



Biometric Access Control System Manual Guide

For General Biometric Access Control Systems

1. Introduction

This manual provides comprehensive guidance for installing, configuring, operating, and maintaining biometric access control systems.

It is intended for installation technicians, system administrators, and security managers responsible for ensuring secure, efficient, and compliant operations.

2. System Overview

Biometric access control systems use unique physiological or behavioral characteristics—such as fingerprints, facial recognition, or iris patterns—to authenticate individuals.

The system ensures that only authorized personnel gain access to secured areas.

3. System Components and Specifications

- **Biometric Readers:** Fingerprint, face, or iris scanners used for identification.
- **Control Panel / Access Controller:** Central unit that processes authentication signals and triggers door mechanisms.
- **Software Management Console:** Used for user enrollment, permissions, and reporting.
- **Locks and Door Hardware:** Magnetic locks, electric strikes, or turnstiles.
- **Power Supply & Backup:** 12V–24V DC with UPS backup.
- **Network Infrastructure:** Ethernet or RS-485 communication.



4. Installation Procedures

4.1 Pre-Installation Checklist

- Confirm system design and layout drawings.
- Verify power and network availability.
- Prepare mounting tools, cabling, and labeling materials.

4.2 Mounting Biometric Readers

1. Mount devices at user height (typically 1.4–1.6m above floor).
2. Avoid direct sunlight and moisture exposure.
3. Ensure proper alignment and secure installation.

4.3 Wiring and Connectivity

- Use shielded Cat6 cables for data lines.
- Connect power, door lock, exit button, and door sensor as per wiring diagram.
- Observe polarity and grounding best practices.

5. Hardware Configuration

1. Power on the access controller and connect via LAN
2. Assign device ID and IP address through configuration software.
3. Set time synchronization and communication parameters.
4. Test door relay and sensor functionality.

6. Software Setup and Integration

1. Install the biometric management software on a server or workstation.
2. Add devices to the system by IP or serial number.
3. Define access zones and door groups.
4. Integrate with Active Directory or HR database (optional).
5. Configure communication with attendance or alarm systems.

7. User Enrollment and Access Management

Enquires@aritofafrica.com, support@aritofafrica.com
www.aritofafrica.com



7.1 Enrollment Process

1. Launch the enrollment interface.
2. Register user details (name, ID, department).
3. Capture biometric data (fingerprint, palm, face, or iris).
4. Assign access levels, time schedules, and validity periods.

7.2 Access Rights Configuration

- Define access groups by department or role.
- Set time zones (e.g., work hours, weekends, restricted hours).
- Enable anti-passback and dual authentication features if available.

8. Operational Guidelines

- Ensure all users are properly enrolled and verified.
- Periodically update biometric templates to maintain accuracy.
- Monitor system status via the dashboard or event logs.
- Lock devices during maintenance to prevent unauthorized access.

9. Monitoring and Reporting

- Access real-time logs of entry/exit events.
- Generate attendance and access reports.
- Export data in CSV, PDF, or Excel formats.
- Set up automated email alerts for security breaches.

10. System Maintenance and Backup

- Perform regular backups of the system database.
- Update firmware and software versions as released.
- Clean biometric sensors periodically.
- Inspect cabling and hardware for wear or corrosion.



11. Troubleshooting Guide

Issue	Possible Cause	Corrective Action
Device not powering on	Faulty power supply or wiring	Check voltage, replace power adapter.
Fingerprint not recognized	Dirty sensor or incorrect template	Clean sensor and re-enroll user.
Door not unlocking	Relay misconfiguration or lock fault	Verify wiring and relay settings.
Software not connecting to device	IP conflict or firewall blocking	Assign static IP, update firewall rules.
Event logs missing	Database service stopped	Restart database service and check storage.

12. Safety and Compliance

- Follow all electrical and network installation codes.
- Ensure compliance with data protection regulations
- Use UPS for power continuity.
- Protect biometric data using encryption and access controls.

13. Best Practices and Recommendations

- Maintain a detailed configuration and change log.
- Train users on proper biometric usage and hygiene.
- Schedule preventive maintenance quarterly.
- Periodically audit user permissions and logs.
- Store backups securely offsite or on a dedicated NAS.