



Digital Intelligent Building Video Intercom System Linux System Outdoor Station User Manual



CONTENTS

1. VIDEO INTERCOM	2
1.1. CALLING THE INDOOR MONITOR	2
1.2. CALLING THE MOBILE APP (OPTIONAL)	2
1.3. CALLING THE MANAGEMENT CENTER	3
2. UNLOCK	3
2.1. INDOOR MONITOR UNLOCK	3
2.2. MOBILE APP UNLOCK (OPTIONAL FEATURE)	3
2.3. MANAGEMENT CENTER UNLOCK	4
2.4. PASSWORD UNLOCK	4
2.5. FACE RECOGNITION UNLOCK (OPTIONAL)	5
2.6. QR CODE UNLOCK (OPTIONAL)	5
2.7. IC CARD UNLOCK	6
2.8. FINGERPRINT UNLOCK (OPTIONAL)	6
3. SYSTEM SETTINGS	6
3.1. ADDRESS SETTINGS	7
3.2. USER PASSWORD	7
3.3. SERIAL NUMBER SETTINGS	7
3.4. ADMIN PASSWORD SETTINGS	7
3.5. PASSWORD UNLOCK	8
3.6. VOLUME SETTINGS	8
3.7. DOOR LOCK SETTINGS	8

3.8. ACCESS CONTROL PERMISSION SETTINGS	8
3.9. ACCESS CONTROL SECTOR AND PASSWORD SETTINGS	8
3.10. ACCESS CONTROL SERVER SETTINGS	9
3.11. DOOR SENSOR SETTINGS	9
3.12. TAMPER SETTINGS	9
3.13. CARD MANAGEMENT	9
3.14. FACIAL RECOGNITION MANAGEMENT	11
3.15. CLOUD VIDEO INTERCOM (OPTIONAL)	11
3.16. ELEVATOR SETTINGS	12
3.17. LANGUAGE SETTINGS	12
3.18. ADVERTISEMENT PLAYBACK (OPTIONAL)	12
3.19. DATE AND TIME SETTINGS	13
3.20. THEME SWITCHING	13
3.21. OPERATION SETTINGS	13
3.22. SYSTEM INFORMATION	13
3.23. FACTORY RESET	13
3.24. TEST MODE	13
3.25. ONE-KEY RESTART	14
4. INSTALLATION METHOD	14
5. THE NOTICE	14

Welcome to choose Our Building Video Intercom Products!

Our product is designed using the most advanced electronic communication technology available today and manufactured with superior SMT technology. It has undergone rigorous testing and inspection under a strict quality assurance system. It features high integration, high reliability, and high cost-performance, making it a trustworthy security intercom product.

Requires 12V DC; do not exceed this voltage or reverse the polarity.

The device contains sensitive electronic components and should be protected from moisture, water, and high temperatures.

The device includes an LCD display panel, which should not be pressed with sharp objects or subjected to excessive force.

The appearance, functions, and interface of the product may differ from the actual device. The actual product should be used as the reference.

1. Video Intercom

1.1. Calling the Indoor Monitor

When the device is on the main interface, visitors can enter the room number to call.

For example, to call "Building 2, Unit 3, Room 0101 in Zone 1", enter 101 or 0101 on the unit outdoor station, or 0102030101 or 102030101 on the community outdoor station.

1.2. Calling the Mobile App (Optional)

When a call comes in from the outdoor station and the indoor monitor does not answer within 25 seconds, the system forwards the call to the resident's bound mobile app. If there is no indoor monitor, the call goes directly to the mobile app. Once one mobile device answers, other devices will be disconnected. The mobile app shows the current caller's image and allows screenshot and door unlocking.



1.3. Calling the Management Center

Follow the on-screen prompts and press "#" + "4" on the keyboard to enter the property management call interface. Use "2" and "8" to switch left and right, select "Call Management Center" or "Call Security Extension", and press "#" to confirm.



2. Unlock

2.1. Indoor Monitor Unlock

When calling or speaking with the resident, the resident can remotely unlock the door through the indoor unit. The outdoor station will display "The door is opened" and provide a voice prompt.

2.2. Mobile App Unlock (Optional Feature)

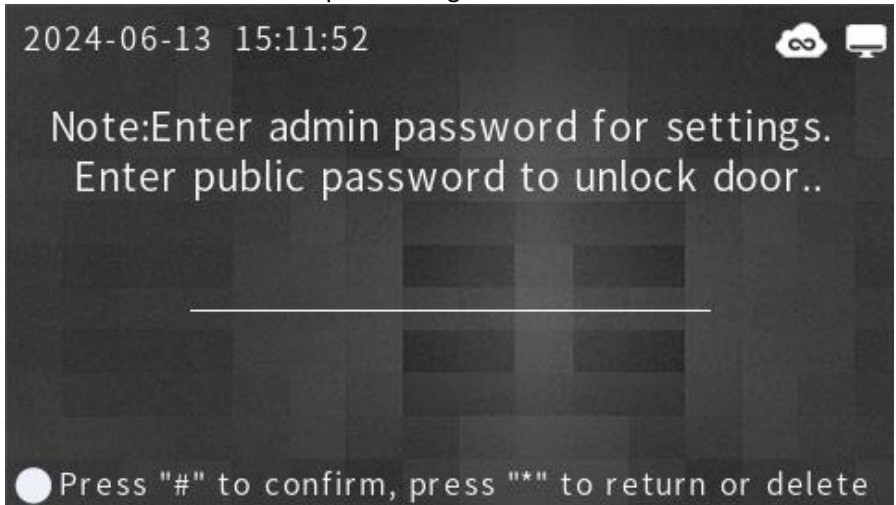
When calling or speaking with the resident, the resident can remotely unlock the door through the mobile app. The outdoor station will display "The door is opened" and provide a voice prompt.

2.3. Management Center Unlock

When calling the management center or security extension, remote unlocking can be performed. The outdoor station will display "The door is opened" and provide a voice prompt.

2.4. Password Unlock

Password unlocking includes public and user passwords. Public (User) hijack password and public (user) unlock password are auto-generated in reverse order and do not require setting.



2.4.1 Public (User) Password Unlock

Default is disabled and needs to be enabled by property personnel via engineering settings. If setting a user password, the resident must also configure it on the indoor monitor for it to be used.

Usage: Follow on-screen instructions, press "#" + "2" to enter "Password Unlocking" screen, navigate with "2" and "8" to select public password unlocking, press "#" to confirm, and enter the public password (user password unlocking, press "#" to confirm, enter room number, and enter user password) . If correct, the door unlocks and a snapshot is taken and

uploaded to the management center. If incorrect, an error message is displayed and a snapshot is taken.

2.4.2 Public (User) Hijack Password Unlock

The public (User) hijacking password is the reverse of the public (User) unlock password. It is auto-generated when the public unlock password is set (the user sets their unlock password) .

Note: The public (User) hijacking password must be different from the public (user) unlock password and is only active when the public (user) unlock password is enabled. For example, if the public (user) unlock password is 123456, the public (user) hijacking password will be 654321. Using the public (user) hijacking password triggers an alarm to the management center and security.

2.5. Face Recognition Unlock (Optional)

2.5.1 Face Registration

- On Device: Property personnel need to enable "Face Recognition Management" -> "Face Recognition Registration" in engineering settings. Follow prompts to enter room number and bind a phone number.
- Mobile App: Open Trudian Cloud app, navigate to "More Services" -> "Face Management" -> "Register Face" and follow prompts.
- Management Center - Photo Upload: Access "Face Management", select room number, enter face details, upload three photos.
- Management Center - Camera Capture: Access "Face Management", select room number, enter face details, capture three photos.

2.5.2 Face Unlock

When face recognition is enabled, the door station uses infrared or microwave sensors to wake up and recognize the face in sleep mode, or manually enter the unlock screen and press "#" + "1" to start face recognition.

2.6. QR Code Unlock (Optional)

2.6.1 Obtaining QR Code

Open the app, click "Authorize Code to Open", generate a QR code.

2.6.2 QR Code Authorization

Click "Authorize to Visitor" under the QR code, set visitor identity, code validity, and rules, then share via WeChat, QQ, or SMS.

2.6.3 QR Code Unlock

Press "#" + "3" to enter the QR code recognition screen and present a valid QR code to the door station.

2.7. IC Card Unlock

Place a valid access card near the reader area to unlock.

2.8. Fingerprint Unlock (Optional)

2.8.1 Fingerprint Registration

Property personnel need to enable "Fingerprint Management" -> "Fingerprint Registration" in engineering settings. Follow prompts to enter room number and complete registration.

2.8.2 Fingerprint Unlock

Press a registered finger on the fingerprint sensor. If recognized, the door station displays "The door is opened" with a voice prompt.

3. System Settings

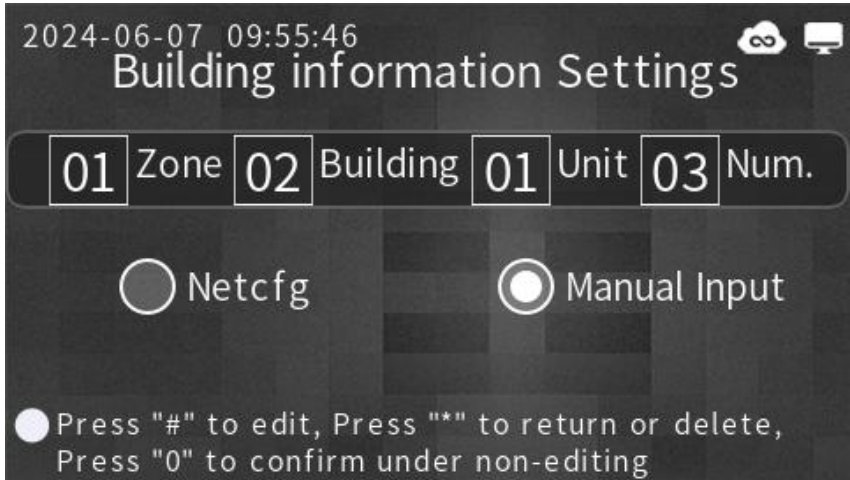
System settings include address setting, admin password setting, unlock password setting, password permissions, volume setting, unlock setting, door sensor setting, language setting, date and time setting, system information, card management, restore setting, access control setting, device serial number, and 24 other settings.

Note: These settings must be operated by professional engineering personnel. Users should not change these settings lightly.

To enter system settings: On the main screen, press "#" + "2". Then enter the six-digit admin password (default is 666666) to access the system

settings menu.

3.1. Address Settings



- 1) Click "Address Settings" to set the building information.
- 2) For example, to set the address for Building 2, Unit 1, Door Station 3 in Zone 1.
- 3) After setting the address, you can either assign an IP address to the door station based on the room number configuration table or manually enter the IP address. The device will automatically restart upon successful configuration.

3.2. User Password

Press the "#" to toggle the switch. When enabled by the administrator, users can set the unlock password via the indoor monitor for unlocking.

3.3. Serial Number Settings

The device serial number is a unique identifier set at the factory and should not be modified.

3.4. Admin Password Settings

Administrators can change the admin password by entering the current password (6 digits) and the new password twice (6 digits each). This allows for easier management.

3.5. Password Unlock

Press the "#" key to toggle the switch. Enter the correct old public unlock password to set a new one. If successful, the interface and voice prompt will indicate success; otherwise, it will indicate failure.

Note: The default public unlocking password is 012345, and the default hijacking password is 543210. If the public unlocking password is set to 666666 or 121121, it will match the hijacking password, violating the rules and causing the setting to fail.

3.6. Volume Settings

Set the advertisement volume and ring volume. Press "4" to decrease the volume and "6" to increase the volume.

3.7. Door Lock Settings

Set the unlock delay for the electric lock. The default unlock method is power-on unlock with a 10-second delay. Users can customize this setting as needed.

3.8. Access Control Permission Settings

Each unit has a unique access control number matching the "Access Control Permission Settings" in the management center.

Access Control Permission Value: Must match the settings in the property management terminal.

3.9. Access Control Sector and Password Settings

Sector: Matches the sector number (01-16) set by property when issuing the access card.

Password: Matches the 12-digit password set by property.

Note: For easier management, use a unified sector and password for the entire community. Settings can be done manually, with a management

card, or via management center software. Refer to the PC terminal user manual for details.

3.10. Access Control Server Settings

Factory set; do not modify. Used for retrieving cloud intercom server address, port, and SIP account info. Each unit has a unique access control number matching the "Access Control Permission Settings" in the management center.

3.11. Door Sensor Settings

Set the door sensor status & delay. Default is disabled. Customize as needed.

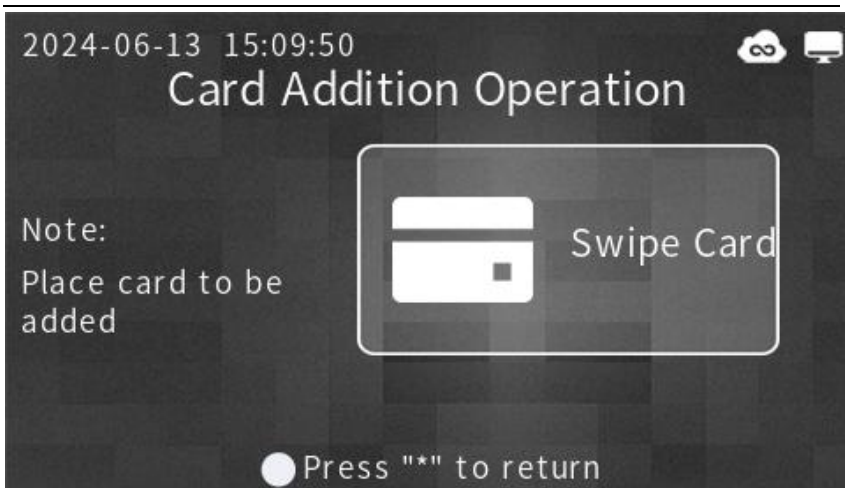
3.12. Tamper Settings

Toggle tamper protection with "#". When enabled, an alarm will notify the management center and security if the device is tampered with.

3.13. Card Management

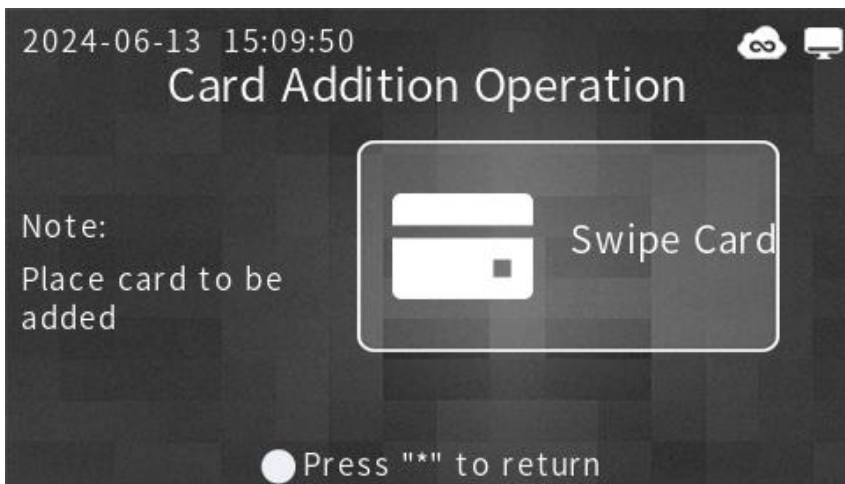
3.13.1 Add Card





To add a card, select "Add Card," enter the room number, and place the card on the reader. The screen will then indicate success.

3.13.2 Delete Card



To delete a card, select "Delete Card" and place the card on the reader. The screen will then indicate success.

Note: Multiple cards can be added or deleted. It's recommended to manage cards via the management center PC terminal.

3.14. Facial Recognition Management

3.14.1 Automatic Facial Recognition

Toggle facial recognition activation via microwave sensor. Press "#" to toggle.

3.14.2 Liveness Detection

Enable liveness detection to prevent unauthorized access using photos, face swaps, masks, obstructions, and screen captures. Toggle with "#".

3.14.3 Liveness Detection Threshold

Adjust liveness threshold to determine pass rates. Real humans score close to 1, non-humans close to 0. Adjust with "4" to decrease, "6" to increase. RGB range: 0.6-0.99.

3.14.4 Recognition Model Threshold

Recommended identification threshold is 80 points. Increasing it reduces false positives but may slow recognition. Adjust with "4" to decrease, "6" to increase. Model range: 80-90.

3.14.5 Facial Recognition Registration

Enter the facial registration interface.

3.14.6 Facial Authorization

Enter the facial recognition authorization code to enable the feature on the device.

3.14.7 Facial Recognition Information

View information such as license number, authorization code, and authentication status.

3.15. Cloud Video Intercom (Optional)

3.15.1 Cloud Video Intercom

The administrator enables this feature. If the indoor unit is not answered within 25 seconds, the call is forwarded to the resident's mobile app. The first phone to answer disconnects the others, displays the caller's image, and allows screenshots and door unlocking.

3.15.2 QR Code Unlock

Admin enables this feature. Residents and visitors can unlock using a QR code.

3.16. Elevator Settings

Requires elevator control module.

3.16.1 Call Elevator

Calls the elevator to the current floor when the door station is accessed.

3.16.2 Elevator Server Setting

Sets the IP address of the elevator controller server.

3.16.3 Elevator Controller Status

Checks the status of the elevator controller.

3.16.4 Elevator Controller Number Setting

Matches the elevator controller number.

3.16.5 Elevator Floor Number Setting

Sets the floor number the elevator will arrive at. The first floor is 0, B1 is 1, B2 is 2, and so on, with a maximum value of 15.

3.17. Language Settings

Set the system language (default is Chinese).

3.18. Advertisement Playback (Optional)

Enable or disable advertisement playback.

3.19. Date and Time Settings

Enable automatic date and time settings, or set manually if needed.

If the time setting is unreasonable, the system will prompt a failure. The door phone will automatically sync time with the property center when turned on or running. The format is YYYY-MM-DD HH, e.g., 2019-01-01 08:00.

3.20. Theme Switching

Select the application theme based on user preference.

3.21. Operation Settings

Enable or disable call hang-up after unlocking.

3.22. System Information

View system information such as device number, IP address, gateway, subnet mask, program version, release date, network configuration version, and system version.

3.23. Factory Reset

Select "Factory Reset," select "confirm" or "#" to reset the system, "cancel" or "*" to return.

3.24. Test Mode

Click "Test Mode" to restart the system and enter test mode. This mode includes tests for continuous flow, loop, camera, microphone, speaker, LCD display, touchscreen, system card reading, wired network, SD card, human presence, tamper detection, pressure test images, pressure test videos, door sensor, unlocking, and door open button.

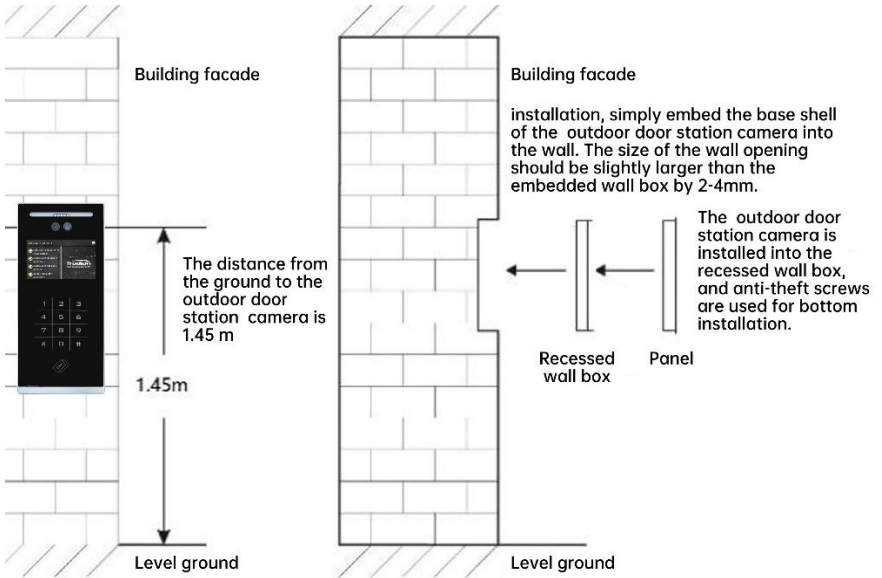
Click the "Hardware" button in the top right corner to test the camera, microphone, speaker, LCD display, touchscreen, GPIO port, serial port, system card reading, system buttons, wired network, and SD card.

Click "Back" to exit test mode.

3.25. One-Key Restart

Click "One-Key Restart" to reboot the device.

4. Installation method



5. The Notice

1. Do not expose the device to wind and rain. If unavoidable, please install a rain cover.
2. Do not aim the camera at direct sunlight or strong light.
3. Ensure the camera has even lighting as much as possible.
4. Do not install the device near strong magnetic fields.
5. Do not install the device in locations where the background noise exceeds 70dB.
6. Only qualified professionals should perform repairs. For technical issues, please call our national service hotline at 400-6116-328.

