Frequently Asked Question

Fingerprint attendance device F18

By : ESSL

❖ General Overview

Q.1: What is the eSSL F18?

- It's a biometric fingerprint reader designed for access control and time attendance. It supports fingerprint, RFID card, and PIN based authentication.

❖ Setup & Operation

Q.2: How do I enroll a user?

1. Power on the device.
2. Go to the main menu → User Management → Enroll User.
3. Choose fingerprint, card, or PIN.
4. Follow onscreen prompts to complete enrollment.

Q.3: How do I verify a fingerprint?

- Place your finger flat and centered on the sensor. If the device says "Thank you," verification is successful.

❖ Troubleshooting

Q.4: What does "User ID error" mean?

- It usually means the ID is not registered, entered incorrectly, or the fingerprint/card/PIN failed verification.

Q.5: Why is the fingerprint not recognized?

- Finger not placed properly
- Dirty or damaged sensor
- Fingerprint not enrolled correctly
- Try reenrolling with a different finger

❖ Software & Integration

Q.6: Which software is compatible?

- eTimeTrackLite (desktop & web)
- SDKs for integration with HRMS/ERP systems

Q.7: Can I connect it to a PC?

- Yes, via TCP/IP or USB. You can also push data to a server using supported software.

Q: How can I integrate eSSL F18 with my HR system?

❖ Integration Options

1. Use eSSL's Official SDK or API

- eSSL provides SDKs and APIs that allow you to:
  - Retrieve real-time attendance logs
  - Manage users (add, delete, update)
  - Monitor device status
- These tools are compatible with many HRMS and payroll systems.

❖ Third-party API Services

2. Companies like Ample Trails and Aperients Systems offer ready to use APIs for eSSL devices:

- Fetch attendance logs between specific dates
  - Add or delete employees
  - Enroll fingerprints remotely
  - Push data to cloud based HR systems
- Example API endpoint:`http://etime.esslsecurity.com:3366/WebAPIService.asmx?op=GetTransactionsLog`

❖ Integration Steps

1. Connect the Device

- Use TCP/IP or USB to connect the F18 to your network or PC.

2. Install Middleware or SDK

- Install the eSSL SDK or third-party API client on your server or HR system.

3. Configure API Access

- Set up API keys, device IP, and port.

- Define endpoints for attendance data and user management.
-

4. **Map Data Fields**
   - Match device fields (User ID, Timestamp, etc.) with your HR system's schema.
5. **Test & Automate**
   - Run test syncs to ensure data flows correctly.
   - Schedule automatic data pulls or use web hooks for real-time updates.

❖ Pro Tips

- **Push Data Feature:** Enable the "Push Data" option on the F18 to send logs automatically to your server.
- **Firewall Settings:** Ensure your network allows traffic on the port used by the device (default is often 3366).
- **Cloud HRMS?** Look for API bridges or middleware that support cloud to device sync.

Q: What security measures should I consider during integration?

❖ Network & Communication Security

- **Use Static IPs & MAC Binding**: Prevent unauthorized devices from spoofing the F18's identity.
- **Secure Protocols:** If possible, use HTTPS or VPN tunnels for data transmission instead of plain HTTP or open TCP/IP.
- **Firewall Rules:** Restrict access to the device's IP and port (commonly 3366) to only trusted systems.

❖ Authentication & Access Control

- **Strong Admin Passwords:** Change default credentials and enforce complex passwords on both the device and HR system.
- **Role Based Access:** Limit who can access biometric logs, device settings, and integration APIs.
- **Audit Logs:** Enable logging to track who accessed what and when.

❖ Data Protection

- **Encrypt Stored Data:** Ensure biometric templates and logs are encrypted both at rest and in transit.
- **Avoid Storing Raw Fingerprints:** The F18 stores fingerprint templates, not images—keep it that way to reduce risk.
- **Regular Backups:** Automate secure backups of attendance logs and user data.

❖ Device Level Safeguards

- **Antipas back:** Prevent users from entering and exiting without proper sequence.
- **Tamper Alerts:** Enable alerts for physical tampering or unauthorized access attempts.
- **Firmware Updates:** Keep the device firmware up to date to patch vulnerabilities.

❖ Cloud & API Security (if applicable)

- **API Key Management:** Use secure, rotating API keys or OAuth tokens for integration.
- **Rate Limiting & Throttling:** Prevent abuse of API endpoints.
- **Data Minimization:** Only sync the fields your HR system actually needs.