IEM®

Flow

Operator Manual
2.3.0_2026-04-24
EN

Copyright

Flow

Flow software is used to configure and visualize measurements taken with the Mobil-O-Graph® and the HeartX recorder.

IEM GmbH
Gewerbepark Brand 42
52078 Aachen
Germany

Email: info@iem.de
Internet: www.iem.de

Table of Contents

1 Installation of the Software

New Installation

Before installing Flow, make sure that all system requirements are met, see 1.2 System Requirements, p. 5.

Download the latest version of Flow from the following URL: www.iem.de/flow/download

To install the software, follow the instructions in chapter 1.3 Install Software, p. 6.

Online-Update-Service for the existing installation

Flow regularly checks this service for updates and offers the user the option to upgrade to the latest version if necessary.

1.1 IT Security Requirements

The controls listed below have been incorporated into the cybersecurity risk assessment and form the basis for the secure operation of the software and the protection of the data required by the software. Partial implementation of these controls results in an increased security risk with regard to confidentiality, integrity, and availability.

Encrypted File System

- Use of a storage location that supports strong encryption (e.g., LUKS, BitLocker, VeraCrypt).
- Secure management of encryption keys.
- Access to unencrypted data during operation must be restricted exclusively to authorized processes.

Encrypted Data Communication

- If data is accessed over a network (e.g., network drive, remote access), communication must be secured using current cryptographic protocols (e.g., TLS 1.3, IPsec, SSH).
- Unencrypted (plaintext) transmissions (e.g., via FTP or SMBv1) are strictly prohibited.

Strict Access Restrictions

- Access rights must be regularly reviewed and documented.
- Access may only be granted to individuals with a legitimate need-to-know.

Backup Strategy

The backup strategy reduces the likelihood of data loss and enables the operator to restore resources within the expected timeframe. The backup strategy also includes a security policy (including modern data encryption) as well as an access policy to prevent unauthorized third-party access.

Monitoring & Logging

Monitoring enables the early detection of system malfunctions. Intelligent log file analysis also enables the operator to detect intruders or malware.

Network and Firewall

Firewalls and packet filters prevent harmful network traffic and communication. Intelligent network segmentation increases reliability and availability in case resources are compromised.

Protection Against Malware

Malware protection on servers and desktop computers enhances the security of the infrastructure.

Strict Access Control and Secure Password Policies

Strict Access Control

- Principle of least privilege
- Multi-factor authentication (MFA)
- Role-based access control
- Just-in-time admin / break-glass accounts

Secure Password Policy

- Minimum password lengths
- Use of password managers
- Lockout mechanisms for failed login attempts

Emergency Plan

An emergency plan following the BSI guideline (100-4: Emergency Management) increases the likelihood of restoring the system infrastructure after a security-related incident.

DNS Configuration

The application uses the system-provided settings for name resolution of the online update service. Correct configuration of these settings, as well as verification of the DNS service's authenticity, reduces the risk of malicious attacks.

Additional security measures have been implemented to ensure the integrity of the update package.

No Security-Critical Applications on the Computer

The computer system running the application is not intended for safety-critical or business-critical functions.

SBoM

The Software Bill of Materials (SBoM) is located in the installation directory under the SBOM subfolder. The SBoM is provided as an CycloneDX document in JSON format. It is recommended to include the third-party libraries listed in the SBoM into the internal monitoring system.

1.2 System Requirements

Supported Medical Devices

- Mobil-O-Graph® with firmware 200007 (GTIN: 04041346100104) with 4-Pin cable (GTIN: 04041346101934)
- Mobil-O-Graph® with firmware 200212 (GTIN: 04041346100784, 04041346102269) with 4-pin cable (GTIN: 04041346101934)
- Mobil-O-Graph® with firmware 200212 (GTIN: 04041346102269) with USB-C cable
- HeartX Recorder (GTIN: 04250903203176), for AI service
- HeartX Recorder (GTIN: 04250903203398)

Operating System

Please note: Administrator rights are required to install the software.

Microsoft	Windows® 10, Windows® 11
Apple	macOS® 26 (Tahoe)

Minimum System Requirements

Screen Size (diagonal)	14 inches
Screen Resolution (in pixels)	1280 x 720
Hard Disk Space (in GB)	1 GB of permanently available free space (required for the software log files)
Device Interface	USB Type A (for connecting the Mobil-O-Graph®)
Optional	Network adapter with internet connection • For future software updates via the integrated online update service

Operating system-dependent system requirements

	Microsoft Windows® 10, 11	macOS® 15, Sequioa
Main memory (RAM), Minimum	4 GB	8 GB
Processor	x86 Intel Core i5 or equivalent AMD counterpart	x86 Intel Core i5 Apple Silicon

1.3 Install Software

Preparations

- Ensure that the system requirements are met, see 1.2 System Requirements, p. 5
- Download the latest version of Flow from the following URL: www.iem.de/flow/download

Execution

1. Start the installation file for your operating system:

Microsoft Windows®	macOS®
flow-<version>-windows-amd64.exe	flow-<version>-macos-amd64.dmg (x86 Intel processor)
	flow-<version>-macos-aarch64.dmg (Apple Silicon processor)

2. Follow the instructions of the **Flow setup assistant**. At the end of the installation, you have the option to enable autostart for Flow.
3. If the software is already installed on the computer and you start the installation again, the **Flow setup assistant** will automatically detect the existing installation along with its installation directory. During reinstallation, all data and previously made settings will be retained.

1.3.1 Notification Icon

After successfully installing and launching the software, you will find the notification icon 

- on Windows® in the lower right part of the taskbar. If you don't see the icon, you may need to expand the menu using the arrow to view all active applications.
- on macOS® in the upper right part of the menu bar.

Exiting the software via the notification icon

Windows®:
Right-click the software icon to exit the application.

macOS®:
Click the software icon with the primary mouse button to exit the application.

1.3.2 Note on using malware protection

FLOW extracts platform-specific native libraries from its installation packages into a temporary directory on startup. This directory is located at: <user home>/.flow/tmp/ . This directory is created only after FLOW is launched for the first time.

The extracted files are signed components of the FLOW application and are required for device communication. They are recreated on each application start if missing.

Some antivirus or endpoint protection software may flag these extracted files as suspicious and quarantine or delete them. When this happens, FLOW may fail to start, crash during startup, or fail to detect connected devices. Log files may contain errors such as "UnsatisfiedLinkError" or "Library not found".

To resolve this, add the directory /.flow/tmp/ to the antivirus exclusion list or whitelist. After applying the exclusion, restart FLOW. The application will re-extract the required files and operate normally.

The exclusion applies only to the specified temporary directory and does not affect the overall security posture of the system.

2 Settings

You can access the Settings menu by clicking the gear icon  in the upper-left corner of the user interface

2.1 Storage Location

Storage Location for Job List

Select the storage location where the software saves all job data. This setting must be defined when the software is started for the first time and can be changed later. Ensure that the software has read and write permissions for the selected folder.

Storage Location for Reports

Select the storage location where the software saves all reports. This setting must be defined when the software is started for the first time and can be changed later. Ensure that the software has read and write permissions for the selected folder.

If no report path has been selected, the reports can only be viewed in FLOW.

Note

Separate Storage Locations

The storage location for the job list and reports must not be the same folder used for the job list; likewise, no subfolders of that folder may be used.

Note

Multi room

The “Multi room” function allows multiple software instances to access the same job data.
Select a storage location for which all software instances have read and write access.
Depending on the network configuration, delays may occur when accessing the shared storage location, resulting in changes to jobs becoming visible with delay in all connected software instances.

2.2 Update

A prerequisite for using the Online Update Service is an internet connection and administrator rights for installation.

The software includes an integrated Online Update Service. FLOW regularly checks this service to determine whether a new program version is available. As soon as an update is available, the software downloads it and notifies the user that a new version can be installed. The user can start the update at any time.

During the update, the software closes and restarts automatically after the update is completed.

Data and settings are transferred to the new program version during the update.

Note

Security-critical updates

Critical updates fix security-related issues. They must be installed to ensure that FLOW continues to function properly.

2.3 Cable List

The software prompts users to register all 4-pin cables used with this software or to specify that they are not used with this software.

This prevents unwanted interactions with other devices and cables connected to the computer.

The "Cable List" feature allows you to delete all stored information about 4-pin cables. This function should be used if a 4-pin cable has been incorrectly categorized.

2.4 Interfaces and Communication Paths

General

Application updates / Microsoft Azure	
Target-ID	A2916
Direction	outgoing
Protocol / Port	HTTPS / TCP 443
Endpoint/ Desription	cd.iem.zone/flow
Security measures	TLS 1.2+
Notes for operator	Internet connection with port 443 required

IEM Sentry Service	
Target-ID	A4941
Direction	outgoing
Protocol / Port	HTTPS / TCP 443
Endpoint / Description	o4510141214621696.ingest.de.sentry.io/
Security measures	TLS 1.2+
Notes for operator	Internet connection with port 443 required

IEM Website **FLOW Application, Release Notes, Device firmware, Data protection regulations**	
Target-ID	A3589
Direction	outgoing
Protocol / Port	HTTPS / TCP 443
Endpoint / Description	iem.de
Security measures	TLS 1.2+
Notes for operator	Internet connection with port 443 required

ABPM

IEM Mobil-O-Graph	
Target-ID	A2926
Direction	Locale I/O
Protocol / Port	USB/ UART

IEM Mobil-O-Graph	
Endpoint / Description	External recorder device
Security measures	-
Notes for operator	Secure physical USB port

Holter

IEM HeartX Holter	
Target-ID	A4585
Direction	Locale I/O
Protocol / Port	USB
Endpoint / Description	External recorder device
Security measures	-
Notes for operator	Secure physical USB port

Azure-Storage / Holter measurement upload	
Target-ID	A5078
Direction	outgoing
Protocol / Port	HTTPS / TCP 443
Endpoint / Description	gtmhxhcustomers05.blob.core.windows.net
Security measures	TLS 1.2+
Notes for operator	Internet connection with port 443 required

ECG AI backend	
Target-ID	A4588
Direction	outgoing
Protocol / Port	HTTPS / TCP 443
Endpoint / Description	hxh-api.prod.heartxholter.com
Security measures	TLS 1.2+
Notes for operator	Internet connection with port 443 required

Webviewer	
Target-ID	A5072
Direction	outgoing
Protocol / Port	HTTPS / TCP 443
Endpoint / Description	heartxholter.com
Security measures	TLS 1.2+
Notes for operator	Internet connection with port 443 required

2.4.1 Setting up the Holter interface

Precondition: HeartX Recorder (GTIN: 04250903203176) and account for Webviewer

To set up the interface to the AI evaluation service for the HeartX Recorder, proceed as follows:

- Log in to Webviewer with your account.
- Open the settings (gear icon).
- Click on the “IEM Integration”
- Create a token by clicking on **Create Token**.
  A .token file will be downloaded automatically.
- Save the file in the HeartX settings.

2.4.2 GDT

FLOW allows operators to configure a data interface to a practice management system (PVS) or hospital information system (HIS) using the GDT 2.1 standard (device data transfer).

For FLOW to accept and process a job from the desired system, the following codes must be included in the file sent to FLOW:

- 3000 – Patient identifier
- 8000 – Expected value “6302”
- 8402 – Expected value:
  - for ABPM "BDM01"
  - for Holter "EKG04"

The GDT specification defines only the file structure and semantics; it does not include security mechanisms such as encryption, authentication, or integrity protection. Data exchange is performed through shared directories (“GDT exchange folders”). The operation and protection of these directories is the responsibility of the operator (e.g., the medical practice or IT service provider). The application strictly supports data exchange within the GDT specification. End-to-end security mechanisms (such as encryption or digital signatures) are not part of the standard and therefore not implemented.

To ensure secure and compliant operation, the operator must implement the following measures:

- Implement access control measures. Only authorized entities may access the HIS-GDT interface.
- Ensure the integrity and confidentiality of GDT file transfers.
- Protect information at rest through encryption and technical safeguards.
- Maintain logging and monitoring of GDT exchanges for accountability.
- Provide adequate backup and recovery mechanisms to guarantee availability of exchanged GDT files.

Note

Multi room

The “Multi room” function allows multiple software instances to access the same job data.

Ensure that the following settings match across all instances that are to be connected via Multi room:

- GDT mode enabled
- Character set encoding

- Import and export directories
  The same directories must be configured that are also used as exchange folders for the PVS/ HIS at the respective workstation.