Jakin ID

ACTA4 Installation Manual (Version 1.7 , August 2025)

Table of Contents

---

1. Safety and Compliance

1.1 Important Safety Information

⚠ **WARNING**: This installation must be performed by a qualified and certified installer with full knowledge of local laws and regulations.

⚠ **ELECTRICAL HAZARD**: Ensure all power is disconnected before making any electrical connections.

⚠ **DO NOT**:

- Modify the power supply or DC jack
- Extend the DC cord of the power supply
- Share power supply with other devices or door locks
- Use power supply other than the provided 12V DC unit

1.2 Compliance Standards

- **CE** Certified
- **FCC** Compliant (Class A Digital Device)

- **SASO** Approved
- **IP65**-rated (dust and water ingress protection)
- **IK10**-rated casing

Minimum 10-year operational lifespan for the latest hardware, ensuring long-term ROI.

1.3 FCC Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits provide reasonable protection against harmful interference when operated in a commercial environment. Operation in a residential area may cause harmful interference, which the user must correct at their own expense.

---

2. Pre-Installation Requirements

2.1 Knowledge Requirements

Installers should be familiar with:

- Basic DC voltage and circuitry
- Basic wiring diagrams
- "Fail-Safe" and "Fail-Secure" concepts
- TCP/IP networking basics
- Local electrical codes and regulations

2.2 Tools Required

- Power drill with appropriate bits
- Screwdrivers (Phillips and flat-head)
- Wire stripper and crimper
- Multimeter for voltage testing
- Network cable tester
- Level
- Pencil or marker
- Measuring tape

2.3 Site Survey

Location Considerations:

1. **Door Proximity**: Install close to door for access control (user must reach door within 8-second timeout)
2. **Network Access**: Ensure network connectivity is available

3. **Power Supply**: Verify 12V DC power outlet or plan power routing
4. **Lighting**: Adequate lighting for facial recognition (if applicable)
5. **Environmental Protection**: Consider weather protection for outdoor installations
6. **Mounting Surface**: Ensure wall can support device weight (432g + mounting hardware)
7. **Height**: Typically 1.2m - 1.5m from ground for ergonomic access

Environmental Requirements:

- Operating Temperature: -20°C to 60°C
- Avoid direct sunlight on fingerprint sensor or camera
- Protect from rain/moisture (use weatherproof housing if needed)
- Minimize vibration

---

3. Package Contents

3.1 Standard Package

Verify the following items are included:

- ☐ ACTA4 Unit
- ☐ Mounting bracket
- ☐ 12V DC / 2.25A Switching Power Supply (Input: 100-240V AC, 50/60Hz)
- ☐ Power cord (country-specific)
- ☐ Straight network cable (RJ-45)
- ☐ Quick Installation Guide
- ☐ Warranty Card
- ☐ Mounting screws and anchors

3.2 Optional Accessories (Sold Separately)

- External I/O Board
- Weatherproof housing
- FingerPrint Sensor Cover

---

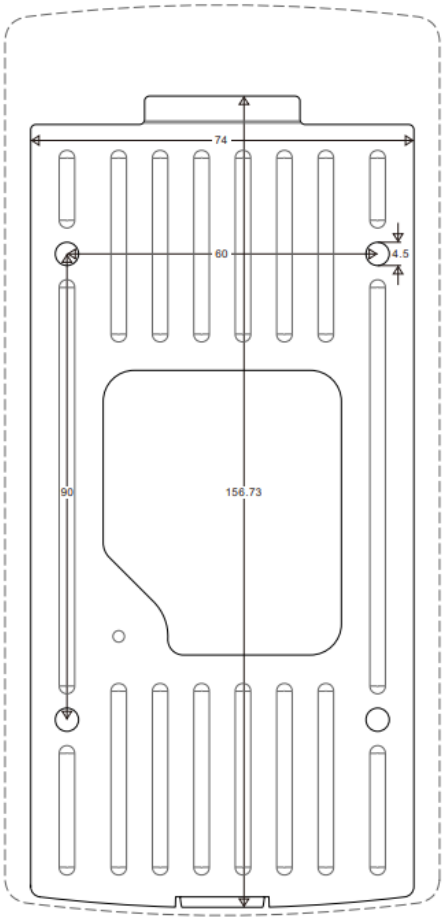
4. Physical Installation

4.1 Mounting Template

Use the provided 1:1 scale drilling template (print at actual size):

Drilling Template Specifications:

- Horizontal spacing: 74mm
- Vertical spacing: 156.73mm
- Top mounting holes: 60mm from top edge
- Bottom mounting holes: 90mm from top holes
- Hole diameter: 4.5mm



Unit: mm

4.2 Device Dimensions

ACTA4 Dimensions:

- Width: 81mm
- Height: 175mm
- Depth: 41mm (plus wall bracket thickness)

4.3 Installation Steps

Step 1: Prepare Mounting Location

1. Mark desired installation height (typically 1.4m from ground)
2. Use level to ensure mounting surface is plumb
3. Place drilling template on wall
4. Mark drill hole locations
5. Verify no obstructions behind wall (pipes, wires)

Step 2: Drill Mounting Holes

1. Drill holes at marked locations (4.5mm diameter)
2. For concrete/brick: use masonry bit and install anchors
3. For drywall: use appropriate wall anchors
4. For wood: drill pilot holes

Step 3: Install Mounting Bracket

1. Attach mounting bracket to wall using provided screws
2. Ensure bracket is level and secure
3. Test bracket strength before mounting device

Step 4: Route Cables

1. Plan cable routing for:
    - Network cable (Cat5e/Cat6)
    - Power cable
    - Door strike wiring
    - Door switch wiring (if applicable)
    - Other accessory connections
2. Use conduit or cable management as required by local codes
3. Leave sufficient slack for service access

Step 5: Mount Device

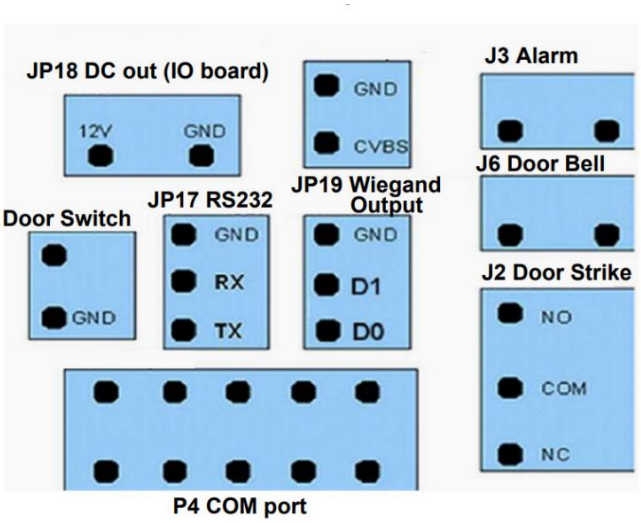
1. Connect required cables to device before mounting
2. Align device with mounting bracket
3. Secure device to bracket
4. Verify device is level and secure

---

5. Wiring and Connections

5.1 Back Panel Overview

Connection Ports (view from back of device):



- **J2**: Door Strike (NO, COM, NC terminals)
- **J3**: Alarm (Tamper Switch)
- **J4**: Door Switch
- **J6**: Door Bell
- **JP17**: RS-232 Debug Port
- **JP18**: 12V DC Output (for ACTAtek External I/O board)
- **JP19**: RS-485 / Wiegand Output (26-bit)
- **P4**: COM Port (reserved)
- **RJ45**: Network Connection
- **DC Jack**: 12V DC Power Input

5.2 Power Supply Connection

⚠ **CRITICAL POWER REQUIREMENTS**:

1. **Use ONLY the provided 12V DC / 2.25A power supply**
2. **ONE power supply per ACTA4 unit** (do NOT share with door locks or other devices)
3. **Do NOT substitute with other power supplies**
4. **Do NOT extend DC cable** (may cause voltage drop and instability)

Connection:

- Insert DC jack into power port on device
- Verify voltage before connecting: 12V DC
- Polarity: Center positive (+), outer negative (-)

5.3 Network Connection

Ethernet Connection:

1. Use Cat5e or Cat6 cable
2. Maximum recommended cable length: 100 meters
3. Connect to network switch or router (NOT directly to PC unless using crossover cable)
4. LED indicators:
    - Green: Link established
    - Amber: Activity

WiFi Connection (if WiFi module installed):

- Configure via device menu or web interface
- Supports IEEE 802.11 a/b/g/n/ac
- Both 2.4GHz and 5GHz frequencies

5.4 Door Strike Wiring

⚠ **IMPORTANT REQUIREMENTS**:

1. **ACTAtek supports 12V DC door strikes/maglocks ONLY**
2. **Maximum current: 1 Amp**
3. **Separate power supply required for door strike** (do NOT share with ACTAtek power)
4. **Diode REQUIRED for all DC strike installations** (prevents EMI damage)

Diode Selection:

- **P/N 1N4004**: For door strikes rated 12V DC / 1A

- **P/N 6A1**: For door strikes with current 1-6A (requires external relay)

Diode Installation:

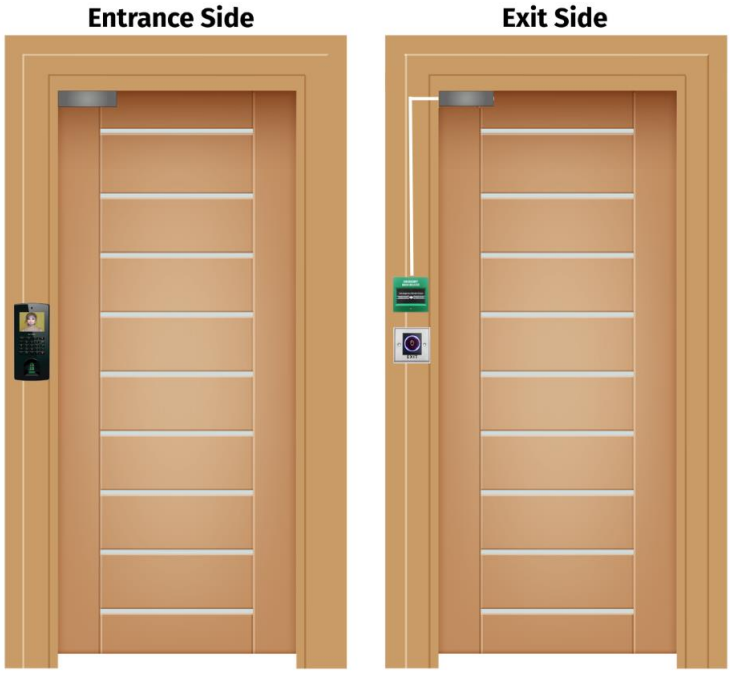
- **Cathode** (marked end): Connect to POSITIVE (+) DC voltage
- **Anode**: Connect to NEGATIVE (-) DC voltage

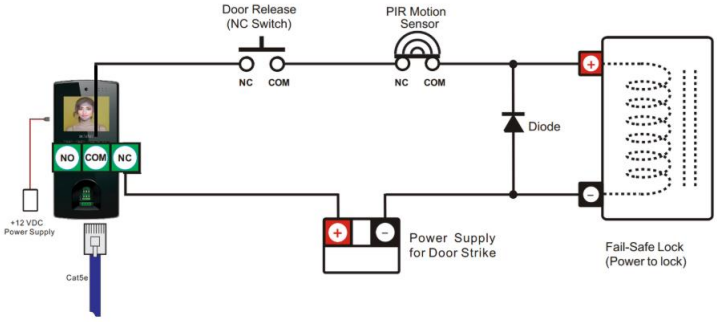
5.4.1 Fail-Safe Lock (Single Unit)

Fail-Safe Definition: Lock is powered when secured; loses power when unlocked (door opens during power failure)

Typical Application: Electromagnetic lock (maglock)

Wiring Diagram:





Connection Steps:

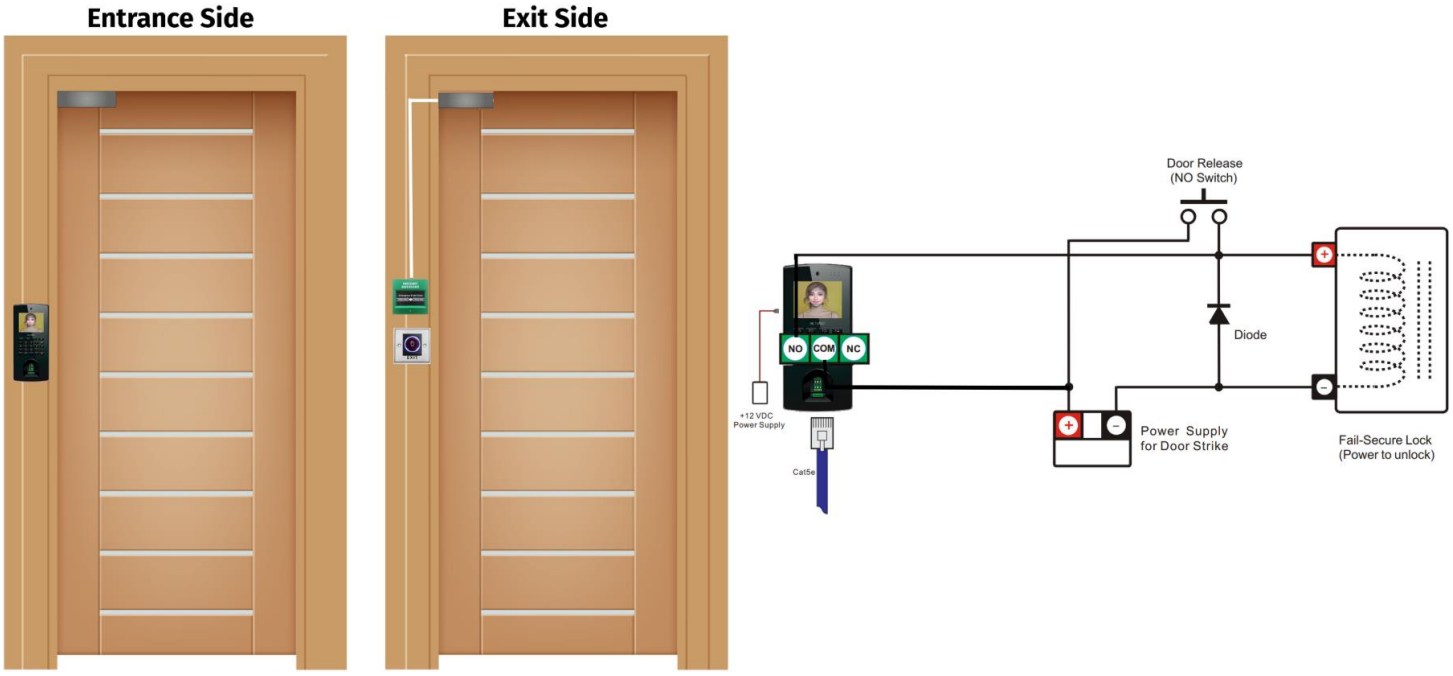
1. Connect ACTA4 power supply (12V DC) to device DC jack
2. Connect separate lock power supply (+) to diode CATHODE
3. Connect diode ANODE to lock (+)
4. Connect lock (-) to power supply (-)
5. Connect J2 NO terminal to lock (+) [before diode]
6. Connect J2 COM terminal to lock (-)
7. Test operation

5.4.2 Fail-Secure Lock (Single Unit)

Fail-Secure Definition: Lock is unpowered when secured; requires power to unlock (door stays locked during power failure)

Typical Application: Electric strike

Wiring Diagram:

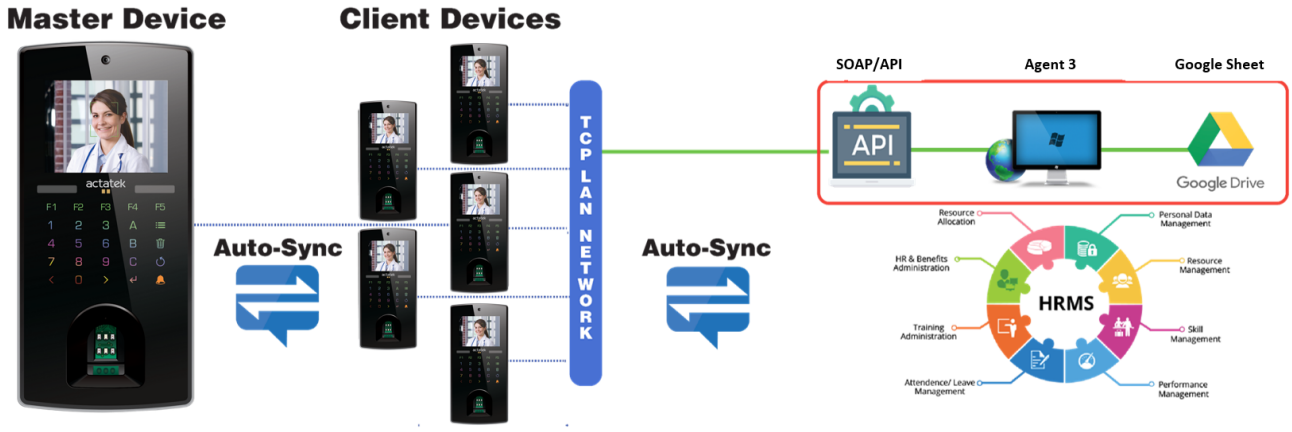


Connection Steps:

1. Connect ACTA4 power supply (12V DC) to device DC jack
2. Connect separate lock power supply (+) to diode CATHODE
3. Connect diode ANODE to lock (+)
4. Connect lock (-) to power supply (-)
5. Connect J2 NC terminal to lock (+) [before diode]
6. Connect J2 COM terminal to lock (-)
7. Test operation

5.4.3 Multiple Units (Master/Client)

For installations with 2 or more ACTA4 units controlling the doors:



Note: All ACTAtek devices need to have the same Firmware version.

For installations with up to 10 units, designate one device as the "Master" terminal and the others as "Client" terminals. The Master and Client devices will automatically synchronize data, including user fingerprint data, event logs, and more. Integration with third-party applications can be achieved using the SOAP API, Agent, or Google Drive API.

Configuration:

1. Connect both units to same network
2. Configure one as Master, others as Client
3. Each unit connects to same door strike (parallel connection)
4. Use fail-safe lock for multi-unit installations
5. Synchronize user database via Master/Client function

5.5 Door Switch/Sensor Connection

Purpose:

- Request to Exit (REX) button for inside access
- Door position sensor for monitoring

Connection:

J4 Terminal:

- Connect door switch/sensor between two terminals
- Normally Closed (NC) or Normally Open (NO) configurable in software
- Low voltage signal (do NOT connect high voltage)

Recommended Door Switch Types:

- Push button (momentary, normally open)
- Break glass emergency exit
- PIR motion sensor
- Door contact sensor (NO magnetic, configured as Door Sensor from the device's web ui)

Configuration:

1. Physical connection to J4
2. Configure in web interface: Terminal Setup → Door SW Mode
3. Options:
    - Door Switch (exit button)
    - Door Sense (position sensor)
    - Door Event OUT/IN (automatic trigger)

5.6 Door Bell Connection

J6 Terminal:

Purpose: Trigger external bell/buzzer when doorbell button pressed

Connection:

1. Connect bell/buzzer between J6 COM and NO terminals
2. Use 12V DC bell/buzzer rated up to 1A maximum
3. Connect separate power supply for bell (do NOT share)
4. Optional: Add diode for inductive load protection

Alternative Use:

- SIP Intercom initiation (if intercom module installed)

5.7 Alarm Connection

J3 Terminal:

Purpose: Tamper detection - triggers when device case opened

Connection:

1. Connect external alarm system to J3 terminals (A and B)
2. Terminals short circuit when case opened
3. Connect to alarm panel input zone

4. No external power required (dry contact)

5.8 External I/O Board Connection

JP18 Terminal:

Purpose: Expand I/O capabilities for advanced installations

External I/O Board Features:

- Additional door strike (Strike 2)
- Additional door sensors (Sensor 2)
- Wiegand input (from external reader)
- Wiegand output (to external controller)
- RS-485 communication

Connection:

1. Connect I/O board to JP18 using provided cable
2. Secure I/O board in accessible location
3. Power I/O board from ACTA4 via JP18 (DC OUT)
4. Configure in web interface: Terminal Setup → External Devices

I/O Board Applications:

- Dual door control (entry/exit)
- Integration with third-party access control panels
- Sliding door controller integration (via external relay)
- Turnstile or gate control

5.9 Wiegand Output

JP19 Terminal (26-bit Wiegand standard):

Purpose: Output authentication data to third-party access control systems

Connection:

1. D0 → Wiegand Data 0
2. D1 → Wiegand Data 1
3. GND → Common Ground
4. Maximum cable length: 500 feet (152 meters)
5. Use shielded twisted pair cable

Configuration:

- Enable in Terminal Setup → Wiegand Configuration
- Select output format (standard 26-bit or custom)
- Can share JP19 with RS-485 (not simultaneously)

5.10 RS-232 / RS-485

JP17 (RS-232): Reserved for debugging

JP19 (RS-485): External device communication

Applications:

- External display boards
- Integration with building management systems
- Custom peripheral devices

---

6. Network Configuration

6.1 Initial Network Setup

Default Network Settings:

- **IP Address**: 192.168.1.100
- **Subnet Mask**: 255.255.255.0
- **Gateway**: 192.168.1.1
- **DHCP**: Disabled

6.2 Connecting to Corporate Network

Option 1: Using DHCP (Automatic IP)

1. Press **Menu** button on device
2. Enter Admin ID: **A999**
3. Press **Enter**
4. Enter Password: **1**
5. Press **Enter**
6. Select **IP Setting** icon
7. Navigate to **DHCP** option
8. Press **Enter** to enable (DHCP ON),and Press **Enter** to disable (DHCP OFF)
9. Return to Clock Screen: Press Enter six times consecutively on the standby screen to view the assigned IP.

Option 2: Static IP Configuration

1. Consult network administrator for available IP address
2. Obtain: IP Address, Subnet Mask, Gateway, DNS
3. Access Admin Menu (Menu → A999 → 1)
4. Select **IP Setting** icon
5. Configure each parameter:
    - IP Address
    - Subnet Mask
    - Gateway
    - DNS IP
6. Confirm each entry with **Enter**

6.3 Verifying Network Connectivity

From Device:

1. Press **Enter** 6 times consecutively on the standby screen
2. View Device Info page showing current IP
3. Verify network icon shows connection

From PC:

1. Open Command Prompt / Terminal
2. Type: ping [device IP address]
3. Verify responses received
4. Open web browser
5. Navigate to: http://[device IP address]
6. Verify web interface loads

6.4 Network Security Recommendations

1. **Change default credentials immediately**
2. **Use HTTPS (secure)** when accessing web interface
3. **Restrict IP access** if device exposed to internet
4. **Configure firewall** to allow only necessary ports:
    - Port 80: HTTP (web interface)
    - Port 443: HTTPS (secure web interface)
    - Custom port if configured
5. **Enable DDNS** for remote access (see Advanced Configurations)
6. **Regular firmware updates** for security patches

7. Initial Setup

7.1 Power-On Sequence

1. Verify all wiring connections complete and correct
2. Verify door strike has separate power supply
3. Connect network cable
4. Connect power supply to device
5. Observe boot sequence:
    - Logo display
    - Initialization messages
    - Standby screen appears (approx. 30-45 seconds)

7.2 First Login

Via Device Console:

1. Press **Menu** button
2. Enter: **A999**
3. Press **Enter**
4. Enter: **1**
5. Press **Enter**
6. Admin Menu appears

Via Web Interface:

1. Open web browser
2. Navigate to device IP (default: 192.168.1.100)
3. Click **Secure** for encrypted connection
4. Accept security certificate
5. Enter Admin ID: **A999**
6. Enter Password: **1**
7. Select login level: **Super Administrator**
8. Click **OK**

7.3 Essential Configuration Steps

Step 1: Change Admin Credentials

1. Access web interface
2. Go to **View User List**
3. Click on **A999**
4. Change User ID and Password

5. Click **Modify**
6. **Document new credentials securely**

Step 2: Set Date and Time

1. Access **Terminal Clock** (web) or **Date & Time** (device)
2. Either:
    - Enable SNTP for automatic time sync
    - Manually set date and time
3. Select correct **Time Zone**
4. Click **Set Time** or press **Enter**

Step 3: Configure Terminal Settings

1. Access **Terminal Setup**
2. Set:
    - Terminal Description
    - Language
    - Console Display Timeout
    - Fingerprint Security Level
    - Door Strike options
3. Click **Submit**

Step 4: Test Door Strike

1. Access **Terminal Settings** (device) or **Remote Door Open** (web)
2. Select **Unlock Door**
3. Verify door lock releases
4. Verify lock re-engages after timeout (default 8 seconds)
5. Adjust **Relay Delay** if needed

Step 5: Create Test User

1. Access **Add New User**
2. Create user with ID: **TEST001**
3. Enroll fingerprint or assign smart card
4. Test authentication
5. Verify event log generated

7.4 Warranty Registration

1. Complete Warranty Form at: http://warranty.actatek.com/
2. Keep copy for your records

---

8. Testing and Verification

8.1 Pre-Operational Checklist

- ☐ Power supply connected and voltage verified (12V DC)
- ☐ Network connection established (link LED active)
- ☐ Device accessible via web browser
- ☐ Admin credentials changed from default
- ☐ Date and time configured correctly
- ☐ Door strike connected with separate power supply
- ☐ Diode installed on door strike wiring
- ☐ Door switch connected (if applicable)
- ☐ Test user enrolled and authenticated successfully
- ☐ Event logs recording properly
- ☐ Door strike operates correctly (lock/unlock)
- ☐ Relay delay appropriate for door type
- ☐ All cable connections secure

8.2 Functional Testing

Authentication Tests:

1. **Fingerprint Test** (if applicable):
    - Enroll test finger (3 samples)
    - Test 1:1 authentication (ID + FP)
    - Test 1:N authentication (Auto-Match)
    - Verify LCD feedback
    - Check event log entry
    - Confirm door unlocks
2. **Smart Card Test** (if applicable):
    - Enroll test card
    - Present card to reader
    - Verify read distance (typically 3-5cm)
    - Check event log entry
    - Confirm door unlocks
3. **PIN Test**:
    - Set password for test user
    - Enter ID + Password
    - Verify authentication

    - Check event log entry
    - Confirm door unlocks
4. **Facial Recognition Test** (if applicable):
    - Enroll test face
    - Test recognition distance
    - Verify lighting adequate
    - Check event log entry
    - Confirm door unlocks

Access Control Tests:

1. **Door Strike Test**:
    - Authenticate valid user
    - Verify door unlocks
    - Time unlock duration
    - Verify re-lock after timeout
    - Test manual unlock (Remote Door Open)
2. **Exit Button Test** (if connected):
    - Press exit button from inside
    - Verify door unlocks
    - Verify event log entry (if logged)
    - Confirm re-lock
3. **Door Sensor Test** (if connected):
    - Open door after authentication
    - Close door
    - Verify status in web interface
    - Test forced door alarm (if configured)

Schedule Tests:

1. **Access Group Test**:
    - Create restricted access group
    - Assign user to group
    - Set limited time range
    - Test during allowed time (should grant access)
    - Test outside allowed time (should deny)
2. **Door Open Schedule Test**:
    - Configure door open schedule
    - Verify door unlocked during schedule
    - Verify normal operation outside schedule
3. **Trigger Test**:
    - Change trigger (F1, F2, F3, F4)
    - Authenticate
    - Verify correct trigger in event log

Network Tests:

1. **Web Access Test**:
    - Access from multiple browsers
    - Test from different computers on network
    - Verify HTTPS connection if required
    - Test concurrent access
2. **Remote Management Test**:
    - Add user via web interface
    - Modify user settings
    - Download event logs
    - Capture remote fingerprint

---

8. Advanced Configurations for Small-Scale Installations

8.1 Master/Client Setup (Standalone Mode)

Purpose: Synchronize up to 10 units without central server

Configuration:

1. **Master Device**:
    - Access web interface
    - Go to **Master/Client Setup**
    - Select **Master** mode
    - Click **Submit**
2. **Client Devices**:
    - Access web interface
    - Go to **Master/Client Setup**
    - Select **Client** mode
    - Enter **Master IP** address
    - Click **Submit**
    - Device will reboot and sync
3. **Verification**:
    - Check Client device status shows "Registered"
    - Verify users sync across all devices
    - Test authentication on all devices

8.2 WiFi Configuration

Normal Mode (Connect to existing WiFi):

1. Access web interface
2. Go to **WiFi Setup**
3. Select WiFi Mode: **Normal**
4. Enter SSID
5. Enter Password
6. Click **Submit**
7. Check Device Info for WiFi IP address

AP Mode (Device as Access Point):

1. Access device console: Admin Login
2. Go to **IP Settings**
3. Select **Enable WiFi AP**
4. Press **Enter**
5. Connect mobile device to SSID: **jakinid4_[serial]**
6. Password: **jakinid4**
7. Access device at: **192.168.4.1**

QR Code WiFi Setup:

1. Generate WiFi QR code at: https://qifi.org/
2. Access device console: Admin Login
3. Go to **IP Settings** → **Scan WIFI QR Code**
4. Scan generated QR code
5. Device auto-configures WiFi

8.3 4G Mobile Broadband

Requirements: 4G module installed, SIM card

Setup:

1. Power off device
2. Remove back case
3. Insert SIM card
4. Reassemble and power on
5. Access web interface
6. Go to **Mobile Broadband**
7. Enter APN (from telecom provider)
8. Leave Username/Password blank (usually)

9. Check **Enable MBB Connection**
10. Click **Submit,** and verify connection status shows "**Connected**"

8.4 External I/O Board Installation

Purpose: Add advanced I/O capabilities

Installation:

1. Mount I/O board near ACTA4 device
2. Connect I/O board to JP18 on ACTA4
3. Power on system
4. Access web interface
5. Go to **External Devices**
6. Verify I/O board detected
7. Configure additional door strikes, sensors, etc.

Applications:

- Second door strike control
- Wiegand output to the 3rd party access controller
- Additional door sensors

8.5 Integration with Third-Party Systems

Wiegand Output to Access Control Panel:

1. Connect JP19 (D0, D1, GND) to panel Wiegand input
2. Access **Terminal Setup**
3. Enable **Wiegand Configuration**
4. Select format (standard 26-bit)
5. Configure ACTA4 as Wiegand reader in panel
6. Test authentication - panel should receive credential

Emergency Mode (with external controller):

1. Connect ACTA4 to third-party controller via I/O board
2. Access **Terminal Setup**
3. Set Door Strike 1 Option: **Emergency Mode**
4. Assign users to **Emergency** department
5. During normal operation, controller controls door
6. If controller fails, Emergency users can unlock via ACTA4

8.6 Video/IP Camera Integration

Built-in Camera (C model):

- Automatic photo capture on authentication
- View in event logs
- Remote door open with live view

RTP mode:

- **RTSP Push Mode** Streams video to an external RTSP server (e.g., MediaMTX).
  Example: rtsp://192.168.1.111:8554/stream
- **Video Camera Mode** View live video directly from the device settings page.
- **RTSP Server Mode** Device acts as an RTSP server; access via VLC or other clients.
  Example: rtsp://192.168.1.108:8554/cam

9.7 DDNS for Remote Access

Purpose: Access device from internet via domain name

Setup:

1. Register DDNS account (e.g., NoIP.com, DynDNS)
2. Obtain: Username, Password, Hostname
3. Configure router port forwarding:
   - External port 80 → Device IP port 80 (HTTP)
   - External port 443 → Device IP port 443 (HTTPS)
4. Access device web interface
5. Go to **DDNS**
6. Enter credentials and hostname
7. Click **Submit**
8. Access device via: http://[hostname]

Security Recommendations:

- Use HTTPS only
- Change default web port
- Restrict IP access if possible
- Use strong passwords
- Enable alert logs

---

10. Troubleshooting Installation Issues

10.1 Device Not Powering On

Symptoms: No display, no lights

Checks:

1. Verify power supply connected
2. Test power supply output: 12V DC
3. Check DC jack connection
4. Try different power outlet
5. Verify power supply is correct model (12V DC / 2.25A)
6. Check for blown fuse in power supply

Resolution:

- Replace power supply if faulty
- Check for short circuit in wiring
- Contact technical support if device damaged

10.2 Network Connection Issues

Symptoms: Cannot access web interface, no network link light

Checks:

1. Verify network cable connected firmly
2. Test cable with cable tester
3. Check network switch/router port operational
4. Verify switch shows link light
5. Try different network port
6. Try different cable
7. Check IP address (press Enter 6x on device)

Resolution:

- Replace faulty cable
- Configure correct IP settings
- Verify DHCP server operational (if using DHCP)
- Check firewall rules on PC
- Ping device from PC: ping [device IP]

10.3 Door Strike Not Operating

Symptoms: Authentication successful but door doesn't unlock

Checks:

1. Verify door strike has separate power supply
2. Test door strike directly (bypass ACTA4)
3. Check door strike voltage: 12V DC
4. Verify current draw <1A
5. Check J2 wiring connections
6. Verify diode installed correctly
7. Test relay with multimeter (continuity)
8. Check Door Strike Option in Terminal Setup

Resolution:

- Reconnect wiring
- Replace diode if failed
- Verify fail-safe vs fail-secure wiring
- Check if external relay needed (>1A strike)
- Test with "Unlock Door" function
- Adjust Relay Delay

10.4 Fingerprint Sensor Issues

Symptoms: Sensor not scanning, poor image quality

Checks:

1. Clean sensor with alcohol and soft cloth
2. Verify sensor not scratched/damaged
3. Check for moisture on sensor
4. Test with different fingers
5. Check lighting (not required for sensor, but helps user)

Resolution:

- Clean sensor properly
- Ensure proper finger placement (core centered)
- Lower security level temporarily
- Re-enroll problematic users
- Contact support if sensor hardware failure

10.5 Smart Card Reader Issues

Symptoms: Card not detected, inconsistent reads

Checks:

1. Verify card type compatible (MiFare, HID, etc.)
2. Check card not damaged
3. Test multiple cards
4. Verify reading distance (3-5cm)
5. Check for interference (metal, magnets)

Resolution:

- Move card slowly across reading area
- Re-register card
- Verify card type in Terminal Setup
- Enable parity error detection (HID Prox)
- Test with known good card

10.6 Web Interface Access Issues

Symptoms: Cannot load web page, timeout errors

Checks:

1. Verify PC and device on same network/subnet
2. Ping device IP address
3. Check PC firewall settings
4. Try different browser
5. Clear browser cache
6. Verify correct IP address
7. Check web port setting (default 80)

Resolution:

- Temporarily disable PC firewall
- Configure correct network settings
- Use device IP directly (not hostname)
- Try HTTPS: https://[device IP]
- Reset web port to default (80)
- Access from different PC

10.7 WiFi Connection Problems

Symptoms: WiFi not connecting, unstable connection

Checks:

1. Verify WiFi module installed
2. Check SSID and password correct
3. Verify WiFi network operational
4. Check signal strength (distance from access point)
5. Verify WiFi security type compatible
6. Check for interference

Resolution:

- Move device closer to access point
- Use 2.4GHz instead of 5GHz
- Verify WiFi credentials
- Try AP mode to verify module works
- Check Device Info for WiFi status
- Reboot device

10.8 Time/Clock Issues

Symptoms: Incorrect time display, time drifts

Checks:

1. Verify Time Zone setting correct
2. Check SNTP enabled and server accessible
3. Verify network connectivity for SNTP
4. Check manual time setting
5. Verify PC time correct (for auto-adjust)

Resolution:

- Enable SNTP for automatic sync
- Configure correct SNTP server
- Manually set time if SNTP unavailable
- Set correct Time Zone
- Device syncs every 3 hours with SNTP

10.9 Event Log Not Recording

Symptoms: No logs appearing, logs not updating

Checks:

1. Verify event logging enabled
2. Check log size not exceeded
3. Verify "Log Event" setting
4. Check memory status
5. Test with known authentication

Resolution:

- Enable logging in Authentication/Log Setup
- Clear old logs if memory full
- Increase log size if needed
- Backup and clear event log
- Verify user activated

10.10 Installation Checklist Issues

If experiencing multiple issues, verify basic installation:

Power:

- ☐ Correct power supply (12V DC / 2.25A)
- ☐ Single device per power supply
- ☐ Stable power (no voltage drops)
- ☐ Proper grounding

Wiring:

- ☐ All connections secure
- ☐ Correct polarity observed
- ☐ Diode installed on door strike
- ☐ Separate power for door strike
- ☐ No shared power supplies
- ☐ Proper wire gauge for distances

Network:

- [ ] Correct IP configuration
- [ ] Network cable tested
- [ ] Switch port operational
- [ ] Firewall configured properly
- [ ] Can ping device

Configuration:

- [ ] Admin credentials changed
- [ ] Date/time set correctly
- [ ] Terminal settings configured
- [ ] Door strike options correct
- [ ] Test user created and works

Appendix A: Pin-Out Reference

J2 - Door Strike

Terminal	Function	Voltage	Current Rating
NO	Normally Open	30V DC	3A max
COM	Common	-	3A max
NC	Normally Closed	30V DC	3A max

J3 - Alarm (Tamper)

Terminal	Function	Type
A	Tamper Switch	Dry Contact
B	Tamper Switch	Dry Contact

J4 - Door Switch

Terminal	Function	Type
A	Door Switch	Low Voltage Input
B (GND)	Ground	Common

J6 - Door Bell

Terminal	Function	Voltage	Current
COM	Common	-	1A max
NO	Normally Open	12V DC	1A max

JP19 - Wiegand Output / RS-485

Pin	Wiegand	RS-485
D0	Data 0	-
D1	Data 1	-
A	-	RS-485 A
B	-	RS-485 B
GND	Ground	Ground

Appendix B: Technical Specifications

Electrical

- **Power Input**: 12V DC / 2.25A
- **Power Consumption**: Max 27W
- **Door Strike Output**: 30V DC / 3A max (internal relay)
- **Door Bell Output**: 12V DC / 1A max

Environmental

- **Operating Temperature**: -20°C to +60°C (-4°F to 140°F)
- **Storage Temperature**: -40°C to +70°C
- **Humidity**: 10% to 90% non-condensing
- **Ingress Protection**: IP65
- **Casing :** IK-10 rated

Physical

- **Dimensions**: 175mm (H) x 81mm (W) x 41mm (D)
- **Weight**: 432g (device only)
- **Mounting**: Wall mount with bracket

Network

- **Ethernet**: 10/100/1000 BaseT (RJ-45)
- **WiFi** (optional): IEEE 802.11 a/b/g/n/ac, 2.4GHz/5GHz
- **4G** (optional): 4G LTE mobile broadband
- **Protocols**: TCP/IP, HTTP, HTTPS, SNMP, SOAP

Capacity

- **Users**: 1,000 to 100,000 (model dependent)
- **Fingerprint Auto-Match**: Up to 20,000
- **Facial Auto-Match**: Up to 50,000
- **Event Logs**: 10,000 to 1,000,000 (configurable)
- **Photos**: Up to 3,500

Appendix C: Regulatory Compliance

Safety Standards

- CE Certified
- FCC Part 15 Class A
- SASO Approved
- IP65 Rated
- IK10 Rated

Electromagnetic Compatibility

- Complies with FCC Part 15
- Complies with CE EMC directives
- Recommended use of shielded cables for long runs

Disposal and Recycling

- Dispose according to local e-waste regulations
- Contains electronic components - do not dispose in regular trash
- Recycle through authorized electronics recycling facility

Appendix D: Maintenance Schedule

Daily

- Visual inspection of device operation
- Check for error messages

Weekly

- Clean fingerprint sensor
- Clean LCD screen
- Check event log for anomalies

Monthly

- Backup system data
- Export and archive event logs
- Check door strike operation

- Verify network connectivity
- Check power supply condition

Quarterly

- Full system test (all authentication methods)
- Test backup/restore procedure
- Review access groups and permissions
- Audit user list (remove inactive users)

Annually

- Check firmware updates
- Replace batteries (if applicable)
- Inspect all wiring connections
- Test emergency procedures
- Review system security settings
- Document changes

Appendix E: Quick Reference

Default Settings

Setting	Default Value
IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
Admin ID	A999
Password	1
Web Port	80
HTTPS Port	443
DHCP	Disabled
Door Unlock Time	8 seconds (adjectable)

Common Key Sequences

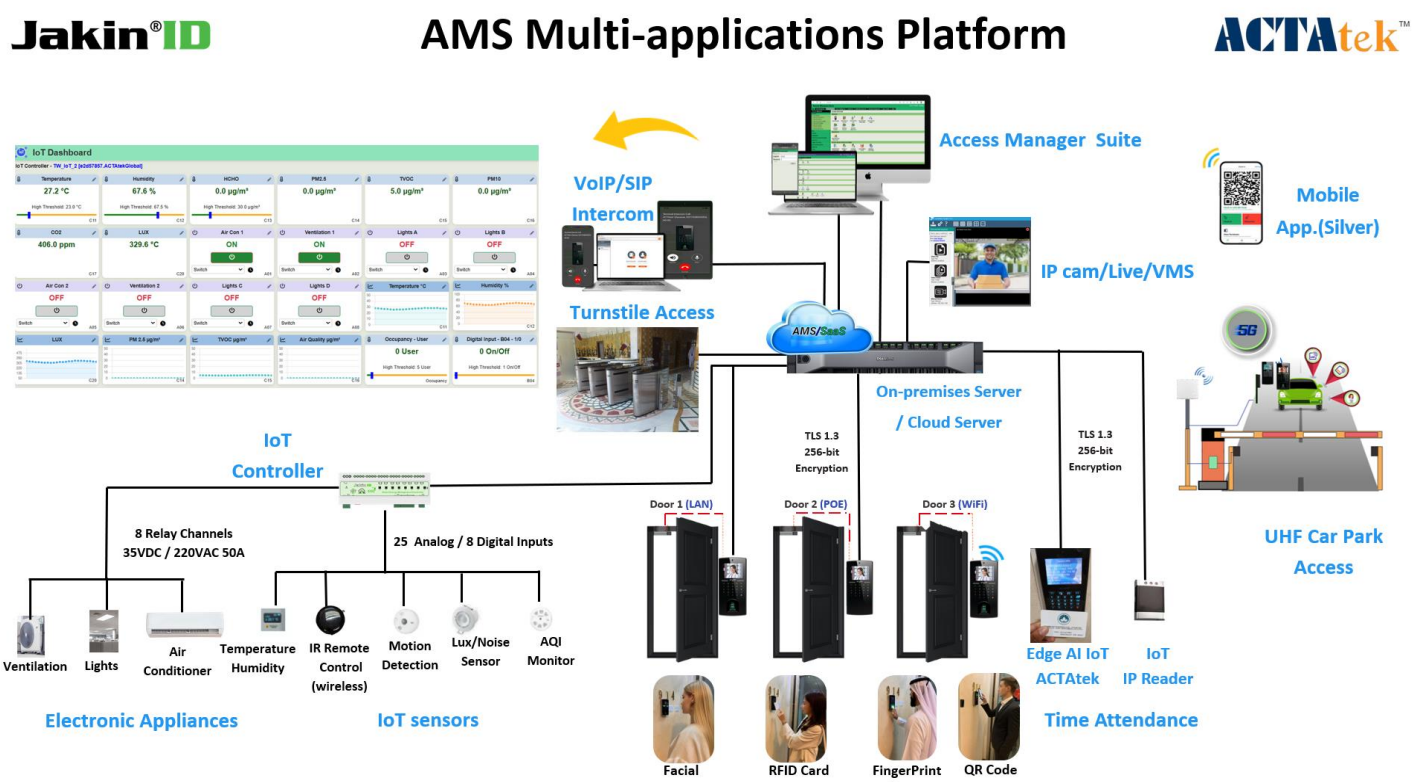
Action	Key Sequence
View Device Info	Press Enter 6 times
Admin Login	Menu → A999 → 1
Change Trigger	F1/F2/F3/F4 before auth
Doorbell	Bell icon (top right)

Support Contacts

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

Phone Support:

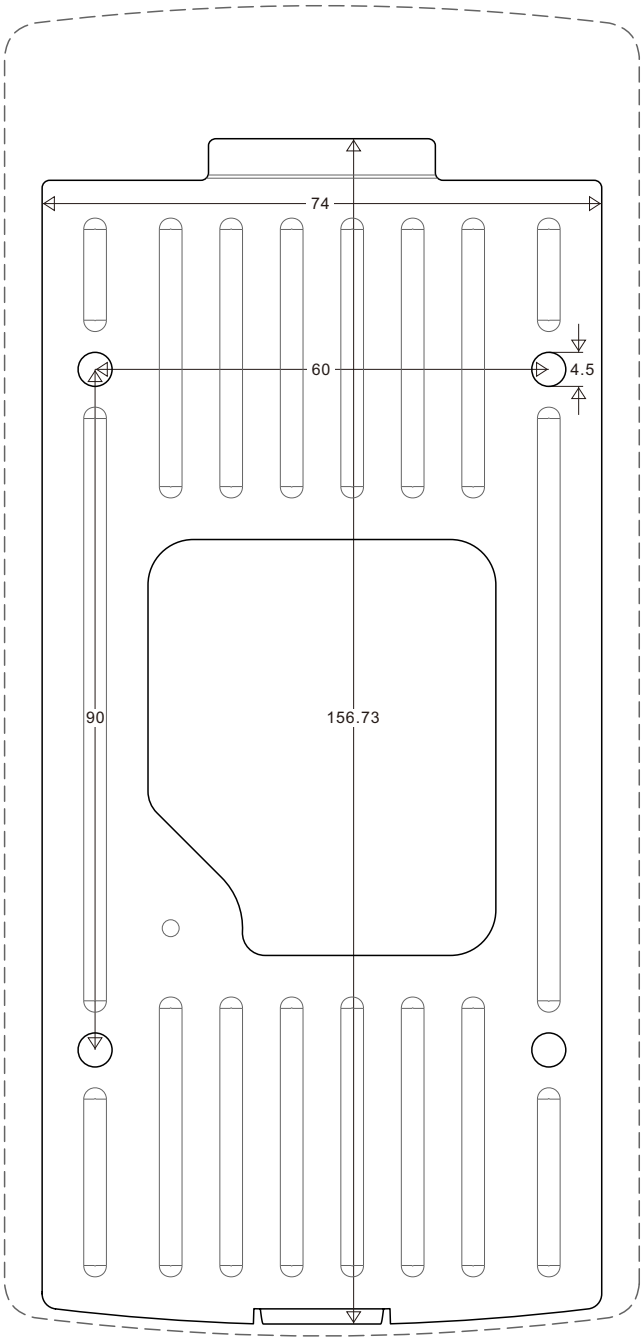
- Asia: +852 2319 1333
- Americas: +1 604 314 7628
- Europe: +44 118 328 2982



ACTAtek 4
1:1 Scale Drilling Template

Printing Instruction
1. Use Adobe Acrobat Reader
2. Open the file > Print
3. Select Actual size
4. Click Print

DO NOT USE CUSTOM SCALE



Unit: mm