

Access Standalone

User Manual



V1.0.3

Foreword

General

This manual introduces the functions and operations of the Access Standalone (hereinafter referred to as the Device). Read carefully before using the device, and keep the manual safe for future reference.

Symbols

The following symbols might appear in the manual.

Symbol	Description
 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
V1.0.3	- Added QR code function. - Added Bluetooth function. - Revised alarm setting functions. - Added back-end comparison function. - Added audio function.	July 2026
V1.0.2	Revised content.	December 2025
V1.0.1	Added initialization description.	December 2024
V1.0.0	First release.	August 2024

Privacy Protection Notice

As the device user, you might collect the personal data of individuals such as their names, email addresses, face images, audio and fingerprints. You shall be fully responsible for any activities associated with processing personal data. You commit to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of individuals, and shall implement measures which are required by applicable law, including but not limited to, providing clear and comprehensive information to individuals before processing their personal data, obtaining consent from individuals when necessary, informing individuals of the existence of the surveillance area, and providing required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

Interface Declaration

This manual mainly introduces the relevant functions of the device. The interfaces used in its manufacture, the procedures for returning the device to the factory for inspection and for locating its faults are not described in this manual. Please contact technical support if you need information on these interfaces.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

Table of Contents

Foreword.....	I
1 Overview.....	1
2 Local Operations.....	2
2.1 Initialization.....	2
2.2 Main Menu.....	3
2.3 User Management.....	4
2.3.1 Adding User.....	4
2.3.2 Deleting User.....	5
2.4 Configuring Door Unlock Mode.....	5
2.5 Configuring Unlock Duration.....	6
2.6 Configuring Door Sensor.....	6
2.7 Password Management.....	6
2.7.1 Changing the Administrator Password.....	6
2.7.2 Adding Public Password.....	7
2.7.3 Deleting Public Password.....	7
2.8 Main Card Management.....	7
2.8.1 Adding Main Card.....	7
2.8.2 Deleting Main Card.....	8
2.8.3 Managing User Cards through Main Card.....	8
2.9 Configuring Door Timeout Period.....	8
2.10 Restoring to Factory Settings.....	9
3 Webpage Operations.....	10
3.1 Initialization.....	10
3.2 Resetting the Password.....	11
3.3 Home Page.....	12
3.4 Person Management.....	13
3.5 Access Monitoring.....	18
3.6 Configuring Access Control.....	20
3.6.1 Configuring Access Control Parameters.....	20
3.6.2 Alarm.....	25
3.6.3 Card Settings.....	29
3.6.4 Configuring Periods.....	34
3.6.5 Configuring QR Code.....	37
3.6.6 Configuring Back-end Comparison.....	38
3.6.7 Configuring Port Functions.....	38
3.6.8 Configuring the Password Unlock.....	39
3.6.9 Configuring First-Person Unlock.....	39

3.6.10	Configuring Anti-Passback.....	40
3.7	Configuring Audio.....	42
3.8	Communication Settings.....	43
3.8.1	Network Settings.....	43
3.8.2	Mode Settings.....	54
3.8.3	Configuring Bluetooth Settings.....	58
3.9	Configuring the System.....	59
3.9.1	User Management.....	59
3.9.2	Viewing Online Users.....	62
3.9.3	Configuring Time.....	62
3.10	Maintenance Center.....	63
3.10.1	One-click Diagnosis.....	63
3.10.2	System Information.....	64
3.10.3	Data Capacity.....	64
3.10.4	Viewing Logs.....	64
3.10.5	Maintenance Management.....	65
3.10.6	Updating the System.....	67
3.10.7	Advanced Maintenance.....	68
3.11	(Optional) Security Settings.....	68
3.11.1	Security Status.....	68
3.11.2	Configuring System Service.....	69
3.11.3	Attack Defense.....	70
3.11.4	Installing Device Certificate.....	73
3.11.5	Installing the Trusted CA Certificate.....	76
3.11.6	Security Warning.....	77
3.11.7	Security Authentication.....	78
4	Phone Operations.....	79
4.1	Initialization.....	79
4.2	Logging in to the Webpage.....	80
4.3	Home Page.....	81
4.4	Person Management.....	83
4.5	Configuring the System.....	86
4.5.1	Viewing Version Information.....	86
4.5.2	Maintenance.....	86
4.5.3	Configuring Time.....	87
4.5.4	Data Capacity.....	89
4.5.5	Language.....	89
4.6	Configuring Access Control.....	89
4.6.1	Configuring Unlock Methods.....	89
4.6.2	Configuring Access Control Parameters.....	90

4.6.3	Configuring Alarms.....	93
4.6.4	Configuring Alarm Linkage.....	95
4.6.5	Configuring Card Settings.....	96
4.7	Communication Settings.....	98
4.7.1	Configuring TCP/IP.....	98
4.7.2	Configuring Wi-Fi.....	100
4.7.3	Configuring Wi-Fi AP.....	100
4.7.4	Configuring Cloud Service.....	101
4.7.5	Configuring Auto Registration.....	102
4.7.6	Configuring Mode.....	102
4.7.7	Configuring Bluetooth.....	106
4.8	Configuring Audio.....	107
4.9	Viewing Logs.....	107
4.9.1	System Logs.....	107
4.9.2	Unlock Records.....	108
4.9.3	Alarm Logs.....	108
5	Smart PSS Lite Configuration.....	109
5.1	Installation.....	109
5.2	Adding Device One by One.....	109
5.3	Adding Users.....	110
Appendix 1 Important Points of Fingerprint Registration Instructions.....		111
Appendix 2 Security Recommendation.....		113

1 Overview

This product is an access control equipment integrating card reading, configuration and execution. The appearance of the product is simple and fashionable, and it is suitable for office buildings, schools, parks, communities, factories, public venues, business centers, government buildings and other application scenarios.

2 Local Operations

2.1 Initialization

After the Device is powered on for the first time, you need to set the administrator password. The administrator password is used to enter the main menu of the Device.

Procedure

Step 1 Power on the Device, and the indicator light will flash red slowly.

Step 2 Press # , enter the administrator password, and then press #.

The password must be 1 to 8 characters in length.

If the indicator light is solid blue, it means the Device is initialized.



After initialization, you can only use the functions on the Device. If you want to login to the webpage of the Device, initialize the Device on its webpage or through the ConfigTool.

Related Operations

- You can only set numbers as the admin account password when you initialize it through the Device.
- You can set numbers, letters and other characters as the admin account password when you initialize it through the platform of the ConfigTool.

After you complete the initialization on the Device, you can only perform operations on the Device itself. If you need to connect the Device to the network, use ConfigTool or the platform to initialize the Device.

When you use ConfigTool or the platform to initialize the Device, after configuring the network account and password, the device will automatically complete initialization and enter the standby status. The local admin password is converted from the network password. If the password exceeds 8 characters, only the first 8 characters are kept. The letters are converted into digits according to the E.161 standard. The password conversion is case-insensitive, and all other symbols are converted to 0.



- After the initialization, if you modify the network password, the local admin password will not be affected.
- If you initialize through the Device first, then initialize through the ConfigTool or the platform, the local admin password will not be affected.

Figure 2-1 E.161 (T9 keypad)

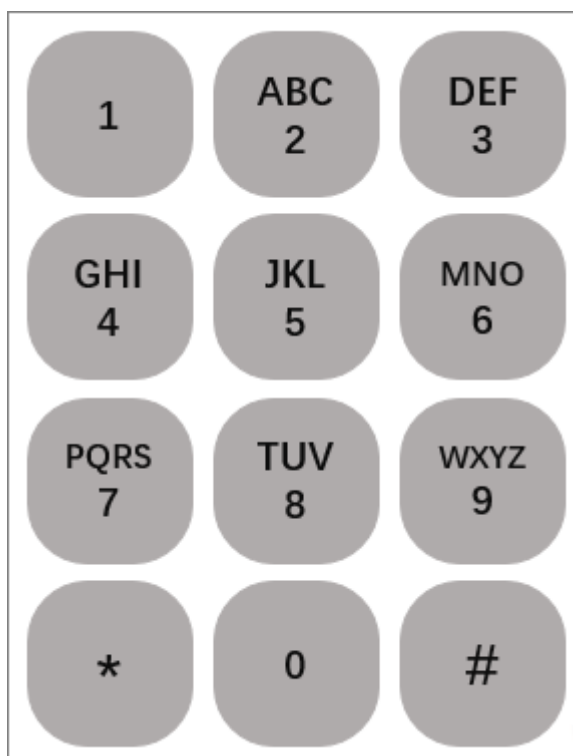


Table 2-1 Conversion example

Network Password	Local Admin Password
ABC12345	22212345
admin123	23646123
admin12!	23646120
admin123456	23646123

2.2 Main Menu

Entering Main Menu

Press # , enter the administrator password, and then press #.

- The indicator flashes blue, and it means you have entered the main menu.
- The indicator flashes red once, the buzzer beeps 3 times, and then the indicator turns solid blue, which means the password is wrong.

Related Prompts

- The indicator flashes green once, and the buzzer beeps once, which means that the operation or access control verification is successful.
- The indicator flashes red once, and the buzzer beeps 3 times, which means that the operation or access control verification failed.
- If the indicator flashes red slowly, it means the Device is not uninitialized.

- If the indicator is solid blue, it means the Device is in the standby status.
- The indicator flashes blue, it means the Device enters the main menu.
- The keypad is white when you operate the device. If there is no operation within 10 seconds, the light turns off and the Device exits the current screen.

2.3 User Management

2.3.1 Adding User



- You can add only one card, one password or one fingerprint for one user. At least one method of card, password, and fingerprint must be added.
- Fingerprint function is available on select models.

Procedure

Step 1 Press # , enter the administrator password, and then press #.

Enter the main menu, and the indicator flashes blue.

Step 2 Press 1 and # to add users.

Step 3 Enter the user ID, and then press #.

- If the indicator does not light up and the Device beeps, the user ID is added successfully.
- If the indicator flashes red and the Device beeps, you fail to add the user ID. The possible reason is the ID already exists. Please try the other ID.



You can only enter numbers for the ID on the Device.

Step 4 After swiping the card, press # to add the card.

If you do not need to add the card, press # to skip it.

Step 5 Enter the user password, and then press #.

If you do not need to set the user password, press # to skip it.



The password can be 1 to 8 characters in length.

Step 6 Add the fingerprint, and then press #.

If you do not need to set the fingerprint, press # to skip it.



This function is available on select models.

Step 7 Repeat Step 2 to Step 6 to add more users.

After adding the user, press * to return to the main menu, and then press * to return to the standby status.

2.3.2 Deleting User

Procedure

Step 1 Press # , enter the administrator password, and then press #.

Enter the main menu, and the indicator flashes blue.

Step 2 Press 2 and #.

Step 3 Delete a user.

- Swipe the card, and then press #.



If you swipe a card that has not been added, the deletion fails.

- Enter the user ID, and then press #.



If you enter the ID that has not been added, the deletion fails.

- Enter 0000, and then press # to delete all users.

After deletion, press * to return to the main menu, and then press * to exit the main menu.

2.4 Configuring Door Unlock Mode

Background Information



The fingerprint function is available on select models.

Procedure

Step 1 Press # , enter the administrator password, and then press #.

Enter the main menu and the indicator flashes blue.

Step 2 Press 3 and #.

Step 3 Select the unlock mode.

- Press 0 and # to set unlocking by card, password, Bluetooth or fingerprint.

Swipe the card, enter the password, or use the fingerprint to open the door. The password consists of the following methods.

- ◇ On the standby screen, enter the user ID, press # , and the Device beeps once. Enter the password, and then press # to verify the identity.
- ◇ On the standby screen, enter the public password, and then press # to verify the identity.
- ◇ When the **PIN Code Authentication** is enabled on the webpage of the Device, people can verify the identity by simply entering the password.
- ◇ When the Device is used with the DMSS app, the temporary password is supported and can be configured on the app.

- Press 1 and # to set unlocking by card and user password.

Swipe the card first. After the Device beeps once, enter the password, and then press # to verify the identity.

- Press 2 and # to set unlocking by card and fingerprint.

Swipe the card first. After the Device beeps once, press the fingerprint to verify the identity.

- Press **3** and **#** to set unlocking by card, password and fingerprint.

Swipe the card first. After the Device beeps once, press the fingerprint. The Device beeps again. Enter the password, and then press **#** to verify the identity.

Step 4 Press ***** to exit the main menu.

2.5 Configuring Unlock Duration

The door remains open after a defined time after it unlocks, which allows people to pass through.

Procedure

Step 1 Press **#**, enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **4** and **#**.

Step 3 Enter the time, and then press **#**.

The value ranges from 1 second to 600 seconds. The default value is 3 seconds.

Step 4 Press ***** to exit the main menu.

2.6 Configuring Door Sensor

After the door sensor is enabled, the door timeout alarm is enabled at the same time by default. If the door stays open after the set door timeout period, the buzzer of the Device generates alarms.

Procedure

Step 1 Press **#**, enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **5** and **#**.

Step 3 Turn on or turn off the door sensor.

The door sensor is turned off by default.

- Press **0** and **#** to turn off the door sensor.
- Press **1** and **#** to turn on the door sensor.

Step 4 Press ***** to exit the main menu.

2.7 Password Management

- Administrator password: Used to enter the main menu of the Device.
- Public password: Used to verify the authentication to unlock the door.

2.7.1 Changing the Administrator Password

To ensure device security, we recommend that you change the administrator password from time to time.

Procedure

Step 1 Press **#**, enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

- Step 2 Press **0** and #.
- Step 3 Enter the new password, and then press #.
- Step 4 Enter the new password again, and then press #.
- Flashing green means the password is modified successfully.
 - Flashing red means that you fail to modify the password.
 - After modification, the Device automatically exits the main menu, and the indicator turns solid blue. Enter the main menu using the new password if you modify the password successfully. Enter the main menu using the original password if you fail to modify the password.

2.7.2 Adding Public Password

Procedure

- Step 1 Press # , enter the administrator password, and then press #.

Enter the main menu and the indicator flashes blue.

- Step 2 Press **6** and #.

- Step 3 Enter the public password, and then press #.

The password can be 1 to 8 characters in length.



You can add only one public password. If you repeat the operations, the new password will replace the original one.

- Step 4 Press * to exit the main menu.

2.7.3 Deleting Public Password

Procedure

- Step 1 Press # , enter the administrator password, and then press #.

Enter the main menu and the indicator flashes blue.

- Step 2 Press **7** and #.

- Step 3 Enter the public password and press #.

- Step 4 Press * to exit the main menu.

2.8 Main Card Management

2.8.1 Adding Main Card

After adding the main card, you can quickly add and delete other user cards through the main card.

Background Information



The main card cannot be used to unlock the door.

Procedure

Step 1 Press # , enter the administrator password, and then press #.

Enter the main menu and the indicator flashes blue.

Step 2 Press 8 and #.

Step 3 Swipe the card, and then press #.

- If the indicator flashes green, and the Device beeps, it means the card is added as the main card.
- If the indicator flashes red, and the Device beeps, it means you fail to add the card as the main card.



- User cards that have been added can also be set as main card.
- If a user card is set to main card, it will not be able to unlock the door.
- Only supports one main card. If a new main card is added, the old main card will be overwritten.

Step 4 Press * to exit the main menu.

2.8.2 Deleting Main Card

Procedure

Step 1 Press # , enter the administrator password, and then press #.

Enter the main menu, and the indicator flashes blue.

Step 2 Press 9 and #.

Step 3 Swipe the card, and then press #.

Step 4 Press * to exit the main menu.

2.8.3 Managing User Cards through Main Card

If no operation is performed in 3 seconds after you swipe the main card, the Device enters the main card mode, and the Device will determine the corresponding function according to the swipe times of the main card. In the main card mode, the indicator flashes red and blue alternately, and if there is no operation for 10 seconds or you swipe the main card again for one time, it returns to the standby status.

- Add user card: Swipe the main card once, and then swipe the user card to add it. User cards can be added continuously.
- Delete the user card: Swipe the main card twice, and then swipe the user card to delete it. User cards can be deleted continuously.
- Clear all user cards: Swipe the main card 5 times in a row.

2.9 Configuring Door Timeout Period

After the door sensor is enabled, if the door stays open after the set time, the buzzer of the Device will give an alarm.

Procedure

Step 1 Press # , enter the administrator password, and then press #.

- Enter the main menu and the indicator flashes blue.
- Step 2 Press **10** and #.
- Step 3 Enter the door timeout period, and then press #.
- The value range is from 1 second to 9999 seconds. The default value is 60 seconds.
- Step 4 Press * to exit the main menu.

2.10 Restoring to Factory Settings

Procedure

- Step 1 Press # , enter the administrator password, and then press #.
- Enter the main menu, and the indicator flashes blue.
- Step 2 Press **11** and #.
- Step 3 Restore the Device to factory settings.
- Press **00** and # to restore factory settings (retain user information).
 - Press **000** and # to restore factory settings (restore all information).

Related Operations

You can use the reset button to restore the Device to factory settings.

3 Webpage Operations

On the webpage, you can also configure and update the Device.



Web configurations differ depending on models of the Device.

3.1 Initialization

Initialize the Device when you log in to the webpage for the first time or after the Device is restored to the factory defaults.

Prerequisites

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

Procedure

Step 1 Open a browser, go to the IP address (the default address is 192.168.1.108) of the Device.



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

Step 2 Select a language for the Device.

Step 3 Set the password and email address according to the screen instructions.



- 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 ' " ; : &). 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.

Related Operations

- You can only set numbers as the admin account password when you initialize it through the Device.
- You can set numbers, letters and other characters as the admin account password when you initialize it through the platform of the ConfigTool.

After you complete the initialization on the Device, you can only perform operations on the Device itself. If you need to connect the Device to the network, use ConfigTool or the platform to initialize the Device.

When you use ConfigTool or the platform to initialize the Device, after configuring the network account and password, the device will automatically complete initialization and enter the standby status. The local admin password is converted from the network password. If the password exceeds 8 characters, only the first 8 characters are kept. The letters are converted into digits according to the E.161 standard. The password conversion is case-insensitive, and all other symbols are converted to 0.



- After the initialization, if you modify the network password, the local admin password will not be affected.
- If you initialize through the Device first, then initialize through the ConfigTool or the platform, the local admin password will not be affected.

Figure 3-1 E.161 (T9 keypad)

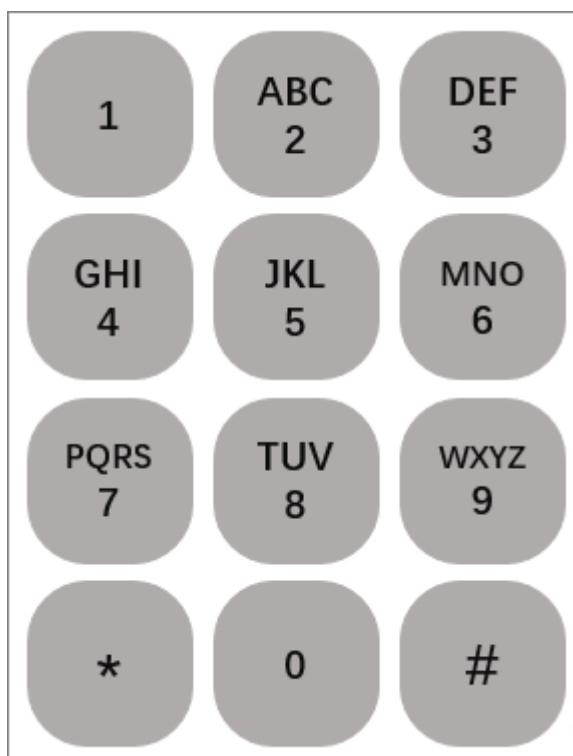


Table 3-1 Conversion example

Network Password	Local Admin Password
ABC12345	22212345
admin123	23646123
admin12!	23646120
admin123456	23646123

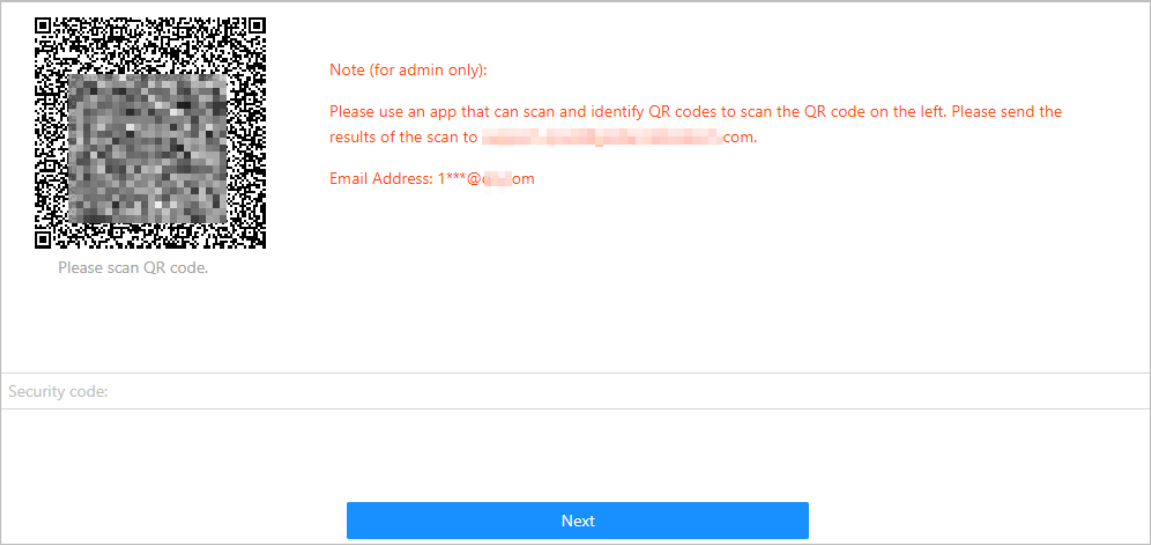
3.2 Resetting the Password

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

Procedure

- Step 1 On the login page, click **Forgot password**.
- Step 2 Read the on-screen prompt carefully, and then click **OK**.
- Step 3 Scan the QR code, and you will receive a security code.

Figure 3-2 Reset password



Please scan QR code.

Note (for admin only):

Please use an app that can scan and identify QR codes to scan the QR code on the left. Please send the results of the scan to [redacted]@[redacted].com.

Email Address: 1***@[redacted].com

Security code:

Next



- Up to two security codes will be generated when the same QR code is scanned. If the security code becomes invalid, refresh the QR code and scan again.
- After you scan the QR code, you will receive a security code in your linked e-mail address. Use the security code within 24 hours after you receive it. Otherwise, it will become invalid.
- If the wrong security code is entered 5 times in a row, the administrator account will be frozen for 5 minutes.

Step 4 Enter the security code.

Step 5 Click **Next**.

Step 6 Reset and confirm the password.



The password should consist of 8 to 32 non-blank characters and contain at least two of the following types of characters: upper case, lower case, number, and special character (excluding ' " ; : &).

Step 7 Click **OK**.

3.3 Home Page

The home page is displayed after you successfully log in.

Figure 3-3 Home page

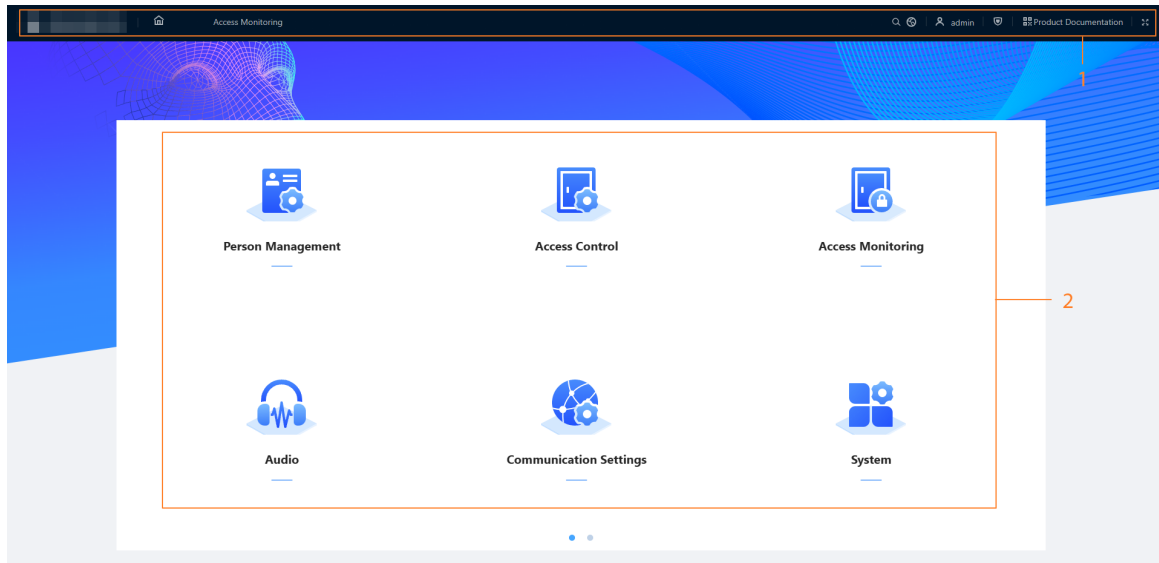


Table 3-2 Home page description

No.	Description
1	• : Enter the home page. • : Searching for function menus by keywords. • : Select a language on the device. • : Log out or restart the device. • : Enter the Security page. • : Scan the QR code to view the product material. This function is available on select models. • : Display in full screen.
2	Main menu.

3.4 Person Management

Procedure

- Step 1 On the home page, select **Person Management** , and then click **Add**.
- Step 2 Configure user information.

Figure 3-4 Add users

Basic Info

* ID

Name

* User Type

General User

* Times Used

Unlimited

* General Plan

255-Default

* Holiday Plan

255-Default

Email

Validity Period

Forever

Verification Mode

☐ Same as Device
 ☒ Custom

Combination Meth...

☐ And
 ☒ Or

* Unlock Method

Card

Password

Table 3-3 Parameters description

Parameter	Description
ID	The ID can be numbers, letters, and their combinations, and the maximum length of the number is 30 characters.
Name	The name can have up to 32 characters (including numbers, symbols, and letters).
User Type	● General User : General users can unlock the door. ● Blocklist User : When users in the blocklist unlock the door, service personnel will receive a notification. ● Guest User : Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. ● Patrol User : Patrol users can take attendance on the Device, but they do not have door permissions. ● VIP User : When VIP unlocks the door, they are not restricted by unlock modes, such as Multi-card and Time Section. ● Other User : When they unlock the door, the door will stay unlocked for 5 more seconds. ● Custom User 1/Custom User 2 : Same as general users.
Email	Enter the email address of the user.
Times Used	Set an unlock limit for guest users. After the unlock times run out, they cannot unlock the door.
General Plan	People can unlock the door or take attendance during the defined period.  You can select more than one plan.

Parameter	Description
Holiday Plan	People can unlock the door or take attendance during the defined holiday.  You can select more than one holiday.
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.
Password	Enter the user password. The maximum length of the password is 8 digits. The duress password is the unlock password + 1. For example, if the user password is 12345, the duress password will be 12346. In special cases, if the last digit of the password is 9, for example the user password is 12349, and the duress password will be 12340. A duress alarm will be triggered when a duress password is used to unlock the door.

Parameter	Description
Card	A user can register up to 5 cards at most. Enter your card number or swipe your card on the Device or an external card reader, and then the card information will be read by the Device. ● Enter the card number manually. 1. Click Add. 2. Enter the card number, and then click Add. ● Read the number automatically through the enrollment reader or the Device. 1. Click Add, and then click Modify to select an enrollment reader or the Device. 2. Read the card. ◇ For the enrollment reader of IC and ID card, click Read Card, and then swipe cards on the card reader. A 60-second countdown is displayed to remind you to swipe cards, and the system will read the card number automatically. If the 60-second countdown expires, click Read Card again to start a new countdown. ◇ For the enrollment reader of the Desfire card, place the card on the enrollment reader, and then click Read Card. If the Desfire card has been written with the card number, it will be read and displayed here. If the card is empty, then the card number needs to be written first. The card number will be automatically generated on the computer, and be written to the card. 3. Click Add. You can enable the Duress Card function. An alarm will be triggered if a duress card is used to unlock the door. ● : Set duress card. ● : Change card number.  One user can only set one duress card.

Parameter	Description
Fingerprint	Register fingerprints. A user can register up to 3 fingerprints, and you can set a fingerprint to the duress fingerprint. An alarm will be triggered when the duress fingerprint is used to unlock the door. Enroll fingerprints through an enrollment reader or the Device. 1. Click Add , and then click Modify to select an enrollment reader or the Device. 2. Press finger on the scanner according to the on-screen instructions. 3. Click Add.  • Fingerprint function is only available on select models. • We do not recommend you set the first fingerprint as the duress fingerprint. • One user can only set one duress fingerprint. • Fingerprint function is available if the Device supports connecting a fingerprint module.
Bluetooth Card	 Bluetooth is only available on select models. You can select Request through Email or Request through Registration Code. • Request through Email : Suitable for the first time a Bluetooth card is requested. You can request up to 5 Bluetooth cards, and have to use the email that is registered to DMSS.  You must have entered your reserved Email before you use the function. 1. Configure the Email that is registered to DMSS. 2. Click Request through Email, and then the Bluetooth cards can be requested. • Request through Registration Code : Suitable when you already have a Bluetooth card and want to reuse it on another access controller supporting Bluetooth function. 1. Copy the Bluetooth registration code from the DMSS. 2. Click Request through Registration Code, and then enter the code. 3. Click OK.

Step 3 Click **OK**.

Related Operations

- Import user information: Click **Export** , download the template and enter user information in it. Click **Import** to import the folder.



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

- Clear: Clear all users.
- Refresh: Refresh the user list.

- Click  to edit the person information.
- Select people, and then click **Delete** to delete users.
- Search: Search by user name or user ID.
- Click **Bluetooth Cards Records**, and then you can view the Bluetooth card records. For users who issued cards unsuccessfully, you can reissue cards here.



You can issue cards in batches on devices that support Bluetooth function.

- Click **Batch Issue Cards** , and then select from **Issue Cards to Selected Users** or **Issue Cards to All Users**.
 - ◇ On **Requestable** tab, you can view all users who can be issued Bluetooth cards, and then click **Request through Email** to issue Bluetooth card in batches.



- Bluetooth cards can only be generated in batches through emails.
- Cloud service should be online.

- ◇ On **Non-Requestable** tab, you can view users without Email who cannot be issued cards.
 - Click **Export Users that Lack Emails** to download the user list on the local compute, and then enter the Email.
 - Click **Import** to import the user list so that you can issue card to them.

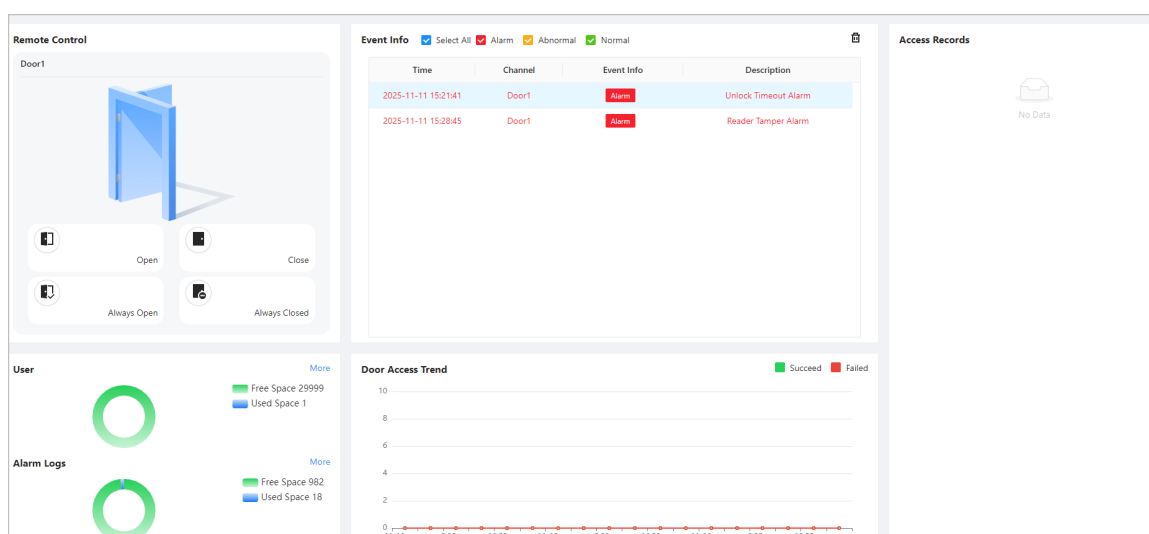
3.5 Access Monitoring

Log in to the web page, and the system automatically goes to the **Access Monitoring** page.



- For first-time use, download and install the plug-in according to the prompt.
- You can also click the web service icon at the upper-left corner to view the access monitoring page.

Figure 3-5 Access monitoring



Remote Control

- Click **Open** or **Close** next to the door to remotely control the door.
- Click **Always Open** or **Always Closed** to remotely control the door. Click **Restore** to restore the door to normal status.

Door Access Trend

The access trend in the last 3 days is displayed. Green means successful access and red means failed access.

Access Records

The real-time access records are displayed, including images, person information, verification method and verification time.

Event Information

In the **Event Info** area, select the event type to view the events. Click  to clear all the events.

User and Alarm Logs

View the space information of users and alarm logs. Click **More** to view the details.

3.6 Configuring Access Control

3.6.1 Configuring Access Control Parameters

3.6.1.1 Configuring Basic Parameters

Procedure

Step 1 Select **Access Control** > **Access Control Parameters**.

Step 2 In **Basic Settings**, configure basic parameters for the access control.

Figure 3-6 Basic parameters

The screenshot shows the 'Basic Settings' window for configuring access control parameters. The window has a title bar 'Basic Settings' and a light gray background. The settings are organized into several rows:

- Name:** A text input field containing 'Door1'.
- Door Status:** Three radio buttons: 'Normal' (selected), 'Always Closed', and 'Always Open'.
- Normally Open Period:** Two dropdown menus, both set to 'Disabled'. The first is labeled 'General Plan' and the second 'Holiday Plan'.
- Normally Closed Period:** Two dropdown menus, both set to 'Disabled'. The first is labeled 'General Plan' and the second 'Holiday Plan'.
- Verification Interval:** A text input field with '0' and a unit 's (0-180)'.
- Card Swiping Interval:** A text input field with '0' and a unit 's (0-86400)'.
- Public Password:** A text input field and a checkbox.
- Tamper Reset:** A toggle switch.

Table 3-4 Basic parameters description

Parameter	Description
Name	The name of the door.
Door Status	Set the door status. • Normal: The door will be unlocked and locked according to your settings. • Always Open: The door remains unlocked all the time. • Always Closed: The door remains locked all the time.
Normally Open Period	When you select Normal , you can select a time template from the drop-down list. The door remains open or closed during the defined time.
Normally Closed Period	 • When the normally open period conflicts with the normally closed period, normally open period takes priority over normally closed period. • When period conflicts with holiday plan, holiday plans take priority over periods.

Parameter	Description
Verification Interval	If you verify your identity multiple times within a defined period, only the earliest verification will be considered valid, and the door will not open after the second or later verifications. From the moment the door fails to open, you must wait for the configured verification time interval before attempting to verify your identity again.
Card Swiping Interval	For first-time verification through card, you can normally unlock the door or perform attendance, and the records are generated. Within the configured period, if you swipe the card for verification again, you cannot unlock the door or perform attendance, and the records are not generated. Please verify the identity after the configured period.  The Card Swiping Interval takes priority over Verification Interval.
Public Password	After the public password is enabled, configure the password. You can use the public password without entering the user ID to unlock the door. Only one public password is supported for one device.
Tamper Reset	When enabled, you can restore to factory defaults through the tamper button on the rear panel of the device. Tamper reset operation: Within 5 minutes after the device starts up, press the tamper-proof button 5 times consecutively within 8 seconds. The standby screen of the device displays a factory reset prompt. Tap Confirm or press and hold the tamper button for 3 seconds or longer. The device restarts. All configurations and information will be restored to the factory default.

Step 3 Click **Apply**.

3.6.1.2 Configuring Unlock Methods

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

Procedure

Step 1 Select **Access Control** > **Access Control Parameters**.

Step 2 In **Unlock Settings**, select an unlock method.

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

Figure 3-7 Combination unlock

Unlock Settings

Unlock Method

Combination Unlock

Combination Method

☒ Or
☐ And

Unlock Method (Multi-select)

☒ Card
☒ Password
☒ Bluetooth Card

Bluetooth Mode

☐ Short-range
☒ Long-range

PIN Code Authentication

☐

Door Unlocked Duration

3.0
s (0.2-600)

Remote Verification

☒

Remote Verification Unlock Period

General Plan

Disabled

Holiday Plan

Disabled

Apply

Refresh

Default

Table 3-5 Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	Unlock methods might differ depending on product models.
PIN Code Authentication	When PIN code authentication is enabled, you can open the door with just the password.
Door Unlocked 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 to 600 seconds.
Remote Verification	Open the door remotely. After the function is enabled, select the general plan and the holiday plan.
Bluetooth Mode	Select the range for Bluetooth. You can select from Long-range and Short-range .  It is only available for devices with Bluetooth function.

- Unlock by multiple users.
 - ◇ If only one group is added, the door unlocks only after the number of people in the group who grant access equals the defined valid number.
 - ◇ If more than one groups are added, the door unlocks only after the number of people in each group who grant access equals the defined valid number.
- 1. In the **Unlock Mode** list, select **Unlock by Multiple Users**.
- 2. Click **Add** to add groups.
- 3. Select the unlock method and users, configure the valid number, and then click **OK**.
 - ◇ You can add up to 4 groups.
 - ◇ The unlock methods only support the relationship of **Or**.

- ◇ The valid number indicates the number of people in each group who need to verify their identities on the Device before the door unlocks. For example, if the valid number is set to 3 for a group, any 3 people in the group need to verify their identities to unlock the door.

The valid number cannot exceed the number of the users in the user list.

Figure 3-8 Add group

Add

No. 1

Unlock Method ... Card x

Valid No. 1 (1-50)

Select Person User ID/Name

	No.	User ID	Name
☒	1	1	
☒	2	1000...	10000002
☐	3	1000...	10000003
☐	4	1000...	10000004
☐	5	1000...	10000005

Selected People

Clear

>

No.	User ID	Name	Operation
1	1		
2	10000...	10000...	

OK

Cancel

Figure 3-9 Unlock by multiple users

Table 3-6 Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	Unlock methods might differ depending on the models of product.
Verification of Multi-person Unlock Timeout Duration	During verification, the interval between every two verifiers must be within this time period.
PIN Code Authentication	When PIN code authentication is enabled and you select user password to unlock, you only need to enter the user password without the user ID. When PIN code authentication is enabled, the remote verification is not supported when using user password to unlock.
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for the person to pass through. It ranges from 0.2 to 600 seconds.
Remote Verification	If this function is enabled, you can control the door on the corresponding platform.
Bluetooth Mode	Select the range for Bluetooth. You can select from Long-range and Short-range. It is only available for devices with Bluetooth function.

- Unlock by period

1. In the **Unlock Method** list, select **Unlock by Period**.
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.

Figure 3-10 Unlock by period

The screenshot shows the 'Unlock Settings' interface. At the top, there's a section for 'Unlock Method' with a dropdown set to 'Unlock by Period'. Below this is a weekly schedule grid with days of the week (Sun to Sat) and time slots (0 to 24). A modal window is open over the grid, showing 'Time' (00:00:00 to 23:59:59), 'Combination' (Or selected), and 'Unlock Method' (Card and Password selected). Below the grid, there are options for 'Bluetooth Mode' (Short-range and Long-range), 'PIN Code Authentication' (toggle), and 'Door Unlocked Duration' (3.0 s).

Step 3 Click **Apply**.

3.6.2 Alarm

3.6.2.1 Configuring Alarm

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

Procedure

Step 1 Select **Access Control** > **Alarm** > **Alarm**.

Step 2 (Optional) Select the door channel.

If you have selected **Lock Extension Module** as the **External Device** through **Communication Settings** > **RS-485 Settings** on the Access Controller, you can select the channel here.

Figure 3-11 Select the channel

The screenshot shows a 'Door Channel' label next to a dropdown menu. The dropdown menu is open, showing the number '1' as the selected option.

Step 3 Configure alarm parameters.

Figure 3-12 Alarm

Duress Alarm

☒

Anti-passback

☒

Door Detector

☒

☐ NC
☒ NO

Intrusion Alarm

☐

Unlock Timeout Alarm

☐

Excessive Attempts Ala...

☒

Buzzer

☐ Enable

Duration

s (1-1800)

Link Alarm Output

☐ Enable

Duration

s (1-1800)

Tamper Alarm

☒

Buzzer

☒ Enable

Duration

s (1-1800)

Link Alarm Output

☐ Enable

Duration

s (1-1800)

Apply

Refresh

Default

Table 3-7 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
Anti-passback	Users need to verify their identities both for entry and exit; otherwise an alarm will be triggered. It helps prevents a card holder from passing an access card back to another person to gain entry. When anti-passback is enabled, the card holder must leave the secured area through an exit reader before system will grant another entry. ● If a person enters after authorization and exits without authorization, an alarm will be triggered when they attempt to enter again, and access is denied at the same time. ● If a person enters without authorization and exits after authorization, an alarm will be triggered when they attempt to enter again, and access is denied at the same time.  If the Device can only connect one lock, verifying on the Device means entry direction, and verifying on the external card reader means exit direction by default. You can modify the setting on the management platform.
Door Detector	With the door detector wired to your device, alarm can be triggered when doors are opened or closed abnormally. The door detector includes 2 types, including NC detector and NO detector. ● NC: The sensor is in a shorted position when the door or window is closed. ● NO: An open circuit is created when the window or door is actually closed.
Intrusion Alarm	If the door is opened abnormally, an intrusion alarm will be triggered and last for a defined time.  The door detector and intrusion need to be enabled at the same time.
Unlock Timeout Alarm	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time.
Unlock Timeout	 The door detector and door timed out function need to be enabled at the same time.
Excessive Use Alarm	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time.
Tamper Alarm	The tamper alarm is triggered by pressing the tamper button.

Step 4 Click **Apply**.

3.6.2.2 (Optional) Configuring Alarm Linkages

You can configure alarm linkages.

Procedure

Step 1 Select **Access Control** > **Alarm** > **Alarm Linkage Setting**.



- If the Device is added to a management platform, the alarm settings will be synchronized to the platform.
- This function is only available on models that have alarm input and alarm output ports.
- The number of alarm input and output ports differs depending on models of the product.

Step 2 Click  to configure alarms.

Figure 3-13 Alarm linkage

Alarm-in Port: 1 Name: Zone1

Alarm Input Type: NO Link Fire Safety Control: ☐

Alarm-out Port: ☐

Duration: 30 s (1-300)

Alarm Output Channel: ☒ 1

Access Control Linkage: ☐

Information: When the heat alarm signal disappears, the door will automatically return to the normal authentication mode.

Linkage Mode: Weak Execution

Channel Type: NO

OK Cancel

Step 3 Create a name for the alarm zone.

Step 4 Enable **Link Fire Safety Control**, and select a type for the alarm input device.

- Normally Closed: The alarm input is in a normally closed (NC) circuit state when the alarm has not been tripped. Opening a normally closed circuit sets off the alarm.
- Normally Open: The alarm input device is in a normally open (NO) circuit state when the alarm has not been tripped. Closing the circuit sets off the alarm.

Step 5 If you want to link access control when the fire alarm is triggered, enable **Access Control Linkage**.



This function takes effect only after **Link Fire Safety Control** is enabled.

Step 6

Select a linkage mode.

- Strong Execution: When the fire alarm signal disappears, the door remains in the current status. Please manually change to its previous door status settings if you want to.
- Weak Execution: When the fire alarm signal disappears, the door automatically returns to its previous door status.

Step 7

Select a channel type.

- NO: The door automatically opens when fire alarm is triggered.
- NC: The door automatically closes when fire alarm is triggered.

Step 8

Click **OK**.

3.6.3 Card Settings

3.6.3.1 Configuring Card Settings



This function is only available on select models.

Procedure

Step 1

Log in to the webpage.

Step 2

Select **Access Control** > **Card Settings** > **Card Settings**.

Step 3

Configure the card parameters.

Figure 3-14 Card parameters

Card Settings

M1 Card

M1 Card Encryption & Verification

FeliCa Card

Block NFC Cards

DESFire Card

DESFire Card Decryption

Apply

Refresh

Default

Table 3-8 Card parameters description

Item	Parameter	Description
Card Settings	M1 Card	The M1 card can be read when this function is enabled.  This function is only available on select models.
	M1 Card Encryption & Verification	Only the encrypted IC card can be read when this function is enabled.  Make sure M1 Card is enabled.
	FeliCa Card	The FeliCa card can be read when this function is enabled.  This function is only available on select models.

Item	Parameter	Description
	Block NFC Cards	Prevent unlocking through duplicated NFC card after this function is enabled.  • This function is only available on models that support IC cards. • Make sure M1 Card is enabled. • NFC function is only available on select models of phones.
	DESFire Card	The Device can read the card number of Desfire card when this function is enabled.  • This function is only available on models that support IC cards. • Only supports hexadecimal format.
	DESFire Card Decryption	Information in the DESFire card can be read when Enable DESFire Card and DESFire Card Decryption are enabled at the same time.  • This function is only available on models that support IC cards. • Make sure that DESFire card is enabled.
Card No. System	Card No. System	Select decimal format or hexadecimal format for the card number when Wiegand card reader is connected. The card No. system is the same for both card number input and output.
DESFire Card Write	Acquisition Device	Select the device, place the card on the reader, enter the card number, and then click Write to write card number to the card.  • Desfire card function and Desfire card decryption function must be enabled. • Only supports hexadecimal format. • Supports up to 8 characters.
	Card Number	

Step 4 Click **Apply**.

3.6.3.2 Configuring Access Card Rule Parameters

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

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Access Control > Card Settings > Access Card Rule Setting**.

Step 3 Click **Add**, and then configure new Wiegand formats.

Figure 3-15 Add new Wiegand formats

Table 3-9 Wiegand format description

Parameter	Description
Wiegand format	The name of the Wiegand format.
Total bits	Enter the total number of bits.
Facility Code	Click Add , 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	- Click Add. - Enter the even parity start bit and even parity end bit. - Enter the odd parity start bit and odd parity end bit.

Step 4 Click **OK**.

Related Operations

- You can also click **Add Protocol** to import a Wiegand file to the platform.
- Facility Code: If the function is enabled, and you have set **Card No. System** to decimal format on the **Person Management** page, the facility code and the card number are transformed into decimal format separately, and then combined together.
- HID26: If the function is turned on:
 - Only Wiegand 26 is supported.
 - The platform only supports displaying card in decimal format.

- ◇ The card number must have 5 characters and the facility code must have 3 characters at most. When you manually enter a card, the system will automatically add leading zeros 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.

3.6.3.3 Configuring Custom Conversion

When reading third-party cards using the built-in reader of the device, the external RS-485 card reader, or the external Wiegand card reader, if the actual card number does not match any card number in the system, you can configure the custom conversion for the card number to ensure that the converted card number matches the one in the system.

Procedure

- Step 1** Log in to the webpage.
- Step 2** Select **Access Control** > **Card Settings** > **Custom Conversion**.
- Step 3** Enable the conversion function, and then select the matching mode.
- Auto match: Use the built-in conversion rule of the Device to convert the card number.
 - Select the input type.
 - ◇ Device input: Swipe the card on the Device to read the card.
 - ◇ RS-485 input: Swipe the card on the connected RS-485 card reader to read the card.
 - ◇ Wiegand input: Swipe the card on the connected Wiegand card reader to read the card.
 - Read the card number through the device or enter the card number before conversion, and then enter the card number after conversion.
 - Click **Auto Match**.
 - ◇ If the card numbers are successfully matched, you can click **Export** to export the rule and import to another device for quickly switching the match rules.
 - ◇ If the card numbers failed to match, it indicates that there is no match rule in the system. You need to customize the match rule script, and select **Import Conversion Rule** to import the rule to the device.
 - ◇ If you need to modify the match rule, click **Change Matching Rule**.

Figure 3-16 Auto match (successfully matched)

The screenshot shows the 'Custom Conversion' configuration page. At the top, there is an 'Enable' toggle switch which is turned on. Below it, the 'Matching Mode' is set to 'Auto Match' (indicated by a selected radio button). The 'Status' is 'Applied'. Under 'Input Type', three checkboxes are checked: 'Device Input', 'RS-485 Input', and 'Wiegand Input'. A table displays card conversion data:

No.	Card No. Before Conversion (Device Input)	Card No. Before Conversion (RS-485 Input)	Card No. Before Conversion (Wiegand Input)	Card No. After Conversion
1	1A283C4D	1A283C4D	1A283C4D	4D3C281A
2				
3				

Below the table, a green checkmark icon and the text 'Successfully Matched' are displayed, along with a sub-note: 'This rule will automatically apply to this device.' At the bottom, there are two buttons: 'Change Matching Rule' and 'Export'.

- Import conversion rule: Import other rules to convert the card number.

Click **Upload File** , select the rule file, and then click **Open**.

Figure 3-17 Import conversion rule

3.6.4 Configuring Periods

Configure general plans and holiday plans, and then you can define when a user has the permissions to unlock doors.

3.6.4.1 Configuring General Plan

You can configure up to 128 periods (from No.0 through No.127) of general plans. In each period, you need to configure door access schedules for a whole week. People can only unlock the door during the scheduled time.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Access Control** > **Period Config** > **General Plan**.
- Step 3 Click **Add**.
 1. Configure the plan number and the plan name.
 2. Drag the time slider to configure time for each day.
 3. (Optional) Click **Copy** to copy the configuration to the rest of the days.

Figure 3-18 Configure general plan

The screenshot shows a web-based configuration window titled "Add". It contains the following elements:

- No.:** A dropdown menu currently showing "0".
- General Plan Name:** A text input field containing "Plan 1".
- Time Plan:** A section with a horizontal timeline at the top labeled 0 through 11. Below this is a table with rows for days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat) and columns for each hour. A blue shaded region covers the time range from 12:30:00 to 23:59:59 across all days. To the right of each row is a "Copy" link.
- Time Selection Pop-up:** A small dialog box is open over the timeline, showing a time range from 12:30:00 to 23:59:59 with "OK" and "Delete" buttons.
- Bottom Buttons:** "OK" and "Cancel" buttons are located at the bottom right of the main window.

Step 4 Click **OK**.

3.6.4.2 Configuring Holiday Plan

You can configure up to 128 holiday groups (from No.0 through No.127), and for each holiday group, you can add up to 16 holidays in it. After that, you can assign the configured holiday groups to the holiday plan. Users can only unlock the door during the defined time of the holiday plan.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Access Control > Period Config > Holiday Plan**.
- Step 3 Click **Holiday Management**, and then click **Add**.
 1. Select a number for the holiday group, and then enter a name for the group.

Figure 3-19 Add a holiday group

The 'Add' dialog box contains the following fields and elements:

- No.:** A dropdown menu with the value '2' selected.
- Holiday Group Name:** A text input field containing 'Holiday Group for 2023'.
- Holiday Group Config:** A section containing an 'Add' button and a table.

No.	Holiday Name	Start Time	End Time	Operation
1	National Day	2023-10-01	2023-10-07	

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

2. Click **Add** , add a holiday to a holiday group, and then click **OK**.

Figure 3-20 Add a holiday to a holiday group

The 'Edit' dialog box contains the following fields and elements:

- Holiday Name:** A text input field containing 'National Day'.
- * Period:** A date range selector showing '2023-10-01' to '2023-10-07' with a calendar icon on the right.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Step 4 Click **OK**.

Step 5 Click **Plan Management** , and then click **Add**.

1. Select a number for the holiday plan, and then enter a name for it.
2. Select a holiday group, and then drag the slider to configure time for each day.
Supports adding up to 4 time sections per day.

Figure 3-21 Add holiday plan

The screenshot shows an 'Edit' dialog box with the following fields:

- No.:** A dropdown menu showing '0'.
- Holiday Plan Name:** A text input field containing 'Holiday plan for 2023'.
- Holiday Group No.:** A dropdown menu showing '1'.
- Time Plan:** A section containing a calendar grid and a time selection pop-up.
 - The calendar grid has a header row with numbers 0 through 8, and a row labeled 'Holid'.
 - The time selection pop-up shows a time range from 08:30:00 to 23:59:59, with 'OK' and 'Delete' buttons.
 - A 'Copy' button is located to the right of the calendar grid.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Step 6 Click **OK**.

3.6.5 Configuring QR Code

Procedure

- Step 1 On the webpage, select **Access Control** > **QR Code**.
- Step 2 Configure illuminator mode and QR code validity period, and then click **Apply**.
- Always on: The illuminator is always on.
 - Close: The illuminator is closed.
 - Auto-sensing: The illuminator lights up upon detecting an object, and turns off after successful scanning. Auto-sensing is selected by default.

Figure 3-22 Configure illuminator

The screenshot shows the 'Configure illuminator' form with the following fields and buttons:

- Illuminator Mode:** A dropdown menu showing 'Auto-Sensing'.
- QR Code Validity Period (sec):** A text input field containing '60', with a range '(0-86400)' indicated to the right.
- Buttons:** 'Apply', 'Refresh', and 'Default' buttons are located at the bottom.

3.6.6 Configuring Back-end Comparison

Before configurations, make sure that the Device is connected to the third-party platform through an SDK. You can directly pass data such as QR code or card number to the third-party platform for data validation rather than validating data on the Device.

Procedure

- Step 1 Log in to the webpage of the device.
- Step 2 Select **Access Control** > **Back-end Comparison**.

Figure 3-23 Back-end comparison

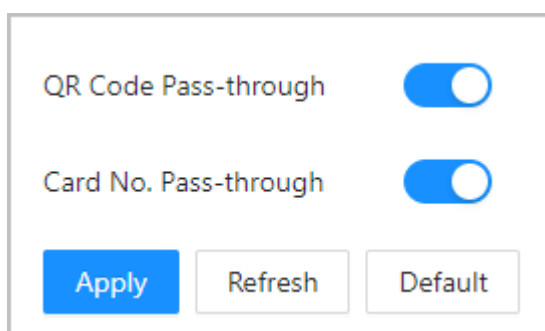


Table 3-10 Back-end comparison

Parameters	Description
QR Code Pass-through	After it is enabled, the scanned QR code is passed to the third-party platform for data validation.
Card No. Pass-through	After it is enabled, the card number is passed to the third-party platform for data validation.

3.6.7 Configuring Port Functions

Some ports can function as different ports. You can set them to different ports based on the actual needs.

Background Information

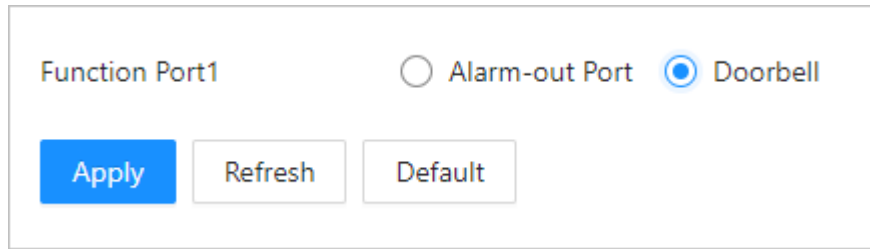


- This function is only available on select models.
- Ports might differ depending on the models of the product.

Procedure

- Step 1 On the webpage, select **Access Control** > **Port Config**.
- Step 2 Select the type of the port.
It is **Doorbell** by default.
- Step 3 Click **Apply**.

Figure 3-24 Configure ports



3.6.8 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, 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 On the home page, select **Access Control** > **Unlock Method Config**.
- 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 and roles 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-card unlock or multi-person unlock function will become ineffective.
- Users need to verify their identities 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 turned off at the same time, all types of users cannot unlock the door using their password.

3.6.9 Configuring First-Person Unlock

Any person can access doors only after the persons you specify pass through. When you specify multiple persons, other persons can access doors after any one of the specified persons passes through.

Prerequisites

Persons can only be set as first persons when they have permissions to access doors.

Procedure

Step 1 On the home page, select **Access Control** > **First-Person Unlock**.

Step 2 Select the door channel, and then enable the function.

Figure 3-25 First-person unlock

Step 3 Configure the parameters.

Table 3-11 Parameter description

Parameter	Description
Time Templates	Select when this rule is effective.
Door Status after First-Card Unlock	● Normal : Other persons must verify their identifications to pass. ● Always Open : All people can pass without verifying their identifications.
Person List	Click + to select one or more persons, and they will have permissions to access the doors.

Step 4 Click **Apply**.

3.6.10 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 system will grant another entry.

- 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 enters 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** On the home page, select **Access Control** > **Anti-passback Group Config**.
- Step 2** Turn on this function, and then configure a reset time.
Specify a time when the anti-passback status of all personnel will be reset.
- Step 3** Select the general plan and the holiday plan.
Anti-passback is effective during the defined time.
- Step 4** In entry group, click **Add**, and then select the card reader.
- Step 5** In exit group, click **Add**, and then select the card reader.

Figure 3-26 Anti-passback

Enable ☒

Reset Time min (5-300)

Time Templates

General Plan Holiday Plan

Anti-passback Group Config [?]

Entry Group

+ Add Clear

/Reader 1
[Remove](#)

Exit Group

+ Add Clear

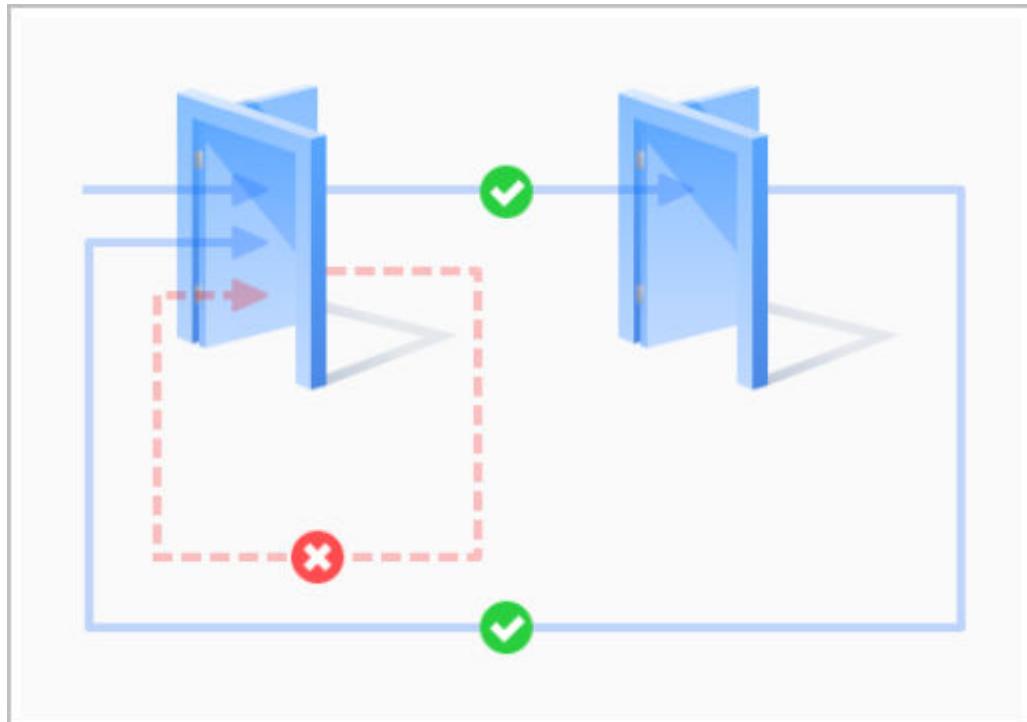
/Reader 2
[Remove](#)

- Step 6** Click **Apply**.

Results

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

Figure 3-27 Anti-passback function



3.7 Configuring Audio

Procedure

- Step 1 Log in to the webpage of the device.
- Step 2 Select **Audio**.
- Step 3 Enable **Key Sound** or **DND Mode** based on your needs.

Figure 3-28 Audio

Audio Config

Key Sound ☒

DND Mode ☐

Apply Refresh Default

Table 3-12 Description of audio parameters

Parameters	Description
Key Sound	When enabled, touchscreen devices will produce a prompt sound for local touch operations, while non-touchscreen devices will produce a prompt sound for key/button operations.
DND Mode	When enabled, there will be no prompt sounds for local verification (such as door access or attendance) during the configured time periods. Supports up to 4 time periods.

Step 4 Click **Apply**.

3.8 Communication Settings

3.8.1 Network Settings

3.8.1.1 Configuring TCP/IP

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

Procedure

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

Step 2 Configure the parameters.

Figure 3-29 TCP/IP

The image shows a TCP/IP configuration window. At the top, there's a 'NIC' dropdown menu set to 'NIC 1'. Below it, the 'Mode' section has two radio buttons: 'DHCP' (unselected) and 'Static' (selected). The 'MAC Address' field is a text box with a light gray background. The 'IP Version' dropdown is set to 'IPv4'. Below this are four text boxes for 'IP Address', 'Subnet Mask', 'Default Gateway', and 'Preferred DNS', each with a light gray background. The 'Alternate DNS' field is also a text box with a light gray background. At the bottom, there's an 'MTU' field set to '1500'. Below the fields are three buttons: 'Apply' (blue), 'Refresh' (light gray), and 'Default' (light gray).

Table 3-13 Description of TCP/IP

Parameter	Description
Mode	• Static: Manually enter IP address, subnet mask, and gateway. • DHCP: It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Device will automatically be assigned with IP address, subnet mask, and gateway.
MAC Address	MAC address of the Device.
IP Version	IPv4 or IPv6.

Parameter	Description
IP Address	If you set the mode to Static , configure the IP address, subnet mask and gateway.
Subnet Mask	
Default Gateway	
	 • IPv6 address is represented in hexadecimal. • IPv6 version does not require setting subnet masks. • The IP address and default gateway must be in the same network segment.
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.
MTU	MTU (Maximum Transmission Unit) refers to the maximum size of data that can be transmitted in a single network packet in computer networks. A larger MTU value can improve network transmission efficiency by reducing the number of packets and associated network overhead. If a device along the network path is unable to handle packets of a specific size, it can result in packet fragmentation or transmission errors. In Ethernet networks, the common MTU value is 1500 bytes. However, in certain cases such as using PPPoE or VPN, smaller MTU values may be required to accommodate the requirements of specific network protocols or services. The following are recommended MTU values for reference: • 1500: Maximum value for Ethernet packets, also the default value. This is a typical setting for network connections without PPPoE and VPN, some routers, network adapters, and switches. • 1492: Optimal value for PPPoE • 1468: Optimal value for DHCP. • 1450: Optimal value for VPN.

Step 3 Click **Apply**.

3.8.1.2 Configuring Wi-Fi



- The Wi-Fi function is available on select models.
- The Wi-Fi and Wi-Fi AP cannot be enabled at the same time.

Procedure

Step 1 Select **Communication Settings** > **Network Setting** > **Wi-Fi**.

Step 2 Turn on Wi-Fi.

All available Wi-Fi networks are displayed.

Figure 3-30 Wi-Fi

Wi-Fi ☒

Mode ☒ DHCP ☐ Static

MAC Address

IP Address

Subnet Mask

Default Gateway

Preferred DNS

Alternate DNS

Name	Signal Strength	Status	Connect
No Data			



- Wi-Fi and Wi-Fi AP cannot be enabled at the same time.
- Wi-Fi function is only available on select models.

Step 3 Click +, and then enter the password of the Wi-Fi.

The Wi-Fi is connected.

Related Operations

- DHCP: Enable this function and click **Apply**, the Device will automatically be assigned a Wi-Fi address.
- Static: Enable this function, manually enter a Wi-Fi address, and then click **Apply**, the Device will connect to the Wi-Fi.

3.8.1.3 Configuring Wi-Fi AP



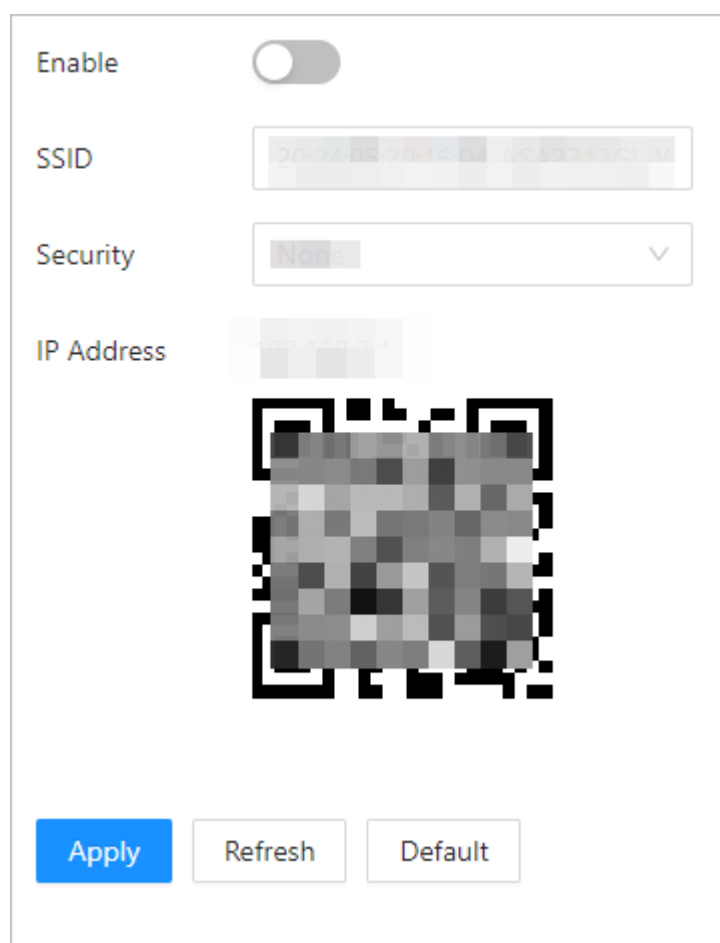
- The Wi-Fi function is available on select models.
- The Wi-Fi and Wi-Fi AP cannot be enabled at the same time.

Procedure

Step 1 Select **Communication Settings** > **Network Setting** > **Wi-Fi AP**.

Step 2 Enable the function, and then click **Apply**.

Figure 3-31 Wi-Fi AP

The image shows a web-based configuration interface for a Wi-Fi Access Point (AP). It features a toggle switch for 'Enable', which is currently turned off. Below this are input fields for 'SSID' (containing a masked string), 'Security' (set to 'None'), and 'IP Address' (containing a masked IP). A large QR code is displayed in the center of the interface. At the bottom, there are three buttons: 'Apply' (blue), 'Refresh' (white), and 'Default' (white).

Results

After it is enabled, you can connect to the Device Wi-Fi through your phone, and log in to the webpage of the Device on your phone.

3.8.1.4 Configuring Port

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

Procedure

- Step 1 Select **Communication Settings** > **Network Setting** > **Port**.
- Step 2 Configure the ports.

Figure 3-32 Configure ports

Max Connection	50	(1-50)
TCP Port	37777	(1025-65535)
HTTP Port	80	
HTTPS Port	443	
Apply Refresh Default		



You need to restart the Device to make the configurations effective after you configure parameters.

Table 3-14 Description of ports

Parameter	Description
Max Connection	You can set the maximum number of clients (such as webpage, desktop client and mobile client) that can access the Device at the same time.
TCP Port	The default value is 37777.
HTTP Port	The default value is 80. If you have changed the port number, add the port number after the IP address when access the webpage.
HTTPS Port	The default value is 443.

Step 3 Click **Apply**.

3.8.1.5 Configuring Basic Service

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

Procedure

Step 1 Select **Communication Settings** > **Network Settings** > **Basic Services**.

Step 2 Configure the basic service.

Figure 3-33 Basic service

SSH ☒

Multicast/Broadcast Search ☒

CGI ☒

ONVIF ☒

Emergency Maintenance ☐

i For easy access to our after-sales service, enable this function. If the device has any trouble performing functions, such as updating, the system will automatically enable this function.

Private Protocol Authentication Mode Security Mode (Recommended) ▾

Private Protocol ☒

*Before enabling private protocol TLS, make sure that the corresponding device or software supports this function.

TLSv1.1 ☐

LLDP ☐

Apply Refresh Default

Table 3-15 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.
Mutlicast/Broadcast Search	Search for devices through multicast or broadcast protocol.
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.
Emergency Maintenance	It is turned on by default.
Private Protocol Authentication Mode	Set the authentication mode, including safe mode and compatibility mode. It is recommended to choose Security Mode. - Security Mode (recommended): Does not support accessing the device through Digest, DES, and plaintext authentication methods, improving device security. - Compatible Mode: Supports accessing the device through Digest, DES, and plaintext authentication methods, with reduced security.
Private Protocol	The platform adds devices through private protocol.

Parameter	Description
TLSv1.1	TLSv1.1 refers to Transport Layer Security version 1.1. TLS is a cryptographic protocol designed to provide secure and authenticated communication over a computer network.  Security risks might present when TLSv1.1 is enabled. Please be advised.
LLDP	LLDP is the abbreviation for Link Layer Discovery Protocol, which is a data link layer protocol. It allows network devices, such as switches, routers, or servers, to exchange information about their identities and capabilities with each other. The LLDP protocol helps network administrators gain a better understanding of network topology and provides a standardized way to automate the discovery and mapping of connections between network devices. This makes it easier to perform network configuration, troubleshoot issues, and optimize performance.

Step 3 Click **Apply**.

3.8.1.6 Configuring Cloud Service

The cloud service provides a NAT penetration service. Users can manage multiple devices through DMSS. You do not have to apply for dynamic domain name, configure port mapping or deploy server.

Procedure

Step 1 On the home page, select **Communication Settings > Network Setting > Cloud Service**.

Step 2 Turn on the cloud service function.

The cloud service goes online if the P2P and PaaS are online.

Figure 3-34 Cloud service

Enable ☒

After the function is enabled and the device connects to the network, we will collect device information such as the IP address, MAC address, device name and serial number. The collected information will only be used to remotely access the device. If you do not want to enable this function, please clear the selection from the check box.

P2P Status ● Offline

PaaS Status ● Offline

SN 8[REDACTED]759



Apply

Refresh

Step 3 Click **Apply**.

Step 4 Scan the QR code with DMSS to add the device.

3.8.1.7 Configuring SDK Auto Registration

The auto registration enables the devices to be added to the management platform without manual input of device information such as IP address and port.

Background Information

The auto registration only supports SDK.

Procedure

Step 1 On the home page, select **Communication Settings > Network Settings > Auto Registration > SDK Auto Registration**.

Step 2 Enable the auto registration function and configure the parameters.

51

Figure 3-35 Auto Registration

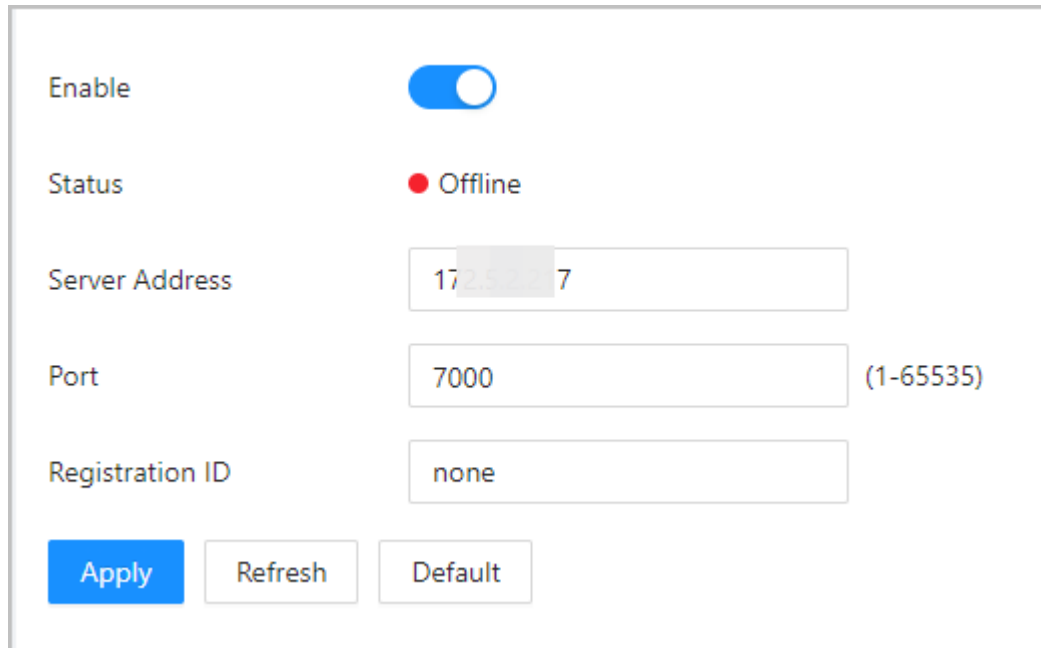


Table 3-16 Automatic registration description

Parameter	Description
Status	Displays the connection status of auto registration.
Server Address	The IP address or the domain name of the server.
Port	The port of the server that is used for automatic registration.
Registration ID	The registration ID (user defined) of the device. You can add the device to the management platform by entering the platform.

Step 3 Click **Apply**.

3.8.1.8 Configuring CGI Auto Registration

Connect to a third-party platform through CGI protocol.

Background Information



Only supports IPv4.

Procedure

Step 1 On the home page, select **Communication Settings** > **Network Settings** > **Auto Registration** > **CGI Auto Registration**.

Step 2 Enable this function, and then click  to configure the parameters.

Table 3-17 Automatic registration description

Parameter	Description
Device ID	Supports up to 32 bytes, including Chinese, numbers, letters, and special characters.
Address Type	Supports 2 methods to register. - Host IP: Enter the IP address of the third-party platform. - Domain Name: Enter the domain name of the third-party platform.
Host IP	
Domain Name	
HTTPS	Access the third-party platform through HTTPS. HTTPS secures communication over a computer network.

Step 3 Click **OK**.

3.8.1.9 Configuring Auto Upload

Send user information and unlock records through the management platform.

Procedure

Step 1 On the home page, select **Communication Settings** > **Network Settings** > **Auto Upload**.

Step 2 (Optional) Enable **Push Person Info**.

When the user information is updated or new users are added, the Device will automatically push user information to the management platform.

Step 3 Enable HTTP upload mode.

Step 4 Click **Add**, and then configure parameters.

Figure 3-36 Automatic upload

Table 3-18 Parameters description

Parameter	Description
IP/Domain Name	The IP or domain name of the management platform.
Port	The port of the management platform.
HTTPS	Access the management platform through HTTPS. HTTPS secures communication over a computer network.
Authentication	Enable account authentication when you access the management platform. Login username and password are required.

Parameter	Description
Event Type	Select the type of event that will be pushed to the management platform.  • Before you use this function, enable Push Person Info. • Person information can only be pushed to one management platform and unlock records can be pushed to multiple management platforms.

Step 5 Click **Apply**.

3.8.2 Mode Settings

Log in to the webp age, and select **Communication Settings** > **Mode Settings**.

Card Reader Mode

Select **Mode** as **Card Reader**. The device serves as a card reader externally connected to an access control controller. It does not perform authentication but directly transmits access control information (such as card, password, fingerprint) to the access control controller, which then authenticates and unlocks the door.

Figure 3-37 Card reader mode

Mode

☒ Card Reader ☐ Access Controller

RS-485 Settings

Baud Rate

9600

▼

Data Bit

8

▼

Stop Bit

1

▼

Parity Code

None

▼

Wiegand Settings

Wiegand Output Type

Wiegand 34

▼

Pulse Width (μs)

200

(20-200)

Pulse Interval (μs)

1000

(200-5000)

The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.

Apply

Refresh

Default

Access Controller Mode

Set **Mode** as **Access Controller**.

Figure 3-38 Access controller mode

Mode

☐ Card Reader ☒ Access Controller

RS-485 Settings

External Device

Card Reader

?

Baud Rate

9600

Data Bit

8

Stop Bit

1

Parity Code

None

Wiegand Settings

Wiegand Settings

☒ Wiegand Input ☐ Wiegand Output

Card No. Inversion

☒

Apply

Refresh

Default

Table 3-19 Description of RS-485

External Device	Description
Access Controller	Select Access Controller when the Device functions as a card reader, and sends data to other external access controllers to control access. Output Data type: • Card Number: Outputs data based on card number when users swipe card to unlock door; outputs data based on user's first card number when they use other unlock methods. • ID: Outputs data based on the user ID.  • When authentication is successful, the relevant information is transmitted to the access controller. In this case, the authentication result displayed is the authentication result of the access controller. • When authentication fails, the relevant information is not transmitted to the access controller, and the authentication result displayed remains as failure.
Card Reader	The device is externally connected to a card reader and transmits access control card information to an access controller or management platform.
Card Reader (OSDP)	The device is externally connected to an OSDP card reader and transmits access control card information to an access controller or management platform.
Door Security Module	The door exit button, lock and fire linkage is not effective after the security module is enabled. • Supports authentication through face, card, fingerprint, password, and other methods to control the door security module for unlocking. • Supports unlocking through an externally connected RS-485 card reader or push-to-open button linked to the door control security module.  Remote unlock of the externally connected door lock through the door security module is not supported.
Lock Extension Module	When the Access Controller is connected to external lock extension module, if you select Lock Extension Module, the local lock is unlocked after you verify the identification on the local device, and the extension lock is unlocked after you verify the identification on the external card reader. After you select Lock Extension Module, you can select channel 2 on the Access Control Parameters and Alarm page on the webpage of the Access Controller.

Table 3-20 Description of Wiegand

Parameter		Description
Wiegand Settings		- When connecting an external card reader device, select Wiegand Input. - When the Device functions as a card reader, and you need to connect it to another access controller, and select Wiegand Output Config.
Wiegand Input	Card No. Inversion	If the card number sequence obtained through Wiegand input does not match the actual card number sequence when interfacing with third-party devices, enable this function.
Wiegand Output	Wiegand Output Type	The bit length of card numbers or ID that the device can recognize and output. - Wiegand 26: Reads 3 bytes or 6 digits. - Wiegand 34: Reads 4 bytes or 8 digits. - Wiegand 66: Reads 8 bytes or 16 digits.
	Pulse Width	Configure the pulse width and interval for wiegand output.
	Pulse Interval	
	Output Data Type	Select a Wiegand format to read card numbers or ID numbers. - User ID: Outputs data based on user ID. - Card: Outputs data based on user's first card number.
	Wiegand Format	When Output Data Type is set as ID , you can select decimal or hexadecimal output formats.

3.8.3 Configuring Bluetooth Settings

Configure the Bluetooth function of the Device. This function is only available on select models.

Procedure

Step 1 Select **Communication Settings** > **Bluetooth Setting**.

Step 2 Enable or turn off **Bluetooth**, and then configure Bluetooth name.

Figure 3-39 Bluetooth

Bluetooth ☒

Bluetooth Name 212F-

Apply Refresh Default

Step 3 Click **Apply**.

Results

You can unlock the door via Bluetooth on the DMSS app..

3.9 Configuring the System

3.9.1 User Management

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

3.9.1.1 Adding Administrators

You can add new administrator accounts, and then they can log in to the webpage of the Device.

Procedure

Step 1 On the home page, select **System** > **Account** > **Account**.

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



- The username cannot be the same as an existing account. The username consists of up to 31 characters and only allows for numbers, letters, underscores, midlines, dots, or @.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: Upper case, lower case, numbers, and special characters (excluding ' " ; : &).

Set a high-security password by following the password strength prompt.

Figure 3-40 Add administrators

The screenshot shows a web-based 'Add' dialog box. It has a title bar with the word 'Add' and a close button (X). The main area contains four labeled input fields: 'Username', 'Password', 'Confirm Password', and 'Remarks'. The 'Password' and 'Confirm Password' fields have a blue strength indicator bar below them. At the bottom right, there are two buttons: 'OK' (blue) and 'Cancel' (white with a grey border).

Step 3 Click **OK**.



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

3.9.1.2 Resetting the Password

Reset the password through the linked email when you forget your password.

Procedure

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

Figure 3-41 Reset Password

Password Reset

Enable ☒

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

Email Address

Password Expires in Days



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

- Step 4 Click **Apply**.

3.9.1.3 Adding ONVIF Users

Background Information

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

Procedure

- Step 1 On the home page, select **System** > **Account** > **ONVIF User**.
- Step 2 Click **Add**, and then configure parameters.

Figure 3-42 Add ONVIF user

Add

*

Username

*

Password

*

Confirm Password

*

Group

OK

Cancel

Table 3-21 ONVIF user description

Parameter	Description
Username	The username cannot be the same as an existing account. The username consists of up to 31 characters and 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 three permission groups which represent different permission levels. admin: You can view and manage other user accounts on the ONVIF Device Manager. Operator: You cannot view or manage other user accounts on the ONVIF Device Manager. User: You cannot view or manage other user accounts and system logs on the ONVIF Device Manager.

Step 3 Click **OK**.

3.9.2 Viewing Online Users

You can view online users who are currently logged in to the web page. On the home page, select **System** > **Online User**.

3.9.3 Configuring Time

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **System** > **Time**.
- Step 3 Configure the time of the Platform.

Figure 3-43 Time settings

Time and Time Zone



Date :
2024-08-05 Monday
Time :
18:50:31

Time

☒ Manually Set ☐ NTP

System Time

2024-08-05 18:50:31 

Sync PC

Time Format

YYYY-MM-DD 

24-Hour 

Time Zone

(UTC+09:30) 

DST

Enable

☐

Type

☒ Date ☐ Week

Start Time

Jan 

1 

00:00 

End Time

Jan 

2 

00:00 

Apply

Refresh

Default

Table 3-22 Time settings description

Parameter	Description
Time	● Manual Set: Manually enter the time or you can click Sync PC to sync time with the computer. ● NTP: The Device will automatically sync the time with the NTP server. ◇ Server : Enter the domain of the NTP server. ◇ Port : Enter the port of the NTP server. ◇ Interval : Enter the time interval for synchronization.
Time Format	Select the time format.
Time Zone	Select the time zone.
DST	1. (Optional) Enable DST. 2. Select Date or Week from the Type. 3. Configure the start time and end time of the DST.

Step 4 Click **Apply**.

3.10 Maintenance Center

3.10.1 One-click Diagnosis

The system automatically diagnoses the configurations and the status of the device to improve its performance.

Procedure

Step 1 On the home page, select **Maintenance Center** > **One-click Diagnosis**.

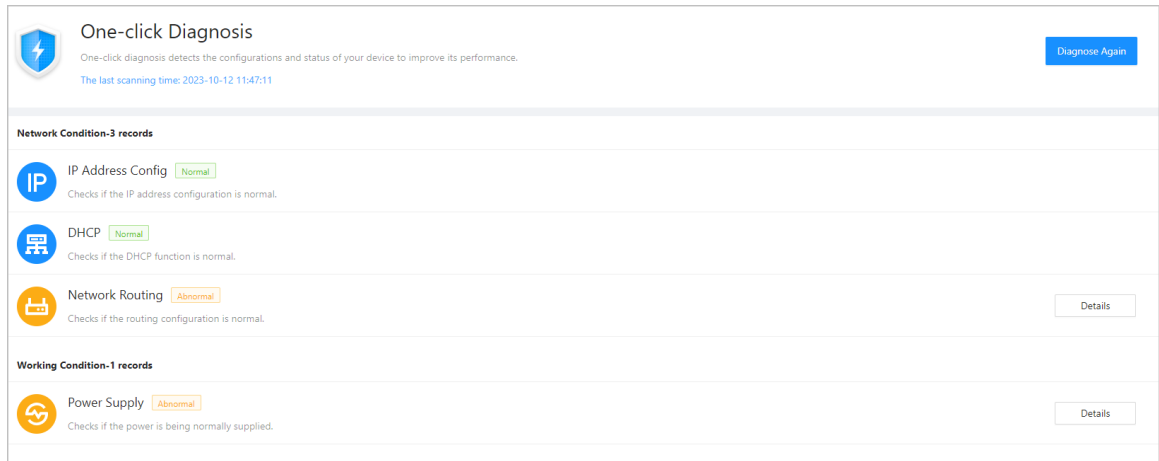
Step 2 Click **Diagnose**.

The system automatically diagnoses the configurations and displays diagnosis results after it completes.

Step 3 (Optional) Click **Details** to view details of abnormal items.

You can ignore the abnormality or optimize it. You can also click **Diagnose Again** to perform automatic diagnosis again.

Figure 3-44 One-click diagnosis



3.10.2 System Information

3.10.2.1 Viewing Version Information

On the webpage, select **Maintenance Center** > **System Info** > **Version**, and you can view version information of the Device.

3.10.2.2 Viewing Legal Information

On the home page, select **Maintenance Center** > **System Info** > **Legal Info**, and you can view the software license agreement, privacy policy and open source software notice.

3.10.3 Data Capacity

You can see how much used/unused space the device can store for users, cards, and Bluetooth cards.

Log in to the web page and select **Maintenance Center** > **Data Capacity**.

3.10.4 Viewing Logs

View logs such as system logs, admin logs, and unlock records.

3.10.4.1 System Logs

View and search for system logs.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Center** > **Log** > **Log**.
- Step 3 Select the time range and the log type, and then click **Search**.

Related Operations

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

3.10.4.2 Unlock Records

Search for unlock records and export them.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Center > Log > Unlock Records**.
- Step 3 Select the time range and the type, and then click **Search**.
- You can click **Export** to download the unlock records.

3.10.4.3 Alarm Logs

View alarm logs.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Center > Log > Alarm Logs**.
- Step 3 Select the type and the time range.
- Step 4 Enter the admin ID, and then click **Search**.

3.10.5 Maintenance Management

When more than one Device need the same configurations, you can configure parameters for them by importing or exporting configuration files.

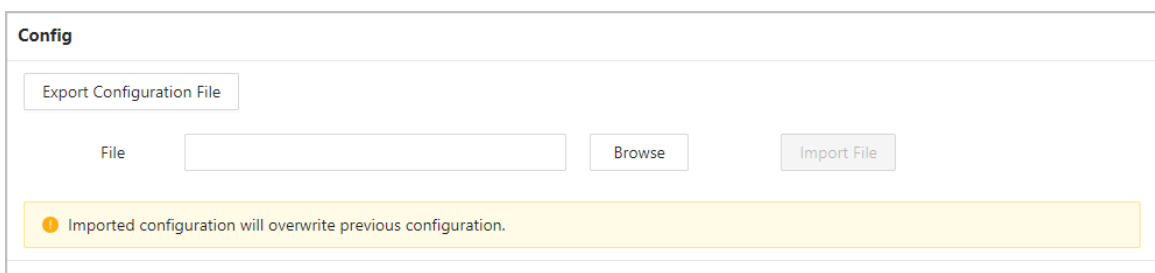
3.10.5.1 Exporting and Importing Configuration Files

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

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Center > Maintenance Management > Config**.

Figure 3-45 Configuration management



The screenshot shows a web interface titled "Config". It contains two main buttons: "Export Configuration File" and "Import File". Below the "Export Configuration File" button, there is a "File" label, a text input field, and a "Browse" button. A yellow warning banner at the bottom states: "Imported configuration will overwrite previous configuration."

Step 3 Export or import configuration files.

- Export the configuration file.

Click **Export Configuration File** to download the file to the local computer.



The IP address will not be exported.

- Import the configuration file.

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

2. Click **Import Configuration**.



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

3.10.5.2 Configuring the Fingerprint Similarity Threshold

Configure the fingerprint similarity threshold. The higher the value is, the higher the accuracy is, and the lower the pass rate.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Maintenance Management** > **Config**.

Step 3 Enter the similarity threshold, and then click **Apply**.



- The parameter is available on the modular access controller with the fingerprint module.
- The parameter is available on the access controller with a fingerprint function.

Figure 3-46 Fingerprint similarity threshold

3.10.5.3 Restoring the Factory Default Settings

Procedure

Step 1 Select **Maintenance Center** > **Maintenance Management** > **Config**.



Restoring the **Device** to its default configurations will result in data loss. Please be advised.

Step 2 Restore to the factory default settings if necessary.

- **Factory Defaults** : Resets all the configurations of the Device and deletes all the data.

- **Restore to Default (Except for User Info and Logs)** : Resets the configurations of the Device and deletes all the data except for user information and logs.

3.10.5.4 Maintenance

Regularly restart the Device during its idle time to improve its performance.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Center** > **Maintenance Management** > **Maintenance**.
- Step 3 Set the time, and then click **Apply**.

The Device will restart at the scheduled time, or you can click **Restart** to restart it immediately.

3.10.6 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 shut down the Device during the update.
- Updating to a lower version might cause potential risks. Please be advised.
- If you start the Device for the first time or restore the Device to factory default settings, the Device automatically backs up the system files within the first 10 minutes. Please do not update in this period.

3.10.6.1 File Update

Procedure

- Step 1 On the home page, select **Maintenance Center** > **Update**.
- Step 2 In **File Update**, click **Browse**, and then upload the update file.



The update file should be a .bin file.

- Step 3 Click **Update**.

The Device will restart after the update finishes.

3.10.6.2 Online Update

Procedure

- Step 1 On the home page, select **Maintenance Center** > **Update**.
- Step 2 In the **Online Update** area, select an update method.
 - Select **Auto Check for Updates**, and the Device will automatically check for the latest version update.
 - Select **Manual Check**, and you can immediately check whether the latest version is available.
- Step 3 (Optional) Click **Update Now** to update the Device immediately.

3.10.7 Advanced Maintenance

Acquire device information and capture packet to make easier for maintenance personnel to perform troubleshooting.

3.10.7.1 Exporting

Procedure

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

3.10.7.2 Packet Capture

Procedure

- Step 1 On the home page, select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.

Figure 3-47 Packet Capture

Packet Capture							
NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size	Packet Sniffer Backup
eth0	1 166	Optional	Optional	Optional	Optional	0.00MB	▶
eth2	1 101	Optional	Optional	Optional	Optional	0.00MB	▶

- Step 2 Enter the IP address, click ▶.
- ▶ changes to ||.
- Step 3 After you acquired enough data, click ||.
- Captured packets are automatically downloaded to your local computer.

3.11 (Optional) Security Settings

3.11.1 Security Status

Scan the user, service, and security modules to check the security status of the Device.

Background Information

- User and service detection: Check whether the current configuration conforms to the recommendation.
- Security modules scanning: Scan the running status of security modules, such as audio and video transmission, trusted protection, security warning and attack defense, not detect whether they are enabled.

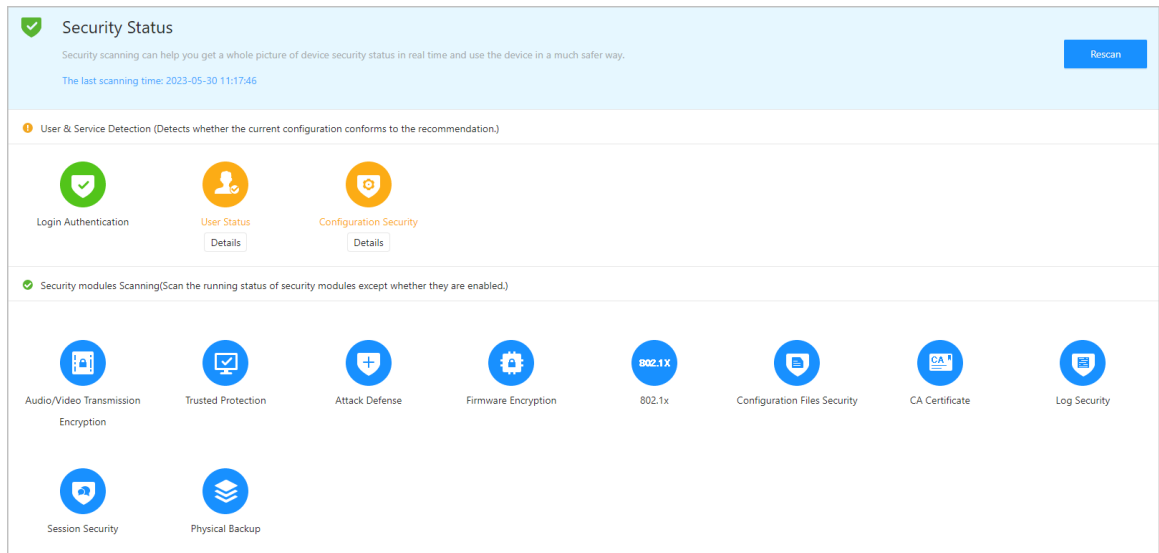
Procedure

- Step 1 Select  > **Security Status**.
- Step 2 Click **Rescan** to perform a security scan of the Device.



Hover over the icons of the security modules to see their running status.

Figure 3-48 Security Status



Related Operations

After you perform the scan, the results will be displayed in different colors. Yellow indicates that the security modules are abnormal, and green indicates that the security modules are normal.

- Click **Details** to view the details on the results of the scan.
- Click **Ignore** to ignore the abnormality, and it will not be scanned. The abnormality that was ignored will be highlighted in grey.
- Click **Optimize** to troubleshoot the abnormality.

3.11.2 Configuring System Service

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 Select  > **System Service** > **System Service**.

Step 2 Turn on the HTTPS service.



If you turn on the compatibility with TLS v1.1 and 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.

Figure 3-49 System service

HTTPS

Enable ☒

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

Auto Redirect to HTTPS ☐

*Select a device certificate [Certificate Management](#)

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
1			2054-06-28 11:07:11			HTTPS, RTSP over TLS

Apply Refresh Default Download Root Certificate

Step 4 Click **Apply**.

Enter "https://IP address: httpsport" 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.

3.11.3 Attack Defense

3.11.3.1 Configuring Firewall

Configure firewall to limit access to the Device.

Procedure

Step 1 Select > **Attack Defense** > **Firewall**.

Step 2 Click ☐ to enable the firewall function.

Figure 3-50 Firewall

Firewall Account Lockout Anti-DoS Attack

Enable ☒

Mode ☒ Allowlist ☐ Blocklist

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

Add Delete

No.	Host IP/MAC	Port	Operation
1	15.0.0.6	All Device Ports	

Total 1 records

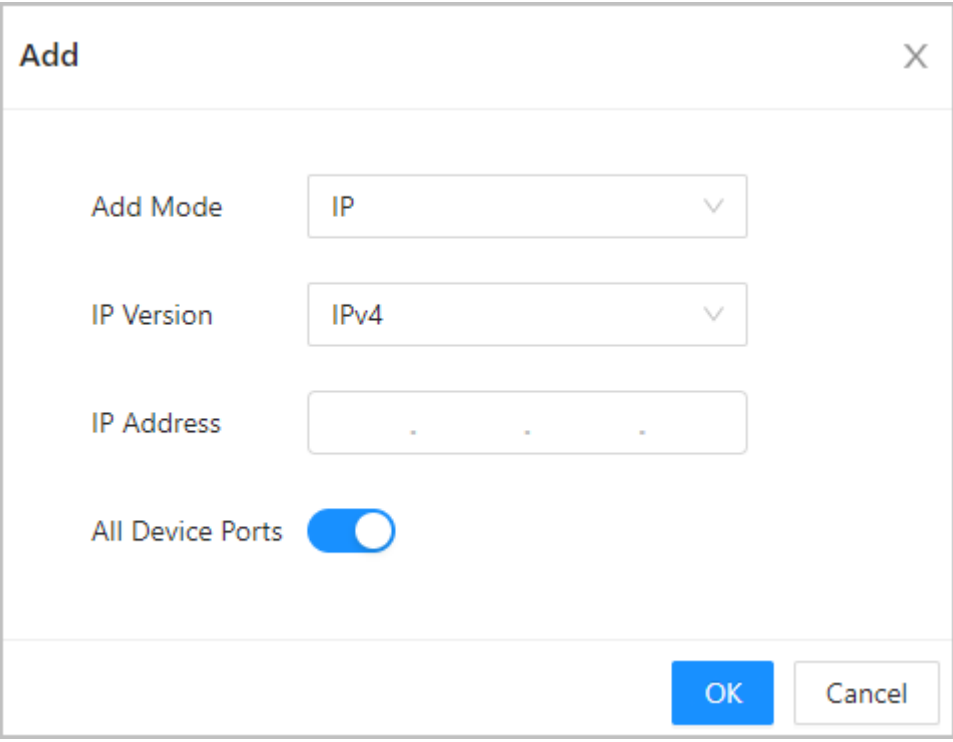
Apply Refresh Default

Step 3 Select the mode: **Allowlist** or **Blocklist**.

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

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

Figure 3-51 Add IP information

A dialog box titled "Add" with a close button (X) in the top right corner. It contains four fields: "Add Mode" with a dropdown menu showing "IP", "IP Version" with a dropdown menu showing "IPv4", "IP Address" with a text input field containing three dots, and "All Device Ports" with a toggle switch that is currently turned on. At the bottom right, there are two buttons: "OK" and "Cancel".

Add X

Add Mode IP

IP Version IPv4

IP Address . . .

All Device Ports ☒

OK Cancel

Step 5 Click **OK**.

Related Operations

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

3.11.3.2 Configuring Account Lockout

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

Procedure

Step 1 Select  > **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.

Figure 3-52 Account lockout

Firewall **Account Lockout** Anti-DoS Attack

Device Account

Login Attempt 5time(s) ▼

Lock Time 5 min

Apply Refresh Default

- 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.

Step 3 Click **Apply**.

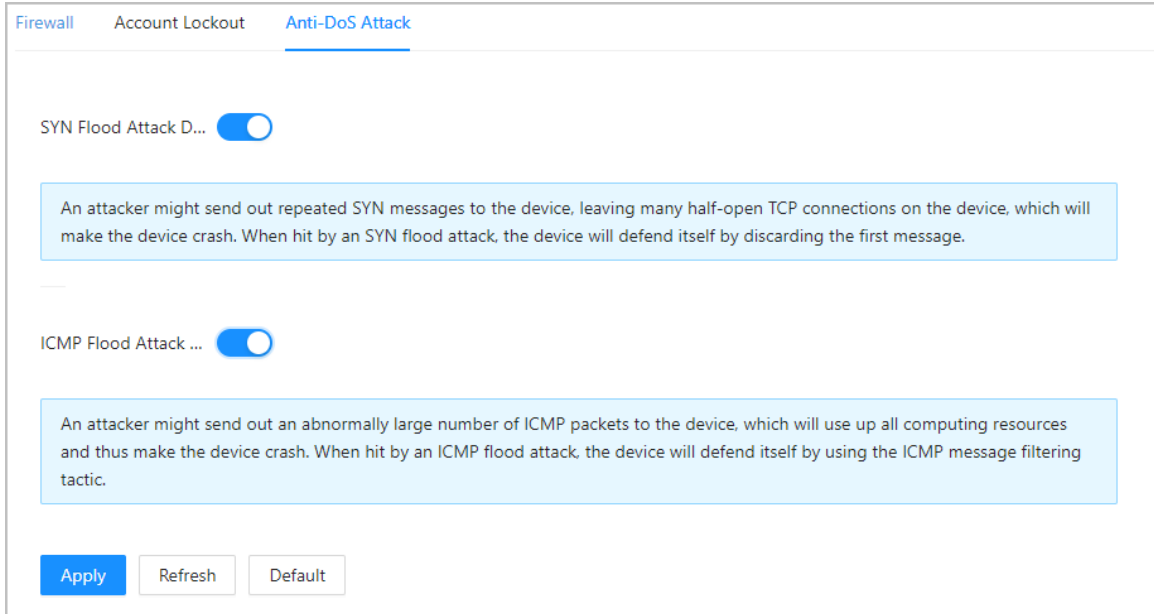
3.11.3.3 Configuring Anti-DoS Attack

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

Procedure

- Step 1 Select  > **Attack Defense** > **Anti-DoS Attack**.
- Step 2 Turn on **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** to protect the Device against DoS attacks.

Figure 3-53 Anti-DoS attack



Firewall Account Lockout **Anti-DoS Attack**

SYN Flood Attack D... ☒

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 ... ☒

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**.

3.11.4 Installing Device Certificate

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

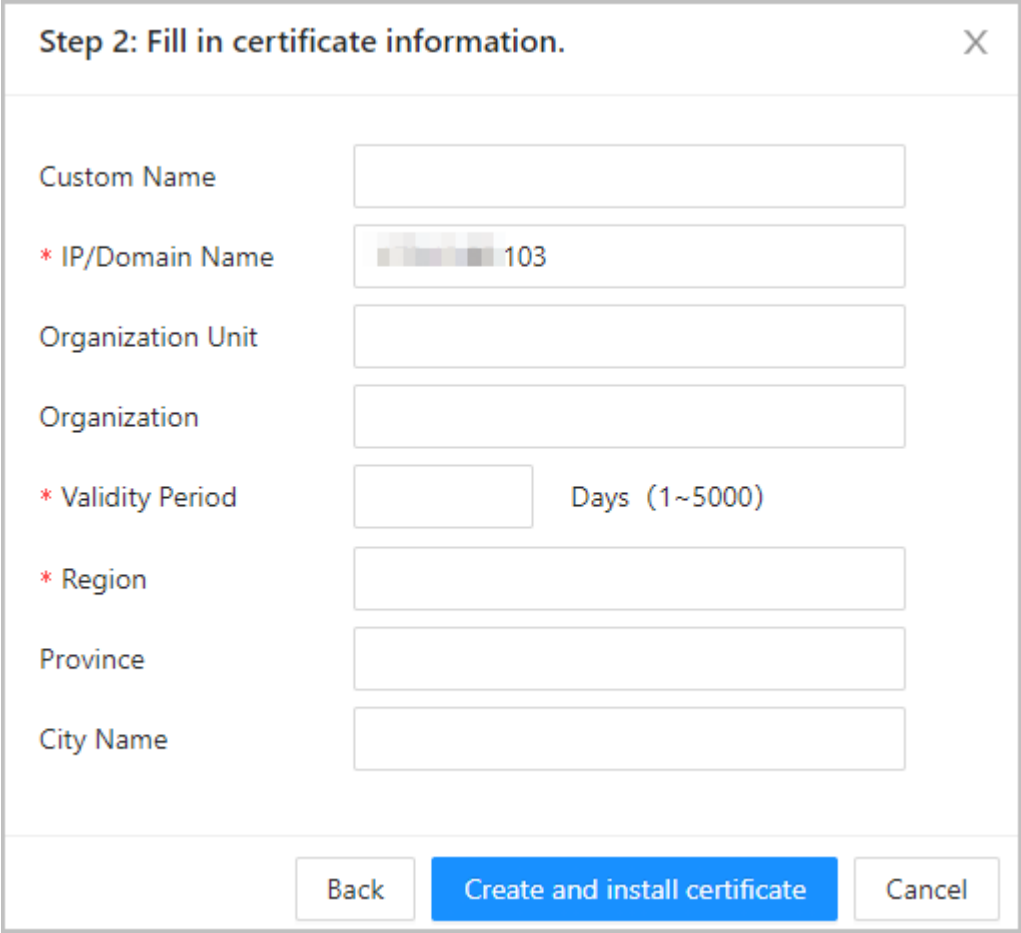
3.11.4.1 Creating Certificate

Create a certificate for the Device.

Procedure

- Step 1 Select  > **CA Certificate** > **Device Certificate**.
- Step 2 Select **Install Device Certificate**.
- Step 3 Select **Create Certificate**, and click **Next**.
- Step 4 Enter the certificate information.

Figure 3-54 Certificate information



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

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.

3.11.4.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the Device.

Procedure

- Step 1** Select  > **CA Certificate** > **Device Certificate**.
- Step 2** Click **Install Device Certificate**.
- Step 3** Select **Apply for CA Certificate and Import (Recommended)**, and click **Next**.
- Step 4** Enter the certificate information.
- IP/Domain name: the IP address or domain name of the Device.

- **Region:** The region name must not exceed 3 characters. We recommend entering the abbreviation of the region name.

Figure 3-55 Certificate information (2)

Step 2: Fill in certificate information.

* IP/Domain Name: 172.16.0.03

Organization Unit:

Organization:

* Region:

Province:

City Name:

Back Create and Download Cancel

Step 5 Click **Create and Download**.

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 **Installing Device Certificate**.
3. Click **Browse** to select the CA certificate.
4. 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.

3.11.4.3 Installing Existing Certificate

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

Procedure

Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

- Step 2 Click **Install Device Certificate**.
- Step 3 Select **Install Existing Certificate**, and click **Next**.
- Step 4 Click **Browse** to select the certificate and private key file, and enter the private key password.

Figure 3-56 Certificate and private key

- 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.

3.11.5 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 their identities.

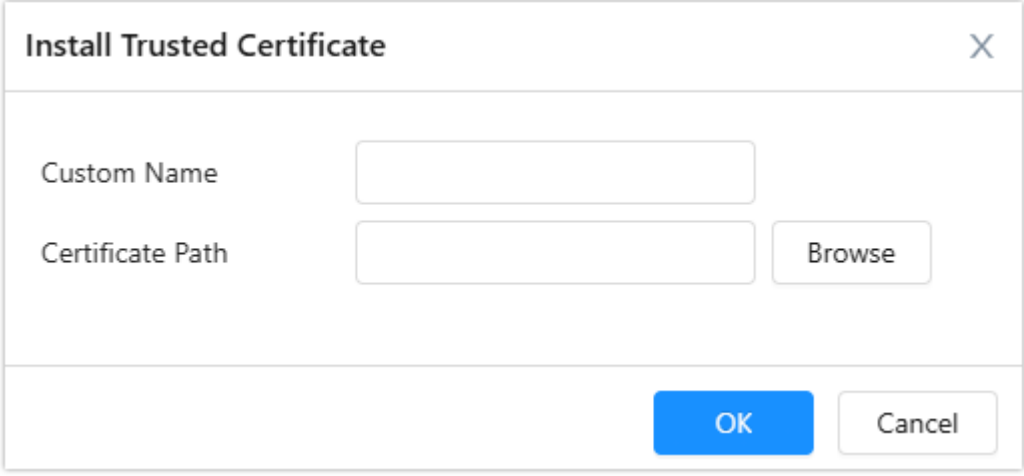
Background Information

802.1X is a network authentication protocol that opens ports for network access when an organization authorizes them to access the network

Procedure

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

Figure 3-57 Install the trusted certificate

A dialog box titled "Install Trusted Certificate" with a close button (X) in the top right corner. It contains two input fields: "Custom Name" and "Certificate Path". To the right of the "Certificate Path" field is a "Browse" button. At the bottom right are "OK" and "Cancel" buttons.

Install Trusted Certificate

Custom Name

Certificate Path

Step 4 Click **OK**.

The newly installed certificate is displayed on the **Trusted CA Certificates** 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.

3.11.6 Security Warning

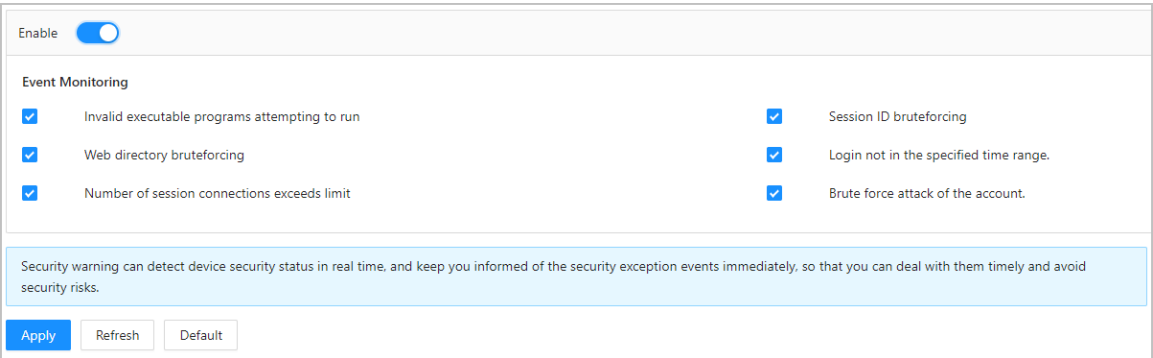
Procedure

Step 1 Select  > **Security Warning**.

Step 2 Enable the security warning function.

Step 3 Select the monitoring items.

Figure 3-58 Security warning

A configuration page for "Security Warning". At the top, there is an "Enable" toggle switch which is turned on. Below this is a section titled "Event Monitoring" containing a list of six items, each with a checked checkbox: "Invalid executable programs attempting to run", "Web directory bruteforcing", "Number of session connections exceeds limit", "Session ID bruteforcing", "Login not in the specified time range.", and "Brute force attack of the account.". A light blue informational box at the bottom states: "Security warning can detect device security status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks." At the very bottom are three buttons: "Apply", "Refresh", and "Default".

Enable ☒

Event Monitoring

☒ Invalid executable programs attempting to run	☒ Session ID bruteforcing
☒ Web directory bruteforcing	☒ Login not in the specified time range.
☒ Number of session connections exceeds limit	☒ Brute force attack of the account.

Security warning can detect device security status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks.

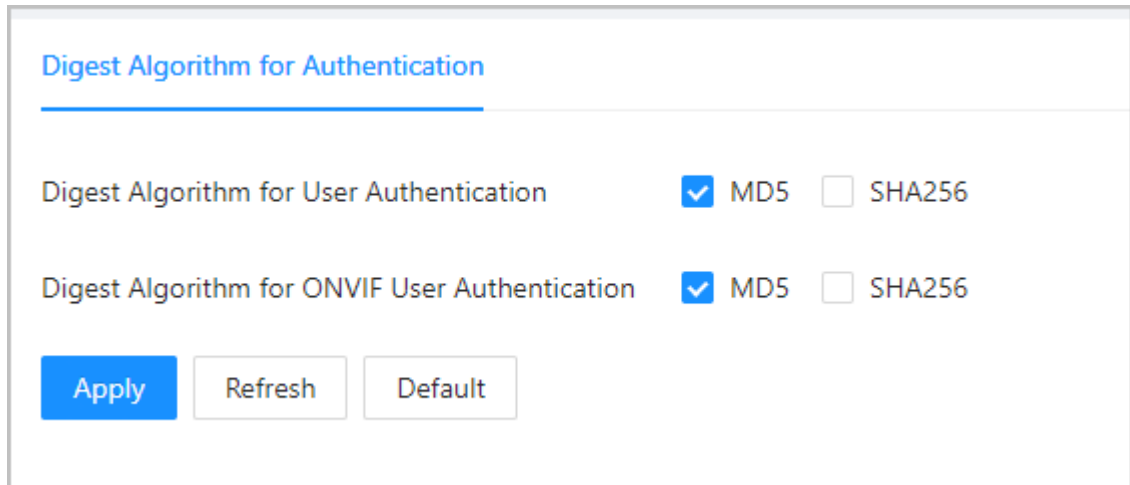
Step 4 Click **Apply**.

3.11.7 Security Authentication

Procedure

- Step 1 Select **Security** > **Security Authentication**.
- Step 2 Select a message digest algorithm.
- Step 3 Click **Apply**.

Figure 3-59 Security authentication



Digest Algorithm for Authentication

Digest Algorithm for User Authentication ☒ MD5 ☐ SHA256

Digest Algorithm for ONVIF User Authentication ☒ MD5 ☐ SHA256

Apply Refresh Default

4 Phone Operations

Before logging in to the webpage of the Device on your phone, make sure that you have initialized the Device through the webpage on the computer.

We recommend you use your phone in portrait mode and day mode. You can log in to the webpage of the Device on your phone through the following methods.

- Connect the Device to the network through the network cable. Make sure the phone and the Device are in the same network. Open the browser on the phone, and then enter the IP address of the Device.
- Connect the Device and the phone to the network through the same Wi-Fi. Open the browser on the phone, and then enter the IP address according to the connected Wi-Fi.
- Connect the phone to the network through the Device Wi-Fi. Open the browser on the phone, and then enter the IP address according to the Wi-Fi AP on the Device (it is 192.168.3.1 by default).



The Device Wi-Fi name is displayed in the **Device serial number + Device model** mode.



- The Wi-Fi and Wi-Fi AP are available on select models.
- Only English is supported when you log in to the webpage on the phone.

4.1 Initialization

When the phone is on the same LAN as the Access Controller, you can initialize the Access Controller for the first time or after the Device is restored to the factory defaults on the webpage of the phone.

Prerequisites

Make sure that the Access Controller is not connected to Wi-Fi or 4G network.

There are mainly 3 ways to connect the Device and the phone to the same network. This section introduces initialization on the phone through Wi-Fi AP.

- Connect the Device to the network through the network cable. Make sure the phone and the Device are on the same network. Open the browser on the phone, and then enter the IP address of the Device.
- Connect the Device and the phone to the network through the same Wi-Fi. Open the browser on the phone, and then enter the IP address according to the connected Wi-Fi.
- Connect the phone to the network through the Device Wi-Fi. Open the browser on the phone, and then enter the IP address according to the Wi-Fi AP on the Device (it is 192.168.3.1 by default).



The Wi-Fi and Wi-Fi AP are available on select models.

Procedure

Step 1 Power on the Access Controller.

Step 2 Connect to the Wi-Fi hotspot on your phone. The hotspot name is **product serial number + device model**.

If you have not connected to the Wi-Fi hotspot within 30 minutes, the hotspot is off.

Step 3 Open a browser on your phone, and go to the IP address (the default address is 192.168.3.1) of the hotspot.

Step 4 Tap **Starting initialization**.

Step 5 Enter and confirm the password, enter an email address.



- 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 ' " ; &). 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.

Step 6 (Optional) Enable the email address, and then configure the address.



If you want to reset the administrator password by scanning the QR code, you need to enable the e-mail function and configure the e-mail address to receive the security code.

Step 7 (Optional) Select **I have read and agree Software License Agreement Privacy Policy**.

Step 8 Tap **Next**.

Step 9 Enable **Auto Check for Updates** as needed, and then tap **Completed**.

The login page is displayed.

4.2 Logging in to the Webpage

Prerequisites

Make sure that the phone used to log in to the webpage is on the same LAN as the Device.

Procedure

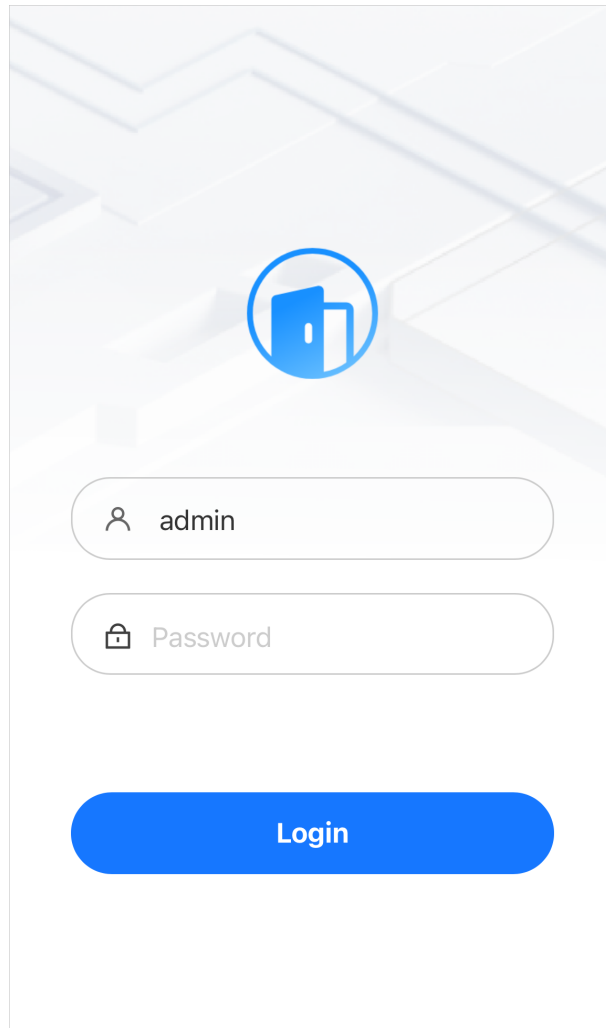
Step 1 Open a browser, and then enter the IP address of the Device.

Step 2 Enter the user name and password.



- The default name is admin, and the password is the one you set up during initialization. We recommend you change the administrator password regularly to increase security.
- If you forget the administrator login password, you can reset the password through the webpage on the computer.

Figure 4-1 Login page

The login page features a light gray background with a subtle geometric pattern of overlapping planes. At the top center is a blue circular icon containing a white door symbol. Below this icon are two rounded rectangular input fields. The first field contains a user icon and the text 'admin'. The second field contains a lock icon and the text 'Password'. At the bottom center is a prominent blue rounded rectangular button with the word 'Login' in white text.

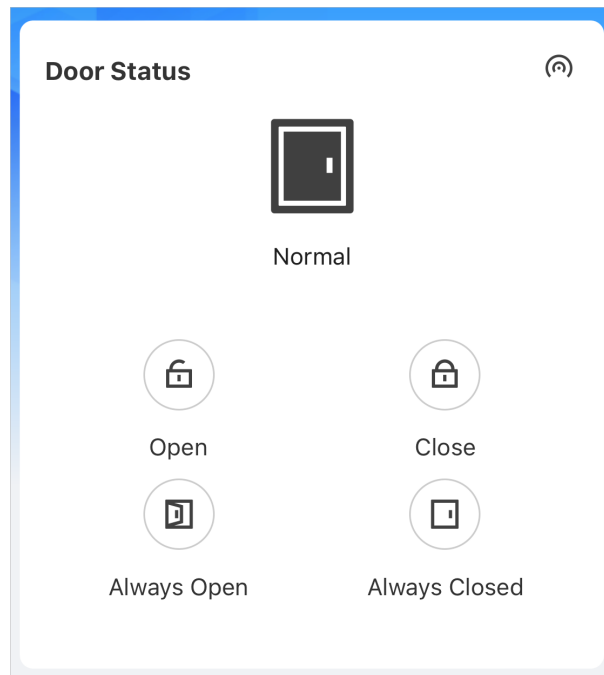
Step 3 Tap **Login**.

4.3 Home Page

The home page is displayed after you successfully log in.

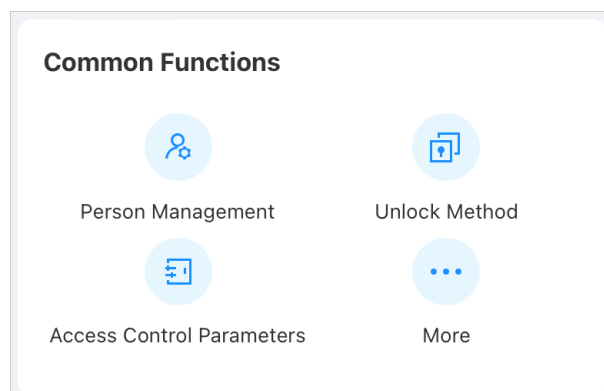
- The **Door Status** area displays the status of the door. You can remotely open or close the door. You can also configure the door status as **Always Open** or **Always Closed**.

Figure 4-2 Door status



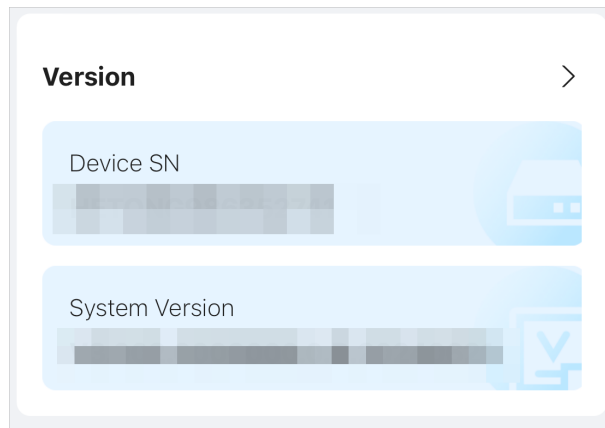
- The **Common Function** area displays the configuration menu of the Device. Click **More** to view all the configuration menus.

Figure 4-3 Common functions



- View the serial number and the version information on the **Version** area. Click > to view the version details.

Figure 4-4 Version



4.4 Person Management

Add a person and configure the permissions.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Click **Person Management**, and then click +.
- Step 3 Configure person information.

Figure 4-5 Add the person (1)

Basic Info

* ID

Name

Access Credentials

PasswordNot Added >

Card0 >

Fingerprint0 >

Bluetooth Card
No email was configured. You cannot request a Bluetooth card through email.0 >

Verification ModeSame as Device >

PermissionUser >

Table 4-1 Parameters description

Parameter	Description
ID	The ID can be numbers, letters, and their combinations, and the maximum length of the number is 30 characters.
Name	The name can have up to 32 characters (including numbers, symbols, and letters).
Password	Configure the user password. The maximum length of the password is 8 digits. The duress password is the unlock password + 1. For example, if the user password is 12345, the duress password will be 12346. A duress alarm will be triggered when a duress password is used to unlock the door.
Card	- Enter the card number manually. - Click Add. - Enter the card number, and then click Add. - Read the number automatically through the Device. - Click Add. - Swipe cards on the card reader. A 60-second countdown is displayed to remind you to swipe cards, and the system will read the card number automatically. If the 60-second countdown expires, click Read Card again to start a new countdown. - Click OK. A user can register up to 5 cards at most. Enter your card number or swipe your card, and then the card information will be read by the Device. You can enable the Duress Card function. An alarm will be triggered if a duress card is used to unlock the door. Duress Card : Click to set duress card. Change Card No. : Click to change the card number.  One user can only set one duress card.
Fingerprint	Register fingerprints. A user can register up to 3 fingerprints, and you can set a fingerprint to the duress fingerprint. An alarm will be triggered when the duress fingerprint is used to unlock the door. Enroll fingerprints through an enrollment reader or the Device. - Click Add. - Press finger on the scanner according to the on-screen instructions. - Click OK.  - Fingerprint function is only available on select models. - We do not recommend you set the first fingerprint as the duress fingerprint. - One user can only sets one duress fingerprint.

Parameter	Description
Bluetooth Card	 Bluetooth is only available on select models. You can select Request through Email or Request through Registration Code. ● Request through Email : Suitable for the first time a Bluetooth card is requested. You can request up to 5 Bluetooth cards, and have to use the email that is registered to DMSS.  You must have entered your reserved Email before you use the function. 1. Configure the Email that is registered to DMSS. 2. Click Request through Email, and then the Bluetooth cards can be requested. ● Request through Registration Code : Suitable when you already have a Bluetooth card and want to reuse it on another access controller supporting Bluetooth function. 1. Copy the Bluetooth registration code from the DMSS. 2. Click Request through Registration Code, and then enter the code. 3. Click OK.
Verification Mode	Configure the verification mode for the person. You can use the mode that is the same as the device or customize the mode. ● Same as Device : The mode is the same as the device. ● Custom : After you select Custom, Combination Method and Unlock Method are displayed. Select the combination method and unlock methods as needed. ◇ Or: Use one of the selected unlock methods to open the door. ◇ And: Use all the selected unlock methods to open the door.  ◇ The customized verification mode is only valid for the local device. It cannot be used in external card readers. ◇ When the customized verification mode is different from the mode of the device, the customized mode takes the priority.
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.
General Plan	People can unlock the door or take attendance during the defined period.  You can select more than one plan.

Parameter	Description
Holiday Plan	People can unlock the door or take attendance during the defined holiday.  You can select more than one holiday.
User Type	● General User : General users can unlock the door. ● Blocklist User : When users in the blocklist unlock the door, service personnel will receive a notification. ● Guest User : Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. ● Patrol User : Patrol users can take attendance on the Device, but they do not have door permissions. ● VIP User : When VIP unlock the door, they are not restricted by unlock modes, such as Multi-card and Time Section. ● Other User : When they unlock the door, the door will stay unlocked for 5 more seconds. ● Custom User 1/Custom User 2: Same with general users.
Time Used	Set an unlock limit for guest users. After the unlock times run out, they cannot unlock the door.

Step 4 Tap **Add**.

4.5 Configuring the System

4.5.1 Viewing Version Information

On the webpage, select **More** > **System** > **Version**, and you can view version information on the Device.

4.5.2 Maintenance

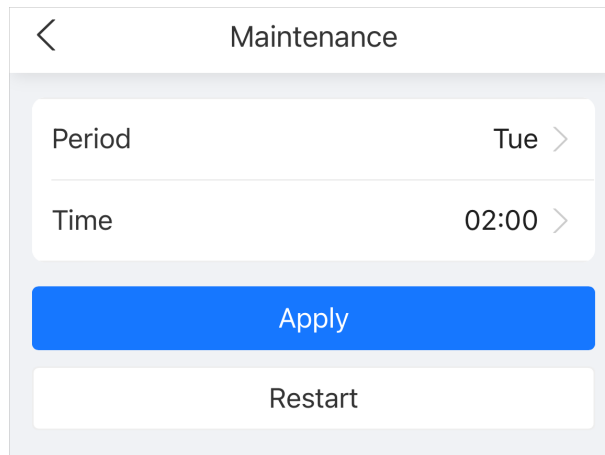
Regularly restart the Device during its idle time to improve its performance.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **System** > **Maintenance**.
- Step 3 Set the time, and then click **Apply**.

The Device will restart at the scheduled time, or you can click **Restart** to restart it immediately.

Figure 4-6 Maintenance



< Maintenance

Period Tue >

Time 02:00 >

Apply

Restart

4.5.3 Configuring Time

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **System** > **Time**.
- Step 3 Configure the time.

Figure 4-7 Configure the time parameters

<

Time

Time

Manually Set >

System Time

2024-06-25 11:13:03 >

Sync Time

Sync Phone

Date Format

YYYY-MM-DD >

Time Format

24-Hour >

Time Zone

(UTC+08:00) Beijing, >

DST

☐

Type

Date >

Start Time

01-01 00:00 >

End Time

01-02 00:00 >

Table 4-2 Time settings description

Parameter	Description
Time	- Manual Set: Manually enter the time or you can click Sync Phone to sync time with the phone. - NTP: The Device will automatically sync the time with the NTP server. Server : Enter the domain of the NTP server. Port : Enter the port of the NTP server. Interval : Enter the time synchronization interval.
Date Format	Select the date format and the time format.
Time Format	
Time Zone	Select the time zone.
DST	(Optional) Enable DST. - Select Date or Week as the Type. - Configure the start time and end time of the DST.

Step 4 Click **Apply**.

4.5.4 Data Capacity

You can see how much used/unused space the device can store for users, cards, and Bluetooth cards.

Log in to the webpage and select **More > System > Data Capacity**.

4.5.5 Language

Log in to the webpage, select **More > System > Language**. Change the language, and then tap **Apply**.

4.6 Configuring Access Control

4.6.1 Configuring Unlock Methods

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

Procedure

Step 1 Log in to the webpage.

Step 2 Click **Unlock Method** on the main menu, or select **More > Access Control > Unlock Method**.

Step 3 (Optional) Configure the combination method and the unlock method, and then click **Apply**.

- Combination method
 - ◇ Or: Use one of the selected unlock methods to open the door.
 - ◇ And: Use all the selected unlock methods to open the door.
- Unlock method

Select the unlock method according to the supported capabilities of the Device.

Figure 4-8 Unlock method

< Unlock Method

Unlock Method Combination Unlock

Combination Method Or >

Unlock Method Card, Fingerprint, Password >

Apply

4.6.2 Configuring Access Control Parameters

Procedure

- Step 1 Log in to the webpage.
- Step 2 Click **Access Control Parameters** on the main menu, or select **More > Access Control > Access Control Parameters**.
- Step 3 Configure basic parameters for the access control, and then tap **Apply**.

Figure 4-9 Access control parameters (1)

Name

Door1

Door Status

Normal >

Verification Interval

0 s

Card Swiping Interval

0 s (0-86400)

Public Password

☐

Normally Open Period

General Plan

Disabled >

Holiday Plan

Disabled >

Normally Closed Period

General Plan

Disabled >

Holiday Plan

Disabled >

Figure 4-10 Access control parameters (2)

Unlock Settings

Unlock Method
Combination Unlock

Combination Method
Or >

Unlock Method
Card, Fingerprint, Password, Bluetooth Card

Bluetooth Mode

PIN Code Authentication

Door Unlocked Duration
3 s

Remote Verification

Apply

Table 4-3 Description of access control parameters

Parameter		Description
Basic Settings	Name	The name of the door.
	Door Status	Set the door status. - Normal: The door will be unlocked and locked according to your settings. - Always Open: The door remains unlocked all the time. - Always Closed: The door remains locked all the time.
	Verification Interval	If you verify your identity multiple times within a set period, only the earliest verification will be considered valid, and the door will not open after the second or later verifications. From the moment the door fails to open, you must wait for the configured verification time interval before attempting to verify your identity again.

Parameter		Description
	Card Swiping Interval	For first-time verification through card, you can normally unlock the door or perform attendance, and the records are generated. Within the configured period, if you swipe the card for verification again, you cannot unlock the door or perform attendance, and the records are not generated. Please verify the identification after the configured period.  The Card Swiping Interval takes priority over Verification Interval.
	Public Password	After the public password is enabled, configure the password. You can use the public password without entering the user ID to unlock the door. Only one public password is supported for one device.
Normally Open Period	Period/Holiday Plan	When you select Normal , you can select a time template from the drop-down list. The door remains open or closed during the defined time.
Normally Closed Period	Period/Holiday Plan	 - When normally open period conflicts with normally closed period, normally open period takes priority over normally closed period. - When periods conflict with holiday plans, holiday plans take priority over periods.
Unlock Settings	Unlock Method	Combination Unlock by default.
	Combination Method	- Or: Use one of the selected unlock methods to open the door. - And: Use all the selected unlock methods to open the door.
	Unlock Method	Select the unlock method according to the supported capabilities of the Device.
	Door Unlocked Duration	Configure the duration for which the door remains open. It is 3 seconds by default. When the door opens for more than the configured time, the door closes.
	Bluebooth Mode	Select the Bluebooth mode according to your need.  This function displays only after you select Bluebooth Card in Unlock Method.
	PIN Code Authentication	When PIN code authentication is enabled, you can open the door with just the password.  You do not have to enter the user ID if this function is enabled. The remote verification is not supported.

Parameter		Description
	Remote Verification	Open the door remotely.

Step 4 Tap **Apply**.

4.6.3 Configuring Alarms

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

Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **Access Control** > **Alarm**.

Step 3 Configure alarm parameters, and then click **Apply**.

Figure 4-11 Alarm settings

The screenshot displays the 'Alarm' settings page. It features a list of alarm types, each with a status indicator and a chevron icon for further configuration. The alarms listed are: Duress Alarm (enabled), Anti-passback (enabled), Door Detector (enabled), Door Detector Status (set to NO), Intrusion Alarm (disabled, with sub-statuses for Buzzer and Link Alarm Output), Unlock Timeout Alarm (disabled, with sub-statuses for Buzzer and Link Alarm Output), Excessive Attempts Alarm (enable), and Tamper Alarm (enable, with sub-statuses for Buzzer and Link Alarm Output). A large blue 'Apply' button is located at the bottom of the settings list.

Table 4-4 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
Anti-passback	Users need to verify their identities both for entry and exit; otherwise an alarm will be triggered. It helps prevents a card holder from passing an access card back to another person to gain entry. When anti-passback is enabled, the card holder must leave the secured area through an exit reader before system will grant another entry. ● If a person enters after authorization and exits without authorization, an alarm will be triggered when they attempt to enter again, and access is denied at the same time. ● If a person enters without authorization and exits after authorization, an alarm will be triggered when they attempt to enter again, and access is denied at the same time.  If the Device can only connect one lock, verifying on the Device means entry direction, and verifying on the external card reader means exit direction by default. You can modify the setting on the management platform.
Door Detector	With the door detector wired to your device, alarm can be triggered when doors are opened or closed abnormally. The door detector includes 2 types, including NC detector and NO detector. ● NC: The sensor is in a shorted position when the door or window is closed. ● NO: An open circuit is created when the window or door is actually closed.
Intrusion Alarm	If the door is opened abnormally, an intrusion alarm will be triggered and last for a defined time.  The door detector and intrusion need to be enabled at the same time.
Unlock Timeout Alarm	When the door remains unlocked for longer than the defined timeout duration, the door timeout alarm will be triggered and last for the defined time.
Unlock Timeout	 The door detector and door timed out function need to be enabled at the same time.
Excessive Use Alarm	If the wrong password or card is used 5 times in a row within 60 seconds, the alarm for excessive use of illegal card will be triggered and lasts for a defined time.
Tamper Alarm	The tamper alarm is triggered by pressing the tamper button.

4.6.4 Configuring Alarm Linkage

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Access Control** > **Alarm Linkage Setting**.
- Step 3 Select the zone to configure alarm.

Figure 4-12 Alarm linkage

Alarm-in Port	1
Name	Zone1
Alarm Input Type	NO >
Link Fire Safety Control	☐

Alarm-out Port	☐
Duration	30 s
Alarm Output Channel	1 >

Access Control Linkage	☐
Linkage Mode	Weak Execution >
When the fire alarm signal disappears, the door will automatically return to the normal authentication mode.	
Channel Type	NC >

OK

- Step 4 Create a name for the alarm zone.
- Step 5 Enable **Link Fire Safety Control**, and select a type for the alarm input device.
- NC: The alarm input is in a normally closed (NC) circuit state when the alarm has not been tripped. Opening a normally closed circuit sets off the alarm.
 - NO: The alarm input device is in a normally open (NO) circuit state when the alarm has not been tripped. Closing the circuit sets off the alarm.
- Step 6 If you want to link access control when the fire alarm is triggered, enable **Access Control Linkage**.



This function takes effect only after **Link Fire Safety Control** is enabled.

Step 7 Select a linkage mode.

- Strong Execution: When the fire alarm signal disappears, the door remains the current status. Please manually changes to its previous door status settings if you want to.
- Weak Execution: When the fire alarm signal disappears, the door automatically returns to its previous door status.

Step 8 Select the channel type.

- NO: The door automatically opens when fire alarm is triggered.
- NC: The door automatically closes when fire alarm is triggered.

Step 9 Tap **OK**.

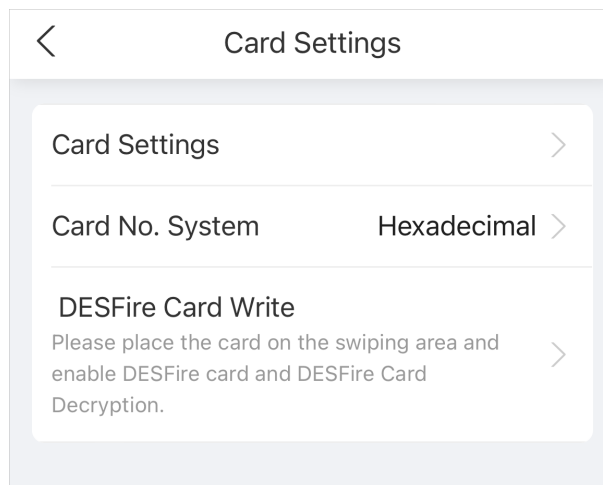
4.6.5 Configuring Card Settings

Procedure

Step 1 Log in to the webpage.

Step 2 Select **More** > **Access Control** > **Card Settings**.

Figure 4-13 Card settings



Step 3 Tap **Card Settings**, configure the card parameters, and then tap **Apply**.

Figure 4-14 Card parameters

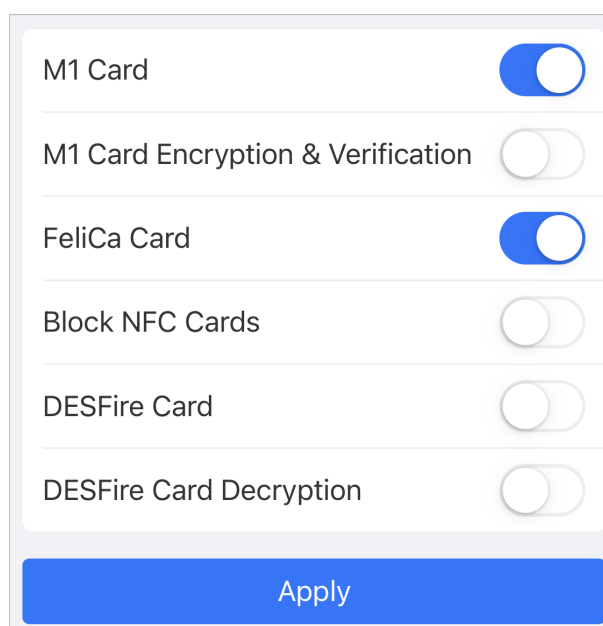


Table 4-5 Card parameters description

Parameter	Description
M1 Card	The M1 card can be read when this function is enabled.  This function is only available on select models.
M1 Card Encryption & Verification	Only the encrypted IC card can be read when this function is enabled.  Make sure M1 Card is enabled.
FeliCa Card	The FeliCa card can be read when this function is enabled.  This function is only available on select models.
Block NFC Cards	Prevent unlocking through duplicated NFC cards after this function is enabled.  • This function is only available on models that support IC cards. • Make sure M1 Card is enabled. • NFC function is only available on select models of phones.

Parameter	Description
Desfire Card	The Device can read the card number of Desfire card when this function is enabled.  • This function is only available on models that support IC cards. • It only supports hexadecimal format.
Desfire Card Decryption	Information in the Desfire card can be read when Enable Desfire Card and Desfire Card Decryption are enabled at the same time.  • This function is only available on models that support IC cards. • Make sure that Desfire card is enabled.

Step 4 Tap **Card No. System**, select the format, and then click **Apply**.

Select decimal format or hexadecimal format for the card number when Wiegand card reader is connected. The card No. system is the same for both card number input and output.

Step 5 Tap **DESFire Card Write**.

Place the card on the reader, enter the card number, and then click **Write** to write card number to the card.



- Desfire card function and Desfire card decryption function must be enabled.
- Only supports hexadecimal format.
- Supports up to 8 characters.

4.7 Communication Settings

4.7.1 Configuring TCP/IP

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

Procedure

Step 1 Log in to the webpage.

Step 2 Select **More > Communication Settings > TCP/IP**.

Step 3 Configure the parameters, and then click **Apply**.

Figure 4-15 TCP/IP

The screenshot displays the TCP/IP configuration screen. At the top, there is a back arrow and the title 'TCP/IP'. Below this, the configuration is organized into sections. The first section shows 'NIC' set to 'NIC 1' with a chevron. The second section shows 'Mode' set to 'Static' with a chevron. The third section shows 'MAC Address' with a hexagonal input field. The fourth section shows 'IP Version' set to 'IPv4' with a chevron. Below this are five fields, each preceded by a red asterisk: 'IP Address', 'Subnet Mask', 'Default Gateway', 'Preferred DNS', and 'Alternate DNS', each with a corresponding hexagonal input field. At the bottom of the configuration area, 'MTU' is set to '1500'. A large blue 'Apply' button is located at the very bottom.

Table 4-6 Description of TCP/IP

Parameter	Description
Mode	• Static: Manually enter IP address, subnet mask, and gateway. • DHCP: It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Device will automatically be assigned with IP address, subnet mask, and gateway.
MAC Address	MAC address of the Device.
IP Version	IPv4 or IPv6.
IP Address	If you set the mode to Static , configure the IP address, subnet mask and gateway.
Subnet Mask	
Default Gateway	
	• IPv6 address is represented in hexadecimal. • IPv6 version does not require setting subnet masks. • The IP address and default gateway must be in the same network segment.

Parameter	Description
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.
MTU	MTU (Maximum Transmission Unit) refers to the maximum size of data that can be transmitted in a single network packet in computer networks. A larger MTU value can improve network transmission efficiency by reducing the number of packets and associated network overhead. If a device along the network path is unable to handle packets of a specific size, it can result in packet fragmentation or transmission errors. In Ethernet networks, the common MTU value is 1500 bytes. However, in certain cases such as using PPPoE or VPN, smaller MTU values may be required to accommodate the requirements of specific network protocols or services. The following are recommended MTU values for reference: • 1500: Maximum value for Ethernet packets, also the default value. This is a typical setting for network connections without PPPoE and VPN, some routers, network adapters, and switches. • 1492: Optimal value for PPPoE • 1468: Optimal value for DHCP. • 1450: Optimal value for VPN.

4.7.2 Configuring Wi-Fi

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Communication Settings** > **Wi-Fi**.
- Step 3 Turn on Wi-Fi.

All available Wi-Fi are displayed.



- The Wi-Fi function is available on select models.
- The Wi-Fi and Wi-Fi AP cannot be enabled at the same time.

- Step 4 Click the Wi-Fi network, and then enter the password.

The Wi-Fi is connected.

Related Operations

- DHCP: Select the **DHCP** mode and click **Apply**, the Device will automatically be assigned a Wi-Fi address.
- Static: Select the **Static** mode, manually enter a Wi-Fi address, and then click **Apply**, the Device will connect to the Wi-Fi.

4.7.3 Configuring Wi-Fi AP

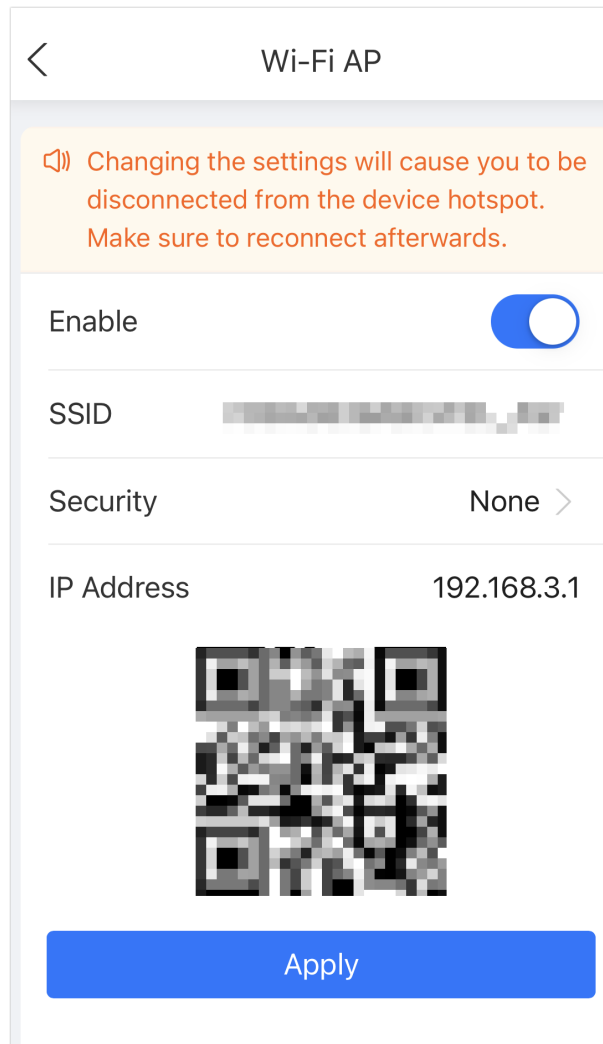


- The Wi-Fi function is available on select models.
- The Wi-Fi and Wi-Fi AP cannot be enabled at the same time.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Communication Settings** > **Wi-Fi AP**.
- Step 3 Enable the function, and then click **Apply**.

Figure 4-16 Wi-Fi AP



4.7.4 Configuring Cloud Service

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Communication Settings** > **Cloud Service**.
- Step 3 Turn on the cloud service function.
The cloud service goes online if the P2P and PaaS are online.
- Step 4 Click **Apply**.

4.7.5 Configuring Auto Registration

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Network Setting** > **Auto Registration**.
- Step 3 Enable the auto registration function, configure the parameters, and then click **Apply**.

Figure 4-17 Auto registration

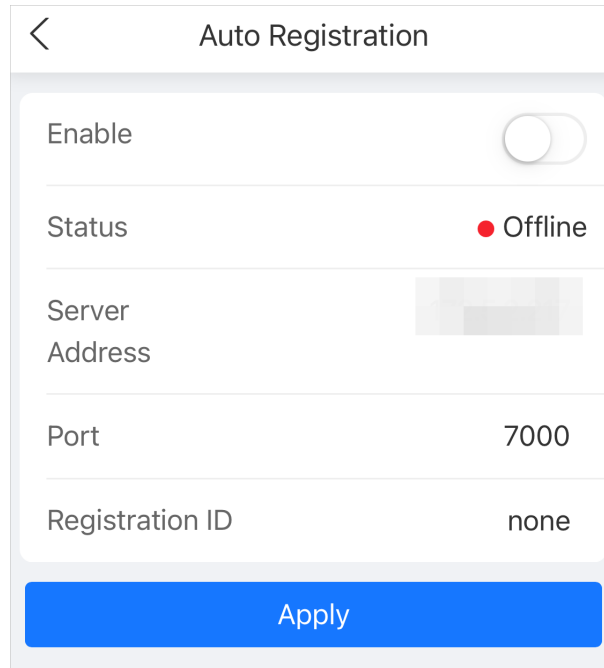


Table 4-7 Automatic registration description

Parameter	Description
Status	Displays the connection status of auto registration.
Server Address	The IP address or the domain name of the server.
Port	The port of the server that is used for automatic registration.
Registration ID	The registration ID (user defined) of the device. Adding the device to the management by entering the registration ID on the platform.

4.7.6 Configuring Mode

Log in to the webpage, and select **Communication Settings** > **Mode Settings**.

Card Reader Mode

Select **Mode** as **Card Reader**. The device serves as a card reader externally connected to an access control controller. It does not perform authentication but directly transmits access control information (such as card, password, fingerprint) to the access control controller, which then authenticates and unlocks the door.

Figure 4-18 Card reader mode

Mode Card Reader >

RS-485 Settings

Baud Rate 9600 >

Data Bit 8 >

Stop Bit 1 >

Parity Code None >

Wiegand Settings

Wiegand Output Type Wiegand 34 >

Pulse Width (µs) 200

The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.

Pulse Interval (µs) 1000

The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.

Apply

Access Controller Mode

Set **Mode** as **Access Controller**.

Figure 4-19 Access controller mode

External Device

Access Controller >

Access controller: This device acts as a card reader, and connects to an access controller, which manages the opening of doors.

Baud Rate

9600 >

Data Bit

8 >

Stop Bit

1 >

Parity Code

None >

Output Data Type

Card Number >

Wiegand Settings

Wiegand Settings

Wiegand Input >

Card No. Inversion

☒

Table 4-8 Description of RS-485

External Device	Description
Access Controller	Select Access Controller when the Device functions as a card reader, and sends data to other external access controllers to control access. Output Data type: • Card Number: Outputs data based on card number when users swipe card to unlock door; outputs data based on user's first card number when they use other unlock methods. • ID: Outputs data based on the user ID.  • When authentication is successful, the relevant information is transmitted to the access controller. In this case, the authentication result displayed is the authentication result of the access controller. • When authentication fails, the relevant information is not transmitted to the access controller, and the authentication result displayed remains as failure.
Card Reader	The device is externally connected to a card reader and transmits access control card information to an access controller or management platform.
Card Reader (OSDP)	The device is externally connected to an OSDP card reader and transmits access control card information to an access controller or management platform.
Door Security Module	The door exit button, lock and fire linkage is not effective after the security module is enabled. • Supports authentication through face, card, fingerprint, password, and other methods to control the door security module for unlocking. • Supports unlocking through an externally connected RS-485 card reader or push-to-open button linked to the door control security module.  Remote unlock of the externally connected door lock through the door security module is not supported.
Lock Extension Module	When the Access Controller is connected to external lock extension module, if you select Lock Extension Module, the local lock is unlocked after you verify the identification on the local device, and the extension lock is unlocked after you verify the identification on the external card reader. After you select Lock Extension Module, you can select channel 2 on the Access Control Parameters and Alarm page on the webpage of the Access Controller.

Table 4-9 Description of Wiegand

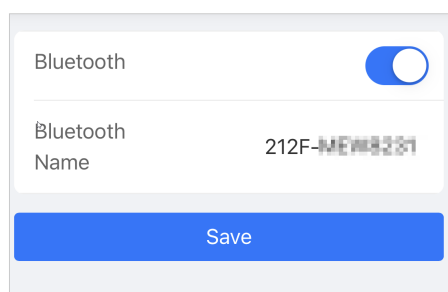
Parameter		Description
Wiegand Settings		- When connecting an external card reader device, select Wiegand Input. - When the Device functions as a card reader, and you need to connect it to another access controller, and select Wiegand Output Config.
Wiegand Input	Card No. Inversion	If the card number sequence obtained through Wiegand input does not match the actual card number sequence when interfacing with third-party devices, enable this function.
Wiegand Output	Wiegand Output Type	The bit length of card numbers or ID that the device can recognize and output. - Wiegand 26: Reads 3 bytes or 6 digits. - Wiegand 34: Reads 4 bytes or 8 digits. - Wiegand 66: Reads 8 bytes or 16 digits.
	Pulse Width	Configure the pulse width and interval for Wiegand output.
	Pulse Interval	
	Output Data Type	Select a Wiegand format to read card numbers or ID numbers. - User ID: Outputs data based on user ID. - Card: Outputs data based on user's first card number.
	Wiegand Format	When Output Data Type is set as ID , you can select decimal or hexadecimal output formats.

4.7.7 Configuring Bluetooth

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Communication** > **Bluetooth Settings**.
- Step 3 Enable or turn off **Bluetooth**.

Figure 4-20 Bluetooth



- Step 4 Tap **Save**.

Results

You can unlock the door via Bluetooth on the DMSS app.

4.8 Configuring Audio

Procedure

- Step 1 Log in to the webpage of the device.
- Step 2 Select **Audio**.
- Step 3 Enable **Key Sound** or **DND Mode** based on your needs.

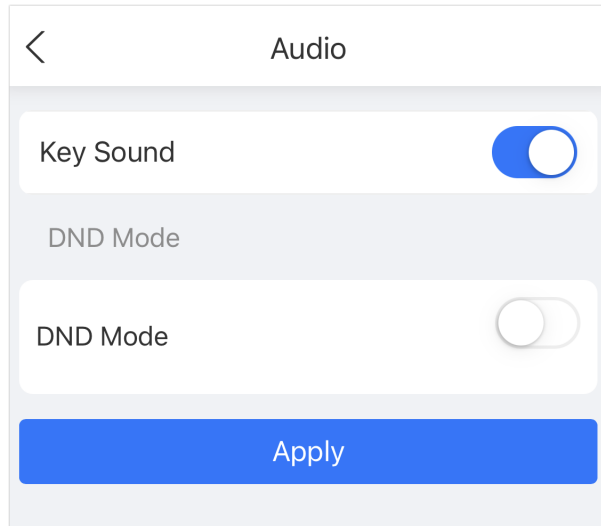


Table 4-10 Description of audio parameters

Parameters	Description
Key Sound	When enabled, touchscreen devices will produce a prompt sound for local touch operations, while non-touchscreen devices will produce a prompt sound for key/button operations.
DND Mode	When enabled, there will be no prompt sounds for local verification (such as door access or attendance) during the configured time periods. Supports up to 4 time periods.

- Step 4 Tap **Apply**.

4.9 Viewing Logs

You can view logs such as system logs, unlock records, and alarm logs.

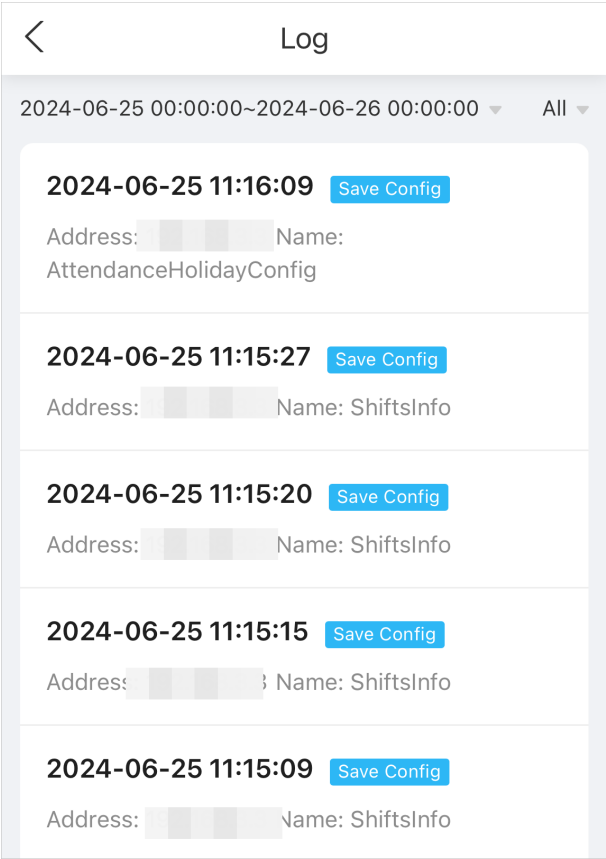
4.9.1 System Logs

View and search for system logs.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Log** > **Log**.

Figure 4-21 Logs



4.9.2 Unlock Records

Search for unlock records.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Log** > **Unlock Records**.
- Step 3 Click the record to view the details.

4.9.3 Alarm Logs

View alarm logs.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **More** > **Log** > **Alarm Log**.

5 Smart PSS Lite Configuration

This section introduces how to manage and configure the device through Smart PSS Lite. For details, see the user's manual of Smart PSS Lite.

5.1 Installation

Contact technical support or go to the official website to get the Smart PSS Lite. If you get the software package of the SmartPSS Lite, install and run the software according to page instructions.

5.2 Adding Device One by One

If you already know the IP address of a device, you can manually add it to the platform.

Procedure

- Step 1** On the home page, click **Devices**.
- Step 2** Click **Add**, and then enter the device information.

Figure 5-1 Add devices

Table 5-1 Parameters of IP adding

Parameter	Description
Device Name	The name of the device.
Add Mode	- IP/Domain Name: Add devices through IP address. - SN (Available on devices that support P2P): Add devices through their serial number. - Auto Register: Add devices through auto registration.

Appendix 1 Important Points of Fingerprint Registration Instructions

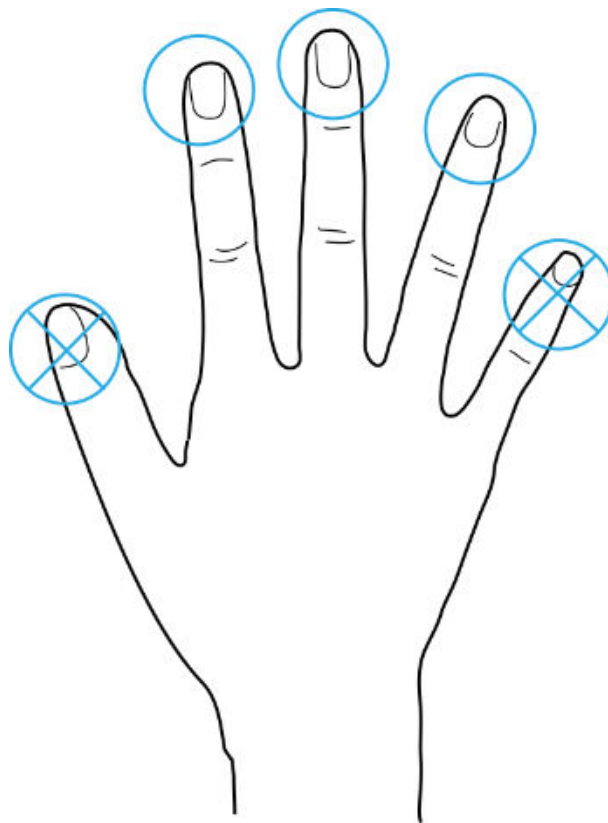
When you register the fingerprint, pay attention to the following points:

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

Fingers Recommended

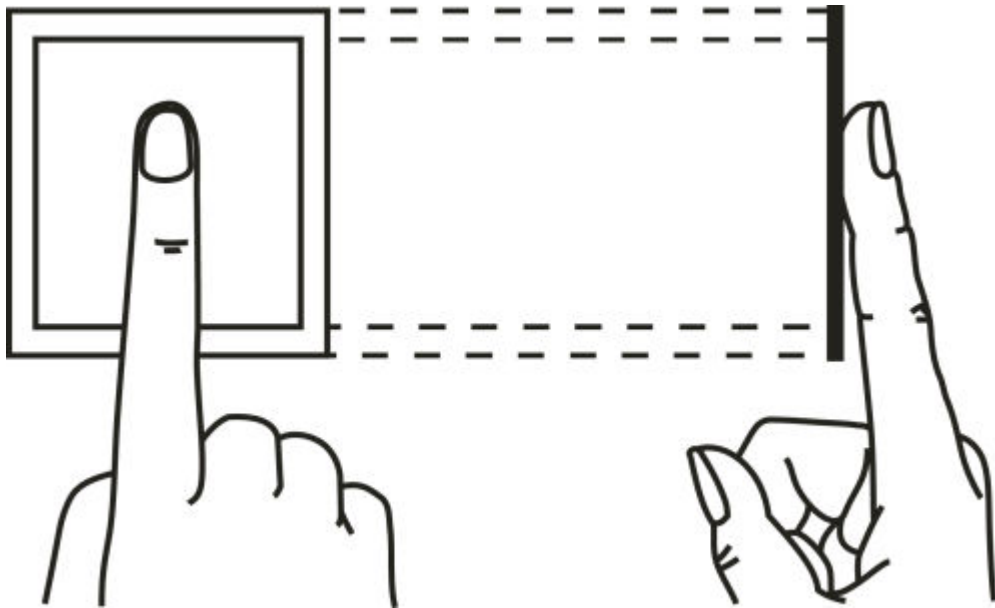
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 1-1 Recommended fingers

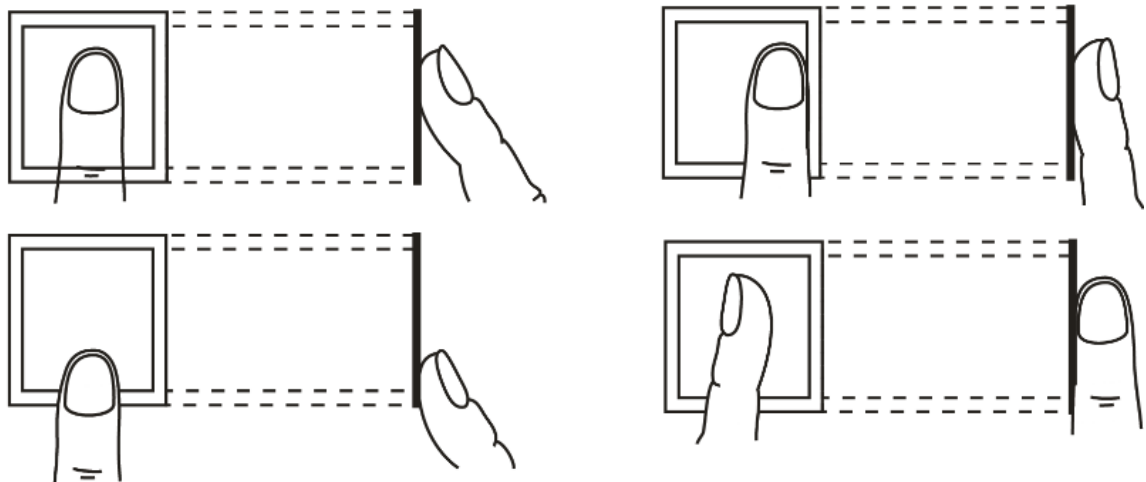


How to Press Your Fingerprint on the Scanner

Appendix Figure 1-2 Correct placement



Appendix Figure 1-3 Wrong placement



Appendix 2 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).