



Face Recognition Terminal (C-F4A)

User Manual

Preface

This user manual covers the features and operations of the Face Recognition Terminal (the "device"). Read it before installing or operating the device and keep it accessible for future reference.

Privacy Notice

Using this device may involve collecting personal data, including facial images, audio, fingerprints, and license plate numbers. Comply with applicable privacy legislation in your jurisdiction. This includes posting notices in monitored areas and making relevant contact information available to those affected.

Safety Instruction

The following signal words are used throughout this user manual.

Signal Words	Meaning
 DANGER	Failure to follow this warning can cause death or serious physical harm.
 WARNING	Disregarding this warning may cause minor or moderate bodily injury.
 CAUTION	Overlooking this notice may result in equipment damage, data loss, reduced performance, or other unintended consequences.
 TIPS	Useful guidance to complete tasks more efficiently.
 NOTE	Indicates supplementary information relevant to the current topic.

Revision History

Version	Revision Content
V1.1	Updated "Export/Import Configuration Files" sections.
V1.0	First release.

About the Manual

- This manual is for reference only. Specifications are subject to change without notice.
- No liability is accepted for losses arising from use of the product in ways that deviate from this user manual.
- This user manual is updated in line with current laws and regulations. For the latest version, refer to the printed copy, CD, QR code, or Luminys website. This manual is for reference only. Minor differences may exist between the electronic and printed versions.
- Designs and software may change without prior notice. Updates to the product may result in differences between the actual product and this user manual. Contact customer service for current information and additional documentation.
- Descriptions of functions, operations, or technical data may contain typographical errors or minor inaccuracies. The right of final interpretation is reserved.
- If this user manual (PDF format) does not open, update your PDF reader or switch to a different one.
- Trademarks, registered trademarks, and company names mentioned in this user manual belong to their respective owners.
- For equipment-related issues, visit the Luminys website to contact the supplier or customer service.

Transportation

Maintain the Terminal within its rated humidity and temperature ranges throughout transport, operation, and storage.

Storage

Always store the Terminal within its rated humidity and temperature ranges.

Installation

- Before connecting the power adapter to the Terminal, disconnect it from its power source.
- Follow all applicable local electrical safety codes. Verify that the supply voltage is stable and within the Terminal's rated power specifications.
- Use a single power source for the Terminal.
- Take care when handling batteries; improper handling can cause fire or explosion.
- Select a power supply that satisfies the Terminal's electrical requirements.
 - ◇ When selecting a power adapter, ensure it meets the following criteria.
 - The power supply must comply with IEC 60950-1 and IEC 62368-1.
 - The voltage must meet SELV (Safety Extra Low Voltage) requirements and stay within the ES-1 limit.
 - For devices rated at or below 100 W, the power supply must comply with LPS requirements and remain within the PS2 rating.
 - ◇ Use the power adapter supplied with the Terminal where possible.
 - ◇ Check the Terminal label for power supply specifications before selecting an adapter.
- Wear a safety helmet and harness when working at height and take all other required precautions.
- Keep the Terminal out of direct sunlight and away from heat sources.
- Shield the Terminal from moisture, dust, and smoke.
- Secure the Terminal on a stable, level surface to prevent it from falling.
- Place the Terminal in a well-ventilated location and ensure all ventilation openings remain clear.
- Only use a power adapter or cabinet power supply obtained from the manufacturer.
- Select a power cord rated to match the Terminal's specified power requirements.
- This Terminal is a Class I electrical device and must be connected to a grounded (protective earth) power outlet.

Operation Requirements

- Confirm the power supply is correct before switching on the Terminal.
- Connect the protective earth before powering on the Terminal.
- Switch off the adapter before unplugging the power cable from the controller.
- During operation, ensure the Terminal's input and output remain within its rated power range.
- Use the Terminal only within its specified humidity and temperature range.
- Do not allow liquids near the Terminal. Keep containers of liquid away from and off the unit.
- Only qualified service personnel may disassemble the Terminal.
- This device is professional-grade and intended for use by qualified personnel.
- Install and use the Terminal in locations inaccessible to children.



Table of Contents

- Preface.....II
- Overview 1
- Local Operations..... 2
 - Basic Configuration Process 2
 - Standby Screen 2
 - Initialization 3
 - Log In..... 4
 - Password Resetting..... 5
 - Unlock Options 5
 - By Cards..... 5
 - By Face..... 5
 - By User Password 5
 - By Administrator Password 6
 - By Temporary Password 6
 - User Management..... 6
 - Add Users 6
 - View User Information 9
 - Access Control Management..... 9
 - Unlock Method 9
 - Combination..... 9
 - By Period..... 10
 - By Multi-user 11

Alarms.....	11
Face Parameters	12
Lock Status Config.....	15
Verification Time Interval	16
Administrator Password	16
Communication Settings	16
Network Settings.....	17
IP Settings	17
Auto Registration	18
Wi-Fi	19
Wi-Fi AP	19
RS-485 Settings.....	20
Wiegand Settings.....	21
Local Functions	22
Reports.....	25
Unlock Records.....	25
System Capacity	25
System Settings.....	25
Time	25
Volume Settings	26
Language.....	26
Screen Settings.....	26
Factory Defaults	27
About	27
Restart	27
Web Operations	28
Basic Configuration Process on Web.....	28
Initialization	28
Log In.....	29
Password Resetting.....	29
Home Page	30
User Management.....	30
Access Control.....	33
Door Parameters.....	33
Basic Settings	33
Unlock Settings	34

Alarm.....	35
Alarm Linkage Setting (Optional)	37
Alarm Event Linkage	38
Face Parameters	39
Card Settings.....	41
Weekly Schedule	43
Holiday Schedule.....	44
Privacy Setting	46
Port Config	46
Back-end Comparison	47
First-Person Unlock.....	47
Intercom Settings	48
Using the device as the SIP Server.....	48
Configuring the SIP Server	48
Local device Config.....	49
Adding the Outdoor Station.....	49
Adding the Indoor Monitor	50
Using the device as the SIP Client.....	52
Configuring a SIP Server for the device.....	52
Local device Config.....	53
Call Config	54
Communication Settings	55
Network Settings.....	55
TCP/IP	55
Wi-Fi	57
Wi-Fi AP	57
Port	58
Basic Services	59
Cloud Service.....	60
Auto Registration	61
Auto Upload.....	62
RS-485 Settings.....	63
Wiegand Settings.....	64
System Settings.....	65
Account.....	65
Adding Administrators.....	65

Adding ONVIF Users	65
Resetting the Password	66
Viewing Online Users	67
Time	67
Shortcut Settings	67
Video	69
Audio	72
Motion Detection	73
View Selection	74
Advertisement	75
Adding Resources	75
Configuring Subject	76
Management Center	77
System Information	77
Version Information	77
Legal Information	77
System Capacity	78
Log	78
System Logs	78
Unlock Records	78
Call History	78
Alarm Logs	78
Admin Logs	79
USB Management	79
Maintenance	79
Export/Import Configuration Files	79
Restore to Default	80
Restart	80
Update	80
File Update	80
Online Update	81
Advanced Maintenance	81
Export	81
Packet Capture	81
Security (Optional)	82
Configure HTTPS	82

Attack Defense	83
Firewall	83
Account Lockout	84
Anti-DoS Attack	84
Installing device Certificate.....	85
Create Certificate	85
Apply for CA Certificate and Import.....	86
Install Existing Certificate	87
Installing the Trusted CA Certificate.....	87
Cybersecurity Recommendations	89

Overview

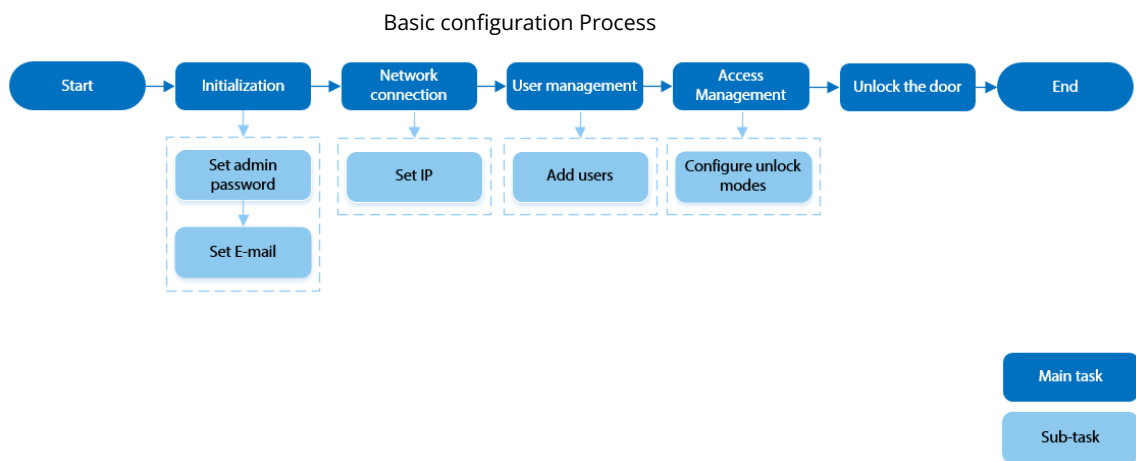
This terminal supports door access via facial recognition, passwords, cards, and combinations of these methods. Deep learning algorithms power its recognition engine. The device integrates with management platforms to support a range of deployment scenarios.

- Configuration options differ by product model. Check your specific unit for exact settings.
- Devices without a touchscreen require a connected mouse to perform configuration. This user manual uses a touchscreen device as its reference model.

Local Operations

- Settings differ by model. Refer to your specific device for details.
- Instructions in this section are based on a touchscreen model.
- External expansion modules are supported on select models only.
- Some UI labels may be truncated when space is limited. Press and hold the label for 3 seconds to reveal.

Basic Configuration Process

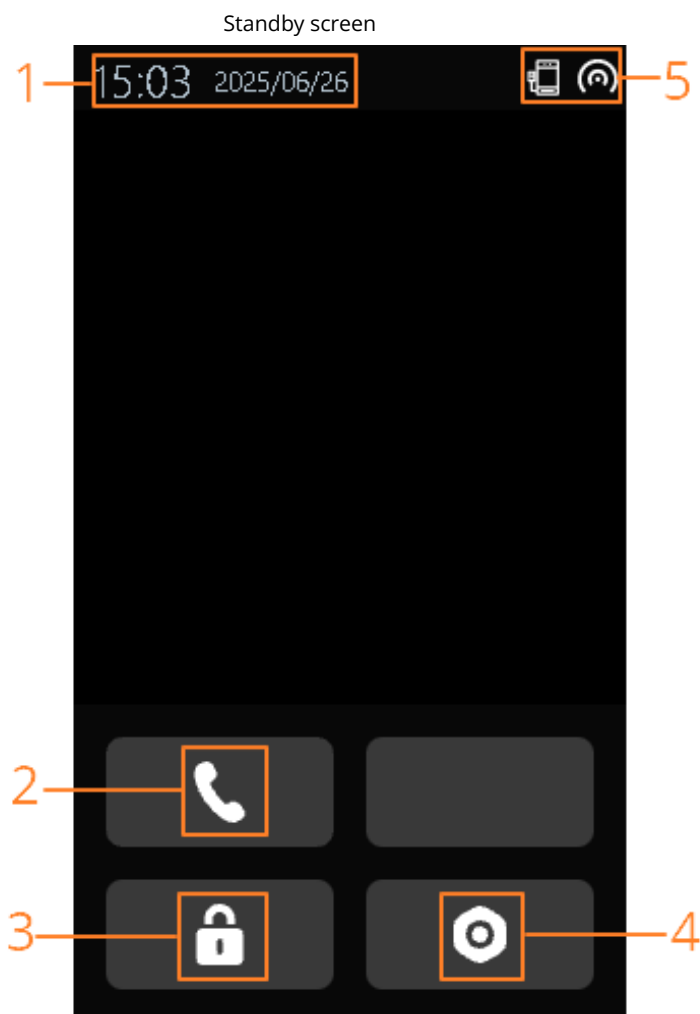


Standby Screen

Access control is available through face recognition, card, and password. The intercom function supports calls. Available unlock methods depend on the product model.

 NOTE

- This manual is for reference only. The standby screen shown here may differ slightly from your device.
- After 30 seconds of inactivity, the device enters standby mode.



Home screen description

No.	Name	Description
1	Date and time	Shows the current date and time.
2	Call	• In server mode, the device can place calls to outdoor stations and indoor monitors. • When the management platform acts as the server, devices can reach outdoor stations, indoor monitors, and the management platform.
3	Password	Unlock the door by entering a user password, administrator password, or temporary password.
4	Main Menu	Tap the icon to open the setting page and configure device functions.
5	Status display	Display Wi-Fi, network, and expansion module status. Wi-Fi and expansion module indicators appear on supported models only. Tap  to enter the Wi-Fi AP screen. For more details, refer to "Wi-Fi AP".

Initialization

On first use or after a factory reset, select a language, then assign a password and email address to the administrator

account. This account gives you access to the device's main menu and web interface.

 NOTE

- If you forget the administrator password, submit a reset request to the email address set during initialization.
- Passwords must be 8–32 characters and contain at least two of the following: uppercase letters, lowercase letters, numbers, or special characters (excluding ' " ; : &).

Log In

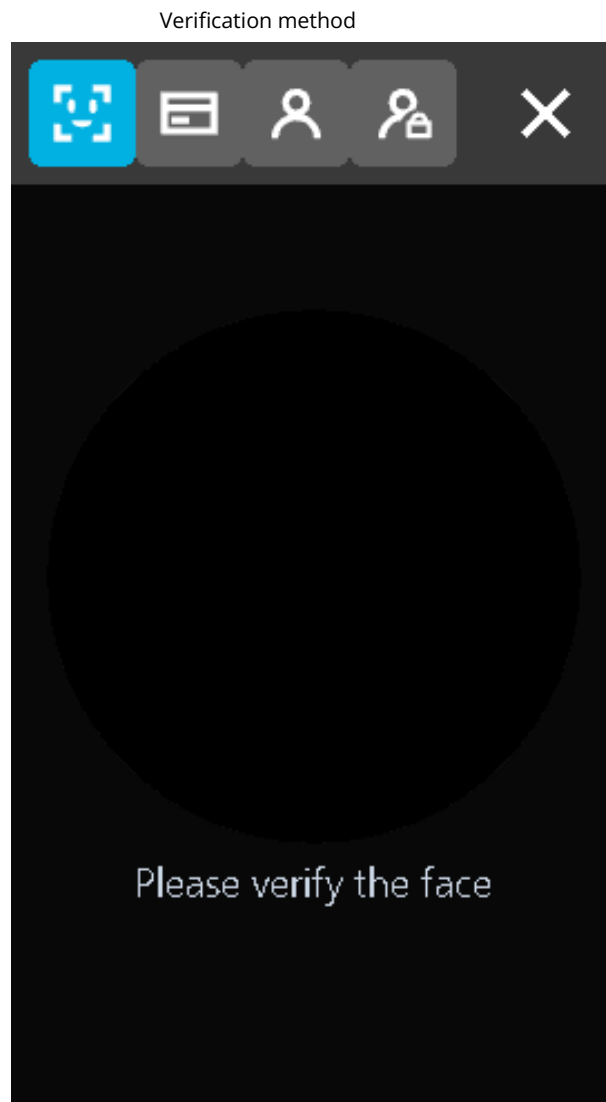
Access the main menu to configure the device. Only administrator and management accounts can enter the main menu. On first use, log in with the administrator account, then create any additional management accounts needed.

Background Information

- Management account: Has main menu access, but no access control permissions.
- Administrator account: Has both main menu access and access control permissions.

Process

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



- Face: Enter the main menu via facial recognition.
- Card: Enter the main menu by swiping your card.
- Password: Enter the administrator account's user ID and password.
- admin: Enter the admin password to open the main menu.

Password Resetting

Reset the administrator password using the email address linked to the account.

Precondition

An email address must have been set up during initialization before you can reset your password.

Process

1. Tap  or press and hold the standby screen for 1.5 seconds.
2. Tap , then tap Forgot password.
3. Review 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

- Scanning the QR code triggers a security code sent to your registered email. The code expires 24 hours after it is issued.
- Each QR code generates a maximum of two security codes. If a code is no longer valid, refresh the QR code and scan it again.

6. Enter the security code.

NOTE

If the wrong security code is entered five times in a row, the administrator account is locked for 5 minutes.

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

NOTE

The new password must be 8–32 characters and include at least two of these character types: uppercase letters, lowercase letters, numbers, or special characters (excluding ' " ; &).

9. Click OK.

Unlock Options

Supported unlock methods include face recognition, passwords, fingerprints, cards, and combinations thereof.

By Cards

Present the card to the card reader to unlock the door.

NOTE

This feature is available on select models only.

By Face

Face recognition verifies identity through the camera. Keep your face centered within the detection frame.

By User Password

Unlock the door by submitting your user ID and password.

Process

1. Tap  on the standby screen.

2. Tap , then enter the user ID and password.
3. Tap OK.
When PIN Code Authentication is enabled under Access Control > Access Control Parameters in the web interface, you can verify with a password only—no user ID is required.

By Administrator Password

Entering the administrator password alone unlocks the door. This method works on all doors except those configured as always locked. Each device supports a single 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.



A door configured as always locked cannot be opened with the administrator password.

By Temporary Password

A temporary password generated by LumiViewer grants time-limited door access.

Process

1. Add the device to LumiViewer.
LumiViewer generates a temporary password valid for door access until its expiry time.
2. Tap  on the home screen, then tap .
3. Enter the temporary password, then tap OK.

User Management

Manage users by adding new accounts, viewing the user and administrator list, and updating user details.



Images in this user manual are illustrative and may not match the actual product appearance.

Add Users

Process

1. Go to User Management >  on the main menu page.
2. Set the required 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)

The screenshot shows a mobile application interface for adding a user. At the top, there is a dark header bar with a back arrow on the left, the text 'Add User' in the center, and a checkmark on the right. Below the header, there are five rows of configuration options, each with a label on the left and a value on the right, followed by a right-pointing chevron. The options are: 'Holiday Schedule' with value '255-No Plan', 'Validity Period' with value '2037-12-31', 'User Type' with value 'General User', 'Department' with value '1-Default', and 'Schedule Mode' with value 'Department Sc...'. At the bottom of the screen, there is a dark bar with a left arrow, the text '2/2' in the center, and a right arrow.

Parameters description

Parameter	Description
User Permission	- User: Door access permission only. - Admin: Can configure the device, with no door access permissions.
User ID	The user ID follows the same format as the employee ID: up to 30 alphanumeric characters.
Name	Accepts up to 32 characters, including letters, numbers, and symbols.
Face	Position your face within the frame; the system captures the image automatically. Re-register if the result is not acceptable.
Card	Each user can register up to 5 cards. Enter the card number manually or swipe it — the device reads the card data automatically. Enable the Duress Card function so that using a forced card to unlock the door triggers an alarm.  NOTE - This function is only available on certain models. - Each user can only set one duress card.
Password	Set a user password of up to 8 digits. The emergency password is derived by incrementing the last digit of the unlock password by 1 (e.g., 12345 → emergency: 12346; 789 → emergency: 780). Using the emergency password to unlock triggers an emergency alarm.
Weekly Schedule	Restricts door access to a defined time window. For details, see "Weekly Schedule".
Holiday Schedule	Extends door access to configured holiday dates. For details, see "Holiday Schedule".

Parameter	Description
Validity Period	Defines the expiry date for this user's access permissions.
User Type	- General User: Has standard door access. - Blocklist User: Triggering a door unlock generates a blocklist alarm. - Guest User: Door access is limited to a set time window or a fixed number of uses. Access is revoked once either limit is reached. - VIP User: When the door is in Normal status, VIP users can open it at any time, bypassing other scheduling rules. - Other User: The door stays unlocked for 5 seconds after this user authenticates.  NOTE This feature is unavailable when remote verification is active.
Department	Assign the user to a department; useful when applying department-level schedules.  NOTE This feature is available on specific models only.
Schedule Mode	- Department Schedule: Applies the department's schedule to this user. - Personal Schedule: Applies an individual schedule to this user.  NOTE This feature is available on specific models only.

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

Use the User Management screen to search, edit, or delete existing users.

- Search for users: Tap  and enter the username or user ID.
- Edit a user: Tap the user's entry to update their information.
- Delete a user: Select the user and tap .

Access Control Management

Set door behavior, including unlock modes, alarm linkage, and access schedules. Supported unlock modes vary by product model.

Unlock Method

Combination

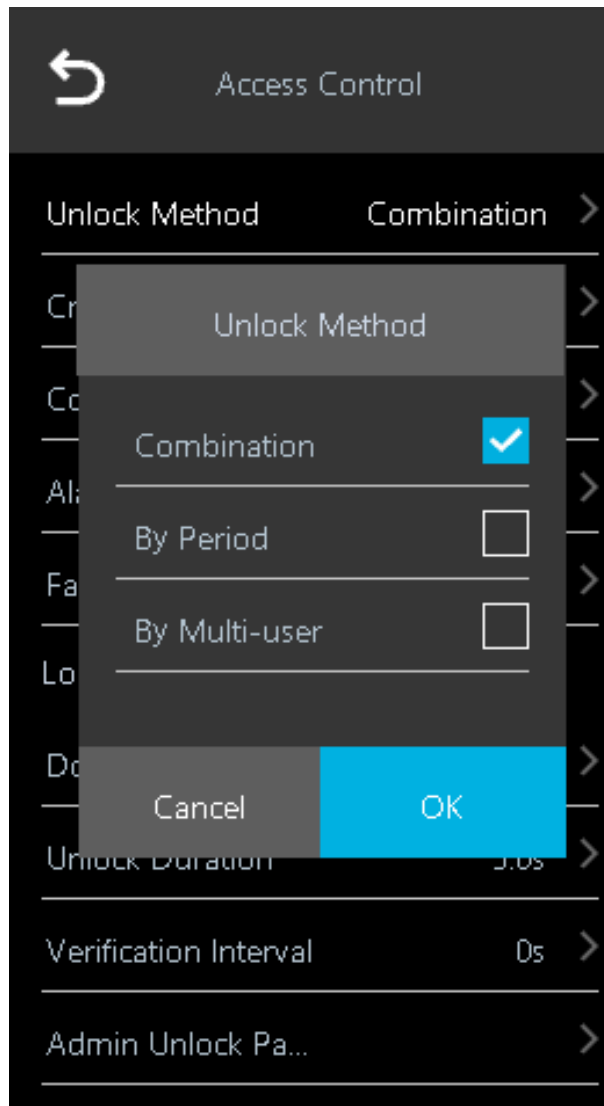
Configure the door to accept a card, face recognition, a password, or a combination as valid credentials. Supported

modes vary by 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, select the unlock combination, and tap OK.
4. Tap Combination Method, select And or Or, and tap OK.
 - And: All selected credentials must be verified to open the door.



NOTE

Verification must follow the sequence: card → face → password.

- Or: Any one of the selected credentials is sufficient to open the door.

By Period

Process

1. On the main menu, select Access Control.
2. Tap Unlock Method and select By Period.
For details on configuring unlock by period, see "Unlock Settings".
3. Tap OK.

By Multi-user

Process

1. On the main menu, select Access Control.
2. Tap Unlock Method and select By Multi-user from the list.
For details on configuring unlock by multiple users, see "Unlock Settings".
3. Tap OK.

Alarms

The device triggers an alarm whenever it detects an irregular entry or exit event.

Process

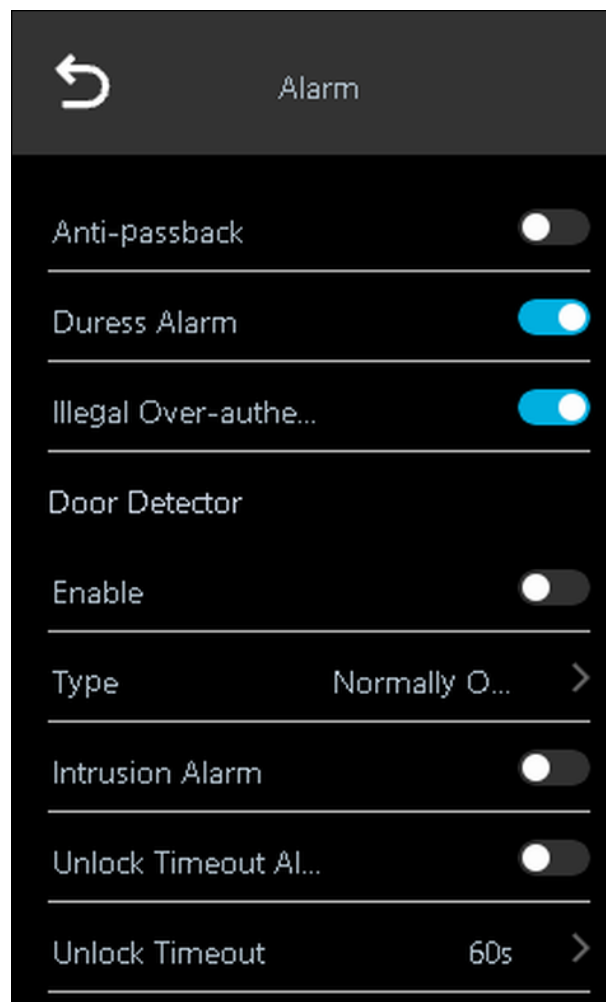
1. Go to Access Control > Alarm on the main menu.
2. Enable the alarm type.



NOTE

Alarm types vary by product model.

Alarm



Description of alarm parameters

Parameter	Description
Anti-passback	Identity verification is required for both entry and exit. This blocks cardholders from sharing their cards with others for access. Once enabled, a cardholder must tap out through the exit card reader before the system grants re-entry. Use the "in" card reader to enter the secure area and the "out" card reader to exit. • A verified entry followed by an unverified exit triggers an alarm on the next entry attempt, which will be denied. • An unverified entry followed by a verified exit also triggers an alarm on the next entry attempt, which will be denied.  NOTE When only one lock is connected, verification on the device counts as entry; verification on the external card reader counts as exit. This is the default behavior.
Duress Alarm	Using a duress card or duress password to open the door activates an alarm.
Illegal Over-authentication Alarm	Five consecutive failed password or card attempts within 60 seconds triggers an excessive invalid-credential alarm, which remains active for a set duration.
Door Detector	Attach a door detector to the device to receive an alarm when the door opens or closes in an unexpected state. Two detector types are supported: normally closed and normally open. • 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.
Type	
Intrusion Alarm	An abnormal door opening activates an intrusion alarm, which runs for a configured duration.
Unlock Timeout Alarm	If the door stays unlocked beyond the configured timeout, a door timeout alarm activates and runs for the defined period  NOTE Both the door detector and door timeout functions must be active at the same time.
Unlock Timeout	

Face Parameters

Available face parameters differ by product model.

Process

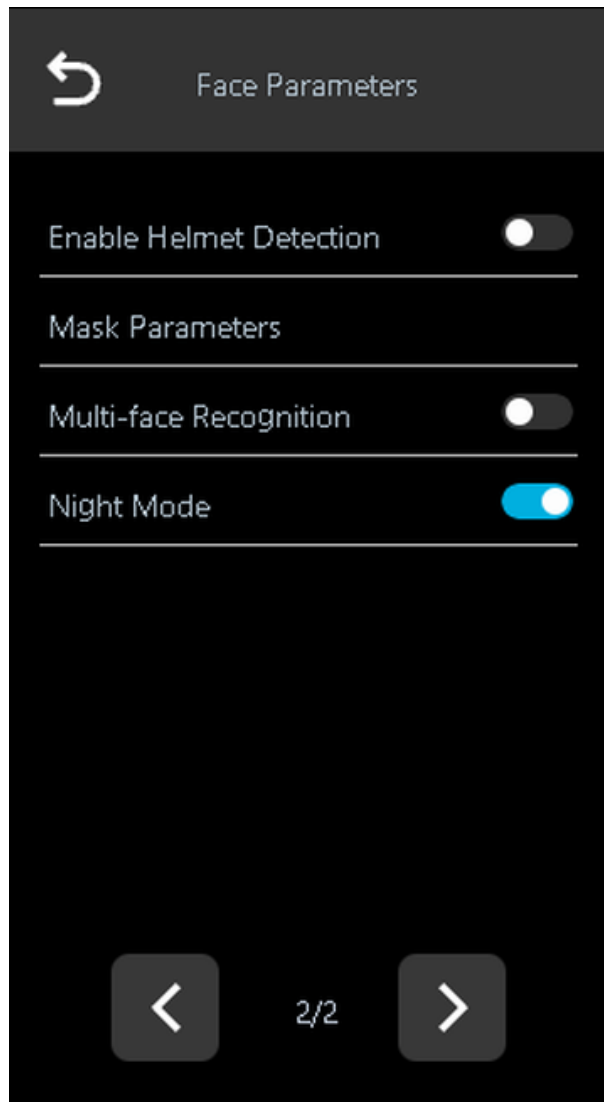
1. Go to Access Control > Face Parameters on the main menu.
2. Configure the face parameters, then tap .

 Face Parameters

Face Recognition Threshold	85
Max Face Recognition Angle ...	30
Valid Face Interval (sec)	3
Invalid Face Interval (sec)	10
Recognition Distance	1.5m
Anti-spoofing Level	Close
Enable Beautifier	☒

 1/2 

Face parameter (2)



Description of face parameters

Name	Description
Face Recognition Threshold	Controls recognition accuracy. Raising the threshold reduces false matches.  NOTE A very low threshold (for example, 0) results in an extremely high error rate.
Max Face Recognition Angle Deviation	Defines the widest face angle the device will accept during detection. A larger value widens the acceptable range; angles outside that range may fail detection.
Valid Face Interval (sec)	After a face is successfully recognized, the device waits for the configured interval before recognizing that same face again.
Invalid Face Interval (sec)	After a failed recognition attempt, the device waits for the configured interval before trying to recognize that face again.
Recognition Distance	The detection range between the face and the lens.
Anti-spoofing Level	Blocks attempt to use photos, videos, masks, or other spoofing materials for unauthorized access.
Enable Beautifier	Applies beautifying enhancement to captured face images.

Name	Description
Enable Helmet Detection	Checks for a safety helmet. The door will not open for anyone not wearing one.
Mask Parameters	- Mask mode: - No Detect: The device does not check whether a mask is worn during face recognition. - Mask Alert: If no mask is detected, the device prompts the user to wear one but still allows entry. - Mask Required: If no mask is detected, the device prompts the user to wear one and denies entry. - Mask Recognition Threshold: A higher threshold increases accuracy when recognizing masked faces and reduces misidentification.
Multi-face Recognition	The device can detect 4 to 6 faces at once, depending on the model. This feature is not available with the combination unlock method; the door unlocks when any one person is successfully verified.  NOTE The number of supported face images varies by product model.
Night Mode	- Turn on: The illuminator activates in low-light conditions. - Turn off: The illuminator always stays off.  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.

Lock status

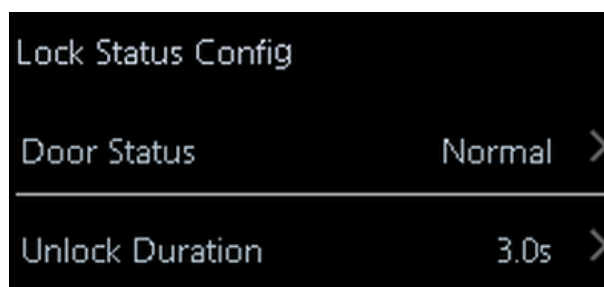


Table 2-5 Parameters description

Parameter	Description
Door Status	- Normally Open: The door always remains in an unlocked state. - Normally Closed: The door always remains in a locked state. - Normal: If Normal is configured, the door will be locked and unlocked according to settings.
Unlock Duration	After access is granted, the door stays unlocked for a set duration to let the person through.

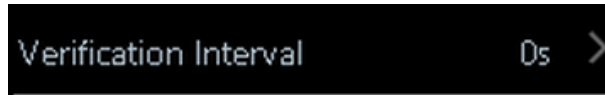
Verification Time Interval

When multiple verifications occur within the configured interval, only the first is accepted. Subsequent attempts within that window will not open the door.

Process

1. Select Access Control on the main menu.

Verification interval



2. Enter the time interval, and then tap .

Administrator Password

The administrator password opens the door regardless of user type. Each device supports a single administrator unlock password.

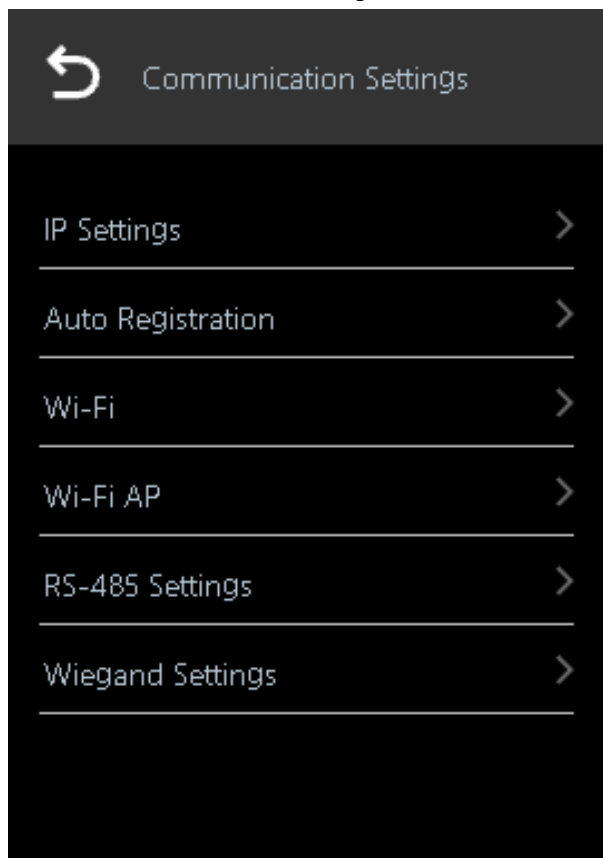
Process

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

Set up network connectivity, RS-485, and Wiegand from this section.

Communication Settings





NOTE

RS-485 and Wiegand port availability varies by product model.

Network Settings

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

IP Settings

Assign an IP address to put the device on the network, which then allows access via the webpage and management platform.

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 (DHCP). When enabled, the network automatically assigns an IP address, subnet mask, and gateway.
IP Address/Subnet Mask/Gateway Address	The IP address, subnet mask, and gateway must belong to the same network segment.
Preferred DNS	Primary DNS server IP address.
Alternate DNS	Secondary DNS server IP address.

Parameter	Description
Cloud Service	Manage the device without DDNS registration by using port mapping and transit servers.

3. Tap .

Auto Registration

Register the device with a management platform to manage it remotely.

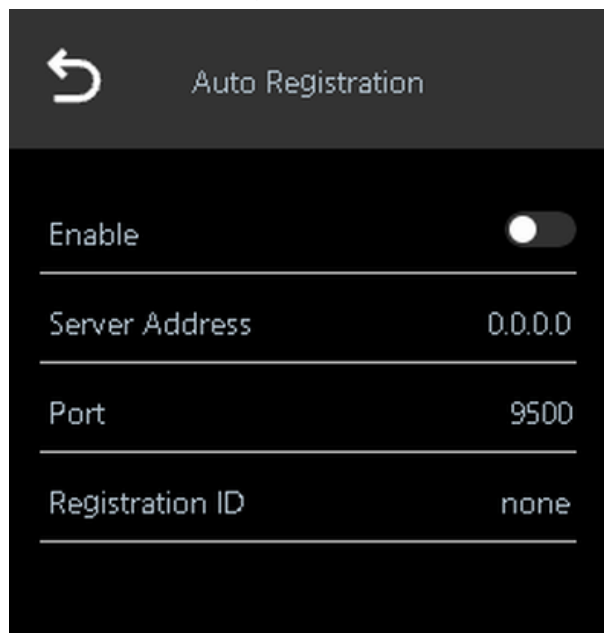
Process

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



Restrict management platform permissions to reduce security risks and prevent data loss.

Active registration



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

Auto registration

Parameter	Description
Server Address	IP address of the management platform.
Port	Port number of the management platform.
Registration ID	Assign a custom device ID to this device.  NOTE The registration ID on the management platform must match the one configured on the device.

Wi-Fi

Connect the device to the network over Wi-Fi.

Background Information



NOTE

This feature is only available on specific models.

Process

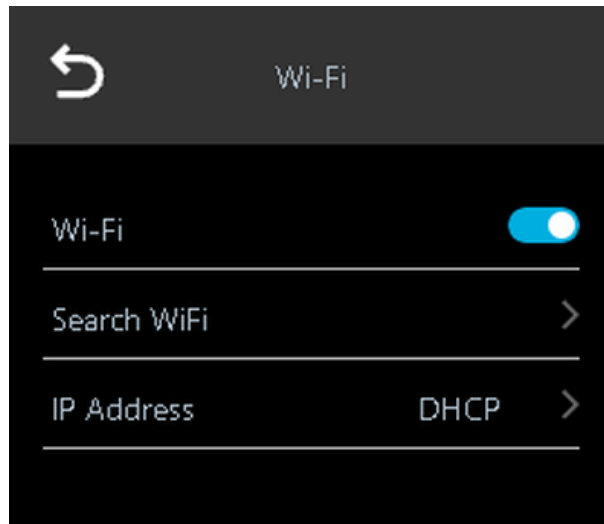
1. Go to Communication Settings > Wi-Fi on the main menu.
2. Enable Wi-Fi.



NOTE

- Wi-Fi is available on certain models only.
 - Wi-Fi and Wi-Fi AP cannot be enabled at the same time.
 - Allow approximately 1 minute for the Wi-Fi connection to establish after enabling.
3. Tap Search Wi-Fi to search for available wireless networks.
 4. Select a Wi-Fi and enter the password.

Connect to Wi-Fi



Related Operations

Tap IP Address to toggle DHCP. When enabled, Wi-Fi IP addresses are assigned automatically.

Wi-Fi AP

Connect a PC or mobile device to the device's Wi-Fi access point to reach the webpage. Available on specific models only.

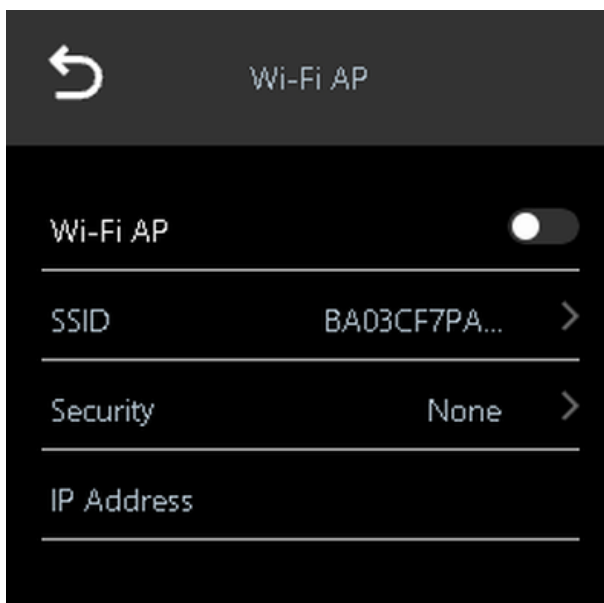
Process

1. Go to Communication Settings > Wi-Fi AP on the main menu.
2. Enable Wi-Fi AP.
Configure the Wi-Fi AP Security.
Select None for connecting to the Wi-Fi AP, or WPA2-Personal to configure a password.

 NOTE

- Wi-Fi AP and Wi-Fi cannot both be active at the same time.
- Wi-Fi AP is automatically active for 30 minutes each time the device powers on.

Connect to Wi-Fi AP



Related Operations

Tap the corner of the standby screen to check Wi-Fi AP status. Log in to the main menu to change any settings.

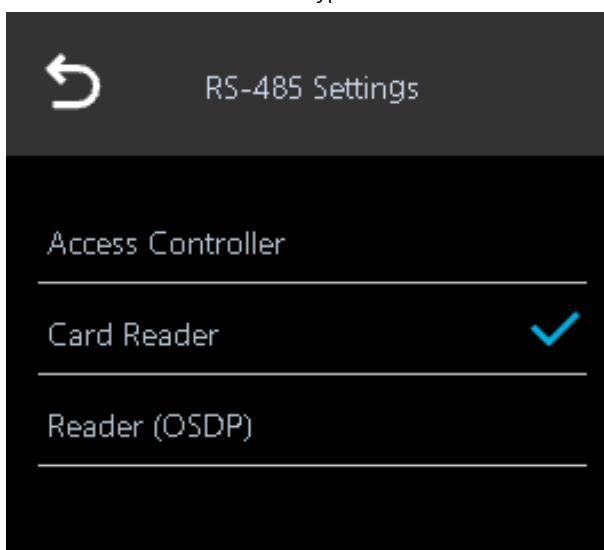
RS-485 Settings

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 operates as a card reader and forwards data to external access controllers. Output Data Type: • Card Number: Card swipe outputs data by card number; other unlock methods output by the user's first card number. • No. : Outputs data based on the user ID.  NOTE • After successful verification, the device sends the data to the access controller and displays the controller's verification result. • After a failed verification on the device, the data is not transmitted to the access controller, and the device shows a failure result.
Card Reader	The device acts as an access controller connected to an external card reader.
Reader (OSDP)	The device connects to a card reader via the OSDP protocol.

Wiegand Settings

The device operates in both Wiegand input and output modes.

NOTE

This feature is only available on specific models.

Process

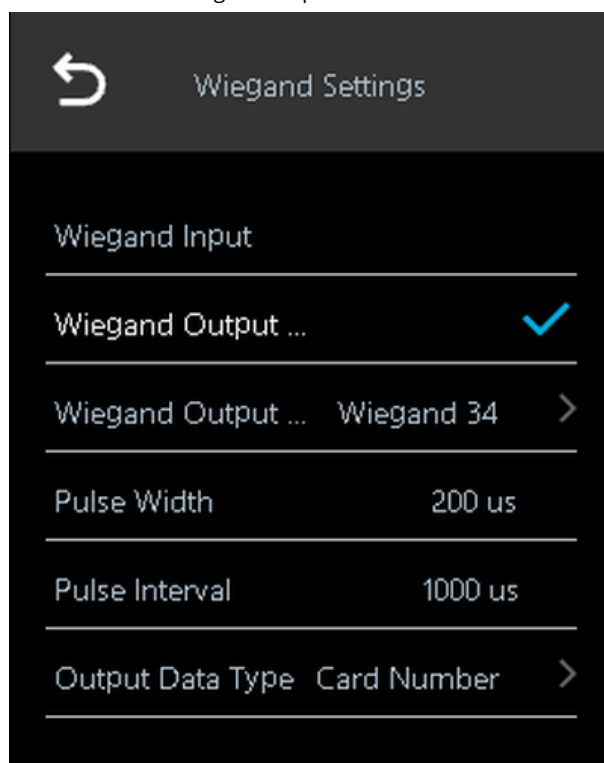
1. Select Communication Settings > Wiegand Settings on the main menu.
2. Select a Wiegand.
 - When connecting an external card reader, select Wiegand Input.

NOTE

If the device is connected to a third-party device through the Wiegand input port and the displayed card number is reversed, enable Card No. Inversion.

- Use Wiegand Output selection when the device used as a card reader, then connected to a controller or another access terminal.

Wiegand output



Description of Wiegand output

Parameter	Description
Wiegand Output Type	Choose a Wiegand format for reading ID 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	Set the pulse width and interval for Wiegand output.
Pulse Interval	
Output Data Type	Choose the data type to output. • User ID: Outputs user ID data in hexadecimal or decimal format. • Card Number: Outputs the user's primary card number.

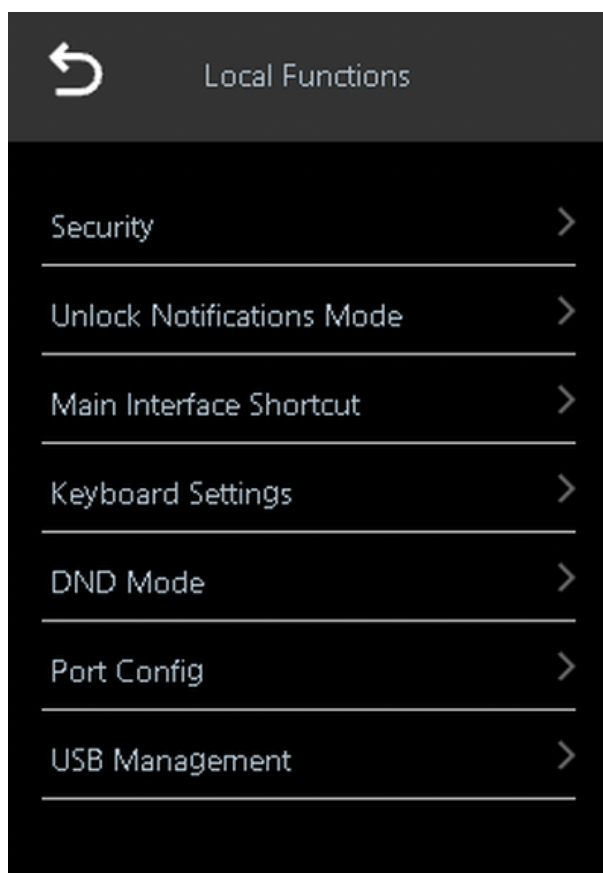
Local Functions

Access Local Functions from the main menu.

 NOTE

Available functions vary by product model.

Functions



Function description

Parameter	Description
Security	• Password Reset: Allows password resets when enabled. • Enable HTTPS: Switches CGI access to HTTPS for encrypted communication. HTTP is used when disabled.  NOTE The device restarts automatically when HTTPS is enabled. • Enable CGI: Allows the web server to execute programs via a standardized protocol. Enabled by default. • Enable SSH: Encrypts transmitted data using the Secure Shell Protocol. • Capture: Automatically captures facial images each time the door is unlocked. • Clear all snapshots: Deletes all automatically captured photos.
Unlock Notifications Mode	Controls the on-screen notification displayed during identity verification. • High Speed Mode: Displays Successfully verified or not authorized. • Simple Mode: Shows user ID, name, and verification time on access; shows Not authorized and the denial time when access is denied. • Standard: Shows the registered face image, user ID, name, and verification time on access; shows Not authorized and the time when denied. • Contrast Mode: Shows both the captured and registered face images alongside user ID, name, and time on access; shows Not authorized when denied.

Parameter	Description
Main Interface Shortcut	Choose the authentication method shown on the standby screen. • Password: Adds a password icon to the standby screen. • Doorbell: Adds a doorbell icon to the standby screen. ◇ Local device Ringer: Tap the bell icon on the standby screen to ring the device. ◇ Ringtone Config: Choose a ringtone. ◇ Ringtone Time (sec): Duration of the ringtone in seconds (1–30). Default is 3. • Call: Adds a call icon to the standby screen. • Call Type ◇ Call room: Tap the call icon, then enter a room number to dial. ◇ Call management center: Tap the call icon to ring the management center. ◇ Call Phone: Tap the call icon to dial a phone number.  NOTE LumiViewer calls are only supported under this call type. • SIP Server: Enable SIP to configure the device as a SIP server.
Keyboard Settings	Choose between a 9-key or 26-key keyboard layout.
DND Mode	Voice prompts are suppressed during identity verification within the configured time periods. Up to 4 periods can be set.
Port Config	Choose which functions this port supports.  NOTE • Display Port Config when the cable supports different functions. • The functions may vary depending on the actual device model.
USB Management	USB Export Exports device data to a USB drive. Exported data is encrypted and cannot be edited directly. Select the data type to export and tap OK.  NOTE • Excel exported are editable. • Use a USB drive formatted as FAT32 with a capacity between 4 GB and 128 GB. Personal data, facial attributes, and card data are all encrypted during export.
	USB Import Imports data from a USB drive to the device. Select the data type to import and tap OK.
	USB Update Installs a system update from a USB drive. 1. Rename the update file to update .bin, copy it to the root directory of the USB drive, and plug the drive into the device. 2. Tap USB Update, and after the update is complete, the device will restart.  NOTE Do not power off the device during the update.

Reports

View unlock records and storage capacity.

Unlock Records

Go to Reports > Unlock Records on the main menu to view access records. Search by user ID to filter results.

System Capacity

Go to Reports > System Capacity on the main menu to view storage capacity by data type.

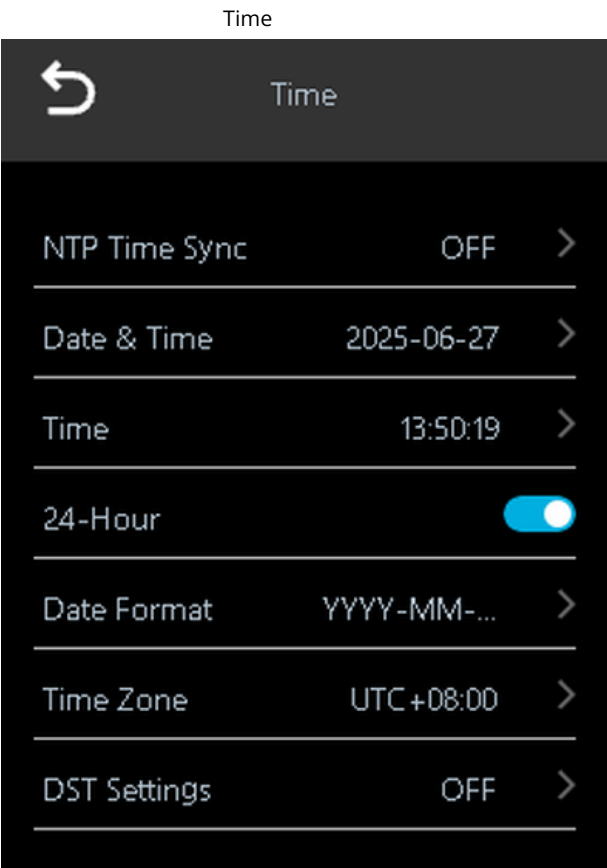
System Settings

Time

Configure the system 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	An NTP server provides the reference time for networked devices. If your computer is set to sync with an NTP server, its clock will match the server time. When the server time is updated, such as for daylight saving time, all synchronized client devices are updated automatically. 1. Tap Time Sync and enable it. 2. Configure the related parameters. • Server Address: Enter the NTP server IP address, and the device will automatically synchronize with the NTP server. • Port: Enter the NTP server port. • Interval: Enter the time synchronization interval.
Date & Time	Set the current date.
Time	Set the current time.
24-Hour	Displays time in 24-hour format.
Date Format	Choose the date display format.
Time Zone	Choose the time zone.
DST Settings	1. Tap DST Settings and enable it. 2. Select Date or Week as the DST type. 3. Enter the DST start and end times. 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	Plays a tap sound on touch screen devices, or a click sound on non-touch devices, when the screen is tapped.
Speaker Volume	Tap the volume, then tap  or  to adjust the volume.
Microphone Volume	

Language

Go to System Settings > Language on the main menu and select the device language.

Screen Settings

Configure the inactivity timeout for logout and screen-off.

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 set inactivity period.
 - Screen off settings:

After the configured idle time, the system returns to the standby screen and then turns the screen off. For

example, if logout is set to 15 seconds and screen-off is set to 30 seconds, the system returns to standby after 15 seconds and turns the screen off 15 seconds later.



NOTE

The logout timeout must be shorter than the screen-off timeout.

Factory Defaults



CAUTION

Warning: Restoring factory settings will erase data. Proceed with caution.

Restore through the Software

1. Go to System Settings > Factory Defaults on the main menu.
2. Select the appropriate reset option.
 - Factory Defaults: Resets all configurations and data, retaining IP settings and expansion module types.
 - Restore to Default Settings (Except for User Information and Logs): Resets all configurations but preserves user information and logs.

Restore through the Hardware

The device supports a tamper button and a reset pinhole.

- Tamper button: Within 5 minutes of powering on, press the tamper button 5 times within 8 seconds. When the prompt appears, tap OK or press the tamper button once to restart the device and restore all settings and data to factory defaults.
- Reset pinhole: Insert a pin to reset the device.
 - ◇ For a partial reset that retains user information, logs, and IP settings: hold the pin for 500 milliseconds.
 - ◇ For a full factory reset: hold the pin for 5 seconds.



NOTE

The reset pinhole is only available on certain models.

About

Go to System Settings > About on the main menu to view the device serial number, software version, and other device information, software version and more.

Restart

Go to System Settings > Restart on the main menu to restart the device.

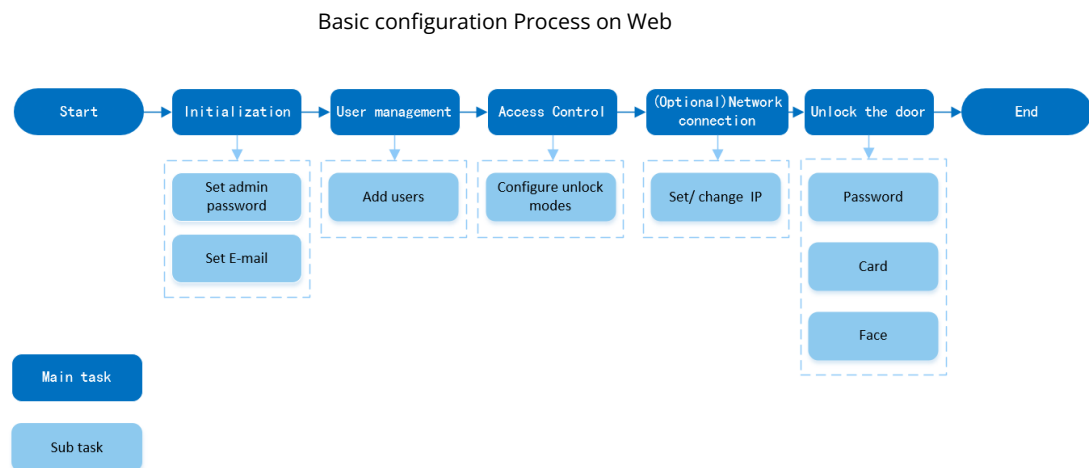
Web Operations

The device can also be configured and updated from a web browser.

NOTE

- Web interface options vary by device model.
- Some functions are only available in the web interface.

Basic Configuration Process on Web



Initialization

Complete initialization the first time you log in to the web interface, or after restoring the device to factory settings.

Precondition

The computer and the device must be on the same local network.

Process

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

NOTE

Tip: Use the latest version of Chrome or Firefox.

2. Select a language for the device.
3. Follow the on-screen instructions to set a password and email address.

NOTE

- The password must be 8–32 characters and include at least two of: uppercase letters, lowercase letters, numbers, or special characters (excluding ' " ; : &). Follow the password strength guidelines to choose a strong password.
 - Store the password securely and change it regularly.
4. Select Auto Check for Updates so the system notifies you when a new version is available, then click Completed to finish initialization.

Log In

Process

1. Draw a face recognition box to set the minimum detectable face size.
2. Enter the username and password.



NOTE

- The default administrator username is admin. The password is the one you set during initialization. Change the administrator password regularly. On process. We recommend that you change the administrator password regularly to enhance security.
 - If you forget the password, click Forgot password? to reset it.
3. Click Login.

Password Resetting

Reset the administrator password using the associated email address.

Process

1. Click Forgot password on the login page.
2. Read the on-screen instructions and click OK.
3. Scan the QR code to receive a security code.

Reset password

Please scan QR code.

Note (for admin only):

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

Email Address: 7***@qq.com

Security code:

Next



NOTE

- Each QR code generates a maximum of two security codes. If a code becomes invalid, refresh the QR code and scan again.
 - The security code is sent to your associated email address. Use it within 24 hours before it expires.
 - Entering an incorrect security code 5 consecutive times will lock the administrator account for 5 minutes.
4. Enter the security code.
 5. Click Next.
 6. Enter and confirm the new password.

NOTE

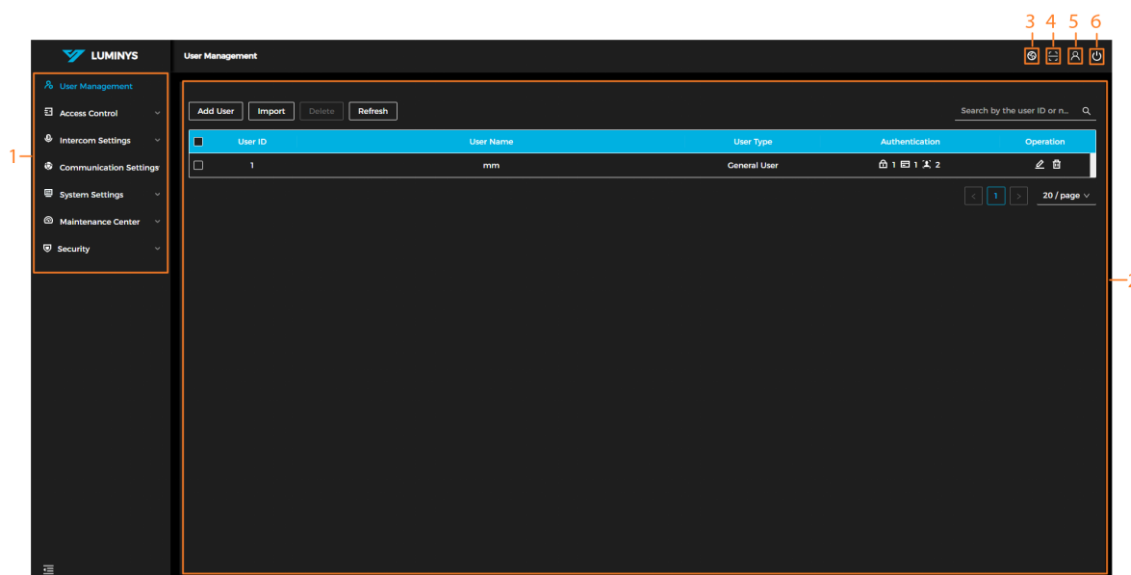
The password must be 8–32 characters and include at least two of: uppercase letters, lowercase letters, numbers, or special characters (excluding ' " ; : &) .ing four character types: uppercase letters, lowercase letters, numbers, and special characters (excluding ' " ; : &) .

7. Click OK.

Home Page

The home page appears after you log in.

Home page



Home page description

No.	Description
1	Navigation menu.
2	Functions
3	Language selector.
4	Scan with a phone to download the mobile app or retrieve the device serial number.
5	Account options.
6	Log out or restart the device.

User Management

Process

1. Go to User Management and click Add User.
2. Set up the user details.

Add the user

Add
X

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

+

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	An alphanumeric identifier for the user ID, up to 30 characters (letters and numbers). with a maximum length of 30 characters.
Username	User display name, up to 32 characters (letters, numbers, and symbols).
Valid from	Start and end dates defining when the user's access is active.
Valid to	
User Type	- General User: Can unlock the door. - VIP User: Can open the door at any time when the door is in Normal status, regardless of other rules. - Guest User: Guests can unlock the door within a set period or up to a specified number of times. Access is automatically revoked when the period expires or the unlock limit is reached. - Blocklist User: Service personnel will receive a notification when users in the blocklist unlock the door. - Other User: When door unlocked, the door will keep open for 5 seconds.
Times Used	Maximum number of unlocks for a Guest user. Once exhausted, access is revoked.
Permission	- User: Users have door access permissions only. - Admin: Administrators have full device configuration permissions in addition to door access.

Parameter	Description
Weekly Schedule	Users can unlock the door during the scheduled time.  NOTE Multiple schedules can be selected.
Holiday Schedule	Users can unlock the door during the configured holiday periods.  NOTE Multiple holidays can be selected.
Face	Click Upload to add a face image. Each user can have up to 2 face images. After uploading, images can be viewed or deleted.  NOTE Face images must be JPG, JPEG, or PNG format, no larger than 100 KB.
Password	User password is up to 8 digits. The emergency password is the user password incremented by 1 (e.g. if the password is 12345, the emergency password is 12346). Using the emergency password triggers an emergency alarm.
Card	 NOTE This feature is only available on specific models. - Manual entry: Type in the card number. - Click Add. - Enter the card number, then click Add. - Automatically read card numbers using a registered reader or device. - Click Add, then click Modify to choose an enrollment reader or the device. - Click Read Card and swipe the card on the reader. A 60-second countdown prompts you to swipe. The card number will read automatically. If the 60-sec countdown expires, click Read Card again to restart. - Click Add. Each user can register up to 5 cards. Enter the card number or swipe to have the device read the card information.

3. Click Add.
Click Add More to add additional users.

Related Operations

- Import: Click Export Template to download the template. Fill in the user information and place face images in the same folder as the template, then click Import User Info to import 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 once.

- Delete: Remove selected users.
- Refresh: Reload the user list.
-  Search by username or user ID.

Access Control

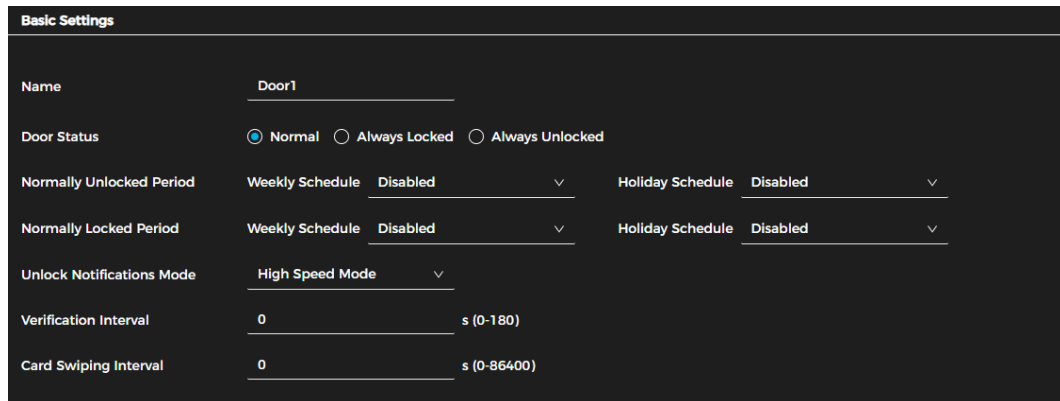
Door Parameters

Basic Settings

Process

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

Basic settings



The screenshot shows the 'Basic Settings' window for 'Door1'. It contains the following settings:

- Name:** Door1
- Door Status:** Normal (selected), Always Locked, Always Unlocked
- Normally Unlocked Period:** Weekly Schedule, Disabled
- Normally Locked Period:** Weekly 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	Name of the door.
Door Status	Select the default door status. • Normal: The door locks and unlocks according to your configured schedules. • Always Locked: The door stays always locked. • Always Unlocked: The door stays always unlocked.
Normally Unlocked Period	When Normal is selected, choose a time template from the drop-down list. The door will remain open or closed for the duration defined in the template.
Normally Locked Period	 NOTE • If a normally open period and a normally closed period overlap, the normally open period takes priority. • If the weekly schedule and the holiday schedule conflict, the holiday schedule takes priority.
Unlock Notifications Mode	Controls the on-screen notification shown after identity verification. • High Speed Mode: Displays only Successfully verified or Not authorized. • Simple Mode: Shows user ID, name, and verification time when access is granted; shows Not authorized and the time when denied. and authorization time after access denied. • Standard: Shows the user's registered face image, user ID, name, and verification time when access is granted; shows Not authorized and the time when denied. • Contrast Mode: Shows the captured face alongside the registered face image, user ID, name, and verification time when access is granted; shows Not authorized and the time when denied.

Parameter	Description
Verification Interval	If multiple verifications are attempted within the set interval, only the first is valid; subsequent attempts will not unlock the door. After a failed attempt, wait for the full interval before trying again.
Card Swiping Interval	The first card swipe within the interval grants access and logs attendance. Subsequent swipes during the interval are ignored — no access, no attendance record, and no log entry. Wait for the interval to expire before swiping again.  NOTE Card Swiping Interval takes priority over Verification Interval.

3. Click Apply.

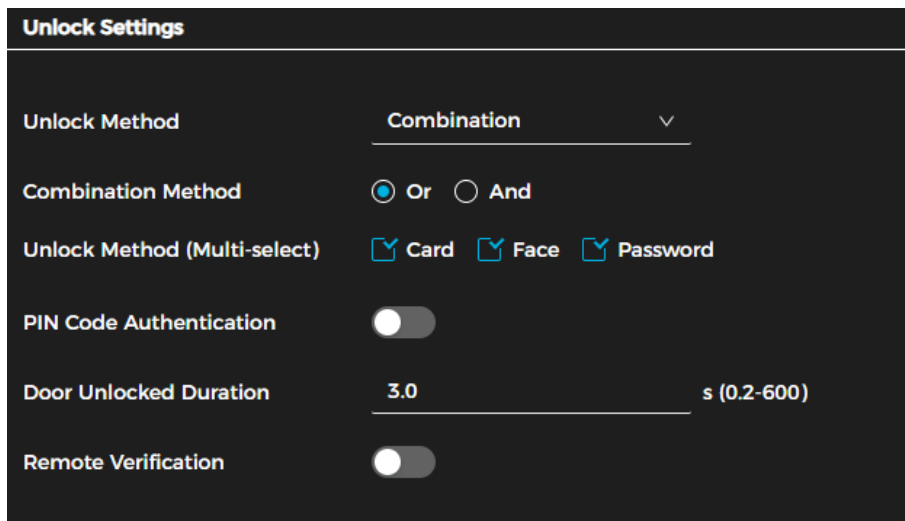
Unlock Settings

Configure how the door can be unlocked — using cards, passwords, or a combination of methods 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: Any one of the selected methods unlocks the door.
 - ◇ And: All selected methods must be used together to unlock the door.
 3. Select unlock methods and configure additional parameters.

Unlock settings



Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	Available unlock methods vary by device model.
PIN Code Authentication	When PIN code authentication is enabled, the door can be unlocked using the PIN code alone.
Door Unlocked Duration	After access is granted, the door remains unlocked for a set duration to allow passage. The configurable range is 0.2–600 seconds.
Remote Verification	Allows the door to be opened remotely.

- Unlock by period
 1. Select By Period in the Unlock Mode list.

2. Drag the slider to set the unlock period for each day.



NOTE

Click Copy to apply the same period to other days.

3. Select a period for the combination method and the unlock method, then configure the remaining parameters.

Unlock by period

- Unlock by multi-users.
 1. Select Multi-users, in the Unlock Mode list.
 2. Click Add to add a group.
 3. Select the unlock method, valid number, and user list for the group.
 - ◇ With one group: the door unlocks when the number of verified users equals the valid number's group equals the defined valid number.
 - ◇ With multiple groups: the door unlocks only when the valid number is met in every group. Each group equals the defined valid number.



NOTE

- ◇ Up to 4 groups can be added.
- ◇ The valid number is the minimum number of users in a group who must verify before the door unlocks. For example, if the valid number is 3, any 3 members of the group must verify. 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

Triggers an alarm when an abnormal access event is detected.

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)

Description of alarm parameters

Parameter	Description
Anti-passback	When anti-passback is enabled, users must verify their identity on both entry and exit. This prevents cardholders from passing their access cards to others. To re-enter, a cardholder must first complete an authorized exit through the exit reader. • If a person enters with authorization but exits without authorization, their next entry attempt will trigger an alarm and be denied. • If a person enters without authorization but exits with authorization, their next entry attempt will trigger an alarm and be denied.  NOTE When the device is connected to only one lock, verification on the device defaults to entry and verification on the external card reader defaults to exit. These directions can be changed on the management platform.
Duress Alarm	Triggers an alarm when the door is unlocked using a duress card, duress password, or duress fingerprint.ck the door.
Illegal Over-authentication Alarm	Triggers an alarm if the wrong password or card is presented 5 times consecutively within 60 seconds. The alarm persists for a configured duration.
Door Detector	A door detector connected to the device triggers an alarm when the door is opened or closed abnormally. Two detector types are supported: normally closed and normally open. • Normally Closed: The sensor circuit is closed when the door is shut. • Normally Open: The sensor circuit is open when the door is shut.
Intrusion Alarm	Triggers an alarm when the door is opened without a valid access event. The alarm persists for a configured duration.  NOTE Door Detector and Intrusion Detection must both be enabled for this alarm to function.
Unlock Timeout Alarm	If the door remains unlocked beyond the configured timeout duration,

Parameter	Description
Unlock Timeout	an unlock timeout alarm is triggered and persists for the configured period.  NOTE Door Detector and Unlock Timeout must both be enabled for this alarm to function.

- Click Apply.

Alarm Linkage Setting (Optional)

Set up the alarm linkage.

Process

- Go to Access Control > Alarm > Alarm Linkage Setting.

 **NOTE**

- When the device is managed by a platform, the alarm settings will be synchronized.
- The number of alarm input and output ports varies by model.
- This function is only available on models with alarm input and output ports.

- Configure the alarm settings.

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

- Enter a name for the alarm zone.
- Enable Link Fire Safety Control and select an alarm input type.
 - Normally Closed: The alarm input circuit is closed when idle. Opening the circuit triggers the alarm. Opening the normally closed circuit will trigger the alarm.
 - Normally Open: The alarm input circuit is open when idle. Closing the circuit triggers the alarm circuit state. Closing the circuit will trigger the alarm.

- To trigger access control actions when a fire alarm is activated, enable Access Control Linkage.

 NOTE

Access Control Linkage only works when Link Fire Safety Control is enabled.

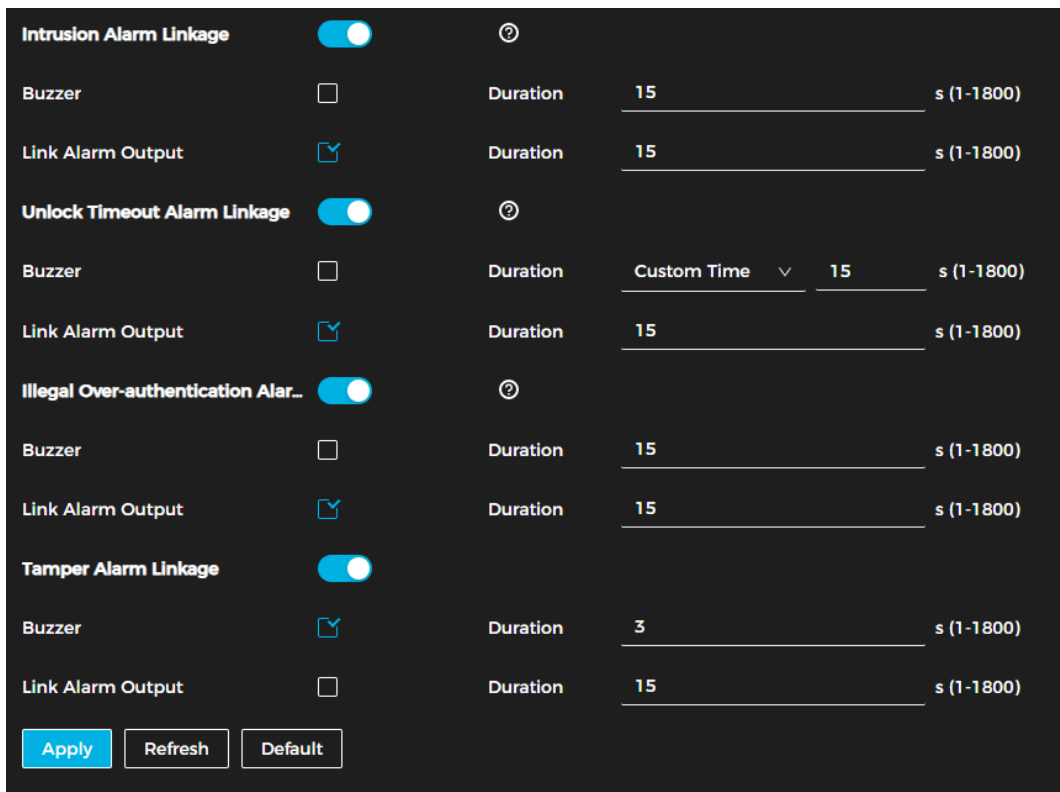
- Select a linkage mode.
 - Strong Execution: The door stays in its fire-alarm state after the signal clears. Manually restore the previous door setting if needed.
 - Weak Execution: The door automatically returns to its previous state after the fire alarm signal clears door status.
- Select a channel type.
 - Normally Open: The door opens automatically when the fire alarm is triggered.
 - Normally Closed: The door closes automatically when the fire alarm is triggered.
- Click OK.

Alarm Event Linkage

Process

- Go to Access Control > Alarm > Alarm Event Linkage.
- Configure Alarm event linkage.

Alarm event linkage



Linkage Type	Enabled	Help	Parameter	Value	Unit/Range
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 Alarm Linkage	☒	?	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)

Buttons: Apply, Refresh, Default

Alarm event linkage

Parameter	Description
Intrusion Alarm Linkage	Triggers when the door is opened without a valid access event. - Buzzer: Sounds when the intrusion alarm triggers. You may configure the alarm duration. - Link Alarm Output: Activates external alarm devices when the intrusion alarm triggers. You may configure the alarm duration.

Parameter	Description
Unlock Timeout Alarm Linkage	Triggers when the door stays unlocked beyond the configured period the defined period. - Buzzer: Sounds when the unlock timeout alarm triggers. You may configure the alarm duration. - Custom time: The buzzer beeps for the configured duration time. - Until the door locks: The buzzer continues until the door locks. - Link Alarm Output: Activates external alarm devices when the unlock timeout alarm triggers. You may configure the alarm duration.
Illegal Over-authentication Alarm	Triggers when the wrong credential is presented 5 consecutive times within 60 seconds. - Buzzer: Sounds when the illegal over-authentication alarm triggers. You may configure the alarm duration. - Link Alarm Output: Activates external alarm devices when the illegal over-authentication alarm triggers. You may configure the alarm duration.
Tamper Alarm Linkage	Triggers when physical tampering with the device is detected. - Buzzer: Sounds when the tamper alarm triggers. You may configure the alarm duration. - Link Alarm Output: Activates external alarm devices when the tamper alarm triggers. You may configure the alarm duration.

Face Parameters

Configure face detection parameters. Available parameters may vary by model.

Process

- Go to Access Control > Face Parameters.

Face detection parameters

The screenshot displays the 'Face detection parameters' configuration window. It features a live video feed on the left side. To the right of the feed, there are controls for 'Target Filter' and 'Detection Area', each with a selection icon and a trash icon. Below these is the 'Min Size' field, set to 256 x 256. The main configuration area is divided into two tabs: 'Recognition' (selected) and 'Exposure'. Under the 'Recognition' tab, the following settings are visible:

- Face Recognition Thresh...: 85 (range 0-100)
- Anti-spoofing Level: Radio buttons for Close, General (selected), High, and Ultra High
- Invalid Face Interval (sec): 10 (range 0-60)
- Mask mode: Not Detect (dropdown menu)
- Snapshot Mode: Toggle switch (off)
- Beautifier: Toggle switch (off)
- Multi-face Recognition: Toggle switch (off)
- Smart Screen Light Up: Toggle switch (on)
- Max Face Recognition A...: 30 (range 0-90)
- Valid Face Interval (sec): 3 (range 1-60)
- Recognition Distance: 1.5 meters (dropdown menu)
- Face Mask Threshold: 75 (range 0-100)
- Face Snapshot Enhance...: Toggle switch (off)
- Enable Helmet Detection: Toggle switch (off)
- Night Mode: Toggle switch (on)

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

- Configure the parameters.

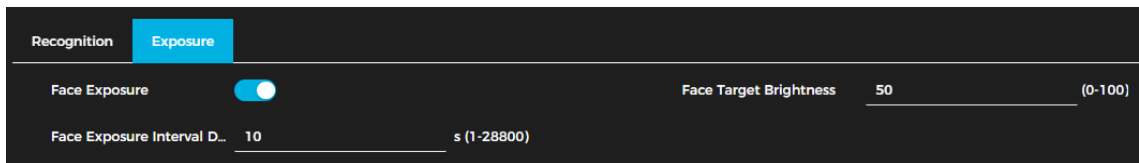
Description of face parameters

Name	Description
Face Recognition Threshold	Sets the face recognition accuracy. A higher threshold improves accuracy and reduces false matches recognition rate.  NOTE Setting the threshold too low (e.g. 0) greatly increases the false recognition rate. Please notice.
Max Face Recognition Angle Deviation	Defines the widest face angle the device will accept during detection. A larger value widens the acceptable range; angles outside that range may fail detection.
Anti-spoofing Level	Prevents unauthorized access using photos, videos, masks, or other spoofing materials, videos, masks, and other substitutes. When enabled, the detection frame is not displayed for non-live subjects.
Illuminator	- On: The illuminator activates automatically in low-light conditions. - Off: The illuminator always remains off.  NOTE The illuminator is only available on specific models.
Valid Face Interval (sec)	After a face is successfully recognized, the device waits for the configured interval before recognizing that same face again.
Invalid Face Interval (sec)	After a failed recognition attempt, the device waits for the configured interval before trying to recognize that face again. Setting this to 0 disables face capture and suppresses unlock records.
Recognition Distance	Sets the recognition distance between the face and the camera lens.
Mask Mode	- Not Detect: No mask was detected. - Mask Alert: If no mask is detected, the user receives a reminder to wear one, but access is still granted. - Mask Required: If no mask is detected, the user receives a reminder to wear one and is denied to access.
Face Mask Threshold	Higher values improve recognition accuracy for masked faces and reduce false matches and the lower the rate of misidentification.
Snapshot Mode	Filters out low-quality snapshots from unlock records.  NOTE - Snapshot Mode and Multi-face Recognition cannot be enabled at the same time. - This function is only available on certain models.
Face Snapshot Enhancement	Improves the quality and clarity of snapshots saved in unlock records.  NOTE Face Snapshot Enhancement and Multi-face Recognition cannot be enabled at the same time.
Beautifier	Applies cosmetic enhancement to captured face images.
Enable Helmet Detection	Detects whether a safety helmet is worn. The door will not unlock if no helmet is detected.

Name	Description
Multi-face Recognition	Recognizes 4–6 faces simultaneously. Incompatible with the And combination unlock method; the door opens as soon as any one person is verified  NOTE The number of simultaneous faces supported may vary by model.
Night Mode	Displays a bright white standby screen in dark environments to improve verifying faces or QR codes.
Smart Screen Light Up	Wakes the screen automatically when a face is detected while the display is off.

3. Configure the exposure parameters.

Exposure parameters



Exposure parameters description

Parameter	Description
Face Exposure	Applies a set brightness level to the detected face area to improve image clarity.
Face Target Brightness	
Face Exposure Interval Detection	Limits exposure adjustments to once within the configured interval.

4. Draw the face detection area.
 - 1) Click .
 - 2) Right-click to draw the detection area, then release the left mouse button to finish.
Face detection is restricted to the drawn area.
5. Draw the target filter.
 - 1) Click .
 - 2) Draw a face recognition box to set the minimum detectable face size.
Faces smaller than the defined minimum size cannot be detected.
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	Enables reading of IC cards.  NOTE This function is only available on specific models.
	IC Card Encryption & Verification	When enabled, only encrypted IC cards are accepted.  NOTE IC Card must be enabled first.
	Block NFC Cards	Prevents access using duplicate NFC cards.  NOTE - This function is only available on models that support IC cards. - IC Card must be enabled. - NFC is only supported on certain mobile phone models.

Item	Parameter	Description
	Enable Desfire Card	Enables the device to read Desfire card numbers.  NOTE • This function is only available on models that support IC cards. • Hexadecimal format only.
	Desfire Card Decryption	When both Enable Desfire Card and Desfire Card Decryption are enabled, the Desfire card data can be read.  NOTE • This function is only available on models that support IC cards. • Desfire Card must be enabled first.
Card No. System	Card No. System	When using a Wiegand card reader, choose decimal or hexadecimal format for card numbers. The same format applies to both input and output. 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 reader, enter the card number, and click Write to encode the card number to the card.  NOTE • Card number supports up to 8 characters. • Enable Desfire Card and Desfire Card Decryption must both be enabled. • Hexadecimal format only.
	Card Number	

3. Click Apply.

Weekly Schedule

Configure up to 128 weekly schedules (numbered 0–127). Each schedule defines when door access is permitted across the week. Users can only unlock the door during the scheduled times.

Background Information

Process

1. Go to Access Control > Weekly Schedule.
2. Click Add.
 - 1) Assign a number and name to the schedule.
 - 2) Drag the time slider to set the access window for each day.
 - 3) (Optional) Click Copy to apply the same setting to all remaining days.

Configure general plan

Add
X

No. 0

Schedule Name

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

Sun		Copy
Mon		Copy
Tue		Copy
Wed		Copy
Thu		Copy
Fri		Copy
Sat		Copy

Apply
Cancel

- Click OK.

Holiday Schedule

Configure up to 128 holiday groups (numbered 0–127), each supporting up to 16 holidays. Assign holiday groups to a holiday plan to control when access is permitted during holidays.

Process

- Go to Access Control > Holiday Schedule.
- Click Holiday Management, then click Add.
 - Select a holiday group number and enter a name for the 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 and 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) Assign a number and name to the holiday plan.
- 2) Select a holiday group and drag the slider to set the access window for each day.
Up to 4-time sections can be configured per day.

Add holiday plan

- Click OK.

Privacy Setting

Process

- Go to Access Control > Privacy Setting on the webpage.
- Enable snapshot function.
Automatically captures a face image each time the door is unlocked.

Enable snapshot

- Click Apply.

Port Config

Some ports support multiple functions. Configure each port for your specific requirements to your actual needs.

Background Information



NOTE

- Available ports vary by device model.
- This function is only available on specific models.

Process

- Go to Access Control > Port Config on the webpage.
- Select the function for each port.



NOTE

If the alarm and doorbell share a cable, configure the port as doorbell to ensure the doorbell can ring correctly.

- Click Apply.

Configure ports

Function Port1	☐ Alarm-in Port	☒ Card Reader Indicator
Function Port2	☒ Alarm-out Port	☐ Doorbell

Back-end Comparison

Sends card numbers and other credential data to a third-party platform for verification, bypassing on-device verification.

Go to Access Control > Back-end Comparison.

Back-end comparison

Card No. Pass-through
☒

Back-end comparison

Parameters	Description
Card No. Pass-through	When enabled, the card number is forwarded to a third-party platform for verification.

First-Person Unlock

The door remains locked to all other users until the designated first person has verified their identity and passed through. If multiple people are designated, the door becomes accessible to others once any one of those designated individuals has passed through.

Precondition

A user must be granted door access permissions before they can be designated as the first person.

- Only general users can be designated as the first person.
- If the device restarts after the first person has verified their identity, the first person must verify again before others can gain access.
- When this function is enabled, patrol users can still clock in as normal.

Process

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

First-person unlock

Door Channel List

Door1

Enable
☒

Time Templates

Weekly Schedule
255-Full Day

Holiday Schedule
255-No Plan

Door Status after First-Card Unlock

Status
Normal

Person List

Remove

+

3. Configure the parameters.

Parameter description	
Parameter	Description
Time Templates	Select the period during which this rule is active.
Door Status after First-Card Unlock	• Normal: Other users must complete identity verification to pass. • Always Unlocked: The door remains open and no verification is required.
Person List	Click + to add one or more users as designated first persons.

4. Click Apply.

Intercom Settings

Configure the device as an entrance station to use its video intercom capabilities.



NOTE

The intercom function is only available on certain models.

Using the device as the SIP Server

Configuring the SIP Server

Set up the device to operate as a SIP server.

Process

1. Go to Intercom Settings > SIP Server.
2. Enable Local SIP Server and leave all other fields at their default values. For parameter details, see “SIP server configuration description”.



CAUTION

If the SIP server status changes, all device settings will be automatically reset to factory defaults.

Configure SIP server

Local SIP Server ☒

Port 5060

SIP No. 8001

Registration Password •••••

SIP Domain DoorPhone

Apply Refresh Default

3. Click Apply.

Local device Config

When the device operates as a SIP server, configure the local device parameters below.

Process

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

Basic parameters

Device Type

Outdoor Station

No.

8001

Management Center

888888

Apply

Refresh

Default

Basic parameters description

Parameter	Description
device Type	Select Outdoor Station.
No.	Unable to set.
Management Center	The management center's default call number is 888888.

- 3. Click Apply.

Adding the Outdoor Station

When the device operates as a SIP server, add the outdoor station to enable calls between the two.

Process

- 1. Go to Intercom Settings > device Setting on the webpage.
- 2. Click Add, then configure the outdoor station.

Add outdoor 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 outdoor station configuration

Parameter	Description
device Type	Select Outdoor Station.
No.	The outdoor station number shown on the device display.
Registration Password	The registration password for the outdoor station.
Building No.	Unable to configure.
Unit No.	
IP Address	The IP address of the outdoor station.
Username	Credentials used to log in to the outdoor station's web page.
Password	

- Click OK.

Adding the Indoor Monitor

When the device operates as a SIP server, add the indoor monitors in the same unit so they can communicate with each other. Up to 500 indoor monitors can be connected.

Process

- Go to Intercom Settings > device Setting on the home page.
- Add the indoor monitor.
 - Add one by one.
 - Click Add.
 - Configure parameters, and then click OK.

Add one by one

Add

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	A name to identify this indoor monitor from others.
Last Name	
Alias	
Room No.	The room number of the indoor monitor. - Room numbers are 1–5 digits and must match the value configured on the indoor monitor itself. - Where a main indoor monitor coexists with extension devices, the main monitor's room number ends in -0 and each extension ends in -1, -2, or -3 (e.g., the main is 101-0 and extensions are 101-1, 101-2, etc.). - The 9901-xx room number format requires the group call feature to be enabled.
Registration Mode	Leave at default values.
Registration Password	

- Add in batches.
 - Click Add in Batches.
 - Configure the parameters.
 - Click Add.

Batch add

Add

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

Add in batches

Parameter	Description
Floors in Unit	Accepts values from 1 to 99.
Rooms on Each Floor	Accepts values from 1 to 99.
First Room No. on 1st Floor	Room number assigned to the first room on the first floor.
First Room No. on 2nd Floor	Increment the leading digit of the first floor start number by 1. For example, if the first floor starts at 101, the second floor must start at 201.

Using the device as the SIP Client

Configuring a SIP Server for the device

When the device functions only as a SIP client (outdoor station), assign a SIP server to it so mutual calling is possible.

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.

Configure 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 description

Parameter	Description
Server Address	The IP address or domain name of the SIP server.
Port	The SIP server port. Defaults to 5060 when the outdoor station acts as the SIP server.
Registration Password	Leave at the default value.
SIP Domain	DoorPhone.
SIP Server Username	Credentials for logging in to the SIP server.
SIP Server Password	

- Click Apply.

Local device Config

When the device operates as a SIP client, configure the local device parameters below.

Process

- Go to Intercom Settings > Local device Config.
- Configure the parameters.

Configure the parameters

Device Type	Outdoor Station
No.	8001
Management Center	888888
Apply	Refresh Default

Parameters description

Parameter	Description
device Type	Defaults to Outdoor Station.
No.	The number assigned to this outdoor station.  NOTE - Must be four digits: the first two are 80, and the last two begin at 01 (e.g., 8001). - Each outdoor station within a unit must have a unique number.
Management Center	The management center call number is 888888. Keep the default value.

3. Click Apply.

Call Config

This section covers how to configure the call function, including adding an indoor monitor in phonebook mode for direct dialing from the device.

Background Information

Once enabled, a call icon appears on the standby screen. Three call types are available; the selection here is linked to 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 again to place the call. - Phone Book: Customize the list on the web page. Tap the call icon on the standby screen; the configured indoor monitors are displayed on screen. Tap an entry to call that monitor. The call list reflects the configuration set on the web page.
Call Management Center	Tap the call icon on the standby screen to reach the management center.
Call Phone	Tap the call icon on the standby screen to dial a phone number.

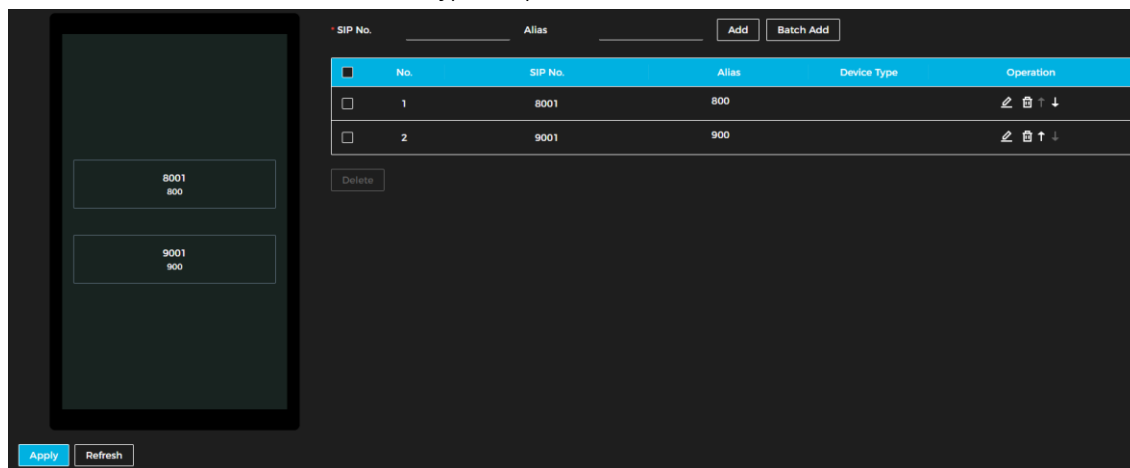
Process

- Go to Intercom Settings > Call Config on the webpage.
- Select the call type.
When Call Room is selected as the type and Phone Book as the mode, a preview screen appears on the left and the list of added indoor monitors on the right.

NOTE

- Call list preview availability depends on the product model.
- Call list preview do not supported in 4.3-inch horizontal series devices.
- A device type appears in the list only when the device is configured as a SIP server and the indoor monitor has been added to the SIP server on the device settings page.

Call room type and phone book mode



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

3. Add indoor monitor.
If the indoor monitor has extensions (for example, 9901-0, 9901-1, and 9901-2) and the SIP number is 9901, dialing 9901 will ring all extensions simultaneously.

Related Operations

- Click  to edit the device alias.
- Click  to remove the device.
- Click  to reorder devices or drag them directly in the preview window.

Communication Settings

Network Settings

TCP/IP

Configure the device's IP address so it can communicate with other devices on the network.

Process

1. Go to Communication Settings > Network Settings > TCP/IP.
2. 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: Manually enter the IP address, subnet mask, and gateway. - DHCP (Dynamic Host Configuration Protocol): The network automatically assigns an IP address, subnet mask, and gateway to the device.
MAC Address	Displays the device's MAC address (read-only).
IP Version	IPv4 or IPv6.
IP Address	Required when Mode is set to Static. Enter the IP address, subnet mask, and gateway. NOTE - IPv6 addresses are written in hexadecimal notation. - IPv6 does not use a subnet mask. - The IP address and default gateway must be on the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS	The IP address of the primary DNS server.
Alternate DNS	The IP address of the secondary DNS server.
MTU	The maximum data size per network packet. Defaults to 1500 bytes.

Parameter	Description
Transmission Mode	• Multicast: Suited to video calls. • Unicast: Suited to group calls.

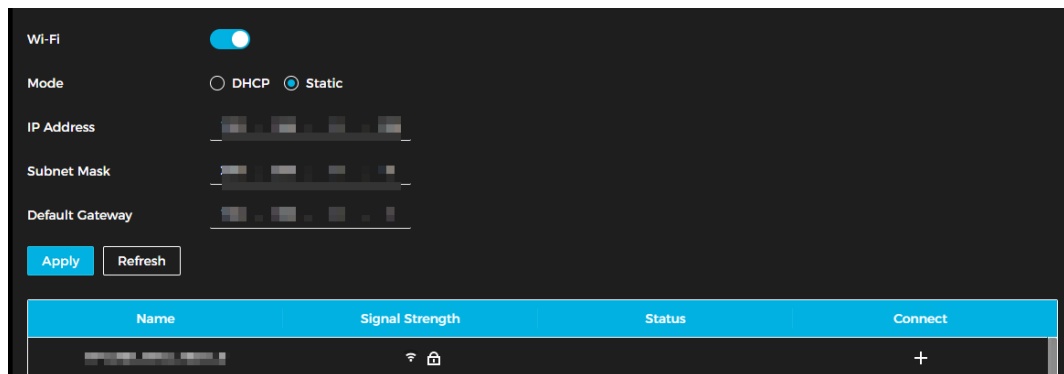
3. Click OK.

Wi-Fi

Process

1. Go to Communication Settings > Network Settings > Wi-Fi.
2. Enable Wi-Fi.
Available Wi-Fi networks will be listed.

Wi-Fi



NOTE

- Wi-Fi and Wi-Fi AP cannot be active at the same time.
- Wi-Fi is only available on supported models.

3. Tap , then enter the Wi-Fi password to connect.

Related Operations

- DHCP: When enabled and click Applied, the device automatically assign a Wi-Fi address.
- Static: Enable this option, manually enter a Wi-Fi address, then click Apply to connect.

Wi-Fi AP

NOTE

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

Process

1. Go to Communication Settings > Network Settings > Wi-Fi AP.
2. Enable the function, then click Apply.

Wi-Fi AP

Enable

☐

SSID

Security

WPA2-Personal

▼

Password

IP Address

Apply

Refresh

Default

Result

Once enabled, connect a mobile phone to the device's Wi-Fi hotspot and open the device's web page from the phone.

Port

Restrict and manage how the device is accessed through web, desktop client, and mobile client.

Process

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



NOTE

Changes to any parameter other than Max Connection and RTSP Port require a device restart 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	Maximum number of clients (web pages, desktop clients, mobile clients) allowed to access the device at the same time.
HTTP Port	Defaults to 80. If the port number is changed, append the new port number to the IP address when accessing the web page (e.g., 192.168.1.108:8080).
HTTPS Port	The default value is 443.
RTSP Port	The default value is 554.

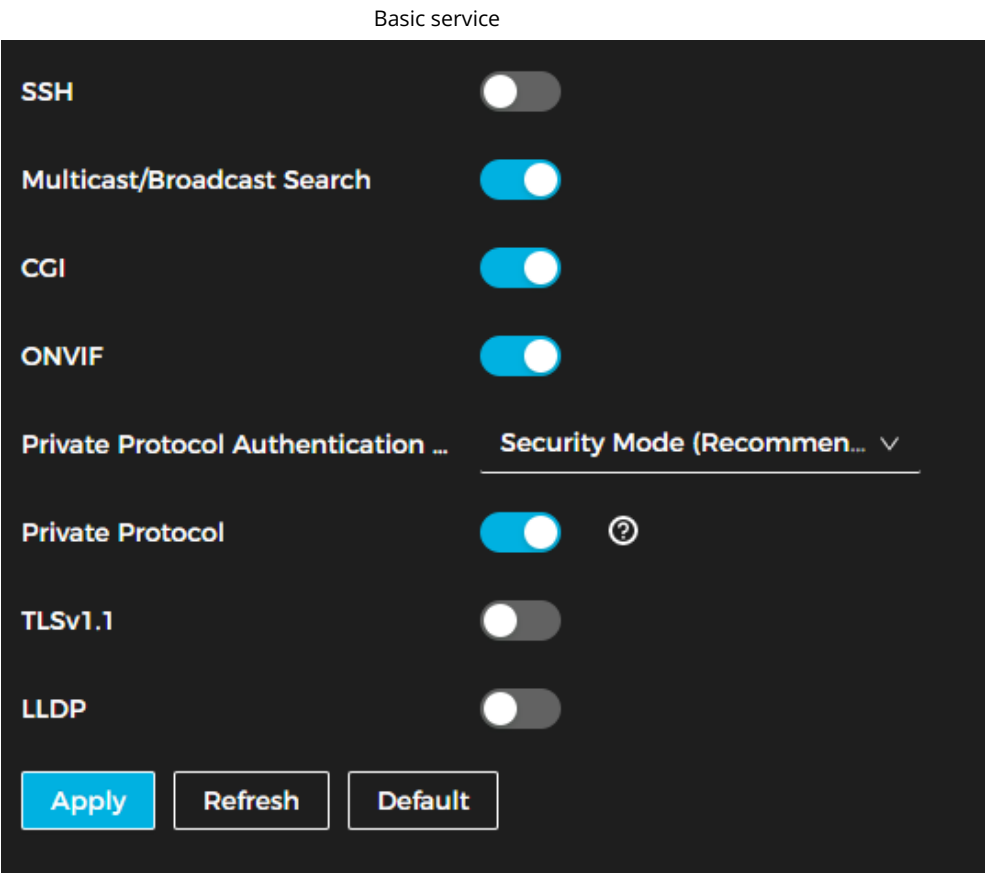
3. Click Apply.

Basic Services

To connect the device to a third-party platform, enable CGI and ONVIF.

Process

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



Basic service parameter description

Parameter	Description
SSH	SSH (Secure Shell Protocol). A remote management protocol for accessing and controlling servers securely over the network.
Multicast/Broadcast Search	Discovers devices on the network using multicast or broadcast protocols.
CGI	CGI (Common Gateway Interface). Enables standardized data exchange between external applications and the web server.
ONVIF	ONVIF (Open Network Video Interface Forum). Provides a common communication standard for IP-based security devices.
Private Protocol Authentication Mode	Select the authentication mode: Security Mode or Compatible Mode. Security Mode is recommended. Security Mode • Security Mode (recommended): Blocks access via Digest, DES, and plaintext authentication, providing stronger device security. • Compatible Mode: Allows access via Digest, DES, and plaintext authentication. Security is reduced.
Private Protocol	The platform connects to devices using a private protocol.

Parameter	Description
TLSv1.1	TLSv1.1 (Transport Layer Security Protocol version 1.1) is a cryptographic protocol that ensures secure, authenticated communication over a network.  NOTE Enabling TLSv1.1 introduces security risks. Use only if required for compatibility.
LLDP	LLDP (Link Layer Discovery Protocol) is a data link layer protocol that enables network devices — such as switches, routers, and servers — to advertise their identity and capabilities to neighbors. It provides a standardized method for automatically discovering and mapping device connections, giving administrators clearer visibility into network topology and simplifying configuration, troubleshooting, and performance optimization.

3. Click Apply.

Cloud Service

The cloud service provides NAT traversal, enabling multiple devices to be managed through LumiViewer without a dynamic domain name, port mapping, or dedicated servers.

Process

1. Go to Communication Settings > Network Settings > Cloud Service.
2. Enable the cloud service function.
Cloud services are online when both P2P and PaaS show as online.

Enable

☒

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

P2P Status

Offline

PaaS Status

Offline

SN

B

2



Apply

Refresh

Default

- Click Apply.
- Use LumiViewer to scan the QR code to add the device.

Auto Registration

Auto Registration lets devices be added to the management platform without manually entering information such as the IP address and port.

Background Information



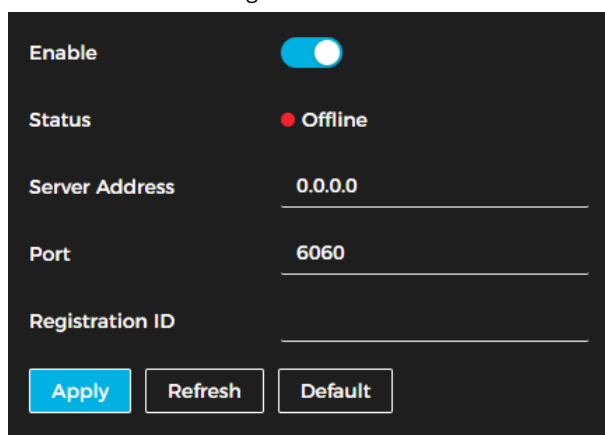
NOTE

Automatic registration is available for SDK integration only.

Process

1. Go to Communication Settings > Network Settings > Auto Registration.
2. Enable Auto Registration and set the parameters.

Auto Registration



Automatic registration description

Parameter	Description
Status	Shows the current Auto Registration connection status.
Server Address	IP address or domain name of the registration server.
Port	Port number of the registration server.
Registration ID	A user-defined identifier for the device. Enter this ID on the platform to add the device to management.

3. Click Apply.

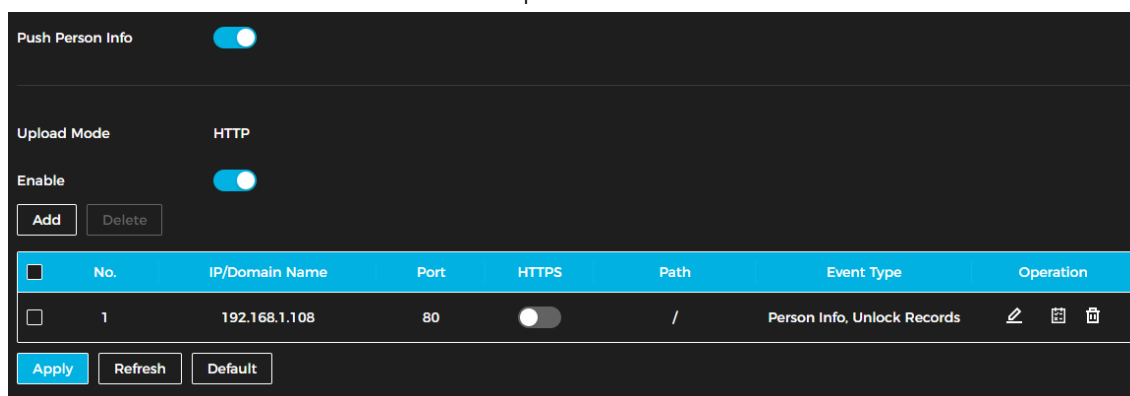
Auto Upload

Configure automatic upload of 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 changes or a new user is added, the device automatically sends the updated information to the management platform.
3. Enable HTTP upload mode.
4. Click Add, then configure parameters.

Auto upload



Parameters description

Parameter	Description
IP/Domain Name	IP address or domain name of the management platform.
Port	Port number of the management platform.
HTTPS	Enable to access the management platform over HTTPS for encrypted communication.

Parameter	Description
	Enable account authentication on the management platform. A username and password are required to log in.
Event Type	The type of event data sent to the management platform.  NOTE - Push Person Info must be enabled before using this function. - Personal information can be pushed to only one management platform; unlock records can be pushed to multiple platforms.

5. Click Apply.

RS-485 Settings

Configure RS-485 parameters when external devices are connected to the RS-485 port.

Process

- Go to Communication Settings > RS-485 Settings.
- 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 this when the device operates as a card reader and forwards data to an external access controller. Output Data type: ◇ Card Number: Outputs data using the card number on a card swipe; for all other unlock methods, the user's first card number is used. ◇ No.: Outputs data using the user ID. - Card Reader: The device acts as an access controller connected to an external card reader. - Reader (OSDP): The device is connected to an OSDP-compliant card reader.
Data Bit	The number of bits used to transmit each unit of data in a serial communication frame.
Stop Bit	A bit appended after the data and parity bits to signal the end of a data frame and allow the receiver to synchronize for the next byte.

Parameter	Description
Parity Code	Extra bits appended after the data bits for error detection. They verify data integrity by checking the count of high or low bits in the transmission.

- Click Apply.

Wiegand Settings

Configure Wiegand settings to match the device's operating mode and transmission mode.

Process

- Go to Communication Settings > Wiegand.
- Select a Wiegand type and set the parameters.
 - Select Wiegand Input when an external card reader is connected to the device.



NOTE

If the card number read via the Wiegand input port appears in reverse order, enable Card No. Inversion to correct it.

- Select Wiegand Output when the device operates as a card reader connected to an external access controller.

Wiegand output

Description of Wiegand output

Parameter	Description
Wiegand Output Type	The Wiegand format used to read card numbers or user IDs. - Wiegand26: Reads 3 bytes or 6 digits. - Wiegand34: Reads 4 bytes or 8 digits. - Wiegand66: Reads 8 bytes or 16 digits.
Pulse Width	The pulse width and pulse interval for the Wiegand output signal.
Pulse Interval	
Output Data Type	Choose the data type to output. - No.: Outputs data using the user ID, in hexadecimal or decimal format. - Card Number: Outputs data using the user's first card number.

- Click Apply.

System Settings

Account

Manage user accounts: add or remove users, change passwords, and set a recovery email for password resets.

Adding Administrators

Add administrator accounts to allow login to the device's web page.

Process

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



NOTE

- Usernames must be unique and may contain up to 31 characters: letters, numbers, underscores, hyphens, periods, or @.
- Passwords must be 8–32 characters and include at least two of the following: uppercase letters, lowercase letters, numbers, or special characters (excluding ' " ; : &).
Use the password strength indicator as a guide when setting your password.

Add Administrators

The screenshot shows a modal dialog titled 'Add Administrators'. The dialog has a blue header bar with the word 'Add' on the left and a close button (X) on the right. The main area of the dialog is dark gray and contains four input fields. The first three fields are labeled 'Username', 'Password', and 'Confirm Password', each with a red asterisk to its left, indicating they are required. The fourth field is labeled 'Remarks'. At the bottom right of the dialog are two buttons: 'OK' and 'Cancel'.

3. Click OK.



NOTE

Administrator accounts cannot be deleted, and only an administrator can change their own password.

Adding ONVIF Users

Background Information

ONVIF (Open Network Video Interface Forum) defines open standards for IP-based security product interfaces, ensuring interoperability across manufacturers. ONVIF users authenticate via the ONVIF protocol. The default ONVIF user is admin.

Process

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

Add ONVIF user

ONVIF user description

Parameter	Description
Username	Must be unique. Up to 31 characters: letters, numbers, underscores, hyphens, periods, or @.
Password	8–32 characters, including at least two of: uppercase letters, lowercase letters, numbers, or special characters (excluding ' " ; : &).
Group	Three permission groups are available, each representing a different access level. • Admin: Can view and manage other user accounts in ONVIF Device Manager. • Operator: Has no access to other user accounts in ONVIF Device Manager. • User: Has no access to other user accounts or system logs in ONVIF Device Manager.

3. Click OK.

Resetting the Password

To reset a forgotten password, use the associated email address.

Process

1. Go to System Settings > Account > Password Reset.
2. Type in the email address and choose a password expiration time.
3. Enable the password reset function.

Reset Password



NOTE

A security code to reset the password can be sent to the associated email address.

4. Click Apply.

Viewing Online Users

View a list of users currently logged in to the web page. Go to System Settings > Online User.

Time

Process

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

Date settings

System Time

06-25-2025 4:49:33 AM

Sync PC

Time Zone

Date Format

Month_Day_Year

Time Format

12-Hour

NTP Settings

☐

Server

time.windows.com

Manual Update

Port

123

(1-65535)

Interval

1440

min

Daylight Saving TI...

☒

Start Time

March

Second

Sunday

02 AM

End Time

November

First

Sunday

02 AM

Apply

Refresh

Default

Time settings description

Parameter	Description
Time	Manual Set: Enter the time manually or click Sync PC to synchronize the time with your PC.
Time Zone	Select the time zone.
Date Format	Select the date format.
Time Format	Select the time format.
NTP Settings	When enabled, the device automatically synchronizes its time with the NTP server. - Server: Enter the NTP server domain. - Port: Enter the NTP server port. - Interval: Set how often the device synchronizes with the NTP server.
Daylight Saving Time	(Optional) Enable Daylight Saving Time. - Set the start and end times for Daylight Saving Time.

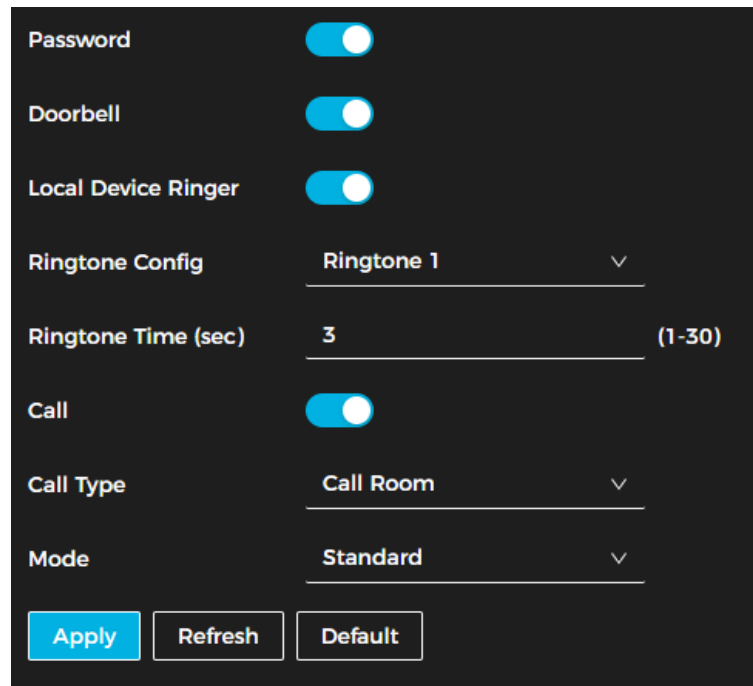
3. Click Apply.

Shortcut Settings

Process

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

Shortcut Settings



Parameters description

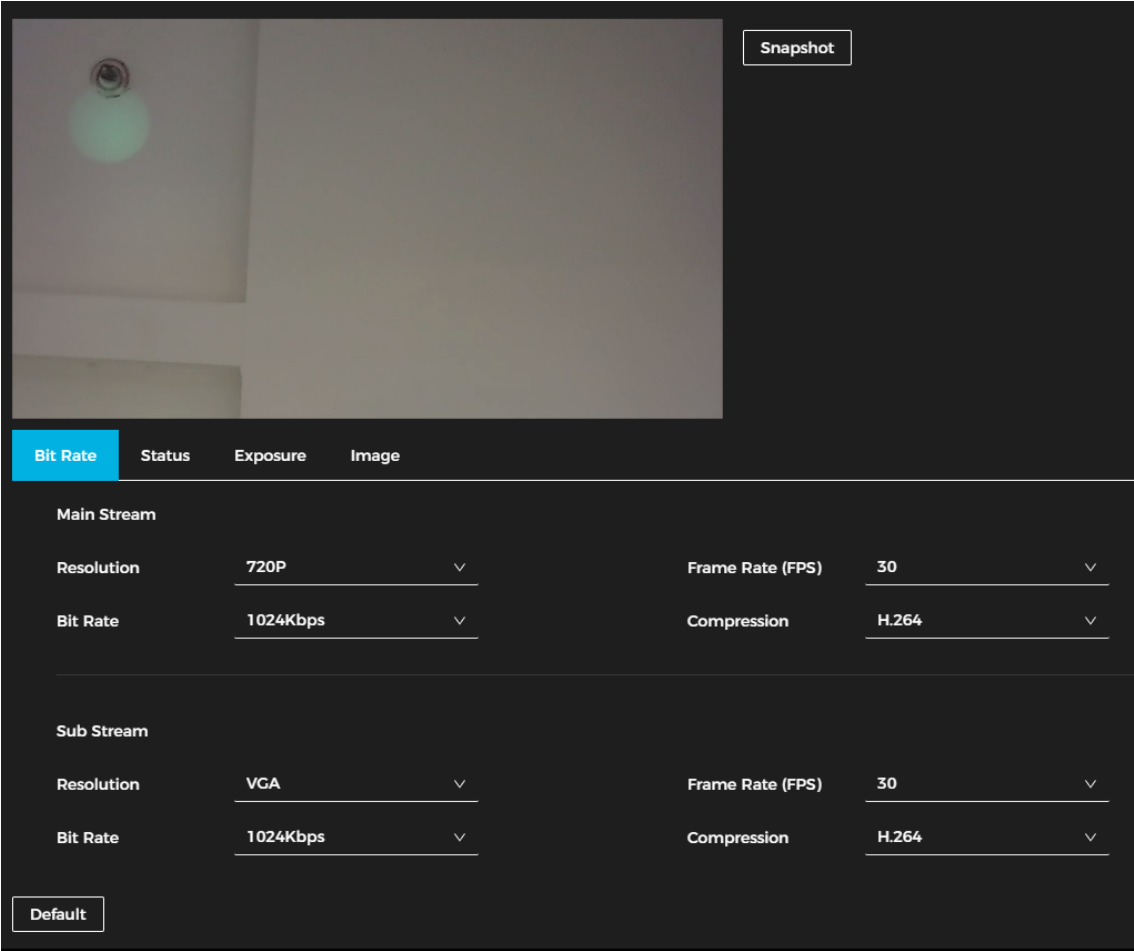
Parameter	Description
Password	Displays the password unlock icon on the standby screen.
Doorbell	When enabled, a doorbell icon appears on the standby screen. - Local device ringer: Tapping the doorbell icon on the standby screen triggers the device's built-in ringer. - Ringtone config: Select the ringtone to play. - Ringtone time (sec): Duration of the ringtone (1–30 seconds). Defaults to 3. - Alarm: Tapping the doorbell icon triggers the connected external alarm device.  NOTE This function is only available on specific models. When the alarm and doorbell cables are shared, set the functional interface to Doorbell. Refer to "Port Config".
Call	Displays the call icon on the standby screen.
Call Type	- Call room: There are 2 modes. ◇ Standard: On the standby screen, tap the call icon, enter the room number, then tap the call icon again to place the call. ◇ Phone book: Configure the list on the web page. On the standby screen, tap the call icon to view the configured indoor monitors, then tap an entry to place the call. The call list reflects the configuration set on the web page. - Call management center: On the standby screen, tap the management center icon to call the management center. - Call Phone: On the standby screen, tap the call icon to dial a phone number.  NOTE You can call LumiViewer only in this call type.

Video

Process

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

Bit rate



Bit rate description

Parameter		Description
Main stream	Resolution	When the device operates as an outdoor station connected to an indoor monitor, the indoor monitor's stream is capped at 720p. Changing the resolution to 1080p will affect call and monitoring functions.
	Frame Rate (FPS)	Number of frames captured or displayed per second.
	Bit Rate	The volume of data transmitted per unit of time. Select a value that matches your network speed.
	Compression	Encodes video to maintain image quality while reducing file size and bandwidth usage.
Sub Stream	Resolution	Supported resolutions: D1, VGA, and QVGA.
	Frame Rate (FPS)	Number of frames captured or displayed per second.
	Bit Rate	The volume of data transmitted per unit of time. Select a value that matches your network speed.
	Compression	Encodes video to maintain image quality while reducing file size and bandwidth usage.

3. Configure the status.

Status

Scene Mode	Auto	▼	Day/Night	Color	▼
Compensation Mode	WDR	▼	Video Standard	NTSC	▼
– + 30					

Parameters description of status

Parameter	Description
Scene Mode	Controls the color tone of the image depending on the shooting environment. - Disable: Scene mode is disabled. - Auto: The system automatically selects the scene mode based on lighting conditions. - Sunny: Reduces the image hue for bright outdoor conditions. - Night: Enhances the image hue for low-light conditions.
Day/Night	Controls how the device adjusts its imaging under different lighting conditions. - Auto: The system automatically switches between day and night modes based on ambient light. - Colorful: Images are colorful. - B/W: The image is in black and white.
Compensation Mode	- Disable: Compensation is disabled. - BLC: Brightens darker foreground areas when strong light comes from behind the subject. - WDR: Balances bright and dark areas of the image to improve overall quality in high-contrast scenes. - HLC: Reduces exposure in areas illuminated by intense light sources (e.g., headlights, spotlights) to improve overall image clarity.
Video Standard	Select from PAL and NTSC.

4. Configure the exposure parameters.

Exposure

Anti-flicker	Outdoor	▼	Exposure Mode	Manual	▼
Shutter	Custom Range	▼	Shutter Range	0	- 20 (0-33.33)ms
Gain	0	- 80 (0-100)	Exposure Compens...	–	+ 50
3D NR	☒		NR Level	–	+ 50

Exposure parameter description

Parameter	Description
Anti-flicker	Reduces flickering and uneven color or exposure caused by artificial lighting. 50Hz: At a 50 Hz mains frequency, exposure adjusts automatically to ambient brightness to prevent horizontal banding. 60Hz: At a 60 Hz mains frequency, exposure adjusts automatically to ambient brightness to reduce horizontal banding. - Outdoor: When Outdoor is selected, you can switch the exposure mode manually.

Parameter	Description
Exposure Mode	Controls image brightness through exposure adjustment. • Auto: The device automatically adjusts image brightness based on ambient lighting conditions. • Shutter Priority: Brightness is adjusted within the configured shutter range. If the shutter limit is reached before the target brightness is achieved, the device automatically compensates by adjusting the gain. • Manual: Manually adjust the gain and shutter values to control image brightness.  NOTE ◇ Shutter Priority is available as an exposure mode only when Outdoor is selected from the Anti-flicker list. ◇ Available exposure modes may vary by device model.
Shutter	Controls how long the sensor is exposed to light. A higher shutter speed means a shorter exposure and a darker image. Select a preset range or define a custom one.
Gain	Sets the amplification applied to the sensor signal. A higher gain improves brightness in low light but may increase noise.
Exposure Compensation	Increases or decreases overall image brightness relative to the automatic exposure level.
3D NR	3D Noise Reduction (NR). When enabled, reduces video noise for improved image clarity.
NR Level	
	Sets the noise reduction intensity. A higher level produces cleaner images but may reduce fine detail.

5. Configure the image.

Image

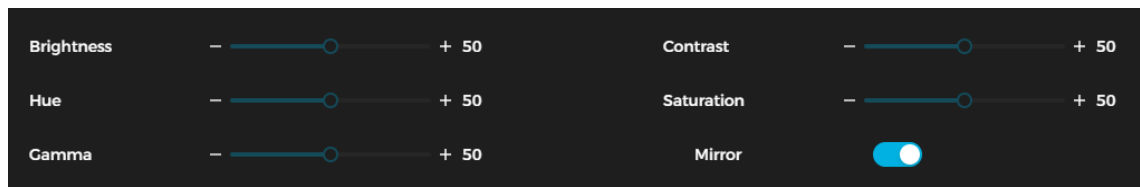


Image description

Parameter	Description
Brightness	Controls overall image brightness. A higher value produces a brighter image.
Contrast	The difference in brightness or color between objects. Higher values produce more pronounced color contrast.
Hue	Shifts the overall color tone of the image along the color spectrum.
Saturation	Controls the intensity of colors in the image. Higher values produce more vivid colors.  NOTE Adjusting saturation does not affect image brightness.
Gamma	Adjusts brightness and contrast non-linearly. Higher values produce a brighter image.
Mirror	When enabled, the image is flipped horizontally.

Audio

Configure audio prompts played during identity verification.

Process

1. Go to System Setting > Audio.
2. Configure the audio parameters.

Configure audio parameters

Speaker Volume 0 (0-100) ⓘ

Microphone Volume 0 (0-100) ⓘ

Key Sound ☐

Audio Collection ☒

Only supports MP3 files that are less than 20 KB with a sampling rate of 16K.

Audio File

Successfully verified.

Audio File: - 

Failed to verify.

Audio File: - 

Not wearing face mask.

Audio File: - 

DND Mode ☐

Apply Refresh Default

Parameters description

Parameters	Description
Speaker Volume	Adjusts the speaker output volume.
Microphone Volume	Adjusts the microphone input volume.
Key Sound	When enabled, the device plays a sound on each key press — a tap sound on touchscreen models and a click sound on non-touchscreen models.
Audio Collection	When enabled, audio from the device's microphone is captured during live view and recording.
Audio File	Click to upload the audio file.
DND Mode	Silences voice prompts during identity verification within the configured time periods. Up to four periods can be set.

3. Click  to upload an audio file for each audio type.

 NOTE

Only MP3 files under 20 KB with a 16 kHz sampling rate are supported.

4. Click Apply.

Motion Detection

The screen wakes when a moving object is detected and the configured threshold is exceeded.

Background Information



NOTE

This function is only available on specific models.

Process

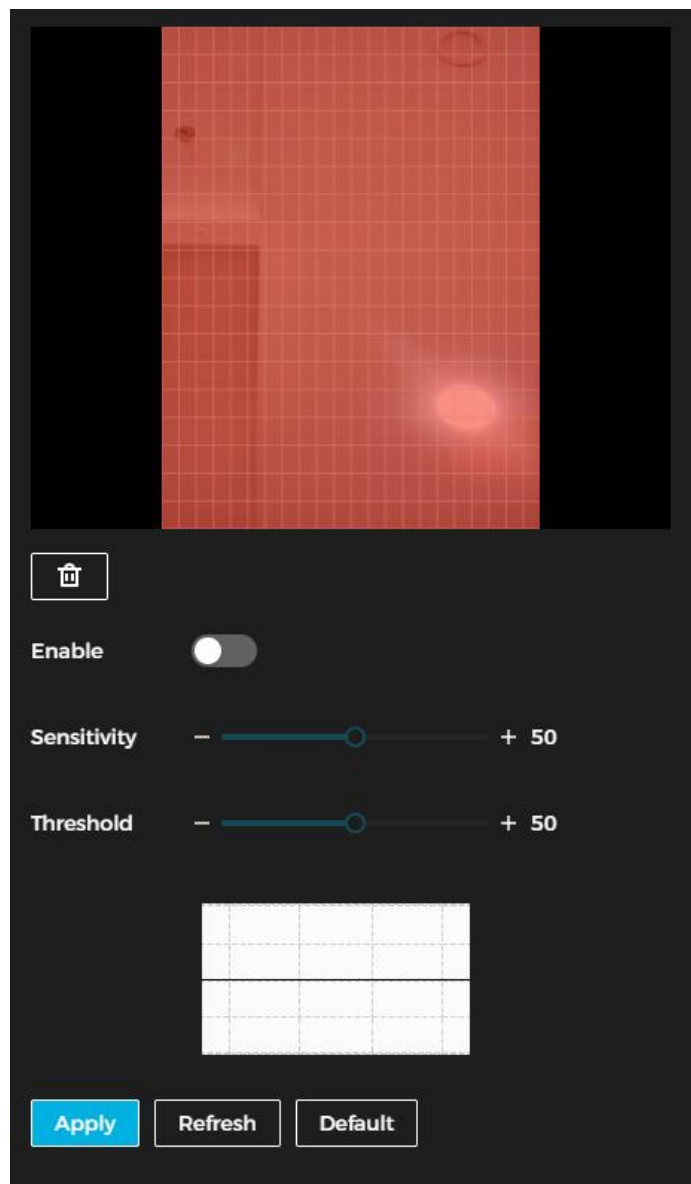
1. Go to System Settings > Motion Detection.
2. Enable motion detection.
3. Click and drag to draw the detection area within the red zone.



NOTE

- The selected motion detection area is highlighted in red.
- To clear the motion detection area, click .
- Drawing within the default motion detection area converts that region into a non-detection area.

Motion detection area



4. Configure the parameters.
 - Sensitivity: How readily the device detects motion. Higher values trigger detection more easily.
 - Threshold: Filters environmental noise (e.g., swaying leaves) by setting the minimum pixel change

- required to trigger an alarm. Lower values trigger detection more easily.
- Click Apply.
A red line indicates motion has been detected; a green line indicates no motion is detected.

View Selection

Define the visible area used during video calls and live preview.

Background Information



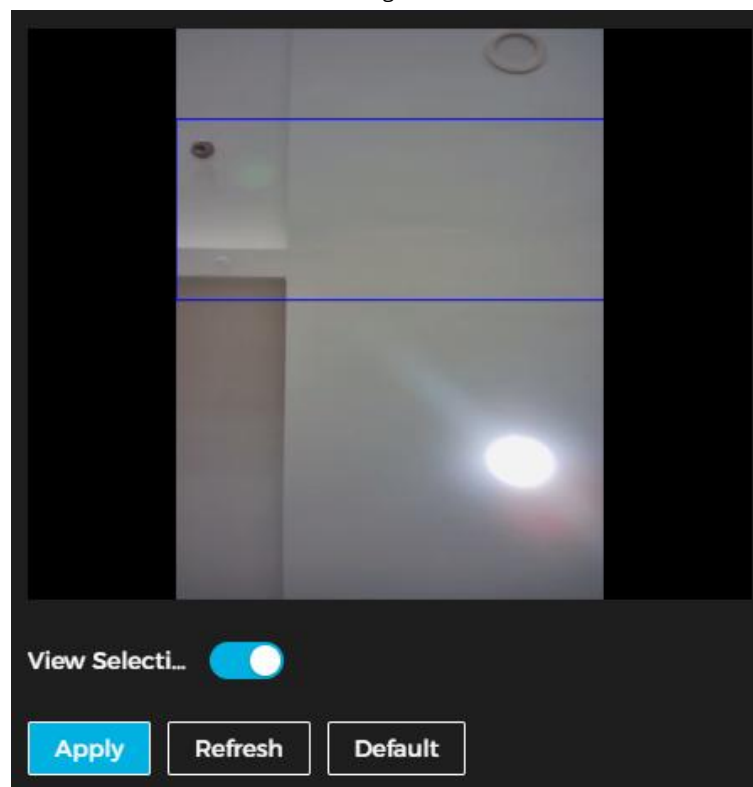
NOTE

- This function is available on specific models only.
- This function is enabled by default when used with an indoor monitor. Disabling it may make the preview inaccessible.

Process

- Go to System Settings > View Selection.
- Enable View Selection.
- Drag the selection box to the desired position.
The selection box defines the area displayed during a video call or preview.

Local coding



- Click Apply.

Advertisement

Select a display theme and upload image or video advertisements shown on the device.

NOTE

- This feature is available on select models only.
- B-frames in platform videos are not supported for decoding.
- 1-bit depth images are not supported.
- Semi-transparent images are not supported.
- Supported advertising resolutions vary by device model.

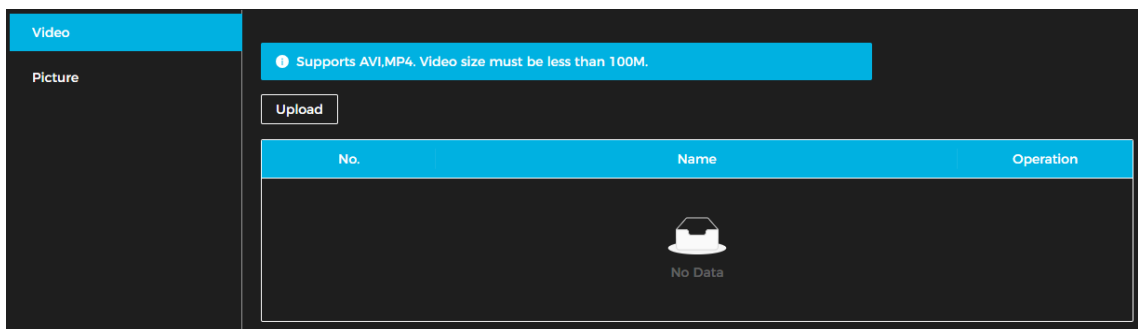
Adding Resources

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

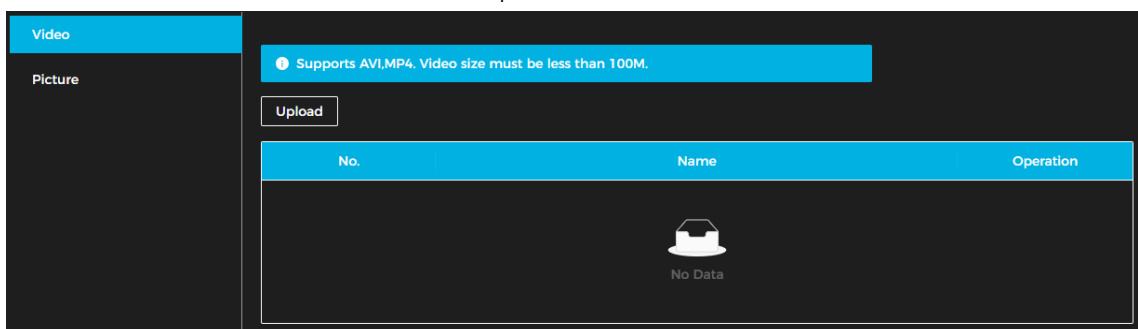
Process

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 a video file, and click Next.The video is automatically uploaded to the platform once transcoding is complete.

NOTE

- ◇ Up to 5 video files can be uploaded.
 - ◇ Supported formats: AVI and MP4. Maximum file size: 100 MB.
 - ◇ Video file upload requires the latest version of Firefox or Chrome.
- Add images.
 1. Click Upload.
 2. Select an image from your computer and upload it.



NOTE

Supported formats: PNG, JPG, and BMP. Maximum file size: 2 MB.

Related Operations

Click  to delete an uploaded image or video.



NOTE

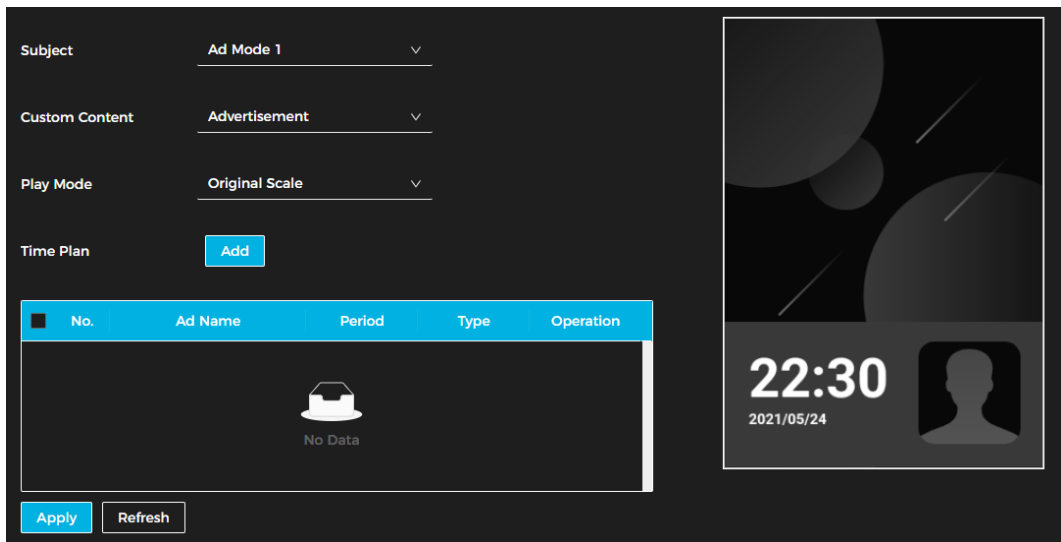
Images and videos currently in use cannot be deleted.

Configuring Subject

Process

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

Advertisement mode



2. Select the play mode.
 - Original Scale: Displays images and videos at their original size.
 - Full Screen: Displays images and videos in full screen.
3. Click Add to create a schedule. Up to 10 schedules can be added.
4. Enter the advertisement name.
5. Select the period and file type.
6. Enter the duration, upload the media files, and click Apply.
 - Sets the display duration per image when images are played in a loop. Range: 1–20 seconds (default: 5 seconds).
 - After uploading videos, you can reorder them.

Figure 3-54 Add time schedules

Add [X]

Ad Name _____

Period 00:00:00 [clock] - 23:59:59 [clock]

Type ☒ **Picture** ☐ **Video**

Duration 5 **s**

Ad Resources

[Cancel] [OK]

4. Configure the greeting message.
 1. Under Custom Content, select Greetings.
 2. Select a template.
 3. Enter the greeting title and subtitle.

Greetings

Subject Ad Mode 1 [v]

Custom Content Greetings [v]

Template

 **Current Tem...**
Galaxy

Content Please edit your content below.

Title _____

Subtitle _____

[Apply] [Refresh]

Preview:

22:30
2021/05/24

[User Silhouette]

4. Click Apply.

Management Center

System Information

Version Information

Go to Maintenance Center > Version to view version information of the device.

Legal Information

Go to Maintenance Center > Legal Info to view the software license agreement, privacy policy, and open-source

software notice.

System Capacity

View the device's storage capacity for users, cards, and face images.
Go to Maintenance Center > System Capacity.

Log

View and search system logs, admin logs, unlock records, and more.

System Logs

Search and view system event logs.

Process

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

Related Operations

- Click Export to save the search results to your computer.
- Click Encrypt Log Backup and set a password. The exported file requires this password to open.
- Click  to view log details.

Unlock Records

Search and export unlock records.

Process

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

Call History

View the call history log.

Process

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

Alarm Logs

View and search alarm logs.

Process

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

Admin Logs

Search administrator logs by admin ID.

Process

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

USB Management

Import or export user information via USB.

Process

1. Go to Maintenance Center > Log > USB Management.



NOTE

- Before exporting data or updating the system, make sure the USB drive is inserted. Do not remove the USB drive or operate the device while the process is running.
 - USB is required to transfer information from this device to others. Facial images cannot be imported via USB.
2. Select a data type, then click USB Import or USB Export.

Maintenance

Use configuration file import/export to apply the same settings across multiple devices.

Export/Import Configuration Files

Import and export device configuration files to replicate settings across multiple devices.

Background Information

- The following configurations can be exported and imported:
 - ◇ Intercom settings
 - ◇ Shortcut settings
 - ◇ Time settings
- Network settings, advertisement settings, and security settings cannot be exported or imported.

Process

1. Go to Maintenance Center > Maintenance > Config.

Configuration management

2. Export or import configuration files.
 - Export.
Click Export to download the configuration file to your computer.
 - Import.

1. Click Browse and select the configuration file.
2. Click Import File.



NOTE

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

Restore to Default

Process

1. Go to Maintenance Center > Maintenance > Config.



CAUTION

Restoring default settings will erase device data.

2. Select a restore option.
 - Factory Defaults: Resets all device settings and deletes all data.
 - Restore to Default (Except for User Info and Logs): Resets all device settings and deletes all data but retains user information and logs.

Restart

Restart the device periodically during idle periods to maintain optimal performance.

Process

1. Go to Maintenance Center > Maintenance > Restart.

Restart

2. Set the maintenance time, then click Apply.
The device will restart at the scheduled time. To restart immediately, click Restart.

Update



CAUTION

- Only use the update file provided by technical support.
- Do not disconnect power or network, and do not restart or shut down the device during the update.

File Update

Process

1. Go to Maintenance Center > Update.
2. Under File Update, click Browse and select the update file.



NOTE

The update file must be in .bin format.

3. Click Update.

The device restarts automatically once the update is complete.

Online Update

Process

1. Go to Maintenance Center > Update.
2. Under Online Update, select an update method.
 - Auto Check for Updates: The device automatically checks for the latest version.
 - Manual Check: Click to check for a new version immediately.
3. (Optional) Click Update Now to apply the update immediately.

Advanced Maintenance

Export device information and capture data packets to aid troubleshooting.

Export

Process

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

Packet Capture

Packet Capture

1. Go to Maintenance Center > Advanced Maintenance.

Packet capture

Packet Capture							
NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size	Packet Sniffer Backup
eth0		Optional	Optional	Optional	Optional	0.00MB	
eth2		Optional	Optional	Optional	Optional	0.00MB	
lo		127.0.0.1	Optional	Optional	Optional	0.00MB	

2. Enter the IP address, then click .
 - changes to .
 3. Once you have collected enough data, click .
- The captured packets will automatically download.

Network Test

1. Under Network Test, enter the destination address and set the data packet size.

Network test

Network Test

Destination Address

Test

Data Packet Size

64

Byte (64-4096)

Test Result

Copy

- Click Test.
Results are displayed in the Test Result area.

Security (Optional)

Configure HTTPS

Create or upload an authenticated certificate to enable HTTPS login to the web interface. HTTPS encrypts communication over the network.

Process

- Go to Security > System Service > HTTPS.
- Enable the HTTPS service.



CAUTION

Enabling TLS v1.1 or earlier versions may introduce security risks.

- Select the certificate.



NOTE

If no certificates appear in the list, click Certificate Management to upload one.

HTTPS

Enable ☒

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

Auto Redirect to HTTPS ☐

Select a device certificate

Certificate Management

	No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
☒	1		333064646161633261356...	06-19-2055 11:30:58 AM	BC067CCYA3EB12	BSC	HTTPS, RTSP over TLS

Apply

Refresh

Default

Download Root Certificate

- Click Apply.
In a browser, go "https://IP address: https port". If the certificate is installed correctly, the login page loads. Otherwise, the browser displays a certificate error or shows the site as untrusted.

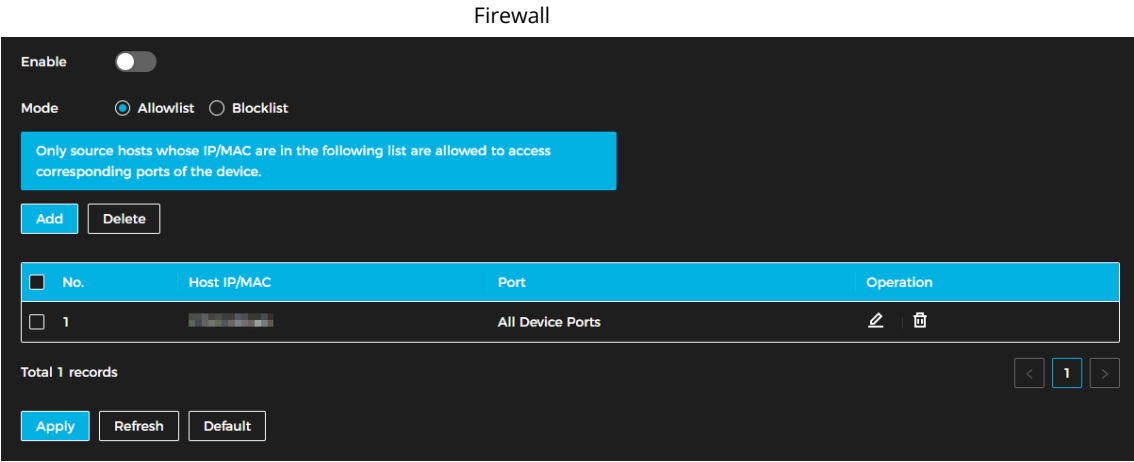
Attack Defense

Firewall

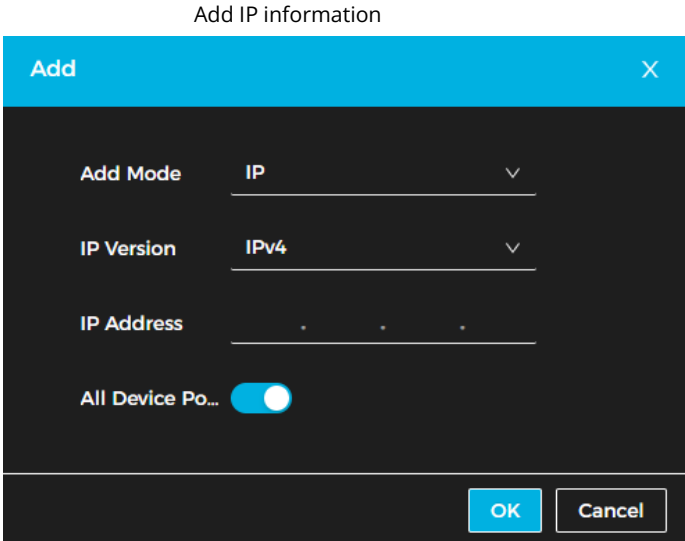
Set up a firewall to control which IP and MAC addresses can access the device.

Process

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



- 3. Select the mode: Allowlist and Blocklist.
 - Allowlist: Permits access only to listed IP and MAC addresses.
 - Blocklist: IP and MAC addresses on the blocklist are blocked from accessing the device.
- 4. Click Add to enter the IP.



- 5. Click OK.

Related Operations

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

Account Lockout

If the number of failed login attempts reaches the configured limit, the account is locked.

Process

1. Go to Security > Attack Defense > Account Lockout.
2. Set the maximum login attempts and the lockout duration for the administrator account and ONVIF user.

Account lockout

The screenshot displays the 'Account lockout' configuration window. It is divided into two sections: 'Device Account' and 'ONVIF User'. Each section has two input fields: 'Login Attempt' and 'Lock Time'. For 'Device Account', 'Login Attempt' is set to 5 (with a dropdown arrow) and 'Lock Time' is set to 5 (with a 'min' unit). For 'ONVIF User', 'Login Attempt' is set to 30 (with a dropdown arrow) and 'Lock Time' is set to 5 (with a 'min' unit). At the bottom of the window, there are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

- Login Attempt: Maximum number of failed attempts before the account is locked.
 - Lock Time: How long the account remains locked after the limit is reached.
3. Click Apply.

Anti-DoS Attack

Protect the device against DoS attacks by enabling SYN Flood and ICMP Flood attack defenses.

Process

1. Go to Security > Attack Defense > Anti-DoS Attack.
2. Enable SYN Flood Attack Defense or ICMP Flood Attack Defense to 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 or upload an authenticated certificate to enable HTTPS login from 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 information.

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 2 characters. Use the regional abbreviation.

5. Click Create and install certificate.
Once installed, the certificate appears on the device Certificate page.

Related Operations

On the Device Certificate page, click Enter Edit Mode to rename the certificate.

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

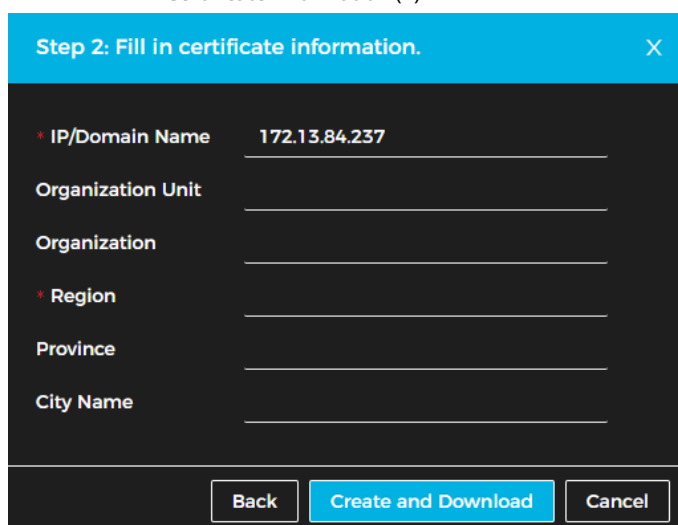
Apply for CA Certificate and Import

Install a CA certificate issued by a third-party certificate authority.

Process

1. Go to Security > CA Certificate > device Certificate.
2. Click Install device Certificate.
3. Select Apply for CA Certificate and Import (Recommended), then click Next.
4. Enter the certificate information.
 - IP/Domain Name: Enter the device's IP address or domain name.
 - Region: Enter up to 3 characters. Use the regional abbreviation.

Certificate information (2)



5. Click Create and Download.
Save the request file to your computer.
6. Submit the request file to a third-party certificate authority to obtain a signed certificate.
7. Install the signed CA certificate.
 - 1) Save the CA certificate to your computer.
 - 2) Click Install Device Certificate.
 - 3) Click Browse and select the CA certificate file.
 - 4) Click Import and Install.
Once installed, the certificate appears on the device certificate page.
 - Click Recreate to generate a new request file.
 - Click Import Later to skip installation and return to it another time.

Related Operations

On the Device Certificate page, click Enter Edit Mode to rename the certificate.

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

Install Existing Certificate

If you already have a certificate and its private key, import them directly into the device.

Process

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

Certificate and private key

Step 2: Select certificate and private key. X

Custom Name

Certificate Path

Browse

Private Key

Browse

Private Key Passwor...

Back

Import and Install

Cancel

5. Click Import and Install.
Once installed, the certificate appears on the device certificate page.

Related Operations

On the device Certificate page, click Enter Edit Mode to rename the certificate.

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

Installing the Trusted CA Certificate

A trusted CA certificate is used to verify the identity of websites and servers. For example, the 802.1X protocol requires the switch's CA certificate to authenticate the switch's identity.

Background Information

802.1X is a port-based network access control protocol that grants access only after authenticating the user's identity.

Process

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

Install the trusted certificate

Install Trusted Certificate X

Custom Name

Certificate Path

Browse

OK

Cancel

4. Click OK.
Once installed, the certificate appears on the Trusted CA Certificates page.

Related Operations

On the Device Certificate page, click Enter Edit Mode to rename the certificate.

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

Cybersecurity Recommendations

Account Management

1. Use complex passwords
Follow these guidelines when creating a password:
 - At least 8 characters long;
 - Contains at least two character types: uppercase letters, lowercase letters, numbers, or symbols;
 - Does not contain the account name or its reverse;
 - Does not use consecutive characters (e.g. 123, abc);
 - Does not use repeated characters (e.g. 111, aaa).
2. Change Passwords Regularly
Change device passwords regularly to reduce the risk of compromise.
3. Allocate accounts and permissions appropriately
Add users based on service and management needs and grant each user only the minimum permissions required.
4. Enable Account Lockout
Account lockout is enabled by default — keep it enabled to protect account security. After multiple failed login attempts, the account and source IP address are locked.
5. Keep Password Reset Information Up to Date
The device supports password reset. Update the reset information promptly whenever it changes to prevent it from being exploited. When setting security questions, choose answers that are not easy to guess.

Service Configuration

1. Enable HTTPS
Enable HTTPS to access network services over a secure, encrypted channel.
2. Encrypt Audio and Video Transmission
For sensitive audio and video data, enable encrypted transmission to reduce the risk of interception.
3. Turn off non-essential services and use safe mode
Disable any services that are not in use — such as SSH, SNMP, SMTP, UPnP, and AP hotspot — to reduce the attack surface.
Where services must remain active, enable safe mode. Recommended settings include:
 - SNMP: Use SNMP v3 with strong encryption and authentication passwords.
 - SMTP: Use TLS when connecting to the mail server.
 - FTP: Use SFTP and set a strong password.
 - AP hotspot: Use WPA2-PSK encryption and set a strong password.
4. Change HTTP and other default service ports
Change the default ports for HTTP and other services to a port between 1024 and 65535 to reduce exposure to targeted attacks.

Network Configuration

1. Enable the Allowlist
Enable the allowlist to restrict device access to trusted IP addresses only. Add your computer's IP address and the IP addresses of any other authorized devices to the allowlist.
2. Bind MAC Addresses
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
Take the following measures to reduce network risk and protect the device:
 - Disable router port mapping to prevent external access to internal network devices;
 - Segment the network based on actual requirements: use VLANs or gateways to isolate subnets that do not need to communicate with each other;
 - Deploy 802.1X access authentication to prevent unauthorized devices from connecting to the private network.

Security Auditing

1. Monitor Online Users
Regularly review the list of online users to detect any unauthorized access.
2. Review Device Logs
Device logs record login attempts — including the source IP address — and key actions performed by logged-in users.
3. Configure Network Logging
The device has limited log storage. To retain logs for longer periods, enable network logging to sync critical logs to a network log server.

Software Security

1. Keep Firmware Up to Date
Keep device firmware updated to the latest version to ensure access to the newest features and security patches.
If the device is connected to a public network, enable automatic update detection to receive manufacturer firmware updates as they are released.
2. Keep Client Software Up to Date
Always download and use the latest version of the client software.

Physical Protection

Implement physical protection for devices — especially storage devices. Place equipment in dedicated server rooms or locked cabinets and apply access control and key management to prevent unauthorized individuals from tampering with hardware or connecting external devices (such as USB drives or serial ports).