

Face Recognition Access Controller

User's Manual








Foreword

General

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

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First Release.	June 2023

Privacy Protection Notice

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

About the Manual

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

might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.

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

Important Safeguards and Warnings

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

Transportation Requirement



Transport, use and store the Access Controller under allowed humidity and temperature conditions.

Storage Requirement



Store the Access Controller under allowed humidity and temperature conditions.

Installation Requirements



- Do not connect the power adapter to the Access Controller while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Access Controller.
- Do not connect the Access Controller to two or more kinds of power supplies, to avoid damage to the Access Controller.
- Improper use of the battery might result in a fire or explosion.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Access Controller in a place exposed to sunlight or near heat sources.
- Keep the Access Controller away from dampness, dust, and soot.
- Install the Access Controller on a stable surface to prevent it from falling.
- Install the Access Controller in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the Access Controller label.
- The Access Controller is a class I electrical appliance. Make sure that the power supply of the Access Controller is connected to a power socket with protective earthing.

Operation Requirements



- Check whether the power supply is correct before use.

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

Table of Contents

Foreword	I
Important Safeguards and Warnings.....	III
1 Overview	1
2 Local Operations	2
2.1 Basic Configuration Procedure.....	2
2.2 Common Icons.....	2
2.3 Standby Screen.....	3
2.4 Initialization	4
2.5 Logging In.....	4
2.6 Unlocking Methods	5
2.6.1 Unlocking by Cards.....	5
2.6.2 Unlocking by Face	5
2.6.3 Unlocking by User Password.....	5
2.6.4 Unlocking by Admin Password.....	5
2.6.5 Unlocking by QR code	6
2.6.6 Unlocking by Fingerprint.....	6
2.6.7 Unlocking by Temporary Password.....	6
2.7 User Management.....	6
2.7.1 Adding Users.....	6
2.7.2 Viewing User Information	9
2.7.3 Configuring the Admin Unlock Password	10
2.8 Access Management	10
2.8.1 Configuring Unlock Combinations	10
2.8.2 Configuring Alarms.....	11
2.8.3 Configuring the Door Status	13
2.9 Attendance Management.....	14
2.9.1 Configuring Departments	14
2.9.2 Configuring Shifts	15
2.9.3 Configuring Holiday Plans	17
2.9.4 Configuring Work Schedules	18
2.9.5 Configuring the Verification Time Interval.....	21
2.9.6 Configuring Attendance Modes.....	21
2.10 Network Communication.....	24
2.10.1 Configuring the IP Address	25
2.10.2 Configuring Active Registration.....	26

2.10.3 Configuring the Wi-Fi	27
2.10.4 Configuring Serial Port	27
2.10.5 Configuring Wiegand	28
2.11 System Settings	29
2.11.1 Configuring Time	29
2.11.2 Configuring Face Parameters	31
2.11.3 Setting the Volume	33
2.11.4 Configuring the Language	33
2.11.5 Screen Settings	33
2.11.6 (Optional) Configuring Fingerprint Parameters	34
2.11.7 Restoring Factory Defaults	34
2.11.8 Restarting the Device	34
2.12 Functions Settings	34
2.13 USB Management	38
2.13.1 Exporting to USB	38
2.13.2 Importing From USB	39
2.13.3 Updating the System	39
2.14 Record Management	39
2.15 System Information	39
2.15.1 Viewing Data Capacity	39
2.15.2 Viewing Device Version	39
3 Web Operations	40
3.1 Initialization	40
3.2 Logging In	40
3.3 Resetting the Password	41
3.4 Home Page	42
3.5 Adding Users	42
3.6 Configuring Intercom	46
3.6.1 Using the Device as the SIP Server	46
3.6.1.1 Configuring SIP Server	46
3.6.1.2 Configuring Local Parameters	47
3.6.1.3 Adding the VTO	48
3.6.1.4 Adding the VTH	49
3.6.1.5 Adding the VTS	52
3.6.2 Using VTO as the SIP server	53
3.6.2.1 Configuring SIP Server	53
3.6.2.2 Configuring Local Parameters	54
3.6.3 Using the Platform as the SIP server	55

3.6.3.1 Configuring SIP Server	55
3.6.3.2 Configuring Local Parameters	57
3.7 Configuring Access Control	58
3.7.1 Configuring Basic Parameters	58
3.7.2 Configuring Unlock Methods	59
3.7.3 Configuring Alarms	61
3.7.4 Configuring Global Alarm linkages (Optional)	63
3.7.5 Configuring Face Detection	65
3.7.6 Configuring Card Settings	68
3.7.7 Configuring QR Code	69
3.7.8 Configuring Schedules	69
3.7.8.1 Configuring Time Periods	69
3.7.8.2 Configuring Holiday Plans	70
3.7.9 Configuring Expansion Modules	72
3.7.10 Configuring Port Functions	72
3.8 Configuring Audio and Video	73
3.8.1 Configuring Video	73
3.8.1.1 Configuring Channel 1	73
3.8.1.2 Configuring Channel 2	77
3.8.2 Configuring Audio Prompts	80
3.8.3 Configuring Motion Detection	80
3.8.4 Configuring Local Coding	81
3.9 Configuring Network	82
3.9.1 Configuring TCP/IP	82
3.9.2 Configuring Wi-Fi	84
3.9.3 Configuring Port	84
3.9.4 Configuring Basic Service	85
3.9.5 Configuring Cloud Service	87
3.9.6 Configuring Active Registration	88
3.10 Configuring RS-485	89
3.11 Configuring Wiegand	91
3.12 Configuring the System	92
3.12.1 User Management	92
3.12.1.1 Adding Administrators	92
3.12.1.2 Adding ONVIF Users	93
3.12.1.3 Resetting the Password	94
3.12.1.4 Viewing Online Users	94
3.12.2 Configuring Time	95

3.12.3 Maintenance.....	96
3.12.4 Configuration Management.....	96
3.12.4.1 Exporting and Importing Configuration Files.....	96
3.12.4.2 Restoring the Factory Default Settings.....	97
3.12.5 Updating the System.....	98
3.12.5.1 File Update.....	98
3.12.5.2 Online Update.....	98
3.12.6 Viewing Version Information.....	98
3.12.7 Viewing Data Capacity.....	99
3.12.8 Viewing Legal Information.....	99
3.13 Personalization.....	99
3.13.1 Adding Resources.....	99
3.13.2 Configuring Themes.....	100
3.13.3 Configuring the Shortcuts.....	103
3.14 Viewing Logs.....	105
3.14.1 System Logs.....	105
3.14.2 Admin Logs.....	105
3.14.3 Unlocking Logs.....	106
3.14.4 Alarm Logs.....	106
3.14.5 Call Logs.....	106
3.14.6 USB Management.....	106
3.15 Data Capacity.....	107
3.16 Security Settings(Optional).....	107
3.16.1 Security Status.....	107
3.16.2 Configuring HTTPS.....	108
3.16.3 Attack Defense.....	108
3.16.3.1 Configuring Firewall.....	108
3.16.3.2 Configuring Account Lockout.....	109
3.16.3.3 Configuring Anti-DoS Attack.....	110
3.16.4 Installing Device Certificate.....	111
3.16.4.1 Creating Certificate.....	111
3.16.4.2 Applying for and Importing CA Certificate.....	112
3.16.4.3 Installing Existing Certificate.....	113
3.16.5 Installing the Trusted CA Certificate.....	114
3.16.6 Data Encryption.....	115
3.16.7 Security Warning.....	116
4 Smart PSS Lite Configuration.....	117
4.1 Installing and Logging In.....	117

4.2 Adding Devices	117
4.2.1 Adding One By One	117
4.2.2 Adding in Batches	118
4.3 User Management	119
4.3.1 Configuring Card Type	119
4.3.2 Adding Users	120
4.3.2.1 Adding One by One	120
4.3.2.2 Adding in Batches	121
4.3.3 Assigning Access Permission	122
4.3.4 Assigning Attendance Permissions	124
4.4 Access Management	126
4.4.1 Remotely Opening and Closing Door	126
4.4.2 Setting Always Open and Always Close	127
4.4.3 Monitoring Door Status	127
Appendix 1 Important Points of Face Registration	129
Appendix 2 Important Points of Intercom Operation	132
Appendix 3 Important Points of Fingerprint Registration Instructions	133
Appendix 4 Important Points of QR Code Scanning	135
Appendix 5 Cybersecurity Recommendations	136

1 Overview

The access controller is an access control panel that supports unlocking through faces, passwords, fingerprint, cards, QR code, and their combinations. Based on the deep-learning algorithm, it features faster recognition and higher accuracy. It can work with management platform which meets various needs of customers.

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

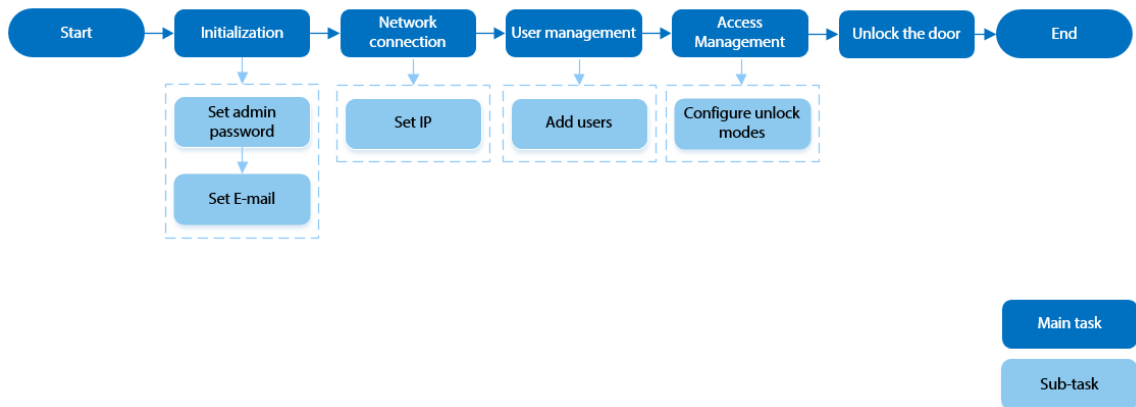
- Configurations might differ depending on the models of the product, please refer to the actual product.
- Devices with non-touch screen must connect to a mouse to perform configurations. This manual uses the device with touch screen as an example.
- Some models support connecting extension modules like QR code module, fingerprint module and more. The type of extension modules that the Access Controller supports might differ, please refer to the actual product.

2 Local Operations

- Configurations might differ depending on the actual product.
- Models with no-touch screen needs connecting a wired USB mouse. This section uses the models with touch screen as an example.
- External expansion modules are only available on select models.
- You might see some UI texts are not displayed because of the limited space. Long press the text for 3 seconds and it will show.

2.1 Basic Configuration Procedure

Figure 2-1 Basic configuration procedure



2.2 Common Icons

Table 2-1 Description of icons

Icon	Description
	Main menu icon.
	Confirm icon.
	Turn to the first page of the list.
	Turn to the last page of the list.
	Turn to the previous page of the list.
	Turn to the next page of the list.
	Return to the previous menu.
	Turned on.
	Turned off.
	Delete
	Search

2.3 Standby Screen

You can unlock the door through faces, card, passwords, and QR code. You can also make calls through the intercom function. Unlock methods might differ depending on the models of the product.



- If there is no operation in 30 seconds, the Access Controller will go to the standby mode.
- This manual is for reference only. Slight differences might be found between the standby screen in this manual and the actual device.

Figure 2-2 Standby screen

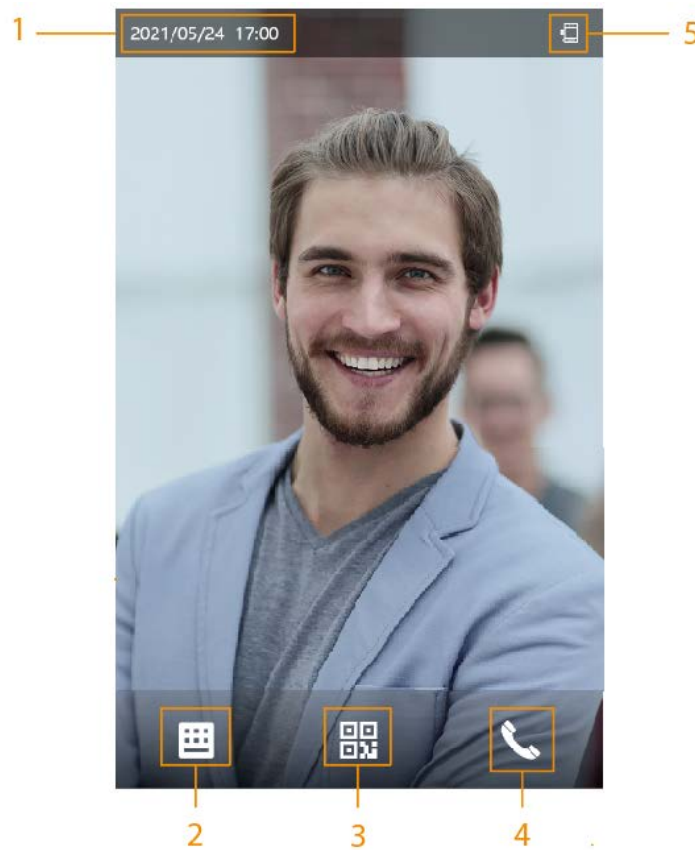



Table 2-2 Home screen description

No.	Name	Description
1	Date and time	Current date and time.
2	Password	Enter user password or administrator password or temporary password to unlock the door.

No.	Name	Description
3	QR code	<p>Tap the QR code icon and scan QR code to unlock the door.</p>  <p>For models that have a standalone QR code module or connects a QR expansion module. The icon will be not displayed. You can simply place your QR code in front of the lens of Access Controller or the expansion module, it will be automatically scanned.</p>
4	Intercom	<ul style="list-style-type: none"> • When the Access Controller functions as a server, it can call the VTO and VTH. • When the management platform functions as a server, the Access Controller can call the VTO, VTS and the management platform. • When it works with DMSS, it can call DMSS.
5	Status display	Displays status of Wi-Fi, network, extension module, USB and more. Wi-Fi and extension modules are only available on select models.

2.4 Initialization

For the first-time use or after restoring factory defaults, you need to select a language on Access Controller, and then set the password and email address for the admin account. You can use the admin account to enter the main menu of the Access Controller and its webpage.



- If you forget the administrator password, send a reset request to your registered e-mail address.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

2.5 Logging In

Log in to the main menu to configure the Access Controller. Only admin account and administrator account can enter the main menu of the Access Controller. For the first-time use, use the admin account to enter the main menu screen and then you can create the other administrator accounts.

Background Information

- admin account: Can log in to the main menu screen of the Access Controller, but does not have door access permissions.
- Administrator account: Can log in to the main menu of the Access Controller and has door access permissions.

Procedure

Step 1 Press and hold the standby screen for 3 seconds.

Step 2 Select a verification method to enter the main menu.

- Face: Enter the main menu by face recognition.
- Fingerprint: Enter the main menu by using fingerprint.



Fingerprint function is only available on select models.

- Card Punch: Enter the main menu by swiping card.
- PWD: Enter the user ID and password of the administrator account.
- admin: Enter the admin password to enter the main menu.

2.6 Unlocking Methods

You can unlock the door through faces, passwords, fingerprints, cards, and more.

2.6.1 Unlocking by Cards

Place the card at the swiping area to unlock the door.


2.6.2 Unlocking by Face

Verify the identity of an individual by detecting their faces. Make sure that the face is centered on the face detection frame.

2.6.3 Unlocking by User Password

Enter the user ID and password to unlock the door.

Procedure

Step 1 Tap  on the standby screen.

Step 2 Tap **Unlock by password**, and then enter the user ID and password.

Step 3 Tap **OK**.


2.6.4 Unlocking by Admin Password

Enter only the admin password to unlock the door. The door can be unlocked through admin password except for normally closed door. One device allows for only one admin password.


Prerequisites

The administrator password was configured. For details, see "2.7.3 Configuring the Admin Unlock Password".

Procedure

Step 1 Tap  on the standby screen.

Step 2 Tap **Unlock through Admin Password**, and then enter the admin password.


Step 3 Tap .



Administrator password cannot be used to unlock when the door status is set to always closed status.

2.6.5 Unlocking by QR code

Procedure

- Step 1 On the standby screen, tap .
- Step 2 Place your QR code in front of the lens.


2.6.6 Unlocking by Fingerprint

Place you finger on the fingerprint scanner. This function is only available select models.

2.6.7 Unlocking by Temporary Password

Unlock the door by the temporary password.

Procedure

- Step 1 Add the Access Controller to DMSS.
DMSS will generate a temporary password, which allow you unlock the door before it expires.
- Step 2 On the home screen, tap , and then tap **Unlock by Temporary Password**.
- Step 3 Enter the temporary password, and then tap

2.7 User Management

You can add new users, view user/admin list and edit user information.



The pictures in this manual are for reference only, and might differ from the actual product.

2.7.1 Adding Users

Procedure



- Step 1 On the **Main Menu**, select **Person Management > Create User**.
- Step 2 Configure the parameters on the interface.



Figure 2-3 Add new user


Parameter	Value
No.	3
Name	
Face	0
Card	0
Password	
User Permissions	User
Period	255-Default
Holiday Plan	255-Default
Validity Period	2037-12-31
User Type	General User

Table 2-3 Parameters description

Parameter	Description
No.	The No. is like employee ID, which can be numbers, letters, and their combinations, and the maximum length of the No. is 32 characters.
Name	The name can have up to 30 characters (including numbers, symbols, and letters).

Parameter	Description
FP	<p>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.</p>  <ul style="list-style-type: none"> • 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 Access Controller supports connecting a fingerprint extension module.
Face	<p>Position your face inside the frame, and a face image will be captured automatically. You can register again if you are not satisfied with the outcome.</p>
Card	<p>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 access controller.</p> <p>You can enable the Duress Card function. An alarm will be triggered if a duress card is used to unlock the door.</p>  <p>One user can only set one duress card.</p>
Password	<p>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. A duress alarm will be triggered when a duress password is used to unlock the door.</p>
User Permission	<ul style="list-style-type: none"> • User: Users only have door access or time attendance permissions. • Admin: Administrators can configure the Access Controller besides door access and attendance permissions.
Period	<p>People can unlock the door or take attendance during the defined period. For details on how to configure periods, see "3.7.8.1 Configuring Time Periods".</p>
Holiday Plan	<p>People can unlock the door or take attendance during the defined holiday. For details on how to configure periods, see "3.7.8.2 Configuring Holiday Plans".</p>
Validity Period	<p>Set a date on which the door access and attendance permissions of the person will be expired.</p>

Parameter	Description
User Type	<ul style="list-style-type: none"> • General User: General users can unlock the door. • Blocklist User: When users in the blocklist unlock the door, an blocklist alarm will be triggered. • 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 Access Controller, but they do not have door permissions. • VIP User: When VIP unlocks the door, service personnel will receive a notification. • 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.
Department	<p>Select departments, which is useful when configuring department schedules. For how to create departments, see "2.9.1 Configuring Departments".</p>  <p>This function is only available on select models.</p>
Schedule Mode	<ul style="list-style-type: none"> • Department Schedule: Apply department schedules to the user. • Personal Schedule: Apply personal schedules to the user. <p>For how to configure personal or department schedules, see "2.9.4 Configuring Work Schedules".</p>  <ul style="list-style-type: none"> ◇ This function is only available on select models. ◇ If you set the schedule mode to department schedule here, the personal schedule you have configured for the user in Attendance > Schedule Config > Personal Schedule become invalid.



Step 3 Tap 



2.7.2 Viewing User Information

Procedure

Step 1 On the **Main Menu**, select **Person Management > User List**, or select **User > Admin List**.





Step 2 View all added users and admin accounts.

- : Unlock through password.
- : Unlock through swiping card.

- : Unlock through face recognition.
- : Unlock through fingerprint.

Related Operations

On the **User** screen, you can manage the added users.

- Search for users: Tap  and then enter the username.
- Edit users: Tap the user to edit user information.
- Delete users
 - ◇ Delete one by one: Select a user, and then tap .
 - ◇ Delete in batches:
 - On the **User List** screen, tap  to delete all users.
 - On the **Admin List** screen, tap  to delete all admin users.

2.7.3 Configuring the Admin Unlock Password

You can unlock the door by only entering the admin password. The password is not limited by user types. Only one admin unlock password is allowed for one device.

Procedure

- Step 1 On the **Main Menu** screen, select **User** > **Admin Unlock Password**.
- Step 2 Tap **Admin Unlock Password**, and then enter a password.
- Step 3 Turn on the admin unlock function.

2.8 Access Management

You can configure settings for doors such as the unlocking mode, alarm linkage and door schedules. The available unlock modes might differ depending on the product model.

2.8.1 Configuring Unlock Combinations

Use card, fingerprint, face or password or their combinations to unlock the door. The available unlock modes might differ depending on the product model.

Procedure

- Step 1 Select **Access Control Management** > **Unlock Combination**.
- Step 2 Select unlock methods.



To cancel your selection, tap the selected method again.

- Step 3 Tap **+And** or **/Or** to configure combinations.

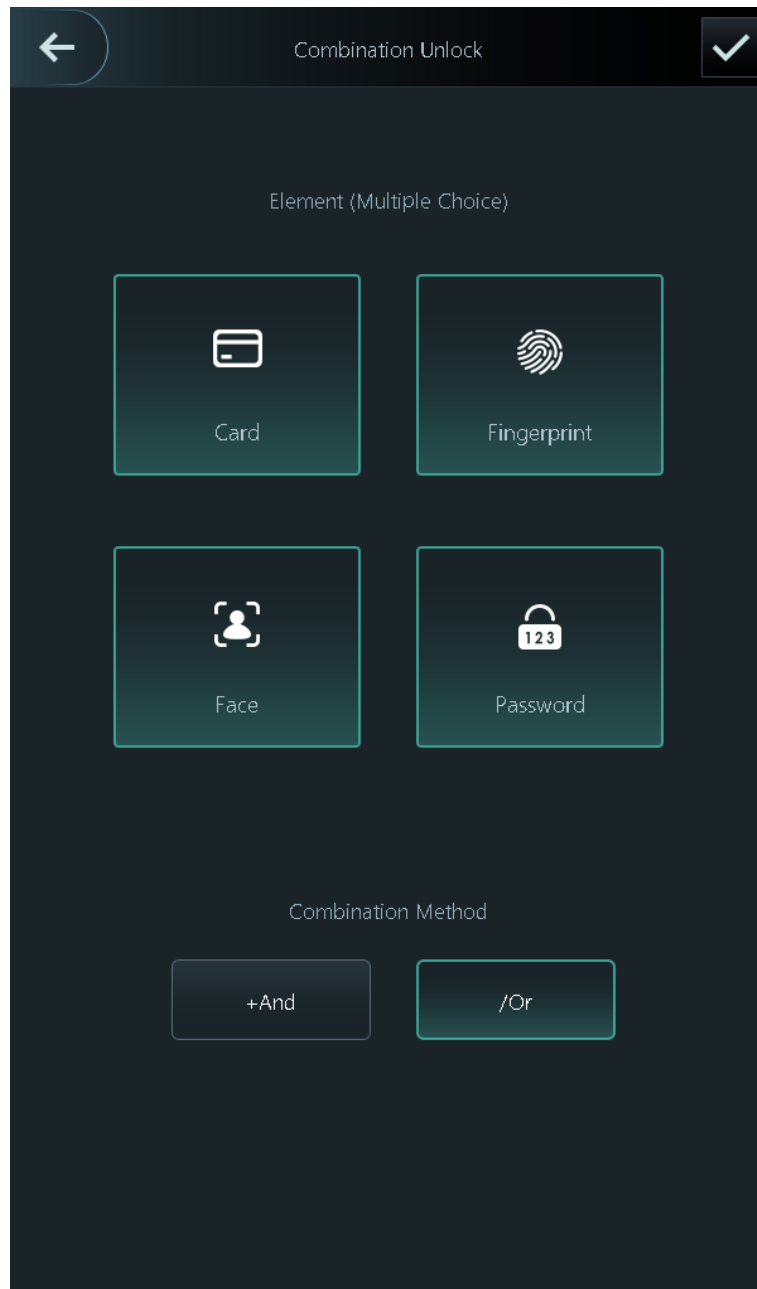
- **+And**: Verify all the selected unlock methods to open the door.



People have to complete verification in the order of card, fingerprint, face and password.

- **/Or**: Verify one of the selected unlock methods to open the door.

Figure 2-4 Element (multiple choice)



Step 4 Tap to save changes.

2.8.2 Configuring Alarms

An alarm will be triggered when the entrance or exit is abnormally accessed.

Procedure

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

Step 2 Enable the alarm type.



Alarm types might differ depending on the models of the product.

Figure 2-5 Alarm

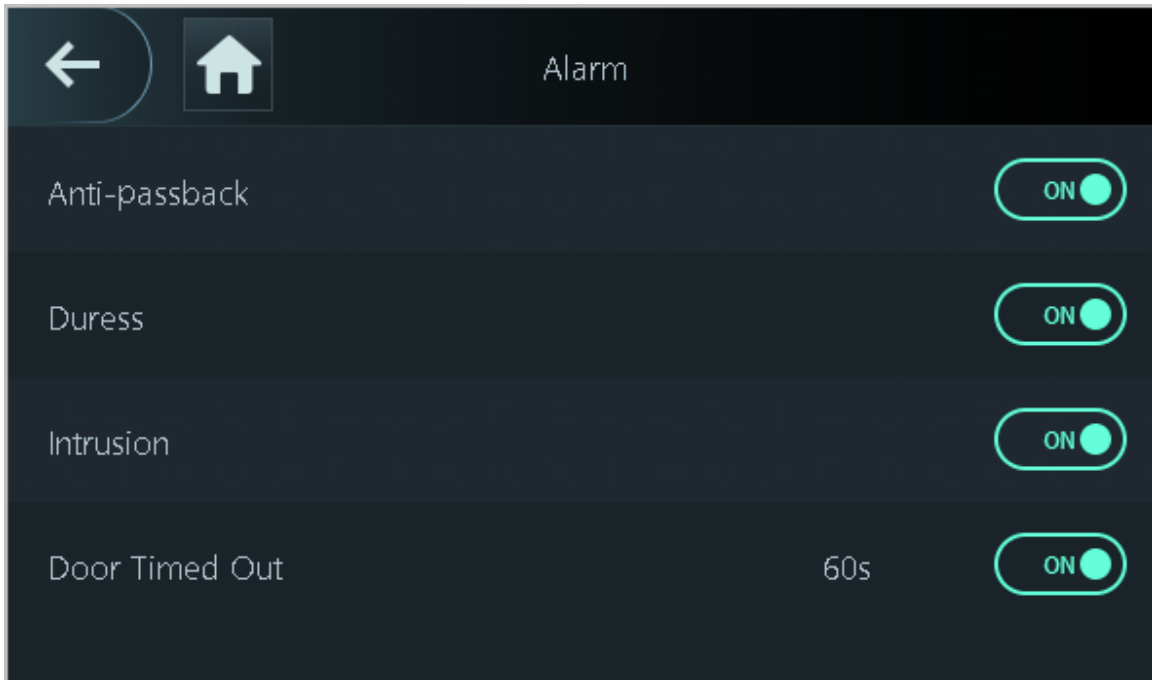



Table 2-4 Description of alarm parameters

Parameter	Description
Anti-passback	<p>Users need to verify their identities both for entry and exit; otherwise an alarm will be triggered. This helps prevent card holders from being able to give their card to other people to allow them access. When anti-passback is enabled, the card holder must leave the secured area through an exit reader before the system will grant them access again.</p> <p>People need to swipe their card at the "in" reader to enter a secured area and swipe it at the "out" reader to get out of it. As long as the sequence is "in, out, in, out , ect", the system will work fine.</p> <ul style="list-style-type: none"> • If a person enters after being verified, but exits without being verified, an alarm will be triggered if they attempt to enter again, and they will be denied access. • If a person enters without being verified, but exits after being verified, an alarm will be triggered if they attempt to enter again, and they will be denied access. <p> If the Access Controller can only connect one lock, verifying on the Access Controller means a "in" direction, and verifying on the external card reader means an "out" direction by default. You can modify the settings on the management platform.</p>
Duress	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.

Parameter	Description
Intrusion	When the door sensor is enabled, an intrusion alarm will be triggered if the door is opened abnormally.
Door Timed Out	An alarm will be triggered when the door remains unlocked for longer than the defined time. It ranges from 1 to 9,999 seconds.

2.8.3 Configuring the Door Status

Procedure

Step 1 On the **Main Menu** screen, select **Access Control Management > Lock Status Config**.

Step 2 Set door status.

Figure 2-6 Lock status

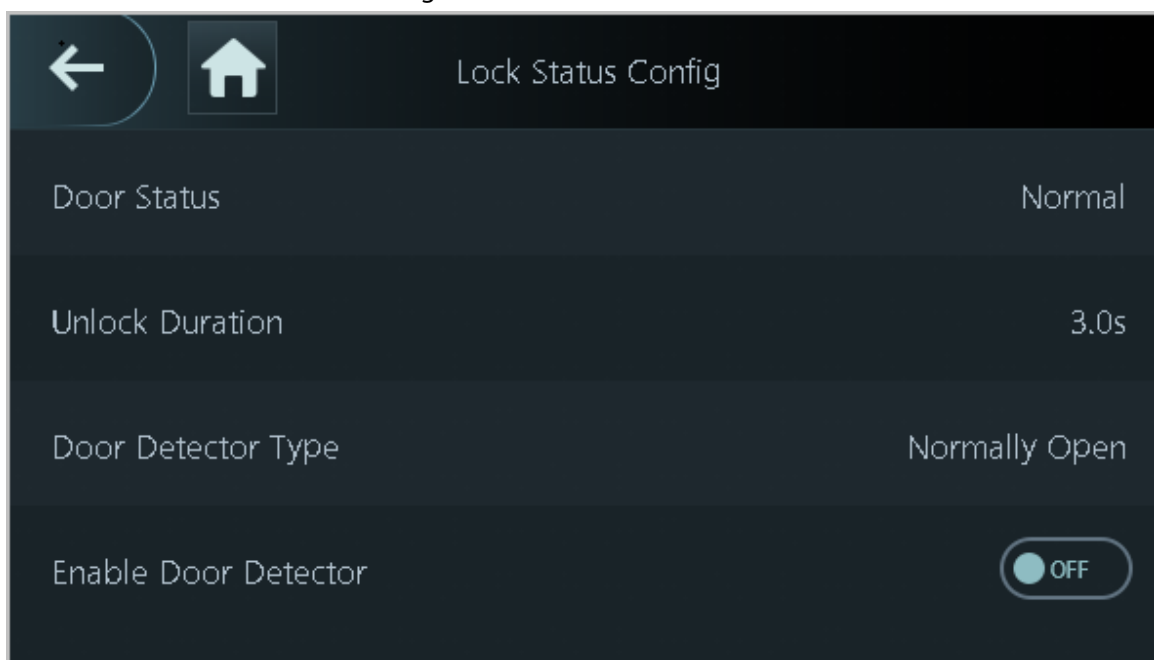


Table 2-5 Parameters description

Parameter	Description
Door Status	<ul style="list-style-type: none"> • Normally Open: The door remains unlocked all the time. • Normally Closed: The door remains locked all the time. • Normal: If Normal is selected, the door will be locked and unlocked according to your settings.
Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through.
Door Detector Type	<p>With the door detector wired to your device, alarms can be triggered when doors are abnormally opened or closed. The door detector includes 2 types, including NC detector and NO detector.</p> <ul style="list-style-type: none"> • Normally Closed: The sensor is in a shorted position when the door or window is closed • Normally Open: An open circuit is created when the window or door is actually closed.

Parameter	Description
Enable Door Detector	The intrusion and door-time out alarms will take effect only after this function is enabled.

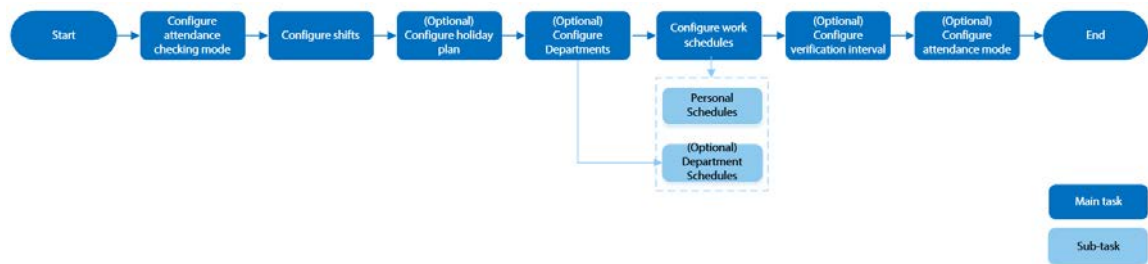
2.9 Attendance Management

Time attendance supports attendance management both on the local device or and Smart PSS Lite. This section only uses configuring attendance on the local device as an example.



This function is only available on select models of 4.3 inch series.

Figure 2-7 Configuration flow chart of time attendance



2.9.1 Configuring Departments


Procedure

- Step 1 Select **Attendance > Department Settings**.
- Step 2 Select a department, and then rename it.
There are 20 default departments. We recommend you rename them.

Figure 2-8 Create departments



ID	Department Group Name
1	Lalai
2	Lalai
3	Lalai
4	Lalai
5	Lalai
6	Lalai
7	Lalai
8	Lalai

Step 3 Tap .


2.9.2 Configuring Shifts

Configure shifts to define time attendance rules. Employees need to come to work at the time scheduled for their shift to start, and leave at the end time, except when they choose to work overtime.

Procedure

Step 1 Select **Attendance > Shift Config**.

Step 2 Select a shift.

Tap  to view more shifts. You can configure up to 24 shifts.

Step 3 Configure the parameters of the shift.

Figure 2-9 Create shifts

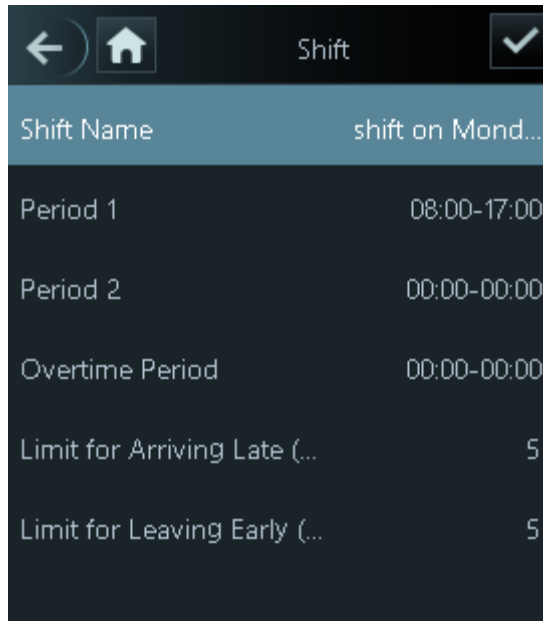
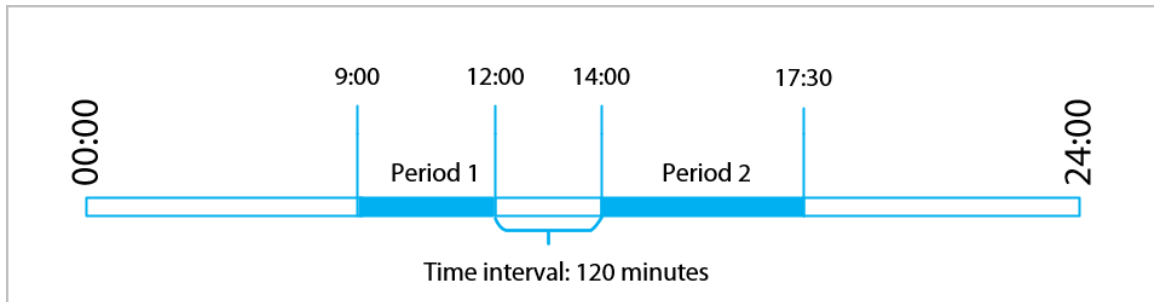


Table 2-6 Shift parameters description

Parameter	Description
Shift Name	Enter the name of the shift.
Period 1	<p>Specify a time range when people can clock in and clock out for the workday.</p> <p>If you only set one attendance period, employees need to clock in and out by the designated times to avoid an anomaly appearing on their attendance record. For example, if you set 08:00 to 17:00, employees must clock in by 08:00 and clock out from 17:00 onwards.</p> <p>If you set 2 attendance periods, the 2 periods cannot overlap. Employees need to clock in and clock out for both periods.</p>
Period 2	
Overtime Period	Employees who clock in or out during the defined period will be considered as working beyond their normal work hours.
Limit for Arriving Late (min)	<p>A certain amount of time can be granted to employees to allow them to clock in a bit late and clock out a bit early. For example, if the regular time to clock in is 08:00, the tolerance period can be set as 5 minutes for employees who arrive by 08:05 to not be considered as late.</p>
Limit for Leaving Early (min)	

- When the time interval between 2 periods is an even number, you can divide the time interval by 2, and assign the first half of the interval to the first period, which will be the clock out time. The second half of the interval should be assigned to the second period as the clock in time.

Figure 2-10 Time interval (Even number)



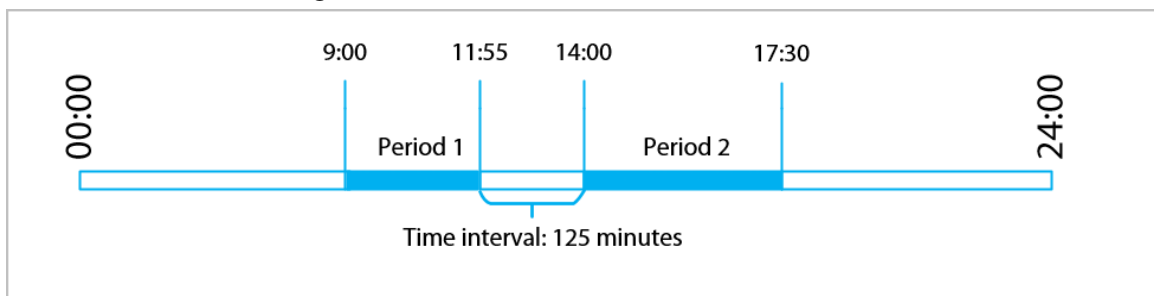
For example: If the interval is 120 minutes, then the clock-out time for period 1 is from 12:00 to 12:59, and the clock-in time for period 2 is from 13:00 to 14:00.



If a person clocks out multiple times during period 1, the latest time will be valid, and if they clock in multiple times during period 2, the earliest time will be valid.

- When the time interval between 2 periods is an odd number, the smallest portion of the interval will be assigned to the first period, which will be the clock out time. The largest portion of the interval will be assigned to the second period as the clock in time.

Figure 2-11 Time interval (even number)



For example: If the interval is 125 minutes, then the clock-out time for period 1 is from 11:55 to 12:57, and the clock-in time for period 2 is from 12:58 to 14:00. Period 1 has 62 minutes, and period 2 has 63 minutes.



If a person clocks out multiple times during period 1, the latest time will be valid, and if they clock in multiple times during period 2, the earliest time will be valid.



All attendance times are precise down to the second. For example, if the normal clock-in time is set to 8:05 AM, the employee who clocks in at 8:05:59 AM will not be considered as arriving late. But, the employee that arrives at 8:06 AM will be marked as late by 1 minute.

Step 4 Tap

2.9.3 Configuring Holiday Plans

Configure holiday plans to set periods for attendance to not be tracked.

Procedure

Step 1 Select **Attendance > Shift Config > Holiday**.

Step 2 Click + to add holiday plans.

Step 3 Configure the parameters.

Figure 2-12 Create holiday plans

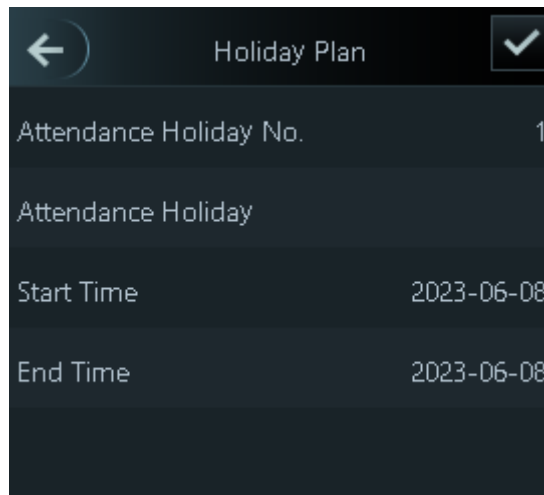



Table 2-7 Parameters description

Parameter	Description
Attendance Holiday No.	The number of the holiday.
Attendance Holiday	The name of the holiday.
Start Time	The start and end time of the holiday.
End Time	

Step 4 Tap .

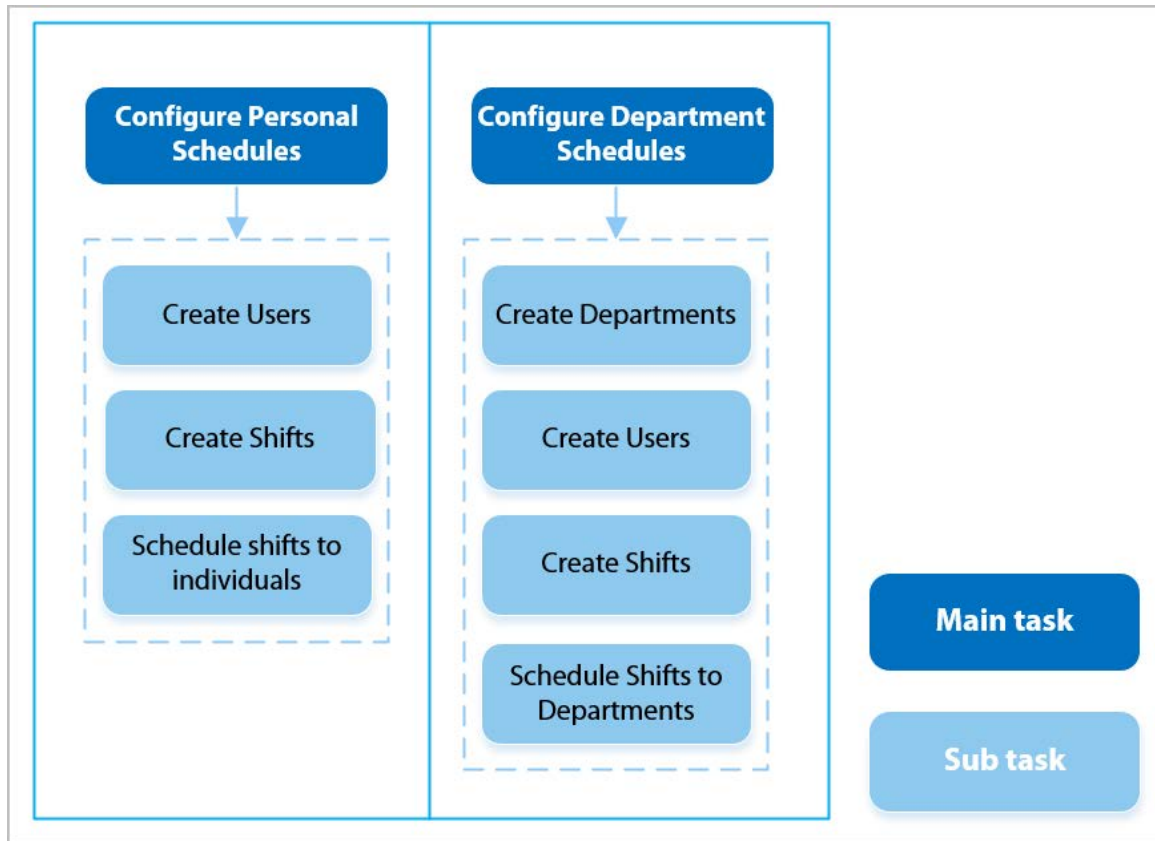
2.9.4 Configuring Work Schedules

A work schedule generally refers to the days per month and the hours per day that an employee is expected to be at their job. You can create different types of work schedules based on different individuals or departments, and then employees must follow the established work schedules.

Background Information

Refer to the flowchart to configure personal schedules or department schedules.

Figure 2-13 Configuring work schedules



Procedure

- Step 1 Select **Attendance > Schedule Config**.
- Step 2 Set work schedules for individuals.
1. Tap **Personal Schedule**.
 2. Enter the user ID, and then tap .
 3. On the calendar, select a day, and then select a shift.
The shift is scheduled for the day.



You can only set work schedules for the current month and the next month.

- 0 indicates break.
- 1 to 24 indicates the number of the per-defined shifts. For how to configure shifts, see "2.9.2 Configuring Shifts".
- 25 indicates business trip.
- 26 indicates leave of absence.

Figure 2-14 Schedule shifts to individuals

Day	Mon	Tue	Wed	Thu	Fri	Sat
28	29	30	31	1 1	1 2	0 3
0 4	1 5	1 6	1 7	1 8	1 9	0 10
0 11	1 12	1 13	1 14	1 15	1 16	0 17
0 18	1 19	1 20	1 21	1 22	1 23	0 24
0 25	1 26	1 27	1 28	1 29	1 30	1
2	3	4	5	6	7	8

4. Tap

Step 3 Set works schedules for departments.

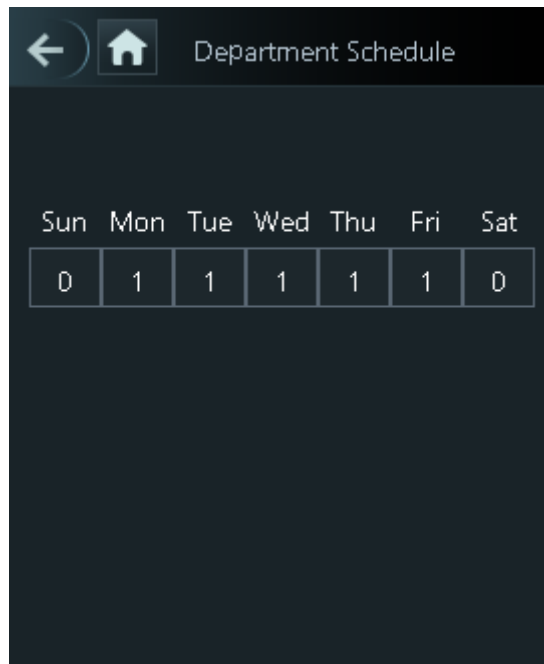
1. Tap **Department Schedule**.

2. Tap a department, and then select shifts for a week.

Shifts are scheduled for the week.

- 0 indicates rest.
- 1 to 24 indicates the number of the per-defined shifts. For how to configure shifts, see "2.9.2 Configuring Shifts".
- 25 indicates business trip.
- 26 indicates leave of absence.

Figure 2-15 Schedule shifts to a department



The defined work schedule is in a week cycle and will be applied to all employees in the department.

Step 4 Tap .

2.9.5 Configuring the Verification Time Interval

When an employee clocks in and out multiple times within a set period, the earliest time will be valid.

Procedure

Step 1 Select **Attendance > Verification Interval (sec)**.

Step 2 Enter the time interval, and then tap .

2.9.6 Configuring Attendance Modes

When you clock in or clock out, you can set the attendance modes to define the attendance status.

Procedure

Step 1 On the main menu screen, select **Attendance > Mode Settings**.

Step 2 Enable **Local or Remote**, and then set the attendance mode.

The attendance records will also be synchronized to the management platform.

Figure 2-16 Attendance mode

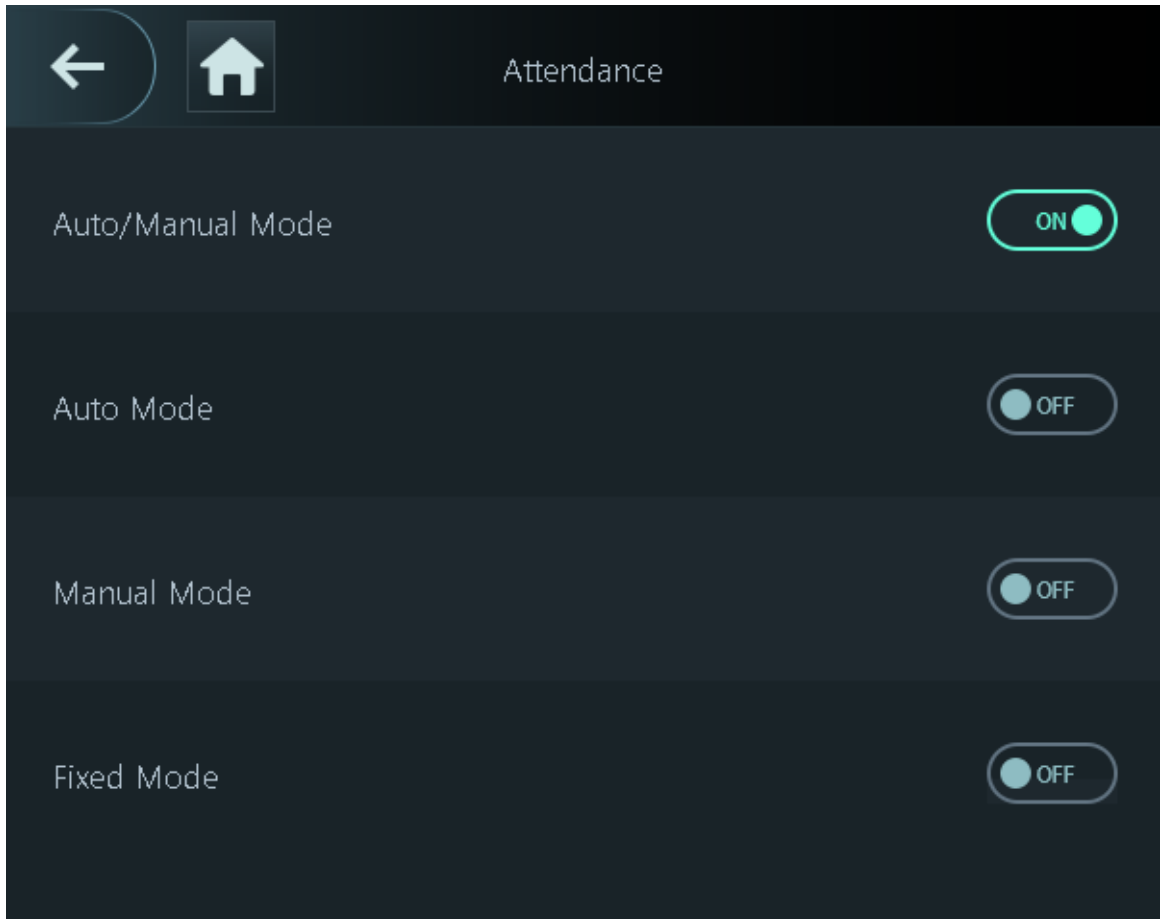


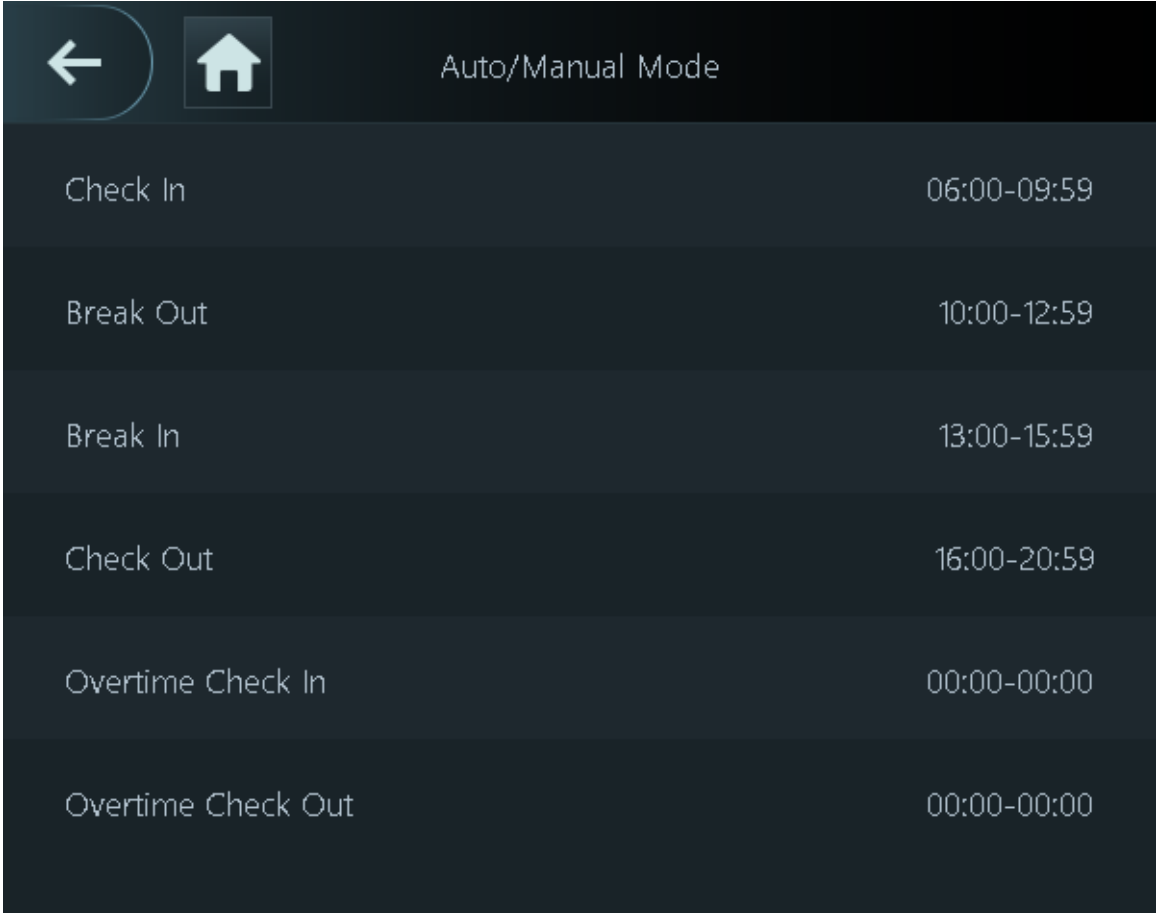
Table 2-8 Attendance mode

Parameter	Description
Auto/Manual Mode	The screen displays the attendance status automatically after you clock in or out, but you can also manually change your attendance status.
Auto Mode	The screen displays your attendance status automatically after you clock in or out.
Manual Mode	Manually select your attendance status when you clock in or out.
Fixed Mode	When you clock in or out, the screen will display the per-defined attendance status all the time.

Step 3 Select an attendance mode.

Step 4 Configure the parameters for the attendance mode.

Figure 2-17 Auto Mode/manual mode



The screenshot displays a mobile application interface for 'Auto/Manual Mode'. At the top, there is a dark header bar containing a back arrow icon on the left, a home icon in a square, and the text 'Auto/Manual Mode' on the right. Below the header is a list of six items, each consisting of a text label on the left and a time range on the right. The items are: 'Check In' (06:00-09:59), 'Break Out' (10:00-12:59), 'Break In' (13:00-15:59), 'Check Out' (16:00-20:59), 'Overtime Check In' (00:00-00:00), and 'Overtime Check Out' (00:00-00:00).

Check In	06:00-09:59
Break Out	10:00-12:59
Break In	13:00-15:59
Check Out	16:00-20:59
Overtime Check In	00:00-00:00
Overtime Check Out	00:00-00:00

Figure 2-18 Fixed mode

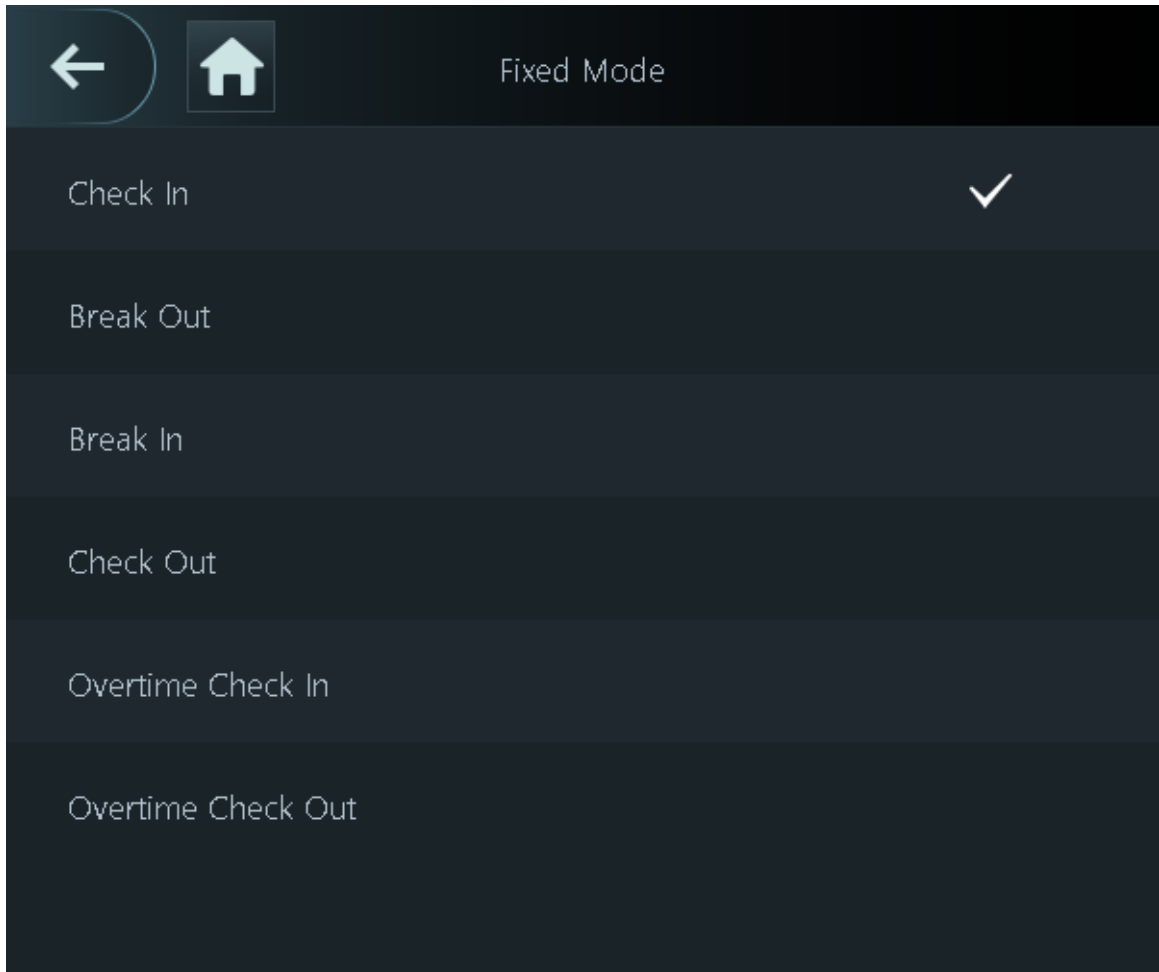


Table 2-9 Attendance mode parameters

Parameters	Description
Check In	Clock in when your normal workday starts.
Break Out	Clock out when your break starts.
Break In	Clock in when your break ends.
Check Out	Clock out when your normal workday starts.
Overtime Check In	Clock in when your overtime period starts.
Overtime Check Out	Clock out when your overtime period ends.

2.10 Network Communication

Configure the network, serial port and Wiegand port to connect the Access Controller to the network.



The serial port and the wiegand port might differ depending on the models of Access Controller.

2.10.1 Configuring the IP Address

Set an IP address for the Access Controller to connect it to the network. After that, you can log in to the webpage and the management platform to manage the Access Controller.

Procedure

Step 1 On the **Main Menu**, select **Communication Settings > Network > IP Address**.

Step 2 Set the IP Address.

Figure 2-19 IP address configuration

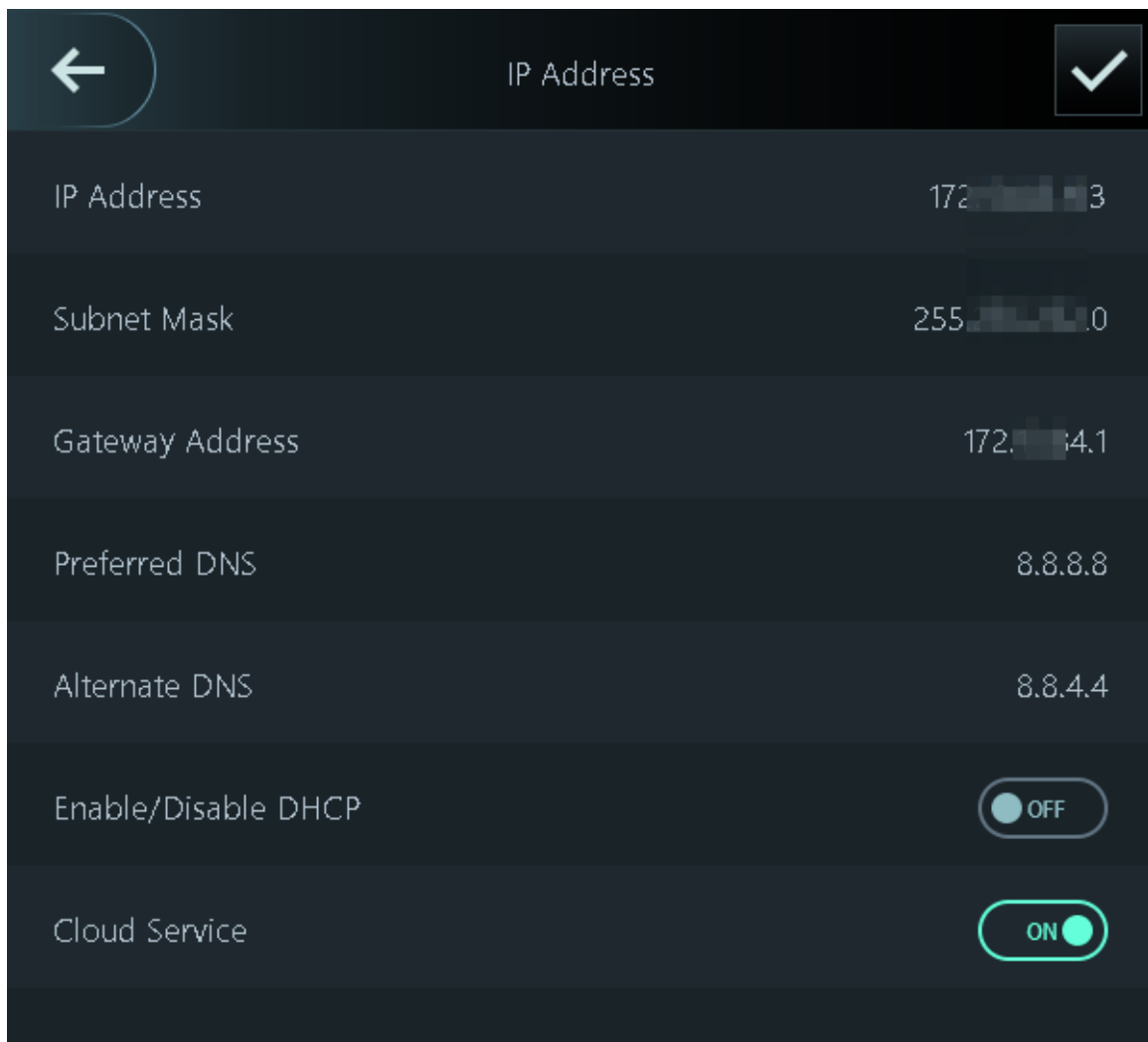


Table 2-10 IP configuration parameters

Parameter	Description
IP Address/Subnet Mask/Gateway Address	The IP address, subnet mask, and gateway IP address must be on the same network segment.
Preferred DNS	The IP of the DNS server.
Alternate DNS	The alternate IP of the DNS server.

Parameter	Description
Enable/Disable DHCP	It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Access Controller will automatically be assigned an IP address, subnet mask, and gateway.
Cloud Service	Manage devices without applying for DDNS, set port mapping and deploy transit servers.

2.10.2 Configuring Active Registration

Add the device to a management platform, so that you can manage it on the platform.

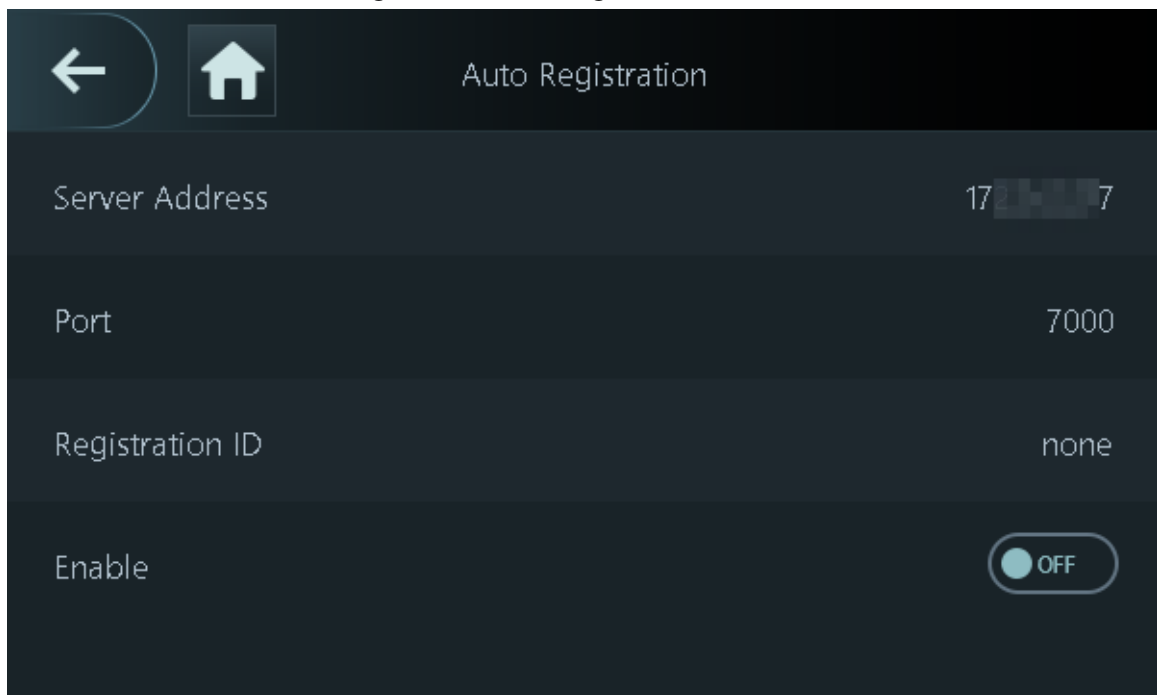
Procedure

Step 1 On the **Main Menu**, select **Communication > Network > Auto Registration**.



To avoid exposing the system to security risks and data loss, control the management platform permissions.


Figure 2-20 Active registration



Step 2 Turn on the automatic registration function and set the parameters.

Table 2-11 Auto registration

Parameter	Description
Server Address	The IP address of the management platform.
Port	The port No. of the management platform.

Parameter	Description
Registration ID	<p>Enter the device ID (user defined).</p>  <p>When you add the Access Controller to the management platform, the registration ID you enter on the management platform must conform to the defined registration ID on the Access Controller.</p>

Step 3 Enable the function.

2.10.3 Configuring the Wi-Fi

You can connect the Access Controller to the network through the Wi-Fi network.


Procedure

Step 1 On the **Main Menu**, select **Communication > Network > Wi-Fi**.

Step 2 Turn on Wi-Fi.



The Wi-Fi function is only available on select models.

Step 3 Tap  to search available wireless networks.

Step 4 Select a wireless network and enter the password.

If the system does not find a Wi-Fi network, tap **SSID** to enter the name of the Wi-Fi.

Step 5 Tap .

2.10.4 Configuring Serial Port

Procedure

Step 1 On the **Main Menu**, select **Communication Settings > Serial Port**.

Step 2 Select a port type.

Table 2-12 Port description

External device	Description
Access Controller	<p>Select Access Controller when the Access Controller functions as a card reader, and the Access Controller will send data to the Access Controller to control access.</p> <p>Output Data type:</p> <ul style="list-style-type: none"> • Card Number: Outputs data based on the card number when users swipe their cards to unlock doors; outputs data based on user's first card number when users use other unlock methods. . • No.: Outputs data based on the user ID.
Card Reader	The Access Controller connects to a card reader.
Reader (OSDP)	The Access Controller is connected to a card reader based on the OSDP protocol.

External device	Description
Door Control Security Module	The door exit button, lock control and fire linkage become not effective after the security module is enabled.
Turnstile	When the Access Controller is connected to a turnstile, and the access controller board of the turnstile is connected to an external QR code module or card swiping module, the board will transmit the verification data to the turnstile.

2.10.5 Configuring Wiegand

The access controller allows for both Wiegand input and output mode.

Procedure

Step 1 On the webpage, select **Communication Settings > Wiegand**.

Step 2 Select a Wiegand.

- Select **Wiegand Input** when you connect an external card reader to the Access Controller.
- Select **Wiegand Output** when the Access Controller functions as a card reader, and you need to connect it to a controller or another access terminal.

Figure 2-21 Wiegand output



Table 2-13 Description of Wiegand output

Parameter	Description
Wiegand Output Type	Select a Wiegand format to read card numbers or ID numbers. <ul style="list-style-type: none"> • Wiegand26: Reads 3 bytes or 6 digits. • Wiegand34: Reads 4 bytes or 8 digits. • Wiegand66: Reads 8 bytes or 16 digits.
Pulse Width	Enter the pulse width and pulse interval of Wiegand output.

Parameter	Description
Pulse Interval	
Output Data Type	Select the type of output data. <ul style="list-style-type: none"> • No.: The system outputs data based on the user ID. The data format is hexadecimal or decimal. • Card Number: The system outputs data based on user's first card number.

Step 3 Click **Apply**.

2.11 System Settings

2.11.1 Configuring Time

Configure system time, such as date, time, and NTP.

Procedure

Step 1 On the **Main Menu**, select **System Settings > Time**.

Step 2 Configure system time.

Figure 2-22 Time



Table 2-14 Description of time parameters

Parameter	Description
24-hour System	The time is displayed in 24-hour format.
Date & Time	Set up the date.
Time	Set up the time.
Date Format	Select a date format.
DST Setting	<ol style="list-style-type: none"> 1. Tap DST Setting and enable it. 2. Select Date or Week from the DST Type list. 3. Enter the start time and end time. 4. Tap <input checked="" type="checkbox"/>.

Parameter	Description
NTP Time Sync	<p>A network time protocol (NTP) server is a machine dedicated as the time sync server for all client computers. If your computer is set to sync with a time server on the network, your clock will show the same time as the server. When the administrator changes the time (for daylight savings), all client machines on the network will also be updated.</p> <ol style="list-style-type: none"> 1. Tap NTP Check, and then enable it. 2. Configure the parameters. <ul style="list-style-type: none"> • Server Address: Enter the IP address of the NTP server, and the Access Controller will automatically sync time with the NTP server. • Port: Enter the port of the NTP server. • Interval: Enter the time synchronization interval.
Time Zone	Select the time zone.

2.11.2 Configuring Face Parameters

Procedure




- Step 1** On the main menu, select **System Settings > Face Parameter Config**.
- Step 2** Configure the face parameters, and then tap .

Figure 2-23 Face parameter (01)



Table 2-15 Description of face parameters

Name	Description
Face Recognition Threshold	Adjust the accuracy level of face recognition. Higher threshold means higher accuracy and lower false recognition rate.
Max Face Recognition Angle Deviation	Set the largest angle that a face can be posed in for face detection. The larger the value, the larger the range for the face angle. If the angle a face is positioned in is not within the defined range, it might not be detected properly.
Pupillary Distance	A certain number of pixels are required between the eyes, called pupillary distance, for recognition to be successful. The default number is 45 pixels. This number changes based on the size of the face and the distance between the face and the lens. If an adult is 1.5 meters away from the lens, the pupillary distance is usually 50 - 70 px.
Valid Face Interval (sec)	When a person has their face successfully verified too many times, Access Controller prompts verification successful within the defined time interval.
invalid Face Interval (sec)	When a person fails to have their face verified too many times, Access Controller prompts verification failed within the defined time interval.
Enable Anti-spoofing	This prevents people from being able to use photos, videos, mask and other substitutes to gain unauthorized access.
Enable Beautifier	Beautify captured face images.
Enable Helmet Detection	Detects safety helmets. The door will not unlock for persons that are not wearing their helmet.
Mask Parameters	<ul style="list-style-type: none"> ● Mask mode: <ul style="list-style-type: none"> ◇ Do Not Detect: Mask is not detected during face recognition. ◇ Mask Reminder: Mask is detected during face recognition. If the person is not wearing a mask, the system will remind them to wear a mask, but they will still be allowed access. ◇ No Authorization without Wearing Face Mask: Mask is detected during face recognition. If a person is not wearing a mask, the system will remind them to wear masks, and access will be denied. ● Mask Recognition Threshold: The higher the threshold, the more accurate face recognition will be when a person is wearing a mask, and there will be a lower false recognition rate.

Name	Description
Multi-face Recognition	<p>Detects 4 to 6 face images at a time. Combination unlock cannot be used with this, and the door will be unlocked when one of the people are successfully verified.</p>  <p>The number of face images which are supported might differ depending on the model of the product.</p>
Illuminator Mode	<ul style="list-style-type: none"> • Auto: The illuminator is turned on in low-light conditions. • Disable: The illuminator is turned off all the time.  <p>This function is only available on select models.</p>

2.11.3 Setting the Volume

You can adjust the volume of the speaker and microphone.

Procedure

Step 1 On the **Main Menu**, select **System Settings > Volume Settings**.

Step 2 Select **Beep Volume** or **Microphone Volume**, and then tap  or  to adjust the volume.

2.11.4 Configuring the Language

Change the language on the Access Controller. On the **Main Menu**, select **System Settings > Language**, select the language for the Access Controller.

2.11.5 Screen Settings

Configure when the display should turn off and the logout time.

Procedure

Step 1 On the **Main Menu**, select **System > Screen Settings**.

Step 2 Tap **Logout Time** or **Screen Off Settings**, and then tap  or  to adjust the time.

- Logout Time: The system goes back to the standby screen after a defined time of inactivity.
- Screen Off Settings: The system goes back to the standby screen and then the screen turns off after a defined time of inactivity. For example, if the logout time is set to 15 seconds, and the screen off time is set to 30 seconds, the system goes back to the standby screen after 15 seconds, and then the screen will turn off after another 15 seconds.



The logout time must be less than the screen off time.

2.11.6 (Optional) Configuring Fingerprint Parameters

Configure fingerprint detection accuracy. The higher the value, the higher the similarity threshold and accuracy is.

Background Information



This function is only available on select models, and some supports being connected to a fingerprint extension module.

Procedure

Step 1 On the **Main Menu**, select **System Settings** > **Fingerprint Parameter Settings**.

Step 2 Tap **+** or **-** to adjust the value.

2.11.7 Restoring Factory Defaults

Procedure

Step 1 On the **Main Menu**, select **System Settings** > **Factory Defaults**.

Step 2 Restore factory defaults if necessary. Restore the factory default settings if necessary.

- **Factory Defaults:** Resets all configurations and data except for IP settings and the type of the extension module.
- **Restore to Default Settings (except for user information and logs):** Resets all the configurations except for user information and logs.

2.11.8 Restarting the Device

On the **Main Menu**, select **System Settings** > **Restart**, and the Access Controller will be restarted.

2.12 Functions Settings

On the **Main Menu** screen, select **Functions**.



The functions might differ depending on the model of the product.

Figure 2-24 Functions

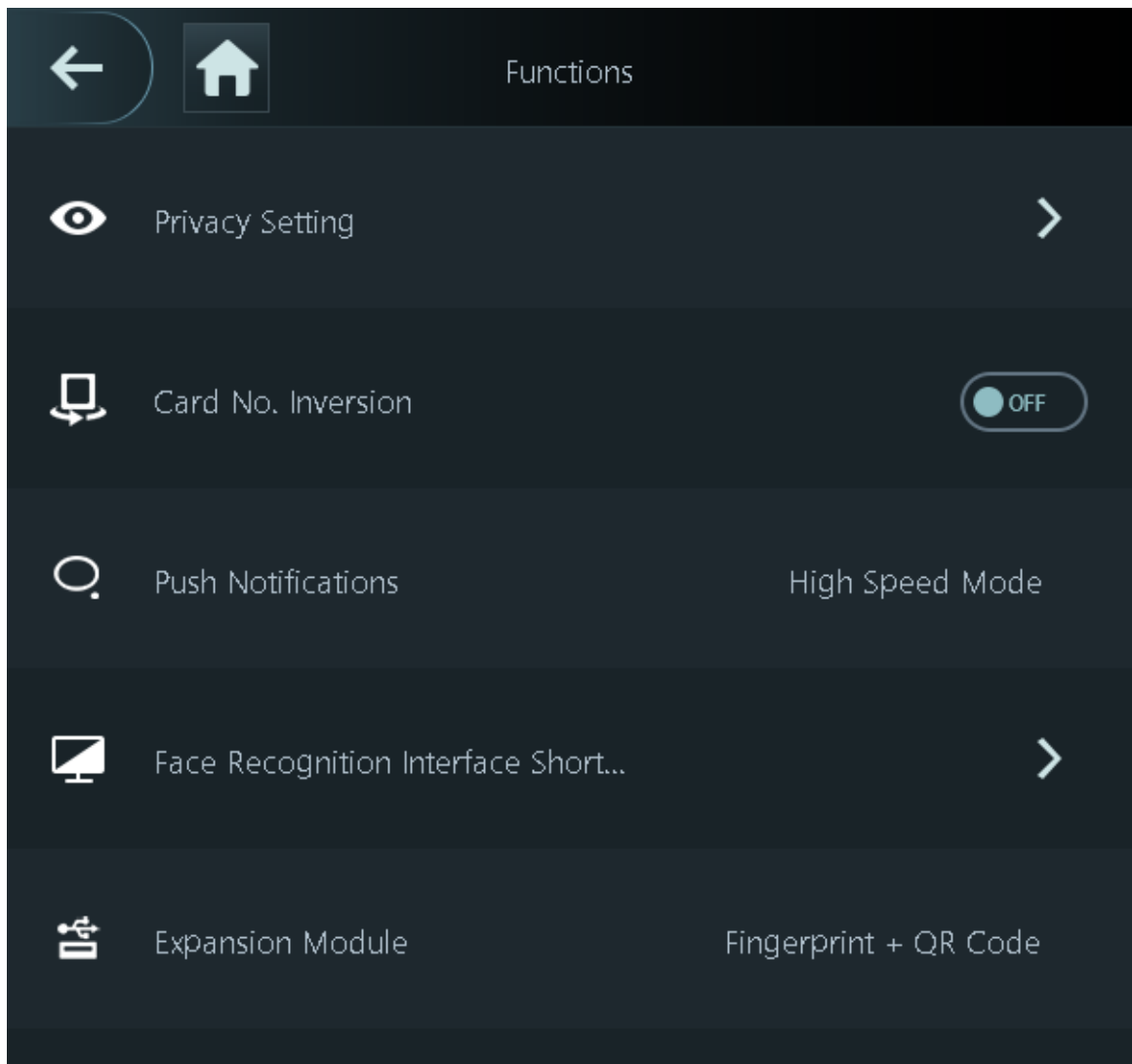









Table 2-16 Function description

Parameter	Description
Private Setting	<ul style="list-style-type: none"> ● Password Reset: The password can be reset when you turn on this function. ● Enable HTTPS: Hypertext Transfer Protocol Secure (HTTPS) is a protocol for secure communication over a computer network. When HTTPS is enabled, HTTPS will be used to access CGI commands; otherwise HTTP will be used. <p style="text-align: center;"></p> <p>When HTTPS is enabled, the Access Controller will automatically restart.</p> <ul style="list-style-type: none"> ● Enable CGI: Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs similar to how console applications run on a server that dynamically generates webpages. The CGI is enabled by default. ● Enable SSH: Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. The data transmitted will be encrypted after this function is enabled. ● Fingerprint Image: The fingerprint image is displayed when you unlock through fingerprint. <p style="text-align: center;"></p> <p>This function is only available on select models.</p> <ul style="list-style-type: none"> ● Capture: Face images will be captured automatically when people unlock the door. The function is enabled by default. ● Clear All Snapshots: Delete all automatically captured photos.
Card No. Inversion	<p>When the Access Controller connects to a third-party device through the Wiegand input port, and the card number read by the Access Controller is in the reverse order from the actual card number. In this case, you can turn on this function.</p>

Parameter	Description
Push Notifications	<p>Displays the notification on the screen when a person is verifying their identity on the Access Controller.</p> <ul style="list-style-type: none"> ● High Speed Mode: The system prompts Successfully verified or Not authorized on the screen. ● Simple Mode: Displays user ID, name and verification time after access is granted, and displays Not authorized and the authorization time after access is denied. ● Standard: Displays the user's registered face image, user ID, name and verification time after access is granted, and displays Not authorized and the verification time after access is denied. ● Contrast Mode: Displays the captured face image and a registered face image of a user, user ID, name and authorization time after access is granted, and displays Not authorized after access is denied.
Face Recognition Interface Shortcut	<p>Select identity verification methods on the standby screen.</p> <ul style="list-style-type: none"> ● Password: It's icon is displayed on the standby screen. ● QR code: It's icon is displayed on the standby screen. ● Doorbell: It's icon is displayed on the standby screen. <ul style="list-style-type: none"> ◇ Ringing: Tap the ring bell icon on the standby screen, and the Access Controller rings. ◇ Alarm: Tap the ring bell icon, and the external alarm device rings. <p style="text-align: center;"></p> <p style="text-align: center;">This function is only available on select models.</p> <ul style="list-style-type: none"> ◇ Ringtone Config: Select a ringtone ◇ Ringtone Time (sec): Set ring time (1-30 seconds). The default value is 3. ● Call: It's icon is displayed on the standby screen. ● Call Type: <ul style="list-style-type: none"> ◇ Call Room: Tap the call icon on the standby mode and enter the room number to make a call. ◇ Call Management Center: Tap the call icon on the standby mode, and then call the management center. ◇ Custom call room: Tap the call icon on the standby screen to call the pre-defined room. <p style="text-align: center;"></p> <p style="text-align: center;">Make sure the Access Controller was added to DMSS.</p> <ul style="list-style-type: none"> ● Enable SIP: You can turn on SIP to set the Access Controller to SIP server.

Parameter	Description
Expansion Module	<p>Select an expansion module, and the Access Controller will restart.</p> <ul style="list-style-type: none"> •  is displayed on the right corner on the standby screen, which means it was successfully set. •  is displayed on the right corner on the standby screen, which means setup failed. <p></p> <ul style="list-style-type: none"> • Expansion module is only available on select models. • Expansion module does not support hot swapping. • The configuration for the expansion module remains unchanged even after the system is restored to its factory settings.

2.13 USB Management

You can use a USB to update the Access Controller, and export or import user information or attendance records through USB.



- Make sure that a USB is inserted to the Access Controller before you export data or update the system. To avoid failure, do not pull out the USB or perform any operation of the Access Controller during the process.
- You have to use a USB to export the information from an Access Controller to other devices. Face images are not allowed to be imported through USB.
- Importing/exporting attendance records is only available on select models.

2.13.1 Exporting to USB

You can export data from the Access Controller to a USB. The exported data is encrypted and cannot be edited.

Procedure

- Step 1 On the **Main Menu**, select **USB Management > USB Export**.
- Step 2 Select the data type you want to export, and then tap **OK**.



- When the data is exported in Excel, it can be edited.
- The USB disk supports the format in FAT32, and the storage capacity is 4 GB—128 GB.

2.13.2 Importing From USB

You can import data from USB to the Access Controller.

Procedure

- Step 1 On the **Main Menu**, select **USB Management** > **USB Import**.
- Step 2 Select the data type that you want to export, and then tap **OK**.

2.13.3 Updating the System

Update the system of the Access Controller through USB.

Procedure

- Step 1 Rename the update file to "update.bin", put it in the root directory of the USB, and then insert the USB to the Access Controller.
- Step 2 On the **Main Menu**, select **USB Management** > **USB Update**.
- Step 3 Tap **OK**.
- The Access Controller will restart when the updating completes.



Do not power off the Access Controller during the update.

2.14 Record Management

On the main menu, select **Record Management** > **Search for Unlock Records**. The unlock records are displayed. You can search for record by user ID.

2.15 System Information

You can view data capacity and device version.

2.15.1 Viewing Data Capacity

On the **Main Menu**, select **System Info** > **Data Capacity**, you can view storage capacity of each data type.

2.15.2 Viewing Device Version

On the **Main Menu**, select **System Info** > **Device Version**, you can view the device version, such as serial No., software version and more.

3 Web Operations

On the webpage, you can also configure and update the Access Controller.



Web configurations differ depending on models of the Access Controller.

3.1 Initialization

Initialize the Access Controller when you log in to the webpage for the first time or after the Access Controller 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 Access Controller.

Procedure

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



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

Step 2 Select a language on Access Controller.

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.

3.2 Logging In

Procedure

Step 1 Open a browser, enter the IP address of the Access Controller in the **Address** bar, and press the Enter key.

Step 2 Enter the user name and password.



- The default administrator 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 click **Forgot password?** For details,

Step 3 Click **Login**.

3.3 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 3-1 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 support_rpwd@global.dawatech.com.
Email Address: 1***@****.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**.

3.4 Home Page

The home page is displayed after you successfully log in.

Figure 3-2 Home page

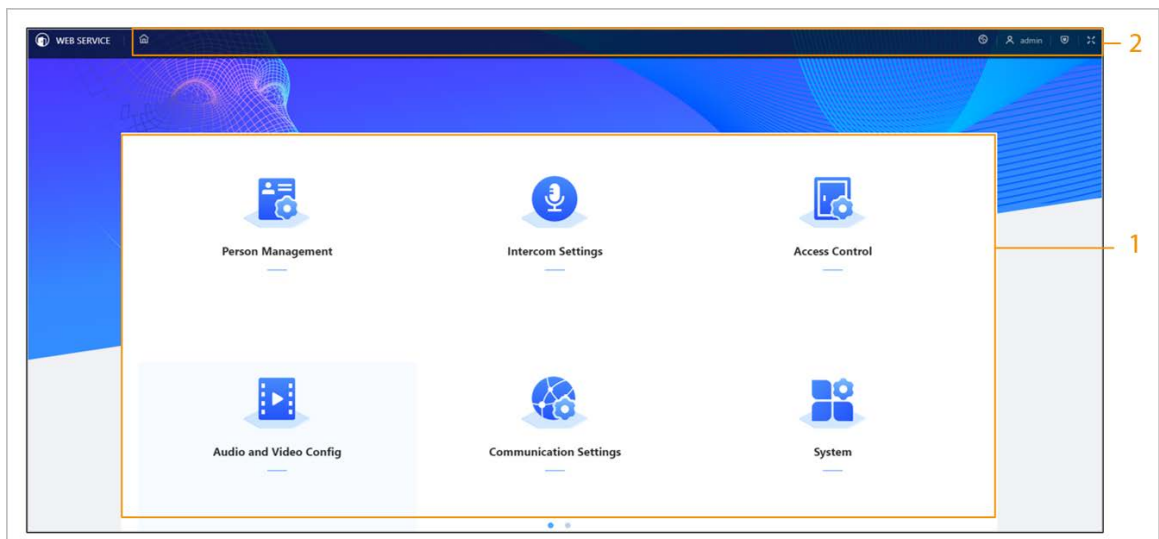


Table 3-1 Home page description

No.	Description
1	Main menu.
2	<ul style="list-style-type: none"> • : Enter the home page. • : Display in full screen. • : Enter the Security page. • : Log out or restart the device. • : Select a language on the device.

3.5 Adding Users

Procedure

Step 1 On the Home page, select **Person Management**, and then click **Add**.

Step 2 Configure user information.

Figure 3-3 Add users

The screenshot shows a 'Add' user interface with the following fields and values:

- * User ID:** 001
- Name:** Tom
- * Permission:** User
- Validity Period:** 2037-12-31 23:59:59
- * User Type:** General User
- * Times Used:** Unlimited
- * Period:** 255-Default
- * Holiday Plan:** 255-Default

Verification Mode: 255-Default


Verification Options:





- > Face: Not Added
- > Password: Not Added
- > Card: Not Added


Buttons: Add, Add More, Cancel

Table 3-2 Parameters description

Parameter	Description
User ID	The User ID. is like employee ID, which can be numbers, letters, and their combinations, and the maximum length of the No. is 32 characters.
Name	The name can have up to 30 characters (including numbers, symbols, and letters).
Permission	<ul style="list-style-type: none"> • User: Users only have door access or time attendance permissions. • Admin: Administrators can configure the Access Controller besides door access and attendance permissions.
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.

Parameter	Description
User Type	<ul style="list-style-type: none"> • 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 Access Controller, but they do not have door permissions. • VIP User: When VIP unlock the door, service personnel will receive a notice. • 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 runs out, they cannot unlock the door.
Period	People can unlock the door or take attendance during the defined period.
Holiday Plan	People can unlock the door or take attendance during the defined period.
Face	<p>Click Upload to upload a face image. Each person can only add up to 2 face images. You can view or delete the face image after you upload it.</p>  <p>The face image is jpg and must be less than 100KB.</p>

Parameter	Description
Card	<ul style="list-style-type: none"> ● Enter the card number manually. <ol style="list-style-type: none"> 1. Click Add. 2. Enter the card number, and then click Add. ● Read the number automatically through a card reader. <ol style="list-style-type: none"> 1. Make sure that the card reader is connected to your computer. 2. 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. 3. Click Add. <p>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 access controller.</p> <p>You can enable the Duress Card function. An alarm will be triggered if a duress card is used to unlock the door.</p> <ul style="list-style-type: none"> ● : Set duress card. ● : Change card number. <p> One user can only set one duress card.</p>
Password	<p>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. A duress alarm will be triggered when a duress password is used to unlock the door.</p>
FP	<p>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.</p> <p></p> <ul style="list-style-type: none"> ● 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. ● Fingerprint function is available if the Access Controller supports connecting a fingerprint module.
Department	<p>Add users to a department. If a department schedule is</p>

Parameter	Description
Schedule Mode	<p>assigned to the person, they will follow the established department schedule. For how to create department, see "2.9.1 Configuring Departments".</p> <ul style="list-style-type: none"> • Department Schedule: Assign department schedule to the user. For details, see "2.9.4 Configuring Work Schedules". • Personal Schedule: Assign personal schedule to the user. For details, see "2.9.4 Configuring Work Schedules". <p></p> <ul style="list-style-type: none"> ◇ This function is only available on select models. ◇ If you set the schedule mode to department schedule here, the personal schedule you have configured for the user in Attendance > Schedule Config > Personal Schedule is invalid.

Step 3 Click **OK**.

Related Operations

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



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

- Clear: Clear all users.

3.6 Configuring Intercom

The Access Controller can function as a door station to realize video intercom.



Intercom function is only available on select models.

3.6.1 Using the Device as the SIP Server

3.6.1.1 Configuring SIP Server

When the Access Controller functions as the SIP server, it can connect up to 500 access control devices and VTHs.

Procedure

Step 1 Select **Intercom Settings > SIP Server**.

Step 2 Turn on **SIP Server**.

Figure 3-4 Use the Access Controller as the SIP server

SIP Server

Server Type Device Name ▾

IP Address 192.168.1.111

Port 5080

Username 8001

Password ●●●●●●●●●●●●●●●●

SIP Domain VDP

SIP Server Username

SIP Server Password

Apply Refresh Default

Step 3 Click **Apply**.

3.6.1.2 Configuring Local Parameters

When the Device functions as the SIP server, configure the parameters of the Device.

Procedure

Step 1 Select **Intercom Settings > Local Device Config**.

Step 2 Configure the parameters.

Figure 3-5 Basic parameter

Table 3-3 Basic parameters description

Parameter	Description
Device Type	Select Door Station .
No	Cannot be set.
Group Call	When you turn on the group call function, the door station calls the main VTH and the extensions at the same time. The setup is effective after the door station restarts.
Management Center	The default call number of the management center is 888888+VTS No. For the VTS No, go to the Project Setting > General of the management center.

Step 3 Click **Apply**.

3.6.1.3 Adding the VTO

When the Access Controller functions as the SIP Servers, you need to add VTOs to the SIP server to make sure they can call each other.

Procedure

Step 1 On the webpage of the Access Controller, select **Intercom Settings > Device Setting**.

Step 2 Click **Add**, and then configure the VTO.

Figure 3-6 Add VTO

Table 3-4 Add VTO configuration

Parameter	Description
Device Type	Select VTO .
No.	Enter the VTO No. For the VTO No, go to the Device screen of VTO.
Registration Password	Keep it default.
Building No.	Cannot be configured.
Unit No.	
IP Address	The IP address of the added VTO.
Username	The username and password that are used to log in to the webpage of the added VTO.
Password	

Step 3 Click **OK**.

3.6.1.4 Adding the VTH

When the Device functions as the SIP Server, you can add all VTHs in the same unit to the SIP server

to make sure they can call each other.

Background Information



- When there are main VTH and extension, you need to turn on the group call function first and then add main VTH and extension on the **VTH Management** page. For how to turn on the group call function, refer to "3.6.1.2 Configuring Local Parameters".
- Extension cannot be added when the main VTHs are not added.

Procedure

Step 1 On the home page, select **Intercom Settings > Device Setting**.

Step 2 Add the VTH.

- Add one by one.
 1. Click **Add**.
 2. Configure parameters, and then click **OK**.

Figure 3-7 Add one by one

Add [X]

Device Type: VTH

Add Mode: Add One by One

First Name: Please enter

Last Name: Please enter

Alias: Please enter

* Room No.: Please enter

Registration Mode: Public

* Registration Password:

OK Cancel

Table 3-5 Room information

Parameter	Description
First Name	Enter the name of the VTH to help you differentiate VTHs.
Last Name	
Alias	
Room No.	<p>Enter the room number of the VTH.</p> <ul style="list-style-type: none"> • The room number consists of 1-5 digits, and must conform to the configured room number on the VTH. • When there are main VTH and extensions, the room number of main VTH ends with -0 and the room number of extension ends with -1, -2 or -3. For example, the main VTH is 101-0, and the room number of the extension is 101-1, 101-2... • If the group call function is not turned on, room number in the format of 9901-xx cannot be set.
Room No.	<p>Enter the room number of the VTH.</p> <ul style="list-style-type: none"> • The room number consists of 1-5 digits, and must conform to the configured room number on the VTH. • When there are main VTH and extensions, the room number of main VTH ends with -0 and the room number of extension ends with -1, -2 or -3. For example, the main VTH is 101-0, and the room number of the extension is 101-1, 101-2... • If the group call function is not turned on, room number in the format of 9901-xx cannot be set.
Registration Mode	Keep them as defaults.
Registration Password	

- Add in batches.
 1. Click **Add in Batches**.
 2. Configure the parameters.
 3. Click **Add**.

Figure 3-8 Batch add

Table 3-6 Add in batches

Parameter	Description
Floors in Unit	The number of floors of the building, which ranges from 1 to 99.
Rooms on Each Floor	The number of rooms on each floor, which ranges from 1 to 99.
First Room No. on 1st Floor	The first room on the first floor.
First Room No. on 2nd Floor	The first room No on the 2nd floor = The first digit of the first room No. on the 1st floor plus 1. For example, if the first room No. on the first floor is 101, the first room No. on the 2nd floor must be 201.

3.6.1.5 Adding the VTS

When the Device functions as the SIP Server, you can add VTSs to the SIP server to make sure they can call each other.

Procedure

- Step 1 On the Homepage, select **Intercom Settings > Device Setting**.
- Step 2 Click **Add**, and then set parameters.

Figure 3-9 VTS management

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

- Device Type:** A dropdown menu with "VTS" selected.
- * VTS No.:** A text input field with the placeholder text "Please enter".
- * IP Address:** A dotted IP address input field.
- * Registration Password:** A password input field with six dots and a visibility toggle icon.

At the bottom right of the dialog are two buttons: "OK" (blue) and "Cancel" (white).

Step 3 Click **OK**.

3.6.2 Using VTO as the SIP server

3.6.2.1 Configuring SIP Server

Use another VTO as the SIP server.

Procedure

Step 1 Select **Intercom Settings > SIP Server**.

Step 2 Select **Device** from the **Server Type**.



Do not enable SIP server.

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

Figure 3-10 Use VTO as the SIP server

Table 3-8 SIP server configuration

Parameter	Description
IP Address	IP address of the VTO.
Port	5060 by default when VTO works as SIP server.
Username	Leave them as default.
Password	
SIP Domain	VDP.
SIP Server Username	The login username and password of the SIP server.
SIP Server Password	

Step 4 Click **Apply**.

3.6.2.2 Configuring Local Parameters

Configure the parameters of the Device when you use another VTO as the SIP server.


Procedure

Step 1 Select **Intercom Settings > Local Device Config**.

Step 2 Configure the parameters.

Figure 3-11 Configure the parameters

Table 3-9 Parameters description

Parameter	Description
Device Type	Select Door Station .
No.	<p>The number of the VTO.</p> <p></p> <ul style="list-style-type: none"> The number must have 4 digits. The first 2 digits must be 80, and the last 2 digits start from 01. For example, 8001. If multiple VTOs exist in one unit, the VTO No. cannot be repeated.
Management Center	The call number for the management center is 888888. Keep it as default.

Step 3 Click **Apply**.

3.6.3 Using the Platform as the SIP server

3.6.3.1 Configuring SIP Server

The management platform is used as the SIP server.

Procedure

Step 1 Select **Intercom Settings > Private SIP Server**.

Step 2 Select **Private SIP Server** from the **Server Type**.




Do not enable SIP Server.

Figure 3-12 Use the management platform as the SIP server

SIP Server	<input type="checkbox"/>	
Server Type	Private SIP Server	
IP Address	192.168.1.1	
Port	5080	Alternate IP
Username	8001	Alternate Server Usern...
Password	Alternate Server Passw...
SIP Domain	VDP	Alternate VTS IP
SIP Server Username		Alternate Server
SIP Server Password		<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>		

Table 3-10 SIP server configuration

Parameter	Description
IP Address	IP address of the platform.
Port	5080 by default when the platform works as SIP server.
Username	Leave them as default.
Password	
SIP Domain	Leave it as default.
SIP Server Username	The login username and password of the platform.
SIP Server Password	
Alternate IP	<p>The alternate server will be used as the SIP server when the platform does not respond.</p>  <ul style="list-style-type: none"> • If you turn on the Alternate Server function, you will set the Access Controller as the alternate server. • If you want another VTO to function as the alternate server, you need to enter the IP address, username, password of the VTO. Do not enable Alternate Server in this case. • We recommend you set the main VTO as the alternate server.
Alternate Server Username	Used to log in to the alternate server.
Alternate Server Password	

Parameter	Description
Alternate VTS IP	Enter the IP address of the alternate VTS. When the management platform does not respond, the alternate VTS will be activated to make sure VTO, VTH and VTS can each other.

Step 3 Click **Apply**.

3.6.3.2 Configuring Local Parameters

Configure the parameters of the Access Controller when the platform is used as the SIP server.

Procedure

Step 1 Select **Intercom Settings > Local Device Config**.

Step 2 Configure the parameters.

Figure 3-13 Basic parameter

The screenshot shows a configuration form with the following fields and values:

- Device Type: Door Station (dropdown menu)
- Building No.: 001 (text input with a checked checkbox to its right)
- Unit No.: 01 (text input with a checked checkbox to its right)
- No.: 8001 (text input)
- Management ...: 888888 (text input)

At the bottom of the form are three buttons: **Apply** (blue), **Refresh** (white), and **Default** (white).

Table 3-11 Parameters description

Parameter	Description
Device Type	Select fence station or door station based on its installation site.
Building No.	Select the checkbox and then enter the number of the building where the unit door station is installed.
Unit No.	Select the checkbox and then enter the number of the unit where the unit door station is installed.
No.	<ul style="list-style-type: none"> The number must have 4 digits. The first 2 digits must be 80, and the last 2 digits start from 01. For example, 8001. If multiple VTOs exist in one unit, the VTO No. cannot be repeated.
Management Center	The default phone number is 888888 when the VTO calls the VTS. Keep it as default.

Step 3 Click **Apply**.

After settings, the username in **Intercom > SIP** page is automatically refreshed. Make sure the user name is same to the call number when you add the device to the management

platform.

3.7 Configuring Access Control

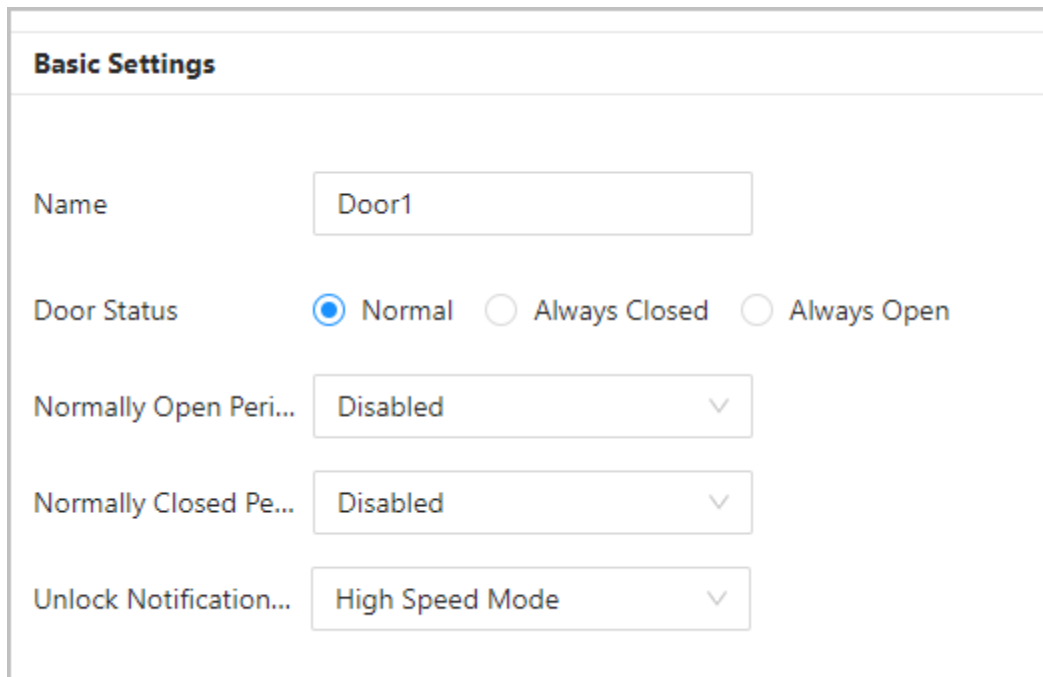
3.7.1 Configuring Basic Parameters

Procedure

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

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

Figure 3-14 Basic parameters



The screenshot shows a web interface titled "Basic Settings". It contains the following configuration options:

- Name:** A text input field containing "Door1".
- Door Status:** Three radio button options: "Normal" (selected), "Always Closed", and "Always Open".
- Normally Open Peri...:** A dropdown menu currently showing "Disabled".
- Normally Closed Pe...:** A dropdown menu currently showing "Disabled".
- Unlock Notification...:** A dropdown menu currently showing "High Speed Mode".

Table 3-12 Basic parameters description

Parameter	Description
Name	The name of the door.
Door Status	Set the door status. <ul style="list-style-type: none">• Normal: The door will be unlocked and locked according to your settings.• Always 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	

Parameter	Description
Unlock Notification	<p>Displays the notification on the screen when a person verifying their identity on the Access Controller.</p> <ul style="list-style-type: none"> • High Speed Mode: The system prompts Successfully verified or Not authorized on the screen. • Simple Mode: Displays user ID, name and verification time after access granted; displays Not authorized and authorization time after access denied. • Standard: Displays user's registered face image, user ID, name and verification time after access granted; displays Not authorized and verification time after access denied. • Contrast Mode: Displays the captured face image and a registered face image of a user, user ID, name and authorization time after access granted; displays Not authorized and authorization time after access denied.

Step 3 Click **Apply**.

3.7.2 Configuring Unlock Methods

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

Procedure

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

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

- Combination unlock
 1. Select **Combination Unlock** from the **Unlock Mode** list.
 2. Select **Or** or **And**.
 - ◇ Or: Use one of the selected 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 3-15 Unlock Settings

Unlock Settings

Unlock Method

Combination Meth... Or And

Unlock Method (Mul... Card Fingerprint Face Password

Door Unlocked Dur... (0.2-600)

Unlock Timeout (1-9999)

Remote Verification

Table 3-13 Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	Unlock methods might differ depending on the models of product.
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through. It ranges from 0.2 s to 600 seconds.
Unlock Timeout	When the door detector and the unlock timeout alarm are enabled, a timeout alarm will be triggered if the door remains unlocked longer than the defined unlock time.
Remote Verification	Open the door remotely.

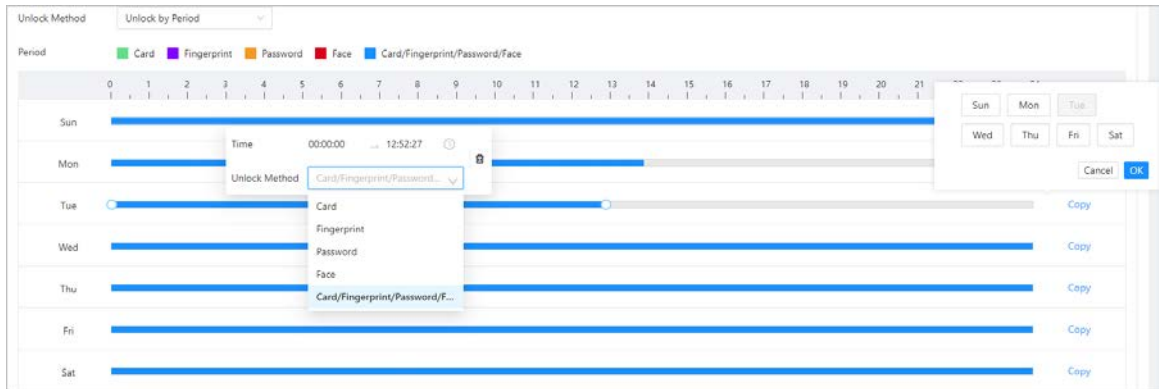
- Unlock by period
 1. In the **Unlock Mode** list, select **Unlock by Period**.
 2. Drag the slider to adjust time period for each day.



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 3-16 Unlock by period



- Unlock by multiple users.
 1. In the **Unlock Mode** list, select **Unlock by multiple users**.
 2. Click **Add** to add groups.
 3. Select unlock method, valid No. and user list.
 - ◇ 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 No.
 - ◇ 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 No.



- ◇ You can add up to 4 groups.
- ◇ The valid No. indicates the number of people in each group who need to verify their identities on the Access Controller before the door unlocks. For example, if the valid No. is set to 3 for a group, any 3 people in the group need to verify their identities to unlock the door.

Step 3 Click **Apply**.

3.7.3 Configuring Alarms

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

Procedure


- Step 1** Select **Access Control > Alarm > Alarm**.
- Step 2** Configure alarm parameters.

Figure 3-17 Alarm

Duress Alarm
 Anti-passback
 Door Detector Normally Closed Normally Open
 Intrusion Alarm
 Local Alarm Li... (0-1800)
 Unlock Timeo...
 Local Alarm Li... (0-1800)
 Excessive Use ...
 Local Alarm Li... (0-1800)

Table 3-14 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	<p>Users need to verify their identities both for entry and exit; otherwise an alarm will be triggered. It helps prevent 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 the system will grant another entry.</p> <ul style="list-style-type: none"> • 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. <p> If the Access Controller can only connect one lock, verifying on the Access Controller means entry direction, and verifying on the external card reader means exit direction by default. You can modify the setting on the management platform.</p>
Door Detector	<p>With the door detector wired to your device, an alarm can be triggered when doors are opened or closed abnormally. The door detector includes 2 types, including NC detector and NO detector.</p> <ul style="list-style-type: none"> • Normally Closed: The sensor is in a shorted position when the door or window is closed. • Normally Open: An open circuit is created when the window or door is actually closed.
Intrusion Alarm	<p>When door detector and intrusion alarm is enabled, an intrusion alarm will be triggered if the door is opened abnormally.</p>
Unlock Timeout Alarm	<p>When the door detector and the unlock timeout alarm are enabled, a timeout alarm will be triggered if the door remains unlocked longer than the defined unlock time.</p>
Excessive Use Alarm	<p>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 15 seconds by default.</p>
Local Alarm Linkage	<p>The duration of the alarm. 15 s by default.</p>

Step 3 Click **Apply**.

3.7.4 Configuring Global Alarm linkages (Optional)

You can configure global alarm linkages.

Procedure

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

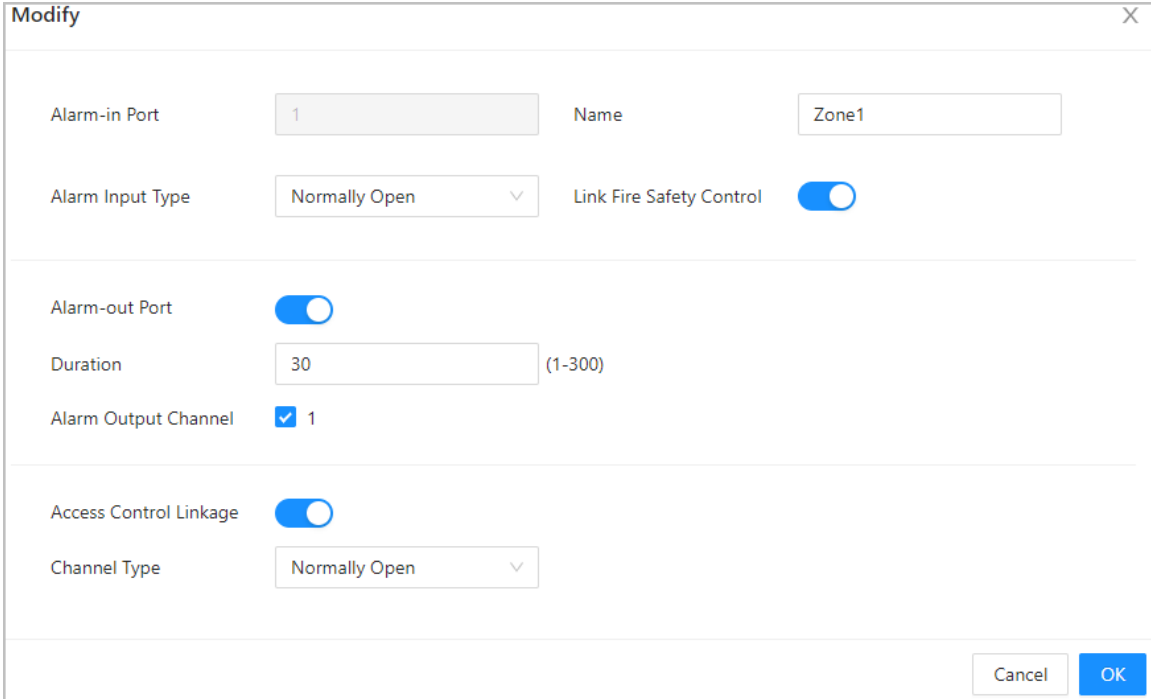


- If the Access Controller is added a management platform, the alarm settings will be synchronized to the platform.
- This function is only available on models that have alarm input and alarm output ports.
- The number of alarm input and output ports differs depending on models of the product.

Step 2 Configure the alarm input.

1. Click .

Figure 3-18 Global alarm linkage



2. Configure name for the alarm.
3. 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.
4. Click **Enable** to turn on the door linkage function.



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

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

Step 3 Turn on the alarm output function and then enter the alarm duration.

Step 4 Turn on the e access control linkage, and then select a door status.

- Normally Closed: The door automatically locks when an alarm is triggered.
- Normally Open: The door automatically unlocks when an alarm is triggered.

Figure 3-19 Alarm output

The 'Modify' dialog box contains the following configuration options:

- Alarm-in Port: 1
- Name: Zone1
- Alarm Input Type: Normally Open
- Link Fire Safety Control:
- Alarm-out Port:
- Duration: 30 (1-300)
- Alarm Output Channel: 1
- Access Control Linkage:
- Channel Type: Normally Open

Buttons: Cancel, OK

3.7.5 Configuring Face Detection

Configure face detection parameters.

Procedure

- Step 1** Log in to the webpage.
- Step 2** Select **Access Control > Face Detect**.

Figure 3-20 Face detection parameters

The configuration page includes a live video feed on the left and a list of parameters on the right:

- Recognition** (selected tab)
- Face Recognition Threshold: 85
- Max Face Recognition Angl...: 30
- Anti-spoofing Level: General, Close, High, Extremely High
- Valid Face Interval (sec): 3 (1-60)
- Invalid Face Interval (sec): 3 (1-60)
- Eye Spacing (Min. pixels of ...): 50 (0-500)
- Mask mode: No Authorization without ...
- Face Mask Threshold: 75
- Beautifier:
- Enable Helmet Detection:
- Multi-face Recognition:
- Night Mode:



Target Filter section:

- Min Size: 256 * 256
- Buttons: Draw Target, Clear
- Detection Area: Clear
- Buttons: Apply, Refresh, Default

- Step 3** Configure the parameters.

Table 3-15 Description of face parameters

Name	Description
Face Recognition Threshold	Adjust the accuracy level of face recognition. Higher threshold means higher accuracy and lower false recognition rate.
Max Face Recognition Angle Deviation	Set the largest angle that a face can be posed in for face detection. The larger the value, the larger the range for the face angle. If the angle a face is positioned in is not within the defined range, it might not be detected properly.
Anti-spoofing Level	This prevents people from being able to use photos, videos, mask and other substitutes to gain unauthorized access.
Valid Face Interval (sec)	When a person has their face successfully verified too many times, Access Controller prompts verification successful within the defined time interval.
Invalid Face Interval (sec)	When a person fails to have their face verified too many times, Access Controller prompts verification failed within the defined time interval.
Eye Spacing (Min. pixels of eye spacing)	A certain number of pixels are required between the eyes, called pupillary distance, for recognition to be successful. The default number is 45 pixels. This number changes based on the size of the face and the distance between the face and the lens. If an adult is 1.5 meters away from the lens, the pupillary distance is usually 50 - 70 px.
Mask Mode	<ul style="list-style-type: none"> ● Mask mode: <ul style="list-style-type: none"> ◇ Do Not Detect: Mask is not detected during face recognition. ◇ Mask Reminder: Mask is detected during face recognition. If the person is not wearing a mask, the system will remind them to wear a mask, but they will still be allowed access. ◇ No Authorization without Wearing Face Mask: Mask is detected during face recognition. If a person is not wearing a mask, the system will remind them to wear masks, and access will be denied. ● Mask Recognition Threshold: The higher the threshold, the more accurate face recognition will be when a person is wearing a mask, and there will be a lower false recognition rate.
Beautifier	Beautify captured face images.
Enable Helmet Detection	Detects safety hats. The door will not unlock if the a person does not wear a helmet.

Name	Description
Multi-face Recognition	<p>Detects 4 to 6 face images at a time. Combination unlock cannot be used with this, and the door will be unlocked when one of the people are successfully verified.</p> <p></p> <p>The number of face images which are supported might differ depending on the model of the product.</p>
Night Mode	<p>In dark environment, the standby screen displays white background image to improve the brightness when verifying face or QR code.</p>
Illuminator Mode	<ul style="list-style-type: none"> • Auto: The illuminator is turned on in low-light conditions. • Disable: The illuminator is turned off all the time. <p></p> <p>This function is only available on select models.</p>

Step 4 Configure the exposure parameters.

Figure 3-21 Exposure parameters

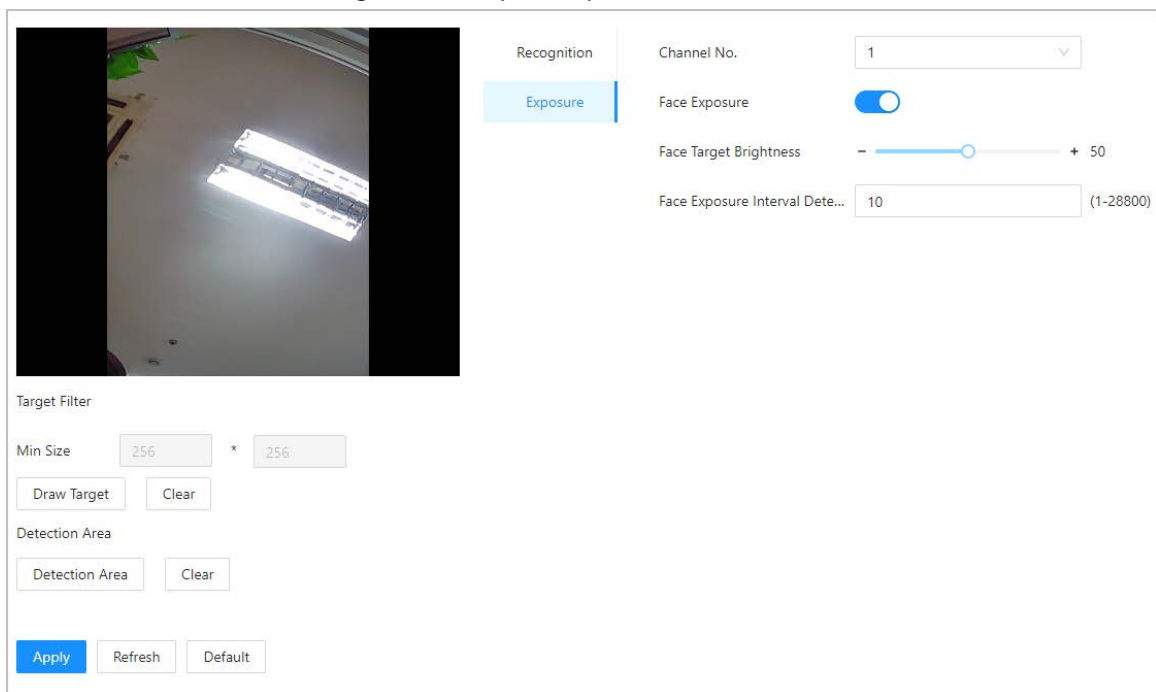


Table 3-16 Exposure parameters description

Parameter	Description
Channel No.	<ul style="list-style-type: none"> • Channel 1 is the white light mode. • Channel 2 is the infrared light mode.
Face Exposure	<p>After the face exposure function is enabled, the face will be exposed at the defined brightness to detect the face image clearly.</p>
Face Exposure Interval Detection	<p>The face will be exposed only once in a defined interval.</p>

Step 5 Draw the face detection area.

- 1) Click **Detect Region**.
- 2) Right-click to draw the detection area, and then release the left button of the mouse to

complete drawing.

The face in the defined area will be detected.

Step 6 Draw the target size.

1) Click **Draw target**

2) Draw the face recognition box to define the minimum size of detected face.

Only when the size of the face is larger than the defined size, the face can be detected by the Access Controller.

Step 7 Draw the detection area.

Step 8 Click **OK**.

3.7.6 Configuring Card Settings

Background Information



This function is only available on select models.

Procedure

Step 1 Log in to the webpage.

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

Step 3 Configure the card parameters.

Figure 3-22 Card parameters

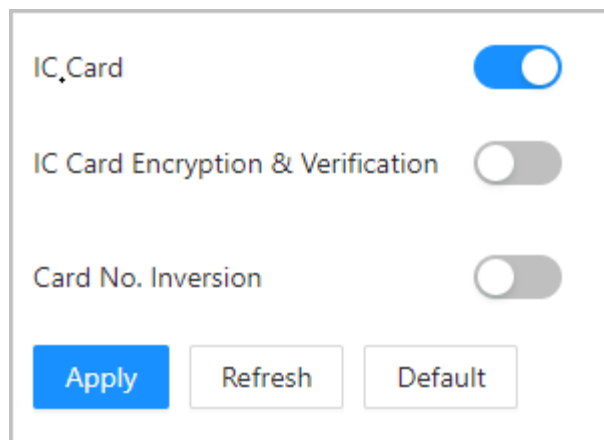



Table 3-17 Card parameters description

Parameter	Description
IC Card	The IC card can be read when this function is enabled.  This function is only available on select models.
IC Card Encryption & Verification	The encrypted card can be read when this function is enabled.
Card No. Inversion	When the Access Controller connects to a third-party device through the Wiegand input, and the card number read by the Access Controller is in the reverse order from the actual card number. In this case, you can turn on this function.

3.7.7 Configuring QR Code

Procedure

Step 1 On the webpage, select **Access Control > Card Settings**.

Figure 3-23 QR code

Table 3-18 QRR code parameters

Parameters	Description
Enable QR Code Exposure	The QR code will be exposed at the defined brightness, and the QR code can be detected and read clearly.
QR Code Brightness	
QR Code Exposure Interval (sec)	The QR code will be exposed only once during the defined interval.
QR Code Pass-through	The QR code read by a third-party platform.
QR Code Validity Period (min)	After the QR code is generated, and the validity of your QR codes will last for a defined time before it expires.

3.7.8 Configuring Schedules

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

3.7.8.1 Configuring Time Periods

You can configure up to 128 groups (from No.0 through No.127) of time periods. 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 > Weekly Plan.**

Step 3 Click **Add.**

Figure 3-24 Configure time periods

Step 4 Drag the time slider to configure time for each day.

Step 5 (Optional) Click **Copy** to copy the configuration to the rest of days.

Step 6 Click **OK.**

3.7.8.2 Configuring Holiday Plans

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 in the defined time in 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.**

Step 4 Select a number for the holiday group, and then enter a name for the group.

Figure 3-25 Add a holiday group

Edit [X]

No.

Holiday Group Name

Holiday Group Config

No.	Holiday Name	Start Time	End Time	Operation
1	national holiday	2023-10-01	2023-10-07	

Step 5 Click **Add**, and then add a holiday in a holiday group.

Step 6 Click **OK**.

Figure 3-26 Add a holiday to a holiday group

Edit [X]

Holiday Name

* Period →

Step 7 Click **Plan Management**, and then click **Add**.

Step 8 Select a number for the holiday plan, and then enter a name for it.

Step 9 Select a holiday group, and then drag the slider to configure time for each day. Supports adding up to 4 time sections on a day.

Figure 3-27 Add holiday plan

Add [X]

No.

Holiday Plan Name

Holiday Group No.

Time Plan

0 1 2 3 4 5 6 7 8 9 10 11 12

Time →

Step 10 Click **OK**.

3.7.9 Configuring Expansion Modules

For Access Controller that supports connecting expansion modules, configure the type of the module that the Access Controller supports.

Background Information





- The type the expansion module might differ depending on models of the Access Controller.
- The settings of expansion module remain after restoring the Access Controller to factory defaults.

Procedure

- Step 1 On the webpage, select **Access Control > Expansion Module**.
- Step 2 Select the type of the module that the Access Controller supports.
- Step 3 Click **Apply**.

The configurations become effective after Access Controller is restarted.

-  is displayed on the right corner of the Access Controller is the setting is effective.
-  is displayed on the right corner of the Access Controller, which means the type of the expansion module you configured does not match the actual expansion module that is connected to Access Controller.
- If **None** is selected and no expansion module is connected to the Access Controller, the expansion module icon will not be displayed.

3.7.10 Configuring Port Functions

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

Background Information

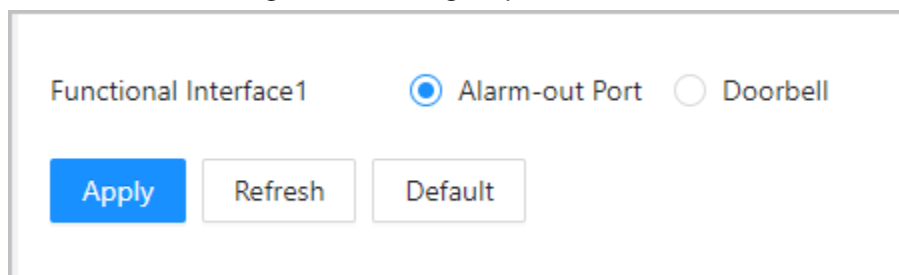


- This function is only available on select models.
- Ports might differ depending on the models of the product.

Procedure

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

Figure 3-28 Configure ports



3.8 Configuring Audio and Video

3.8.1 Configuring Video

On the home page, select **Video Setting**, and then configure the video stream, status, image and exposure.

Background Information

- Video Standard: Select **NTSC**.
- Channel Id: Channel 1 is for configurations of visible light image. Channel 2 is for configurations of infrared light image.
- Default: Restore to defaults settings.
- Capture: Take a snapshot of the current image.



PAL video standard is 25 fps and the NTSC video standard is 30 fps.

3.8.1.1 Configuring Channel 1

Procedure

- Step 1 Select **Audio and Video Config > Video**.
- Step 2 Select **1** from the **Channel No.** list.
- Step 3 Configure the bit rate.

Figure 3-29 Date rate

Channel No. 1

Bit Rate

Main Stream

Status

Resolution 720P

Exposure

Frame Rate (FPS) 30

Image

Bit Rate 2Mbps

Sub Stream


Resolution VGA

Frame Rate (FPS) 30

Bit Rate 1024Kbps

Default Snapshot

Table 3-19 Bit rate description

Parameter		Description
Main Format	Resolution	 When the Access Controller functions as the a VTO and connects the VTH, the acquired stream limit of VTH is 720p. When resolution is changed to 1080p, the call and monitor function might be affected.
	Frame Rate (FPS)	The number of frames (or images) per second.
	Bit rate	The amount of data transmitted over an internet connection in a given amount of time. Select a proper bandwidth based on your network speed.
Sub Stream	Resolution	The sub-stream supports D1, VGA and QVGA.
	Frame Rate (FPS)	The number of frames (or images) per second.
	Bit Rate	It indicates the amount of data transmitted over an internet connection in a given amount of time.

Step 4 Configure the status.

Figure 3-30 Status

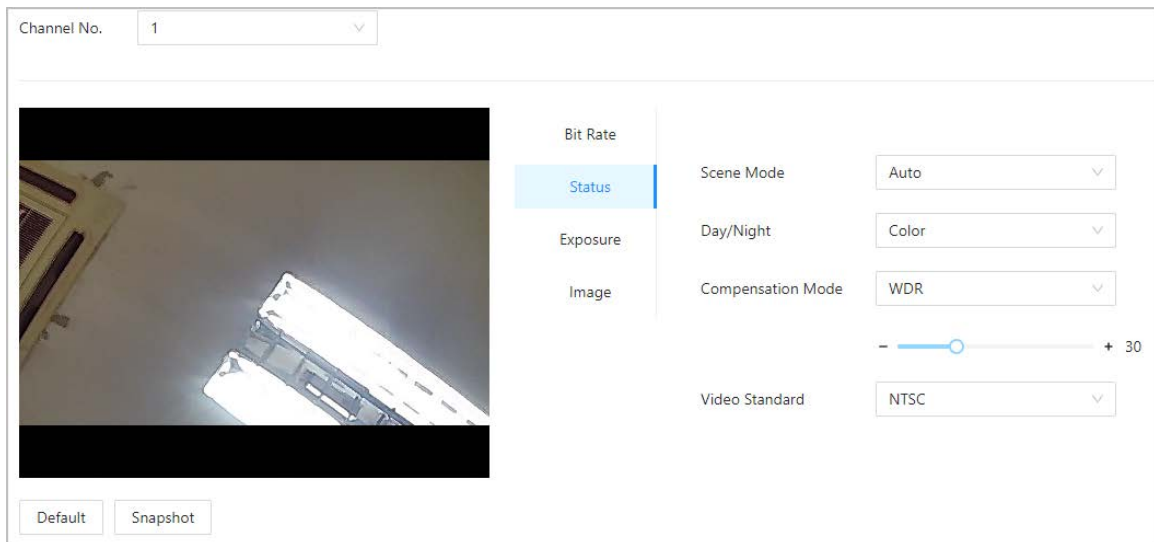


Table 3-20 Image description

Parameter	Description
Scene Mode	<p>The image hue is different in different scene mode.</p> <ul style="list-style-type: none"> ● Close: Scene mode function is turned off. ● Auto: The system automatically adjusts the scene mode based on the photographic sensitivity. ● Sunny: In this mode, image hue will be reduced. ● Night: In this mode, image hue will be increased.

Parameter	Description
Day/Night	<p>Day/Night mode affects light compensation in different situations.</p> <ul style="list-style-type: none"> ● Auto: The system automatically adjusts the day/night mode based on the photographic sensitivity. ● Colorful: In this mode, images are colorful. ● Black and white: In this mode, images are in black and white.
Compensation Mode	<ul style="list-style-type: none"> ● Disable: Compensation is turned off. ● BLC: Backlight compensation automatically brings more light to darker areas of an image when bright light shining from behind obscures it. ● WDR: The system dims bright areas and compensates for dark areas to create a balance to improve the overall image quality. ● HLC: Highlight compensation (HLC) is a technology used in CCTV/IP security cameras to deal with images that are exposed to lights like headlights or spotlights. The image sensor of the camera detects strong lights in the video and reduces exposure in these spots to enhance the overall quality of the image.

Step 5 Configure the exposure parameters.

Figure 3-31 Exposure

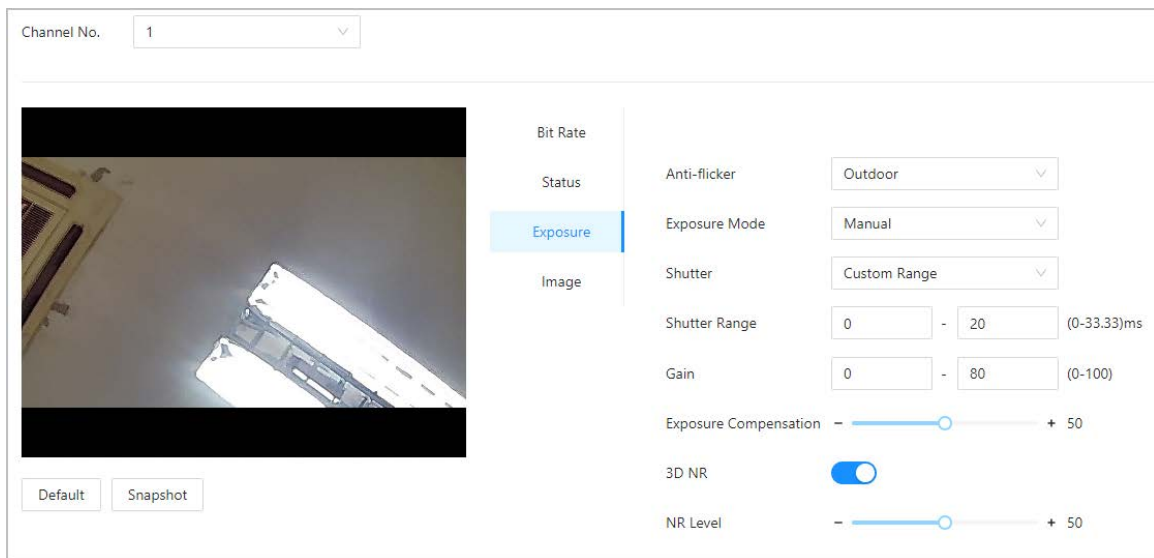



Table 3-21 Exposure parameter description

Parameter	Description
Anti-flicker	<p>Set anti-flicker to reduce flicker and decrease or reduce uneven colors or exposure.</p> <ul style="list-style-type: none"> ● 50Hz: When the mains electricity is 50 Hz, the exposure is automatically adjusted based on brightness of the surroundings to prevent the appearance of horizontal lines. ● 60Hz: When the mains electricity is 60 Hz, the exposure is automatically adjusted based on brightness of the surroundings to reduce the appearance of horizontal lines. ● Outdoor: When Outdoor is selected, the exposure mode can be switched.

Parameter	Description
Exposure Mode	<p>You can set the exposure to adjust image brightness.</p> <ul style="list-style-type: none"> • Auto: The Access Controller automatically adjusts the brightness of images based the surroundings. • Shutter Priority: The Access Controller adjust the image brightness according to the set range of the shutter. If the image is not bright enough but the shutter value has reached its upper or lower limit, the Access Controller will automatically adjust the gain value for ideal brightness level. • Manual: You can manually adjust the gain and shutter value to adjust image brightness. <p></p> <ul style="list-style-type: none"> ◇ When you select Outdoor from the Anti-flicker list, you can select Shutter Priority as the exposure mode. ◇ Exposure mode might differ depending on models of Access Controller.
Shutter	Shutter is a component that allows light to pass for a determined period. The higher the shutter speed, the shorter the exposure time, and the darker the image.
Gain	When the gain value range is set, video quality will be improved.
Exposure Compensation	The video will be brighter by adjusting exposure compensation value.
3D NR	When 3D Noise Reduction (RD) is turned on, video noise can be reduced to ensure higher definition of videos.
Grade	

Step 6 Configure the image.

Figure 3-32 Image

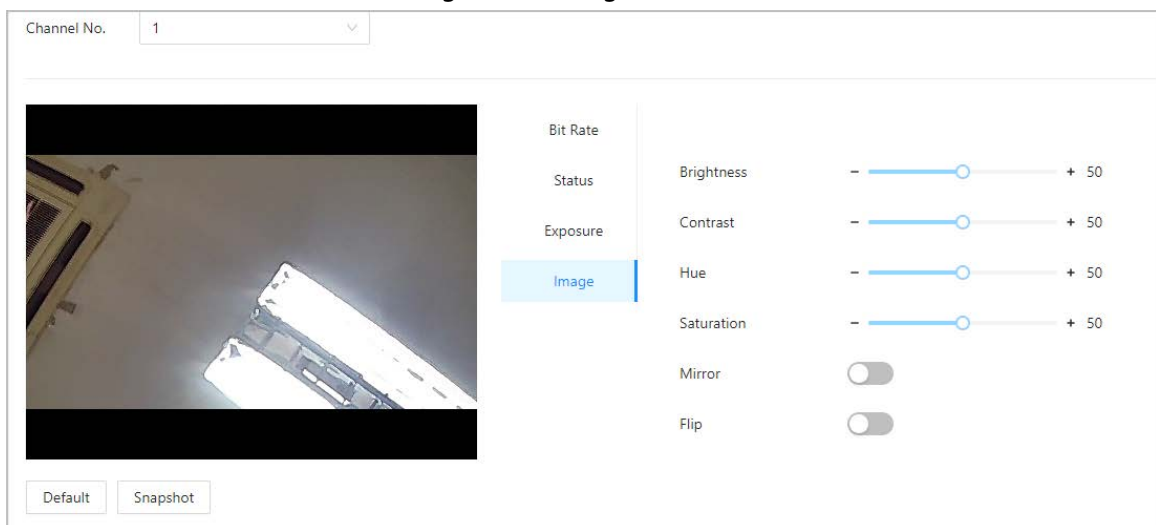



Table 3-22 Image description

Parameter	Description
Brightness	The brightness of the image. Higher value means brighter images.
Contrast	Contrast is the difference in the luminance or color that makes an object distinguishable. The larger the contrast value is, the greater the color contrast will be.
Hue	Refers to the strength or saturation of a color. It describes the color intensity, or how pure it is.
Saturation	Color saturation indicates the intensity of color in an image. As the saturation increases, the appear stronger, for example being more red or more blue.  The saturation value does not change image brightness.
Mirror	When the function is turned on, images will be displayed with the left and right side reversed.
Flip	When this function is turned on, images can be flipped over.

3.8.1.2 Configuring Channel 2

Procedure

- Step 1** Select **Audio and Video Config > Video**.
- Step 2** Select **2** from the **Channel No.** list.
- Step 3** Select 2 from the **Channel No.**.
- Step 4** Configure the video status.



We recommend you turn on the WDR function when the face is in back-lighting.

Figure 3-33 Configure status

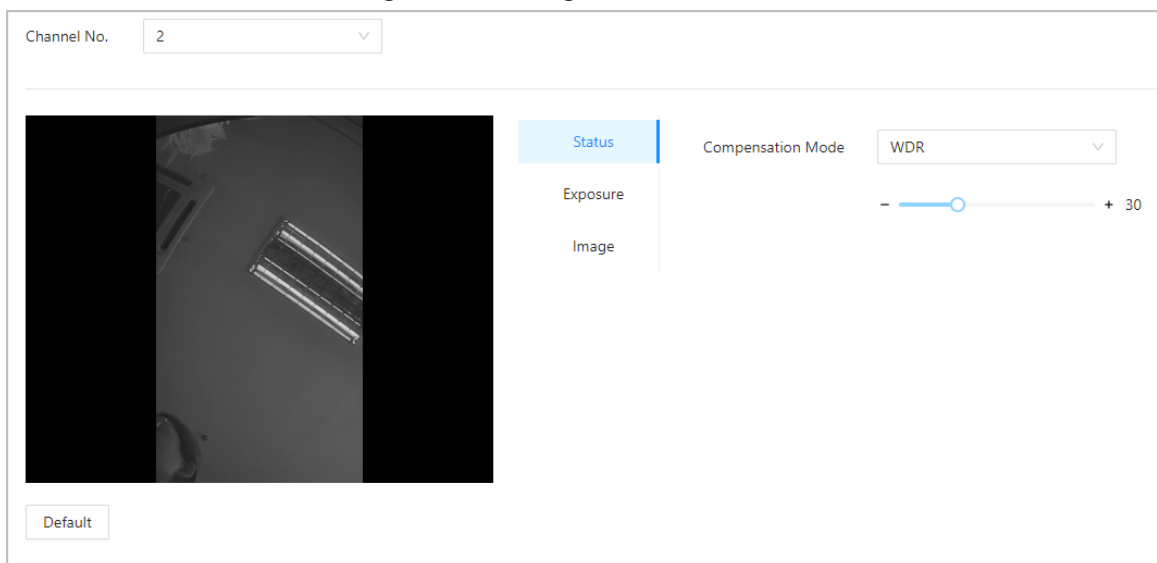


Table 3-23 Status description

Parameter	Description
Compensation Mode	<ul style="list-style-type: none"> ● Disable: Compensation is turned off. ● BLC: Backlight compensation automatically brings more light to darker areas of an image when bright light shining from behind obscures it. ● WDR: The system dims bright areas and compensates for dark areas to create a balance to improve the overall image quality. ● HLC: Highlight compensation (HLC) is a technology used in CCTV/IP security cameras to deal with images that are exposed to lights like headlights or spotlights. The image sensor of the camera detects strong lights in the video and reduces exposure in these spots to enhance the overall quality of the image.

Step 5 Configure the exposure parameters.

Figure 3-34 Exposure parameter

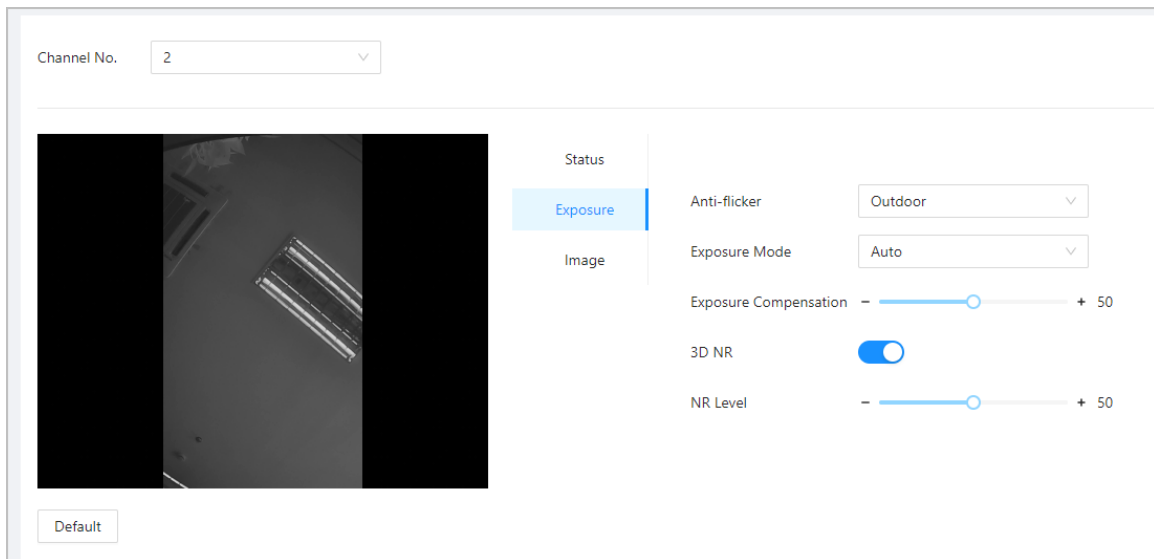



Table 3-24 Exposure parameter description

Parameter	Description
Anti-flicker	<p>Set anti-flicker to reduce flicker and decrease or reduce uneven colors or exposure.</p> <ul style="list-style-type: none"> ● 50Hz: When the mains electricity is 50 Hz, the exposure is automatically adjusted based on brightness of the surroundings to prevent the appearance of horizontal lines. ● 60Hz: When the mains electricity is 60 Hz, the exposure is automatically adjusted based on brightness of the surroundings to reduce the appearance of horizontal lines. ● Outdoor: When Outdoor is selected, the exposure mode can be switched.

Parameter	Description
Exposure Mode	<p>You can set the exposure to adjust image brightness.</p> <ul style="list-style-type: none"> • Auto: The Access Controller automatically adjusts the brightness of images based the surroundings. • Shutter Priority: The Access Controller adjust the image brightness according to the set range of the shutter. If the image is not bright enough but the shutter value has reached its upper or lower limit, the Access Controller will automatically adjust the gain value for ideal brightness level. • Manual: You can manually adjust the gain and shutter value to adjust image brightness. <p></p> <ul style="list-style-type: none"> ◇ When you select Outdoor from the Anti-flicker list, you can select Shutter Priority as the exposure mode. ◇ Exposure mode might differ depending on models of Access Controller.
Exposure Compensation	The video will be brighter by adjusting exposure compensation value.
3D NR	When 3D Noise Reduction (RD) is turned on, video noise can be reduced to ensure higher definition of videos.
NR Level	

Step 6 Configure the image parameters.

Figure 3-35 Image parameters

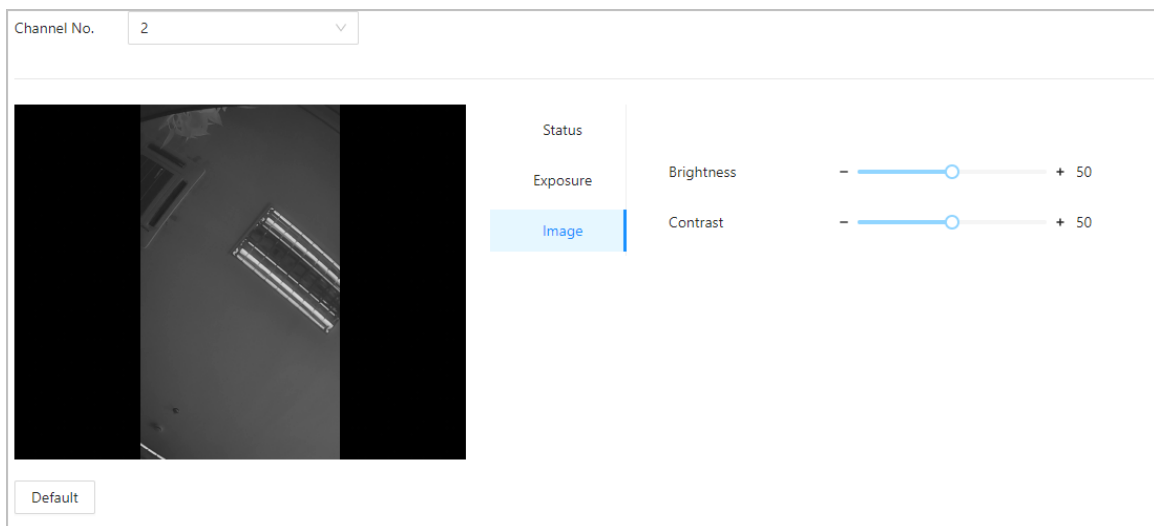


Table 3-25 Image description

Parameter	Description
Brightness	The brightness of the image. Higher value means brighter images.
Contrast	Contrast is the difference in the luminance or color that makes an object distinguishable. The larger the contrast value is, the greater the color contrast will be.

3.8.2 Configuring Audio Prompts

Set audio prompts during identity verification.

Procedure

- Step 1 Select **Audio and Video Config > Audio**.
- Step 2 Configure the audio parameters.

Figure 3-36 Configure audio parameters

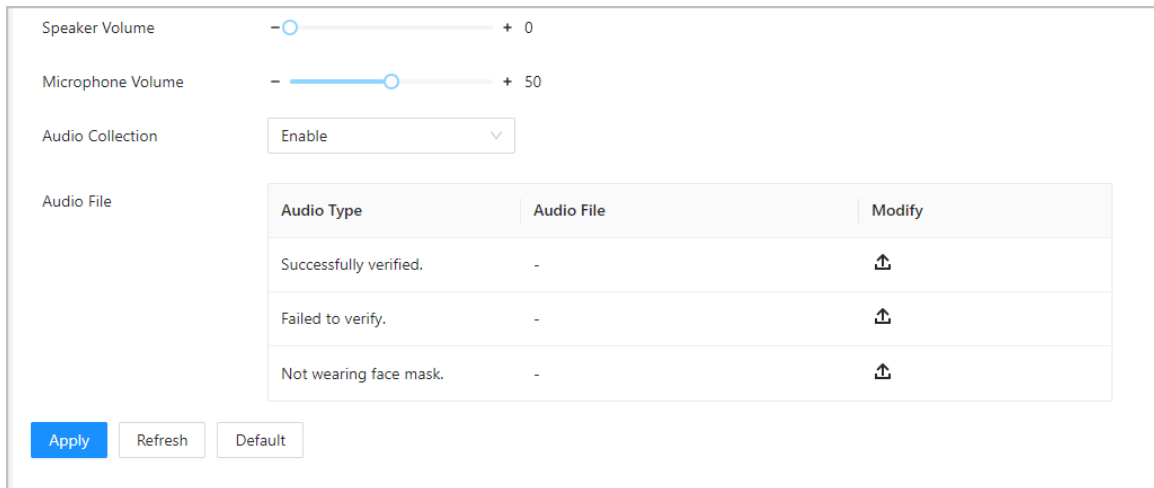



Table 3-26 Parameters description

Parameters	Description
Speaker	Drag the slider to adjust the volume of the speaker.
Microphone Volume	Drag the slider to adjust the volume of the microphone.
Audio Collection	The audio will not be recorded during video talk when this function is not enabled.
Audio File	Click Upload audio files to the platform.

- Step 3 Click  to upload audio files to platform for each audio type.



The format is MP3 and the size is less than 20KB.

- Step 4 Click **Apply**.

3.8.3 Configuring Motion Detection

When there are moving objects detected and reaches the set threshold, the screen will be awoken.

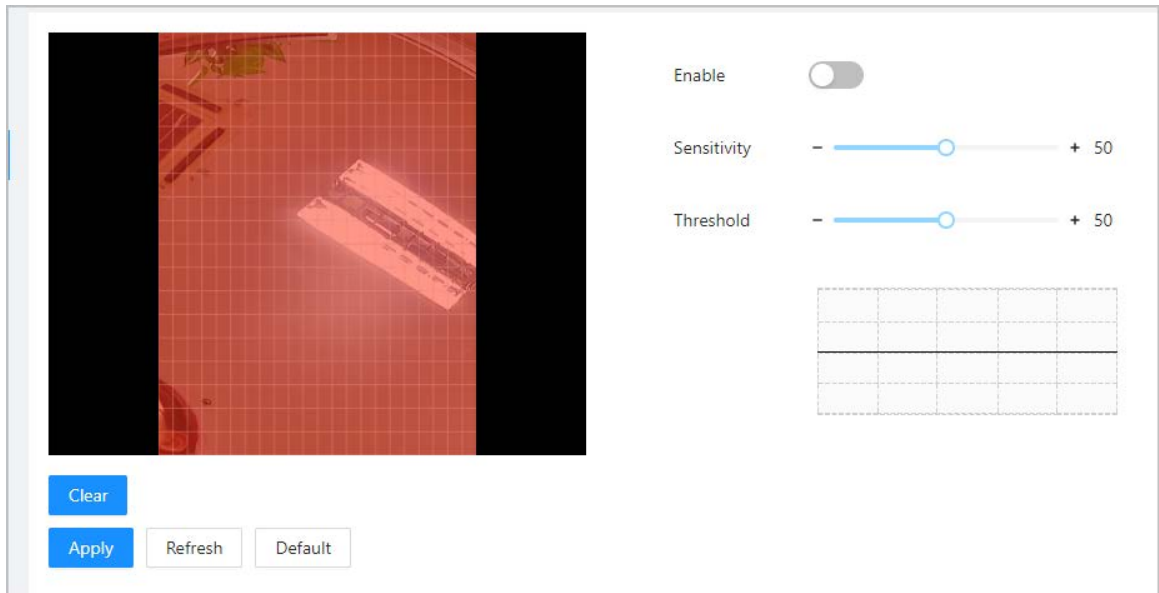
Procedure

- Step 1 Select **Audio and Video Config > Motion Detection Settings**.
- Step 2 Enable the motion detection function.
- Step 3 Press and hold the left mouse button, and then draw a detection area in the red area.



- The motion detection area is displayed in red.
- To remove the existing the motion detection area, click **Clear**.
- The motion detection area you draw will be a non-motion detection area if you draw in the default motion detection area.

Figure 3-37 Motion detection area



Step 4 Configure the parameters.

- Sensitivity: The sensible to the surroundings. Higher sensitivity means easier to trigger alarms.
- Threshold: The percentage of the moving object area in the motion detection area. Higher threshold means easier to trigger alarms.

Step 5 Click **Apply**.

The motion detection is triggered when the red lines are displayed; the green lines are displayed when it is not triggered.

3.8.4 Configuring Local Coding

Set the view area in the video talk and preview.

Background Information



- This function is only available on select models.
- This function is enabled by default when it works with a VTH. The preview might be not accessible when this function is disabled.

Procedure

Step 1 Log in to the webpage.

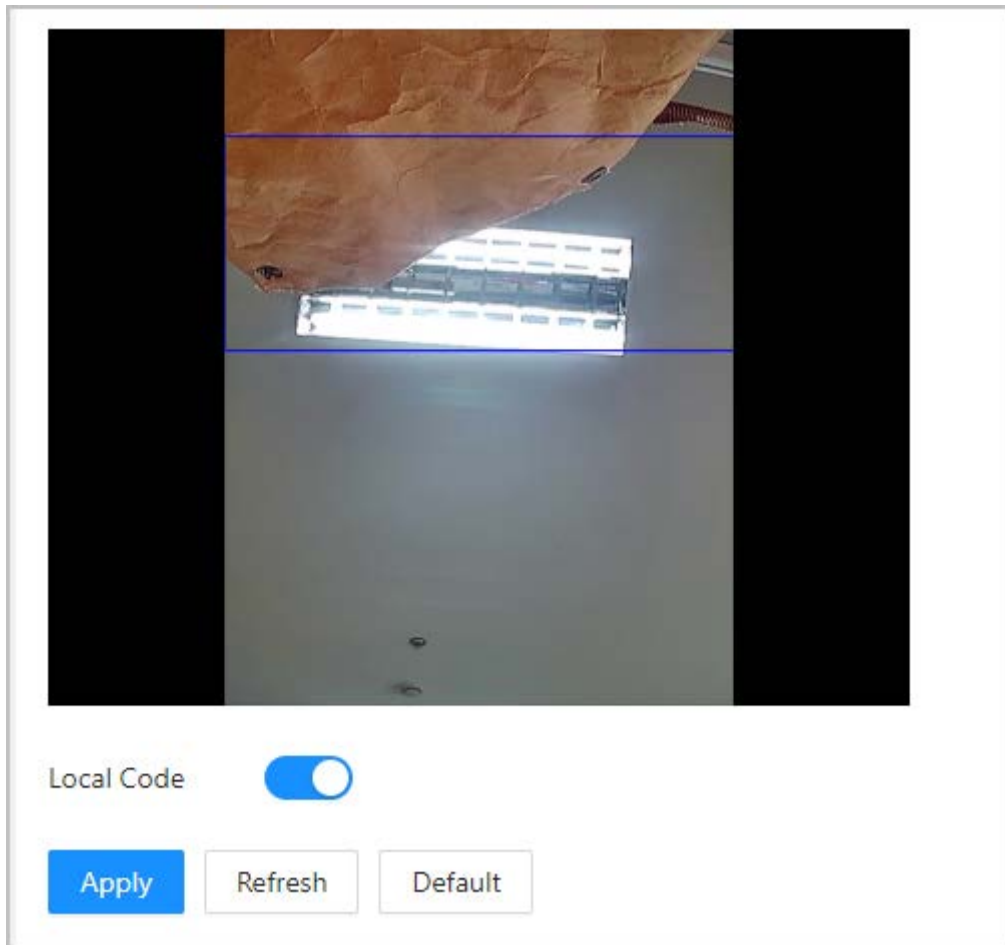
Step 2 Select **Audio and Video Config > Motion Detection Settings**.

Step 3 Select **Enable** to turn on the function.

Step 4 Drag the box to a designated position.

The box indicates the preview area during the video talk.

Figure 3-38 Local coding



Step 5 Click **Apply**.

3.9 Configuring Network

3.9.1 Configuring TCP/IP

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

Procedure

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


Step 2 Configure the parameters.

Figure 3-39 TCP/IP

The screenshot displays a TCP/IP configuration window. At the top, the 'NIC' is set to 'NIC 1'. The 'Mode' is set to 'Static' (selected with a blue radio button), with 'DHCP' also available. The 'MAC Address' is shown as '90 : 02 : [blurred] : 51 : 9f'. The 'IP Version' is set to 'IPv4'. The 'IP Address' is '172 . [blurred] . [blurred] . 103'. The 'Subnet Mask' is '255 . [blurred] . [blurred] . 0'. The 'Default Gateway' is '172 . [blurred] . [blurred] . 1'. The 'Preferred DNS' is '8 . [blurred] . [blurred] . 8'. The 'Alternate DNS' is '8 . [blurred] . [blurred] . 4'. The 'MTU' is set to '1500'. The 'Transmission Mode' is set to 'Multicast' (selected with a blue radio button), with 'Unicast' also available. At the bottom, there are three buttons: 'Apply' (blue), 'Refresh', and 'Default'.

Table 3-27 Description of TCP/IP

Parameter	Description
Mode	<ul style="list-style-type: none"> • Static: Manually enter IP address, subnet mask, and gateway. • DHCP: It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Access Controller will automatically be assigned with IP address, subnet mask, and gateway.
MAC Address	MAC address of the Access Controller.
IP Version	IPv4 or IPv6.
IP Address	If you set the mode to Static , configure the IP address, subnet mask and gateway.
Subnet Mask	

Parameter	Description
Default Gateway	 <ul style="list-style-type: none"> IPv6 address is represented in hexadecimal. IPv6 version do not require subnet masks to be set. 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	<p>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:</p> <ul style="list-style-type: none"> 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.
Transmission Mode	<ul style="list-style-type: none"> Multicast: Ideal for video talk. Unicast: Ideal for group call.

Step 3 Click **OK**.

3.9.2 Configuring Wi-Fi

Procedure

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

Step 2 Turn on Wi-Fi.
All available Wi-Fi are displayed.



Wi-Fi function is only available on select models.

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

3.9.3 Configuring Port

You can limit access to the Access Controller at the same time through webpage, desktop client and

mobile client.

Procedure

Step 1 Select **Communication Settings > Port**.

Step 2 Configure the ports.

Figure 3-40 Configure ports

Max Connection	1000	(1-1000)
TCP Port	37777	(1025-65534)
HTTP Port	80	
HTTPS Port	443	
RTSP Port	554	

Apply Refresh Default



Except for **Max Connection** and **RTSP Port**, you need to restart the Access Controller to make the configurations effective after you change other parameters.

Table 3-28 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 Access Controller at the same time.
TCP Port	Default value is 37777.
HTTP Port	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	Default value is 443.
RTSP Port	Default value is 554.

Step 3 Click **Apply**.

3.9.4 Configuring Basic Service

When you want to connect the Access Controller to a third-party platform, turn on the CGI and

ONVIF functions.

Procedure


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

Step 2 Configure the basic service.

Figure 3-41 Basic service

Table 3-29 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 . <ul style="list-style-type: none"> Security Mode (recommended): Does not support accessing the device through Digest, DES, and plaintext authentication methods, improving device security. Compatible Mode: Supports accessing the device through Digest, DES, and plaintext authentication methods, with reduced security.

Parameter	Description
Private Protocol	<p>The platform adds devices through TLSv1.1 protocol.</p>  <p>Security risks might present when TLSv1.1 is enabled. Please be advised.</p>

Step 3 Click **Apply**.

3.9.5 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, configuring port mapping or deploying server.

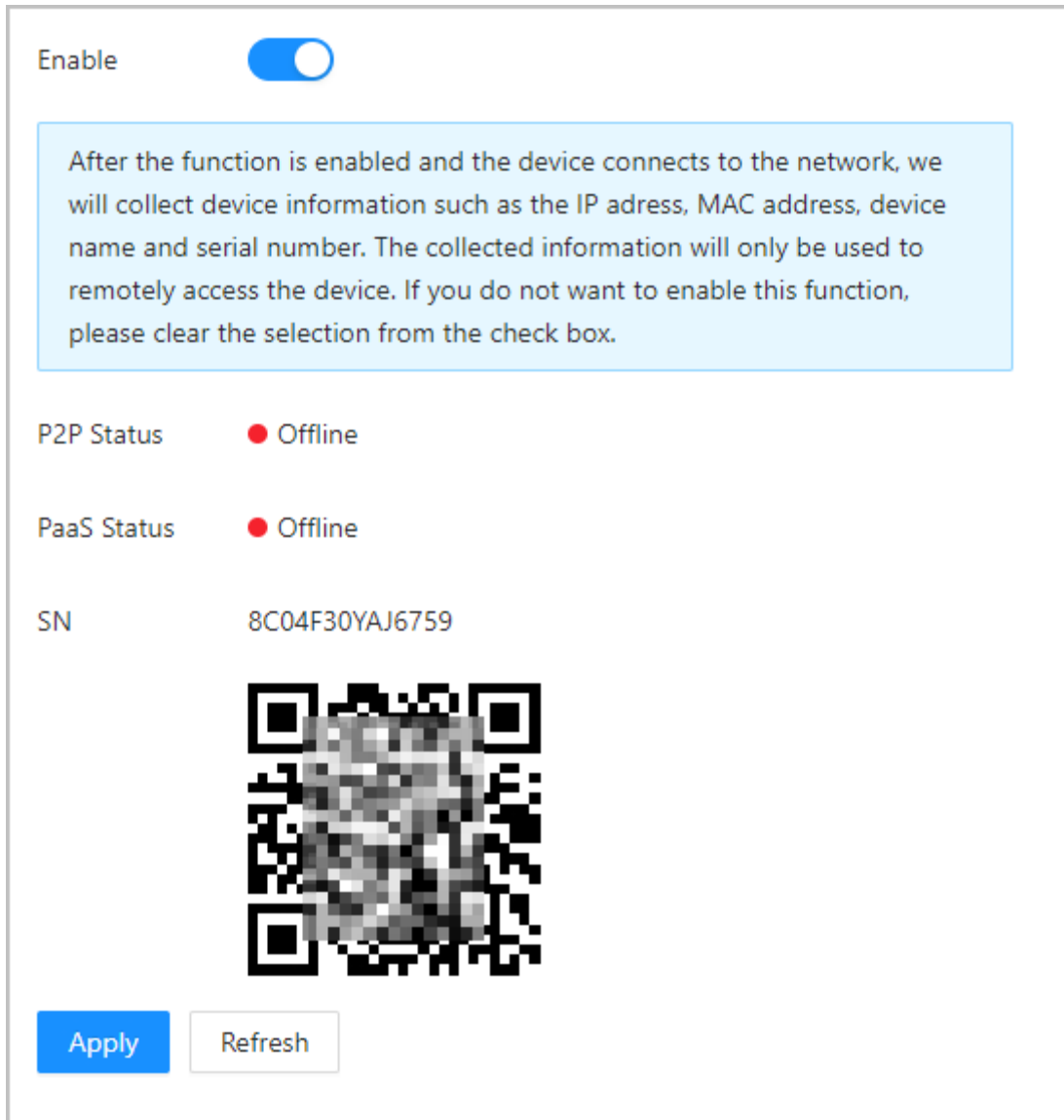
Procedure

Step 1 On the home page, select **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 3-42 Cloud service



Step 3 Click **Apply**.

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

3.9.6 Configuring Active Registration

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

Procedure

Step 1 On the home page, select **Network Setting > Auto Registration**.

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

Figure 3-43 Auto Registration

Table 3-30 Automatic registration description

Parameter	Description
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.

Step 3 Click **Apply**.

3.10 Configuring RS-485

Configure the RS-485 parameters if you connect an external device with the RS-485 port.

Procedure

Step 1 Select **Communication Settings > RS-485 Settings**.

Step 2 Configure the parameters.

Figure 3-44 Configure parameters

External Device	Turnstile
Baud Rate	9600
Data Bit	8
Stop Bit	1
Parity Code	None
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>	

Table 3-31 Configure the Wiegand format

Parameter	Description
External Device	<ul style="list-style-type: none"> ● Access Controller: Select Access Controller when the Access Controller functions as a card reader, and the Access Controller will send data to the Access Controller to control access. <p>Output Data type:</p> <ul style="list-style-type: none"> ◇ 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. ◇ No.: Outputs data based on the user ID. <ul style="list-style-type: none"> ● Card Reader: The Access Controller connects to a card reader. ● Reader (OSDP): The Access Controller is connected to a card reader based on OSDP protocol. ● Door Control Security Module: The door exit button, lock and fire linkage is not effective after the security module is enabled. ● Turnstile: When the Access Controller connects to a turnstile, and the access controller board of the turnstile connects to an external QR code module or card swiping module, the board will transmit the verification data to the turnstile.
Data Bit	The number of bits used to transmit the actual data in a serial communication. It represents the binary digits that carry the information being transmitted.

Parameter	Description
Stop Bit	A bit sent after the data and optional parity bits to indicate the end of a data transmission. It allows the receiver to prepare for the next byte of data and provides synchronization in the communication protocol.
Parity Code	An additional bit sent after the data bits to detect transmission errors. It helps verify the integrity of the transmitted data by ensuring a specific number of logical high or low bits.

Step 3 Click **Apply**.

3.11 Configuring Wiegand

Configure the RS-485 parameters if you connect an external device with the RS-485 port.

Procedure

Step 1 Select **Communication Settings > Wiegand**.

Step 2 Configure the parameters.

Figure 3-45 Configure parameters

Wiegand Wiegand Input Wiegand Output

Wiegand Output Type

Pulse Width (μs) (20-200)

Pulse Interval (μs) (200-5000)

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

Output Data Type Card Number No.

Apply Refresh Default

Table 3-32 Description of Wiegand output

Parameter	Description
Wiegand Output Type	Select a Wiegand format to read card numbers or ID numbers. <ul style="list-style-type: none"> • Wiegand26: Reads 3 bytes or 6 digits. • Wiegand34: Reads 4 bytes or 8 digits. • Wiegand66: Reads 8 bytes or 16 digits.

Parameter	Description
Pulse Width	Enter the pulse width and pulse interval of Wiegand output.
Pulse Interval	
Output Data Type	Select the type of output data. <ul style="list-style-type: none"> • No.: Outputs data based on user ID. The data format is hexadecimal or decimal. • Card Number: Outputs data based on user's first card number.

Step 3 Click **Apply**.

3.12 Configuring the System

3.12.1 User Management

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

3.12.1.1 Adding Administrators

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

Procedure

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

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



- The username cannot be the same with existing account. The username consists of up to 31 characters and only allows for numbers, letters, underscores, midlines, dots, or @.
- The password must consist of 8 to 32 non-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 3-46 Add administrators

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

- * Username**: A text input field.
- * Password**: A text input field with a password strength indicator below it.
- * Confirm Password**: A text input field.
- Remarks**: A text input field.

At the bottom right of the dialog are two buttons: a blue **OK** button and a white **Cancel** button.

Step 3 Click **OK**.



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

3.12.1.2 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 allows the compatibility from different manufactures. 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 3-47 Add ONVIF user

The 'Add' dialog box contains the following fields:

- * Username: Text input field
- * Password: Password input field with strength indicator (four bars)
- * Confirm Password: Password input field with strength indicator (four bars)
- * Group: Dropdown menu with a downward arrow

Buttons: OK (blue), Cancel (white)

Step 3 Click **OK**.

3.12.1.3 Resetting the Password

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

Procedure

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

Figure 3-48 Reset Password

The 'Password Reset' configuration page includes:

- Enable: (toggle switch)
- Info: 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**.

3.12.1.4 Viewing Online Users

You can view online users who currently log in to the webpage. On the home page, select **System >**


3.12.2 Configuring Time

Procedure

- Step 1 On the home page, select **System > Time**.
- Step 2 Configure the time of the Platform.

Figure 3-49 Date settings

Time and Time Zone



Date :
2023-05-30 Tuesday

Time :
16:18:35

Time Manually Set NTP

System Time

Time Format

Time Zone

DST

Enable

Type Date Week

Start Time

End Time

Table 3-34 Time settings description

Parameter	Description
Time	<ul style="list-style-type: none"> • Manual Set: Manually enter the time or you can click Sync Time to sync time with computer. • NTP: The Access Controller will automatically sync the time with the NTP server. <ul style="list-style-type: none"> ◇ Server: Enter the domain of the NTP server. ◇ Port: Enter the port of the NTP server. ◇ Interval: Enter its time with the synchronization interval.
Time format	Select the time format.
Time Zone	Enter the time zone.
DST	<ol style="list-style-type: none"> 1. (Optional) Enable DST. 2. Select Date or Week from the Type. 3. Configure the start time and end time of the DST.

Step 3 Click **Apply**.

3.12.3 Maintenance

Regularly restart the Access Controller during its idle time to improve its performance.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **System > Maintenance**.

Step 3 Set the time, and then click **Apply**.

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

3.12.4 Configuration Management

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

3.12.4.1 Exporting and Importing Configuration Files

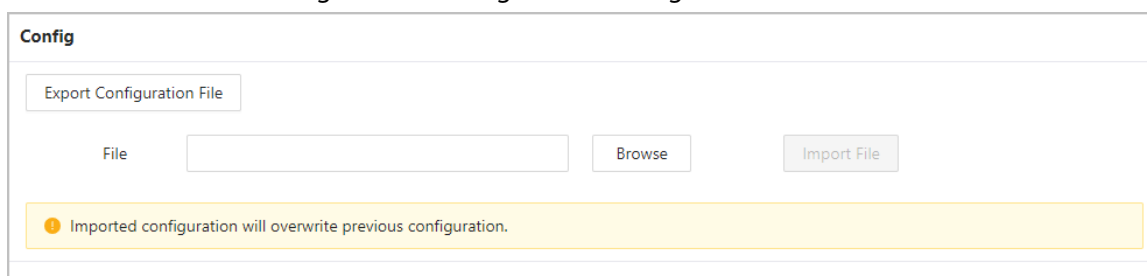
You can import and export the configuration file for the Access Controller. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **System > Config**.

Figure 3-50 Configuration management



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 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.

3.12.4.2 Restoring the Factory Default Settings

Procedure

- Step 1** Select **System > Config**.



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



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

3.12.5 Updating the System



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

3.12.5.1 File Update

Procedure

- Step 1 On the home page, select **System > 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 Access Controller will restart after the update finishes.

3.12.5.2 Online Update

Procedure

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

3.12.6 Viewing Version Information

On the webpage, select **System > Version**, and you can view version information of the Access Controller.

3.12.7 Viewing Data Capacity

On the webpage, select **System** > **Data Capacity**, view the data capacity of the Access Controller.

3.12.8 Viewing Legal Information

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

3.13 Personalization

Configure themes and add video or image resources to the Access Controller.

3.13.1 Adding Resources

Add images or videos to be displayed on the standby screen of the Access Controller.

Procedure

Step 1 On the home page, select **Personalization** > **Advertisement** > **Ad Resources**.

Step 2 Add videos or images.

Figure 3-51 Add videos or images


The screenshot displays a web interface for adding resources. It is divided into two main sections: 'Video' and 'Picture'.
The 'Video' section has a blue information bar stating 'Supports AVI,DAV,MP4. Video size must be less than 100M.' Below this is an 'Upload' button. A table lists the added video:

No.	Name	Operation
1	A...p.dav	[Delete icon]

The 'Picture' section has a blue information bar stating 'Supports PNG,JPG,BMP. Image size must be less than 2M.' Below this is a preview of a small image of a person's face and a dashed box with a '+' sign and the word 'Upload'.

- Add videos.
 1. Click **Upload**.
 2. Click **Browse**, select the video file, and then click **Next**.

The video is automatically uploaded to the platform after transcoding.



 - ◇ You can upload up to 5 video files.
 - ◇ Supports DAV, AVI, MP4. Video size must be less than 100 M.
 - ◇ Only supports latest version of FireFox and Chrome to upload video files.
- Add images.
 1. Click +.

2. Select image from the local and upload it.



Supports PNG, JPG, BMP. Image size must be less than 2 M.

Related Operations

Click  to delete uploaded images or videos.



Videos and images in use cannot be deleted.

3.13.2 Configuring Themes

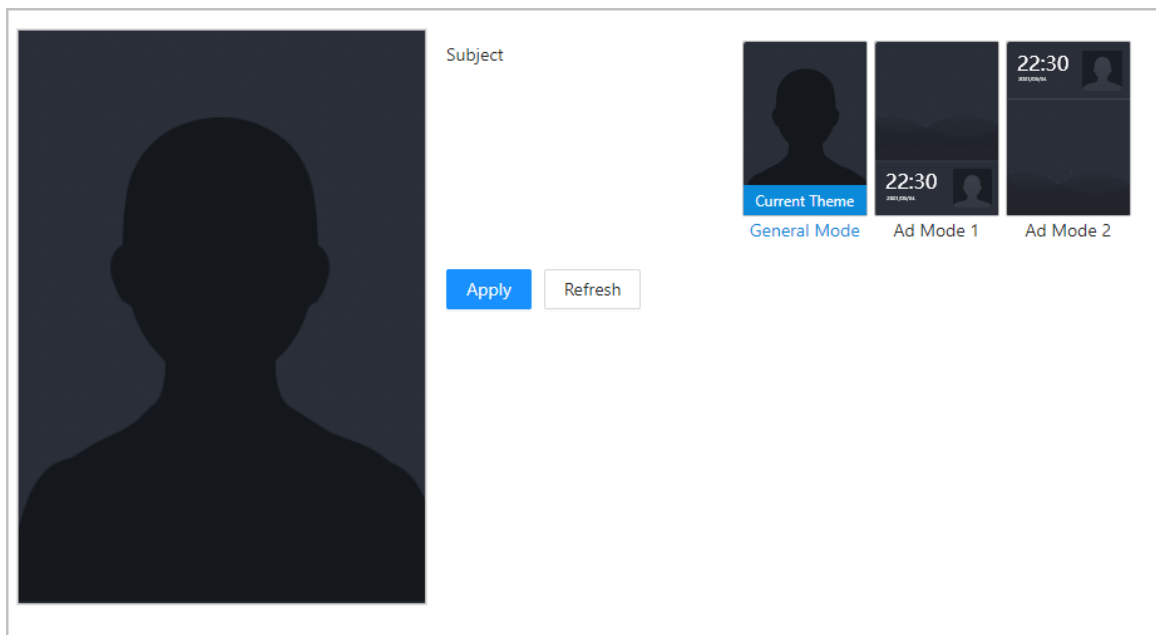
Procedure

Step 1 On the home page, select **Personalization** > **Advertisement** > **Subject**.

Step 2 Select the theme.

- General Theme: Displays the face image in full screen.
- Ad Mode 1: The upper area displays the advertisements, and the lower area displays the time and the face detection box.
- Ad Mode 2: The upper area displays the time and the face detection box, and the lower area displays the advertisements.

Figure 3-52 Theme

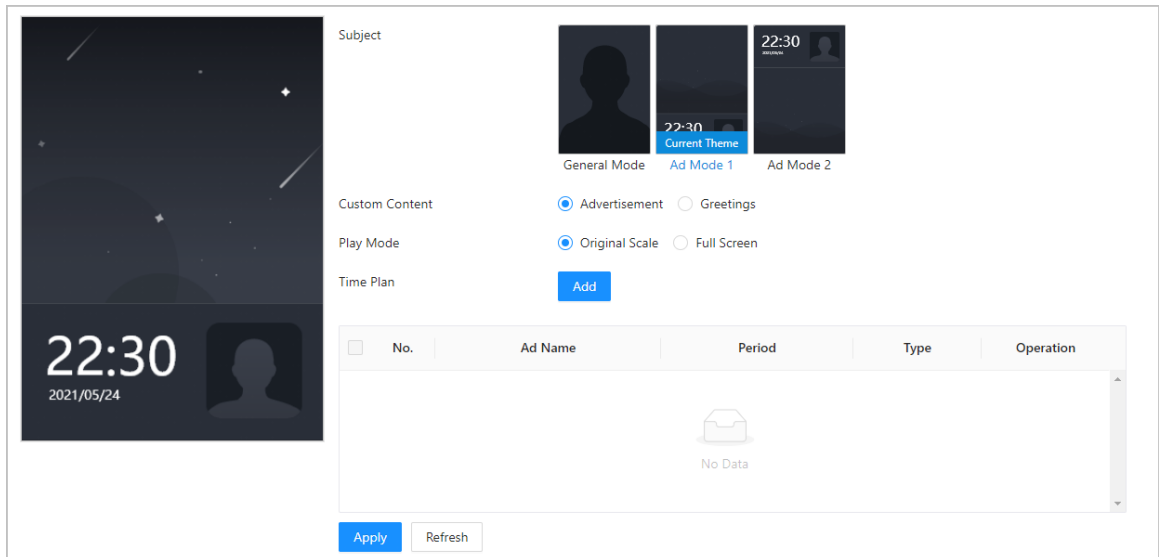


Step 3 Select the voice prompt for successful identity verification.

Step 4 Set advertisement display.

1. Select Ad mode 1 or Ad mode 2, and then select **Advertisement**.

Figure 3-53 Advertisement mode



2. Select the display mode.
 - Original Scale: Plays the image and video in the original size.
 - Full Screen: Plays the image and video in full screen.
3. Click **Add** to add time schedules.



You can add up to 10 schedules.
4. Enter the name of the advertisement.
5. Select the time section, file type and file.
6. Enter the duration, and then click **Apply**.

Set the duration for a single picture when pictures are played in a loop. The duration ranges from 1 s to 20 s and it is 5 s by default.

Figure 3-54 Add time schedules

Add ✕

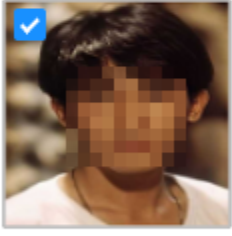
Ad Name

Period  - 

Type Picture Video

Duration sec

Ad Resources



- Step 5 Configure greetings.
1. Select **Greetings** from the **Custom Content**.
 2. Select the template.
 3. Enter the title and subtitle.

Figure 3-55 Greetings

The screenshot shows a configuration interface for greetings. On the left is a preview of a dark-themed greeting card with the text "Welcome Home" and "Good Night", a large digital clock showing "22:30", and the date "2021/05/24". On the right, there are several configuration sections:

- Subject:** Three preview cards are shown: "General Mode", "Ad Mode 1" (highlighted as "Current Theme"), and "Ad Mode 2".
- Custom Content:** Two radio buttons are present: "Advertisement" (unselected) and "Greetings" (selected).
- Template:** Three preview cards are shown: "Galaxy" (highlighted as "Current Template"), "Mist", and "Dream".
- Content:** A text area with the instruction "Please edit your content below." contains two input fields: "Title" with the value "Welcome Home" (12 / 30) and "Subtitle" with the value "Good Night" (10 / 60).

At the bottom of the configuration area, there are two buttons: "Apply" and "Refresh".

4. Click **Apply**.

3.13.3 Configuring the Shortcuts

Procedure


- Step 1 On the webpage of the Access Controller, select **Personalization > Shortcut Settings**.
- Step 2 Configure the shortcut parameters.


Figure 3-56 Shortcut Settings

The screenshot shows the 'Shortcut Settings' interface. It contains the following elements:

- Password:** A blue toggle switch is turned on.
- QR Code:** A blue toggle switch is turned on.
- Doorbell:** A blue toggle switch is turned on.
- Ringing:** A grey toggle switch is turned off.
- Alarm:** A grey toggle switch is turned off.
- Ringtone Config:** A dropdown menu showing 'Ringtone 1' with a downward arrow.
- Ringtone Time (sec):** A text input field containing '3', with '(1-30)' to its right.
- Call:** A blue toggle switch is turned on.
- Call Type:** A dropdown menu showing 'Call Room' with a downward arrow.
- Buttons:** Three buttons at the bottom: 'Apply' (blue), 'Refresh' (white), and 'Default' (white).

Table 3-35 1

Parameter	Description
Password	The icon of the password unlock method is displayed on the standby screen.
QR code	The QR code icon is displayed on standby screen. This function is not available for Access Controller with a standalone QR code module.
Doorbell	<p>After the doorbell function is turned on, doorbell icon is displayed on the standby screen.</p> <ul style="list-style-type: none"> • Ringing: Tap the ring bell icon on the standby screen, and the Access Controller rings. • Alarm: Turn on the alarm linkage function, and then doorbell rings. <p> This function is only available on select models.</p> <ul style="list-style-type: none"> • Ringtone Config: Select the ring bell. • Ringtone Times (sec): Set ring time (1-30 s). The default value is 3.
Call	The icon of call is displayed on the standby screen.

Parameter	Description
Call Type	<ul style="list-style-type: none"> • Call Room: Tap the call icon on the standby mode and enter the room number to make calls. • Call Management Center: Tap the call icon on the standby mode, and then call the management center. • Custom Call room: Enter the number of room, and then you can tap the call icon on the standby screen to call the pre-defined room number.  <p>Make sure the Access Controller was added to DMSS.</p>

3.14 Viewing Logs

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


3.14.1 System Logs

View and search for system logs.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **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 entering the password.
- Click  to view details of a log.

3.14.2 Admin Logs

Search for admin logs by using admin ID.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Log > Admin Log**.
- Step 3 Enter the admin ID, and then click **Search**.
Click **Export** to export admin logs.

3.14.3 Unlocking Logs

Search for unlock records and export them.

Procedure

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

3.14.4 Alarm Logs

View alarm logs.

Procedure

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

3.14.5 Call Logs

View call logs.

Procedure

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

3.14.6 USB Management

Export user information from/to USB.

Procedure

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



- Make sure that a USB is inserted to the Access Controller before you export data or update the system. To avoid failure, do not pull out the USB or perform any operation of the Access Controller during the process.
- You have to use a USB to export the information from an Access Controller to other devices. Face images are not allowed to be imported through USB.

- Step 3 Select a data type, and then click **USB Import** or **USB Export** to import or export the data.

3.15 Data Capacity

You can see how many users, cards and face images that the Access Controller can store. Log in to the webpage and select **Data Capacity**.

3.16 Security Settings(Optional)

3.16.1 Security Status

Scan the users, service, and security modules to check the security status of the Access Controller.

Background Information

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

Procedure

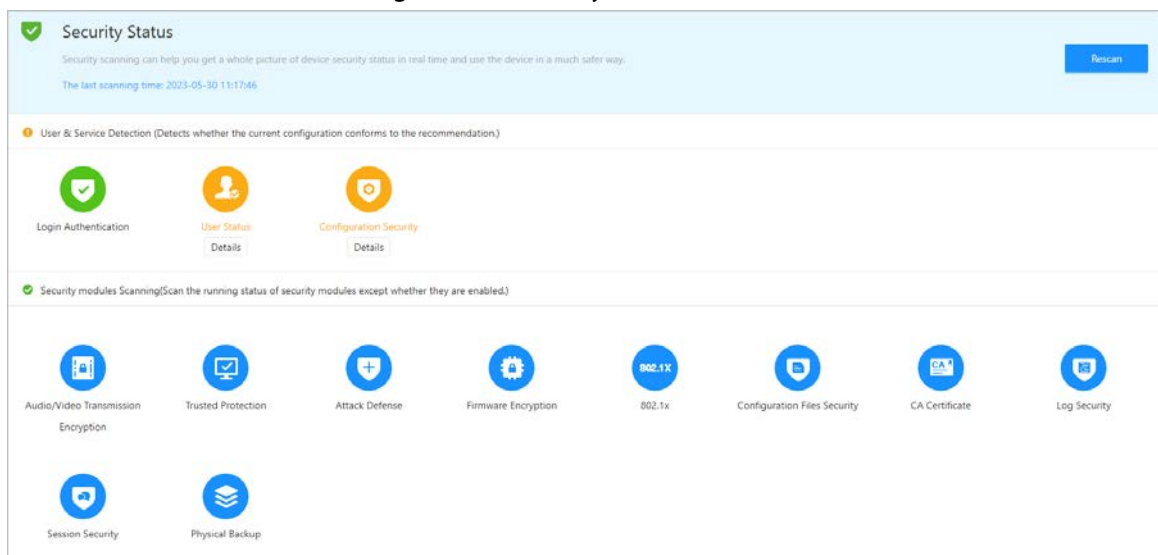
Step 1 Select **Security > Security Status**.

Step 2 Click **Rescan** to perform a security scan of the Access Controller.



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

Figure 3-57 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.

3.16.2 Configuring HTTPS

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

Procedure

Step 1 Select **Security > System Service > HTTPS**.

Step 2 Turn on the HTTPS service.



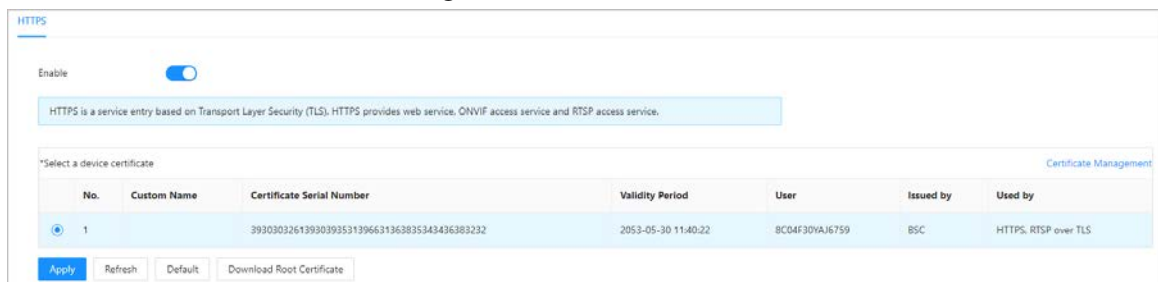
If you turn on the compatible with TLS v1.1 and earlier versions, security risks might occur. Please be advised.

Step 3 Select the certificate.



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

Figure 3-58 HTTPS



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.

3.16.3 Attack Defense

3.16.3.1 Configuring Firewall

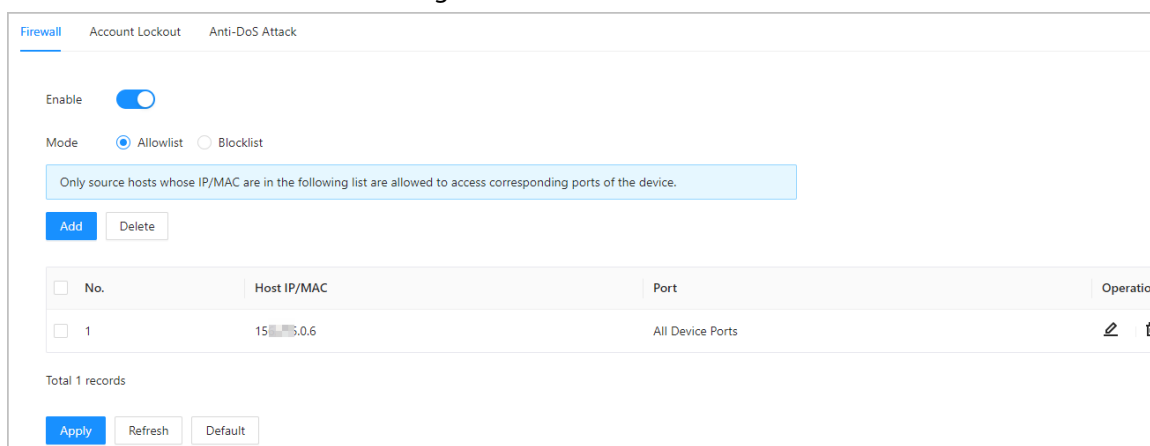
Configure firewall to limit access to the Access Controller.

Procedure

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

Step 2 Click to enable the firewall function.

Figure 3-59 Firewall

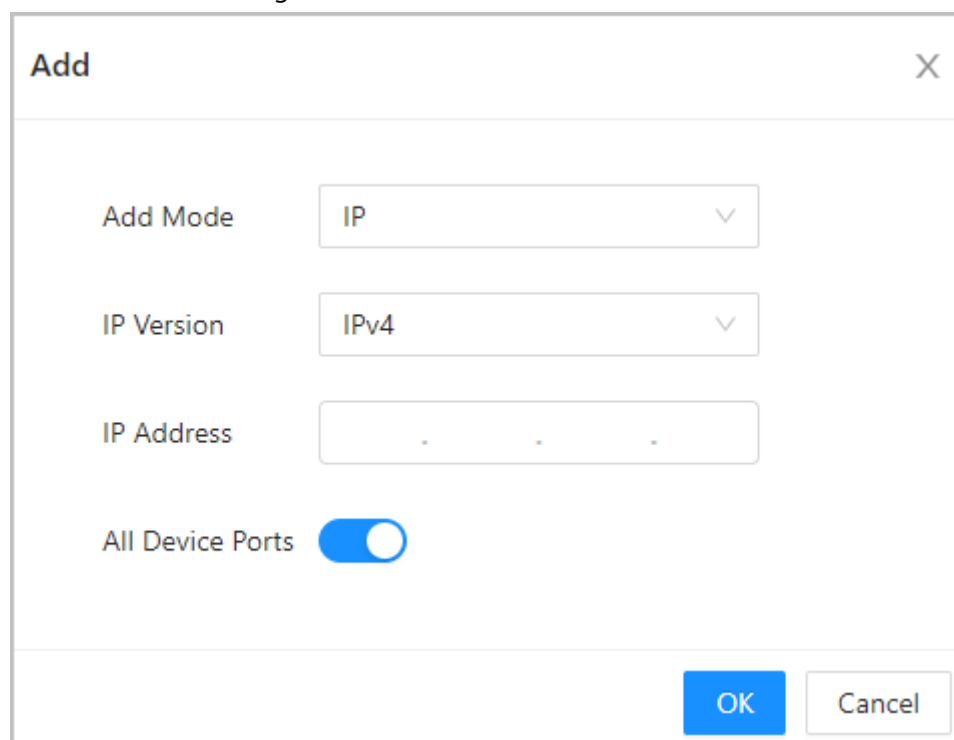


Step 3 Select the mode: **Allowlist** and **Blocklist**.

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



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

Figure 3-60 Add IP information



Step 5 Click **OK**.

Related Operations

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

3.16.3.2 Configuring Account Lockout

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

Procedure

Step 1 Select **Security > Attack Defense > Account Lockout**.

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

Figure 3-61 Account lockout

The screenshot shows the 'Account Lockout' configuration page. It features three tabs: 'Firewall', 'Account Lockout' (which is active and underlined), and 'Anti-DoS Attack'. Below the tabs, the 'Device Account' section is visible. It contains two configuration fields: 'Login Attempt', which is a dropdown menu currently set to '5time(s)', and 'Lock Time', which is a text input field containing the number '5' followed by the unit 'min'. At the bottom of the configuration area, there are three buttons: 'Apply' (highlighted in blue), 'Refresh', and '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**.

3.16.3.3 Configuring Anti-DoS Attack

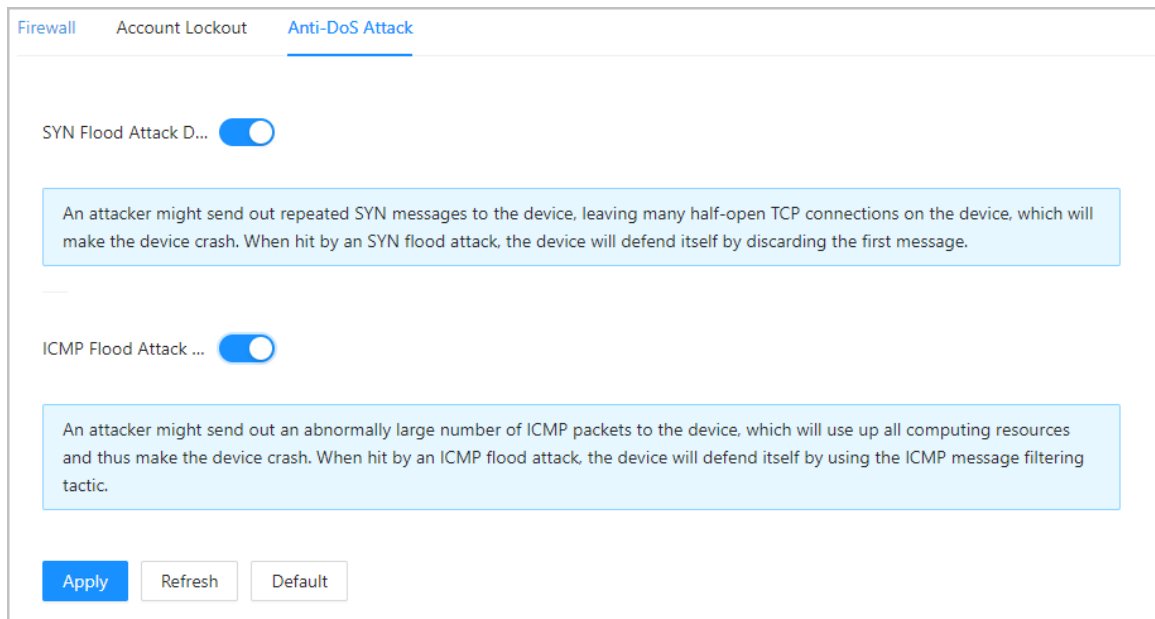
You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Access Controller against Dos attacks.

Procedure

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

Step 2 Turn on **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** to protect the Access Controller against Dos attack.

Figure 3-62 Anti-DoS attack



Step 3 Click **Apply**.

3.16.4 Installing Device Certificate

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

3.16.4.1 Creating Certificate

Create a certificate for the Access Controller.

Procedure

- Step 1** Select **Security > 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 3-63 Certificate information

Step 2: Fill in certificate information. X

Custom Name

* IP/Domain Name

Organization Unit

Organization

* Validity Period Days (1~5000)

* Region

Province

City Name

Back Create and install certificate Cancel



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

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

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

Related Operations

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

3.16.4.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the Access Controller.

Procedure

Step 1 Select **Security > 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 Access Controller.
- Region: The name of region must not exceed 3 characters. We recommend you enter

the abbreviation of region name.

Figure 3-64 Certificate information (2)

The screenshot shows a dialog box with the title "Step 2: Fill in certificate information." and a close button (X) in the top right corner. The form contains the following fields:

- * IP/Domain Name: 17 [blurred] 03
- Organization Unit: [empty]
- Organization: [empty]
- * Region: [empty]
- Province: [empty]
- City Name: [empty]

At the bottom of the dialog, there are three buttons: "Back", "Create and Download" (highlighted in blue), and "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.

3.16.4.3 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 3-65 Certificate and private key

Step 2: Select certificate and private key.

Custom Name

Certificate Path Browse

Private Key Browse

Private Key Password

Back Import and Install Cancel

- 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.

3.16.5 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 its identity.

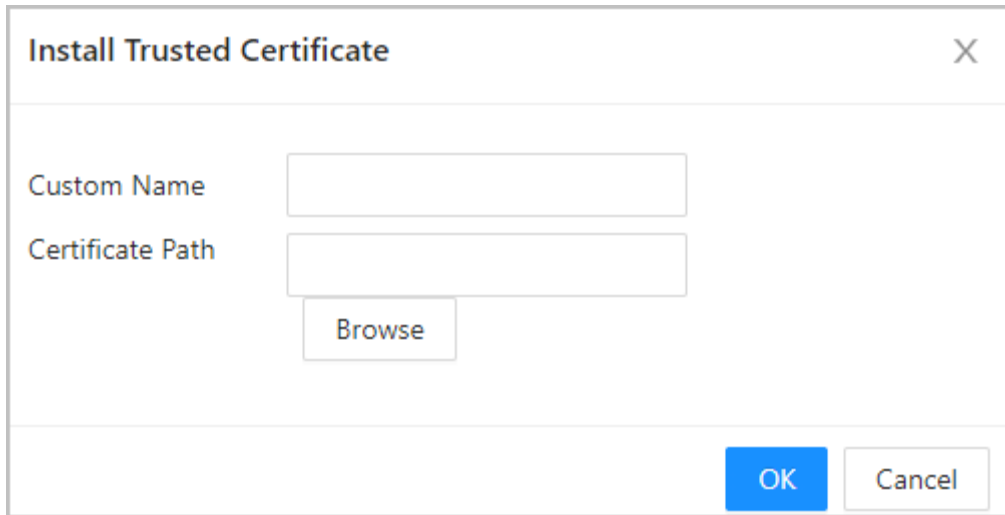
Background Information

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

Procedure

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

Figure 3-66 Install the trusted certificate



Step 4 Click **OK**.

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

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.

3.16.6 Data Encryption

Procedure

Step 1 Select **Security > Data Encryption**.

Step 2 Configure the parameters.

Figure 3-67 Data encryption

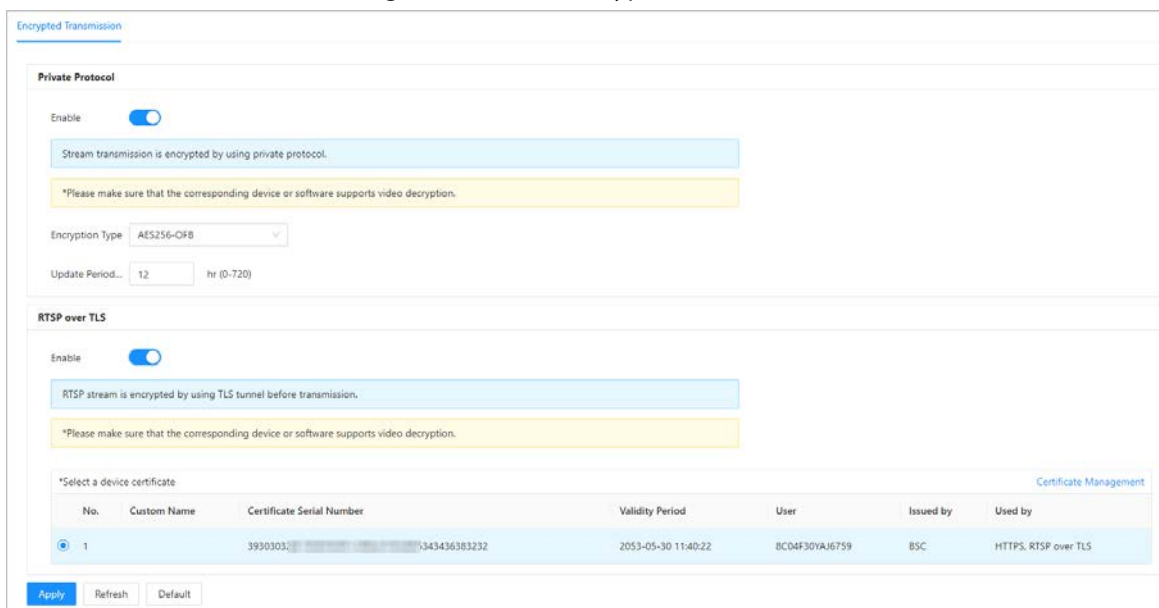


Table 3-36 Data encryption description

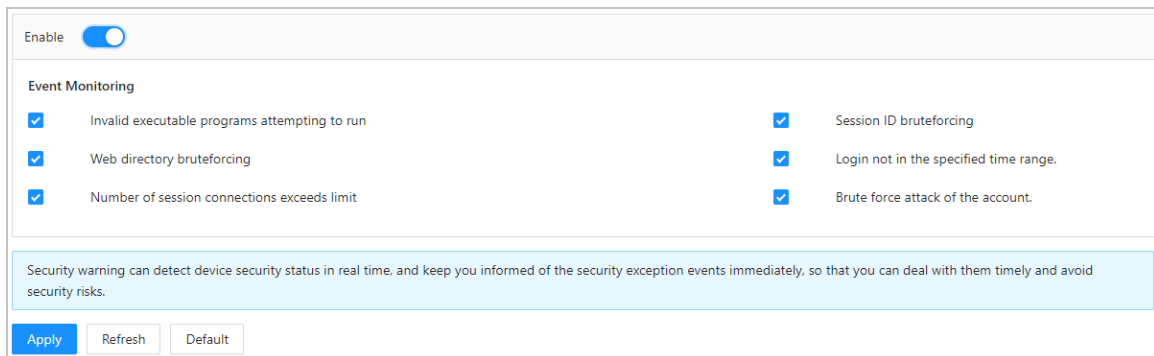
	Parameter	Description
Private Protocol	Enable	Streams are encrypted during transmission through private protocol.
	Encryption Type	Keep it as default.
	Update Period of Secret Key	Ranges from 0 h -720 h. 0 means never update the secret key.
RTSP over TLS	Enable	RTSP stream is encrypted during transmission through TLS tunnel.
	Certificate Management	Create or import certificate. For details, see"3.16.4 Installing Device Certificate". The installed certificates are displayed in the list.

3.16.7 Security Warning

Procedure

- Step 1** Select **Security > Security Warning**.
- Step 2** Enable the security warning function.
- Step 3** Select the monitoring items.

Figure 3-68 Security warning



- Step 4** Click **Apply**.

4 Smart PSS Lite Configuration

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

4.1 Installing and Logging In

Install and log in to Smart PSS Lite. For details, see the user manual of Smart PSS Lite.

Procedure

Step 1 Get the software package of the Smart PSS Lite from the technical support, and then install and run the software according to instructions.

Step 2 Initialize Smart PSS Lite when you log in for the first time, including setting password and security questions.



Set the password is for the first-time use, and then set security questions to reset your password when you forgot it.

Step 3 Enter your username and password to log in to Smart PSS Lite.

4.2 Adding Devices

You need to add the Access Controller to Smart PSS Lite. You can add them in batches or individually.

4.2.1 Adding One By One

You can add Access Controller one by one through entering their IP addresses or domain names.

Procedure

Step 1 Log in to Smart PSS Lite.

Step 2 Click **Device Manager** and click **Add**.

Step 3 Enter the device information.

Figure 4-1 Device information

The screenshot shows a web form for adding a device. It has the following fields and values:

- Device Name:** Access Terminal
- Method to add:** IP
- IP:** [Redacted]
- Port:** 37777
- User Name:** admin
- Password:** [Redacted]

At the bottom, there are three buttons: "Add and Continue" (blue), "Add" (blue), and "Cancel" (grey).

Table 4-1 Device parameters description

Parameter	Description
Device Name	Enter a name of the Access Controller. We recommend you name it after its installation area.
Method to add	Select IP to add the Access Terminal by entering its IP Address.
IP	Enter IP address of the Access Controller.
Port	The port number is 37777 by default.
User Name/Password	Enter the username and password of the Access Terminal.

Step 4 Click **Add**.

The added Access Controller displays on the **Devices** page. You can click **Add and Continue** to add more Access Controllers.

4.2.2 Adding in Batches

We recommend you use the auto-search function when you add want to Access Controllers in batches. Make sure the Access Controllers you add must be on the same network segment.

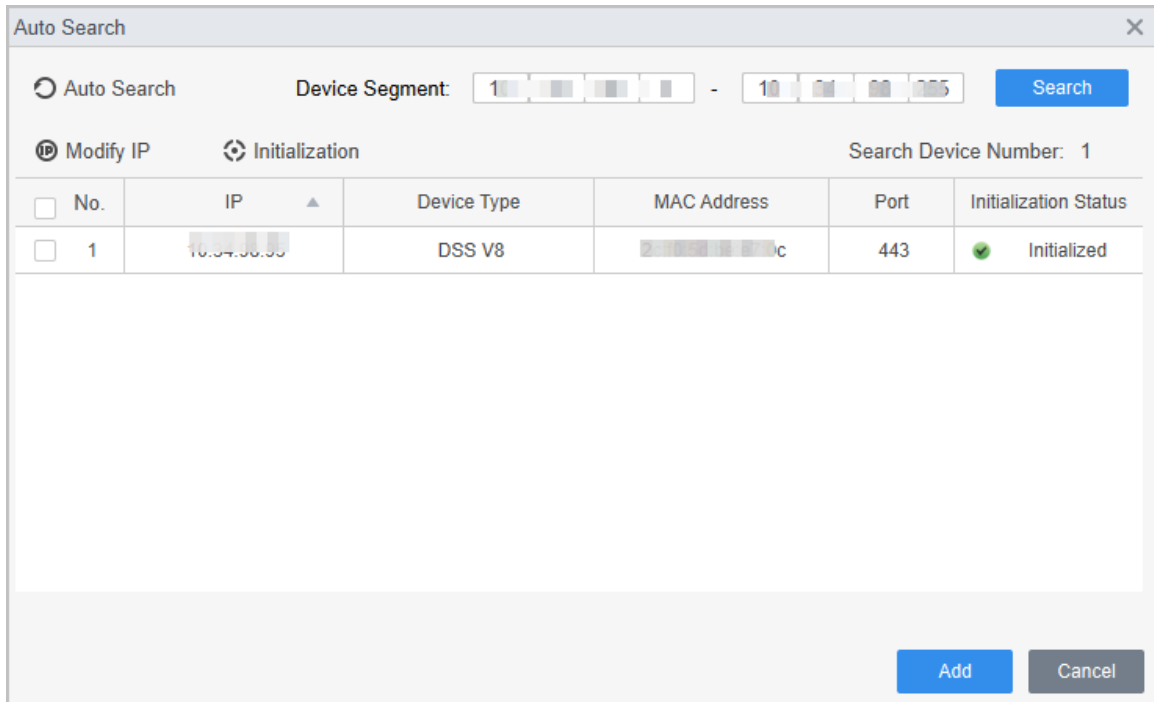
Procedure

Step 1 Log in to Smart PSS Lite.

Step 2 Click **Device Manager** and search for devices.

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

Figure 4-2 Auto search



A device list will be displayed.



Select a device, and then click **Modify IP** to modify its IP address.

Step 3 Select the Access Controller that you want to add to Smart PSS Lite, and then click **Add**.

Step 4 Enter the username and the password of the Access Controller.
You can view the added Access Controller on the **Devices** page.



The Access Controller automatically logs in to Smart PSS Lite after being added. **Online** is displayed after successful login.

4.3 User Management

Add users, assign cards to them, and configure their access permissions.

4.3.1 Configuring Card Type

Set the card type before you assign cards to users. For example, if the assigned card is an ID card, set card type to ID card.

Procedure

- Step 1** Log in to Smart PSS Lite.
- Step 2** Click **Access Solution > Personnel Manager > User**.
- Step 3** On the **Card Issuing Type** and then select a card type.



Make sure that the card type is same to the actually assigned card; otherwise, the card number cannot be read.

Step 4 Click **OK**.

4.3.2 Adding Users

4.3.2.1 Adding One by One

You can add users one by one.

Procedure

Step 1 Log in to Smart PSS Lite.

Step 2 Click **Access Solution > Personnel Manger > User > Add**.

Step 3 Click **Basic Info** tab, and enter the basic information of the user, and then import the face image.

Figure 4-3 Add basic information


The screenshot shows the 'Add basic information' form in the Smart PSS Lite software. The form is divided into three tabs: 'Basic Info', 'Certification', and 'Permission configuration'. The 'Basic Info' tab is active. It contains the following fields and options:

- User ID: *
- Name: *
- Department: Default Company
- User Type: General
- Valid Time: 2022/6/9 0:00:00 to 2032/6/9 23:59:59 (3654 Days)
- Number of use: Limitless
- Face image section: 'Next' button, 'Take Snapshot', 'Upload Picture', and 'Image Size: 0 ~ 100KB'.
- Details section:
 - Gender: Male (selected), Female
 - Title: Mr
 - DOB: 1985/3/15
 - Tel:
 - Email:
 - Mailing Address:
 - Administrator:
 - ID Type: ID
 - ID No.:
 - Company:
 - Occupation:
 - Entry Time: 2022/6/8 20:18:31
 - Resign Time: 2031/6/9 20:18:31
 - Remark:

At the bottom of the form are three buttons: 'Continue', 'Finish', and 'Cancel'.

Step 4 Click the **Certification** tab to add certification information of the user.

- Configure password: The password must consist of 6–8 digits.
- Configure card: The card number can be read automatically or entered manually. To read the card number automatically, select a card reader, and then place the card on the card reader.

1. On the **Card** area, click  and select **Card issuer**, and then click **OK**.

2. Click **Add**, swipe a card on the card reader. The card number is displayed.
3. Click **OK**.

After adding a card, you can set the card to main card or duress card, or replace the card with a new one, or delete the card.


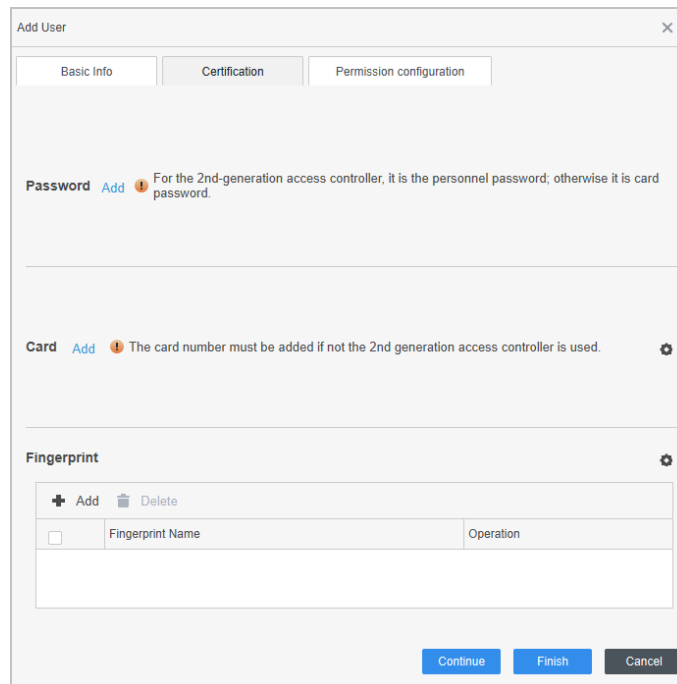
- Configure fingerprint.
 1. On the **Fingerprint** area, click  and select **Fingerprint Scanner**, and then click **OK**.
 2. Click **Add Fingerprint**, press your finger on the scanner three times in a row.

Figure 4-4 Add password, card, and fingerprint



The screenshot shows the 'Add User' configuration window. It has three tabs: 'Basic Info', 'Certification', and 'Permission configuration'. The 'Basic Info' tab is selected. The window contains three main sections: 'Password', 'Card', and 'Fingerprint'. Each section has an 'Add' button and a warning icon. The 'Fingerprint' section includes a table with columns for 'Fingerprint Name' and 'Operation'. At the bottom of the window are three buttons: 'Continue', 'Finish', and 'Cancel'.

Step 5 Configure permissions for the user. For details, see "4.3.3 Assigning Access Permission".

Step 6 Click **Finish**.

4.3.2.2 Adding in Batches

You can add users in batches.

Procedure

Step 1 Log in to Smart PSS Lite.

Step 2 Click **Personnel Manger** > **User** > **Batch Add**.

Step 3 Select **Card issuer** from the **Device** list, and then configure the parameters.

Figure 4-5 Add users in batches

The screenshot shows a dialog box for adding users in batches. It includes the following fields and controls:

- Device:** A dropdown menu set to "Card issuer" and an "Issue" button.
- Start No.:** A text input field containing "1".
- Quantity:** A text input field containing "30".
- Department:** A dropdown menu set to "Default Company".
- Effective Time:** A date-time picker set to "2022/4/1 0:00:00".
- Expired Time:** A date-time picker set to "2032/4/1 23:59:59".
- Issue Card:** A table with 11 rows. The first column is labeled "ID" and contains numbers 1 through 11. The second column is labeled "Card No." and is currently empty.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Table 4-2 Add users in batches parameters

Parameter	Description
Start No.	The user ID starts with the number you defined.
Quantity	The number of users you want to add.
Department	Select the department that the user belongs to.
Effective Time/Expired Time	The users can unlock the door within the defined period.

Step 4 Click **Issue**.

The card number will be read automatically.

Step 5 Click **OK**.

Step 6 On the **User** page, click  to complete user information.

4.3.3 Assigning Access Permission

Create a permission group that is a collection of door access permissions, and then associate users with the group so that users can unlock corresponding doors.

Procedure

Step 1 Log in to the Smart PSS Lite.

Step 2 Click **Access Solution > Personnel Manger > Permission configuration**.

Step 3 Click **+** .

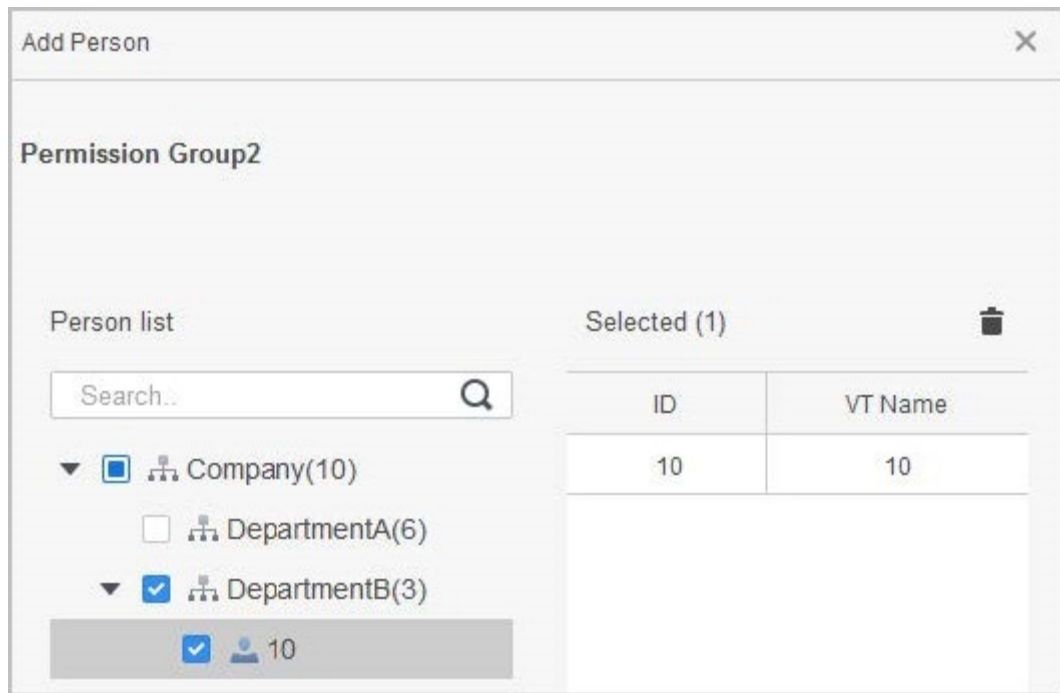
- Step 4 Enter the group name, remarks (optional), and select a time template.
- Step 5 Select the access control device.
- Step 6 Click **OK**.

Figure 4-6 Create a permission group

The screenshot shows the 'Add Access Group' dialog box. The 'Basic Info' section contains 'Group Name' (Permission Group3) and 'Remark' (empty), both highlighted with a red box labeled '1'. The 'Time Template' dropdown is set to 'All Day Time Template', highlighted with a red box labeled '2'. The 'All Device' section shows a search bar and a list of devices: 'Default Group' (expanded), '1' (expanded), and 'Door 1'. A red box labeled '3' highlights the 'All Device' section. At the bottom right, the 'OK' button is highlighted with a red box.

- Step 7 Click of the permission group you added.
- Step 8 Select users to associate them with the permission group.

Figure 4-7 Add users to a permission group



- Step 9** Click **OK**.
Users in the permission group can unlock the door after valid identity verification.

4.3.4 Assigning Attendance Permissions

Create a permission group that is a collection of time attendance permissions, and then associate employees with the group so that they can punch in/out through defined verification methods.

Procedure

- Step 1** Log in to the Smart PSS Lite.
Step 2 Click **Access Solution > Personnel Manger > Permission configuration**.
Step 3 Click + .
Step 4 Enter the group name, remarks (optional), and select a time template.
Step 5 Select the access control device.
Step 6 Click **OK**.

Figure 4-8 Create a permission group

Add Access Group

Basic Info

Group Name: Remark:

Time Template:

All Device Selected (0)

Search...

Default Group

1 3

Door 1

OK Cancel

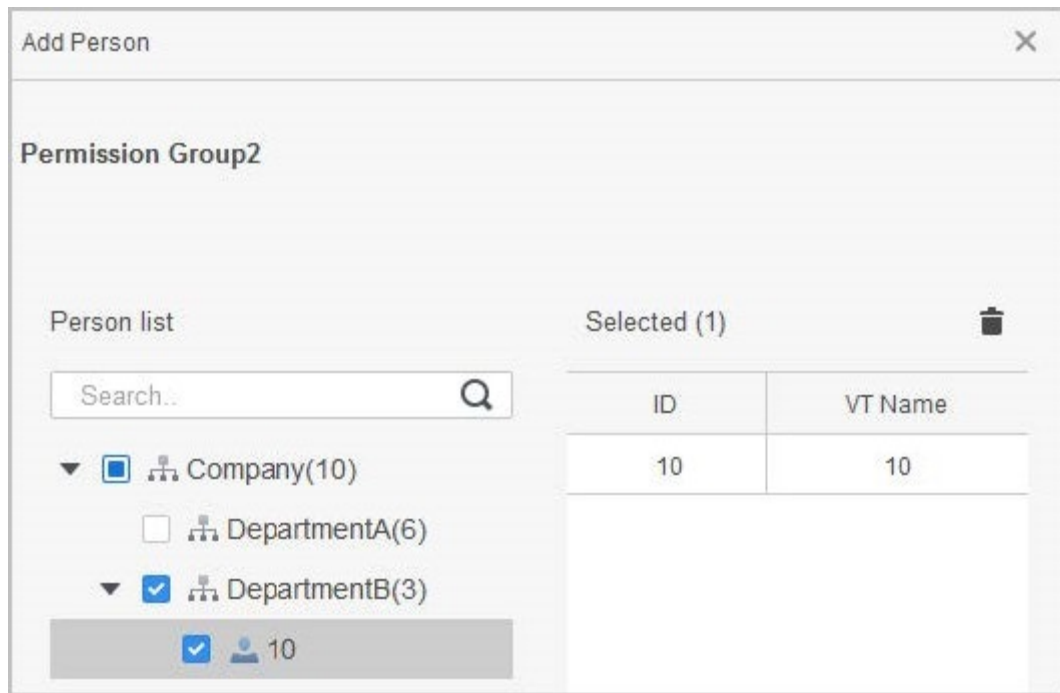


The Time & Attendance only supports punch-in/out through password and face attendance.

Step 7 Click of the permission group you added.

Step 8 Select users to associate them with the permission group.

Figure 4-9 Add users to a permission group



Step 9 Click **OK**.

4.4 Access Management

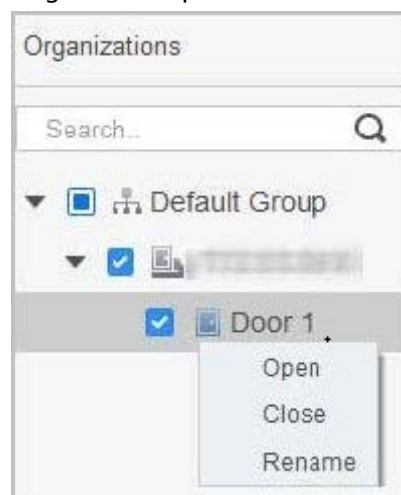
4.4.1 Remotely Opening and Closing Door



You can remotely monitor and control door through Smart PSS Lite. For example, you can remotely open or close the door.

Procedure




- Step 1 Click **Access Solution** > **Access Manager** on the Home page.
- Step 2 Remotely control the door.
- Select the door, right click and select **Open** or **Close**.

Figure 4-10 Open door



- Click  or  to open or close the door.

Related Operations

- Event filtering: Select the event type in the **Event Info**, and the event list displays the selected event type, such as alarm events and abnormal events.
- Event refresh locking: Click  to lock the event list, and then event list will stop refreshing. Click  to unlock.
- Event deleting: Click  to clear all events in the event list.

4.4.2 Setting Always Open and Always Close

After setting always open or always close, the door remains open or closed all the time.

Procedure

- Step 1 Click **Access Solution** > **Access Manager** on the Home page.
- Step 2 Click **Always Open** or **Always Close** to open or close the door.

Figure 4-11 Always open or close



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

4.4.3 Monitoring Door Status

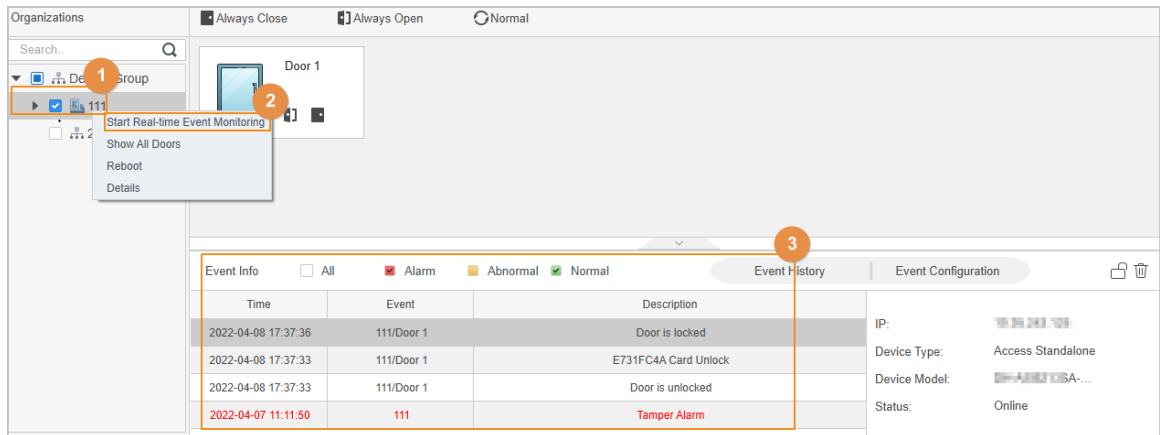
Procedure

- Step 1 Click **Access Solution** > **Access Manager** on the home page.
- Step 2 Select the Access Controller in the device tree, and right click the Access Controller and then select **Start Real-time Event Monitoring**.
Real-time access control events will display in the event list.



Click **Stop Monitor**, real-time access control events will not display.

Figure 4-12 Monitor door status



Related Operations

- Show All Door: Displays all doors controlled by the Access Controller.
- Reboot: Restart the Access Controller.
- Details: View the device details, such as IP address, model, and status.

Appendix 1 Important Points of Face Registration

Before Registration

- Glasses, hats, and beards might influence face recognition performance.
- Do not cover your eyebrows when wearing hats.
- Do not change your beard style greatly if you use the Access Controller; otherwise face recognition might fail.
- Keep your face clean.
- Keep the Access Controller at least 2 meters away from light source and at least 3 meters away from windows or doors; otherwise backlight and direct sunlight might influence face recognition performance of the access controller.

During Registration

- You can register faces through the Access Controller or through the platform. For registration through the platform, see the platform user manual.
- Make your head center on the photo capture frame. The face image will be captured automatically.

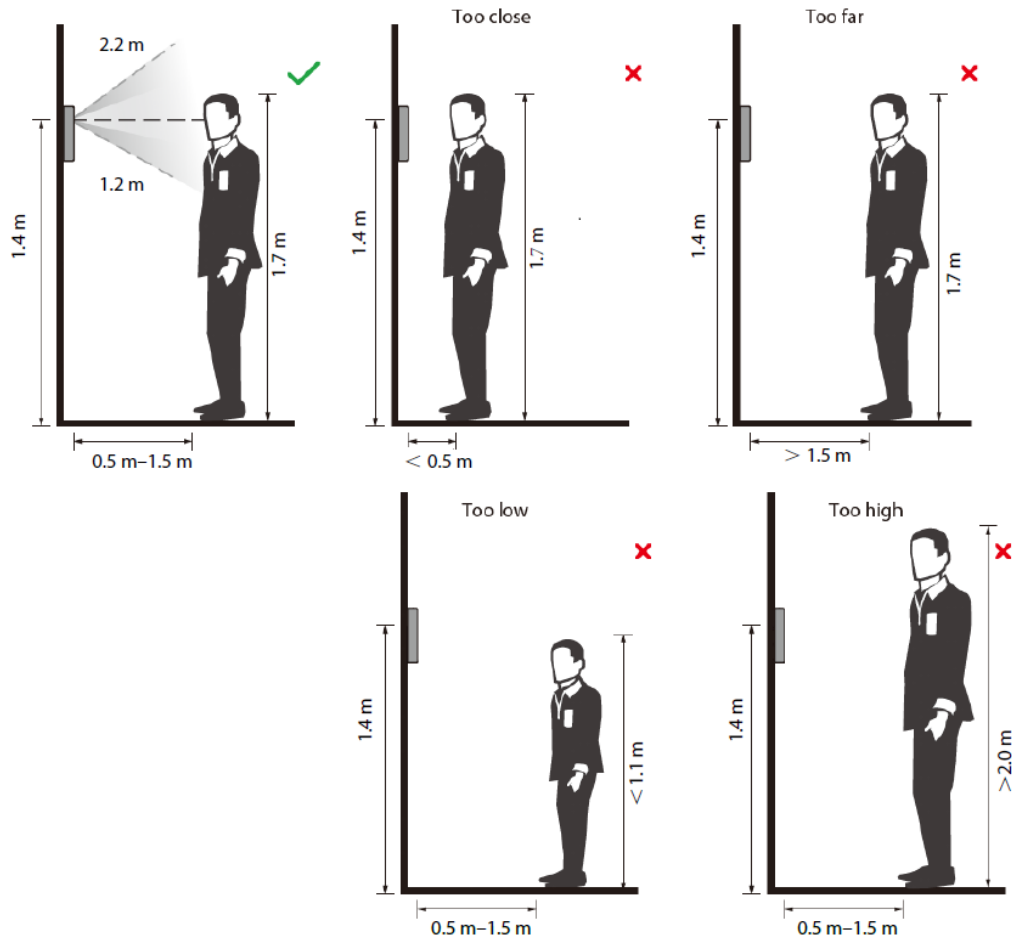


- Do not shake your head or body, otherwise the registration might fail.
- Avoid 2 faces appear in the capture frame at the same time.

Face Position

If your face is not at the appropriate position, face recognition accuracy might be affected.

Appendix Figure 1-1 Appropriate face position



Requirements of Faces

- Make sure that the face is clean and forehead is not covered by hair.
- Do not wear glasses, hats, heavy beards, or other face ornaments that influence face image recording.
- With eyes open, without facial expressions, and make your face toward the center of camera.
- When recording your face or during face recognition, do not keep your face too close to or too far from the camera.

Appendix Figure 1-2 Head position



Appendix Figure 1-3 Face distance



- When importing face images through the management platform, make sure that image resolution is within the range 150 × 300 pixels–600 × 1200 pixels; image pixels are more than 500 × 500 pixels; image size is less than 100 KB, and image name and person ID are the same.
- Make sure that the face takes up more than 1/3 but no more than 2/3 of the whole image area, and the aspect ratio does not exceed 1:2.


Appendix 2 Important Points of Intercom Operation


The Access Controller can function as VTO to realize intercom function.

Prerequisites

The intercom function is configured on the Access Controller and VTO.

Procedure

Step 1 On the standby screen, tap .

Step 2 Enter the room No, and then tap .

Appendix 3 Important Points of Fingerprint Registration Instructions

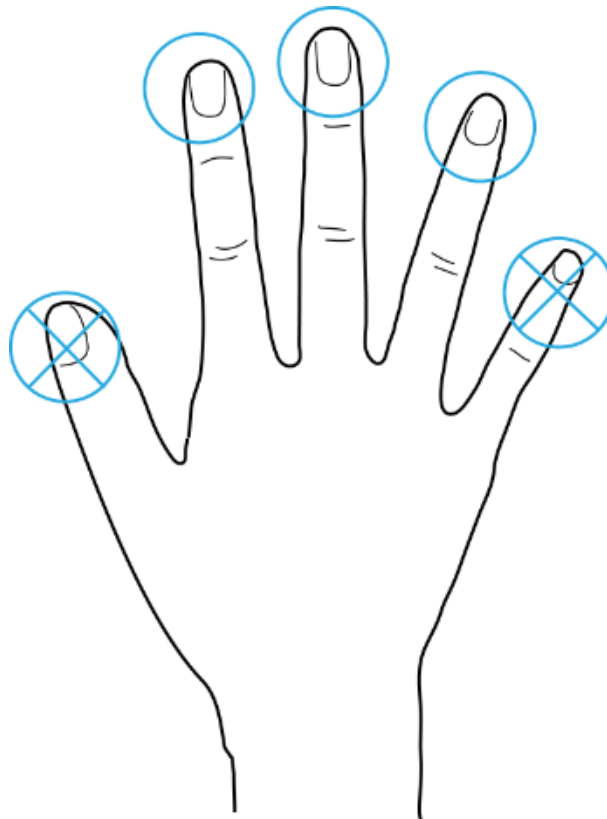
When you register the fingerprint, pay attention to the following points:

- 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

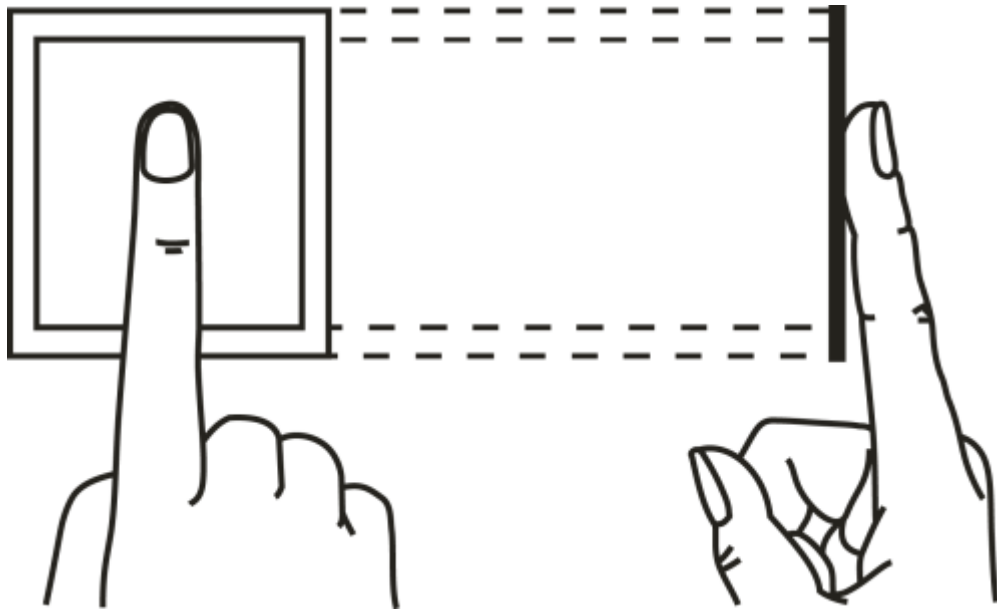
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 3-1 Recommended fingers

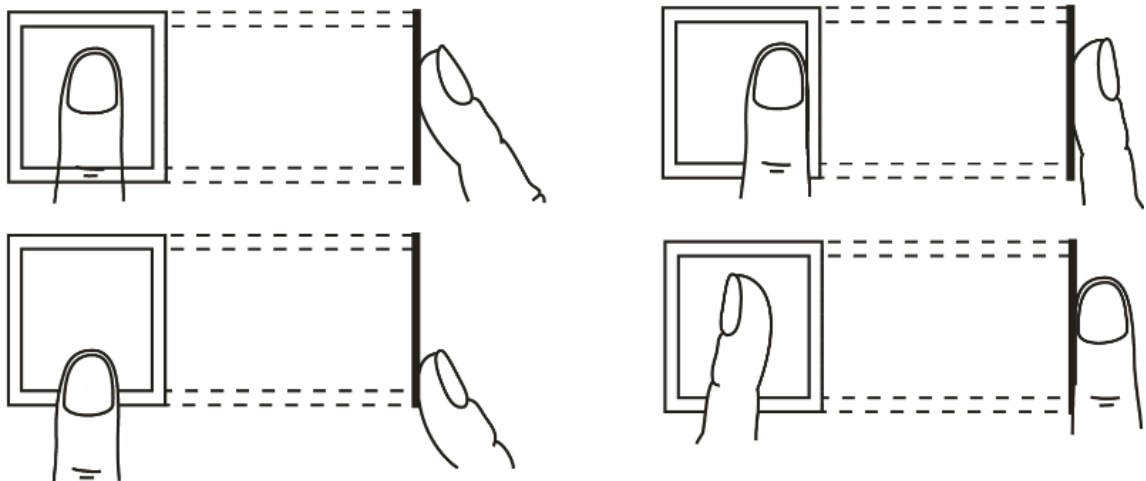


How to Press Your Fingerprint on the Scanner

Appendix Figure 3-2 Correct placement



Appendix Figure 3-3 Wrong placement



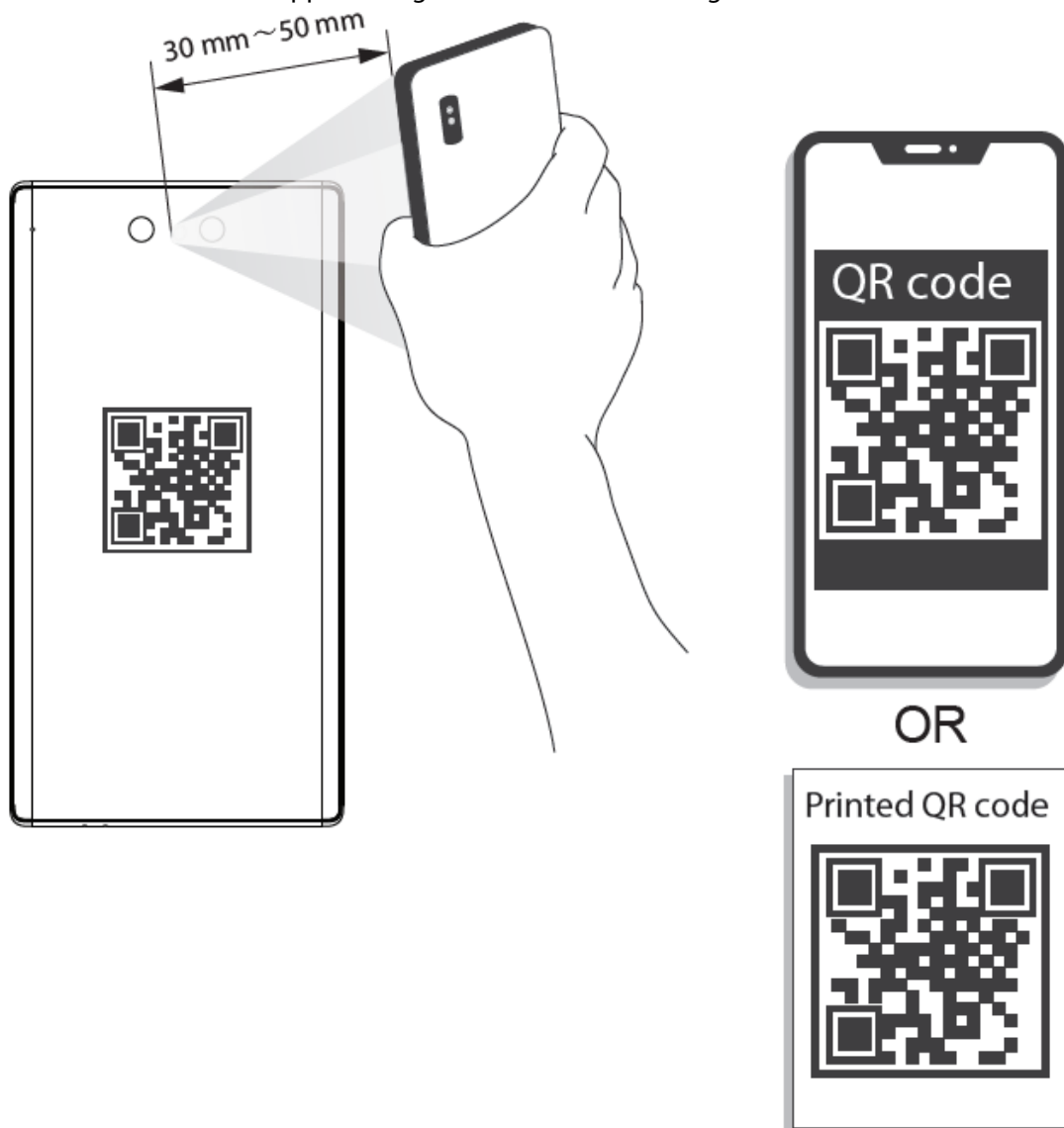
Appendix 4 Important Points of QR Code Scanning

Access Controller: Place the QR code on your phone at a distance of 30 mm–50 mm away from the QR code scanning lens. It supports QR code that must be larger than 30 mm× 30 mm and less than 128 bytes in size.



QR code detection distance differs depending on the bytes and size of QR code.

Appendix Figure 4-1 QR code scanning



Appendix 5 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. Use Strong 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; character types include 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 overlapped characters, such as 111, aaa, etc.

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the “auto-check for updates” function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. Physical Protection

We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The device supports password reset function. Please set up related information for password reset in time, including the end user’s mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing

the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

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

10. **Audio and Video Encrypted Transmission**

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.