

## I. Activate Secure Mode

**Settings**

Touch to toggle ON

Enter Admin Password

Enter

Reset Admin Password

Enter

Enter admin user first name and last name

Enter

Enter admin password

Enter

Read & acknowledge warning

Enter

Provide Bluetooth ID and Date/Time (shown on screen)

Enter

New Administrator Required

OK Cancel

Secure mode requires the purchase of a separate license to activate. Contact Gemini/Orflo Sales or Customer Service for a quote.

## 2. System Settings

Set system settings that are key to 21 CFR, Part 11

- Default data gating behavior (auto vs. manual)
- Set timeout for screen lock
- Password expiration period
- Secure Mode - On/Off Toggle

## 3. User Management

User Management under new "Users" Icon on Home Screen

User Management Options

**User Roles**

All Users must be assigned one of three roles when created. Brief overview below.

**Administrator**

- Generate Data
- Modify Data
- Manage Users
- System Settings
- Transfer Data
- Access System logs

**Reviewer**

- Generate Data
- Modify Data

**Normal User**

- Generate Data only

## Electronic Signatures & Data Output

Signature (User ID and Password) required for all data operations

Auto - BMP output for all data events = permanent results & signature snapshot/log

Date	User - name	Role	Action
Jun 11 13:38:32 2021	LabStop - Lab Supervisor	Reviewer	Approved
Jun 11 13:38:32 2021	LabTech - Lab Tech	User	Modified

**All data also stored as FCS 3.1 data file with checksum protection & signature log**

## Data Review

**Administrator & Reviewer - only review of saved user data**

Parent Folder (Up)

Select User ID folder to review user's data

Select test file to review.  
Notes: Signature required for any data change. All changes are logged

## USB Data Transfer

Connect System to PC with USB power cable

USB Disk Icon on Home Screen

**Administrator - only access**

- User Data
  - \*older data in "Test-Files" folder
  - \*Secure data in /Users sub-folder under UserID of owner
  - \*FCS, .BMP, and .CSV data
- System Logs (2 week's logs per file) in /Users/admin folder - logs of all relevant system events

- The Moxi V software does not ensure 21 CFR, Part 11 compliance, by itself, as proper procedures, training, and internal controls (e.g. cGMP/GLP) are also required by companies in conjunction with the firmware in order to be 21 CFR, Part 11 compliant.
- The Moxi V is a research use only (RUO) instrument, not for use in diagnostic procedures