Jakin ID

ACTA4 Operation Manual (Version 1.8 , March 2025)

Table of Contents

---

1. Introduction

1.1 Purpose

The ACTA4 device is an IoT hardware platform for cloud- and web-based ID management, providing solutions for both physical security and workforce management. This manual guides you through the operation and administration of the ACTA4 system.

1.2 Key Features

- **Multi-modal Authentication**: Fingerprint, facial recognition, smart card, PIN, and QR code
- **Web-Based Management**: Access from anywhere using any web browser
- **Embedded Web Server**: No additional software required for operation
- **Access Control**: Door strike control with configurable unlimited AccesGroups/Rights schedules
- **Time Attendance**: Comprehensive reporting for workforce management
- **Network Connectivity**: Ethernet, PoE(optional), WiFi (optional), and 4G/5G (optional)

1.3 Software Version

This manual covers ACTA4 firmware version 4_00.2247 or above.

2. Product Overview

2.1 Physical Security Applications

- Access control for doors, gates, turnstiles, and barriers
- Integration with electric strikes, electromagnetic locks, and electric deadbolts
- Video surveillance integration

2.2 Workforce Management Applications

- Time and attendance tracking
- Job code tracking
- Payroll integration (CSV/TXT export)

2.3 Operating Modes

Standalone Mode: Single unit or Master/Client setup (up to 10 units synchronized)

Enterprise Mode: Integration with Access Manager Suite (AMS) for large-scale deployments

---

3. Getting Started

3.1 Default Credentials

- **Default IP Address**: 192.168.1.100
- **Default Admin ID**: A999
- **Default Password**: 1

⚠ **IMPORTANT**: Change the default administrator credentials immediately after first login.

3.2 Changing Default Credentials

1. Open a web browser and navigate to http://192.168.1.100
2. Login with Admin ID: **A999**, Password: **1**
3. Go to "View User List"
4. Click on ID "A999"
5. Enter new Administrator ID and Password
6. Click "Modify"

3.3 Standby Screen

When idle, the ACTA4 displays:

- Company logo
- Current time
- Current trigger type
- Date and day of week

---

4. Fingerprint Usage Guidelines

4.1 Technical Specifications

- **Image Resolution**: 500 DPI
- **False Rejection Rate (FRR)**: 0.01%
- **False Acceptance Rate (FAR)**: 0.0001%
- **Allowable Rotation**: ±15 degrees
- **Matching Speed**: 0.05 seconds
- **Scanning Speed**: 1.50 seconds

4.2 Enrollment Best Practices

Critical Success Factors:

1. **Finger Placement**: Center the fingerprint core on the sensor
2. **Pressure**: Apply medium pressure (not too hard, not too soft)
3. **Rotation**: Keep rotation minimal (within ±10 degrees)
4. **Coverage**: Cover the entire sensor surface with your finger
5. **Condition**: Ensure finger is neither too dry nor too wet

Three-Image Enrollment Method:

1. **First Image**: Place finger centered on sensor
2. **Second Image**: Place finger slightly left of center
3. **Third Image**: Place finger slightly right of center

4.3 Finger Preparation

For Dry Fingers:

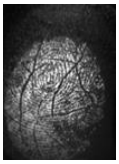
- Breathe on your finger
- Touch your forehead to pick up natural oils
- Apply small amount of skin-moisturizing lotion

For Wet Fingers:

- Wipe with a clean cloth or paper towel

4.4 Good vs. Bad Images


Good Image: Clear fingerprint core with well-defined ridges

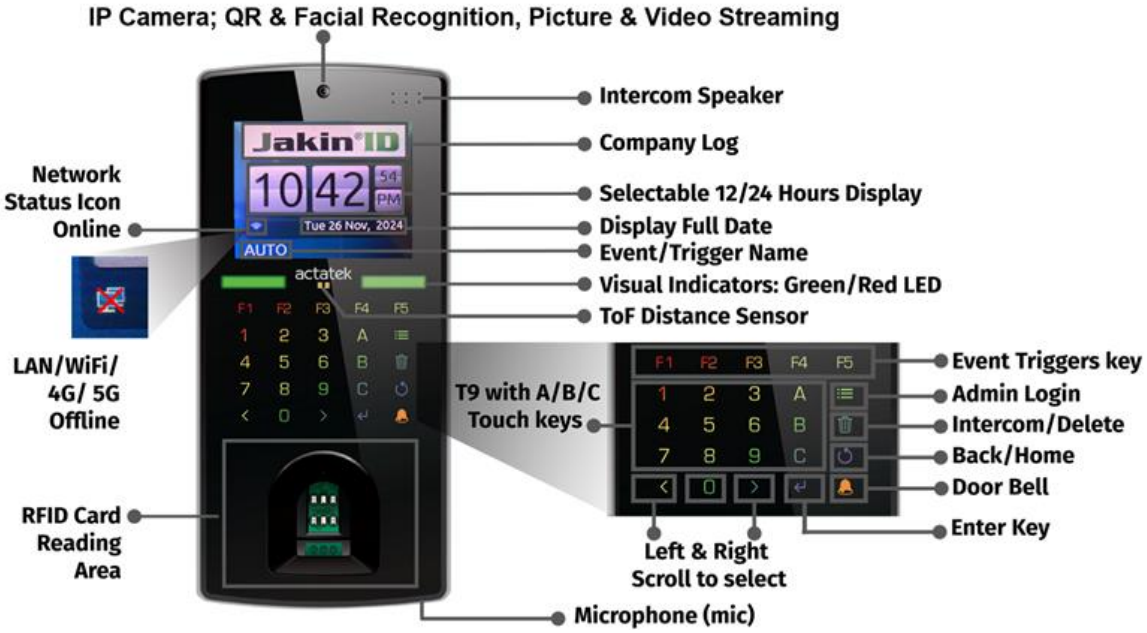

Bad Image: Blurred, smudged, or displaced fingerprint with unclear core

4.5 Recommended Fingers

- Use thumbs or index fingers for best results
- Avoid using pinky fingers (often have smaller cores)

---

5. Device Interface



5.1 LCD Display

The color LCD screen displays:

- Authentication prompts
- User messages
- System status
- Menu options

5.2 Keypad Layout

- **Numeric Keys (0-9)**: Enter IDs and passwords
- **Function Keys (F1-F4)**: Trigger selection and special functions
- **Enter**: Confirm selection
- **Back**: Return to previous screen
- **Previous/Next**: Navigate menu options
- **Menu**: Access administrator menu
- **Bell Icon**: Doorbell/Intercom function

5.3 Fingerprint Scanner

- Optical scanner with 500 DPI resolution
- Located below the keypad
- Supports 1:1 authentication (ID + fingerprint) or 1:N authentication (Auto-Match)

---

6. User Operations

6.1 Clocking In/Out

Method 1: ID + Fingerprint

1. Enter your User ID
2. Press Enter
3. Place enrolled finger on scanner
4. Wait for confirmation

Method 2: Auto-Match (enabled by default)

1. Place enrolled finger on scanner
2. Wait for confirmation

Method 3: Smart Card

1. Present card to the bottom of the front panel
2. Wait for confirmation

Method 4: PIN

1. Enter your User ID
2. Press Enter
3. Enter your password
4. Press Enter

Method 5: QR Code

1. Display QR code on mobile device (keep 20cm distance from camera)
2. Wait for confirmation

6.2 Trigger Selection

Triggers define the purpose of your authentication (IN, OUT, Lunch, etc.)

Changing Trigger:

1. Press F1, F2, F3, or F4 before authentication
2. The selected trigger appears on screen
3. Proceed with authentication

6.3 Viewing Personal Messages (Pre-configured User Messages)

After successful authentication, any personal messages assigned to you will display on the LCD screen.

6.4 Using the Doorbell

Press the doorbell button (top right of keypad) to:

- Ring the connected bell/buzzer
- Initiate intercom call (if configured)

7. Administrator Functions (via Device Console)

7.1 Accessing Admin Menu

1. Press the **Menu** button
2. Enter Admin ID (default: **A999**)
3. Press Enter
4. Enter Password (default: **1**)
5. Press Enter

7.2 Adding New Users

Adding User via Fingerprint:

1. From Admin Menu, select "Add User" icon
2. Press Enter
3. Select "Fingerprint"
4. Press Enter
5. Enter new User ID (minimum 3 characters)
6. Press Enter
7. Place finger on sensor (wait for "Please Remove Finger")
8. Repeat for 2nd fingerprint sample
9. Repeat for 3rd fingerprint sample
10. Confirmation: "User Added"

Adding User via Smart Card:

1. From Admin Menu, select "Add User" icon
2. Select "Smart Card"
3. Select "New User"
4. Enter new User ID
5. Press Enter
6. Present smart card to reader
7. Confirmation: "Success"

Adding User via Password:

1. From Admin Menu, select "Add User" icon
2. Select "Password"
3. Enter new User ID
4. Press Enter
5. Enter password for user
6. Press Enter
7. Confirmation: "Success"

Adding User via Face:

1. From Admin Menu, select "Add User" icon
2. Select "Face"
3. Enter new User ID
4. Press Enter
5. Face capture begins automatically
6. Confirmation: "User Added"

7.3 User Management

Activating a User:

1. Select "User Management" icon
2. Select "Activate User"
3. Enter User ID
4. Press Enter

Deactivating a User:

1. Select "User Management" icon
2. Select "Deactivate User"
3. Enter User ID
4. Press Enter

Deleting a User:

1. Select "User Management" icon
2. Select "Delete User"
3. Enter User ID
4. Press Enter

⚠ **Warning**: Deleting a user removes ALL information including access logs.

7.4 Auto-Match Configuration

Auto-Match allows users to authenticate without entering an ID first.

Enabling Auto-Match:

1. Select "Auto Match" icon
2. Select "Auto Match"
3. Enter User ID
4. Press Enter
5. Confirmation: "Automatch Enabled"

Disabling Auto-Match:

1. Select "Auto Match" icon
2. Select "Auto Match"
3. Enter User ID
4. Press Enter
5. Confirmation: "Automatch Disabled"

7.5 Date & Time Settings

Adjusting Date:

1. Select "Date & Time" icon
2. Select "Adjust Date"
3. Enter new date (YYYY/MM/DD format)
4. Press Enter

Adjusting Time:

1. Select "Date & Time" icon
2. Select "Adjust Time"
3. Enter new time (HH:MM:SS format)
4. Press Enter

7.6 Network Settings (IP Configuration)

Setting Static IP Address:

1. Select "IP Setting" icon
2. Select "IP Address"
3. Enter new IP address
4. Press Enter

Setting Gateway:

1. Select "IP Setting" icon
2. Select "Gateway"
3. Enter gateway address
4. Press Enter

Setting DNS:

1. Select "IP Setting" icon
2. Select "DNS IP"
3. Enter DNS server address
4. Press Enter

Enabling DHCP:

1. Select "IP Setting" icon
2. Select "DHCP"
3. Press Enter to toggle ON
4. Confirmation: "DHCP Enabled"

7.7 Terminal Settings

Fingerprint Security Level:

1. Select "Terminal Settings" icon
2. Select "FP Quality"
3. Choose: High / Normal / Low
4. Press Enter

Unlocking Door Manually:

1. Select "Terminal Settings" icon
2. Select "Unlock Door"
3. Press Enter

System Reboot:

1. Select "Terminal Settings" icon
2. Select "Reboot"
3. Press Enter

7.8 Reset Functions

Resetting Event Log:

1. Select "Reset" icon
2. Select "Reset Event Log"
3. Press Enter
4. Confirm

Resetting User Database:

1. Select "Reset" icon
2. Select "Reset Database"
3. Press Enter
4. Confirm

Factory Default:

1. Select "Reset" icon
2. Select "Factory Default"
3. Press Enter
4. Confirm (system will reboot)

---

8. Web Administration

8.1 Accessing Web Interface

1. Open web browser (Edge, Chrome, Firefox, or Safari)
2. Enter device IP address (e.g., http://192.168.1.100)
3. Click "Secure" for encrypted connection (recommended)
4. Accept security certificate
5. Enter login credentials

8.2 User Access Levels

Personal User: View personal attendance records only

User Administrator: Manage users, departments, access groups, and reports

Network Administrator: Configure system settings, network, and technical parameters

Super Administrator: Full access to all functions

8.3 Terminal Status Dashboard

The main page displays:

- Model number and serial number
- Firmware version
- IP address and uptime
- Registered users / Maximum capacity
- Auto-match user count
- Memory status

8.4 User Administration

Viewing Event Logs:

1. Login to web interface
2. Select "View Event Log"
3. Filter by: Name, User ID, Department, Event, or Date Range
4. Click column headers to sort
5. Export to CSV/TXT if needed

Adding Users via Web:

1. Select "Add New User"
2. Enter User ID, Name, Password
3. Select Access Group and Department
4. Choose authentication methods
5. Click "Add"

Remote Fingerprint Enrollment:

1. Add new user via web
2. Click "Activate Capture"
3. User places finger on device scanner
4. Repeat for required samples
5. Click "Add" to save

Remote Smart Card Enrollment:

1. Add new user via web
2. Click "Activate Read"
3. User presents card to device
4. Click "Add" to save

Uploading Facial Photo:

1. Add new user via web
2. Click "Choose File"
3. Select JPEG photo (max 1000x1000 pixels)
4. Click "Upload"
5. Click "Add" to save

8.5 Department Management

Adding Department:

1. Select "Departments"
2. Enter Department Name and Description
3. Click "Add"

Modifying Department:

1. Click on Department ID
2. Make changes
3. Click "Modify"

Deleting Department:

1. Check box next to department
2. Click "Delete"

8.6 Access Control

Creating Access Groups:

1. Select "Access Groups"
2. Select department
3. Enter group name
4. Click "Add"

Adding Access Rights:

1. Open Access Group
2. Click "Add Access Right"
3. Select terminal
4. Set Quick Access (Enable/Disable)
5. Click "Set Terminal"
6. Select days and time range
7. Set Enabled/Disabled
8. Click "Set Time"
9. Click "Submit Access Group"

Configuring Triggers:

1. Select "Triggers"
2. Click on trigger name
3. Modify schedule for each terminal
4. Set time periods as Enabled/Disabled

5. Click "Modify"

Setting Holidays:

1. Select "Holidays"
2. Click calendar dates or type date (YYYY/MM/DD)
3. Click "Add"
4. To remove, click on existing holiday

8.7 Terminal Settings (Refer to the User Manual for detailed information)

Terminal Setup:

- Terminal Description
- Network Settings (IP, Subnet, Gateway, DNS)
- Fingerprint Security Level
- Smart Card Settings
- Facial Recognition Settings
- Console Display Timeout
- Terminal Mode (Standalone / Access Manager)
- Door Strike Options
- Language Selection

Authentication/Log Setup:

- Enable/Disable Event Logging
- Log Size Configuration
- Log Unauthorized Events
- Accept Unregistered Smart Cards
- Photo Options for Authorized/Unauthorized Events
- Security Options:
    - Auto IN/OUT
    - Reject Repeated Event
    - Anti-Passback
    - Lunch Break Lockout
    - Crowd Control Limit

Door Open Schedule:

1. Select "Door Open Schedule"
2. Set time periods when door remains unlocked
3. Click "Submit"

Bell Schedule (Requires ACTAtek External I/O Board):

1. Enable via Terminal Setup (Door Strike 2 Option)
2. Select "Bell Schedule"
3. Set schedule times
4. Click "Submit"

Terminal Clock:

1. Select "Terminal Clock"
2. Enable SNTP for automatic time sync
3. Or manually set date/time
4. Select correct Time Zone
5. Click "Set Time"

8.8 User Messages

Sending Personal Messages:

1. Select "User Messages"
2. Enter User ID
3. Enter message (max 25 characters per line, 5 lines)
4. Choose delivery method:
    - Display on LCD
    - Send to email
    - Send via SMS
5. Optional: Delete after display once
6. Click "Submit"

8.9 Advanced Features

Cloud Storage (Google Drive):

1. Create Google Spreadsheet
2. Import template eventlog file
3. Configure Cloud Storage Service
4. Enter Client ID, Client Secret, Spreadsheet Key
5. Authorize Google access
6. Submit and reboot

SMS Service:

1. Register with SMS gateway provider (e.g., SMS.SG)
2. Enter SMS User ID and Password
3. Configure User Messages with SMS notification
4. Set up Alert Log for SMS alerts

DDNS Configuration:

1. Register DDNS account (e.g., NoIP.com)
2. Enter Username, Password, Hostname
3. Click "Submit"
4. Access device via DDNS hostname

WiFi Configuration:

- **Normal Mode**: Connect to existing WiFi network
- **AP Mode**: Device becomes WiFi access point

4G Mobile Broadband:

1. Insert SIM card
2. Enter APN settings
3. Enable MBB Connection
4. Click "Submit"

---

9. Reports and Monitoring

9.1 Attendance Report

Features:

- Shows IN/OUT times (up to 10 sets per day)
- Calculates total working hours
- Filters by Name, User ID, Department, or Date Range

Generating Report:

1. Select "Attendance Report"
2. Choose search criteria
3. Select date range
4. Click "Search"
5. Export to CSV/TXT

9.2 Daily Report

Features:

- Shows First IN and Last OUT times
- Displays current status (Inside/Outside)
- Useful for payroll integration

Generating Report:

1. Select "Daily Report"
2. Choose search criteria
3. Select date range
4. Click "Search"
5. Export to CSV/TXT

9.3 Event Log

Viewing Event Logs:

1. Select "View Event Log"
2. Filter by: User Name, ID, Department, Event, or Date
3. Review details:
    - User ID and Name
    - Date and Time
    - Event Type
    - Terminal
    - Capture Image (if enabled)
    - Remark (authentication method)

Deleting Event Logs:

1. Use drop-down menu at bottom
2. Select timeframe (this week, last week, this month, last month)
3. Confirm deletion

Adding Manual Event Log:

1. Select "Add Event Log"
2. Enter Employee ID
3. Enter Date/Time (YYYY/MM/DD, HH:MM:SS)
4. Select Event and Terminal
5. Add remark (optional)
6. Click "Add"

9.4 Downloading Reports

1. Select "Download Report"
2. Choose filter criteria
3. Select format (CSV or TXT)
4. Click "Download"

---

10. Troubleshooting

10.1 Common Error Messages

"Bad Quality"

- **Cause**: Poor fingerprint image due to pressure, placement, or finger condition
- **Solution**: Re-enroll finger following best practices; clean sensor

"User Exist"

- **Cause**: Attempting to add duplicate User ID
- **Solution**: Use unique ID or choose to overwrite existing user

"No User Record"

- **Cause**: Invalid ID, password, fingerprint, or smart card
- **Solution**: Verify credentials; re-enroll if necessary

"Unauthorized"

- **Cause**: User accessing outside permitted time or accessing restricted terminal
- **Solution**: Check Access Group settings; verify user's access rights

"Anti-pass back Violation"

- **Cause**: Attempting IN-IN or OUT-OUT sequence
- **Solution**: Follow proper IN-OUT-IN-OUT sequence

"Reject Repeated Login"

- **Cause**: Same trigger used within reject duration
- **Solution**: Wait for duration to expire or use different trigger

"Exceeded Occupancy Limit"

- **Cause**: Crowd control limit reached
- **Solution**: Wait for OUT event to free capacity

10.2 Fingerprint Issues

High Rejection Rate:

- Clean sensor with alcohol or contact cleaner
- Re-enroll fingerprint using proper technique
- Lower security level (Terminal Settings > FP Quality)

- Use different finger
- Check for dry/wet finger condition

Auto-Match Too Slow:

- Reduce number of Auto-Match enabled users
- Use ID + Fingerprint instead
- Increase fingerprint security level

10.3 Network Issues

Cannot Access Web Interface:

- Verify device IP address (press Enter 6 times on device)
- Check network cable connection
- Verify PC and device are on same subnet
- Disable PC firewall temporarily
- Ping device IP address

DHCP Not Working:

- Verify DHCP server is operational
- Check network cable
- Reboot device
- Set static IP temporarily

10.4 Door Strike Issues

Door Not Opening:

- Check door strike wiring
- Verify power supply to door strike
- Test "Unlock Door" from Terminal Settings
- Check Access Rights configuration
- Verify diode installation (prevent EMI damage)

Door Opens But Stays Open:

- Check Relay Delay setting
- Verify door sensor connection
- Check Terminal Setup > Door Strike Options

10.5 Maintenance

Regular Cleaning:

- Clean fingerprint sensor weekly with alcohol and soft cloth
- Clean LCD screen with microfiber cloth
- Remove dust from camera lens (if applicable)

⚠ **Do NOT**:

- Use sharp objects on sensor
- Use abrasive cleaners
- Spray liquid directly on device

Backup Recommendations:

- Backup system data monthly
- Export event logs before clearing
- Keep backup of Access Group configurations

10.6 System Recovery

Restoring Backup:

1. Select "Restore System Data"
2. Click "Browse"
3. Select backup file
4. Click "Upload"
5. Wait for confirmation
6. Reboot device

Factory Reset:

1. Access Admin Menu or Web Interface
2. Select "Reset" > "Factory Default"
3. Confirm reset
4. Device will reboot with default settings
5. Reconfigure network and users

Appendix A: Specifications

Hardware Specifications

- **Operating Temperature**: -20°C to 60°C
- **Flash Memory**: 4GB/8GB
- **Maximum Users**: 1,000 to 100,000 (model dependent)
- **Maximum Auto-Match Users**: Up to 20,000 (FLI), 50,000 (Facial)
- **Maximum Event Logs**: 10,000 to 1,000,000
- **Maximum Photos**: 3,500
- **Product Weight**: 432g
- **Dimensions**: 175 x 81 x 41 mm
- **Case Rating**: IP65 (dust and water resistant)
- **Power**: 12V DC / 2.25A
- **Network**: 1000BaseT Ethernet, WiFi (optional), 4G (optional)

Authentication Methods

- **Fingerprint**: 500 DPI optical sensor, FAR 0.0001%, FRR 0.01%
- **Facial Recognition**: AI-based, anti-spoofing support
- **Smart Card**: MiFare, EM, HID Proximity, HID iClass, CEPAS, Felica
- **PIN**: Alphanumeric password
- **QR Code**: Standard and Google Authenticator 2FA

Copyright © 2025 Jakin ID Limited. All rights reserved.

Appendix B: Contact Information

Technical Support

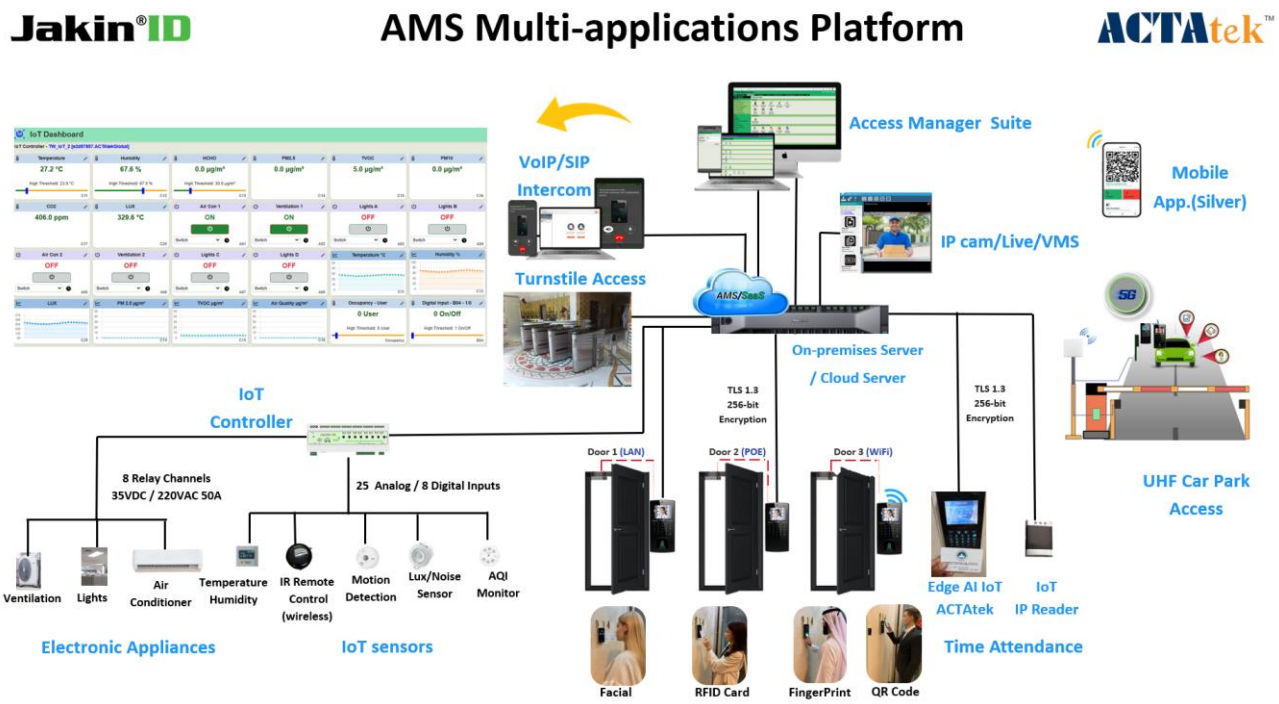
Website: www.jakinid.com
Email: support@actatek.com
Knowledge Base: http://www.jakinid.com/supportkb/

Regional Offices

Asia and Rest of World
Unit 913-914, 9/F., Worldwide Industrial Centre
43-47 Shan Mei Street, Fotan, Shatin, N.T., Hong Kong
Tel: +852 2319 1333

Americas
411-1221 Homer St, Vancouver BC V6B 1C5, Canada
Phone: +1 604 314 7628

Europe, Middle East & Africa
118 Pall Mall, London SW1Y 5EA, U.K.
Phone: +44 118 328 2982



Copyright © 2025 Jakin ID Limited. All rights reserved.