Frequently Asked Question

Fingerprint attendance device SpeedFace 7

By : BioMax

Sure! Here's a handy overview of frequently asked questions for the **Biomax SpeedFace 7** device:

❖ Device Setup & Configuration

- **How to add a new user?**

Go to: Menu → User → Enroll → Enter User ID & Name → Add Fingerprint/Password/Card/Face.

- **How to modify or delete a user?**

Menu → User → Modify → Select user → Edit or Delete → OK.

- **How to reset the device?**

Menu → Setting → Initial → Reset Default → OK.

- **How to update firmware?**

Insert a formatted USB → Menu → Setting → Initial → Upgrade From USB → OK.

❖ Attendance & Logs

- **Download attendance logs via USB:**

Insert USB → Menu → Report → Logs → ESC to cancel encryption → Logs download begins.

- **View logs for a specific user:**

Menu → ViewInfo → User Log → Enter Employee ID → Set date range → OK.

- **Check device capacity:**

Menu → ViewInfo → Reg.Info → View capacity for users, logs, fingerprints, etc.

❖ Access Control & Security

- **Set verification mode:**

Menu → Setting → Device → Verification Mode.

INSIGNIA

- **Configure lock/unlock timing:**

  Menu → Setting → LockCtrl → Unlock For → Set time (1–200 sec).

- **Enable Anti-Passback:**

  Menu → Setting → LockCtrl → Anti-Passback → Yes/No → OK.

❖ Network & Connectivity

- **Connect to Wi-Fi:**

  Menu → Setting → Network → Wi-Fi → Search → Select router → Enter password → OK.

- **Set IP address or Server URL:**

  Menu → Setting → Network → ETH → Set IP & Port.

- **Find Cloud ID:**

  Menu → Setting → Network → Cloud ID.

❖ Device Settings

- **Adjust volume or keypad sound:**

  Menu → Setting → Device → Volume or Keyboard Sound → Set level or toggle Yes/No.

- **Set screen saver or sleep time:**

  Menu → Setting → Device → Screen Saver or Sleep Time → Set duration.

- **Set alarm/bell timing:**

  Menu → Setting → Device → Bell → Set time & buzzer count.

INSIGNIA

Q: What are some common troubleshooting tips for biometric devices?

Biometric devices can be finicky, but with the right approach, most issues are easy to fix. Here's a go-to checklist for troubleshooting:

❖ Sensor & Hardware Checks

- **Clean the sensor**: Dirt, oil, or moisture can interfere with fingerprint or facial recognition. Use a soft, dry cloth—no harsh chemicals!
- **Inspect for damage**: Scratches or cracks on the sensor or camera lens can affect accuracy.
- **Check power supply**: Loose cables or unstable voltage can cause the device to reboot or freeze.

❖ Software & Configuration

- **Restart the device**: A simple reboot can clear temporary glitches.
- **Update firmware/software**: Manufacturers often release patches to fix bugs and improve performance.
- **Recalibrate sensors**: If recognition is inconsistent, recalibration may help—refer to the device manual.

❖ Connectivity & Syncing

- **Verify network settings**: Ensure correct IP, port, and Wi-Fi credentials are set.
- **Check cloud/server sync**: If attendance isn't syncing, confirm server settings and firewall permissions.
- **Try another network**: Sometimes switching to a different Wi-Fi or LAN resolves sync issues.

INSIGNIA

❖ User Enrollment & Recognition

- **Re-enroll users**: Poor-quality biometric data during enrollment can cause failed recognition.
- **Use multiple samples**: Register more than one fingerprint or facial scan per user.
- **Optimize lighting and positioning**: Ensure users face the camera directly and stand at the recommended distance.

❖ System Settings & Compatibility

- **Review verification settings**: Adjust sensitivity, angle limits, and recognition thresholds.
- **Check for software conflicts**: Ensure biometric software is compatible with your operating system.
- **Scan for malware**: Viruses can corrupt biometric software—run a security check if things seem off.

❖ When All Else Fails

- **Factory reset**: As a last resort, reset the device to default settings (after backing up data).
- **Contact support**: Reach out to the manufacturer or service provider for deeper diagnostics.

Q: What are common issues with biometric devices?

Biometric devices are powerful tools for authentication and access control, but they're not without their quirks. Here are some of the most common issues users and administrators run into:

❖ Sensor & Hardware Problems

- **Dirty or damaged sensors**: Dust, smudges, or scratches can prevent accurate readings—especially for fingerprint scanners.
- **Wear and tear**: Frequent use can degrade sensor performance over time.
- **Environmental interference**: Humidity, extreme temperatures, or poor lighting can affect facial and iris recognition.

❖ Software Glitches & Compatibility

- **Outdated firmware**: Can cause bugs, slow performance, or incompatibility with newer systems.
- **System crashes**: Software bugs may lead to failed authentications or frozen interfaces.
- **Poor integration**: Conflicts with HR or payroll systems if not updated regularly.

❖ Recognition Failures

- **Low-quality enrollment data**: Blurry face scans or partial fingerprints lead to false rejections.
- **Changes in appearance**: Injuries, makeup, aging, or facial hair can confuse recognition algorithms.
- **False positives/negatives**: Especially in facial recognition, where bias and poor training data can cause errors.

❖ Connectivity & Sync Issues

- **Network failures**: Prevent real-time syncing of attendance or access logs.
- **Server downtime**: Cloud-based systems may fail if the central server is unreachable.

❖ Security & Privacy Concerns

- **Spoofing attacks**: Fake fingerprints or 3D masks can trick some devices.
- **Data breaches**: Biometric data is permanent—once stolen, it can't be changed like a password.
- **Surveillance risks**: Facial recognition systems can be misused for tracking without consent.

❖ User Errors

- **Improper usage**: Misalignment, incorrect finger placement, or standing too far from the camera.
- **Lack of training**: Users unaware of how to interact with the device properly.

Q: What should I do if the device won't recognize a user?

If your **Biomax SpeedFace 7** device isn't recognizing a user, here are some steps you can take to troubleshoot the issue:

❖ Check User Enrollment

- Ensure the user is properly enrolled with clear face data.
- Re-enroll the user if the original capture was blurry, poorly lit, or obstructed (e.g., mask, glasses, hat).

❖ Optimize Face Recognition Conditions

- **Lighting:** Make sure the area is well-lit but not backlit.
- **Distance:** Users should stand about 1 meter from the device.
- **Angle:** Face should be directly in front of the camera, not tilted.

❖ Adjust Recognition Settings

- Go to: Menu → Setting → Device → Face Parameters
  - Increase **recognition sensitivity** or **face angle threshold** if needed.
  - Default values are typically:
    - Recognition threshold: 80
    - Face angle limit: 20°
    - Recognition distance: 65–320 cm

❖ Restart or Reset

- Try restarting the device.
- If the issue persists, consider a **soft reset** via:
  Menu → Setting → Initial → Reset Default → OK
  (Note: This may erase settings—backup first!)

❖ Connectivity Check

- If using cloud or server-based verification, ensure the device is connected to Wi-Fi or LAN properly.

❖ Enable Live Body Detection

- This feature helps prevent spoofing and improves accuracy. Check under: Menu → Setting → Device → Live Body Detection → Enable