p>The type of user.</p> <ul style="list-style-type: none"> ● General: General users can unlock the door. ● VIP: When the VIP unlocks the door, service personnel will receive a notice. ● Guest: Guests can unlock the door within a defined period or for a defined number of times. After the defined period expires or the number of times for unlocking runs out, they cannot unlock the door. ● Staff: Staff users will have their permissions recognized, but they have no permission to unlock the door. ● Blocklist: When users in the blocklist unlock the door, service personnel will receive a notification. ● Manager: Manager users enjoys the highest permissions, which will not be affected by unlocking mode or door status. ● Other: When they unlock the door, the door will stay unlocked for 5 more seconds.
Valid from	Set the period that the access permissions of the person are effective.
Valid to	
Email	The email address must be the same as the one that was used to sign up for PRO-X.
Use limit	The number of times that a guest user can unlock the door.

2. Click **Add**.

You can click **Add More** to add more users.

- Add users through importing the template.
 1. Click **Import > Download Template** to download the user template.
 2. Enter user information in the template, and then save it.
 3. Click **Import > Import**, and upload the template to the platform.
The users are added to the platform automatically.
- Use **Batch Add** to easily add users.
 1. Click **Batch Add**.
 2. Enter the start number of the user ID, and the number of total users.
The platform will generate a sequence of numbers starting from the defined user ID. For example, if the **User ID** is 001, and the **Total Users** is 5, the system will generate a sequence of numbers from 001 to 005.

Figure 2-18 Batch add

The screenshot shows a 'Batch Add' window with the following fields and controls:

- * User ID: 001
- * Total Users: 5
- Group: Default Group\Group 1 (dropdown)
- Effective Time: 12-25-2024 12:00:00 AM → 12-31-2037 11:59:59 PM (calendar icon)
- Table with columns: User ID, Card Number
- Table rows: 001, 002, 003, 004, 005
- Issue Card Config section:
 - Card Reader: Enrollment Reader (Modify button)
 - Card Number: Press the Enter key to enter. (Start Issuing Cards button)
- Bottom buttons: Add, Cancel

3. Select the group, and set the effective time.
4. Issue cards to the users in batches.
You can manually enter the card number, or use the enrollment reader or card reader to read the card number. For details, see "2.2.6.3.2 Adding Cards".

2.2.6.3 Adding Authentication Methods

Add password, cards, fingerprint or Bluetooth cards to users, so that users can unlock the door through authentication. Each user can have up to 1 password, 5 IC/ID cards, 3 fingerprints, and 5 Bluetooth cards.

2.2.6.3.1 Adding Passwords

Add passwords to users for them to gain access by entering their password.

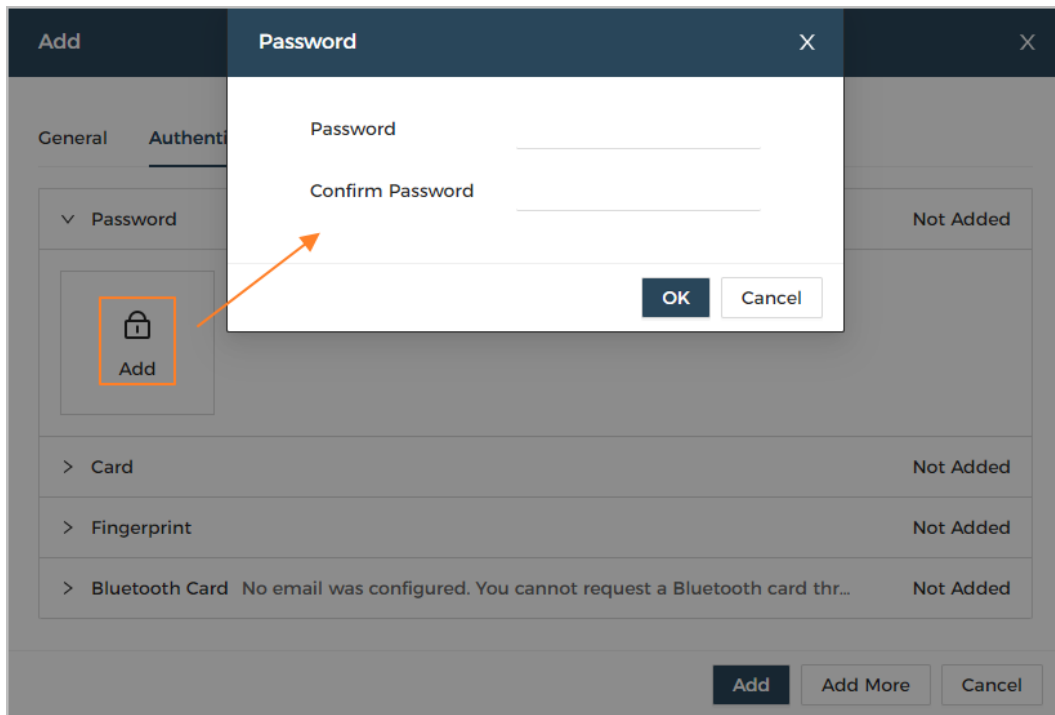
Procedure

Step 1 When adding a user, click the **Authentication** tab.

Step 2 Click **Add**, and then enter and confirm the password.

Step 3 Click **OK**.

Figure 2-19 Add the password



- 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, and then you must enter **123#12345#** to unlock the door.
- 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, and then you must enter **12345#** to unlock the door.

2.2.6.3.2 Adding Cards

Add IC cards or ID cards to users for them to gain access by swiping their cards.

Procedure

Step 1 (optional) Before you assign cards to users, set the card type and the type of card number.

1. On the **User Management** page, select **More > Card Type**.
2. If you plan to issue cards through using enrollment reader, select a card type, and then click **OK**.



Make sure that the card type is the same as the card type that will be issued when you plan on issuing cards through using enrollment reader.

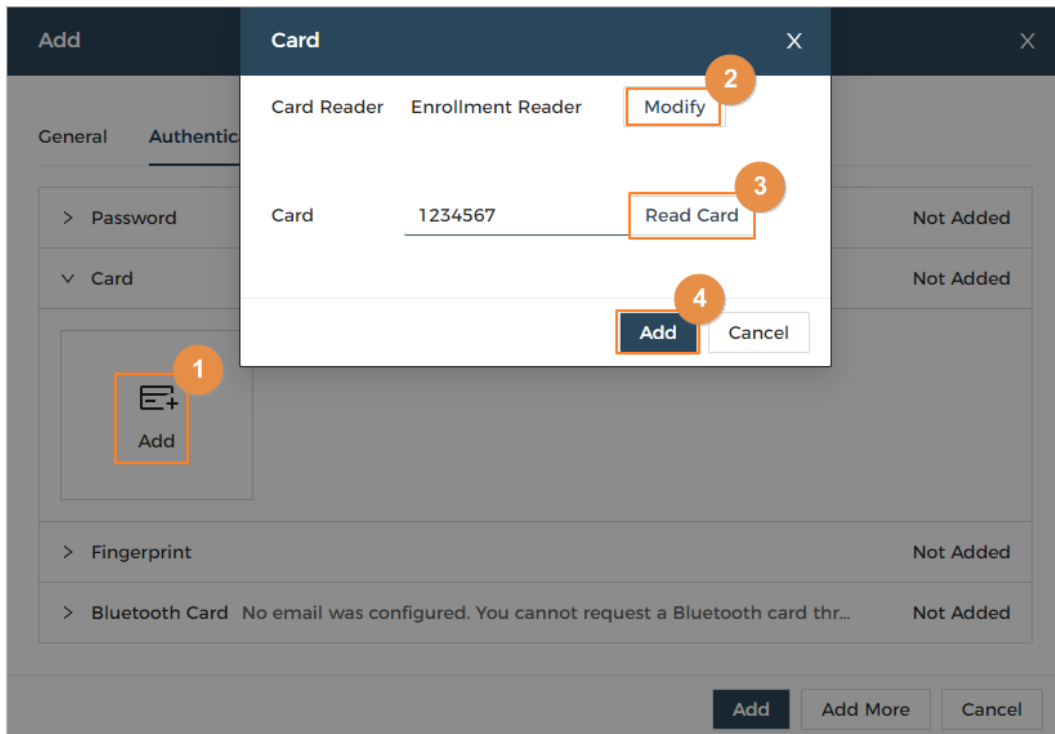
3. Select **More > Card No. System**.
4. Select decimal format or hexadecimal format for the card number.

Step 2 When adding a user, click the **Authentication** tab, and then click **Card** to add cards.

- 4 methods are available to add cards.
 - Enter the card number manually.

1. Click **Add**.
 2. Enter the card number, and then click **Add**.
- Use the enrollment reader to read the card number.

Figure 2-20 Use the enrollment reader to read the card number



1. Click **Add**.
 2. Click **Modify**, and then select **Enrollment Reader**.
Make sure that the card enrollment reader is connected to your computer.
 3. Follow the on-screen instructions to download and install the plug-in.
 4. Click **Read Card**, and then swipe the cards on the enrollment reader.
A 60-second countdown is displayed to remind you to swipe the card, and the system will read the card number automatically. If the 60-second countdown expires, click **Read Card** again to start a new countdown.
 5. Click **Add**.
- Use the card reader to read the card number.
 1. Click **Add**.
 2. Click **Modify**, and then select a card reader.
Make sure that the card reader is connected to the access controller.
 3. Click **Read Card**, and then swipe the cards on the card reader.
A 60-second countdown is displayed to remind you to swipe the card, and the system will read the card number automatically. If the 60-second countdown expires, click **Read Card** again to start a new countdown.
 4. Click **Add**.
 - Add cards in batches: Issue cards to users in batches.
 1. On the **User Management** page, click **Batch Issue Cards**, and then select **Issue Cards to Selected Users** or **Issue Cards to All Users**.
 2. You can manually enter the card number, or click **Modify** to issue cards through the enrollment reader or card reader.

Figure 2-21 Issue cards through the enrollment reader or card reader

The screenshot shows a web interface titled "Batch Issue Cards" with a close button (X) in the top right corner. Below the title, it indicates "Card Bluetooth Card".

The main section is titled "Issue Cards" and contains a table with the following data:

User ID	User Name	Card Number	Hide User
123	123		⊖
124	124		⊖

Below the table, there are user details for User ID 124:

User ID: 124 User Name: 124
User Type: General Email:
Group: Group 1
Effective Time: 2024-12-25 00:00:00-2037-12-31 23:59:59

The "Issue Card Config" section includes:

- Card Reader: Enrollment Reader (with a "Modify" button circled in orange and labeled "1")
- Card Number: Press the Enter key to enter. (with a "Start Issuing Cards" button circled in orange and labeled "2")

At the bottom, there are "OK" and "Cancel" buttons, with the "OK" button circled in orange and labeled "3".

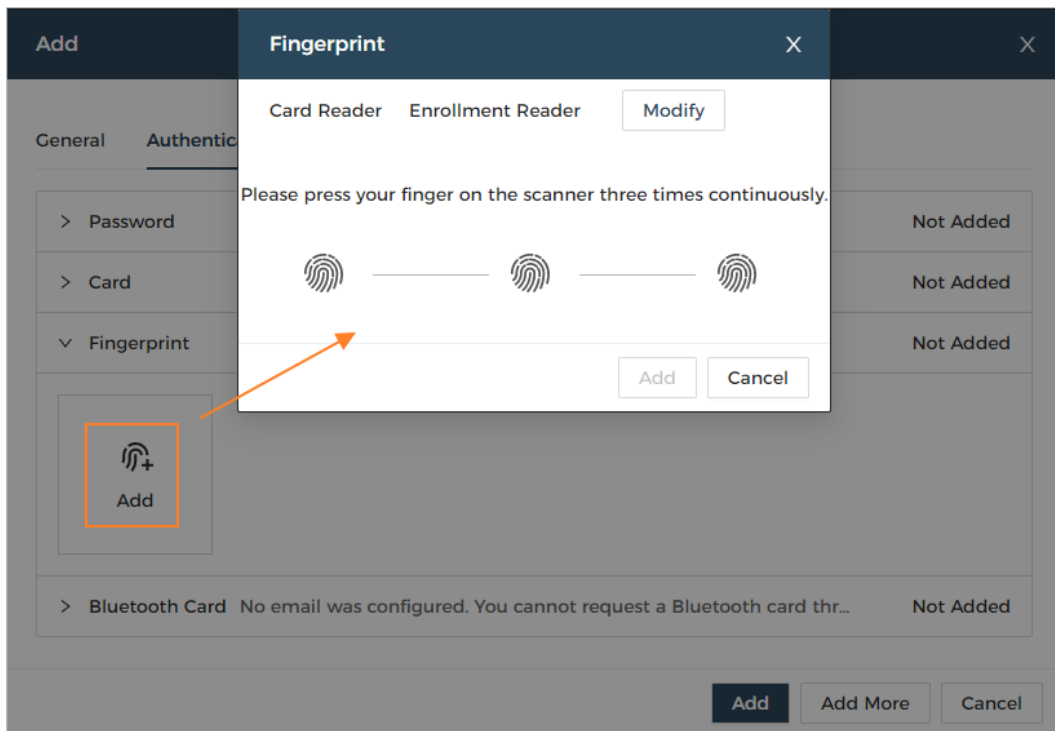
2.2.6.3.3 Adding Fingerprints

Add fingerprints to users for them to use their fingerprints to unlock doors.

Procedure

Step 1 When adding a user, click the **Authentication** tab, and then click **Fingerprint**.

Figure 2-22 Fingerprint



Step 2 Connect a fingerprint scanner to the computer, and follow the on-screen instructions to register the fingerprint.

Step 3 Click **Add**.

2.2.6.3.4 Adding Bluetooth Cards

Add Bluetooth cards to users for them to gain access through Bluetooth cards.

Prerequisites

- The Bluetooth unlock function has been turned on.
- The main controller has been added to PRO-X. For details, see "2.2.10.2.3 Configuring Cloud Service".
- Users have been added to the platform of the access controller.
- General users, such as company employees, have installed and signed up for PRO-X with their email.

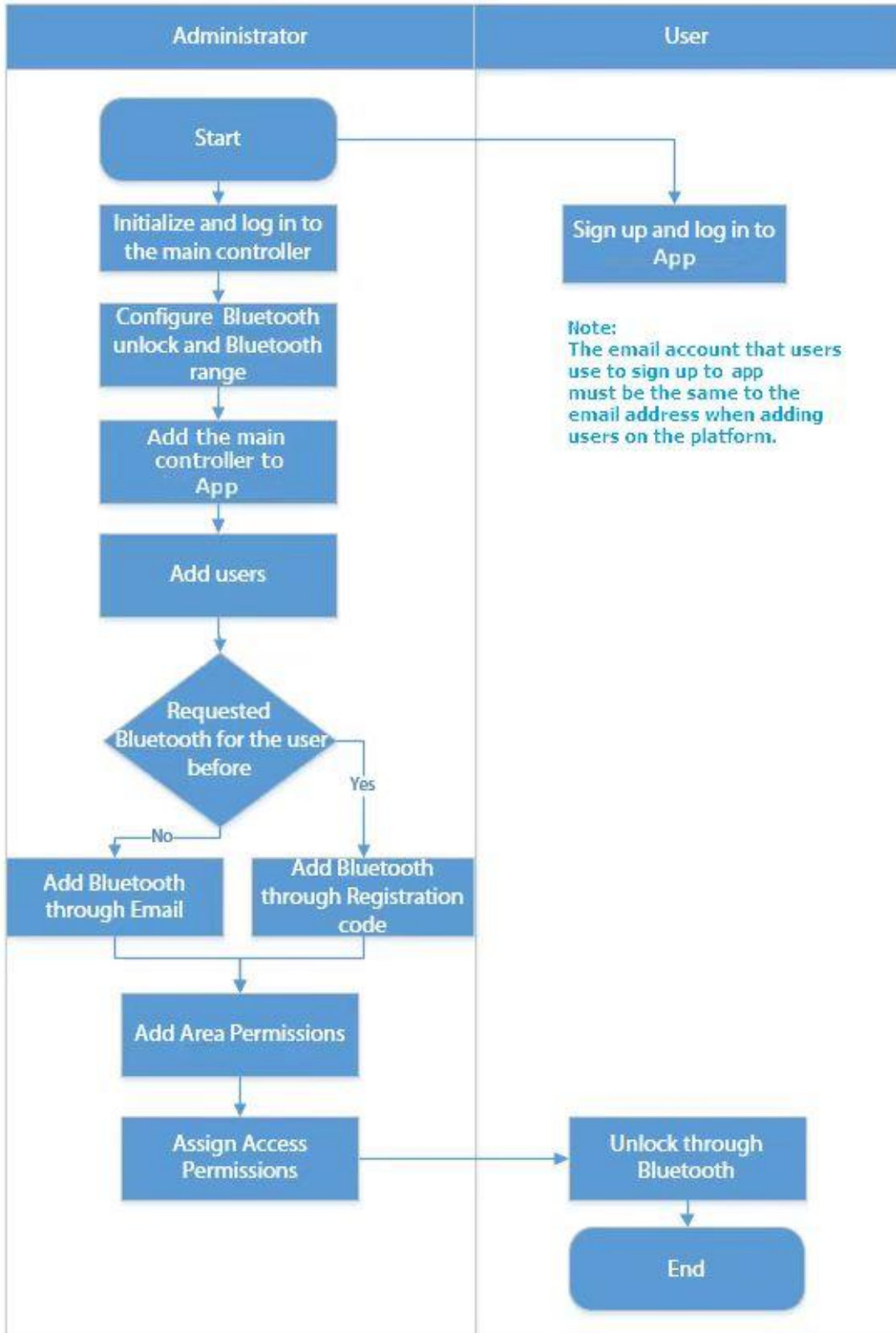


The email that users use to sign up for PRO-X must be the same as the one you used to add them to the access controller.

Background Information

Refer to the flowchart for configuring Bluetooth unlock. Administrator and general users need to perform different operations to complete the process. General users, like company employees, only need to sign up and log in to PRO-X with their email to unlock doors using Bluetooth cards that were issued to them.

Figure 2-23 Flowchart for configuring Bluetooth unlock



Procedure

- Step 1 On the **Authentication** tab, click **Bluetooth Card**.
 3 methods are available to add Bluetooth cards.
- Request through email one by one: Click **Request through Email**.

A Bluetooth card is generated automatically. You can generate up to 5 cards for each user.

- Request through email in batches.
 1. On the **User Management** page, click **Batch Issue Cards**.



Batch issue cards only supports requesting through Email.

- ◇ Issue Bluetooth cards to all the users on the list: Click **Issue Cards to All Users**.
 - ◇ Issue Bluetooth cards to selected users: Select users, and then click **Issue Cards to Selected Users**.
2. Click **Bluetooth Card**.
 3. Click **Request through Email**.



- ◇ Users who do not have an email or already have 5 Bluetooth cards will be displayed on the non-requestable list.
- ◇ Export users that lack emails: Click **Export Users that Lack Emails**, enter the emails in the correct format, and then click **Import**. They will be moved to the requestable list.

Figure 2-24 Batch issue cards

Batch Issue Cards

Card **Bluetooth Card**

Bluetooth cards can only be generated in batches through emails.

Issue Cards

Requestable (2) Non-Requestable (0) Export Users that Lack Emails Import

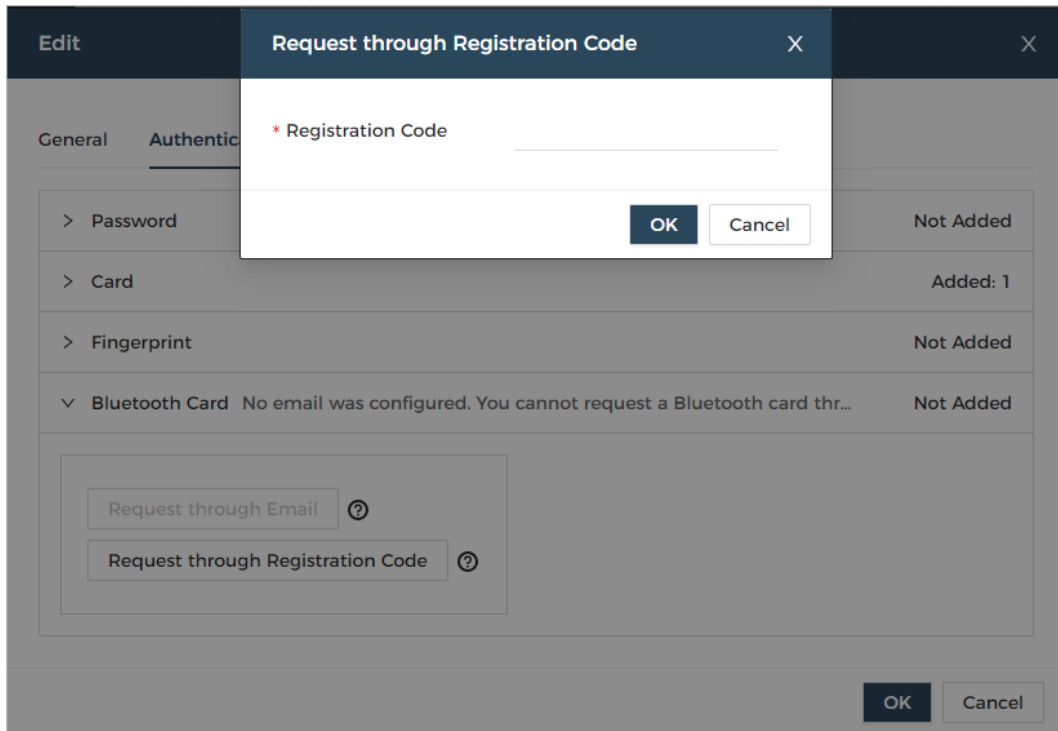
User ID	User Name	Email	Bluetooth Card No.	Status	Settings
123	123	[REDACTED]	0		⊖
124	124	[REDACTED]	0		⊖

User ID 123 User Name 123
User Type General Email
Group Group 1
Effective Time 2024-12-25 00:00:00-2037-12-31 23:59:59

Request through Email

- If you have requested Bluetooth cards for the user before, you can add the Bluetooth cards through registration code.
 1. On PRO-X, tap **Registration Code** of a Bluetooth card.
The registration code is automatically generated by PRO-X.
 2. Copy the registration code.
 3. On the **Bluetooth Card** tab, click **Request through Registration Code**, paste the registration code, and then click **OK**.

Figure 2-25 Request through registration code



4. Click **OK**.

The Bluetooth card is added.

Step 2 Click **OK**.

Result

After users sign up and log in to PRO-X with the Email address, they can open PRO-X to unlock the door through Bluetooth cards. For details, see the user's manual of PRO-X.

- Auto unlock: The door automatically unlocks when you are in the defined Bluetooth range, which allows the Bluetooth card to transmit signals to the card reader.



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: The door unlocks when you shake your phone to allow the Bluetooth card to transmit signals to the card reader.

Related Operations

- Users can manage Bluetooth cards on PRO-X.
 - ◇ Move to the Top: If multiple Bluetooth cards have been added, you can move cards to the top that are currently in use.
 - ◇ Rename: Rename the Bluetooth card.
 - ◇ Delete: Delete the Bluetooth card.
- Export users that lack emails: Click **Export**, enter the emails in the correct format and then click **Import**. They will be moved to the requestable list.
- View the request records: On the **User Management** page, select **More > Bluetooth Card Records** to view the request status.

- ◇ **View Details:** View the details of the request, including user information, reasons for failed requests and more. You can also request again for failed users.
- ◇ **Request Again:** Request again for failed users.

2.2.7 Access Rules

2.2.7.1 Adding Weekly Plans


The weekly plan is used to set the unlock schedule for the week. The platform offers a default template with a full daytime schedule. You can also create your own templates.

Procedure

Step 1 Select **Access Rules > Weekly Plan**, and then click **Add**.



- The default full-day time template cannot be modified.
- You can create up to 128 weekly plans.

Step 2 Click  to edit the time template.

- 1) Define the name of the weekly plan.
- 2) Click on the date that you want to set (for example, **Mon**), and then drag the slider to adjust the time period for each day.

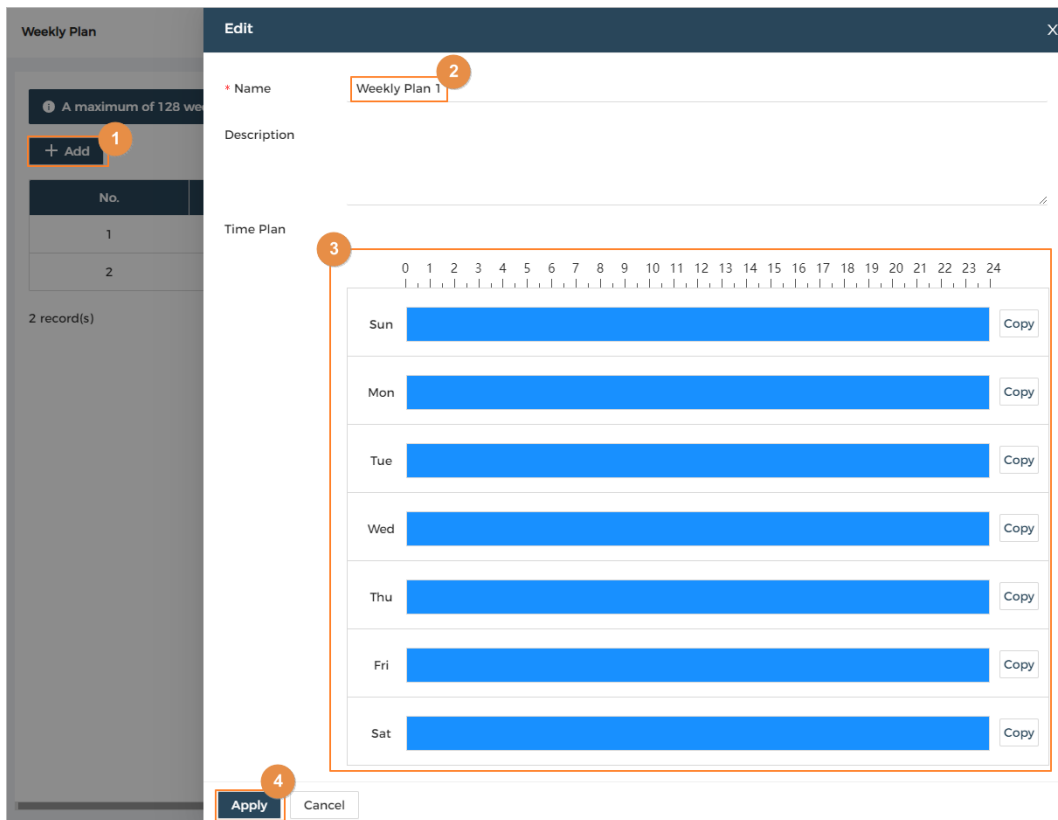
You can also click **Copy** to apply the configured time period to other days.



You can only configure up to 4 periods for each day.

- 3) Click **Apply**.

Figure 2-26 Add the weekly plan



2.2.7.2 Adding Holiday Plans (Optional)


The holiday plan is used to set the unlock schedule for holidays.

Procedure

Step 1 Select **Access Rules > Holiday Plan**, and then click **Add**.



You can create up to 128 holiday plans.

Step 2 Click  to edit the time template.

- 1) Define the name of the holiday plan.
- 2) Click on the time plan bar, and then drag the slider to adjust the time period.



You can only configure up to 4 periods on the time plan bar.

Figure 2-27 Add holiday plan

Holiday Plan Edit

A maximum of 128 holiday plans can be created.

Details

Name: Holiday Plan 1

Description:

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.	Name	Type	Date	Settings
No data				

Apply Cancel

3) Click **Add** to add holidays to the holiday plan, and then click **OK**.

- **Name:** Define the name of the holiday, such as National Day.
- **Start Time, Duration:** Set the date that the holiday begins, and then duration of the holiday.
- **Type:** By selecting **Public**, the holiday will be shared with all your holiday plans; if you select **Custom**, it means that the holiday is only used on the current holiday plan.

Figure 2-28 Add holidays

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- * Name**: A text input field.
- * Start Time**: A date input field showing "12-25-2024" with a calendar icon to its right.
- Duration**: A text input field showing "1" followed by the label "Days".
- Type**: A section with a help icon (?) and two radio buttons: "Public" (which is selected) and "Custom".

At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

Step 3 Click **Apply**.

2.2.7.3 Adding Zone

A zone is a collection of door access permissions. Create a zone, and then link users to the zone so that they can gain access permissions set for the zone.

Procedure

Step 1 Select **Access Rules > Zone Settings**.

Step 2 Click **Add** to add zones.

You can add up to 40 zone permissions.

Figure 2-29 Add zones

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- * Zone Name**: A text input field containing "Zone1".
- Door List**: A section with a search bar and a magnifying glass icon. Below the search bar, there are two entries, each with a checkbox and a door icon:
 - Entry 1: [Door Icon] A [blurred text]
 - Entry 2: [Door Icon] 1 [blurred text]

Step 3 Enter the name of the zone.

Step 4 Select doors.

Step 5 Click **OK**.

2.2.7.4 Adding Permission Rules

By creating permissions rules, you can assign access permissions to users by linking them to the zones. This will allow authorized personnel to gain access to secure zones.

Procedure

Step 1 Select **Access Rules > Permission Settings**.

Step 2 Click **Add** to add a permission rule.

Figure 2-30 Assign permissions in batches

Step 3 Enter the name of the permission rule.

Step 4 Select the weekly plan and the holiday plan.

Step 5 In the **User Info** section, click **Add** to select user, and then click **OK**.

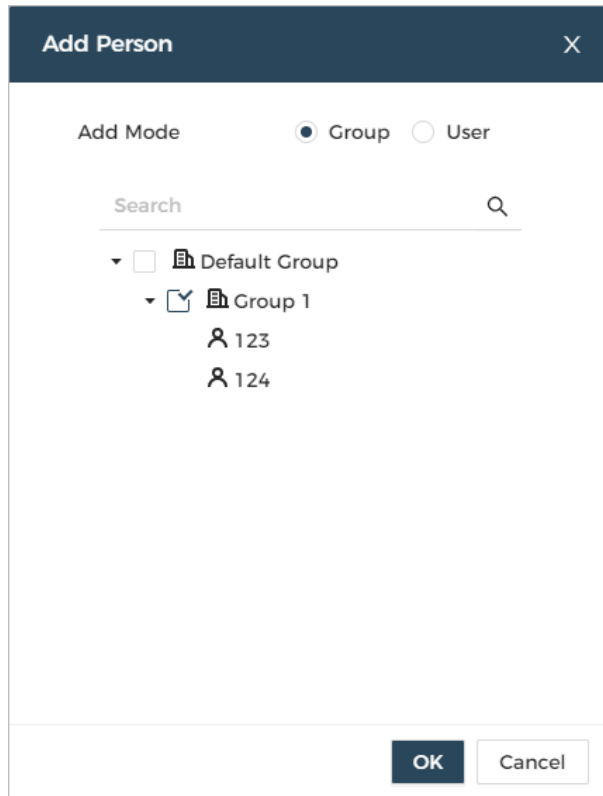
You can select users by group or by user.

- Group: All users in the group will be assigned with access permissions.
- User: Only selected users will be assigned with access permissions.



When you want to assign permission to a new person or change access permissions for an existing person, you can simply add the user in an existing group, they will be automatically assigned access permissions defined for the group.

Figure 2-31 Add person



Step 6 In the **Zone Info** section, click **Add** to select a zone, and then click **OK**.

Step 7 Click **Apply**.

2.2.7.5 Viewing Data Synchronization Progress

After you assign access permissions to users, you can view the data synchronization process.

Procedure

Step 1 Go to **Access Rules > Data Sync**.

Step 2 View the data synchronization progress.

Figure 2-32 Data synchronization progress

Time	Zone Permission	Device Name	Details	Results	Settings
12-25-2024 04:29:06 PM	A	SS	Sync Person Info to Main Controller	2, 0, 0	
12-25-2024 04:22:28 PM	A	SS	Sync Person Info to Main Controller	2, 0, 0	
12-25-2024 04:05:05 PM	A	SS	Sync Person Info to Main Controller	1, 0, 0	
12-25-2024 04:04:45 PM	A	SS	Sync Person Info to Main Controller	1, 0, 0	
12-25-2024 04:02:14 PM	A	SS	Sync Person Info to Main Controller	1, 0, 0	
12-25-2024 04:02:04 PM	A	SS	Sync Person Info to Main Controller	1, 0, 0	

2.2.7.6 Configuring Access Control (Optional)

2.2.7.6.1 Configuring Basic Parameters

Procedure

Step 1 Go to **Access Rules > Door Parameters**.

Step 2 Select the door from the list on the left, and then in the **Basic Settings** section, configure basic parameters for the access control.

Figure 2-33 Basic parameters

Table 2-7 Basic parameters description

Parameter	Description
Name	The name of the door.
Unlock Type	<ul style="list-style-type: none"> ● Fail Secure: Locks remain locked during power outage. ● Fail Safe: Set locks to lock during power outage.
Door Status	Set the door status. <ul style="list-style-type: none"> ● Normal: The door will be unlocked and locked according to your settings. ● Always Unlocked: The door remains unlocked all the time. ● Always Locked: The door remains locked all the time.
Keep Door Unlocked for	The door remains unlocked during the defined weekly plan or holiday plan.
Keep Door Locked for	The door remains locked during the defined weekly plan or holiday plan.
Holiday Plan Authentication	Authorized access is allowed for always closed door in the defined holiday plan.
Public Unlock Password	Enable this function, enter a password, and then you can unlock the door by only entering the public password.

2.2.7.6.2 Configuring Unlock Methods

You can use multiple unlock methods to unlock the door, such as Bluetooth card, fingerprint, card, and password unlock. You can also combine them to create your own personal unlock method.

Procedure

Step 1 Go to **Access Rules > Door Parameters**.

Step 2 Select the door from the list on the left, and then in the **Unlock Settings** section, select an unlock mode.

- Combination unlock
 1. Select **Combination Unlock** from the **Unlock Mode** list.
 2. Select **Or** or **And**.
 - ◇ **Or:** Use one of the selected unlocking methods to unlock the door.
 - ◇ **And:** Use all the selected unlocking methods to unlock the door.




Bluetooth card cannot be selected when you set the combination method to **And**.

3. Select unlock methods, and then configure other parameters.

Figure 2-34 Unlock settings

Unlock Settings	
Unlock Mode	Combination Unlock ▼
Combination Method	<input checked="" type="radio"/> Or <input type="radio"/> And
Unlock Method (Multi-select)	<input checked="" type="checkbox"/> Card <input type="checkbox"/> Password <input type="checkbox"/> Bluetooth Card <input type="checkbox"/> Fingerprint
Bluetooth Mode	<input type="radio"/> Short-range <input checked="" type="radio"/> Mid-range <input type="radio"/> Long-range
Door Unlock Duration	3.0 s (0.2-600)
Unlock Timeout	60 s (1-9999)

Table 2-8 Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	Supports unlocking through card, fingerprint, password or Bluetooth card. The Bluetooth card function is turned off by default.
Bluetooth Mode	<p>The Bluetooth card must be a certain distance away from the access control device to exchange data and unlock the door. The following includes the ranges that are most suitable for it.</p> <ul style="list-style-type: none"> • Short-range: The Bluetooth unlock range is less than 0.66 ft (0.2 m). • Mid-range: The Bluetooth unlock range is less than 6.56 ft (2 m). • Long-range: The Bluetooth unlock range is less than 32.81 ft (10 m). <p> The Bluetooth unlock range might differ depending on models of your phone and the environment.</p>
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through. It ranges from 0.2 seconds to 600 seconds.
Unlock Timeout	A timeout alarm is triggered when the door remains unlocked for longer than the defined value.

- Unlock by period
 1. Select **Unlock by Period** from **Unlock Mode**.
 2. Drag the slider to adjust time period for each day.



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

3. Select an unlock method for the time period, and then configure other parameters.



You can only configure up to 4 time sections for each day.

Figure 2-35 Unlock by period

Step 3 Click **Apply**.

2.2.7.6.3 Configuring Alarms

An alarm will be triggered when an abnormal access event occurs.

Procedure

Step 1 Go to **Access Rules > Door Parameters > Alarm Settings**.

Step 2 Configure alarm parameters.

Figure 2-36 Alarm settings

Table 2-9 Description of alarm parameters

Parameter	Description
Duress Alarm	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.

Parameter	Description
Door Sensor	Select the type of door detector.
Intrusion Alarm	<ul style="list-style-type: none"> When door detector is enabled, an intrusion alarm will be triggered if the door is opened abnormally. A timeout alarm will be triggered if the door remains unlocked longer than the defined unlock time. When Card reader beeps is enabled, the card reader beeps when the intrusion alarm or timeout alarm is triggered.
Unlock Timeout Alarm	

Step 3 Click **Apply**.

2.2.7.7 Configuring the Password Unlock

When the PIN Code Authentication is enabled, people can unlock the door by simply entering the password.

Background Information



- 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, and then you must enter **123#12345#** to unlock the door.
- 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, and then you must enter **12345#** to unlock the door.

Procedure

Step 1 Go to **Access Rules > PIN Code Unlock**.

Step 2 Turn on **PIN Code Authentication**, and then click **Apply**.



There are some safety risks in enabling PIN code authentication. When it is turned on, the user types become ineffective, and the following situations occur.

- First-card holders and users in multi-person unlock groups need to verify their identities through the defined unlock methods, except password. If they verify through password, the first-person unlock or multi-person unlock function will become ineffective.
- Users need to verify their through defined unlock methods except password. If they gain access through password, the anti-passback function will become ineffective.
- Patrol users and block-listed users can simply enter their password to unlock the door.
- Frozen and expired accounts can still unlock doors by simply entering their password.
- When the password unlock method is disabled at the same time, all types of users cannot unlock the door using their password.

2.2.7.8 Configuring Global Alarm linkages (Optional)

You can configure global alarm linkages across different access controllers.

Procedure

Step 1 Go to **Access Rules > Global Alarm Linkage**.

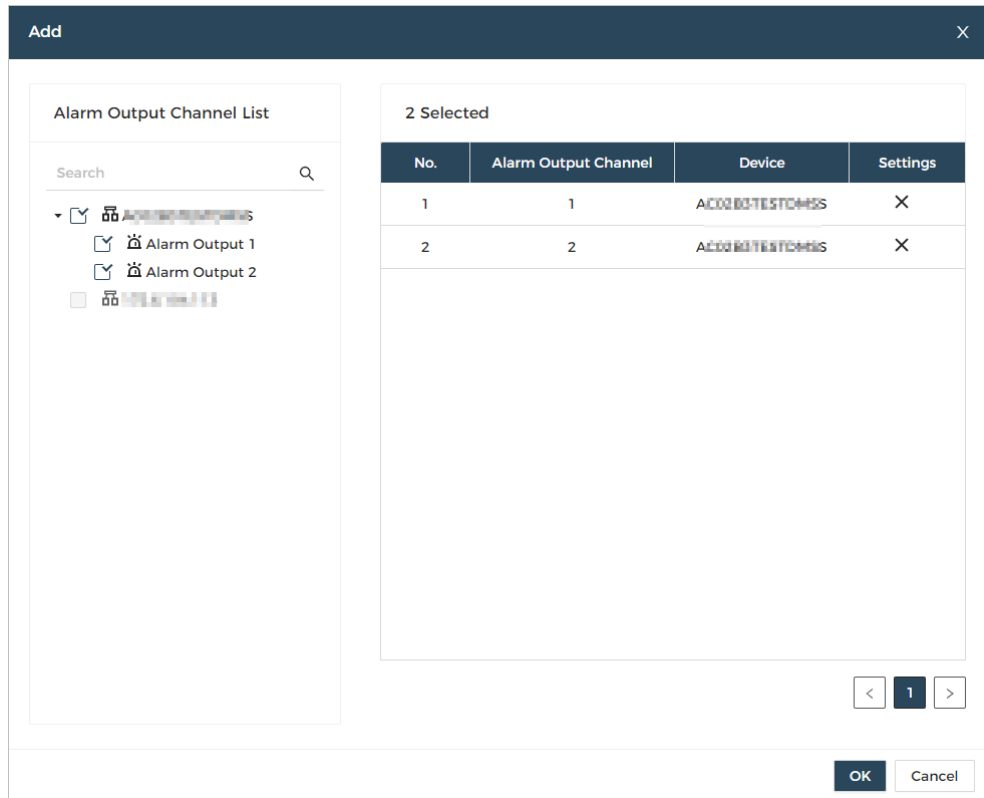


- When you have configured both global alarm linkages and local alarm linkages, and if the global alarm linkages conflict with the local alarm linkages, the last alarm linkages you have configured will take effective.
- When you have configured alarm linkages for sub controllers through the main controller, if the main controller has been restored to the factory defaults, we recommended you restore the sub controller to factory defaults at the same time.

Step 2 Configure the alarm output.

1. Select an alarm input from the alarm input channel list, and then click **Link Alarm Output**.
2. Click **Add**, select an alarm output channel, and then click **OK**.

Figure 2-37 Alarm output

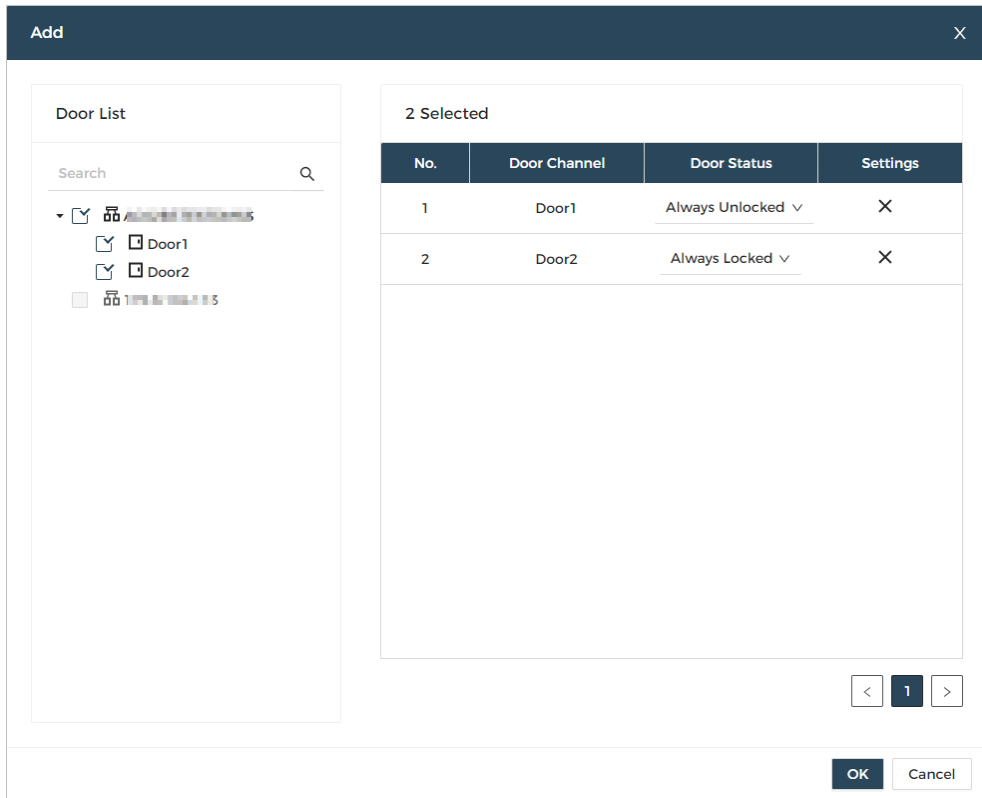


3. Turn on the alarm output function and then enter the alarm duration.
4. Click **Apply**.

Step 3 Configure the door linkage.

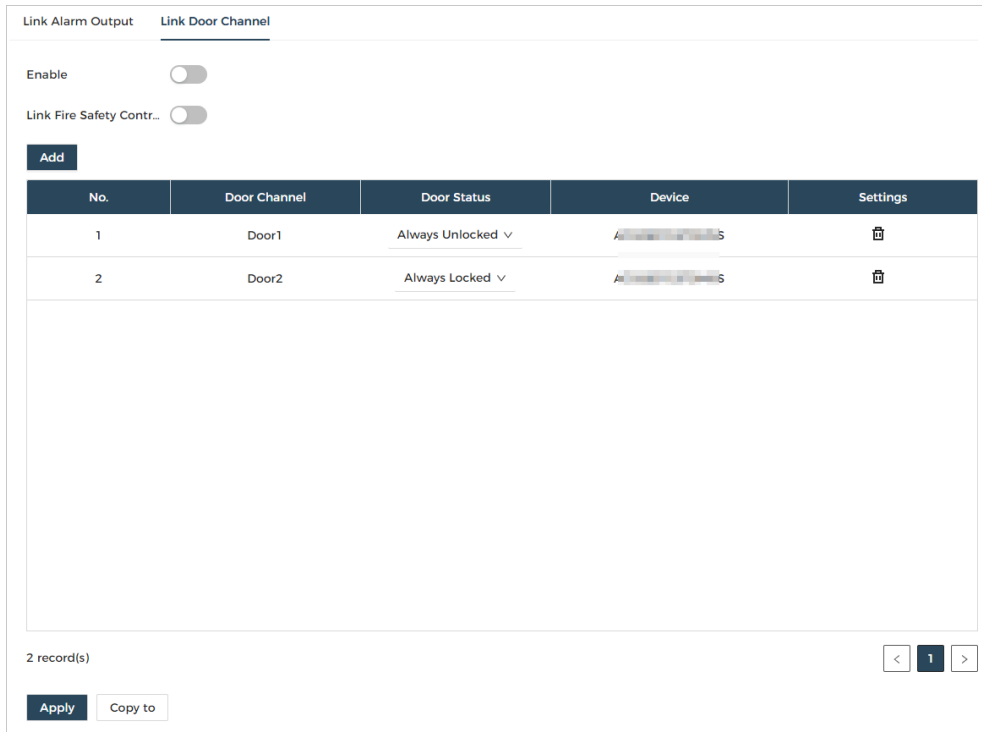
1. Click the **Link Door Channel** tab.
2. Select an alarm input from the channel list, and then click **Add**.
3. Select the linkage door, select the door status, and then click **OK**.
 - **Always Unlocked**: The door automatically unlocks when an alarm is triggered.
 - **Always Locked**: The door automatically locks when an alarm is triggered.

Figure 2-38 Door linkage (1)



4. Click **Enable** to turn on the door linkage function.

Figure 2-39 Door linkage (2)



If you turn on link fire safety control, all door linkages will automatically change to the **Always Unlocked** status, and all the doors will open when the fire alarm is triggered.

5. Click **Apply**.

You can click **Copy to** to apply the defined alarm linkages to other alarm input channels.

2.2.7.9 Configuring First-Person Unlock

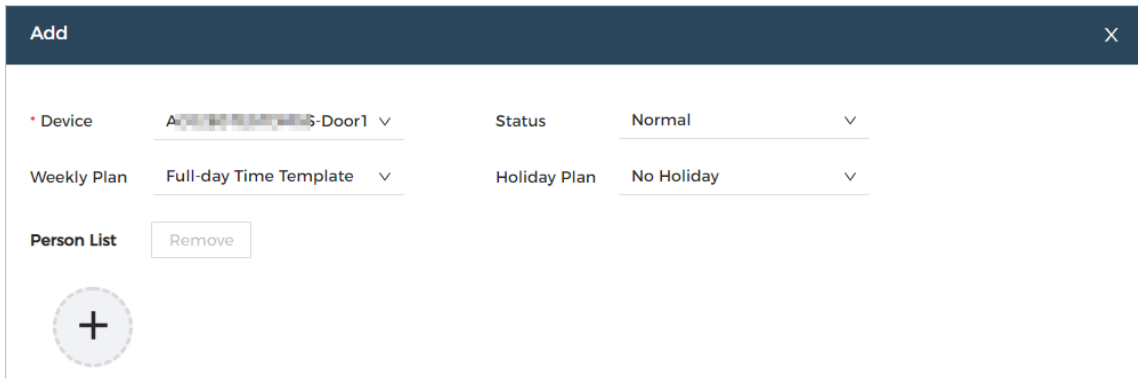
Define certain people as the first-card holders, other users can verify their identities to unlock the door only after the first-card holders verify their identities first.

Procedure

Step 1 Go to **Access Rules > First-person Unlock**.

Step 2 In the device list, click **Add**, and then select the door.

Figure 2-40 Assign first-card permissions to users



The screenshot shows a configuration window titled "Add" with a close button (X) in the top right corner. The window contains the following fields and controls:

- Device:** A dropdown menu showing "A-Door1" with a downward arrow.
- Status:** A dropdown menu showing "Normal" with a downward arrow.
- Weekly Plan:** A dropdown menu showing "Full-day Time Template" with a downward arrow.
- Holiday Plan:** A dropdown menu showing "No Holiday" with a downward arrow.
- Person List:** A section with a "Remove" button and a large circular button with a plus sign (+) for adding users.

Step 3 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 unlocked after first-card users grant access on the access controller.

Step 4 Select the weekly plan and the holiday plan.

First-card is valid only during the defined time.


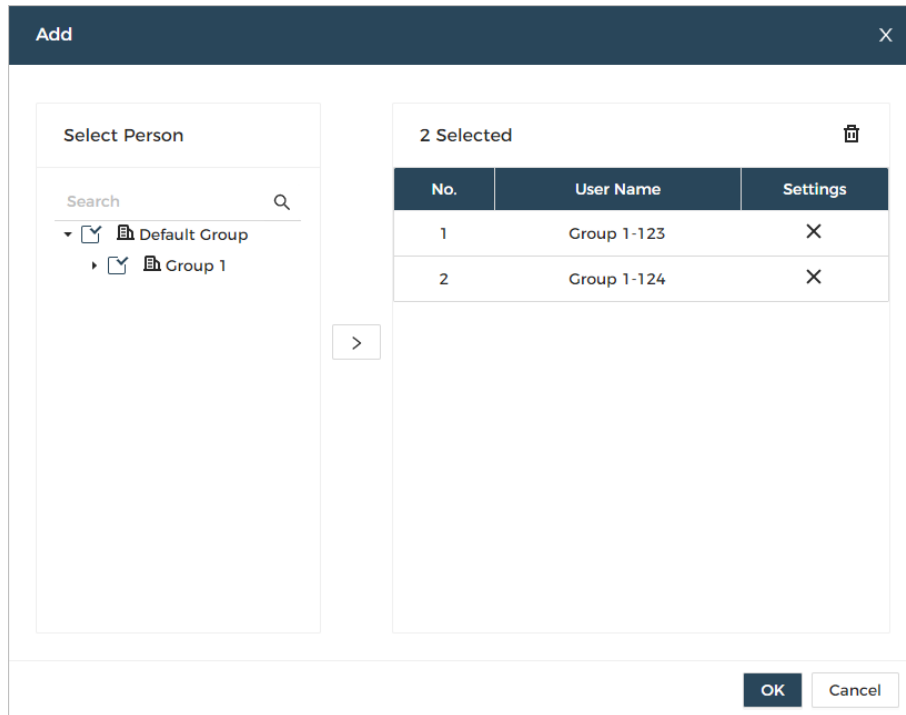
Step 5 Click  to add first-card users, and then click **OK**.

Figure 2-41 Add first-card users



2.2.7.10 Configuring Multi-Person Unlock

Users must verify their identities on the access controller in an established sequence before the door unlocks.

Background Information

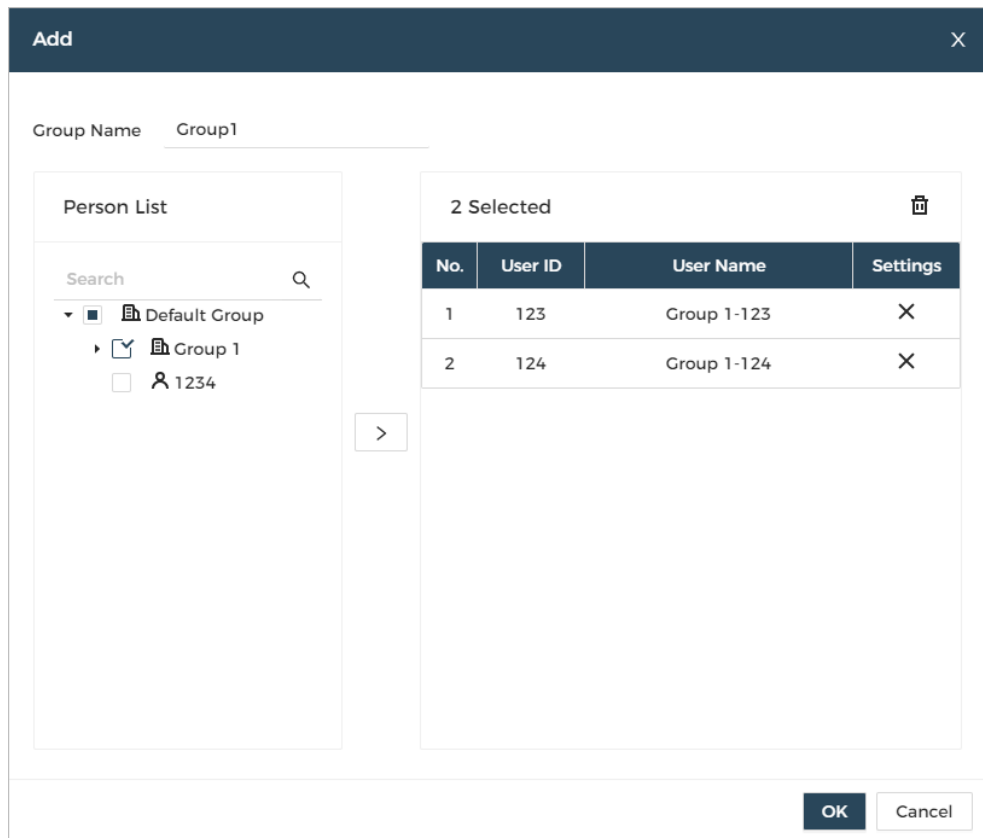


We do not recommend you add first-card users into groups of multi-person unlock.

Procedure

- Step 1 Go to **Access Rules > Multi-person Unlock**.
- Step 2 Click **Add** to add doors to the device list.
- Step 3 Click **Add Person Groups**, and then click **Add** to add groups of multi-person unlock.
 1. Create a name for the group.
 2. Select users from the user group.
 3. Click **OK**.

Figure 2-42 Add groups



Step 4 Select a door, and then click **Add Person Groups**.

Step 5 Select groups, and then click **OK**.



You can add up to 4 groups for each door. Each group can have up to 50 users.

Step 6 Configure the parameters of multi-person unlock.

1. Enter the valid No.



The valid No. indicates the number of people in each group who need to verify their identities on the access controller before the door unlocks. For example, if the valid No. is set to 2 for a group, any 2 people from the group need to verify their identities to unlock the door.



The valid number ranges from 1 to 5 in each group.

2. Select the unlock method.

Users in the group must verify their identities through the defined unlock methods.

3. (Optional) Click  or  to change the sequence of groups.

If more than one groups are added, users must verify their identities according to the defined sequence of groups.

Figure 2-43 Configure multi-person unlock

The screenshot shows a configuration interface for multi-person unlock. At the top, there is a dark blue header with the word "Add". Below the header, the device is identified as "AC02B3TESTDMSS-Door1". The configuration is organized into two main sections, labeled "1" and "2".

Section 1, "Group1(2)", includes a "Valid No." field with the value "1", two person icons with IDs "123: 123" and "124: 124", and an "Unlock Method" dropdown menu set to "Card/Password/Fingerpr...". To the right of the dropdown is a control panel with up, down, and delete icons.

Section 2, "Group2(1)", includes a "Valid No." field with the value "1", one person icon with ID "1234: 1234", and an "Unlock Method" dropdown menu set to "Card/Password/Fingerpr...". It also has a control panel with up, down, and delete icons.

At the bottom of the configuration area, there is a button labeled "+ Add Person Groups". At the very bottom of the page, there are "Apply" and "Cancel" buttons.

Step 7 Click **Apply**.

2.2.7.11 Configuring Anti-Passback

Users need to verify their identities both for entry and exit; otherwise, an anti-passback alarm will be triggered. It prevents a card holder from passing an access card back to another person so they gain entry. When anti-passback is enabled, the card holder must leave the secure area before the system will grant another entry.

Background Information

- If a person enters after being authorized and exits without being authorized, an alarm will be triggered when they attempt to enter again, and access is denied at the same time.
- If a person without being authorized and exits after being authorized, an alarm will be triggered when they attempt to enter again, and access is denied at the same time.



- When you have configured anti-passback for sub controllers through the main controller, and you plan on restoring the main controller to its factory defaults, we recommend you also restore the sub controller to its factory defaults at the same time.
- If the anti-passback rule is used when the network is not stable, the door might open after an identity is verified, but a time-out alarm might be triggered on the card reader. Please make sure your network is stable.

Procedure

Step 1 Go to **Access Rules > Anti-passback**.

Step 2 Turn on the **Reset Anti-Passback** function, and then select a reset time. Specify a time when the anti-passback status of all personnel will be reset.

Figure 2-44 Global configuration

The screenshot shows the 'Global Config' tab for 'Anti-passback'. At the top, there are three tabs: 'Anti-passback', 'Global Config' (selected), and 'Anti-passback Group List'. Below the tabs is a dark blue information banner that reads: 'Anti-passback will reset at the specified time, resetting access for affected users.' Underneath, there is a 'Reset Anti-Passback' toggle switch which is currently turned off. Below the toggle is a 'Reset Time' field set to '00:00:00' with a dropdown arrow. At the bottom, there are three buttons: 'Apply' (highlighted in dark blue), 'Refresh', and 'Default'.

Step 3 Click **Anti-passback Group List**, and then click **Add** to add an anti-passback group.

Figure 2-45 Configure anti-passback

The screenshot shows the 'Add' dialog for configuring an anti-passback group. The dialog has a dark blue header with 'Add' and a close button. The main content area is divided into two sections. The top section contains form fields for 'Name' (set to 'Anti-passback Group 1'), 'Reset Time' (set to '60 min (5-1440)'), 'Weekly Plan' (set to 'Full-day Time Template'), 'Execution' (set to 'Strong Execution'), and 'Holiday Plan' (set to 'No Holiday'). The bottom section, titled 'Anti-passback Group Config', shows two existing groups, 'Group 1' and 'Group 2', each with a trash icon and an 'Add' button. To the right of these groups is a dashed box containing a plus sign and the text 'Add Door Groups'. At the bottom of the dialog are 'Apply' and 'Cancel' buttons.

Step 4 Create a name for the anti-passback group, enter a reset time, and then select the execution mode.

Set a time period when the anti-passback alarm will be triggered. For example, if the reset time is set to 60 minutes, when a person enters after being authorized, and exits without being authorized, if they attempt to enter again in 60 minutes, an anti-passback alarm will be triggered.

- **Strong Execution:** The sub controller and main controller perform the anti-passback function even when they go offline.
- **Weak Execution:** The sub controller and main controller do not perform the anti-passback function when they go offline.

Step 5 Select the weekly plan and the holiday plan.

Anti-passback is effective during the defined time.

Step 6 In group 1, click **Add**, and then select card readers.

Step 7 In group 2, click **Add**, and then select card readers.



At least 2 groups must be added.

Step 8 (Optional) You can click **Add Door Groups** to add more groups.

You can add more than one readers in a group, and users can swipe at any one of the readers to gain access.

Step 9 Click **Apply**.

Result

The group number indicates the sequence of swiping cards. Card must be used following the specific sequence of groups. For example, you must swipe card at a reader in group 1, and then at a reader for group 2, and then at a reader in group 3, and more. As long as you swipe card following the established sequence, the system works fine.

2.2.7.12 Configuring Multi-Door Interlock

Multi-door interlock controls the locking of two or more doors. If one door is unlocked, access will be

prohibited for the remaining doors.



- When you have configured multi-door interlock for sub controllers through the main controller, and you plan on restoring the main controller to its factory defaults, we recommend you also restore the sub controller to its factory defaults at the same time.
- If the multi-door interlock rule is used when the network is not stable, the door might open after an identity is verified, but a time-out alarm might be triggered on the card reader. Please make sure your network is stable.

2.2.7.12.1 Configuring Interlock within a Group

If any doors in a group is opened, the other doors in the group cannot be unlocked.

Procedure

- Step 1 Go to **Access Rules > Interlock > Interlock within Group**.
- Step 2 Click **Add**, and then add an interlock group.
- Step 3 Create a name for the interlock group, and then select the execution mode.
- **Strong Execution:** The sub controller and main controller perform the interlock function even when they go offline.
 - **Weak Execution:** The sub controller and main controller do not perform the interlock function when they go offline.
- Step 4 Click **Add** to add doors in a device group.



At least 2 doors must be added to a group.

Figure 2-46 Interlock within a group

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields and sections:

- Name:** Interlock within Group 1
- Execution:** Strong Execution (with a dropdown arrow and a help icon)
- Device Group Config:** A section with a help icon containing:
 - Device Group:** Group 1
 - A large empty box with the text "No data" and an "Add" button centered inside it.
- Buttons:** "Apply" and "Cancel" buttons at the bottom.

Step 5 Click **Apply**.

Result

After a person's identity has been verified and they opened the door, they have to close the door behind them first before they can open the next door.

2.2.7.12.2 Configuring Interlock between Groups

If any doors in a group is unlocked, the doors in the other groups cannot open.

Procedure

Step 1 Go to **Access Rules > Interlock**, and then click **Interlock between Groups**.

Step 2 Click **Add**, and then add an interlock group.

Figure 2-47 Interlock between groups

The screenshot shows a configuration window titled "Add". At the top, there is a dark blue header with the text "Add" and a close button (X). Below the header, the "Name" field is set to "Interlock between Groups 1". The "Execution" dropdown menu is set to "Strong Execution". Underneath, there is a section titled "Device Group Config" with a help icon. This section contains two columns, "Group 1" and "Group 2", each with a "No data" message and an "Add" button. At the bottom of the window, there are "Apply" and "Cancel" buttons.

- Step 3** Create a name for the interlock group, and then select the execution mode.
- **Strong Execution:** The sub controller and main controller perform interlock function even when they go offline.
 - **Weak Execution:** The sub controller and main controller do not perform interlock function when they go offline.

Step 4 In group 1, click **Add** to add doors to the group.

Step 5 In group 2, click **Add** to add doors to the group.

Step 6 Click **Apply**.

Result

If any doors in one group is unlocked, the doors in the other group cannot open.

2.2.8 Access Monitoring

2.2.8.1 Remotely Locking and Unlocking Doors

You can remotely monitor and control the door through platform. For example, you can remotely lock

or unlock the door.

Procedure

Step 1 Select **Access Monitoring**.



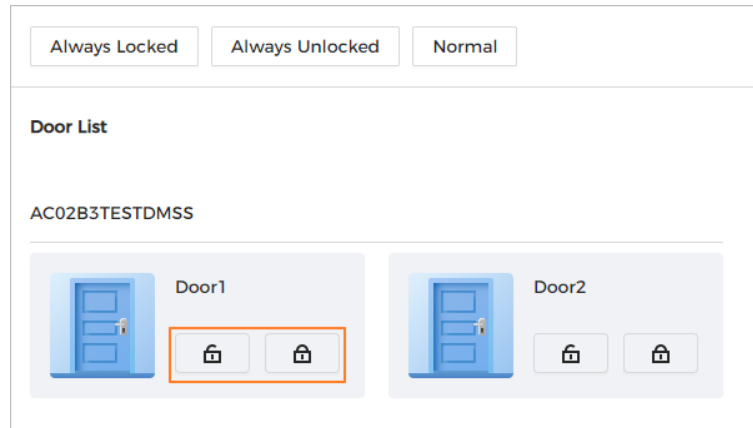

Step 2 Click  or  to remotely unlock or lock the door.

Figure 2-48 Remotely control the door



Related Operations

- Filter events: Select the event type in **Event Info**, and the event list displays the selected event types, such as alarm events and abnormal events.
- Delete events: Click  to clear all events from the event list.

2.2.8.2 Setting Always Locked and Always Unlocked

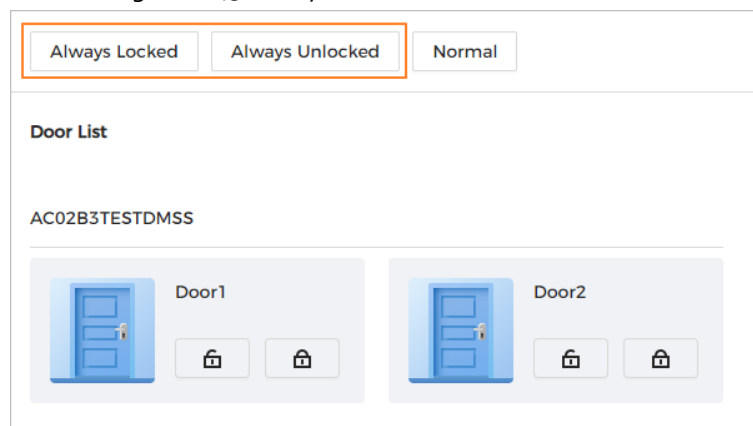
After setting always locked or always unlocked, the door remains locked or unlocked all the time.

Procedure

Step 1 Select **Access Monitoring**.

Step 2 Click **Always Locked** or **Always Unlocked** to lock or unlock the door.

Figure 2-49 Always locked or unlocked



The door will remain locked or unlocked all the time. You can click **Normal** to restore access control to its normal status, and the door will be locked or unlocked based on the configured verification methods.

2.2.9 Reports

You can view alarm logs and unlock logs.

2.2.9.1 Viewing Alarm Records

Procedure

Step 1 Go to **Reports > Alarm Records**.

Step 2 Select the device, group and period, and then click **Search**.

Figure 2-50 Alarm records

The screenshot shows the 'Alarm Records' interface. At the top, there are filters for 'Device' (All x), 'Event Type' (All), and 'Period' (12-22-2024 12:00:00 AM to 12-27-2024 12:00:00 AM). A 'Search' button is on the right. Below the filters are two buttons: 'Export' and 'Extract Device Records' (with a help icon). The main area contains a table with the following headers: 'No.', 'Time', 'Device', 'Door', and 'Event Type'. The table is currently empty, displaying 'No data'. At the bottom left, it says '0 record(s)', and at the bottom right, there are navigation buttons: '<', '1', and '>'.

- **Export:** Exports unlock logs on the main controller to a local computer.
- **Extract Device Records:** When logs for sub controller are generated when they go online, you can extract logs from the sub controller to the main controller.

2.2.9.2 Viewing Unlock Records

Procedure

Step 1 Go to **Reports > Unlock Records**

Step 2 Select the device, group and period, and then click **Search**.

Figure 2-51 Unlock logs

The screenshot shows the 'Unlock Logs' interface. At the top, there are filters for 'Device' (All x), 'Group' (Default Group), and 'Period' (12-26-2024 12:00:00 AM to 12-27-2024 12:00:00 AM). A 'Search' button is on the right. Below the filters are two buttons: 'Export' and 'Extract Device Records' (with a help icon). The main area contains a table with the following headers: 'No.', 'Time', 'User ID', 'Username', 'Card', 'Group', 'Device', 'Door', and 'Status'. The table is currently empty, displaying 'No data'. At the bottom left, it says '0 record(s)', and at the bottom right, there are navigation buttons: '<', '1', and '>'.

- **Export:** Exports unlock logs.
- **Extract Device Records:** When logs on the sub controller are generated when they go online, you can extract logs on the sub controller to the main controller.

2.2.10 System Settings

System settings can only be applied to the local access controllers.

2.2.10.1 Configuring Time

Procedure

Step 1 Go to **System Settings > Time Settings**.

Step 2 Configure the time of the platform.

Figure 2-52 Time settings

The screenshot displays the 'Time settings' configuration interface. It includes the following fields and controls:

- System Time:** 12-26-2024 9:58:54 AM, with a 'Synchronize PC' button.
- Time Zone:** (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi (dropdown menu).
- Date Format:** Month_Day_Year (dropdown menu).
- Time Format:** 12-Hour (dropdown menu).
- NTP Settings:** Unchecked checkbox.
- NTP Server:** time.windows.com, with a 'Manual Update' button.
- Port:** 123 (with a note '(1-65535)').
- Update Cycle:** 1440 min.
- Daylight Saving Time:** Checked checkbox.
- Start Time:** March (dropdown), Second (dropdown), Sunday (dropdown), 02 AM (dropdown).
- End Time:** November (dropdown), First (dropdown), Sunday (dropdown), 02 AM (dropdown).

At the bottom, there are three buttons: 'Apply' (highlighted in dark blue), 'Refresh', and 'Default'.

Table 2-10 Time settings description

Parameter	Description
System Time	Manually enter the time or you can click Synchronize PC to synchronize time with computer.
Time Zone	Select the time zone, date format, and time format of the access controller.
Date Format	
Time Format	
NTP Settings	The access controller will automatically synchronize the time with the NTP server. Enable NTP Settings , set the domain of the NTP server, the port of the NTP server, and update cycle (the synchronization interval).
NTP Server	
Port	
Update Cycle	
Daylight Saving Time	<ol style="list-style-type: none"> 1. Enable Daylight Saving Time. 2. Configure start time and end time.

Step 3 Click **Apply**.

2.2.10.2 Configuring Network

2.2.10.2.1 Configuring TCP/IP

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

Procedure


Step 1 Select **System Settings > Network Setting > TCP/IP**.


Step 2 Configure the parameters.

Figure 2-53 TCP/IP

The screenshot shows a configuration window for TCP/IP. At the top, 'NIC' is set to 'NIC 1'. The 'Mode' is set to 'DHCP' (selected with a radio button) and 'Static' is unselected. Below this are fields for 'MAC Address', 'IP Version' (set to 'IPv4'), 'IP Address' (172.16.1.114), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (172.16.1.1), 'Preferred DNS' (8.8.8.8), and 'Alternate DNS' (8.8.4.4). At the bottom, the 'MTU' is set to 1500. There are three buttons: 'Apply' (highlighted in dark blue), 'Refresh', and 'Default'.

Table 2-11 Description of TCP/IP

Parameter	Description
Mode	<ul style="list-style-type: none"> • Static: Manually enter IP address, subnet mask, and gateway. • DHCP: When DHCP is turned on, the access controller will automatically be assigned IP address, subnet mask, and gateway.  <p>After initializing the sub controller, change its network mode to Static. DHCP is only used for initialization.</p>
MAC Address	MAC address of the access controller.
IP Version	IPv4.
IP Address	If you select static mode, configure the IP address, subnet mask and gateway.
Subnet Mask	

Parameter	Description
Default Gateway	 IP address and gateway must be on the same network segment.
Preferred DNS	Set the IP address of the preferred DNS server.
Alternate DNS	Set the IP address of the alternate DNS server.

Step 3 Click **Apply**.

2.2.10.2.2 Configuring Ports

You can limit access to the access controller at the same time through webpage, desktop client and phone.

Procedure

Step 1 Go to **System Settings > Network Setting > Port**.

Step 2 Configure port numbers.

Figure 2-54 Configure ports

Max Connection	50	(1-50)
HTTP Port	80	(1-65535)
HTTPS Port	443	(1-65535)

Apply Refresh Default

Table 2-12 Description of ports

Parameter	Description
Max Connection	You can set the maximum number of clients that can access the access controller at the same time, such as the webpage, desktop client and phone.
HTTP Port	It is 80 by default. If you want to change the port number, add the new port number after the IP address when you log in to the webpage.
HTTPS Port	It is 443 by default.

Step 3 Click **Apply**.

2.2.10.2.3 Configuring Cloud Service

Add the main controller to PRO-X before you request Bluetooth cards for users. For details on using PRO-X, see the user's manual of PRO-X.




If you have changed the password of the main controller, or restored it to factory defaults, you need to delete the controller on PRO-X and add it to PRO-X again.

Procedure

Step 1 Go to **System Settings > Network Setting > Cloud Service**.

Step 2 Turn on the cloud service function.

Parameter	Description
Port	The port of the server used for automatic registration.
Sub-Device ID	<p>Enter the sub-device ID (user defined).</p>  <p>When you add the access controller to the management platform, the sub-device ID on the management platform must conform to the defined sub-device ID on the access controller.</p>

Step 3 Click **Apply**.

2.2.10.2.5 Configuring Basic Service

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

Procedure

Step 1 Go to **System Settings > Network Settings > Basic Services**.

Step 2 Configure the basic service.

Figure 2-57 Basic services

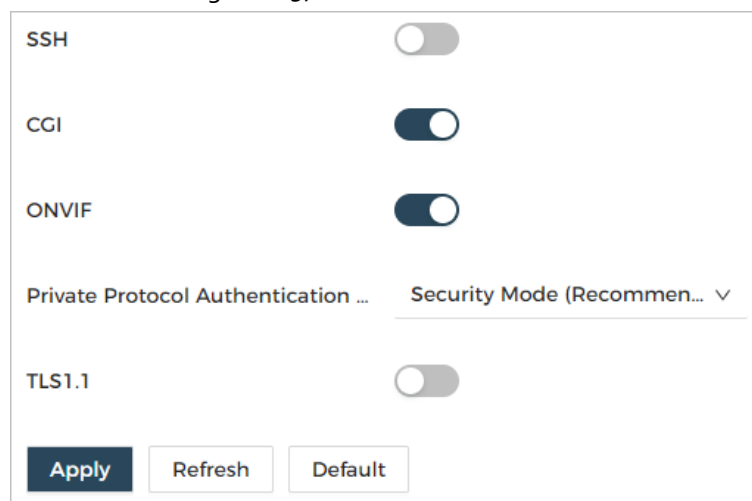



Table 2-14 Basic service parameter description

Parameter	Description
SSH	SSH, or Secure Shell Protocol, is a remote administration protocol that allows users to access, control, and modify their remote servers over the internet.
CGI	The Common Gateway Interface (CGI) is an intersection between web servers through which the standardized data exchange between external applications and servers is possible.
ONVIF	ONVIF stands for Open Network Video Interface Forum. Its aim is to provide a standard for the interface between different IP-based security devices. These standardized ONVIF specifications are like a common language that all devices can use to communicate.

Parameter	Description
Private Protocol Authentication Mode	<p>Set the authentication mode, including security mode (recommended) and compatibility mode.</p> <ul style="list-style-type: none"> • Security Mode (Recommended): Does not support accessing the device through Digest, DES, and plaintext authentication methods, improving device security. • Compatibility Mode: Supports accessing the device through Digest, DES, and plaintext authentication methods, with reduced security.
TLSv1.1	<p>The platform adds devices through TLSv1.1 protocol.</p>  <p>Security risks might present when TLSv1.1 is enabled. Please be advised.</p>

Step 3 Click **Apply**.

2.2.10.3 Updating the System



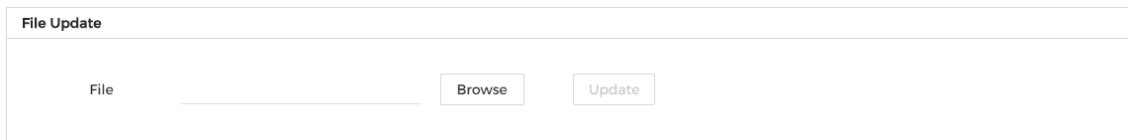
- Use the correct update file. Make sure that you get the correct update file from technical support.
- Do not disconnect the power supply or network, and do not restart or shutdown the access controller during the update.

2.2.10.3.1 File Update

Procedure

Step 1 Go to **System Settings > System Update**.

Figure 2-58 File update



Step 2 In the **File Update** area, click **Browse**, and then upload the update file.



The update file should be a .bin file.

Step 3 Click **Update**.

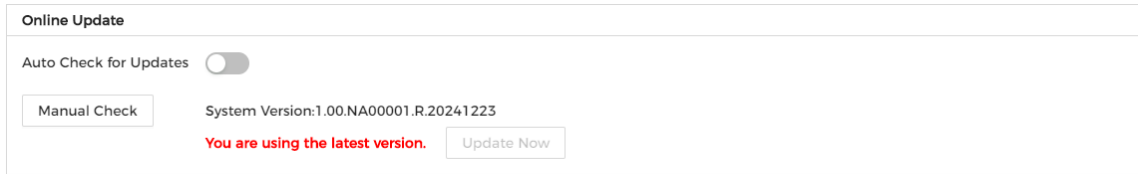
The access controller will restart after the update finishes.

2.2.10.3.2 Online Update

Procedure

Step 1 Go to **System Settings > System Update**.

Figure 2-59 Online update



- Step 2** In the **Online Update** area, select an update method.
- Select **Auto Check for Updates**, and the access controller will automatically check for the latest version update.
 - Select **Manual Check**, and you can immediately check whether the latest version is available.
- Step 3** Click **Manual Check** to update the access controller when the latest version update is available.

2.2.10.4 Advanced Settings

When more than one access controller requires the same configurations, you can configure them quickly by importing or exporting configuration files.

2.2.10.4.1 Exporting and Importing Configuration Files

You can import and export the configuration file for the access controller. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Background Information

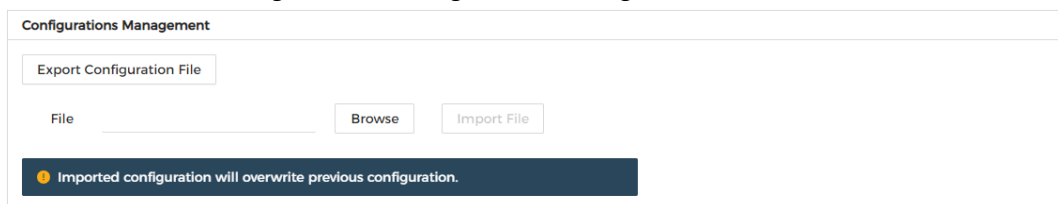


Configurations on device management, advanced access control, time schedules, hardware cannot be exported.

Procedure

- Step 1** Go to **System Settings > Advanced Settings**.

Figure 2-60 Configuration management



- Step 2** Export or import configuration files.
- Export the configuration file.
Click **Export Configuration File** to download the file to the local computer.



The IP will not be exported.

- Import the configuration file.
 1. Click **Browse** to select the configuration file.
 2. Click **Import File**.



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

2.2.10.4.2 Configuring the Card reader

Procedure

Step 1 Go to **System Settings > Advanced Settings**.

Step 2 Configure the card reader.

Figure 2-61 Configure the card reader

Table 2-15 Card reader parameter description

Parameter	Description
Door Channel	Select the door channel that you want to enable card number inversion. You do not have to select the door channel when a single channel device is used. You can change the door type from System Settings > Hardware Wiring > Reset Hardware Config .
Card No. Inversion	Enable Card No. Inversion , and then the card number will be reversed when collecting or swiping cards. For example, if the card number is 123456, the reversed card number will be 654321. The card number inversion function is only available for card readers connected through Wiegand wires.
Reader	Select the card reader.
Baud Rate	Select the baud rate that the card reader supports. It is 9600 by default.

Step 3 Click **Apply**.

2.2.10.4.3 Configuring RS-485 Expansion

If the access controller is mounted to the access controller metal case, you can go to **System**

Settings > Advanced Settings > RS-485 Expansion, and then select **Access Control Metal Case**.

2.2.10.4.4 Restoring the Factory Default Settings

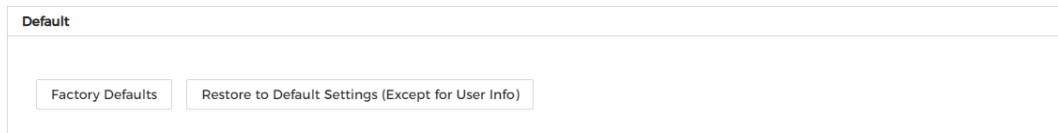
Procedure

Step 1 Go to **System Settings > Advanced Settings**.



Restoring the access controller to its default configurations will result in data loss. Please be advised.

Figure 2-62 Default



Step 2 Restore to the factory default settings if necessary.

- **Factory Defaults:** Resets all the configurations of the access controller and delete all the data.
- **Restore to Default Settings (Except for User Info):** Resets the configurations of the access controller and deletes all the data except for user information, and information that was configured during the login wizard).



Only the main controller supports **Restore to Default Settings (Except for User Info)**.

2.2.10.5 Configuring Card Rules

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

Procedure

Step 1 Go to **System Settings > Card Rule Settings**.

Step 2 Click **Add**, and then configure new Wiegand formats.

You can also Click **Add Protocol** to import a Wiegand file to the platform.

Figure 2-63 Add new Wiegand formats

Add
✕

• Wiegand Format

• Total Bits (1-128)

Facility Code Add

No.	Start Bit	End Bit	Total Bits	Settings
No data				

Card Number Add

No.	Start Bit	End Bit	Total Bits	Settings
No data				

Parity Code Add

Parity Code	Type	Start Bit	End Bit	Total Bits	Settings
No data					

Apply
Cancel

Table 2-16 Configure the Wiegand format

Parameter	Description
Wiegand Format	The name that identifies the Wiegand format.
Total Bits	Enter the total number of bits.
Facility Code	Click Add , and then enter the start bit and the end bit for the facility code.
Card number	Click Add , and then enter the start bit and the end bit for the card number.
Parity Code	<ol style="list-style-type: none"> 1. Click Add. 2. Enter the even parity start bit and even parity end bit. 3. Enter the odd parity start bit and odd parity end bit.

Step 3 Click **Apply**.

Related Operations

- **Facility Code:** If this function is enabled and you set **Card No. System** to decimal format on the **User Management** page, the facility code and the card number are transformed into decimal

format separately, and then combine together.

- **HID26:** If this 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 have 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 56, leading zero is added to fix the number length to 5 characters, like 00056, and another 0 is added to function as a facility code. Therefore, the final card No. will be 000056.

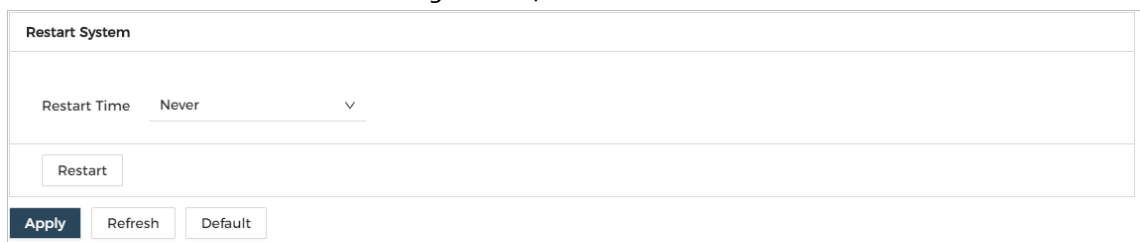
2.2.10.6 Restart

You can regularly restart the access controller during its idle time to improve its performance. It is **Never** by default, and we recommend you change it to one day a week.

Procedure

Step 1 Go to **System Settings > Restart**.

Figure 2-64 Restart



Step 2 Set the restart time, and then click **Apply**.

Step 3 (Optional) Click **Restart**, and the access controller restarts immediately.

2.2.10.7 Backing up System Logs

Procedure

Step 1 Go to **System Settings > System Logs**.


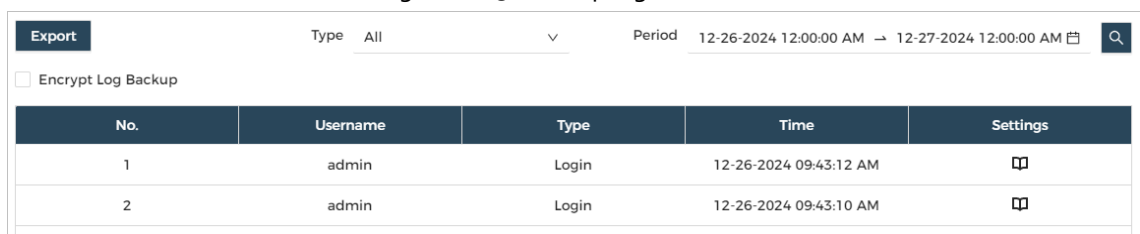


Step 2 Select the type of log, set the period, and then click .

Figure 2-65 Back up logs



No.	Username	Type	Time	Settings
1	admin	Login	12-26-2024 09:43:12 AM	
2	admin	Login	12-26-2024 09:43:10 AM	

Step 3 Click **Encrypt Log Backup**, and then enter the password to back up encrypted logs.

Step 4 (optional) You can also click **Export** to export logs.

2.2.10.8 Configure Local Alarm Linkages

You can only configure local alarm linkages on the same access controller. Each controller has 2 alarm

inputs and 2 alarm outputs.

Procedure

Step 1 Go to **System Settings > Alarm Settings**.


Step 2 Click  to configure local alarm settings.

Figure 2-66 Alarm settings

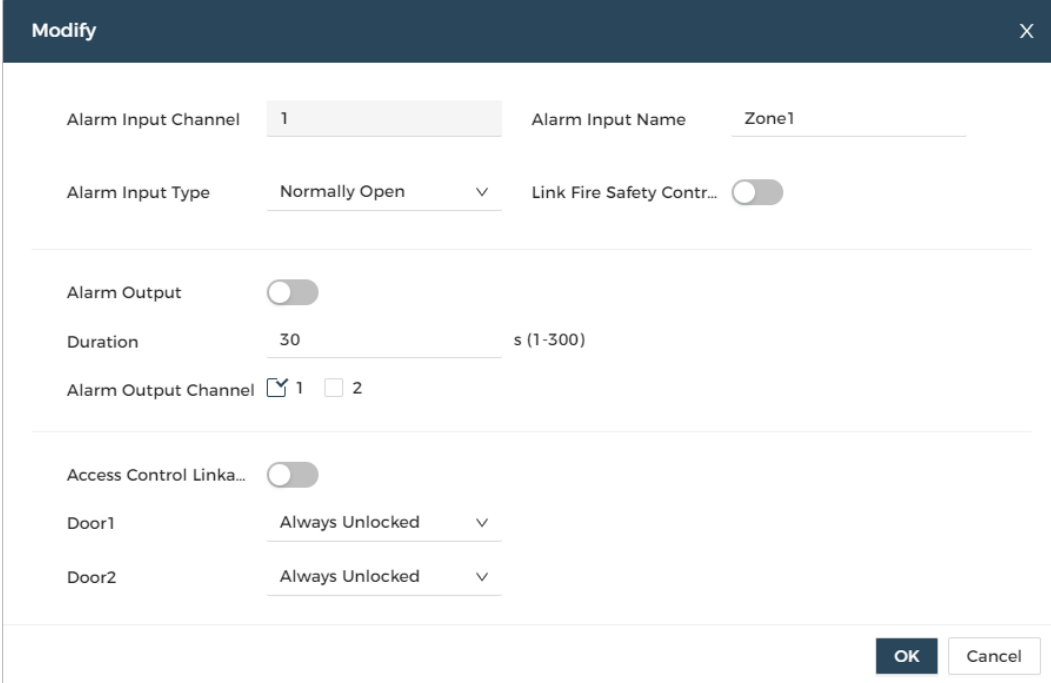



Table 2-17 Local alarm linkage

Parameter	Description
Alarm Input Channel	The number of the alarm input channel.  Each controller has 2 alarm inputs and 2 alarm outputs.
Alarm Input Name	The name that identifies the alarm input.
Alarm Input Type	The type of the alarm input, which includes normally open and normally closed.
Link Fire Safety Control	If you turn on the link fire safety control, all the doors will open when the fire alarm is triggered.
Alarm Output	Enable Alarm Output , set the duration and select the alarm output channels, when an alarm is triggered, the alarm remains on for the defined duration, and links the selected channels with linkage actions.
Duration	
Alarm Output Channel	
Access Control Linkage	Turn on this function to configure the door linkage. Set the door to Always Locked or Always Unlocked . When an alarm is triggered, the door will automatically lock or unlock.
Door1/Door2	

Step 3 Click **OK**.

2.2.10.9 Account Management

You can add or delete users, change user password, and enter an email address for resetting your password if you forget it.

2.2.10.9.1 Adding Administrator Accounts

Add administrators on the access controller.

Procedure

Step 1 Go to **System Settings > Account Management > Account**.

Step 2 Click **Add**, and then enter the user information.



- The username cannot be the same as the existing account. The username can contain up to 31 characters, and supports numbers, letters, underlines, dots, and @.
- The password must contain 8 to 32 non-blank characters and contain at least 2 types of the following characters: upper case and lower case letters, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.

Figure 2-67 Add an administrator account

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Username:** A text input field with a red asterisk indicating it is required.
- Password:** A text input field with a red asterisk indicating it is required.
- Confirm Password:** A text input field with a red asterisk indicating it is required.
- Remarks:** A text area for entering additional information.
- Permission:** A list of permissions, each with a checked checkbox:
 - Device Management
 - User Management
 - Access Rules
 - Weekly Plan
 - Holiday Plan
 - Zone Settings
 - Permission Settings

At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

Step 3 Click **OK**.



Only administrator account can change password and the admin account cannot be deleted.

2.2.10.9.2 Resetting the Password

Reset the password through the linked e-mail when you forget your password.

Procedure

- Step 1 Go to **System Settings > Account Management > Account**.
- Step 2 Enter the email address, and then set the password expiration time.
- Step 3 Turn on the password reset function.

Figure 2-68 Reset password

Enable

Email address used to receive security codes for password reset.

Email Address

Password Expires in Never Days

Apply Refresh Default



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

- Step 4 Click **Apply**.

2.2.10.9.3 Adding ONVIF Users

Open Network Video Interface Forum (ONVIF), a global and open industry forum that was established for the development of a global open standard for the interface of physical IP-based security products, which allows the compatibility from different manufactures. ONVIF users have their identities verified through ONVIF protocol. The default ONVIF user is admin.

Procedure

- Step 1 Go to **System Settings > Account Management > ONVIF User**.
- Step 2 Click **Add**, and then configure the parameters.

Figure 2-6g Add the ONVIF user

Table 2-18 ONVIF user description

Parameter	Description
Username	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 @.
Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: Upper case, lower case, numbers, and special characters (excluding ' " ; &).
Group	There are 3 permission groups which represent different permission levels. <ul style="list-style-type: none"> • 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.

Step 3 Click **OK**.

2.2.10.10 Configuring Hardware

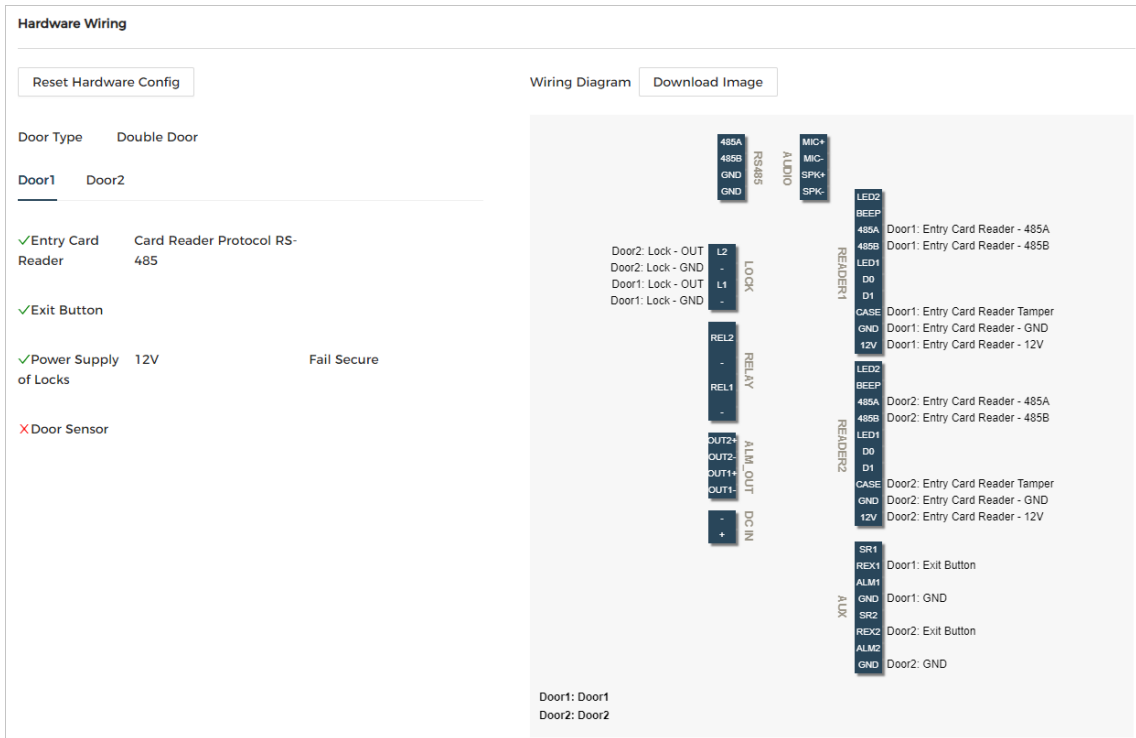
Go to **System Settings > Hardware Wiring**. You can view the hardware that you have configured when you log in to the platform for the first time. You can also click **Reset Hardware Config** to configure the hardware again. For details, see Table 2-1.



When you switch between single door and double doors, we recommend you restore the main controller to factory defaults.

The wiring diagram is generated for your reference. You can download it to your computer.

Figure 2-70 Hardware



2.2.10.11 Viewing Legal Information

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

2.2.10.12 Viewing Version Information

Go to **System Settings > Version Info**, and you can view information on the version, such as device model, serial number, hardware version, legal information and more.

2.2.11 Maintenance Center

2.2.11.1 Packet Capture

Retrieve network interaction data between the device and a specified network card on the client, and store it on the computer.

Procedure

Step 1 Go to **Maintenance Center > Packet Capture**.

Figure 2-71 Packet capture

Packet Capture						
NIC	Device Address	IP 1: Port 1	IP 2: Port 2	Packet Sniffer Size	Packet Sniffer Backup	
eth0	172.6.104.114	Optional	: Optional	Optional	: Optional	0.30MB ▶

Step 2 Capture.

Click ▶ to start capturing. **Packet Sniffer Size** will display the size of the packet.

Click || to end capturing. The capture file will be saved locally.

2.2.11.2 Running Log

Run debug log and export it.

Procedure

- Step 1 Go to **Maintenance Center > Run Log**.
- Step 2 Click **Start** to run log, then click **End** to stop running.
- Step 3 Click **Export** to export debug log.

2.2.12 Security

2.2.12.1 Configuring HTTPS

Create a certificate or upload an authenticated certificate, and then you can log in to the webpage through HTTPS on your computer. HTTPS secures communication over a computer network.

Procedure

- Step 1 Go to **Security > System Service**.
- Step 2 Turn on the HTTPS service.



If you turn on the HTTPS compatible with TLS v1.1 or earlier versions, security risks might occur. Please be advised.

- Step 3 Select the certificate.



If there are no certificates in the list, click **Certificate Management** to upload a certificate. For details, see "2.2.12.3 Installing Device Certificate".

Figure 2-72 HTTPS

Enable

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

*Select a device certificate Certificate Management

No.	Custom Name	Certificate Serial Number	Valid from	User	Issued by	Used by
<input checked="" type="radio"/> 1		65343234366334323336326631373335303631343130	12-18-2054 06:30:10 AM	AC02B3TESTDMSS	BSC	HTTPS, RTSP over TLS

- Step 4 Click **Apply**.
Enter "https://IP address:https port" in a web browser. If the certificate is installed, you can log in to the webpage successfully. If not, the webpage will display the certificate as wrong or untrusted.

2.2.12.2 Attack Defense

2.2.12.2.1 Configuring Firewall

Configure firewall to limit access to the access controller.

Procedure

Step 1 Go to **Security > Attack Defense > Firewall**.

Step 2 Click to enable the firewall function.

Figure 2-73 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	Settings
1	202.202.202.202	All Device Ports	

Total 1 records

Apply Refresh Default

Step 3 Select the mode.

- **Allowlist:** Only IP/MAC addresses on the allowlist can access the access controller.
- **Blocklist:** The IP/MAC addresses on the blocklist cannot access the access controller.

Step 4 Click **Add** to enter the IP information.

Step 5 Click **OK**.

Related Operations

- Click to edit the IP information.
- Click to delete the IP address.

2.2.12.2.2 Configuring Account Lockout

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

Procedure

Step 1 Go to **Security > Attack Defense > Account Lockout**.

Step 2 Enter the number of login attempts and the time the administrator account and ONVIF user will be locked for.

- **Login Attempt:** The limit of login attempts. If the incorrect password is entered for a defined number of times, the account will be locked.
- **Lock Time:** The duration during which you cannot log in after the account is locked.

Figure 2-74 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

Step 3 Click **Apply**.

2.2.12.2.3 Configuring Anti-DoS Attack

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

Procedure

Step 1 Select **Security > Attack Defense > Anti-DoS Attack**.

Step 2 Turn on **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** to protect the access controller against DoS attack.

Figure 2-75 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

Step 3 Click **Apply**.

2.2.12.3 Installing Device Certificate

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS on

your computer.

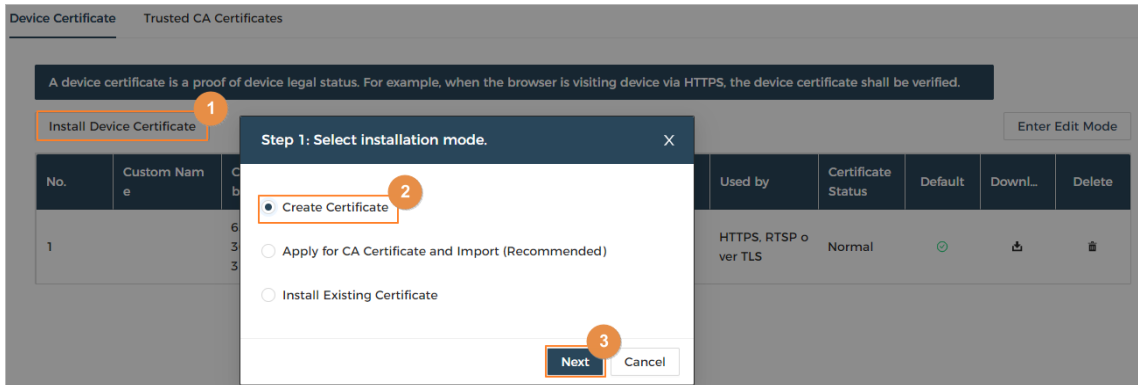
2.2.12.3.1 Creating Certificate

Create a certificate for the access controller.

Procedure

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

Figure 2-76 Create certificate





- Step 4 Enter the certificate information.



The name of country/region cannot exceed 2 characters. We recommend entering the abbreviation of the name of the country/region.

- Step 5 Click **Create and install certificate**.
The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.

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.

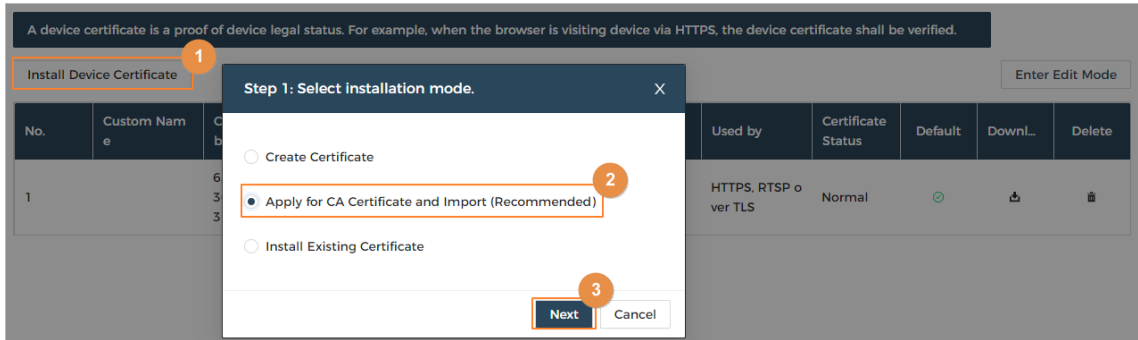
2.2.12.3.2 Applying for and Importing CA Certificate

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

Procedure

- Step 1 Go to **Security > CA Certificate > Device Certificate**.
- Step 2 Click **Install Device Certificate**.
- Step 3 Select **Apply for CA Certificate and Import (Recommended)**, and then click **Next**.

Figure 2-77 Apply for and Import CA Certificate



Step 4 Enter the certificate information.

- IP/Domain name: the IP address or domain name of the access controller.
- Country/Region: The name of country/region must not exceed 3 characters. We recommend you enter the abbreviation of country/region name.

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

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



Step 7 Import the signed CA certificate.

- 1) Save the CA certificate to your computer.
- 2) Click **Browse** to select the CA certificate.
- 3) Click **Import and Install**.

The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.

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

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.

2.2.12.3.3 Installing Existing Certificate

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

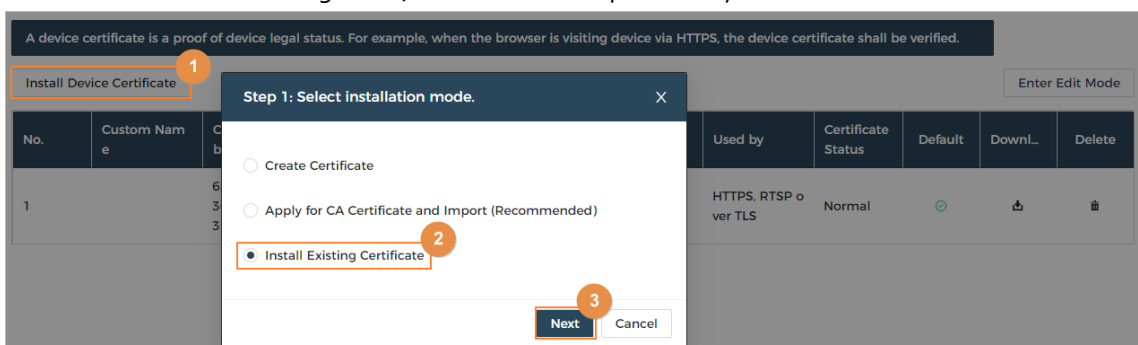
Procedure

Step 1 Go to **Security > CA Certificate > Device Certificate**.

Step 2 Click **Install Device Certificate**.



Step 3 Select **Install Existing Certificate**, and click **Next**.

Figure 2-78 Certificate and private key



- Step 4** Click **Browse** to select the certificate and private key file, and enter the private key password.
- Step 5** Click **Import and Install**.
The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.

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.

2.2.12.4 Installing the Trusted CA Certificate

A trusted CA certificate is a digital certificate that is used for validating the identities of websites and servers. For example, when 802.1x protocol is used, the CA certificate for switches is required to authenticate its identity.

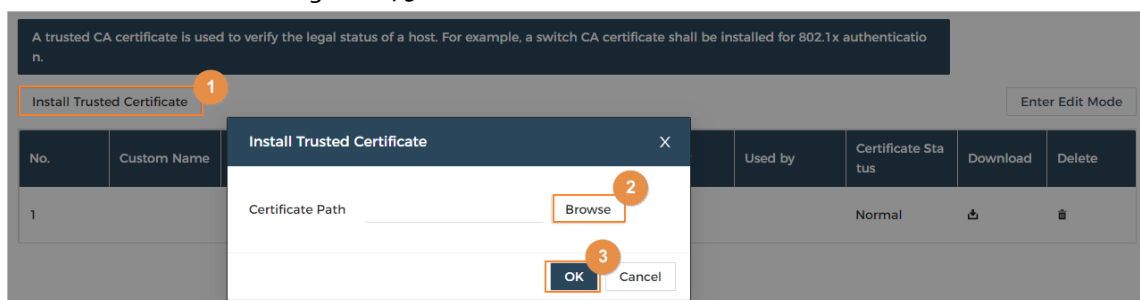
Background Information

802.1x is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them access to the network.



Procedure

- Step 1** Go to **Security > CA Certificate > Trusted CA Certificates**.
- Step 2** Select **Install Trusted Certificate**.
- Step 3** Click **Browse** to select the trusted certificate.
- Step 4** Click **OK**.
The newly installed certificate is displayed on the **Trusted CA Certificates** page after the certificate is successfully installed.

Figure 2-79 Install the trusted certificate



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.

2.3 Configurations of Sub Controller

You can log in to the webpage of the sub controller to configure it locally.

2.3.1 Initialization

Initialize the sub controller when you log in to the webpage for the first time or after the sub controller is restored to its factory default settings. For details on how to initialize the sub controller, see "2.2.2 Initialization".



After initializing the sub controller, change its network mode to **Static**. **DHCP** is only used for initialization.

2.3.2 Logging In

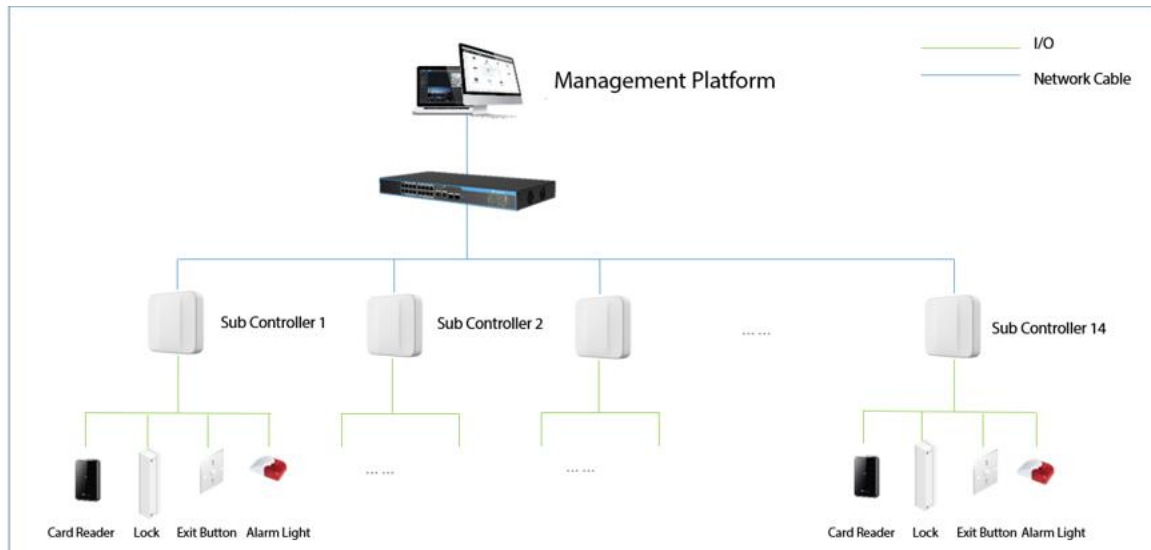
Set the access controller to sub controller while going through the login wizard. For details, see "2.2.3 Logging In".

3 X Station-Sub Controllers

3.1 Networking Diagram

The sub controllers are added to a standalone management platform, such as X Station. You can manage all sub controllers through X Station.

Figure 3-1 Networking Diagram



3.2 Configurations on X Station

Add sub controllers to X Station and configure them on the platform. For details, see the user's manual of X Station.

3.3 Configurations on Sub Controller

For details, see "2.3 Configurations of Sub Controller".

Appendix 1 Security Recommendation

Account Management

1. Use complex passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters: upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use repeating characters, such as 111, aaa, etc.

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account lockout function

The account lockout function is enabled by default. You are advised to keep it 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 device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access web services through secure channels.

2. Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped 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 highly recommended to choose safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up complex passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.

4. Change HTTP and other default service ports

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

Network Configuration

1. **Enable Allow list**

It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.

2. **MAC address binding**

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. **Build a secure network environment**

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
- Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

It is recommended to check online users regularly to identify illegal users.

2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such

as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).