Frequently Asked Question

Fingerprint attendance device WL20

By : ESSL

❖ General Information

- **What is the ESSL WL20?**
  - It's a compact biometric attendance system with Wi-Fi connectivity, fingerprint recognition, and real-time data sync capabilities.
- **Who is it for?**
  - Ideal for offices, schools, warehouses, gyms, and retail chains that need efficient, wireless attendance tracking.

❖ Authentication Modes

- Fingerprint
- Password
- RFID card
- Combination of the above

❖ Features

- **Built-in SSR Excel software** for shift and report management
- **Infrared auto-on** for power saving
- **Push Data support** for real-time cloud sync
- **Hotspot mode** for mobile setup without a router

❖ Installation & Setup

- **Do I need Ethernet?**
  - Nope! Wi-Fi and hotspot mode make it cable-free.
- **Can I connect it to my phone?**
  - Yes, via hotspot mode for setup or log access.
- **Is software required?**
  - It comes with built-in software, but can also integrate with payroll or HRMS systems using SDKs.

❖ Maintenance & Support

- **How do I update firmware?**
  - Via USB—just plug in and follow the prompts.
- **Can I back up logs?**
  - Yes, logs can be backed up and restored via USB.
- **What if the fingerprint sensor fails?**
  - You can use password or RFID as backup methods.

Q: Can you explain the authentication modes in detail?

1. Fingerprint Authentication

- **How it works:** Users place their finger on the sensor. The device compares the fingerprint with stored templates using the **VX10.0 algorithm**.
- **Speed & Accuracy:** Fast recognition even under strong lighting or with slightly wet/rough fingers.
- **Security Level:** High—biometric data is unique and hard to replicate.
- **Use Case:** Ideal for secure areas or where proxy attendance is a concern.

2. Password Authentication

- **How it works:** Users enter a numeric password on the keypad.
- **Customizable:** Each user can have a unique password.
- **Security Level:** Moderate—depends on password strength and user discretion.
- **Use Case:** Useful as a backup method or for users who prefer not to use biometrics.

3. RFID Card Authentication

- **How it works:** Users tap a registered RFID card (e.g., EM or Mifare) on the reader.
- **Speed:** Instant recognition.
- **Security Level:** Moderate—cards can be lost or shared.
- **Use Case:** Great for high-traffic environments like gyms or schools.

4. Combination Modes

- **How it works:** The device can be configured to require two or more methods (e.g., fingerprint + password).
- **Security Level:** Very high—adds an extra layer of verification.
- **Use Case:** Best for sensitive zones like server rooms or finance departments.

Q: Can you provide examples of successful implementations?

❖ Corporate Offices

- **Use Case:** Streamlining employee attendance and integrating with payroll systems.
- **Impact:** Reduced manual errors and improved punctuality through real-time fingerprint logs synced via Wi-Fi.

❖ Educational Institutions

- **Use Case:** Preventing proxy attendance among students and staff.
- **Impact:** Enhanced accountability in libraries, labs, and classrooms with fingerprint and RFID verification.

❖ Manufacturing & Warehouses

- **Use Case:** Managing multiple shifts and controlling access to restricted zones.
- **Impact:** Rugged performance under harsh lighting and dusty conditions, with real-time data sync to central systems.

❖ Healthcare Facilities

- **Use Case:** Securing sensitive areas like ICUs, pharmacies, and admin offices.
- **Impact:** Multi-factor authentication (e.g., fingerprint + password) ensures only authorized personnel gain access.

❖ Fitness & Membership Clubs

- **Use Case:** Member check-ins and usage tracking.
- **Impact:** Quick RFID or fingerprint scans improve flow at peak hours and help optimize services based on attendance trends.

❖ Retail Chains

- **Use Case:** Managing staff attendance across multiple locations.
- **Impact:** Centralized data collection via cloud sync helps HR teams monitor attendance in real time.