

Face Recognition Terminal

FC01

User Manual

Revision 1.0



Face Recognition Terminal User Manual

Preface

The manual introduces the functions and operations of the Face Recognition Terminal (hereinafter referred to as the "Device"). Please read it carefully before using the device, and keep this manual in a safe place for future reference.

Privacy Notice

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

Safety Instruction

The following signal words may appear in the manual.

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

About the Manual

- This manual is for reference only. There may be slight differences between the manual and the product.
- We are not responsible for any losses resulting from the operation of the product in a manner that does not comply with the manual.
- The manual will be updated in accordance with the latest laws and regulations of the relevant jurisdictions. For detailed information, please refer to the printed user manual, use our CD, scan the QR code, or visit our official website. This manual is for reference only. There may be slight differences between the electronic version and the printed version.

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

Important Safety Instruction and Warning

Transportation Requirement

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

Storage Requirement

Store the Terminal under permissible humidity and temperature conditions.

Installation Requirements

- Do not connect the power adapter to the Terminal while the adapter is powered on.
- Strictly follow to local electrical safety regulations and standards. Ensure that the environmental voltage is stable and meets the power requirements for the Terminal.
- Do not connect the Terminal to two or more power sources to avoid damage to the Terminal.
- Improper use of batteries may result in fire or explosion.
- Please follow the electrical requirements to power the Terminal.
 - ◊ The following are the requirements for selecting a power adapter.
 - The power supply system must comply with the requirements of IEC 60950-1 and IEC 62368-1 standards.
 - The voltage must comply with SELV (Safety Extra Low Voltage) requirements and must not exceed the ES-1 standard.
 - When the power of the device does not exceed 100 watts, the power supply must comply with LPS requirements and must not exceed PS2.
 - ◊ We recommend using the power adapter provided with the Terminal.
 - ◊ When selecting a power adapter, the power supply requirements (such as rated voltage) should follow the instructions on the Terminal label.

Face Recognition Terminal User Manual

- Personnel working at heights must take all necessary measures to ensure personal safety, including wearing safety helmets and safety harnesses.
- Do not place the Terminal in direct sunlight or near heat sources.
- Keep the Terminal away from moisture, dust, and smoke.
- Install the Terminal on a stable surface to prevent it from falling.
- Install the Terminal in a well-ventilated area and do not block its ventilation openings.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the recommended power cord that meets the rated power specifications.
- The access control controller is classified as a Class I electrical device. Ensure that the power supply for the Terminal is connected to a power outlet with protective grounding.

Operation Requirements

- Check whether the power supply is correct before use.
- Before powering on, ground the device to the protective ground.
- Do not unplug the power cable from the side of the controller while the adapter is powered on.
- Operate the Terminal within the rated input and output power range.
- Use the Terminal under permitted humidity and temperature conditions.
- Do not spill or splash liquids onto the Terminal, and ensure that there are no items containing liquids on the Terminal to prevent liquids from entering it.
- Do not disassemble the Terminal without professional instruction.
- This product is a professional device.
- This Terminal is not suitable for use in areas where children may be present.

Contents

Preface 1

Overview..... 1

Local Operations..... 2

 Basic Configuration Process 2

 Standby Screen..... 2

 Initialization..... 3

 Log In 3

 Password Resetting..... 3

 Unlock Options..... 4

 By Cards..... 4

 By Face..... 4

 By User Password..... 4

 By Administrator Password..... 4

 By Temporary Password 4

 User Management..... 5

 Add Users 5

 View User Information..... 6

 Access Control Management..... 6

 Unlock Method 7

 Combination 7

 By Period 7

 By Multi-user 7

 Alarms 7

 Face Parameters 9

 Lock Status Config 11

 Verification Time Interval..... 11

 Administrator Password..... 11

Communication Settings..... 11

 Network Settings..... 12

 IP Settings..... 12

 Auto Registration 13

 Wi-Fi 13

 Wi-Fi AP..... 13

 RS-485 Settings..... 14

 Wiegand Settings..... 15

Local Functions 15

Reports..... 18

 Unlock Records..... 18

 System Capacity..... 18

System Settings 18

 Time..... 18

 Volume Settings..... 19

 Language..... 19

 Screen Settings..... 19

 Factory Defaults 19

 About 20

 Restart 20

Web Operations 21

 Basic Configuration Process on Web..... 21

 Initialization..... 21

 Log In 21

 Password Resetting..... 21

 Home Page..... 22

 User Management..... 22

 Access Control 24

 Door Parameters..... 24

 Basic Settings..... 24

 Unlock Settings..... 25

 Alarm 26

 Alarm Linkage Setting (Optional) 27

 Alarm Event Linkage..... 28

 Face Parameters..... 29

 Card Settings..... 31

 Weekly Schedule..... 32

 Holiday Schedule..... 33

Face Recognition Terminal User Manual

Privacy Setting	34	Video	49
Port Config	34	Audio	51
Back-end Comparison	34	Motion Detection	52
First-Person Unlock	34	View Selection	53
Intercom Settings	35	Advertisement	53
Using the Device as the SIP Server	35	Adding Resources	53
Local Device Config	35	Configuring Subject	54
SIP Server	35	Management Center	55
Adding the Outdoor Station	36	System Information	55
Adding the Indoor Monitor	36	Version Information	55
Using VTO as the SIP server	38	Legal Information	55
SIP Server	38	System Capacity	55
Local Device Config	38	Log	55
Call Config	39	System Logs	55
Communication Settings	40	Unlock Records	55
Network Settings	40	Call History	55
TCP/IP	40	Alarm Logs	55
Wi-Fi	41	Admin Logs	56
Wi-Fi AP	41	USB Management	56
Port	41	Maintenance	56
Basic Services	42	Export/Import Configuration Files	56
Cloud Service	43	Restore to Default	56
Auto Registration	43	Restart	56
Auto Upload	44	Update	57
RS-485 Settings	44	File Update	57
Wiegand Settings	45	Online Update	57
System Settings	46	Advanced Maintenance	57
Account	46	Export	57
Adding Administrators	46	Packet Capture	57
Adding ONVIF Users	46	Security (Optional)	58
Resetting the Password	47	Configure HTTPS	58
Viewing Online Users	47	Attack Defense	58
Time	47	Firewall	58
Shortcut Settings	48	Account Lockout	58

Face Recognition Terminal User Manual

- Anti-DoS Attack.....59
- Installing Device Certificate59
 - Create Certificate59
 - Apply for CA Certificate and Import60
 - Install Existing Certificate60
- Installing the Trusted CA Certificate61
- Cybersecurity Recommendations.....62

Overview

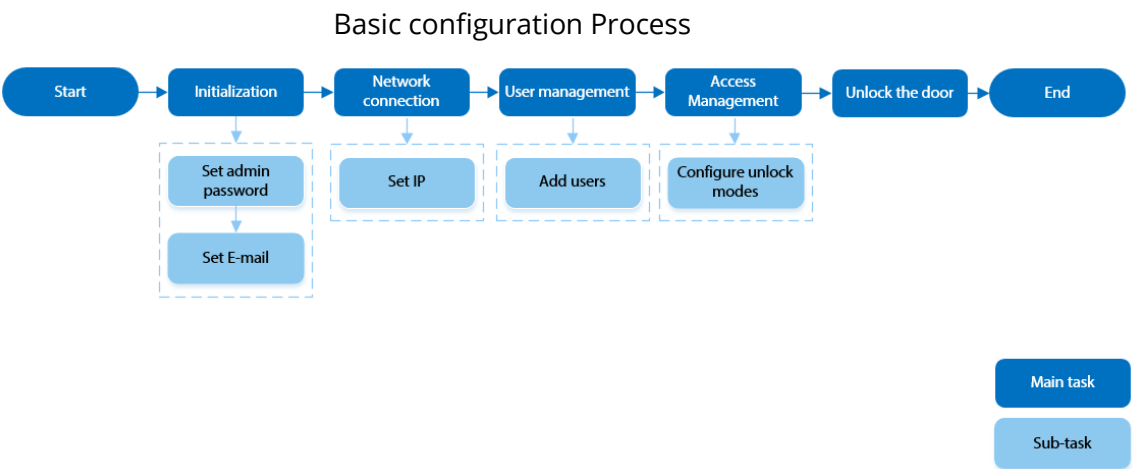
This device is a terminal that supports unlocking through facial recognition, passwords, cards, and their combinations. Based on deep learning algorithms, it offers faster recognition speed and higher accuracy. It can work in collaboration with management platforms that meet various customer needs.

- The configuration may vary depending on the product model; please refer to the actual product.
- Non-touchscreen devices must be connected to a mouse for configuration. This manual takes touchscreen devices as an example.

Local Operations

- The configuration may vary depending on the actual product.
- This section takes the touchscreen model as an example
- External expansion modules are only available for specific models.
- You may find that certain UI text is not displayed due to limited space. Press and hold the text for 3 seconds, and it will be displayed.

Basic Configuration Process



Standby Screen

Unlock the door using faces, cards and passwords. You can also make calls using the intercom function. The unlocking methods may vary depending on the product model.

NOTE

- This manual is for reference only. There may be slight differences between the standby screen in the manual and the actual device.
- If there is no operation within 30 seconds, the device will enter standby mode.



Home screen description

No.	Name	Description
1	Date and time	Display the current date and time.
2	Call	• When the device operates as a server, it can call the VTO and indoor monitor. • When the management platform operates as a server, devices can call the VTO and the management platform.
3	Password	Enter the user password, administrator password, or temporary password to unlock the door.

Face Recognition Terminal User Manual

No.	Name	Description
4	Main Menu	Tap the icon to login to Setting page. You can configure device function in this page.
5	Status display	Displays status of Wi-Fi, network, expansion module and more. Wi-Fi and expansion modules are only available on select models. Tap  to enter the Wi-Fi AP screen. For more details, refer to "Wi-Fi AP".

Initialization

After the first use or factory reset, you need to select a language on the device, and then set a password and email address for the administrator account. You can use the administrator account to access the device's main menu and its web page.

 NOTE

- If you have forgotten the administrator password, please send a reset request to the email address you registered with.
- The password must consist of 8 to 32 non-empty characters and must include at least two types of characters, including uppercase letters, lowercase letters, numbers, and special characters (excluding ' " ; : &).

Log In

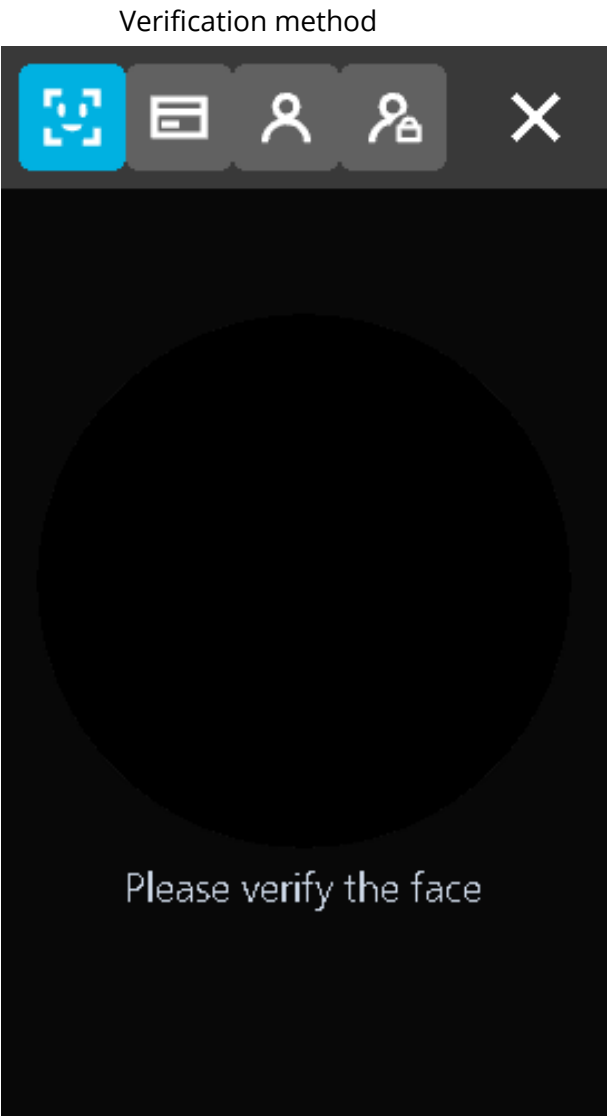
Log in to the main menu to configure the device. Only administrator accounts and management accounts can access the device's main menu. When using for the first time, please enter the main menu interface using the administrator account, after which you can create additional management accounts.

Background Information

- Management account: Can log in to the device's main menu interface, but does not have access control permissions.
- Administrator account: Can log into the device's main menu and has access control permissions.

Process

1. Click  or press and hold the standby screen for 1.5 seconds.
2. Select a verification method to access the main menu.



- Face: Access the main menu through facial recognition.
- Card: Access the main menu by swiping card.
- Password: Access the user ID and password of the administrator account.
- admin: Enter the admin password to access the main menu.

Password Resetting

When you forget the administrator password, please reset it through the associated email.

Precondition

If you wish to reset your password, please ensure that an email address was configured during initialization.

Process

1. Click  or press and hold the standby screen for 1.5 seconds.

Face Recognition Terminal User Manual

- 2. Tap , then tap **Forgot password**.
- 3. Read the on-screen prompt, then click **Enter**.
- 4. Tap **QR Code** and scan the QR code.
- 5. Send the scanning results to the associated email address.
You will receive an email containing a security code.

 NOTE

- After scanning the QR code, you will receive a security code sent to your associated email address. Please use the security code within 24 hours of receiving it, otherwise it will expire.
- When scanning the same QR code, a maximum of two security codes will be generated. If the security code becomes invalid, please refresh the QR code and scan it again.

- 6. Enter the security code.

 NOTE

If the incorrect security code is entered five times in a row, the administrator account will be frozen for five minutes.

- 7. Click **Next**.
- 8. Reset and confirm the password.

 NOTE

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

- 9. Click **OK**.

Unlock Options

Unlock the door using faces, passwords, fingerprints, cards, and more.

By Cards

Place the card in the card reading area to unlock the door.

 NOTE

This feature is only available on specific models.

By Face

Verify identity by detecting the individual's face. Ensure that the face is centered within the face detection box.

By User Password

Enter the user ID and password to unlock the door.

Process

- 1. Tap  on the standby screen.
- 2. Tap , then enter the user ID and password.
- 3. Tap **OK**.
If you enable **PIN Code Authentication** through **Access Control > Access Control Parameters** on the device's web page, you can verify your identity using a password without the need for a user ID.

By Administrator Password

The door can be unlocked by entering the administrator password only. All doors, except for those that are always locked, can be unlocked with the administrator password. Each device is allowed only one administrator password.

Precondition

The administrator password has been configured. For more details, refer to "Administrator Password".

Process

- 1. Tap  on the standby screen.
- 2. Tap , then enter the administrator password.
- 3. Tap **OK**.

 NOTE

When the door status is set to always locked, the administrator password cannot be used to unlock it.

By Temporary Password

Unlock the door with a temporary password.

Process

- 1. Add the Device to LumiViewer.
LumiViewer will generate a temporary password that allows you to unlock the door before it expires.
- 2. Tap  on the home screen, then tap .

Face Recognition Terminal User Manual

3. Enter the temporary password, then tap **OK**.

User Management

Add new users, view user/admin list and edit user information.

 NOTE

The images in this manual are for reference only and may differ from the actual product.

Add Users

Process

1. Go to **User Management** >  on the main menu page.
2. Configure the related parameters.

Add the user (1)



Add User



User Permission

User >

User ID

2

Name

Face

0 >

Card

0 >

Password

Weekly Schedule

255-Full Day >

<

1/2

>

Add the user (2)



Add User



Holiday Schedule

255-No Plan >

Validity Period

2037-12-31 >

User Type

General User >

Department

1-Default >

Schedule Mode

Department Sc... >

<

2/2

>

Parameters description

Parameter	Description
User Permission	• User: Users only have door access permissions. • Admin: The administrator can configure the device, except for door access permissions.
User ID	The user ID is similar to the employee ID and can consist of a combination of numbers and letters, with a maximum length of 30 characters.
Name	The name can contain a maximum of 32 characters (including numbers, symbols, and letters).
Face	Place your face within the frame, and the system will automatically capture the facial image. If you are not satisfied with the result, you can re-register.

Parameter	Description
Card	Users can register up to 5 cards. Please enter your card number or swipe the card, and the device will read the card information. You can enable the Duress Card function. If the door is unlocked using a forced card, an alarm will be triggered.  NOTE • This function is only available on certain models. • Each user can only set one duress card.
Password	Enter the user password. The maximum length of the password is 8 digits. The emergency password is obtained by adding 1 to the last digit of the unlock password. For example, if the user password is 12345, the emergency password will be 12346; if the user password is 789, the emergency password will be 780. When the emergency password is used to unlock the door, an emergency alarm will be triggered.
Weekly Schedule	People can unlock doors within the specified time. For details on how to configure periods, refer to "Weekly Schedule".
Holiday Schedule	People can unlock doors during the designated holidays For details on how to configure holiday, refer to "Holiday Schedule".
Validity Period	Set a date for the expiration of the access permissions for that individual.
User Type	• 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 specified time or a certain number of times. Once the specified time expires or the unlocking attempts are exhausted, they will no longer be able to unlock the door. • VIP User: If the door is in "Normal" status, VIP users can open it at any time, regardless of other rules. • Other User: When they unlock the door, the door will remain unlocked for 5 seconds.  NOTE This feature is disabled when remote verification is enabled.

Parameter	Description
Department	Select departments, which is useful when configuring department schedules.  NOTE This feature is only available on specific models.
Schedule Mode	• Department Schedule: Apply department schedules to the user. • Personal Schedule: Apply personal schedules to the user.  NOTE This feature is only available on specific models.

3. Tap .

View User Information

Process

1. Select **User Management** on the main menu.
2. View all added user and administrator accounts.
 - : Unlock by reading card.
 - : Unlock by face recognition.
 - : Unlock by password.

Related Operations

- You can manage the added users on the **User Management** screen.
- Search for users: Tap  Search and then enter the username or user ID.
 - Edit users: Tap the user to edit user information.
 - Delete users: Select a user and then tap .

Access Control Management

Configure settings for the door, such as unlocking modes, alarm linkage, and the door's schedule. The available unlocking modes may vary depending on the product model.

Unlock Method

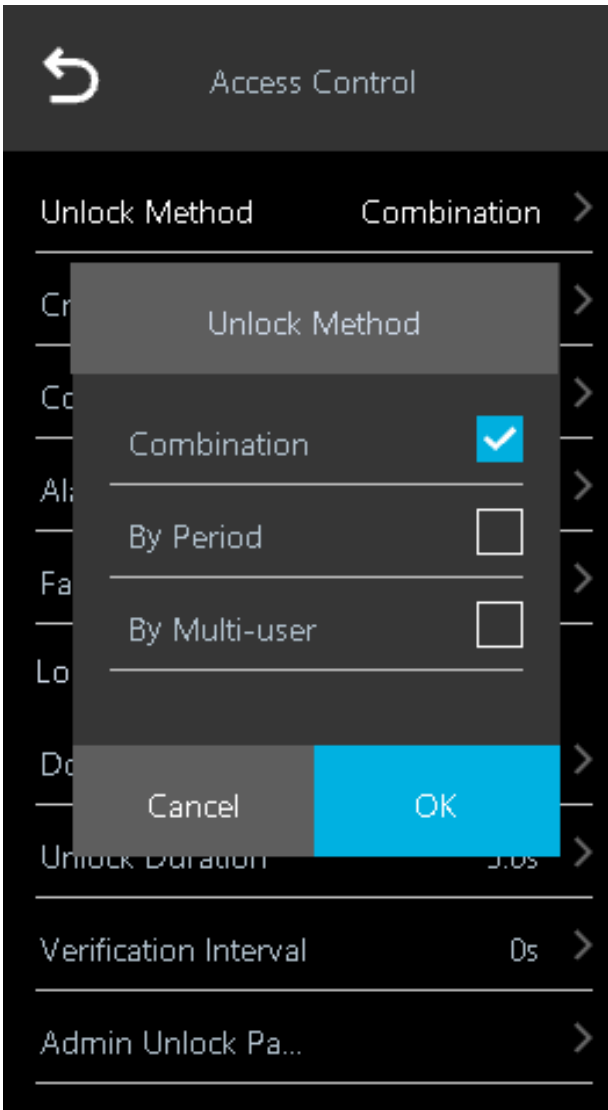
Combination

Unlock the door using a card, face recognition, a password, or a combination of these. The available unlocking modes may vary depending on the product model.

Process

- 1. Select **Access Control** on the main menu.
- 2. Tap **Unlock Method**, select **Combination** from the list, then tap **OK**.

Combination unlock



- 3. Tap **Credentials** to select unlock combination, then tap **OK**.
- 4. Tap **Combination Method**, select **And** or **Or**, then tap **OK**.
 - **And**: Verify all the selected unlock methods to open the door.



NOTE

Users must complete the verification in the order of card, face, and password.

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

By Period

Process

- 1. Select **Access Control** on the main menu.
- 2. Tap **Unlock Method**, then select **By Period** from the list.
For details on how to configure unlock by period, refer to "Unlock Settings".
- 3. Tap **OK**.

By Multi-user

Process

- 1. Select **Access Control** on the main menu.
- 2. Tap **Unlock Method**, then select **By Multi-user** from the list.
For details on how to configure unlock by multiple users, refer to "Unlock Settings".
- 3. Tap **OK**.

Alarms

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

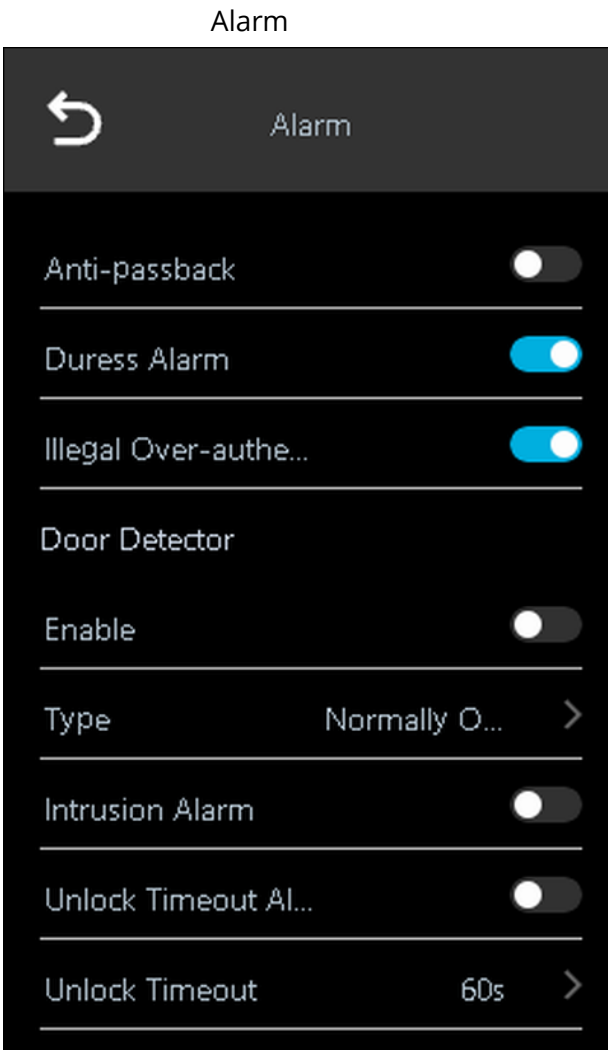
Process

- 1. Go to **Access Control > Alarm** on the main menu.
- 2. Enable the alarm type.



NOTE

The type of alarm may vary depending on the product model.



Description of alarm parameters	
Parameter	Description
Anti-passback	Users are required to verify their identity when entering and exiting; otherwise, an alarm will be triggered. This helps prevent cardholders from handing their cards to others to allow them entry. When the reverse passage feature is enabled, cardholders must exit the secure area through the exit card reader before the system will allow them to enter again. People need to swipe their cards on the "in" card reader to access the secure area and swipe their cards on the "out" card reader to leave the area. • If a person enters after verification but exits without verification, an alarm will be triggered if they attempt to enter again, and they will be denied entry. • If a person enters without verification but exits after verification, an alarm will be triggered if they attempt to enter again, and they will be denied entry.  NOTE If the device can only connect to one lock, verifying through the device means that a person is entering from the "in" direction, while verifying through the external card reader means they are exiting from the "out" direction. This is the default setting.
Duress Alarm	An alarm will be triggered when a duress card or duress password is used to unlock the door.
Illegal Over-authentication Alarm	If the wrong password or card is entered consecutively 5 times within 60 seconds, an alert for excessive use of an invalid card will be triggered and will last for a period of time.
Door Detector	By connecting a door detector to your device, an alarm can be triggered when the door is opened or closed abnormally. There are two types of door detectors: normally closed detectors and normally open detectors.
Type	• Normally Closed: A short circuit in the sensor indicates that the door is close. • Normally Open: An open circuit indicates that the door is open.
Intrusion Alarm	If the door opens abnormally, an intrusion alarm will be triggered and will last for a defined period of time.

Face Recognition Terminal User Manual

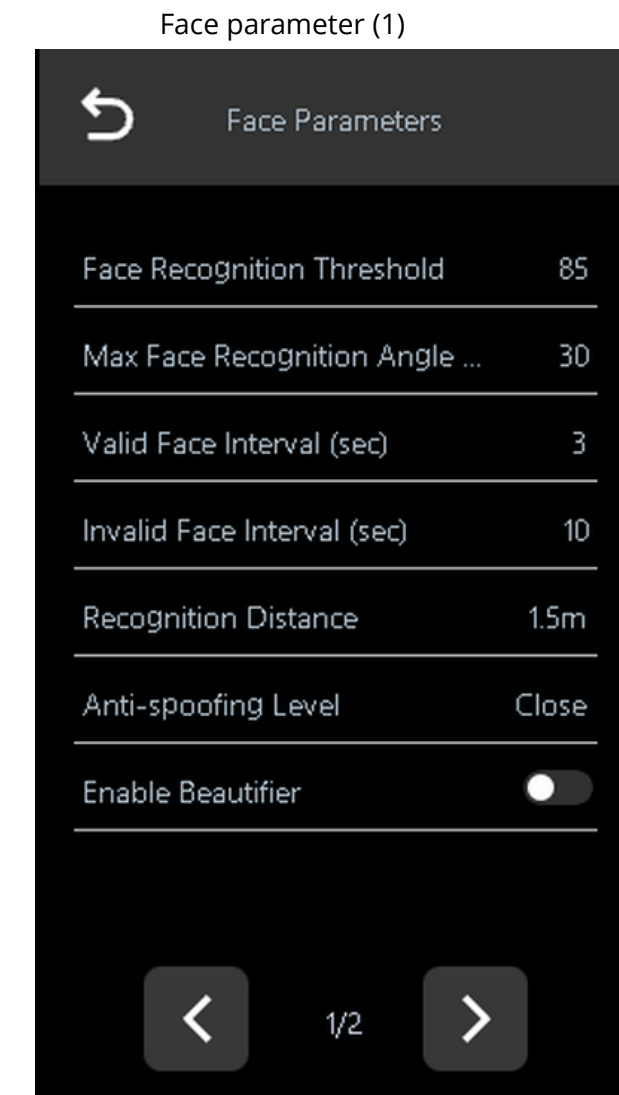
Parameter	Description
Unlock Timeout Alarm	When the door remains in an unlocked state for longer than the defined timeout duration, the door timeout alarm will be triggered and will last for the defined period
Unlock Timeout	 NOTE The door detector and door timeout function need to be enabled simultaneously.

Face Parameters

Face parameters may vary depending on the device model.

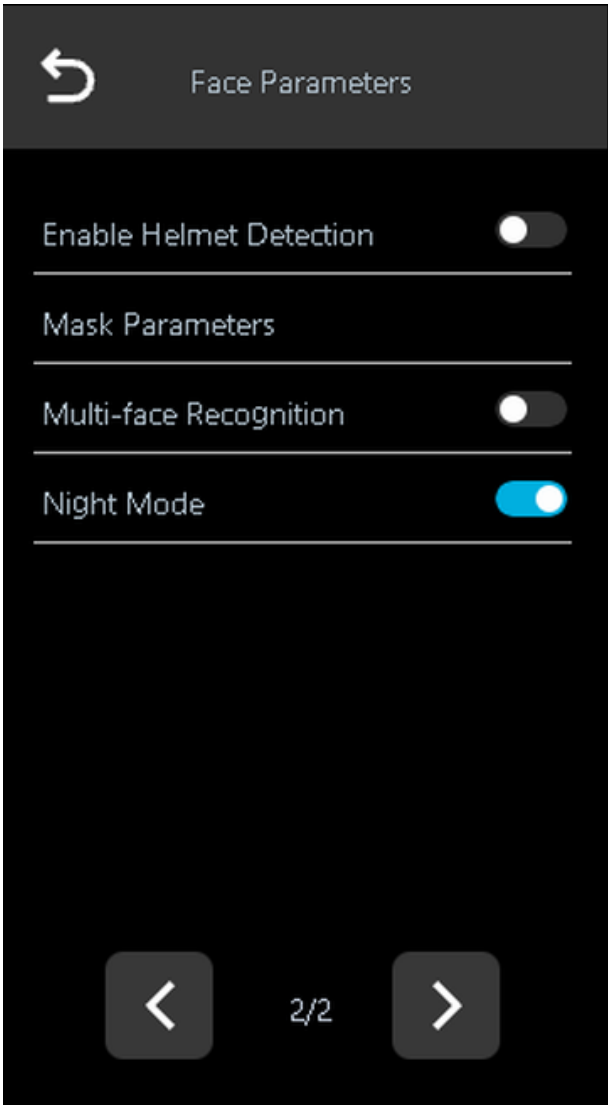
Process

1. Go to **Access Control > Face Parameters** on the main menu.
2. Configure the face parameters, then tap .



Face Recognition Terminal User Manual

Face parameter (2)



Description of face parameters

Name	Description
Face Recognition Threshold	Adjust the accuracy level of face recognition. A higher threshold means higher accuracy and a lower false recognition rate. NOTE When the threshold is too low, for example, at 0, the error recognition rate will be extremely high. Please take note.
Max Face Recognition Angle Deviation	Set the maximum angle at which the face can be presented during face detection. The larger the value, the greater the range of face angles. If the angle of the face is not within the defined range, it may not be detected correctly.

Name	Description
Valid Face Interval (sec)	When the same face appears in front of the camera again after being successfully recognized for the first time, the device will re-identify that face after a defined time interval.
Invalid Face Interval (sec)	When the same face appears in front of the camera again after the first recognition attempt fails, the device will attempt to recognize that face again after a defined time interval.
Recognition Distance	The distance between the face and the lens.
Anti-spoofing Level	This prevents individuals from using photos, videos, masks, and other substitutes to gain unauthorized access.
Enable Beautifier	Beautify the captured facial images.
Enable Helmet Detection	Detecting safety helmets. Individuals not wearing helmets cannot unlock the door.
Mask Parameters	- Mask mode: No Detect: No mask detected during the facial recognition process. Mask Alert: A mask has been detected during the facial recognition process. If the individual is not wearing a mask, the system will remind them to wear one, but will still allow them to enter. Mask Required: A mask is detected during the facial recognition process. If an individual is not wearing a mask, the system will remind them to wear one and deny them entry. - Mask Recognition Threshold: The higher the threshold, the greater the accuracy of facial recognition when a person wearing a mask is identified, and the lower the misidentification rate will be.
Multi-face Recognition	Up to 4 to 6 facial images can be detected at a time. This feature cannot be used in And combination unlock method; the door will be unlocked when one of the individuals is successfully verified. NOTE The number of supported facial images may vary depending on the product model.

Face Recognition Terminal User Manual

Name	Description
Night Mode	- Turn on: The illuminator is turned on under low-light conditions. - Turn off: The illuminator is always in the off state.  NOTE This feature is only available on specific models.

Lock Status Config

Process

1. Select **Access Control** on the main menu.
2. Set the door status.

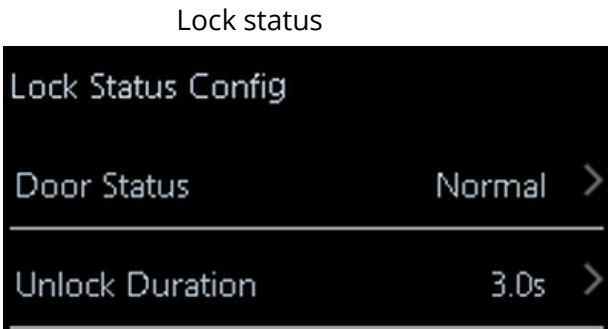


Table 2-5 Parameters description

Parameter	Description
Door Status	Normally Open: The door remains in an unlocked state at all times. Normally Closed: The door remains in a locked state at all times. Normal: If Normal is selected, the door will be locked and unlocked according to your settings.
Unlock Duration	Once a person has been granted access, the door will remain unlocked for a period of time to allow them to pass through.

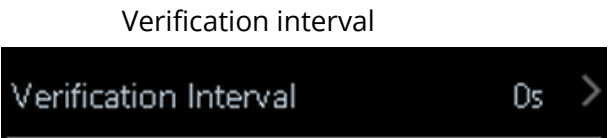
Verification Time Interval

If you verify your identity multiple times within a defined period, only the earliest verification will be

considered valid, and the door will not open after the second or later verifications.

Process

1. Select **Access Control** on the main menu.



2. Enter the time interval, and then tap .

Administrator Password

You only need to enter the administrator password to unlock the door. This password is not restricted by user type. Each device allows only one administrator to unlock the password.

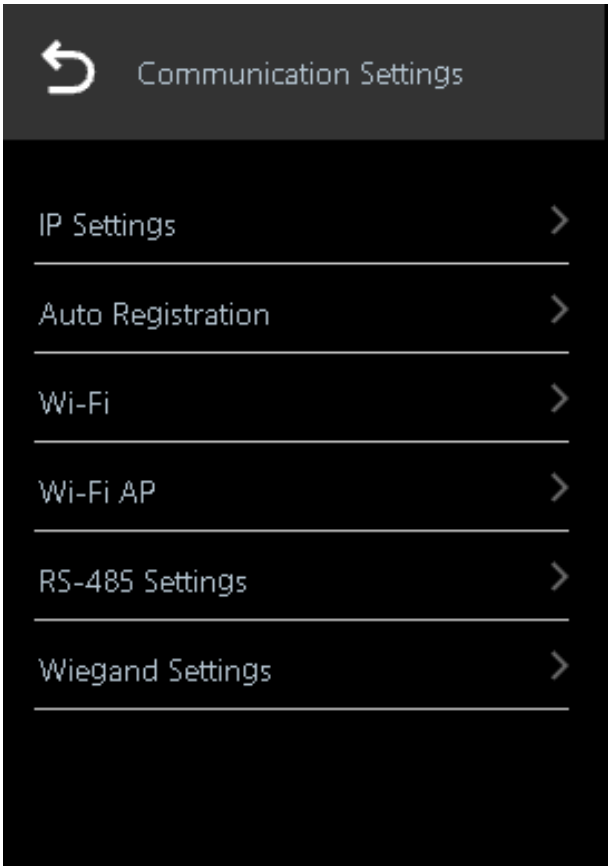
Process

1. Select **Access Control** on the main menu.
2. Tap **Admin Unlock Password**, then tap **Public Password** to enter a password.
3. Enable the Administrator password function.

Communication Settings

Configure the network, RS-485 and Wiegand.

Communication Settings



 NOTE

The RS-485 port and the Wiegand port may vary depending on the device model.

Network Settings

Configure IP address, auto registration, Wi-Fi and Wi-Fi AP.

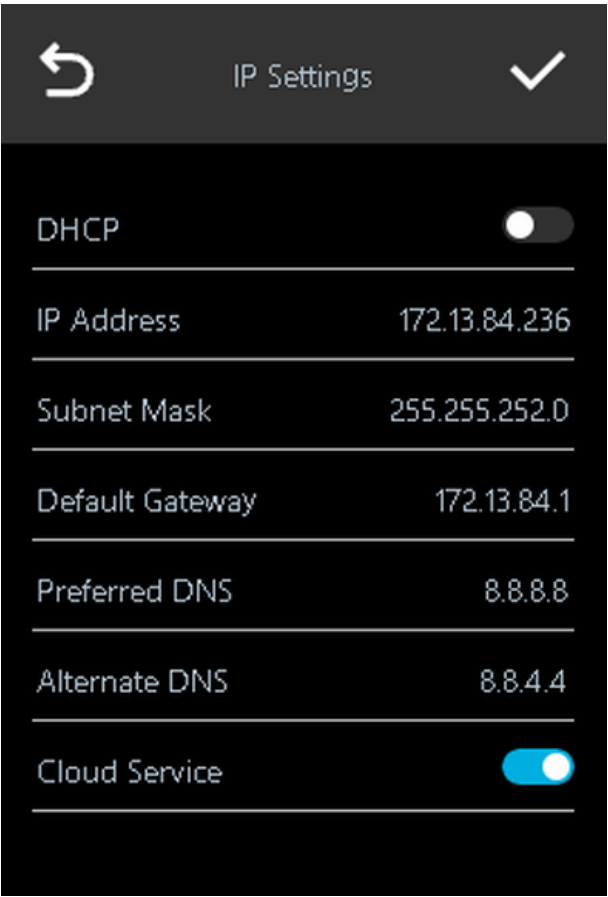
IP Settings

Set an IP address for the device to connect it to the network. After that, you can log in to the web page and management platform to manage the device.

Process

- 1. Go to **Communication Settings > IP Settings** on the main menu.
- 2. Set the IP address.

IP address



IP configuration parameters

Parameter	Description
DHCP	Dynamic Host Configuration Protocol. When DHCP is enabled, the device will automatically assign an IP address, subnet mask, and gateway.
IP Address/Subnet Mask/Gateway Address	The IP address, subnet mask, and gateway IP address must be on the same network segment.
Preferred DNS	IP of the DNS server.
Alternate DNS	The backup IP of the DNS server.
Cloud Service	Manage devices without applying for DDNS, set port mapping and deploy transit servers.

- 3. Tap .

Face Recognition Terminal User Manual

Auto Registration

Add the device to a management platform and you can manage it on the platform.

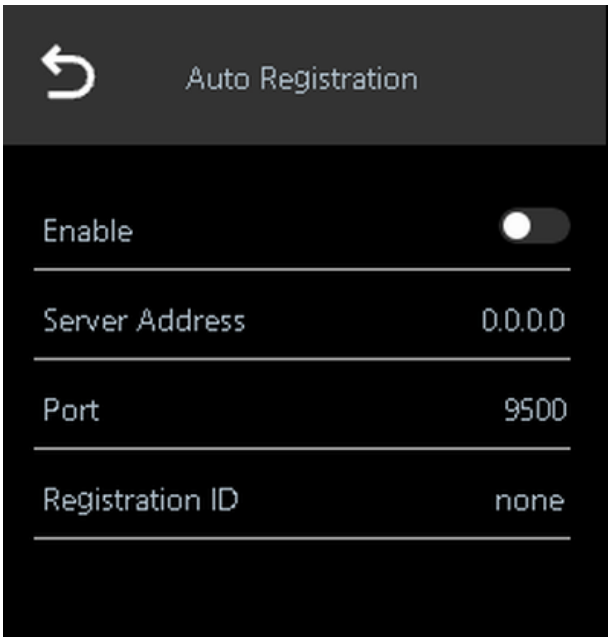
Process

1. Go to **Communication Settings > Auto Registration** on the main menu.



To avoid security risks and data loss for the system, control the permissions of the management platform.

Active registration



2. Enable the automatic registration feature and set the parameters.

Auto registration

Parameter	Description
Server Address	The IP address of the management platform.
Port	The port number of the management platform.
Registration ID	Enter the device ID (user defined). NOTE When you add a device to the management platform, the registration ID you enter on the management platform must match the registration ID defined on the device.

Wi-Fi

You can connect the device to the network via a Wi-Fi network.

Background Information



This feature is only available on specific models.

Process

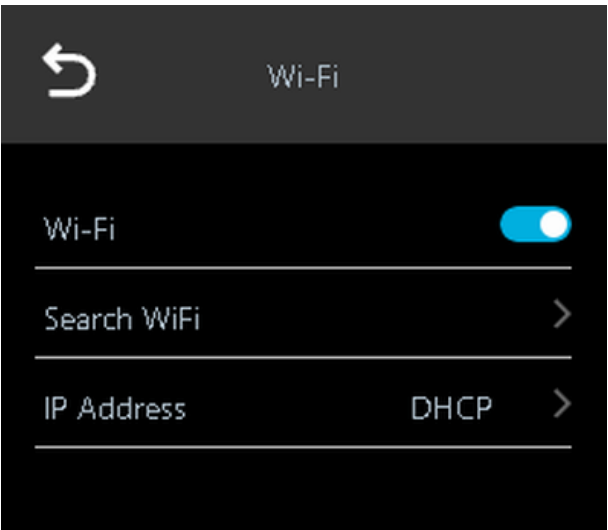
1. Go to **Communication Settings > Wi-Fi** On the main menu.
2. Enable Wi-Fi.



- The Wi-Fi function is only available on certain models.
- Wi-Fi AP and Wi-Fi function cannot be enabled simultaneously.
- After Wi-Fi is enabled, wait about 1 minute to connect Wi-Fi.

3. Tap **Search WiFi** to search for available wireless networks.
4. Select a WiFi and enter the password.

Connect to Wi-Fi



Related Operations

Tap **IP Address** to enable/disable DHCP: Once this feature is enabled, the device will automatically assign Wi-Fi addresses.

Wi-Fi AP

Use your PC or mobile device to connect to the device's Wi-Fi access point to access its webpage.

Face Recognition Terminal User Manual

This feature is only available on specific models.

Process

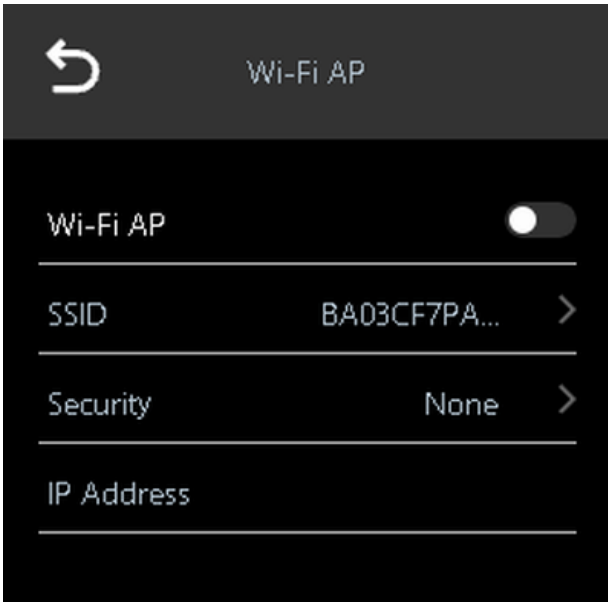
1. Go to **Communication Settings > Wi-Fi AP** on the main menu.
2. Enable Wi-Fi AP.
Configure **Security** of the Wi-Fi AP.
Select **None** to directly connect to the Wi-Fi AP. Select **WPA2-Personal** to configure the password and connect to the Wi-Fi AP through the password.



NOTE

- Wi-Fi AP and Wi-Fi function cannot be enabled simultaneously.
- Every time you turn on the device, the Wi-Fi AP function will be automatically enabled for 30 minutes.

Connect to Wi-Fi AP



Related Operations

You can also tap the right corner on the standby screen to view the Wi-Fi AP status. If you wish to configure the parameters, please log in to the main menu first.

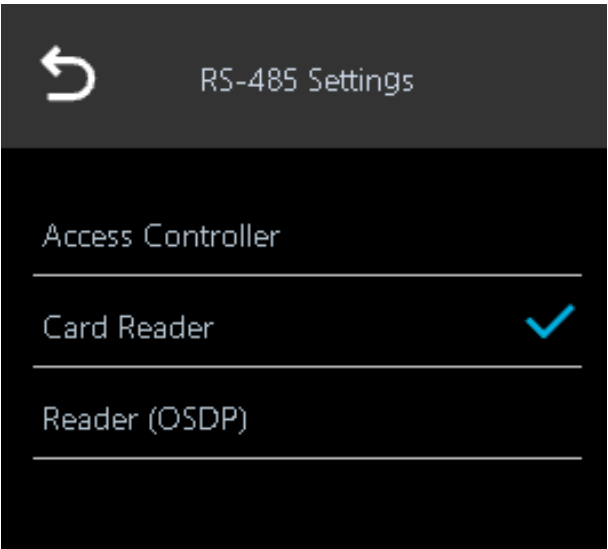
RS-485 Settings

This feature is only available on specific models.

Process

1. Go to **Communication Settings > RS-485 Settings** on the main menu.
2. Select an external device.

External device type



Port description

External device	Description
Access Controller	The device serves as a card reader, sending data to other external access controllers to control access. Output Data Type: • Card Number: When the user unlocks the door by swiping the card, data is output based on the card number; when the user uses other unlocking methods, data is output based on the user's first card number • No.: Outputs data based on the user ID.  NOTE • After successful verification on the device, the data will be transmitted to the access controller. The verification results displayed on the device reflect the results from the access controller. • After the verification fails on the device, the data will not be transmitted to the access controller, and the result on the device will be a failure.
Card Reader	The device serves as an access controller and is connected to an external card reader.
Reader (OSDP)	The device is connected to a card reader based on the OSDP protocol.

Wiegand Settings

The device supports Wiegand input and output modes.

 NOTE

This feature is only available on specific models.

Process

1.

Select **Communication Settings** > **Wiegand Settings** on the main menu.
2.

Select a Wiegand.

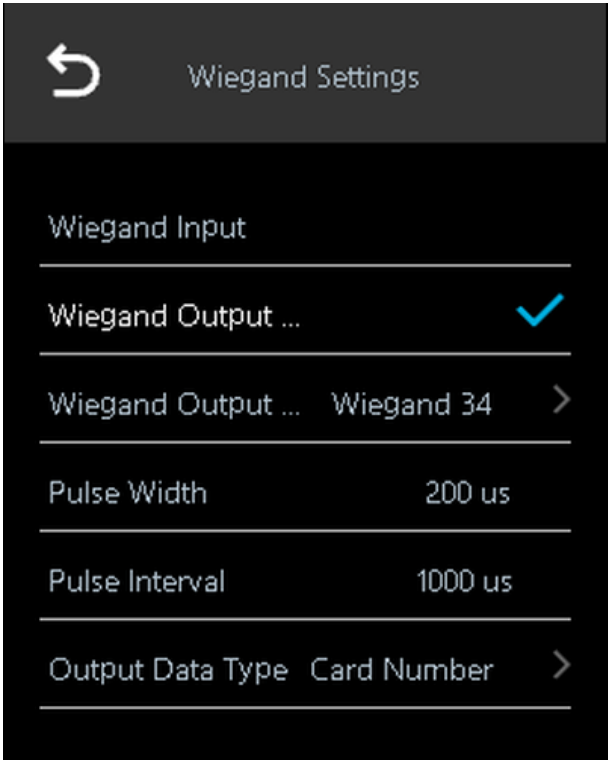
- When you connect an external card reader to the device, please select **Wiegand Input**.

 NOTE

When the device is connected to a third-party device via the Wiegand input port, the **Card No. Inversion** function can be enabled if the card number read by the device is in the reverse order of the actual card number.

 - When the device is used as a card reader, please select **Wiegand output** and connect it to the controller or other access terminal.

Wiegand output



Description of Wiegand output

Parameter	Description
Wiegand Output Type	Select a Wiegand type to read ID numbers or card numbers. 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.
Pulse Interval	
Output Data Type	Select the output data type. User ID: 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.

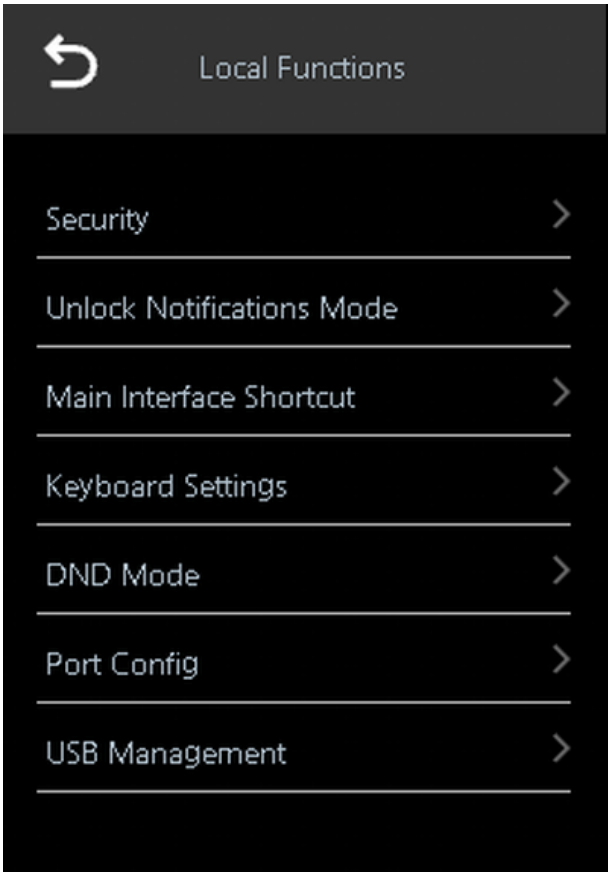
Local Functions

Select **Local Functions** on the main menu screen.

 NOTE

Functions may vary by product model.

Functions



Function description

Parameter	Description
Security	• Password Reset: When you enable this feature, you can reset your password. • Enable HTTPS: Hypertext Transfer Protocol Secure (HTTPS) is a protocol used for secure communication over a computer network. When HTTPS is enabled, CGI commands will be accessed using HTTPS; otherwise, HTTP will be used.  NOTE The device will automatically restart when HTTPS is enabled. • Enable CGI: The Common Gateway Interface (CGI) provides a standard protocol for web servers to execute programs, similar to how console applications run on servers that dynamically generate web pages. CGI is enabled by default. • Enable SSH: The Secure Shell Protocol (SSH) is an encrypted network protocol used to securely operate network services over an insecure network. Once this feature is enabled, the data transmitted will be encrypted. • Capture: Facial images will be automatically captured when individuals unlock the door. • Clear all snapshots: Delete all automatically captured photos.

Parameter	Description
Unlock Notifications Mode	On the device, when a person is verifying their identity, a notification will be displayed on the screen. • 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.

Parameter	Description
Main Interface Shortcut	Select the authentication method on the standby screen. • Password: The icon will be displayed on the standby screen. • Doorbell: The icon will be displayed on the standby screen. ◊ Local Device Ringer: Tap the ring bell icon on the standby screen and the device will ring. ◊ Ringtone Config: Select a ringtone. ◊ Ringtone Time (sec): Set the ringtone duration (1-30 seconds). The default value is 3. • Call: The icon will be displayed on the standby screen. • Call Type ◊ 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. ◊ Call Phone: Tap the call icon on the standby screen to call the phone.  NOTE You can call LumiViewer only in this call type. • SIP Server: Enable SIP to set the device to SIP server.
Keyboard Settings	Select from 9-Key keyboard or 26-Key keyboard .
DND Mode	There are no voice prompts during the specified time for identity verification on your device. You can set up to 4 periods.
Port Config	Select the functions that can be used for this port.  NOTE • Display Port Config when the cable can be used for different functions. • The functions may vary depending on the actual device model.

Parameter	Description
USB Management	USB Export Export the data from the device to a USB. The exported data is encrypted and cannot be edited. Select the type of data you want to export, then tap OK.  NOTE - When the data is exported in Excel, it can be edited. - The USB disk supports the FAT32 format, with storage capacities ranging from 4 GB to 128 GB. During export, personal data, facial attributes, and card data have all been encrypted.
	USB Import Import data from USB to the Device. Select the type of data you want to export, then tap OK.
	USB Update Update the device's system through USB. - Rename the update file to "update.bin" and place it in the root directory of the USB, then insert the USB into the device. - Tap USB Update, and after the update is complete, the device will restart.  NOTE During the update, please do not turn off the device.

Reports

View unlock records and data capacity.

Unlock Records

Select **Reports > Unlock Records** on the main menu. The unlock records will be displayed. You can search for records by user ID.

System Capacity

Go to **Reports > System Capacity** on the main menu, you can view storage capacity of each data

type.

System Settings

Time

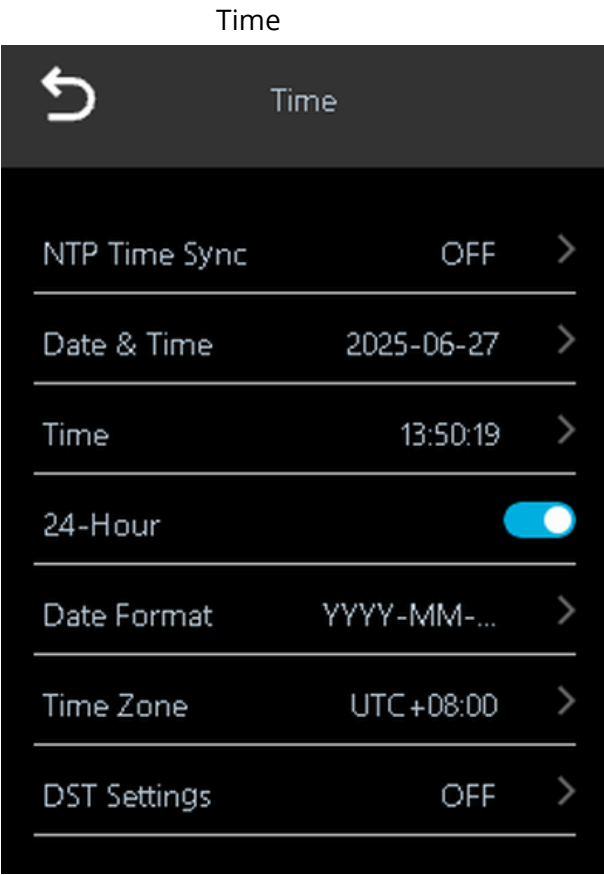
Configure system time, such as date, time, and NTP.

Process

1.

Go to **System Settings > Time** on the main menu.
2.

Configure system time.



Description of time parameters

Parameter	Description
NTP Time Sync	The Network Time Protocol (NTP) server is a machine specifically designated as the time synchronization server for all client computers. If your computer is configured to synchronize with a time server on the network, your clock will display the same time as the server. When the administrator changes the time (for example, for daylight saving time), all client machines on the network will also be updated. 1. Tap Time Sync, then enable it. 2. Configure the related parameters. • Server Address: Enter the IP address of the NTP server, and the device will automatically synchronize the time with the NTP server. • Port: Enter the port of the NTP server. • Interval: Enter the time synchronization interval.
Date & Time	Set the date.
Time	Set the time.
24-Hour	The time will be displayed in 24-hour format.
Date Format	Select the date format.
Time Zone	Select the time zone.
DST Settings	1. Tap DST Settings and enable it. 2. Select Date or Week from the DST Type list. 3. Enter the start time and end time. 4. Tap ☒.

Volume Settings

Process

1.
- Go to **System Settings > Volume Settings** on the main menu.
2.
- Configure the related parameters.

Parameters description

Parameters	Description
Screen Tap Sound	When this function is enabled, touch screen devices will emit a tapping sound, while non-touchscreen devices will produce a mouse click sound.

Parameters	Description
Speaker Volume	Tap the volume, then tap  or  to adjust the volume.
Microphone Volume	

Language

Change the device language. Go to **System Settings > Language** on the main menu, select the device's language.

Screen Settings

Configure the time for the display monitor to turn off and the logout time.

Process

1.
- Go to **System > Screen Settings** on the main menu.
2.
- Tap  or  to adjust the time or screen brightness.
 - **Logout:** The system returns to the standby screen after the defined period of inactivity.
 - **Screen off settings:**

The system will return to the standby screen, and then the screen will turn off after the defined inactive period. For example, if the logout time is set to 15 seconds and the screen off time is set to 30 seconds, the system will return to the standby screen after 15 seconds, and then the screen will turn off after another 15 seconds.

 NOTE

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

Factory Defaults

 CAUTION

Restoring the device to factory settings may result in data loss. Please be aware.

Restore through the Software

1.
- Go to **System Settings > Factory Defaults** on the main menu.
2.
- If necessary, please restore the factory settings.
 - **Factory Defaults:** Reset all configurations and data, but retain IP settings and expansion module types.
 - **Restore to Default Settings (Except for User Information and Logs):** Reset all configurations, excluding user information and logs.

Face Recognition Terminal User Manual

Restore through the Hardware

The device supports the tamper and reset button.

- Tamper button: Within 5 minutes after the device is powered on, if the tamper button is pressed 5 times within 8 seconds, the device will display a prompt. Click **OK** or press the tamper button once, and the device will restart. All configurations and information will be restored to factory settings.
- Reset hole: To reset the device, you need to short it by inserting a pin into the pinhole.
 - ◊ If you wish to perform a partial reset while retaining user information, logs, and IP configuration, you must insert the pin for 500 milliseconds.
 - ◊ If you wish to perform a complete reset, the inserted pin must be held for 5 seconds.



The reset pinhole is available on certain models.

About

Go to **System Settings** > **About** on the main menu, you can view the device version, such as SN, software version and more.

Restart

Go to **System Settings** > **Restart** on the main menu, and the device will be restarted.

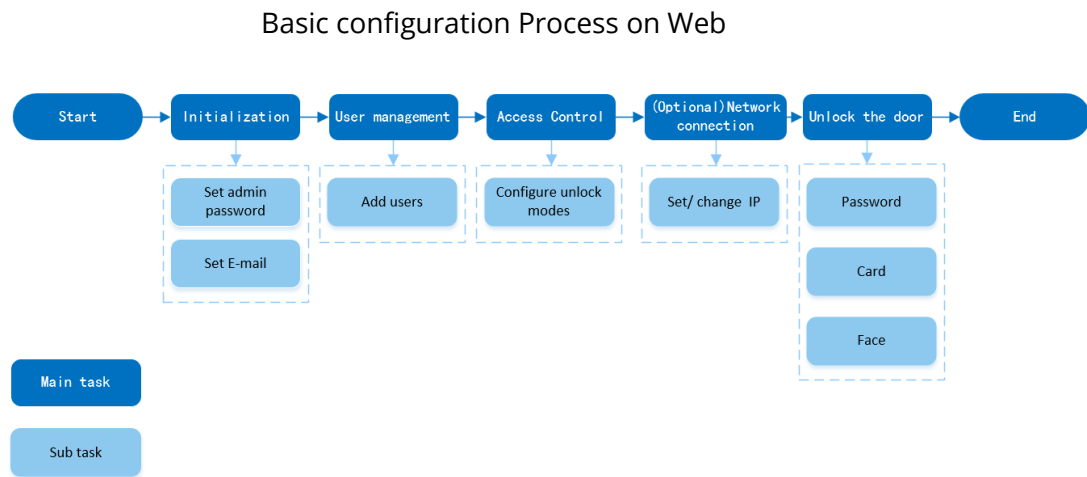
Web Operations

You can also configure and update the device on the webpage.

NOTE

- Web configurations varies by device model.
- Some functions are currently exclusive to the web interface and unavailable on local device.

Basic Configuration Process on Web



Initialization

Initialize the device after the first login to the webpage or after the device has been restored to factory settings.

Precondition

Ensure that the computer and device used to log in to the webpage are on the same local area network.

Process

1. Open a browser and enter the IP address of the device.

NOTE

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

2. Select a language for the device.
3. Set up your password and email address according to the instructions on the screen.

NOTE

- The password must consist of 8 to 32 non-empty characters and must include at least two of the following types of characters: uppercase letters, lowercase letters, numbers, and special characters (excluding ' " ; &). Please set a high-security password according to the password strength guidelines.
- After initialization, please keep the password secure and change it regularly to enhance security.

4. Select **Auto check for Updates**, the system will notify when a version update is detected. Then click **Completed** to finish initialization.

Log In

Process

1. Open the browser, enter the device's IP address in the address bar, and then press the Enter key.
2. Enter the user name and password.

NOTE

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

3. Click **Login**.

Password Resetting

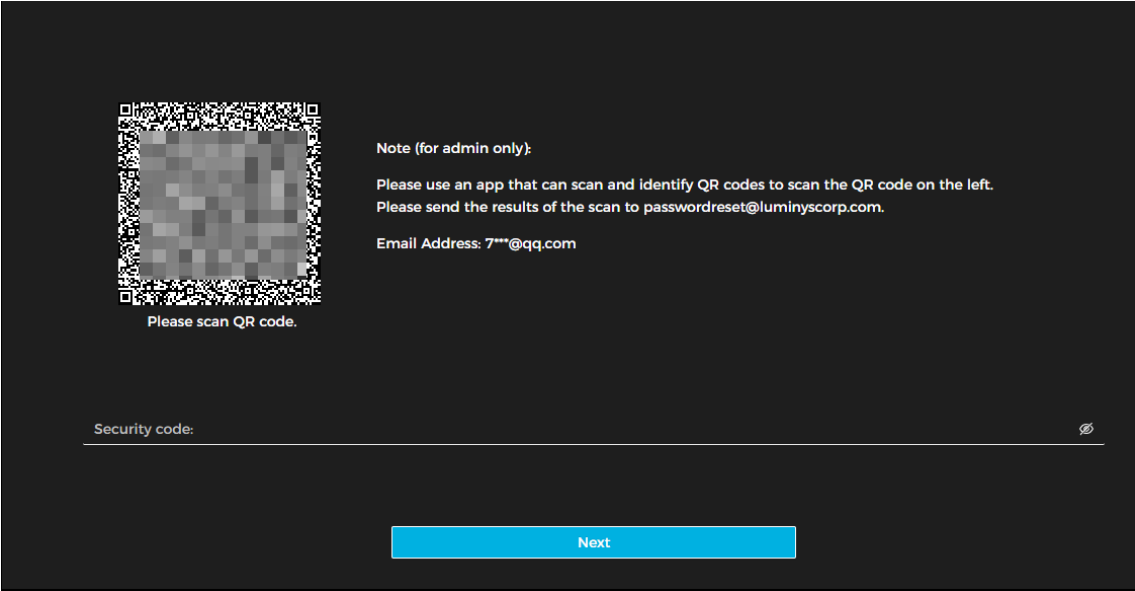
When you forget the administrator password, please reset it through the associated email.

Process

1. Click **Forgot password** on the login page.
2. Carefully read the prompts on the screen, then click **OK**.
3. Scan the QR code, and you will receive a security code.

Face Recognition Terminal User Manual

Reset password



NOTE

- When scanning the same QR code, a maximum of two security codes will be generated. If the security code becomes invalid, please refresh the QR code and scan it again.
- After scanning the QR code, you will receive a security code sent to your associated email address. Please use the security code within 24 hours of receiving it; otherwise, the code will expire.
- If the incorrect security code is entered consecutively 5 times, the administrator account will be frozen for 5 minutes.

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

NOTE

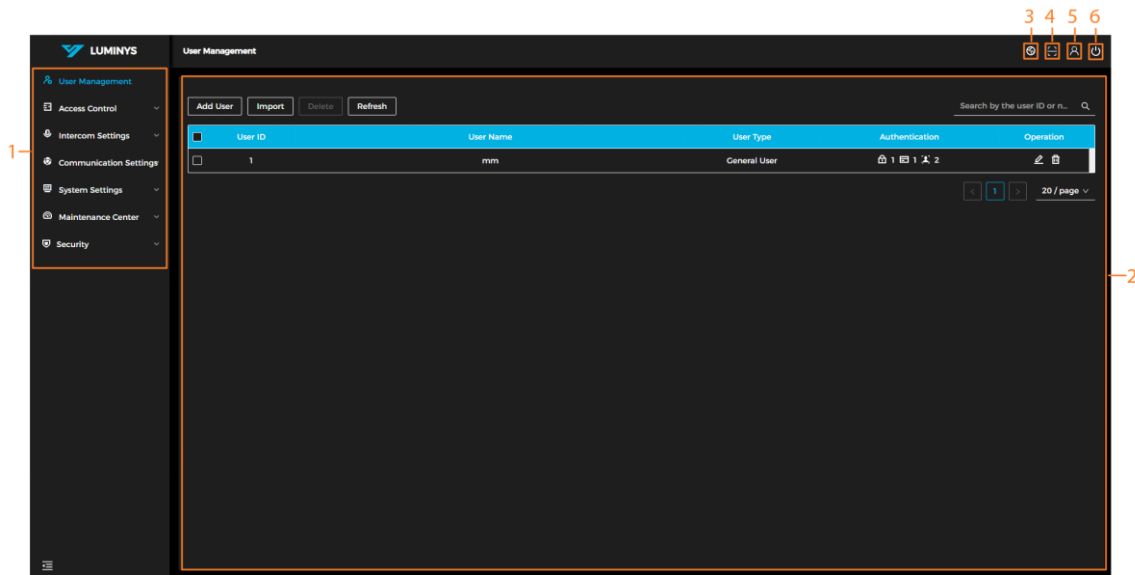
Passwords should consist of 8 to 32 non-empty characters and must include at least two of the following four character types: uppercase letters, lowercase letters, numbers, and special characters (excluding ' " ; : &).

7. Click **OK**.

Home Page

After successfully logging in, the homepage will be displayed.

Home page



Home page description

No.	Description
1	Function list.
2	Details of the functions.
3	Select a language for the device.
4	Scan the QR code with your phone to download the mobile APP or get the device SN.
5	Select the account.
6	Log out or restart the device.

User Management

Process

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

Face Recognition Terminal User Manual

Add

Basic Info

User ID

User Name

Valid from

06-24-2025 12:00:00 AM

Valid to

12-31-2037 11:59:59 PM

User Type

General User

Times Used

Unlimited

Weekly Schedul...

255-Full Day

Holiday Schedu...

255-No Plan

Permission

User

Authentication

Face

Not Added

+
Upload

The image size must not exceed 100KB. Supported formats: jpg,jpeg,png.

Password

Not Added

Card

Not Added

Add

Add More

Cancel

Parameters description

Parameter	Description
User ID	The user ID is similar to the employee ID and can consist of a combination of numbers and letters, with a maximum length of 30 characters.
User Name	The name can contain a maximum of 32 characters (including numbers, symbols, and letters).
Valid from	Set a period on which the door access permissions of the user will be expired.
Valid to	

Parameter	Description
User Type	General User: General users can unlock the door. VIP User: If the door is in "Normal" status, VIP users can open it at any time, regardless of other rules. Guest User: Guests can unlock the door within a defined period or for certain amount of times. Once the specified time expires or the number of unlocks is exhausted, they will no longer be able to unlock the door. Blocklist User: When users in the blocklist unlock the door, service personnel will receive a notification. Other User: When they unlock the door, the door will remain unlocked for 5 seconds.
Times Used	Set an unlock limit for guest users. After the unlock times run out, they cannot unlock the door.
Permission	User: Users only have door access permissions. Admin: Administrators can configure the device besides door access permissions.
Weekly Schedule	People can unlock the door within the specified time. NOTE You can select multiple plans.
Holiday Schedule	People can unlock the door during the defined holiday. NOTE You can select multiple holidays.
Face	Click Upload to upload a face image. Each person can add a maximum of 2 facial images. After uploading, you can view or delete the facial images. NOTE Facial images must be in jpg, jpeg, or png format, and the size must not exceed 100 KB.
Password	Enter the user password. The maximum length of the password is 8 digits. The emergency password is the unlock password plus 1. For example, if the user password is 12345, the emergency password will be 12346. When the door is unlocked using the emergency password, an emergency alarm will be triggered.

23

Parameter	Description
Card	NOTE This feature is only available on specific models. Manually enter the card number. 1. Click Add. 2. Enter the card number, then click Add. Automatically read numbers through registered readers or devices. 1. Click Add, then click Modify to select an enrollment reader or the Device. 2. Click Read Card, and then swipe cards on the card reader. Display a 60-second countdown to remind you to swipe the card, and the system will automatically read the card number. If the 60-second countdown expires, please click to Read Card again to start a new countdown. 3. Click Add. Users can register up to 5 cards. Please enter your card number or swipe the card, and the device will read the card information.

3. Click **Add**.
- Click **Add More** to add other users.

Related Operations

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



NOTE

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

- Delete: Delete the selected users.

Refresh: Refresh the user list.

Search by user name or user ID.

Access Control

Door Parameters

Basic Settings

Process

1. Go to **Access Control > Door Parameters**.
2. In **Basic Settings**, configure basic parameters for the access control.

Basic settings

Basic Settings

Name

Door1

Door Status

Normal

Always Locked

Always Unlocked

Normally Unlocked Period

Weekly Schedule

Disabled

Holiday Schedule

Disabled

Normally Locked Period

Weekly Schedule

Disabled

Holiday Schedule

Disabled

Unlock Notifications Mode

High Speed Mode

Verification Interval

0

s (0-180)

Card Swiping Interval

0

s (0-86400)

Basic parameters description

Parameter	Description
Name	The door's name.
Door Status	Set the door status. Normal: The door will be locked and unlocked according to your settings. Always Locked: The door remains locked all the time. Always Unlocked: The door remains unlocked all the time.

Parameter	Description
Normally Locked Period	during the defined time. NOTE - When normally unlocked period conflicts with normally locked period, normally open period takes priority over normally closed period. - When the weekly schedule conflicts with the holiday schedule, the holiday plan takes priority over the general plan.
Unlock Notifications Mode	Display a notification on the screen when verifying identity on the device. - 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.
Verification Interval	If you verify your identity multiple times within the specified time frame, only the earliest verification will be considered valid, and the second or subsequent verification attempts will not unlock the door. From the moment the door fails to open, you must wait for the configured verification time interval before you can attempt to verify your identity again.

Parameter	Description
Card Swiping Interval	When verifying for the first time using the card, you can typically unlock the door or record attendance, and generate a record. During the configured time period, if you swipe the card again for verification, you will not be able to unlock the door or record attendance, and no record will be generated. Please perform the verification after the configured time period. NOTE The Card Swiping Interval takes priority over Verification Interval.

3. Click **Apply**.

Unlock Settings

Use various unlocking methods to open the door, such as cards and passwords. You can also combine them to create your own personal unlocking method.

Process

1.

Go to **Access Control > Door Parameters**.
2.

In **Unlock Settings**, select an unlock mode.
 - Combination unlock

1. In the **Unlock Mode** list, select **Combination**.

2. Select combination method.

Or: Use one of the selected unlock methods to open the door.

And: Use all the selected unlock methods to open the door.

3. Select unlock methods, then configure other parameters.

Unlock settings

Unlock Settings

Unlock Method

Combination

Combination Method

Or

And

Unlock Method (Multi-select)

Card

Face

Password

PIN Code Authentication

Door Unlocked Duration

3.0

s (0.2-600)

Remote Verification

Face Recognition Terminal User Manual

Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	The unlocking method may vary depending on the product model.
PIN Code Authentication	When PIN code authentication is enabled, you can open the door with just the password.
Door Unlocked Duration	Once a person has been granted access, the door will remain unlocked, allowing the person to pass through within a specified time frame. This time range varies from 0.2 seconds to 600 seconds.
Remote Verification	Remote door opening.

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

 NOTE

Click **Copy** to apply the configured time period to other days.

 3. Select the time period for the combination method and unlocking method, then configure the other parameters.

 NOTE

Click **Copy** to apply the configured time period to other days.

Unlock by period

Unlock Method

By Period ▾

Period	Card	Face	Password	Card/Password	Card/Face	Face/Password	Card/Face/Password
Sun							
Mon							
Tue							
Wed							
Thu							
Fri							
Sat							

- Unlock by multi-users.
 1. Select **Multi-users**, in the **Unlock Mode** list.
 2. Click **Add** to add a group.
 3. Select unlock method, valid number and user list.
 - ◇ If only one group is added, the door will only unlock when the number of people in the granted access group equals the defined valid number.
 - ◇ If multiple groups are added, the door will only unlock when the number of people granted access in each group equals the defined valid number.

 NOTE

- ◇ You can add up to 4 groups.
- ◇ The valid number indicates the number of people in each group who need to verify their identity on the device in order for the door to unlock. For example, if the valid number is set to 3 for a group, any 3 people in the group need to verify their identities to unlock the door.

3. Click **Apply**.

Alarm

When an abnormal access event occurs, an alarm will be triggered.

Process

1. Go to **Access Control** > **Alarm** > **Alarm**.
2. Configure alarm parameters.

Alarm

Anti-passback

☒

Duress Alarm

☒

Illegal Over-authentication Alar...

☒

Door Detector

☒ ☒ Normally Open ☐ Normally Closed

Intrusion Alarm

☐

Unlock Timeout Alarm

☐

Unlock Timeout

60

s (1-9999)

Apply

Refresh

Default

Description of alarm parameters

Parameter	Description
Anti-passback	Users are required to verify their identity when entering and exiting; otherwise, an alarm will be triggered. This helps prevent cardholders from transferring their access cards to others for entry privileges. When the anti-passback is enabled, cardholders must exit the secure area through the exit card reader before the system will allow re-entry. • If a person enters after being authorized but exits without authorization, an alarm will be triggered when they attempt to enter again, and access will be denied. • If a person enters without authorization and leaves after obtaining authorization, an alarm will be triggered when they attempt to enter again, and access will be denied simultaneously.  NOTE If the device can only connect to one lock, then verification on the device indicates an entry direction, while verification on the external card reader defaults to an exit direction. You can modify this setting on the management platform.
Duress Alarm	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Illegal Over-authentication Alarm	If the wrong password or card is entered consecutively 5 times within 60 seconds, an alarm for excessive use of an invalid card will be triggered and will last for a period of time.
Door Detector	By connecting a door detector to your device, an alarm can be triggered when the door is opened or closed abnormally. There are two types of door detectors: normally closed detectors and normally open detectors. • Normally Closed: When the door or window is closed, the sensor is in a short-circuit state. • Normally Open: When the window or door is actually closed, it creates an open circuit.

Parameter	Description
Intrusion Alarm	If the door is opened abnormally, an intrusion alarm will be triggered and last for a defined time.  NOTE The door detector and intrusion detection need to be enabled simultaneously.
Unlock Timeout Alarm	When the door remains in an unlocked state for longer than the defined timeout duration, the door timeout alarm will be triggered and will last for the defined period.  NOTE The door detector and door timeout function need to be enabled simultaneously.
Unlock Timeout	

3. Click **Apply**.

Alarm Linkage Setting (Optional)

Configure the alarm linkages.

Process

1. Go to **Access Control > Alarm > Alarm Linkage Setting**.
-  NOTE
 - If the Device is added to a management platform, the alarm settings will be synchronized to the platform.
 - The number of alarm input and output ports varies depending on the product model.
 - This function is only applicable to models with alarm input and alarm output ports.
2. Configure related alarm.

Alarm linkage

Zone1

Name

Zone1

Alarm Input Type

Normally Open

Link Fire Safety Control

Alarm-out Port

Duration

30

s (1-300)

Alarm Output Channel

1

Access Control Linkage

Linkage Mode

Weak Execution

Channel Type

Normally Open

Apply

3. Enter a name for the alarm zone.
4. Enable **Link Fire Safety Control**, and select an alarm input type.
 - Normally Closed: When the alarm is not triggered, the alarm input is in a normally closed circuit state. Opening the normally closed circuit will trigger the alarm.
 - Normally Open: When the alarm has not been triggered, the alarm input device is in a normally open circuit state. Closing the circuit will trigger the alarm.
5. If you want to link access control when the fire alarm is triggered, enable **Access Control Linkage**.
- NOTE

This function only takes effect after **Link Fire Safety Control** is enabled.
6. Select a linkage mode.
 - Strong Execution: When the fire alarm signal disappears, the door remains in its current state. If desired, you can manually change it back to the previous door state setting.
 - Weak Execution: When the fire alarm signal disappears, the door automatically returns to its previous door status.
7. Select a channel type.
 - Normally Open: When fire alarm is triggered, the door will open automatically.

- Normally Closed: When the fire alarm is triggered, the door will close automatically.
8. Click **OK**.

Alarm Event Linkage

Process

1. Go to **Access Control > Alarm > Alarm Event Linkage**.
2. Configure alarm event linkages.

Alarm event linkage

Intrusion Alarm Linkage

Buzzer

Duration

15

s (1-1800)

Link Alarm Output

Duration

15

s (1-1800)

Unlock Timeout Alarm Linkage

Buzzer

Duration

Custom Time

15

s (1-1800)

Link Alarm Output

Duration

15

s (1-1800)

Illegal Over-authentication Alar..

Buzzer

Duration

15

s (1-1800)

Link Alarm Output

Duration

15

s (1-1800)

Tamper Alarm Linkage

Buzzer

Duration

3

s (1-1800)

Link Alarm Output

Duration

15

s (1-1800)

Apply

Refresh

Default

Alarm event linkage

Parameter	Description
Intrusion Alarm Linkage	If the door opens abnormally, it will trigger the intrusion alarm. - Buzzer: When the intrusion alarm is triggered, the buzzer will emit a sound. You can configure the duration of the alarm. - Link Alarm Output: When the intrusion alarm is triggered, external alarm devices will generate an alarm. You can configure the duration of the alarm.

Face Recognition Terminal User Manual

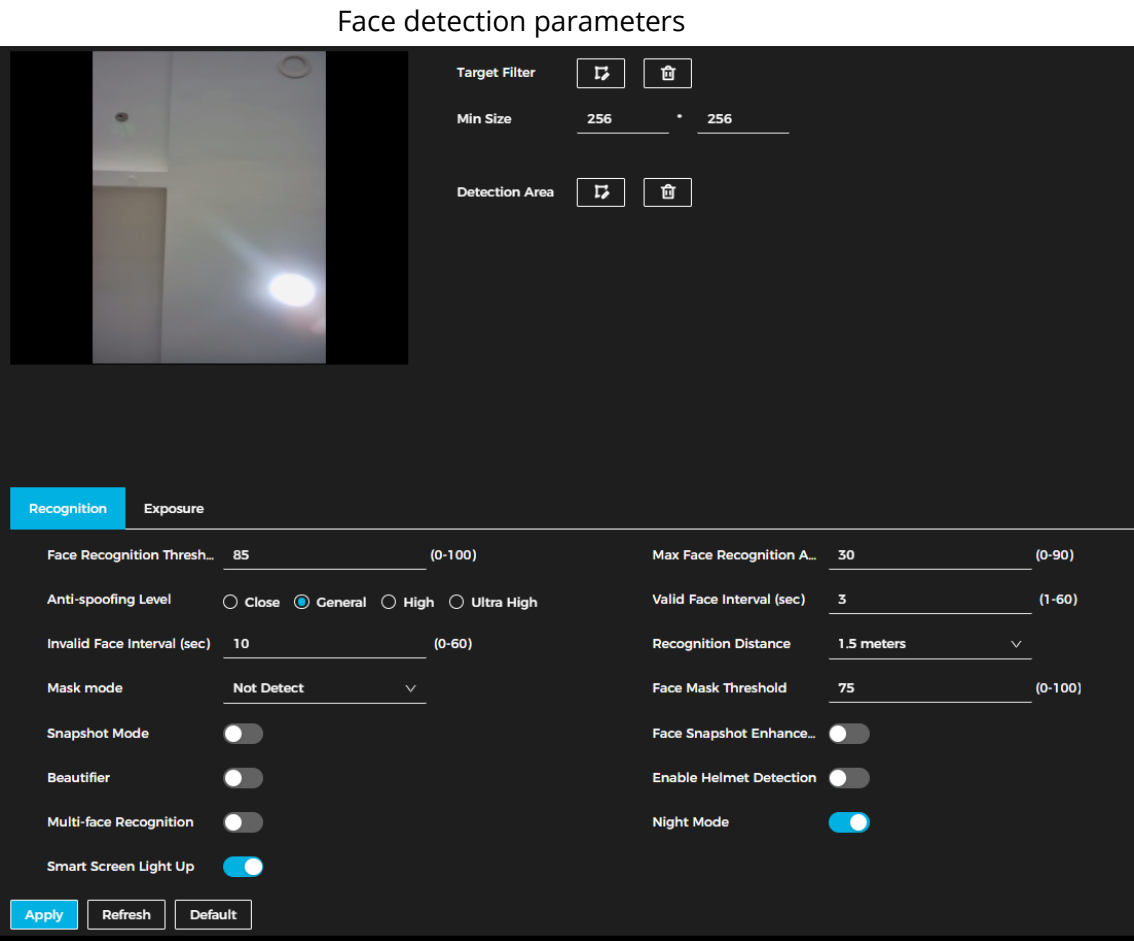
Parameter	Description
Unlock Timeout Alarm Linkage	When the door remains in an unlocked state for longer than the defined timeout duration, the door timeout alarm will be triggered and will last for the defined period. - Buzzer: The buzzer will sound when the unlock timeout alarm is triggered. You can configure the duration of the alarm. - Custom time: Customize the duration. The access controller emits a beep according to the configured time period - Until the door locks: The access controller keeps beeping until the door locks. - Link Alarm Output: The external alarm device generates alarms when the unlock timeout alarm is triggered. You can configure the alarm duration.
Illegal Over-authentication Alarm	If the wrong password or card is entered continuously 5 times within 60 seconds, an alarm for excessive use of an invalid card will be triggered and will last for a period of time. - Buzzer: When the excessive use alarm is triggered, the buzzer will emit a sound. You can configure the alarm duration. - Link Alarm Output: When the unlock timeout alarm is triggered, external alarm devices will generate an alarm. You can configure the duration of the alarm.
Tamper Alarm Linkage	When someone attempts to physically damage the device, the tamper alarm will be triggered. - Buzzer: When the tamper alarm is triggered, the buzzer will emit a sound. You can configure the duration of the alarm. - Link Alarm Output: When the tamper alarm is triggered, external alarm devices will generate an alarm. You can configure the duration of the alarm.

Face Parameters

Configure face detection parameters. Face parameters might differ depending on models of the product.

Process

- Go to **Access Control > Face Parameters**.



- Configure the parameters.

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. NOTE When the threshold is set too low, for example at 0, the error recognition rate will be very high. Please take note.
Max Face Recognition Angle Deviation	Set the maximum angle at which the face can be presented during face detection. The larger the value, the greater the range of face angles. If the angle of the face is not within the defined range, it may not be detected correctly.

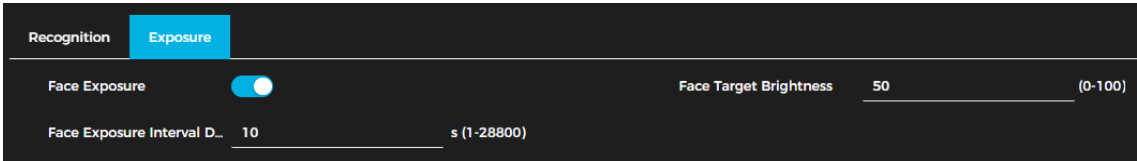
Face Recognition Terminal User Manual

Name	Description
Anti-spoofing Level	Once this feature is enabled, it can prevent individuals from gaining unauthorized access using photos, videos, masks, and other substitutes. After enabling this feature, the frame will not be displayed during non-living verification.
Illuminator	- Turn on: The illuminator is activated under low light conditions. - Turn off: The illuminator is always in the off state.  NOTE This function is only available on specific models.
Valid Face Interval (sec)	When the same face appears in front of the camera again after being successfully recognized for the first time, the device will re-identify that face after a defined time interval.
Invalid Face Interval (sec)	When the same face appears in front of the camera again after the first recognition attempt fails, the device will attempt to recognize that face again after a set time interval. If you configure 0 , the face will not be captured, and there will be no unlocking records.
Recognition Distance	The distance between the face and the lens.
Mask Mode	Not Detect: No mask detected during the face recognition process. Mask Alert: A mask is detected during the face recognition process. If the person is not wearing a mask, the system will remind them to wear one, but will still allow them to enter. Mask Required: A mask is detected during the face recognition process. If a person is not wearing a mask, the system will remind them to wear one and deny them access.
Face Mask Threshold	The higher the threshold, the greater the accuracy of face recognition when a person is wearing a mask, and the lower the rate of misidentification.

Name	Description
Snapshot Mode	After the function is enabled, low-quality snapshots in the unlock records can be filtered out.  NOTE - The function and Multi-face Recognition cannot be enabled simultaneously. - This function is only available on certain models.
Face Snapshot Enhancement	After the function is enabled, the quality and clarity of snapshots in the unlock records will be enhanced.  NOTE The function and Multi-face Recognition cannot be enabled simultaneously.
Beautifier	Beautify captured face images.
Enable Helmet Detection	Detects safety helmet. If the helmet is not worn, the door will not be able to unlock.
Multi-face Recognition	Up to 4 to 6 facial images can be detected at a time. This feature cannot be used in And combination unlock method; the door will be unlocked when one of the individuals is successfully verified.  NOTE The number of supported face images may vary depending on the product model.
Night Mode	In a dark environment, the standby screen displays a white background image to enhance brightness when verifying faces or QR codes.
Smart Screen Light Up	After the function is enabled, the screen will light up when a face is detected while the screen is turned off.

3. Configure the exposure parameters.

Exposure parameters



Face Recognition Terminal User Manual

Exposure parameters description

Parameter	Description
Face Exposure	After enabling the face exposure feature, the face will be exposed at the set brightness to clearly detect the face image.
Face Target Brightness	
Face Exposure Interval Detection	The face will be exposed only once in a defined interval.

4. Draw the face detection area.

1) Click .

2) Right-click to draw the detection area, then release the left mouse button to complete the drawing.

The face will be performed within the defined area.
5. Draw the target filter.

1) Click .

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

The device can only detect a face when the size of the face is greater than the defined size.
6. Click **Apply**.

Card Settings

Background Information

 NOTE

This function is only available on specific models.

Process

1. Go to **Access Control > Card Settings**.
2. Configure the card parameters.

Card parameters

Card Settings

IC Card

☒

IC Card Encryption & Verifica...

☐

Block NFC Cards

☐

Enable DESFire Card

☐

DESFire Card Decryption

☐

Apply

Refresh

Default

Card No. System

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

Card No. System

☒ Hexadecimal

☐ Decimal

Apply

Refresh

Default

DESFire Card Write

Acquisition Device

Device

Please place the card on the swiping area and enable DESFire card and DESFire Card Decryption.

Card Number

Write

Card parameters description

Item	Parameter	Description
Card Settings	IC Card	When this function is enabled, IC cards can be read.  NOTE This function is only available on specific models.
	IC Card Encryption & Verification	When this function is enabled, only the encrypted IC card can be read.  NOTE Ensure IC Card is enabled.

Item	Parameter	Description
	Block NFC Cards	After enable this function, unlocking with duplicate NFC cards is prevented.  NOTE • This function is only applicable to models that support IC cards. • Ensure IC Card is enabled. • NFC function is only available on certain mobile phone models.
	Enable Desfire Card	When this function is enabled, the Device can read the card number of Desfire card.  NOTE • This function is only available on models that support IC cards. • Only supports hexadecimal format.
	Desfire Card Decryption	when Enable Desfire Card and Desfire Card Decryption are enabled simultaneously, information in the Desfire card can be read.  NOTE • This function is only applicable on models that support IC cards. • Ensure that Desfire card is enabled.
Card No. System	Card No. System	When connecting the Wiegand card reader, select either the decimal format or the hexadecimal format for the card number. The card number system is the same for both input and output of the card number.
DESFire Card Write	Acquisition Device	Select the device, place the card on the

Item	Parameter	Description
	Card Number	reader, enter the card number, and then click Write to write card number to the card.  NOTE • Supports up to 8 characters. • Desfire card function and Desfire card decryption function must be enabled. • Only supports hexadecimal format.

3. Click **Apply**.

Weekly Schedule

You can configure up to 128 time periods (from number 0 to number 127). Within each time period, you need to set up an access control schedule for the entire week. People can only unlock the door during the scheduled times.

Background Information

Process

1. Go to **Access Control > Weekly Schedule**.
2. Click **Add**.

1) Set the number and the schedule name.

2) Drag the time slider to configure time for each day.

3) (Optional) Click **Copy** to copy the configuration to the remaining days.

Configure general plan

Add

No.

0

▼

Schedule Name

Time Plan

0123456789101112131415161718192021222324

Sun

Copy

Mon

Copy

Tue

Copy

Wed

Copy

Thu

Copy

Fri

Copy

Sat

Copy

Apply

Cancel

3. Click **OK**.

Holiday Schedule

You can configure up to 128 holiday groups (numbered from 0 to 127), and for each holiday group, you can add up to 16 holidays. Afterwards, you can assign the configured holiday groups to the holiday schedule. Users can only unlock the door during the times defined in the holiday schedule.

Process

1.

Go to **Access Control > Holiday Schedule**.
2.

Click **Holiday Management**, then click **Add**.

1) Select a holiday group number, and then enter the name of that group.

Add a holiday group

Add

No.

0

▼

Holiday Group Name

Holiday Group Config

Add

No.

Holiday Name

Start Time

End Time

Operation

No Data

Apply

Cancel

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

Add a holiday to a holiday group

Add

Holiday Name

Period

Start date

→

End date

OK

Cancel

3.

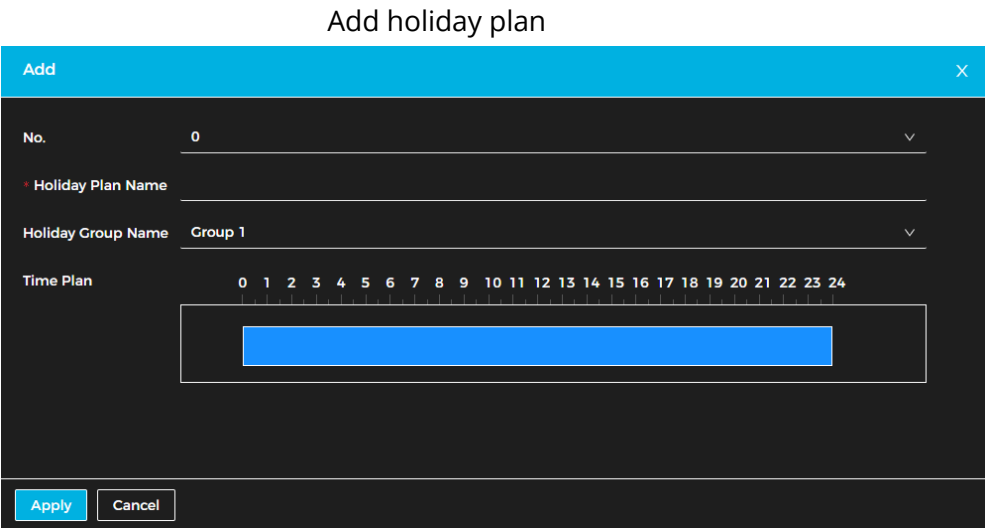
Click **OK**.
4.

Click **Plan Management**, then click **Add**.

1) Select a number for the holiday plan, then enter a name.

2) Select a holiday group, then drag the slider to configure time for each day.

Supports adding up to 4 time sections within a day.

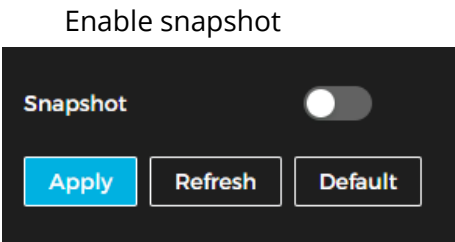


5. Click **OK**.

Privacy Setting

Process

- 1. Go to **Access Control > Privacy Setting** on the webpage.
- 2. Enable snapshot function.
When people unlock the door, facial images will be automatically captured.



3. Click **Apply**.

Port Config

Certain ports can be used as different ports, and you can configure them as different ports according to your actual needs.

Background Information



- The ports may vary depending on the product model.
- This function is only available on specific models

Process

- 1. Go to **Access Control > Port Config** on the webpage.

- 2. Select the port type.



NOTE

When the alarm cable and doorbell cable are shared, please configure the port for the doorbell to ensure that the doorbell can ring.

- 3. Click **Apply**.

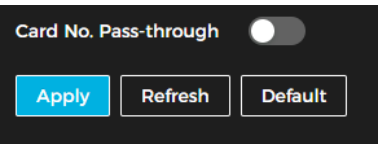


Back-end Comparison

Directly transmit card numbers and other data to third-party platforms for data verification, rather than performing data verification on the device.

Go to **Access Control > Back-end Comparison**.

Back-end comparison



Back-end comparison

Parameters	Description
Card No. Pass-through	Once enabled, the card number will be transmitted to a third-party platform for data verification.

First-Person Unlock

No one can access the door until the person you specified has passed through. When you specify multiple people, others can access the door after any one of the designated individuals has passed through.

Precondition

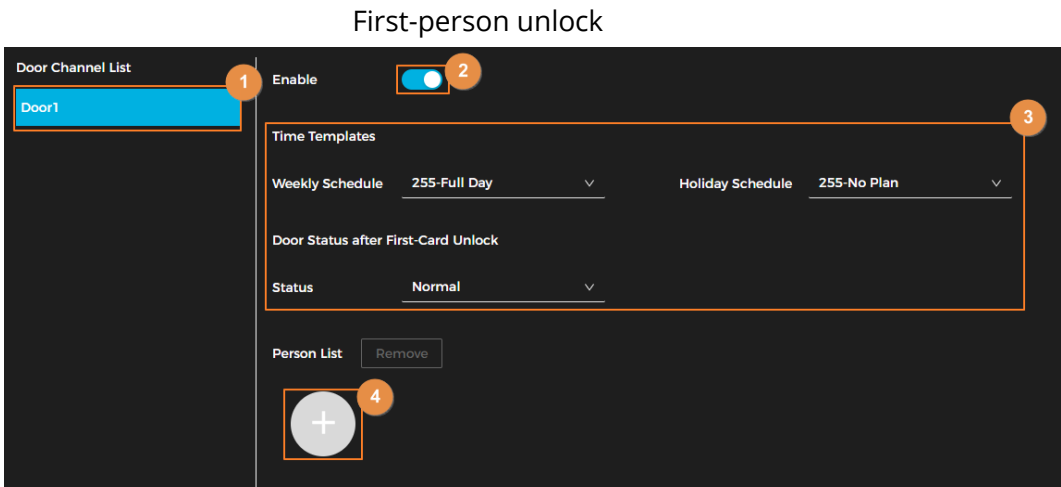
Only when access door permissions are granted can personnel be designated as the first person.

- Only the general users can be configured as the first person.
- After the first person verifies the identity, if the Device restarts, the first person needs to verify the identity again.
- After enable this function, patrol users can clock in normally.

Face Recognition Terminal User Manual

Process

- 1. Go to **Access Control > First-Person Unlock**.
- 2. Select the door channel, and then enable the function.



- 3. Configure the parameters.

Parameter description

Parameter	Description
Time Templates	Select the time for this rule to take effect.
Door Status after First-Card Unlock	• Normal: Other persons must verify their identifications to pass. • Always Unlocked: Anyone can pass through without identity verification.
Person List	Click + to select one or more persons who will be granted access to the door.

- 4. Click **Apply**.

Intercom Settings

The device can be used as an entrance station, enabling video intercom functionality.



The intercom function is only available on certain models.

Using the Device as the SIP Server

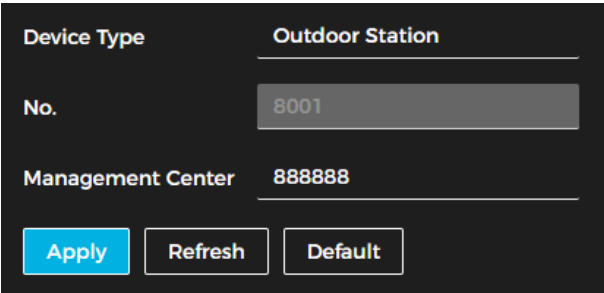
Local Device Config

When the device operates as a SIP server, please configure the parameters of the device.

Process

- 1. Go to **Intercom Settings > Local Device Config**.
- 2. Configure the parameters.

Basic parameters



Basic parameters description

Parameter	Description
Device Type	Select Outdoor Station .
No.	Unable to set.
Management Center	The default call number of the management center is 888888.

- 3. Click **Apply**.

SIP Server

When the device functions as a SIP server, it can connect up to 500 indoor monitors.

Process

- 1. Go to **Intercom Settings > SIP Server**.
- 2. Enable **SIP Server**.

Face Recognition Terminal User Manual



If the status of the SIP server changes, the device settings will automatically revert to the factory default values.

SIP server

Local SIP Server

☒

Port

5060

SIP No.

8001

Registration Password

•••••

SIP Domain

DoorPhone

Apply

Refresh

Default

3. Click **Apply**.

Adding the Outdoor Station

When the device acts as a SIP server, you need to add the door station to the SIP server to ensure that they can call each other.

Process

1. Go to **Intercom Settings > Device Setting** on the webpage.
2. Click **Add**, then configure the door station.

Add door station

Add

X

Device Type

Outdoor Station

▼

* No.

Please enter

* Registration Password

•••••

⌫

Building No.

Unit No.

* IP Address

0 . 0 . 0 . 0

* Username

Please enter

* Password

Please enter

⌫

OK

Cancel

Add VTO configuration

Parameter	Description
Device Type	Select Door Station .
No.	To view the number of the door station, please access the device screen at the door station and enter the door station number on this page.
Registration Password	Enter the registration password
Building No.	Unable to configure.
Unit No.	
IP Address	The IP address of the door station.
Username	Username and password for the door station used for login webpage.
Password	

3. Click **OK**.

Adding the Indoor Monitor

When the device acts as a SIP server, you can add all indoor monitors within the same unit to the

Face Recognition Terminal User Manual

SIP server to ensure they can call each other.

Process

1.
- Go to **Intercom Settings > Device Setting** on the home page.
2.
- Add the indoor monitor.

• Add one by one.

1. Click **Add**.

2. Configure parameters, and then click **OK**.

Add one by one

Add

X

Device Type

Indoor Monitor

▼

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

Room information

Parameter	Description
First Name	Enter the name of the indoor monitor to help you distinguish between different indoor monitors.
Last Name	
Alias	

Parameter	Description
Room No.	Enter the room number of the indoor monitor. • The room number consists of 1 to 5 digits and must match the room number configured on the indoor monitor. • When both the main indoor monitor and the extension devices are present, the room number of the main VTH ends with -0, while the room numbers of the extension devices end with -1, -2, or -3. For example, the room number of the main indoor monitor is 101-0, and the room numbers of the extension devices are 101-1, 101-2, and so on. • If the group call feature is not enabled, it is not possible to set the room number format to 9901-xx.
Registration Mode	Keep them as default settings.
Registration Password	

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

Batch add

Add

X

Device Type

Indoor Monitor

▼

Add Mode

Add in Batches

▼

Floors in Unit

5

Rooms on Each Floor

4

First Room No. on 1st Floo...

101

First Room No. on 2nd Flo...

201

OK

Cancel

Face Recognition Terminal User Manual

Add in batches

Parameter	Description
Floors in Unit	The number of floors in the building ranges from 1 to 99.
Rooms on Each Floor	The number of rooms on each floor 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 room number of the first room on the second floor is equal to the first digit of the room number of the first room on the first floor plus 1. For example, if the room number of the first room on the first floor is 101, then the room number of the first room on the second floor must be 201.

Using VTO as the SIP server

SIP Server

Use another VTO as the SIP server.

Process

1.

Go to **Intercom Settings** > **SIP Server**.
2.

Select **Device** from the **Server Type**.
- NOTE

Do not enable **SIP server**.
3.

Configure the parameters.

Use VTO as the SIP server

Local SIP Server

Server Type

Device

Server Address

192.168.1.111

Port

5060

SIP No.

8001

Registration Password

SIP Domain

DoorPhone

SIP Server Username

SIP Server Password

Apply

Refresh

Default

SIP server configuration

Parameter	Description
Server Address	IP address or domain name of the VTO.
Port	When VTO operates as a SIP server, it uses port 5060 by default.
Registration Password	Keep the default settings.
SIP Domain	DoorPhone.
SIP Server Username	Login username and password for the SIP server.
SIP Server Password	

4.

Click **Apply**.

Local Device Config

When you use another VTO as the SIP server, please configure the parameters of the device.

Process

1.

Go to **Intercom Settings** > **Local Device Config**.
2.

Configure the parameters.

Configure the parameters

Device Type

Outdoor Station

No.

8001

Management Center

888888

Apply

Refresh

Default

Parameters description

Parameter	Description
Device Type	Default setting is Outdoor Station .
No.	The VTO number. NOTE - The number must be four digits. The first two digits must be 80, and the last two digits start from 01. For example, 8001. - If there are multiple VTOs within a unit, the VTO numbers must not be duplicated.
Management Center	The phone number for the management center is 888888. Please keep the default.

3. Click **Apply**.

Call Config

Configuring the call function of the device. This section describes how to add an indoor monitor in phonebook mode, allowing direct dialing to the indoor monitor on the device.

Background Information

After enabling this feature, a call icon will be displayed on the standby screen. You can choose from three types of calls. The configuration is consistent with the settings in **System Settings > Shortcut Settings**.

Call type description

Type	Description
Call Room	Standard: Tap the call icon on the standby screen, enter the room number, then tap the call icon to call the room. Phone Book: Custom the contents on the webpage. Tap the call icon on the standby screen, and the added indoor monitor will be displayed on the screen. Tap the icon to call the indoor monitor. The call list will be displayed according to your configurations on the webpage.
Call Management Center	Tap the call icon on the standby screen to call the management center.
Call Phone	Tap the call icon on the standby screen to call the phone.

Process

1. Go to **Intercom Settings > Call Config** on the webpage.
2. Select the call type.
Select **Call Room** as the type and **Phone Book** as the mode. The preview screen is displayed on the left, and the added indoor monitor is shown on the right.

NOTE

- The call list preview window varies by product model.
- The 4.3-inch horizontal series devices do not support call list preview.
- The corresponding device type will only be displayed when the device is set as a SIP server and the indoor monitor is added to the SIP server on the device settings page.

Call room type and phone book mode

8001
800

9001
900

SIP No. Alias Add Batch Add

No.	SIP No.	Alias	Device Type	Operation
☐	1	8001	800	
☐	2	9001	900	

Delete

Apply Refresh

3. Add indoor monitor.

Face Recognition Terminal User Manual

If the indoor monitor has extensions (such as 9901-0, 9901-1, and 9901-2), and the SIP number is 9901, then you only need to dial the SIP number, and 9901-0, 9901-1, and 9901-2 will be called simultaneously.

Related Operations

- Click  to edit the alias of the device.
- Click  to delete the device.
- Click  to adjust the devices order, or you can simply drag the devices in the preview window.

Communication Settings

Network Settings

TCP/IP

You need to configure the device's IP address to ensure it can communicate with other devices.

Process

- Go to **Communication Settings > Network Settings > TCP/IP**.
- Configure the parameters.

TCP/IP

NIC

NIC 1

Mode

☒ DHCP ☐ Static

MAC Address

30 : dd : : : a5 : c3

IP Version

IPv4

IP Address

172 . . 237

Subnet Mask

255 . . 0

Default Gateway

172 . . 1

Preferred DNS

8 . . 8

Alternate DNS

8 . . 4

MTU

1500

Transmission Mode

☒ Multicast ☐ Unicast

Apply

Refresh

Default

Description of TCP/IP

Parameter	Description
Mode	- Static: Enter IP address, subnet mask, and gateway. - DHCP: It stands for Dynamic Host Configuration Protocol. When DHCP is enabled, devices will automatically be assigned an IP address, subnet mask, and gateway.
MAC Address	The MAC address of the device.
IP Version	IPv4 or IPv6.
IP Address	If you set the mode to Static , configure the IP address, subnet mask and gateway.
Subnet Mask	

Face Recognition Terminal User Manual

Parameter	Description
Default Gateway	NOTE - IPv6 address is represented in hexadecimal. - The IPv6 version does not require the configuration of a subnet mask. - The IP address and the default gateway must be within the same network segment.
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.
MTU	MTU (Maximum Transmission Unit) refers to the maximum size of data that can be transmitted in a single network packet within a computer network. The default value is 1500.
Transmission Mode	- Multicast: Ideal for video talk. - Unicast: Ideal for group call.

3. Click **OK**.

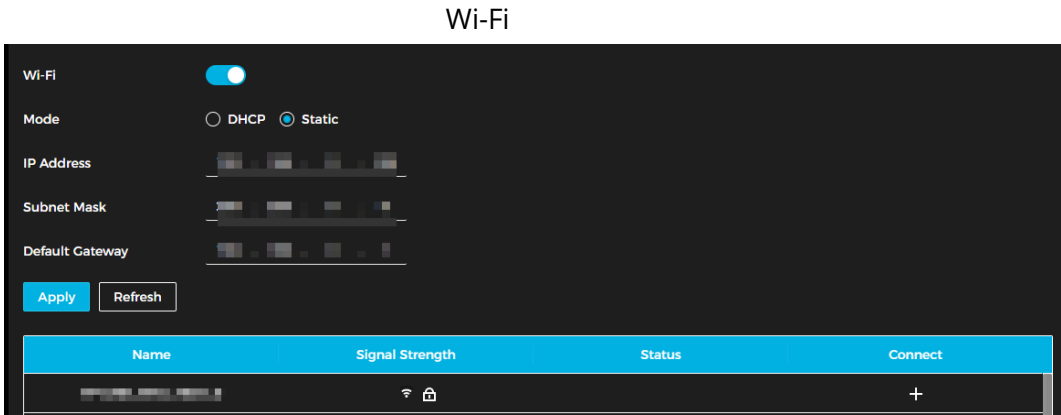
Wi-Fi

Process

1.

Go to **Communication Settings > Network Settings > Wi-Fi**.
2.

Enable Wi-Fi.
All available Wi-Fi are displayed.



NOTE

- Wi-Fi and Wi-Fi AP cannot be enabled simultaneously.
- Wi-Fi function is only available on certain models.

3. Tap **+**, then enter the Wi-Fi password. The Wi-Fi will be connected.

Related Operations

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

Wi-Fi AP

NOTE

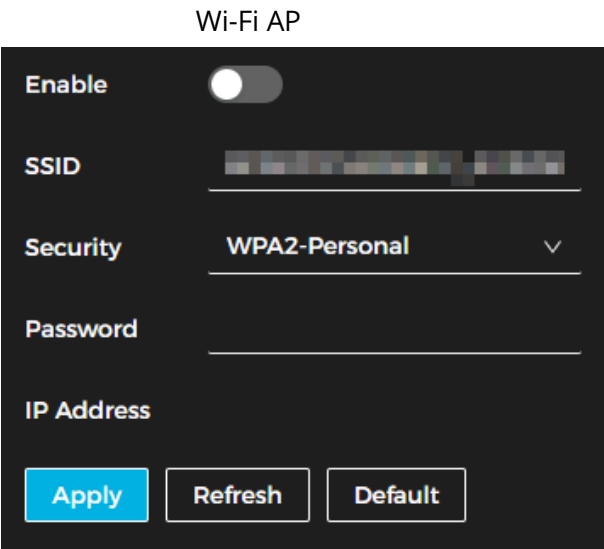
- The Wi-Fi and Wi-Fi AP cannot be enabled simultaneously.
- The Wi-Fi function is available on certain models.

Process

1.

Go to **Communication Settings > Network Settings > Wi-Fi AP**.
2.

Enable the function, then click **Apply**.



Result

Once enabled, you can connect to the device's Wi-Fi using your mobile phone and log in to the device's web page on your phone.

Port

You can simultaneously restrict access to devices through the web, desktop client, and mobile client.

Process

1.

Go to **Communication Settings > Network Settings > Port**.
2.

Configure the ports.

Face Recognition Terminal User Manual



NOTE

Except for **Max Connection** and **RTSP Port**, you need to restart the device after changing other parameters for the configuration to take effect.

Configure ports

Max Connection

50

(1-50)

HTTP Port

80

HTTPS Port

443

RTSP Port

554

Apply

Refresh

Default

Description of ports

Parameter	Description
Max Connection	You can set the maximum number of clients that can access the device simultaneously (for example, web pages, desktop clients, and mobile clients).
HTTP Port	The default value is 80. If you have changed the port number, please add the port number after the IP address when accessing the webpage.
HTTPS Port	The default value is 443.
RTSP Port	The default value is 554.

3. Click **Apply**.

Basic Services

When you want to connect the device to a third-party platform, please enable the CGI and ONVIF functions.

Process

- Go to **Communication Settings > Network Settings > Basic Services**.
- Configure the basic service.

Basic service

SSH

☐

Multicast/Broadcast Search

☒

CGI

☒

ONVIF

☒

Private Protocol Authentication ...

Security Mode (Recommen... ▾)

Private Protocol

☒ ⓘ

TLSv1.1

☐

LLDP

☐

Apply

Refresh

Default

Basic service parameter description

Parameter	Description
SSH	SSH, or Secure Shell Protocol, is a remote management protocol that allows users to access, control, and modify their remote servers over the Internet.
Mutlicast/Broadcast Search	Search for devices using multicast or broadcast protocols.
CGI	The Common Gateway Interface (CGI) is an intersection between web servers that enables standardized data exchange between external applications and the server.
ONVIF	ONVIF stands for Open Network Video Interface Forum. Its purpose is to provide a standard for communication between different IP-based security devices. These standardized ONVIF specifications serve as a common language that all devices can use to communicate.

Face Recognition Terminal User Manual

Parameter	Description
Private Protocol Authentication Mode	Set the authentication mode, including security mode and compatible mode. It is recommended to select Security Mode . - Security Mode (recommended): Does not support accessing the device through Digest, DES, and plaintext authentication methods, improving device security. - Compatible Mode: Supports accessing the device through Digest, DES, and plaintext authentication methods, with reduced security.
Private Protocol	The platform adds devices through private protocol.
TLSv1.1	TLSv1.1 refers to Transport Layer Security Protocol version 1.1. TLS is an encryption protocol designed to provide secure and authenticated computer network communication. NOTE Enabling TLSv1.1 may pose security risks. Please be aware.
LLDP	LLDP stands for Link Layer Discovery Protocol, which is a data link layer protocol. This protocol allows network devices, such as switches, routers, or servers, to exchange information about their identity and capabilities. The LLDP protocol helps network administrators better understand the network topology and provides a standardized method for the automatic discovery and mapping of connections between network devices. This makes network configuration, troubleshooting, and performance optimization much easier.

3. Click **Apply**.

Cloud Service

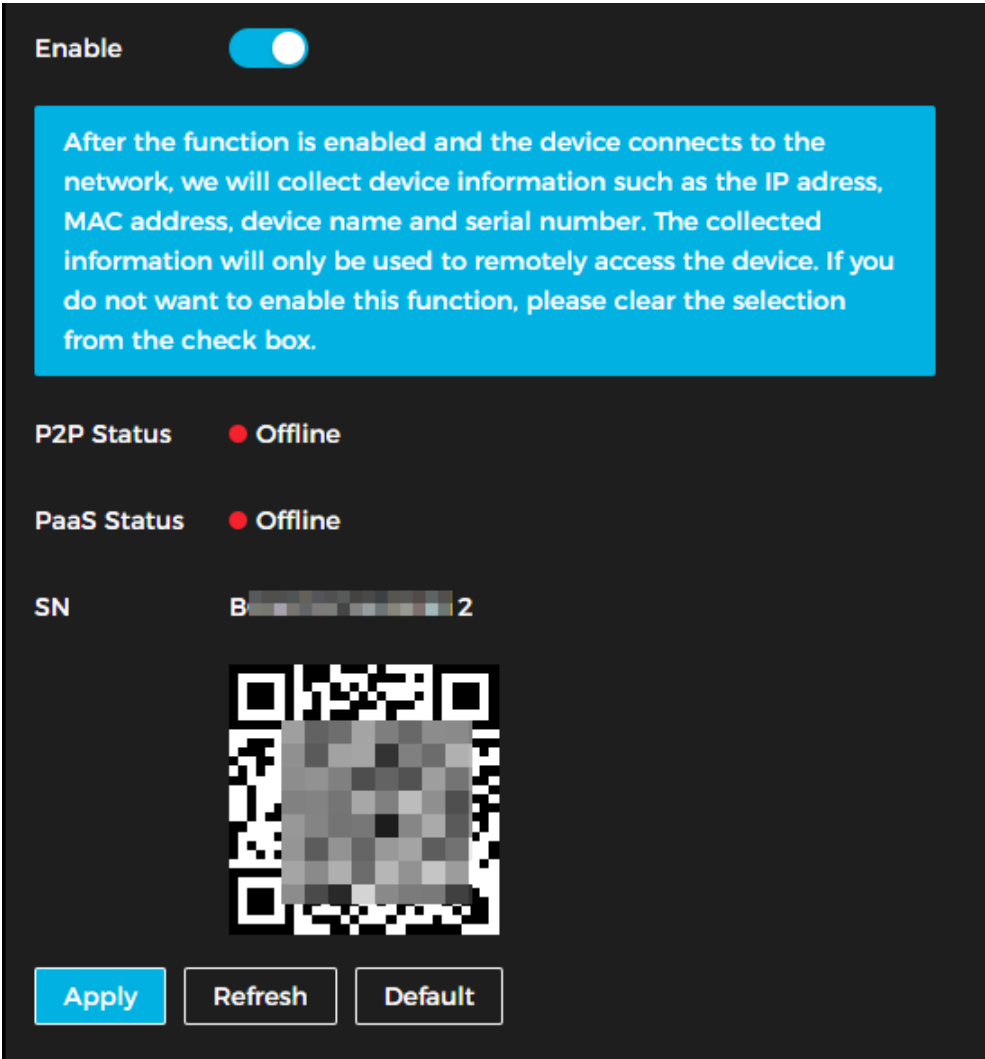
This cloud service provides NAT traversal services. Users can manage multiple devices through LumiViewer. There is no need to apply for a dynamic domain name, configure port mapping, or deploy servers.

Process

1. Go to **Communication Settings > Network Settings > Cloud Service**.
2. Enable the cloud service function.

If P2P and PaaS are online, then cloud services will be online.

Cloud service



3. Click **Apply**.
4. Use LumiViewer to scan the QR code to add the device.

Auto Registration

The automatic registration function enables devices to be added directly to the management platform without the need for manual input of device information, such as IP address and port.

Background Information

NOTE
Automatic registration is supported only for the SDK.

Process

1. Go to **Communication Settings > Network Settings > Auto Registration**.
2. Enable the auto registration function and configure the parameters.

Face Recognition Terminal User Manual

Auto Registration

Enable

Status

Offline

Server Address

0.0.0.0

Port

6060

Registration ID

Apply

Refresh

Default

Automatic registration description

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

3. Click **Apply**.

Auto Upload

Send user information and unlock records to the management platform.

Process

1. Go to **Communication Settings > Network Settings > Auto Upload**.
2. (Optional) Enable **Push Person Info**.
When user information is updated or a new user is added, the device will automatically push the user information to the management platform.
3. Enable HTTP upload mode.
4. Click **Add**, then configure parameters.

Auto upload

Push Person Info

Upload Mode

HTTP

Enable

Add

Delete

No.	IP/Domain Name	Port	HTTPS	Path	Event Type	Operation
☐	1	192.168.1.108	80		/	Person Info, Unlock Records

Apply

Refresh

Default

Parameters description

Parameter	Description
IP/Domain Name	The IP or domain name of the management platform.
Port	The management platform port.
HTTPS	Access the management platform via HTTPS. HTTPS ensures secure communication over computer networks.
	When accessing the management platform, please enable account authentication. A username and password are required for login.
Event Type	Select the event type to be pushed to the management platform. NOTE • Enable Push Person Info before you use this function. • Personal information can only be pushed to one management platform, while unlock records can be pushed to multiple management platforms.

5. Click **Apply**.

RS-485 Settings

If you connect external devices to the RS-485 port, please configure the RS-485 parameters.

Process

1. Go to **Communication Settings > RS-485 Settings**.
2. Configure the parameters.

Configure parameters

External Device

Card Reader

▼

Baud Rate

9600

▼

Data Bit

8

▼

Stop Bit

1

▼

Parity Code

None

▼

Apply

Refresh

Default

Configure the RS-485 parameters

Parameter	Description
External Device	• Access Controller Select Access Controller when the Device functions as a card reader, and sends data to other external access controllers to control access. Output Data type: ◊ Card Number: When the user swipes the card to unlock the door, data is output based on the card number; when the user uses other unlocking methods, data is output based on the user's first card number. ◊ No.: Outputs data based on the user ID. • Card Reader: The device serves as an access controller and is connected to an external card reader. • Reader (OSDP): The device is connected to a card reader based on the OSDP protocol.
Data Bit	In serial communication, the number of bits used to transmit actual data. It represents the binary digits that carry the transmitted information.
Stop Bit	A bit sent after the data and optional parity bits, used to indicate the end of data transmission. It allows the receiver to prepare for the next data byte and provides synchronization in the communication protocol.
Parity Code	Additional bits sent after the data bits, used for error detection during transmission. They help verify the integrity of the transmitted data by ensuring a specific number of logical high or low bits.

3. Click **Apply**.

Wiegand Settings

Support access to Wiegand devices. According to your actual device configuration mode and transmission mode.

Process

1.

Go to **Communication Settings > Wiegand**.
2.

Select a Wiegand type, then configure parameters.

• When you connect an external card reader to the device, please select **Wiegand Input**.

NOTE

When the Device connects to a third-party device through the Wiegand input port, and the card number read by the Device is in the reverse order from the actual card number. In this case, you can enable **Card No. Inversion** function.

• When the device is used as a card reader and needs to be connected to another access control controller, please select **Wiegand Output**.
- Wiegand output
- Wiegand Settings

Wiegand Input

Wiegand Output

Wiegand Output Type

Wiegand 34

▼

Pulse Width (μs)

200

(20-200)

Pulse Interval (μs)

1000

(200-5000)

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

Output Data Type

Card Number

No.

Apply

Refresh

Default
- Description of Wiegand output
- | Parameter | Description |
|---------------------|---|
| Wiegand Output Type | Select a Wiegand format to read card numbers or ID numbers. <div><div>• Wiegand26: Reads 3 bytes or 6 digits.</div><div>• Wiegand34: Reads 4 bytes or 8 digits.</div><div>• Wiegand66: Reads 8 bytes or 16 digits.</div></div> |
| Pulse Width | Enter the pulse width and pulse interval of the wiegand output. |
| Pulse Interval | |
- 45

Face Recognition Terminal User Manual

Parameter	Description
Output Data Type	Select the output data type. • 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.

3. Click **Apply**.

System Settings

Account

Add or delete users, change users' passwords, and enter an email address to reset the password when you forget it.

Adding Administrators

Add new administrator accounts, and they can log in to the devices webpage.

Process

1. Go to **System Settings > Account > Account** on the home page.
2. Click **Add** and enter the user information.

 NOTE

- The username cannot be the same as an existing account. The username consists of up to 31 characters and may only include numbers, letters, underscores, hyphens, periods, or @.
 - The password must consist of 8 to 32 non-empty characters and must include at least two of the following types of characters: uppercase letters, lowercase letters, numbers, and special characters (excluding ' " ; &).
- Set a high-security password according to the password strength prompt.

Add administrators

Add

Username

Password

Confirm Password

Remarks

OK

Cancel

3. Click **OK**.

 NOTE

Only administrator accounts can change the password, and administrator accounts cannot be deleted.

Adding ONVIF Users

Background Information

The Open Network Video Interface Forum (ONVIF) is a global and open industry forum aimed at developing global open standards for the interfaces of physical IP-based security products, thereby achieving compatibility among different manufacturers. ONVIF users authenticate their identity through the ONVIF protocol. The default ONVIF user is admin.

Process

1. Go to **System Settings > Account > ONVIF User**.
2. Click **Add**, then configure parameters.

Face Recognition Terminal User Manual

Add ONVIF user

Add

Username

Password

Confirm Password

Group

OK

Cancel

ONVIF user description

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

3. Click **OK**.

Resetting the Password

When you forget your password, please reset it through the associated email.

Process

- Go to **System Settings > Account > Password Reset**.
- Enter the email address, and set the password expiration time.
- Enable the password reset function.

Reset Password

Enable

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

Email Address

Password Expires in

Apply

Refresh

Default

NOTE

If you have forgotten your password, you can receive a security code to reset your password via the associated email address.

4. Click **Apply**.

Viewing Online Users

View online users who currently log in to the webpage. Go to **System Settings > Online User**.

Time

Process

- Go to **System Settings > Time** on the home page.
- Configure the platform's time.

Date settings

System Time

06-25-2025 4:49:33 AM

Sync PC

Time Zone

Month_Day_Year

Time Format

12-Hour

NTP Settings

Server

time.windows.com

Manual Update

Port

123

1-65535

Interval

1440

min

Daylight Saving TL...

Start Time

March

Second

Sunday

02 AM

End Time

November

First

Sunday

02 AM

Apply

Refresh

Default

Face Recognition Terminal User Manual

Time settings description

Parameter	Description
Time	Manual Set: Manually enter the time or click Sync PC to synchronize the time with your PC.
Time Zone	Enter the time zone.
Date Format	Select the date format.
Time Format	Select the time format.
NTP Settings	The device will automatically synchronize time with the NTP server. Server: Enter the domain of the NTP server. Port: Enter the port of the NTP server. Interval: Enter its time with the synchronization interval.
Daylight Saving Time	1. (Optional) Enable Daylight Saving Time. 2. Configure the start time and end time of the Daylight Saving Time.

3. Click **Apply**.

Shortcut Settings

Process

1. Go to **System Settings > Shortcut Settings**.
2. Configure the shortcut parameters.

Shortcut Settings

Password

Doorbell

Local Device Ringer

Ringtone Config

Ringtone 1

Ringtone Time (sec)

3

(1-30)

Call

Call Type

Call Room

Mode

Standard

Apply

Refresh

Default

Parameters description

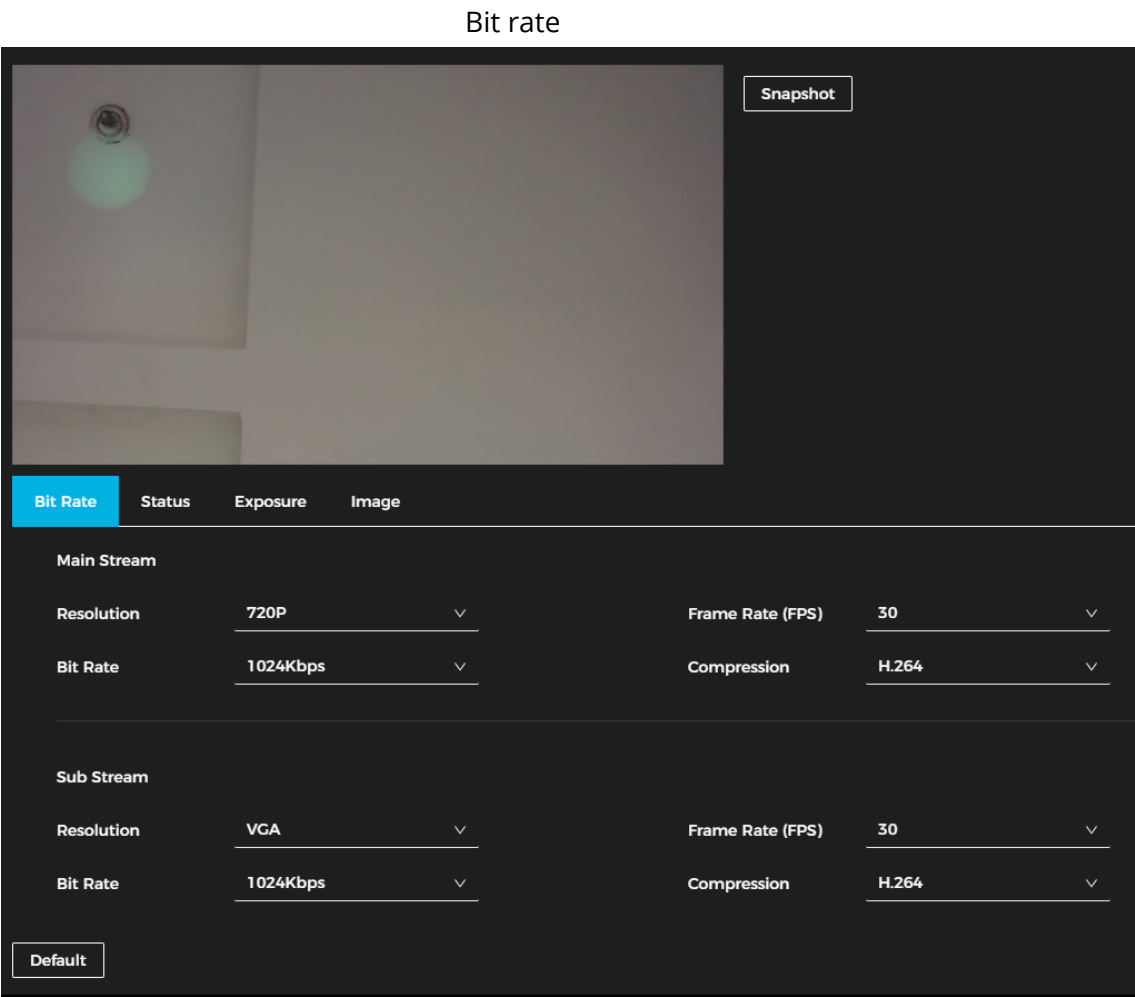
Parameter	Description
Password	The icon of the password unlock method is displayed on the standby screen.
Doorbell	After the doorbell function is activated, the doorbell icon will be displayed on the standby screen. - Local device ringer: Tap the doorbell icon on the standby screen and the device will ring. - Ringtone config: Select a ringtone. - Ringtone time (sec): Set the ringtone duration (1-30 seconds). The default value is 3. - Alarm: Tap the doorbell icon, and the external alarm device rings. NOTE This function is only available on specific models. When the alarm cable and the doorbell cable are shared, please ensure the functional interface is set to Doorbell. For more details, refer to "Port Config".
Call	The standby screen displays the call icon.
Call Type	- Call room: There are 2 modes. - Standard: Tap the call icon on the standby screen, enter the room number, then tap the call icon to call the room. - Phone book: Customize the contents on the webpage. Tap the call icon on the standby screen, and the added indoor monitor is displayed on the screen. Tap the icon to call the indoor monitor. The call list will be displayed according to your configurations on the webpage. - Call management center: Tap the icon on the standby screen to call the management center. - Call Phone: Tap the call icon on the standby screen to call phone. NOTE You can call Lumiviewer only in this call type.

Face Recognition Terminal User Manual

Video

Process

1.
- Go to **System Settings > Video**.
2.
- Configure the bit rate.

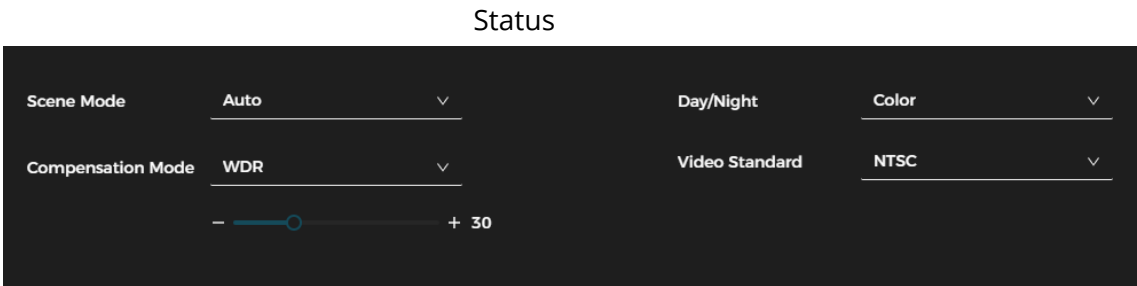


Bit rate description

Parameter		Description
Main Stream	Resolution	When the device is used as a VTO and connected to an indoor monitor, the acquisition stream limit for the indoor monitor is set to 720p. When the resolution is changed to 1080p, the call and monitoring functions will be affected.
	Frame Rate (FPS)	Frames per second (or images per second).

Parameter		Description
	Bit Rate	The amount of data transmitted over an internet connection within a specific time frame. Choose an appropriate value based on your network speed.
	Compression	Video compression standards aim to provide good video quality at lower bit rates.
Sub Stream	Resolution	The sub stream supports D1, VGA and QVGA.
	Frame Rate (FPS)	Frames per second (or images per second).
	Bit Rate	It represents the amount of data transmitted through an internet connection over a specific period of time.
	Compression	Video compression standards aim to provide good video quality at lower bit rates.

3.
- Configure the status.



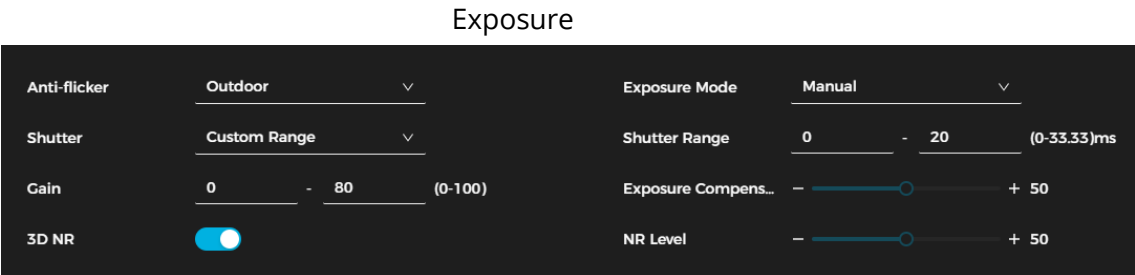
Parameters description of status

Parameter	Description
Scene Mode	In different scene modes, the image hue is different. • Disable: Scene mode function is disabled. • Auto: The system automatically adjusts the scene mode based on the sensitivity of the photography. • Sunny: In this mode, the hue of the image will be reduced. • Night: In this mode, the hue of the image will be enhanced.

Face Recognition Terminal User Manual

Parameter	Description
Day/Night	The day/night mode affects light compensation under different circumstances. • Auto: The system automatically adjusts the day and night modes based on the sensitivity of the photography. • Colorful: In this mode, images are colorful. • B/W: In this mode, the image is in black and white.
Compensation Mode	• Disable: Compensation is disabled. • BLC: The backlight compensation function automatically brings more light to the darker areas of the image when bright light sources illuminate from the rear, in order to prevent them from being obscured. • WDR: This system dims the bright areas and compensates for the dark areas to create balance, thereby improving overall image quality. • HLC: High Light Compensation (HLC) is a technology used in CCTV/IP security cameras designed to handle images that are illuminated by strong light sources, such as headlights or spotlights. The camera's image sensor detects the strong light in the video and reduces exposure in those areas to enhance the overall quality of the image.
Video Standard	Select from PAL and NTSC .

4. Configure the exposure parameters.

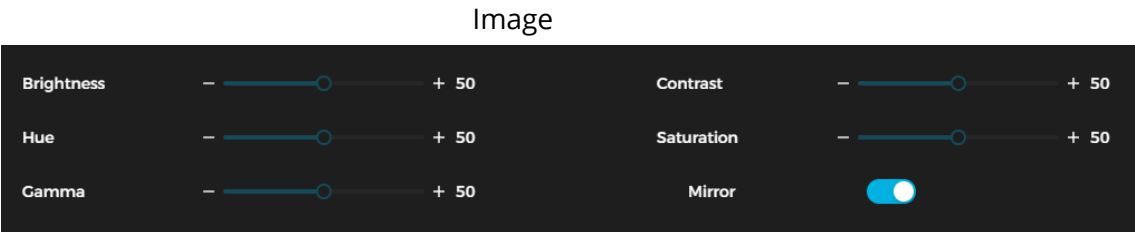


Exposure parameter description	
Parameter	Description
Anti-flicker	Set the anti-flicker function to reduce flicker and lower or minimize uneven colors or exposure. • 50Hz: When the mains frequency is 50 Hertz, the exposure automatically adjusts according to the surrounding brightness to prevent the appearance of horizontal lines. • 60Hz: When the mains frequency is 60 Hertz, the exposure automatically adjusts according to the surrounding brightness to reduce the appearance of horizontal lines. • Outdoor: When selecting Outdoor, you can switch the exposure mode.
Exposure Mode	Adjust the exposure to modify the brightness of the image. • Auto: The device automatically adjusts the brightness of the image based on the surrounding environment. • Shutter Priority: The device adjusts the image brightness based on the set shutter range. If the image brightness is insufficient, but the shutter value has reached its upper or lower limit, the device will automatically adjust the gain value to achieve the desired brightness level. • Manual: You can manually adjust the gain and shutter values to regulate the brightness of the image. NOTE ◇ When you select Outdoor from the Anti-flicker list, you can select Shutter Priority as the exposure mode. ◇ The exposure mode may vary depending on the device model.
Shutter	The shutter is a component that allows light to pass through for a certain period of time. The higher the shutter speed, the shorter the exposure time, resulting in a darker image. You can choose a shutter range or add a custom range.
Gain	Once the gain value range is set, the video quality will be improved.
Exposure Compensation	By adjusting the exposure compensation value, the video will become brighter.
3D NR	When the 3D Noise Reduction (RD) function is enabled, video

Face Recognition Terminal User Manual

Parameter	Description
NR Level	noise can be reduced, ensuring higher clarity of the video. You can set its level when this feature is enabled. A higher level means clearer images.

5. Configure the image.



Parameter	Description
Brightness	Brightness of the image. The higher the value, the brighter the image.
Contrast	Contrast is the difference in brightness or color that makes objects distinguishable. The greater the contrast value, the more pronounced the color contrast becomes.
Hue	It refers to the intensity or saturation of a color. It describes the concentration or purity of the color.
Saturation	Color saturation indicates the intensity of colors in an image. As saturation increases, the representation of colors becomes more intense, for example, becoming more red or more blue. NOTE The saturation value does not change the brightness of the image.
Gamma	Change the brightness and contrast of the image in a nonlinear manner. The higher the value, the brighter the image.
Mirror	When this feature is enabled, the image will be displayed in a mirrored format.

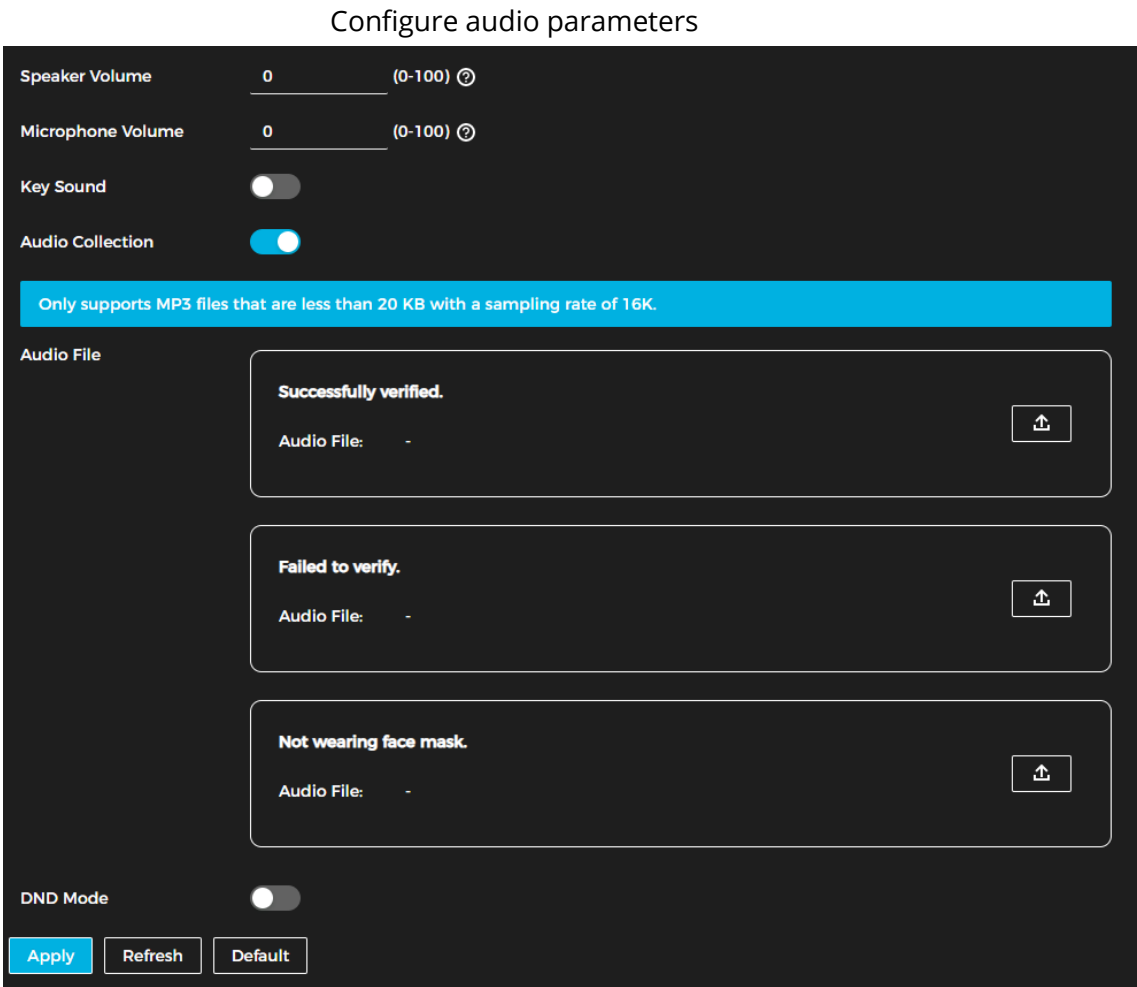
Audio

Set audio prompts during identity verification.

Process

1. Go to **System Setting > Audio**.

2. Configure the audio parameters.



Parameters	Description
Speaker Volume	Set the speaker volume.
Microphone Volume	Set the microphone volume.
Key Sound	When this function is enabled, touchscreen devices will emit a tapping sound, while non-touchscreen devices will produce a mouse click sound.
Audio Collection	If this function is enabled, the sound from the device's microphone will be captured during live viewing and recording.
Audio File	Click to upload the audio file to the platform.
DND Mode	There are no voice prompts during the set time for identity verification through the device. You can set up to 4 time periods.

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



NOTE

Only MP3 files smaller than 20 KB and with a sampling rate of 16K are supported.

4. Click **Apply**.

Motion Detection

The screen will be awakened when a moving object is detected and the set threshold is reached.

Background Information



NOTE

This function is only available on specific models.

Process

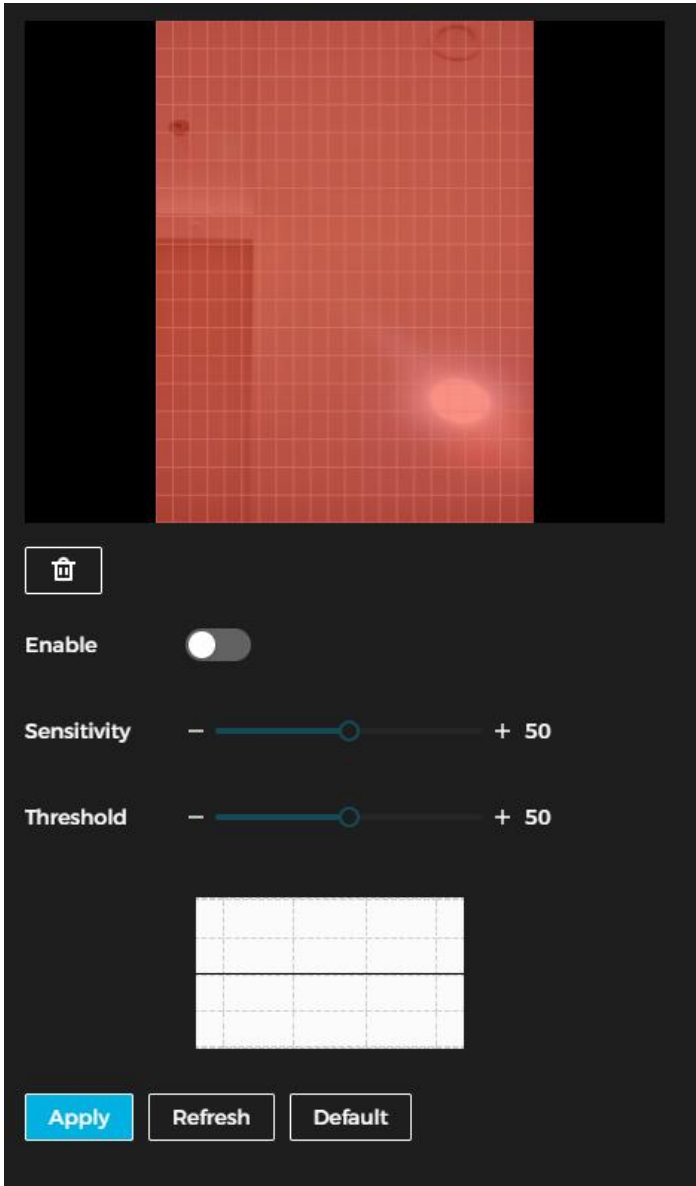
1. Go to **System Settings > Motion Detection**.
2. Enable the motion detection function.
3. Press and hold the left mouse button, then draw the detection area within the red zone.



NOTE

- The motion detection area is displayed in red.
- To remove the existing the motion detection area, click .
- If you draw within the default motion detection area, the motion detection area you have drawn will become a non-motion detection area.

Motion detection area



4. Configure the parameters.
- Sensitivity: The sensible to the surroundings. The higher the sensitivity means that the alarm is triggered more easily.
 - Threshold: The function sets dynamic pixel change thresholds to filter out environmental noise (e.g. swaying leaves), ensuring only valid moving objects trigger alarms. A lower threshold means that the alarm is triggered more easily.
5. Click **Apply**.

Face Recognition Terminal User Manual

When the red line is displayed, motion detection is triggered; when not triggered, a green line is displayed.

View Selection

Set the view area in the video talk and preview.

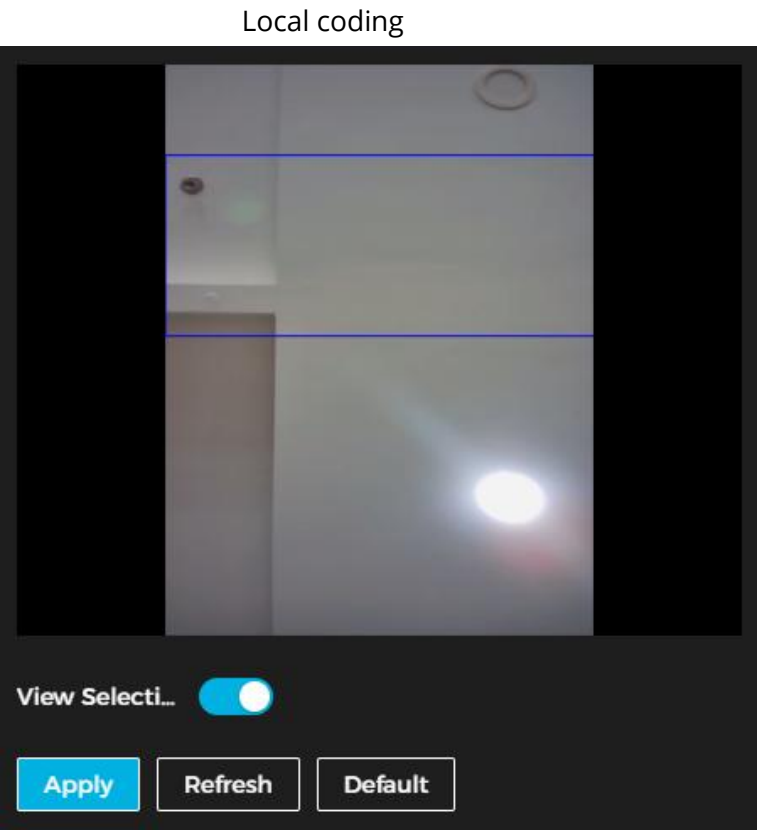
Background Information

 NOTE

- This function is only applicable to specific models.
- This function is enabled by default when it works with an indoor monitor. When this function is turned off, the preview may not be accessible.

Process

1. Go to **System Settings > View Selection**.
2. Enable the function.
3. Drag the box to a designated position.
This box represents the preview area in the video call.



4. Click **Apply**.

Advertisement

Configure the theme and add video or image advertisements to the device.

 NOTE

- The function is available on certain models.
- B-frames contained in videos from the platform are not supported for decoding.
- Images with a bit depth of 1 cannot be processed.
- Parsing of semi-transparent images is not supported.
- Different devices support different advertising resolutions.

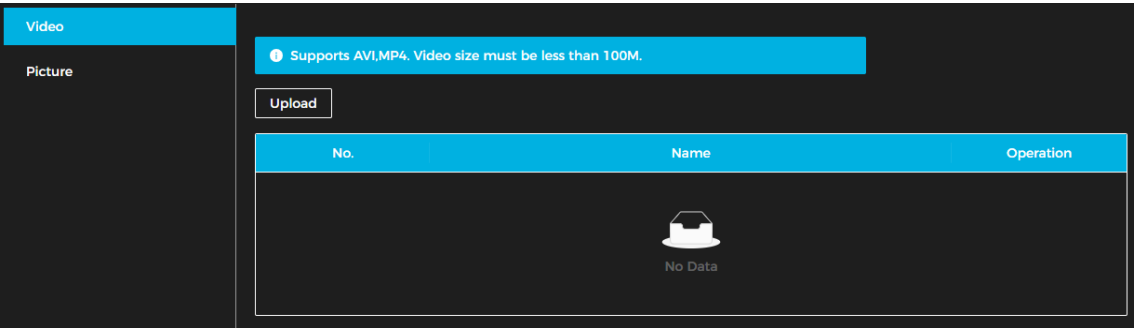
Adding Resources

Add images or videos to be displayed on the device's standby screen.

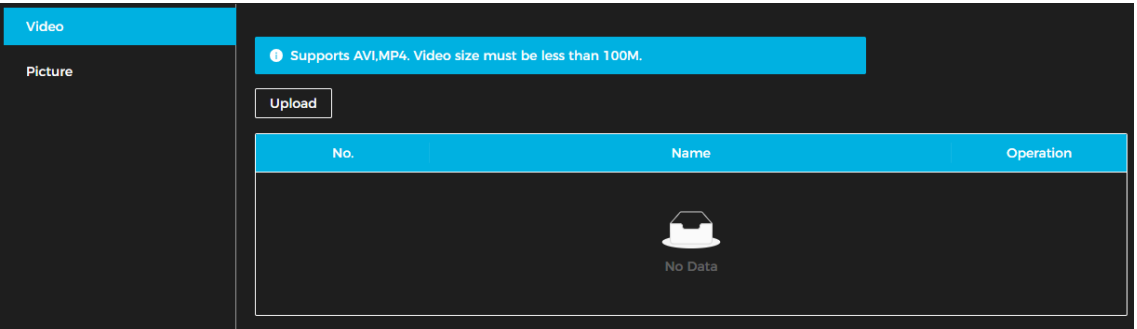
Process

1. Go to **System Settings > Advertisement > Ad Resources** on the home page.
2. Add videos or pictures.

Add videos



Add pictures



- Add videos.
 1. Click **Upload**.
 2. Click **Browse**, select the video file, then click **Next**.
The video will be automatically uploaded to the platform after transcoding.

Face Recognition Terminal User Manual

 NOTE

- ◇ You can upload up to 5 video files.
- ◇ Supports AVI, MP4. The video size must be less than 100 MB.
- ◇ Only the latest versions of Firefox and Chrome are supported for uploading video files.

- Add pictures.
 1. Click **Upload**.
 2. Select image from the local and upload it.

 NOTE

Supports PNG, JPG, and BMP formats. The image size must be less than 2MB.

Related Operations

Click  to delete uploaded images or videos.

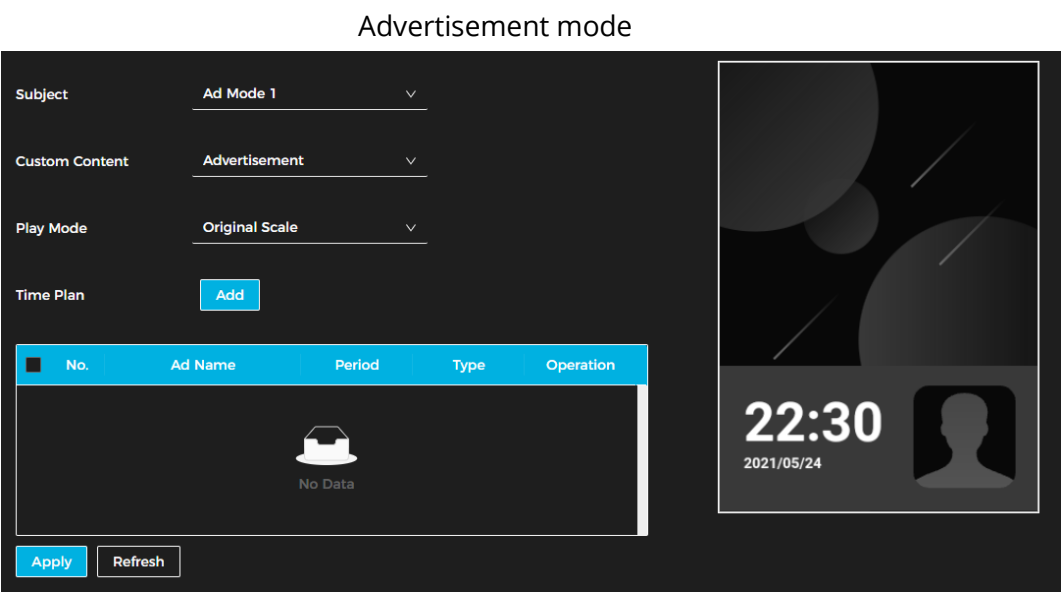
 NOTE

The videos and images currently in use cannot be deleted.

Configuring Subject

Process

1. Go to **System Settings > Advertisement > Subject**.
2. Select the subject.
 - General Mode: Displays the face image in full screen.
 - Ad Mode 1: The upper area displays advertisements, while the lower area shows the time and face detection box.
 - Ad Mode 2: The upper area displays the time and face recognition frame, while the lower area displays the advertisement.
3. Set advertisement display.
 1. Select Ad mode 1 or Ad mode 2, then select **Advertisement**.

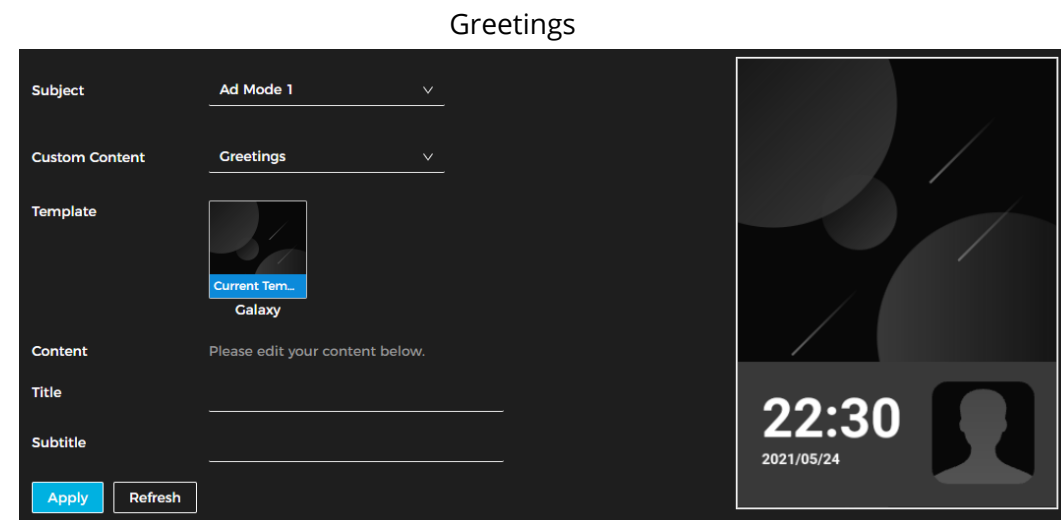


2. Select the play mode.
 - Original Scale: Plays images and videos at their original size.
 - Full Screen: Plays the image and video in full screen.
3. Click **Add** to add the schedule. You can add up to 10 schedules.
4. Enter the advertisement name.
5. Select the time period, file type.
6. Enter the duration, upload the resources, then click **Apply**.
 - Set the duration for a single picture when pictures are played in a loop. The duration range is from 1 second to 20 seconds, with a default value of 5 seconds.
 - When you upload videos, you can adjust the order of the videos.

Figure 3-54 Add time schedules

Face Recognition Terminal User Manual

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



4. Click **Apply**.

Management Center

System Information

Version Information

Go to **Maintenance Center > Version**, and you can view version information of the device.

Legal Information

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

System Capacity

You can check the number of users, the number of cards, and the number of face images that the device can store.

Go to **Maintenance Center > System Capacity**.

Log

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

System Logs

Search and view system logs.

Process

1. Go to **Maintenance Center > Log > Log**.
2. Select the time range and the log type, then click **Search**.

Related Operations

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

Unlock Records

Search unlock records and export them.

Process

1. Go to **Maintenance Center > Log > Unlock Records**.
2. Select the time range and type, then click **Search**.
Click **Export** to download the log.

Call History

View call logs.

Process

1. Go to **Maintenance Center > Log > Call History**.

Alarm Logs

View alarm logs.

Process

1. Go to **Maintenance Center > Log > Alarm Log**.
2. Select the type and the time range.
3. Click **Search**.

Face Recognition Terminal User Manual

Admin Logs

Search the administrator logs using the administrator ID.

Process

1. Go to **Maintenance Center > Log > Admin Logs**.
2. Enter the admin ID, then click **Search**.
Click **Export** to export administrator logs.

USB Management

Export user information from/to USB.

Process

1. Go to **Maintenance Center > Log > USB Management**.
 NOTE
 - Before exporting data or updating the system, please ensure that the USB is inserted into the device. To avoid failure, do not remove the USB or perform any operations on the device during this process.
 - You must use USB to export information from the device to other devices. Facial images are not allowed to be imported via USB.
2. Select a data type, then click **USB Import** or **USB Export** to import or export the data.

Maintenance

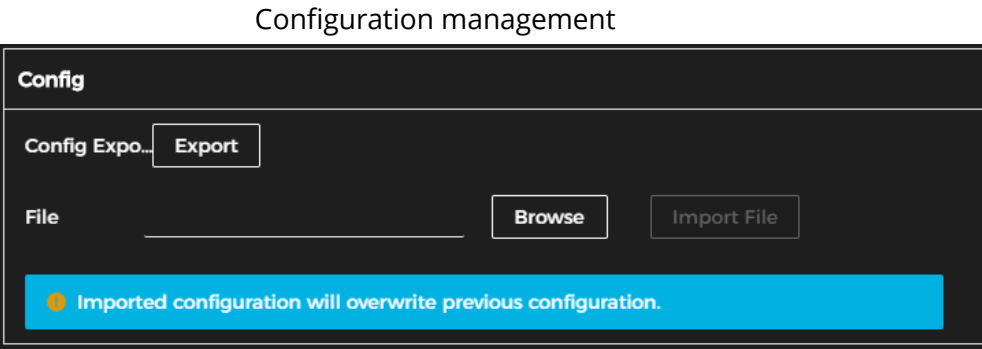
When multiple devices require the same configuration, you can configure parameters for them by importing or exporting configuration files.

Export/Import Configuration Files

Import and export device configuration files. When you wish to apply the same configuration to multiple devices, you can import the configuration file into those devices.

Process

1. Go to **Maintenance Center > Maintenance > Config**.



2. Export or import configuration files.
 - Export.
Click **Export** to download the file to the local PC.
 NOTE
The IP will not be exported.
 - Import.
 1. Click **Browse** to select the configuration file.
 2. Click **Import File**.
 NOTE
The configuration file can only be imported into devices of the same model.

Restore to Default

Process

1. Go to **Maintenance Center > Maintenance > Config**.
 CAUTION
Restoring the device to its default configuration will result in data loss. Please be aware.
2. If necessary, restore to factory default settings.
 - **Factory Defaults:** Resets all the configurations of the Device and delete all the data.
 - **Restore to Default (Except for User Info and Logs):** Reset the device's configuration and delete all data, while retaining user information and logs.

Restart

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

Process

1. Go to **Maintenance Center > Maintenance > Restart**.

Restart

Restart System

Maintenance Time

Tue

▼

02:00

▼

Manual Operation

Restart

Apply

Refresh

2. Set the maintenance time, then click **Apply**.
The device will restart at the scheduled time, or you can click **Restart** to restart it immediately.

Update



- 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 Device during the update.

File Update

Process

1. Go to **Maintenance Center > Update**.
2. In **File Update**, click **Browse**, then upload the update file.



The update file should be a .bin file.

3. Click **Update**.
The device will restart after the update is completed.

Online Update

Process

1. Go to **Maintenance Center > Update**.
2. In the **Online Update** area, select an update method.
 - Select **Auto Check for Updates**, and the device will automatically check for the latest version updates.
 - Click **Manual Check** to see if a new version is available immediately.
3. (Optional) Click **Update Now** to update the device immediately.

Advanced Maintenance

Obtain device information and capture data packets to facilitate troubleshooting for maintenance personnel.

Export

Process

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

Packet Capture

Packet Capture

1. Go to **Maintenance Center > Advanced Maintenance**.

Packet capture

NIC	Device Address	IP 1: Port 1	IP 2: Port 2	Packet Sniffer Size	Packet Sniffer Backup
eth0		Optional	Optional	Optional	Optional
eth2		Optional	Optional	Optional	Optional
lo		127.0.0.1	Optional	Optional	Optional

2. Enter the IP address, then click .
- changes to .
3. After you have gathered sufficient data, please click .
- The captured packets will be automatically downloaded to your PC.

Network Test

1. In the **Network Test** area, enter the destination address, then configure data packet size.

Network test

Network Test

Destination Address

Test

Data Packet Size

64

Byte (64-4096)

Test Result

Copy

2. Click **Test**.

Face Recognition Terminal User Manual

The result will be displayed in the **Test Result** area.

Security (Optional)

Configure 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.

Process

1.

Go to **Security > System Service > HTTPS**.
2.

Enable the HTTPS service.

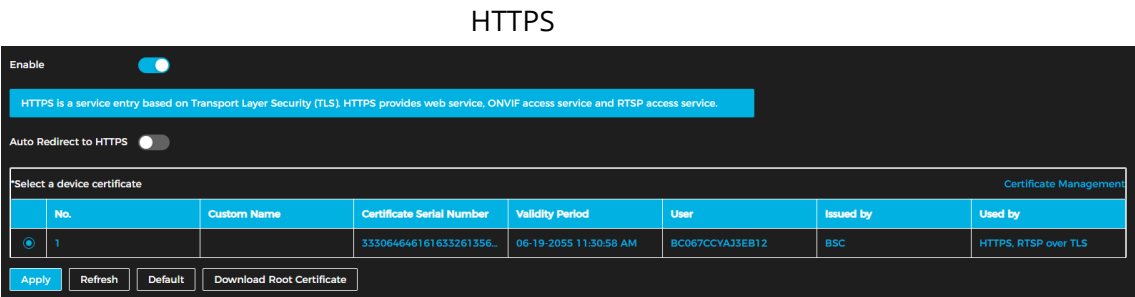
⚠ CAUTION

Enabling features compatible with TLS v1.1 and earlier versions may pose security risks. Please be aware.
3.

Select the certificate.

📝 NOTE

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



4.

Click **Apply**.
Enter "https://IP address: https port" in a web browser. If the certificate is installed, you will be able to successfully log in to the webpage. If not, the webpage will display a certificate error or be untrusted.

Attack Defense

Firewall

Configure the firewall to restrict access to the device.

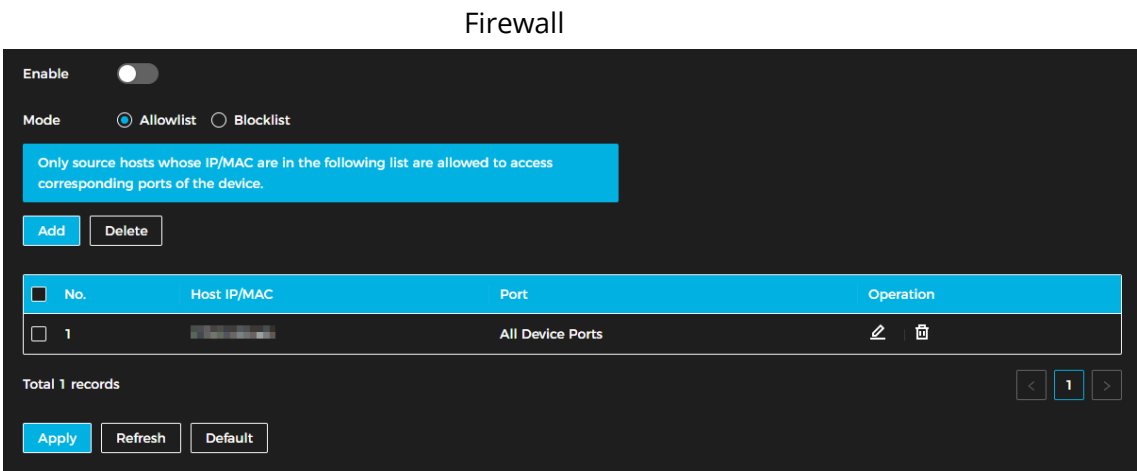
Process

1.

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

2.

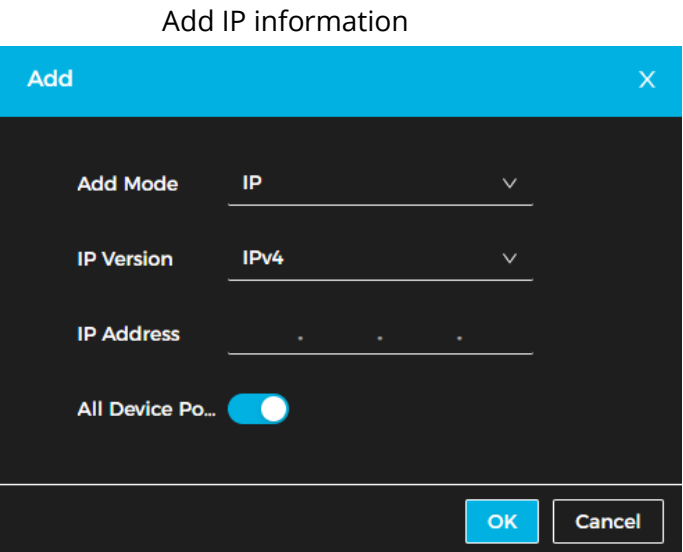
Click to enable the firewall function.



3.

Select the mode: **Allowlist** and **Blocklist**.
 - **Allowlist**: Only IP/MAC addresses on the allowlist can access the Device.
 - **Blocklist**: The IP/MAC addresses on the blocklist cannot access the Device.
4.

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



5.

Click **OK**.

Related Operations

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

Account Lockout

If the number of incorrect password entries reaches the set limit, the account will be locked.

Process

1.

Go to **Security > Attack Defense > Account Lockout**.
2.

Enter the number of login attempts and the duration for which the administrator account

and ONVIF user will be locked.

Account lockout

Device Account

Login Attempt

5time(s)

▼

Lock Time

5

min

ONVIF User

Login Attempt

30time(s)

▼

Lock Time

5

min

Apply

Refresh

Default

- Login Attempt: The limit of login attempts. If the incorrect password is entered within the specified number of times, the account will be locked.
- Lock Time: The period during which you are unable to log in after your account has been locked.

3. Click **Apply**.

Anti-DoS Attack

Enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the device against Dos attacks.

Process

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

Anti-DoS attack

SYN Flood Attack Defe...

☐

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

ICMP Flood Attack Def...

☐

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

Apply

Refresh

Default

3. Click **Apply**.

Installing Device Certificate

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

Create Certificate

Create a certificate for the Device.

Process

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

Face Recognition Terminal User Manual

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



NOTE

The region name must not exceed two characters. We recommend entering the abbreviation of the region name.

5. Click **Create and install certificate**.
After successfully installing the certificate, the newly installed certificate is displayed on the **Device Certificate** page.

Related Operations

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

Apply for CA Certificate and Import

Import the third-party CA certificate into the device.

Process

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

Certificate information (2)

Step 2: Fill in certificate information. X

* IP/Domain Name 172.13.84.237

Organization Unit

Organization

* Region

Province

City Name

Back Create and Download Cancel

5. Click **Create and Download**.
Save the request file to your PC.
6. Apply for a certificate from a third-party certificate authority by using the request file.
7. Import the signed CA certificate.
 - Save the CA certificate to your PC.
 - Click **Installing Device Certificate**.
 - Click **Browse** to select the CA certificate.
 - Click **Import and Install**.
After successfully installing the certificate, the newly installed certificate will be displayed on the device certificate page.
 - Click **Recreate** to regenerate the request file.
 - Click **Import Later** to import the certificate at another time.

Related Operations

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

Install Existing Certificate

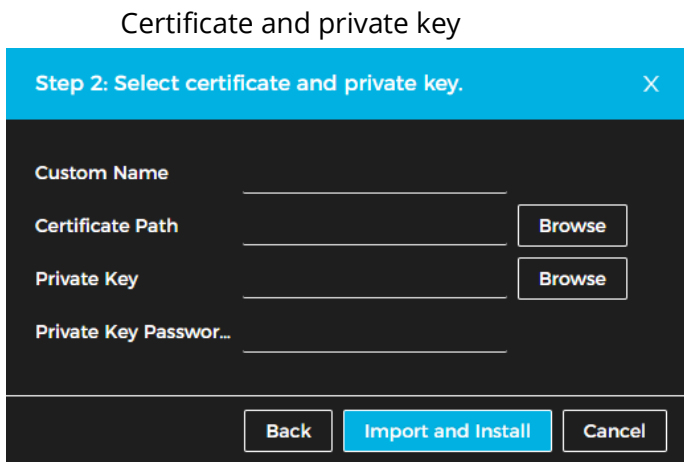
If you already have the certificate and private key files, please import the certificate and private key files.

Process

- Go to **Security > CA Certificate > Device Certificate**.
- Click **Install Device Certificate**.
- Select **Install Existing Certificate**, then click **Next**.
- Click **Browse** to select the certificate and private key file, and enter the private key

Face Recognition Terminal User Manual

password.



5. Click **Import and Install**.
After successfully installing the certificate, the newly installed certificate will be displayed on the device certificate page.

Related Operations

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

Installing the Trusted CA Certificate

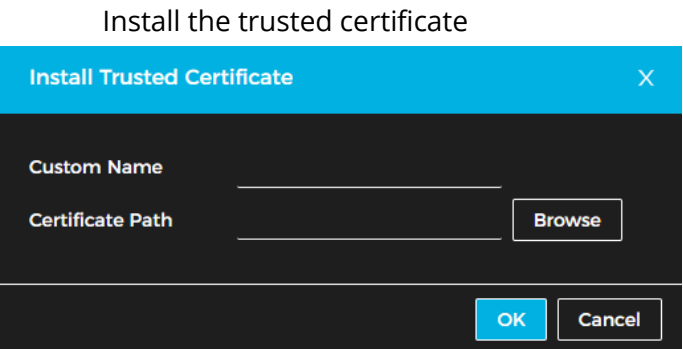
A trusted CA certificate is a type of digital certificate used to verify the identity of websites and servers. For example, when using the 802.1x protocol, the CA certificate of the switch is necessary for verifying its identity.

Background Information

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

Process

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



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

Related Operations

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

Cybersecurity Recommendations

Account Management

1. Use complex passwords

Please refer to the following suggestions for setting a password:

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

2. Change passwords Regularly

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

3. Allocate accounts and permissions appropriately

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

4. Enable account lockout function

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

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

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

Service Configuration

1. Enable HTTPS

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

2. Encrypted transmission of audio and video

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

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

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

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

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

4. Change HTTP and other default service ports

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

Network Configuration

1. Enable Allow list

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

2. MAC address binding

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

3. Build a secure network environment

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

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

Security Auditing

1. Check online users

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

2. Check device log

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

3. Configure network log

Due to the limited storage capacity of the device, the number of logs stored is also restricted. If you need to retain logs for an extended period, it is recommended to enable the network

Face Recognition Terminal User Manual

logging feature to ensure that critical logs can be synchronized to the network log server for tracking.

Software Security

1. Update firmware in time

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

2. Update client software in time

We recommended to download and use the latest client software.

Physical Protection

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

could void the user’s authority to operate the equipment.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Non-modification Statement:

Changes or modifications not expressly approved by the party responsible for compliance