IEM®

Flow

Betreiberanleitung
2.4.1_2026-10-28
DE

Copyright

Flow

Die Software Flow dient zur Konfiguration und Darstellung von Messungen mit dem Mobil-O-Graph® und dem HeartX Recorder.

IEM GmbH
Gewerbepark Brand 42
52078 Aachen
Deutschland

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

Der Inhalt dieses Dokuments darf ohne schriftliche Genehmigung der IEM GmbH weder vervielfältigt noch veröffentlicht werden.

Alle in diesem Dokument genannten Produkt- und Firmennamen sind Marken oder eingetragene Marken ihrer jeweiligen Inhaber.

Die Software Flow ist urheberrechtlich geschützt und ist Eigentum des Herstellers. Es sind alle Rechte vorbehalten. Flow darf nicht ausgelesen, kopiert, dekompiliert, zurückentwickelt, zerlegt oder in ein von Menschen lesbares Format gebracht werden. Alle Rechte der Nutzung und des Besitzes an der Software verbleiben bei der IEM GmbH.

© IEM GmbH 2026 Alle Rechte vorbehalten.

Inhaltsverzeichnis

1 Installation der Software....4
1.1 IT-Sicherheitsvorgaben....4
1.2 Systemvoraussetzungen....6
1.3 Software installieren....6
1.3.1 Benachrichtigungssymbol....7
1.3.2 Hinweis zum Einsatz von Schadsoftware-/Malware-Schutz....7
2 Einstellungen....9
2.1 Speicherorte....9
2.2 Update....10
2.3 Kabelliste....10
2.4 Schnittstellen und Kommunikationswege....10
2.4.1 Einrichtung der Holter-Schnittstelle....13
2.4.2 GDT....13
2.4.3 HL7....14

1 Installation der Software

Neuinstallation

Stellen Sie vor der Installation von Flow sicher, dass alle Systemvoraussetzungen erfüllt sind, siehe 1.2 Systemvoraussetzungen, S. 6.

Laden Sie die aktuelle Version von Flow unter der folgenden URL herunter: https://www.iem.de/flow/download

Folgen Sie den Anweisungen in Kapitel 1.3 Software installieren, S. 6, um die Software zu installieren.

Online-Update-Service der vorhandenen Installation

Flow prüft diesen Dienst regelmäßig auf Aktualisierungen und bietet dem Benutzer an, bei Bedarf auf die neueste Version zu aktualisieren.

1.1 IT-Sicherheitsvorgaben

Die nachfolgend genannten Controls sind in die Risikobetrachtung bzgl. Cybersecurity eingeflossen und bilden die Grundlage für den sicheren Betrieb der Software und die Sicherheit der von der Software benötigten Daten. Eine nur teilweise Umsetzung der Controls führt zu einem erhöhten Sicherheitsrisiko bzgl. der Vertraulichkeit, Integrität und Verfügbarkeit.

Verschlüsseltes Dateisystem

- Verwendung eines Speicherorts, der starke Verschlüsselung unterstützt (z. B. LUKS, BitLocker, VeraCrypt).
- Sichere Verwaltung der Verschlüsselungsschlüssel.
- Der Zugriff auf unverschlüsselte Daten muss während des Betriebs ausschließlich autorisierten Prozessen vorbehalten sein.

Verschlüsselte Datenkommunikation

- Wenn auf die Daten über ein Netzwerk zugegriffen wird (z. B. Netzlaufwerk, Fernzugriff), muss die Kommunikation durch aktuelle kryptografische Protokolle gesichert werden (z. B. TLS 1.3, IPsec, SSH).
- Unverschlüsselte (Klartext-)Übertragungen (z. B. über FTP oder SMBv1) sind strikt untersagt.

TLS-Verbindungen und SSL/TLS-Inspektion

FLOW baut TLS-Verbindungen mit strikter Prüfung des Serverzertifikats auf. Diese Verbindungen dürfen von keinem Proxy, keiner Firewall, keiner SSL/TLS-Inspection-Appliance, keiner Antivirus-Lösung und keiner anderen Netzwerk-Sicherheitskomponente abgefangen, terminiert, entschlüsselt oder neu verschlüsselt werden. Dies ist eine zwingende technische Voraussetzung für den korrekten Betrieb von FLOW. Die betroffenen Verbindungen und die Einzelheiten stehen in den Steckbriefen im Abschnitt 2.4 Schnittstellen und Kommunikationswege, S. 10 unter Hinweis 2.

Strikte Zugriffsbeschränkungen

- Zugriffsrechte müssen regelmäßig überprüft und dokumentiert werden.
- Zugriff darf nur Personen gewährt werden, die ein berechtigtes Need-to-know haben.

Backup-Strategie

Die Backup-Strategie verringert die Wahrscheinlichkeit eines Datenverlusts und ermöglicht es dem Betreiber, Ressourcen innerhalb des erwarteten Zeitrahmens wiederherzustellen. Die Backup-Strategie umfasst außerdem eine Sicherheitsrichtlinie (einschließlich moderner Datenverschlüsselung) sowie eine Zugriffsrichtlinie, um den Zugriff durch unbefugte Dritte zu verhindern.

Monitoring & Logging

Monitoring ermöglicht die frühzeitige Erkennung von Systemstörungen. Eine intelligente Logdateianalyse erlaubt es dem Betreiber zudem, Eindringlinge oder Schadsoftware zu erkennen.

Netzwerk und Firewall

Firewalls und Paketfilter verhindern schädlichen Netzwerkverkehr und -kommunikation. Intelligente Netzwerksegmentierung erhöht die Zuverlässigkeit und Verfügbarkeit, falls Ressourcen kompromittiert werden.

Schutz vor Schadsoftware-/Malware-Schutz

Malware-Schutz auf Servern und Desktop-Rechnern erhöht die Sicherheit der Infrastruktur.

Strikte Zugriffskontrolle und sichere Passwortrichtlinien

Strikte Zugriffskontrolle

- Prinzip der minimalen Rechtevergabe (Least Privilege)
- Multi-Faktor-Authentifizierung (MFA)
- Rollenbasierte Zugriffskontrolle
- Just-in-Time-Admin-/Break-Glass-Konten

Sichere Passwortrichtlinie

- Mindestlängen
- Einsatz von Passwortmanagern
- Sperrmechanismen bei Fehlversuchen

Notfallplan

Ein Notfallplan nach Vorgabe des BSI (100-4: Notfallmanagement) erhöht die Wahrscheinlichkeit der Wiederherstellung der Systeminfrastruktur aufgrund eines sicherheitsbedingten Vorfalls.

DNS-Konfiguration

Die Applikation nutzt für die Namensauflösung des Online-Update Service die über das System bereitgestellten Einstellungen. Die korrekte Konfiguration der Einstellungen, sowie die Überprüfung der Authentizität des DNS Dienstes verringert die Wahrscheinlichkeit eines bösartigen Angriffs. Zur Sicherstellung der Integrität des Update-Pakets wurden weitere Sicherungsmaßnahmen implementiert.

Keine sicherheitskritischen Anwendungen auf dem Computer

Das Computersystem, auf dem die Anwendung betrieben wird, ist nicht für sicherheitsrelevante (Safety) oder unternehmenskritische Funktionen vorgesehen.

SBoM und VEX

Die SBoM (Software Bill of Materials) liegt im Installationsverzeichnis im Unterordner SBOM. Sie liegt als CycloneDX-Dokument im JSON-Format vor. Es wird empfohlen, die darin enthaltenen Fremdbibliotheken in das interne Überwachungssystem aufzunehmen.

Für jede veröffentlichte FLOW-Version stellt IEM die SBoM zusätzlich zusammen mit einem Vulnerability-Exploitability-eXchange-Dokument (VEX) und einer Cosign-Signatur unter https://www.cd.iem.zone/security/flow/ bereit. Das VEX-Dokument gibt für jede bekannte CVE an, ob sie in FLOW ausnutzbar ist, und begründet die Einschätzung. Unter https://www.cd.iem.zone/security/README.md sind die URL-Konventionen, die Signaturprüfung und Informationen zur Einbindung in Ihr Überwachungssystem beschrieben.

Das Security-Team von IEM erreichen Sie unter security@iem.de.

1.2 Systemvoraussetzungen

Unterstützte, medizinische Geräte

- Mobil-O-Graph® mit Firmware 200007 (GTIN: 04041346100104) mit 4-Pin Kabel (GTIN: 04041346101934)
- Mobil-O-Graph® mit Firmware 200212 (GTIN: 04041346100784, 04041346102269) mit 4-Pin Kabel (GTIN: 04041346101934)
- Mobil-O-Graph® mit Firmware 200212 (GTIN: 04041346102269) mit USB-C Kabel
- HeartX Recorder (GTIN: 04250903203176), für KI-Service
- HeartX Recorder (GTIN: 04250903203398)

Betriebssystem

Bitte beachten Sie: Für die Installation der Software werden Administratorrechte benötigt.

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

Minimale Systemanforderungen

Bildschirmgröße (Diagonale)	14 Zoll
Bildschirmauflösung (in Pixel)	1280 x 720
Festplattenspeicher (in GB)	1 GB ständig freier Speicherplatz (wird für die Log-Dateien der Software benötigt)
Schnittstelle für Geräteanschluss	USB Typ A (zum Anschluss des Mobil-O-Graph®)
Optional	Netzwerkadapter mit Internetzugang: • Für zukünftige Aktualisierungen der Software über den integrierten Online-Update-Service

Betriebssystem abhängige Systemanforderungen

	Microsoft Windows® 10, 11	**macOS® 15, Sequoia**
Arbeitsspeicher (RAM), Minimum	4 GB	8 GB
Prozessor	x86 Intel Core i5 oder entsprechendes AMD-Pendant	x86 Intel Core i5 Apple Silicon

1.3 Software installieren

Vorbereitungen

- Stellen Sie sicher, dass die Systemvoraussetzungen erfüllt sind, siehe 1.2 Systemvoraussetzungen, S. 6
- Laden Sie die aktuelle Version von Flow unter der folgenden URL herunter: https://www.iem.de/flow/download

Durchführung

1. Starten Sie die Installationsdatei für Ihr Betriebssystem:

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

2. Folgen Sie den Anweisungen des Flow-Einrichtungsassistenten. Am Ende der Installation haben Sie die Möglichkeit, Autostart für Flow einzustellen.
3. Ist die Software bereits auf dem Computer installiert und Sie starten die Installation erneut, erkennt der Flow-Einrichtungsassistent automatisch die bereits vorhandene Installation samt Installationsverzeichnis. Bei einer erneuten Installation bleiben alle Daten und bereits vorgenommenen Einstellungen erhalten.

1.3.1 Benachrichtigungssymbol

Wenn Sie die Software erfolgreich installiert und gestartet haben, finden Sie das Benachrichtigungssymbol

- unter Windows® im rechten, unteren Teil der Taskleiste. Sehen Sie das Symbol nicht, müssen Sie vielleicht das Menü mittels Pfeil aufklappen, um alle aktiven Anwendungen sehen zu können.
- unter macOS® im rechten, oberen Teil der Menüleiste.

Beenden der Software im Benachrichtigungssymbol

Windows®:

Klicken Sie mit der sekundären Taste auf das Symbol der Software, um die Software zu beenden.

macOS®:

Klicken Sie mit der primären Taste auf das Symbol der Software, um die Software zu beenden.

1.3.2 Hinweis zum Einsatz von Schadsoftware-/Malware-Schutz

FLOW extrahiert beim Start plattformspezifische native Bibliotheken aus seinen Installationspaketen in ein temporäres Verzeichnis. Dieses Verzeichnis befindet sich unter: <Benutzerverzeichnis>/.flow/tmp/. Dieses Verzeichnis wird erst nach dem ersten Start von FLOW erstellt.

Die extrahierten Dateien sind signierte Komponenten der FLOW-Anwendung und für die Kommunikation mit Geräten erforderlich. Fehlen sie, werden sie bei jedem Anwendungsstart neu erstellt.

Manche Antiviren- oder Endpoint-Schutzprogramme stufen diese extrahierten Dateien möglicherweise als verdächtig ein und verschieben sie in die Quarantäne oder löschen sie. In diesem Fall kann FLOW möglicherweise nicht starten, während des Startvorgangs abstürzen oder angeschlossene Geräte nicht erkennen. Die Protokolldateien enthalten möglicherweise Fehler wie „UnsatisfiedLinkError" oder „Library not found".

Um dies zu beheben, fügen Sie das Verzeichnis /.flow/tmp/ zur Ausschlussliste oder Whitelist Ihres Antivirenprogramms hinzu. Starten Sie FLOW nach dem Anwenden des Ausschlusses neu. Die Anwendung extrahiert die erforderlichen Dateien erneut und läuft normal.

Der Ausschluss gilt nur für das angegebene temporäre Verzeichnis und hat keinen Einfluss auf die allgemeine Sicherheitslage des Systems.

Installation

Der Installer entpackt während der Installation temporäre Dateien. Stuft ein Antiviren- oder Endpoint-Schutzprogramm diese als verdächtig ein, kann die Installation fehlschlagen oder unvollständig bleiben.

Erlauben Sie in diesem Fall die Ausführung des Installers in Ihrem Antiviren- oder Endpoint-Schutzprogramm und starten Sie die Installation erneut.

2 Einstellungen

Sie erreichen das Menu für Einstellungen über das Zahnrad links oben in der Benutzeroberfläche.

2.1 Speicherorte

Speicherort für die Jobliste

Sie wählen den Speicherort, in dem die Software alle Informationen zu den Jobs ablegt. Diese Einstellung muss beim ersten Start der Software definiert werden und kann später verändert werden. Bitte stellen Sie sicher, dass die Software für den gewählten Ordner Lese- und Schreibrechte hat.

Speicherort für Berichte

Sie wählen den Speicherort, in dem die Software alle Berichte ablegt. Diese Einstellung muss beim ersten Start der Software definiert werden und kann später verändert werden. Bitte stellen Sie sicher, dass die Software für den gewählten Ordner Lese- und Schreibrechte hat.

Wenn kein Pfad für Berichte gewählt wurde, können die Berichte nur in FLOW angezeigt werden.

Achtung

Separate Speicherorte

Der Speicherort für Jobliste und Berichte darf nicht dem Ordner entsprechen, der für die Jobliste genutzt wird; ebenso dürfen keine Unterordner von diesem genutzt werden.

Achtung

Multi room

Die Funktion “Multi room” ermöglicht es, dass mehrere Software-Instanzen auf dieselben Jobdaten zugreifen können.

Wählen Sie Speicherorte, für die alle Software-Instanzen Lese- und Schreibrechte haben.

Für den gemeinsamen Speicherort im Multi-room-Betrieb wird ein direkt erreichbares Netzlaufwerk im lokalen Netzwerk empfohlen. Cloud-Speicher mit Synchronisationsclient (z. B. Microsoft OneDrive, Google Drive, Dropbox, Nextcloud, Infomaniak kDrive) ist dafür ungeeignet und wird nicht unterstützt, da es durch Synchronisationsverzögerungen, erhöhte Latenzen oder inkonsistente Datenstände zu verzögerter Anzeige oder fehlerhaftem Verhalten kommen kann. Das gilt unabhängig davon, ob die Dateien lokal vorgehalten oder erst beim Zugriff heruntergeladen werden.

Ein NAS ist als Netzlaufwerk über eine SMB-Freigabe geeignet, über seinen Synchronisationsclient (z. B. Synology Drive) dagegen nicht.

Achtung

Anforderungen an die Netzwerkverbindung

FLOW benötigt einen schnellen Zugriff auf den Speicherort für die Jobliste. Alle Arbeitsplätze greifen fortlaufend auf diesen Speicherort zu. Verzögerungen von mehreren Sekunden beim Zugriff auf den Speicherort sind für den Betrieb von FLOW nicht geeignet.

Verwenden Sie ein Netzlaufwerk im lokalen, kabelgebundenen Netzwerk. Treten spürbare Verzögerungen auf, lassen Sie die Netzwerkverbindung von Ihrem IT-Dienstleister prüfen, bevor Sie FLOW weiter verwenden.

2.2 Update

Voraussetzung für die Nutzung des Online-Update-Services ist eine Internetverbindung sowie Administratorrechte für die Installation.

Die Software besitzt einen integrierten Online-Update-Service. FLOW überprüft diesen Dienst regelmäßig, ob eine neue Programmversion verfügbar ist. Sobald ein Update verfügbar ist, lädt die Software das Programm herunter und informiert den Benutzer, dass eine neue Version installiert werden kann. Der Benutzer kann das Update jederzeit starten.

Während des Updates schließt sich die Software und startet automatisch nach Abschluss des Updates.

Daten und Einstellungen werden während des Updates auf die neue Programmversion übertragen.

Achtung

Sicherheitskritische Updates

Kritische Updates beheben sicherheitsrelevante Probleme. Sie müssen installiert werden, damit FLOW weiterhin funktioniert.

2.3 Kabelliste

Die Software fordert die Benutzer auf, alle verwendeten 4-Pin Kabel für diese Software zu registrieren bzw. festzulegen, dass sie nicht für diese Software genutzt werden.

Damit werden unerwünschte Wechselwirkungen mit anderen Geräten und Kabeln, die an den Computer angeschlossen werden, verhindert.

Die Funktion “Kabelliste” ermöglicht, alle gespeicherten Informationen zu 4-Pin Kabeln zu löschen. Diese Funktion sollte genutzt werden, wenn ein 4-Pin Kabel falsch kategorisiert wurde.

2.4 Schnittstellen und Kommunikationswege

Allgemein

Microsoft Azure / Online-Update	
Ziel-ID	A2916
Richtung	ausgehend
Protokoll / Port	HTTPS / TCP 443
Endpunkt / Beschreibung	cd.iem.zone/flow
Übertragene Daten	Prüfung auf eine neue Version alle 6 Stunden, Download des Installationspakets
Sicherheitsmaßnahmen	TLS 1.2+
Hinweise für Betreiber	1, 2

sentry.io, EU-Region	
Ziel-ID	A4941
Richtung	ausgehend
Protokoll / Port	HTTPS / TCP 443

sentry.io, EU-Region	
Endpunkt / Beschreibung	o4510141214621696.ingest.de.sentry.io/
Übertragene Daten	Fehlermeldungen mit Stacktrace, vorangegangene Logzeilen, Installations-ID, Programmversion, Betriebssystem, Spracheinstellung, IP-Adresse
Sicherheitsmaßnahmen	TLS 1.2+
Hinweise für Betreiber	1, 2

IEM Website	
Ziel-ID	A3589
Richtung	ausgehend
Protokoll / Port	HTTPS / TCP 443
Endpunkt / Beschreibung	iem.de
Übertragene Daten	FLOW Anwendung, Release Notes, Geräte-Firmware, Datenschutzbestimmungen
Sicherheitsmaßnahmen	TLS 1.2+
Hinweise für Betreiber	1, 3

ABDM

IEM Mobil-O-Graph	
Ziel-ID	A2926
Richtung	Lokales I/O
Protokoll / Port	USB / UART
Endpunkt / Beschreibung	Externes Aufnahmegerät
Übertragene Daten	Zum Gerät beim Vorbereiten: Auftragsreferenz (Job-ID). Keine Patientennamen, keine Patienten-ID.
Sicherheitsmaßnahmen	-
Hinweise für Betreiber	4

Holter

IEM HeartX Holter	
Ziel-ID	A4585
Richtung	Lokales I/O
Protokoll / Port	USB
Endpunkt / Beschreibung	Externes Aufnahmegerät
Übertragene Daten	Zum Gerät beim Vorbereiten: Auftragsreferenz (Job-ID), Geburtsdatum auf den Monat gerundet, Geschlecht, Herzschrittmacher-Kennzeichen, Aufnahmedauer. Keine Patientennamen, keine Patienten-ID.
Sicherheitsmaßnahmen	-

IEM HeartX Holter	
Hinweise für Betreiber	4

Azure-Speicher / Hochladen von Holter-Messungen	
Ziel-ID	A5078
Richtung	ausgehend
Protokoll / Port	HTTPS / TCP 443
Endpunkt / Beschreibung	gtmhxhcustomers05.blob.core.windows.net
Übertragene Daten	EKG-Messsignal, Auftragsreferenz (Job-ID), Geburtsdatum auf den Monat gerundet, Geschlecht, Herzschrittmacher-Kennzeichen; dazu die Logdatei des Recorders. Keine Patientennamen, keine Patienten-ID.
Sicherheitsmaßnahmen	TLS 1.2+
Hinweise für Betreiber	1, 2

ECG AI backend	
Ziel-ID	A4588
Richtung	ausgehend
Protokoll / Port	HTTPS / TCP 443
Endpunkt / Beschreibung	hxh-api.prod.heartxholter.com
Sicherheitsmaßnahmen	TLS 1.2+
Hinweise für Betreiber	1, 2

Webviewer	
Ziel-ID	A5072
Richtung	ausgehend
Protokoll / Port	HTTPS / TCP 443
Endpunkt / Beschreibung	heartxholter.com
Sicherheitsmaßnahmen	TLS 1.2+
Hinweise für Betreiber	1, 3

1. Internetverbindung mit Port 443 erforderlich.
2. Verbindung wird von FLOW selbst aufgebaut. Jede TLS-Unterbrechung nach Art eines Man-in-the-Middle, die das ursprüngliche Serverzertifikat ersetzt, führt dazu, dass FLOW die Verbindung ablehnt. Der resultierende Fehler ist typischerweise ein Java-PKIX-Fehler bei der Prüfung des Zertifikatspfads. In der Fehlermeldung von FLOW und in der Logdatei lautet er zum Beispiel „PKIX path building failed“. Diese Verbindungen müssen ausdrücklich von der SSL/TLS-Inspektion ausgenommen und unverändert durchgeleitet werden, sodass die ursprüngliche Ende-zu-Ende-TLS-Sitzung und die Zertifikatskette erhalten bleiben. FLOW prüft Serverzertifikate anhand der mit der Anwendung ausgelieferten Zertifikatsliste, nicht anhand des Zertifikatsspeichers des Betriebssystems; eigene Zertifikate, etwa die CA eines Proxys, können nicht hinterlegt werden. FLOW bietet keine Proxy-Einstellung; die so gekennzeichneten Ziele müssen vom Arbeitsplatz direkt oder über einen transparenten Proxy ohne TLS-Entschlüsselung erreichbar sein.

3. Aufruf im Systembrowser des Arbeitsplatzes. Es gelten Zertifikatsprüfung und Proxy-Einstellungen des Browsers; eine Ausnahme von der SSL/TLS-Inspektion ist hier nicht erforderlich.
4. Sicherer physischer USB-Anschluss.

2.4.1 Einrichtung der Holter-Schnittstelle

Voraussetzung: HeartX Recorder (GTIN: 04250903203176) und Account für Webviewer

Um die Schnittstelle zum KI-Auswerteservice für den HeartX Recorder einzurichten, gehen Sie wie folgt vor:

- Melden Sie sich mit Ihrem Account im Webviewer an
- Öffnen Sie die Einstellungen (Zahnrad)
- Klicken Sie auf den Eintrag “IEM Integration”
- Erstellen Sie ein Token mit einem Klick auf Create Token. Es wird automatisch eine .token Datei heruntergeladen.
- Hinterlegen Sie die Datei in den Einstellungen zum HeartX. Die Dateibenennung muss unverändert bleiben!

2.4.2 GDT

FLOW bietet Betreibern die Möglichkeit, eine Datenschnittstelle zu einem Praxisverwaltungssystem (PVS) oder Krankenhausinformationssystem (KIS) unter Verwendung des GDT 2.1-Standards (Gerätedatentransfer) zu konfigurieren.

Damit FLOW einen Job aus dem gewünschten System annehmen und verwerten kann, sind die Informationen folgender Codes in der Datei erforderlich, die an FLOW gesendet wird:

- 3000 - Patientenkennung
- 8000 - erwarteter Wert “6302”
- 8402 - erwarteter Wert:
  - für ABDM “BDM01”
  - für Holter “EKG04”

Zeichensatz

Der eingestellte Zeichensatz muss dem entsprechen, den das sendende System beim Schreiben der GDT-Datei verwendet. Enthält die Datei den Code 9206 (Zeichensatz), richtet sich FLOW danach. Fehlt der Code oder entspricht er keinem der Werte in der folgenden Tabelle, wird der in den Einstellungen hinterlegte Zeichensatz verwendet.

Code 9206	Einstellung	Zeichensatz
1	ASCII	7-Bit-ASCII - enthält keine Umlaute
2	IBM437	DOS-Zeichensatz
3	ISO-8859-1	Latin-1, üblich in Windows-Umgebungen

Eine falsche Einstellung wirkt sich unterschiedlich aus:

- Mit “ASCII” werden alle Umlaute und Sonderzeichen durch “?” ersetzt, da dieser Zeichensatz sie nicht enthält - aus “Schröder” wird “Schr?der”. Wählen Sie ASCII nur, wenn Ihr PVS/KIS die Dateien tatsächlich so schreibt.
- Bei einer Verwechslung von “IBM437” und “ISO-8859-1” erscheint kein “?”. Umlaute werden stattdessen als falsche Zeichen dargestellt - aus “Schröder” wird dann z. B. “Schr÷der”.

Werden Zeichen im Report falsch dargestellt oder erscheinen “?”, entnehmen Sie den zu verwendenden Zeichensatz dem Handbuch Ihres PVS/KIS.

Die GDT-Spezifikation definiert nur die Dateistruktur und Semantik, enthält jedoch keine Sicherheitsmechanismen wie Verschlüsselung, Authentifizierung oder Integritätsschutz. Der Datenaustausch erfolgt über gemeinsam genutzte Verzeichnisse („GDT-Austauschordner"). Der Betrieb und Schutz dieser Verzeichnisse liegt in der Verantwortung des Betreibers (z. B. der Arztpraxis oder des IT-Dienstleisters). Die Anwendung unterstützt den Datenaustausch streng innerhalb der GDT-Spezifikation. End-to-End-Sicherheitsmechanismen (wie Verschlüsselung oder digitale Signaturen) sind nicht Teil des Standards und daher nicht implementiert.

Um einen sicheren und konformen Betrieb zu gewährleisten, muss der Betreiber folgende Maßnahmen ergreifen:

- Zugangskontrollmaßnahmen implementieren. Nur autorisierte Stellen dürfen auf die HIS-GDT-Schnittstelle zugreifen.
- Die Integrität und Vertraulichkeit der GDT-Dateiübertragungen sicherstellen.
- Speicherte Informationen durch Verschlüsselung und technische Sicherheitsvorkehrungen schützen.
- Die Protokollierung und Überwachung des GDT-Austauschs zur Rechenschaftspflicht aufrechterhalten.
- Angemessene Sicherungs- und Wiederherstellungsmechanismen bereitstellen, um die Verfügbarkeit der ausgetauschten GDT-Dateien zu gewährleisten.

Hinweise zur Konfiguration des PVS

Das HIS/KIS muss nach Verarbeitung/Import der GDT Datei die GDT Datei und die ggf. damit verbundenen und importierten Berichte löschen.

Wichtig: Ein Löschen weiterer in dem Verzeichnis vorhandenen Dateien kann zu Datenverlust und Fehlfunktionen führen.

Achtung

Multi room

Die Funktion “Multi room” ermöglicht es, dass mehrere Software-Instanzen auf dieselben Jobdaten zugreifen können.

Stellen Sie dafür sicher, dass in allen Instanzen, die über Multi room verbunden werden sollen, folgende Einstellungen übereinstimmen:

- GDT Modus eingeschaltet
- Zeichensatz Encoding
- Import- und Exportverzeichnisse
  Es müssen die gleichen Verzeichnisse eingestellt sein, die für den jeweiligen Arbeitsplatz auch als Austauschordner für das PVS/KIS konfiguriert wurden.

2.4.3 HL7

FLOW bietet Betreibern die Möglichkeit, eine Datenschnittstelle zu einem Praxisverwaltungssystem (PVS) oder Krankenhausinformationssystem (KIS) auf Basis von HL7 v2 zu konfigurieren. Der Austausch erfolgt dateibasiert: Das sendende System legt Aufträge als Nachrichtendateien in einem Importverzeichnis ab, FLOW schreibt die Ergebnisnachricht zu einem abgeschlossenen Auftrag in ein Exportverzeichnis. Eine Netzwerkanbindung (z. B. MLLP) ist nicht Bestandteil dieser Version.

GDT und HL7 können gleichzeitig eingeschaltet sein. Ein Auftrag wird immer über die Schnittstelle exportiert, über die er hereingekommen ist.

Einstellungen

Die HL7-Seite unter ***Interfaces*** enthält die folgenden Bedienelemente. Alle übrigen Werte der Schnittstelle sind vorgegeben und über die Oberfläche nicht einstellbar; sie sind im nächsten Abschnitt aufgeführt.

Einstellung	Bedeutung
HL7-Modus	Schaltet die Schnittstelle ein und aus. Bestehende Aufträge behalten den Modus, mit dem sie angelegt wurden, bis sie abgeschlossen sind.
Importverzeichnis	Verzeichnis, in das das sendende System die Aufträge schreibt
Exportverzeichnis	Verzeichnis, in das FLOW die Ergebnisnachrichten schreibt
Quarantäneverzeichnis	Verzeichnis, in dem FLOW nicht verarbeitbare Nachrichten aufbewahrt
Dokumentverzeichnis	Verzeichnis, in das FLOW den Bericht als PDF kopiert - nur im Dokumentmodus „File Reference"
Dokumentmodus	„Embedded": Der Bericht wird in die Nachricht eingebettet. „File Reference": Die Nachricht enthält nur den Pfad zur PDF-Datei.

Bei eingeschaltetem HL7-Modus müssen Import-, Export- und Quarantäneverzeichnis gesetzt sein, im Dokumentmodus „File Reference" zusätzlich das Dokumentverzeichnis. FLOW benötigt für alle Verzeichnisse Lese- und Schreibrechte.

Der Dokumentmodus „File Reference" setzt voraus, dass Sender und Empfänger dasselbe Dateisystem sehen. Wählen Sie als Dokumentverzeichnis ein eigenes Verzeichnis, nicht das Exportverzeichnis: Aus dem Exportverzeichnis holt das Empfangssystem die Nachrichten ab und behandelt andere Dateien dort unter Umständen als Fremddateien, die es verschiebt oder löscht. Eine PDF-Datei im Exportverzeichnis kann so verschwinden, bevor das Empfangssystem den Pfad aus der Nachricht öffnet.

Achtung

Eigene Verzeichnisse

Die vier Verzeichnisse dürfen sich weder untereinander noch mit den GDT-Austauschordnern überschneiden.

FLOW verarbeitet **jede** reguläre Datei, die im Importverzeichnis erscheint, und löscht sie nach erfolgreicher Verarbeitung. Legen Sie dort deshalb keine anderen Dateien ab.

Vorgegebene Werte

Die folgenden Werte sind fest vorgegeben und können in der Oberfläche nicht geändert werden.

Parameter	Wert
Übertragungsweg	Dateiablage (File Drop)
Akzeptierter Nachrichtentyp (Eingang)	ORM^O01
Unterstützte HL7-Versionen (Eingang)	2.3, 2.3.1, 2.4, 2.5, 2.5.1
Nachrichtentyp (Ausgang)	ORU^R01
Kodierung	ER7 (Pipe-Format)

Parameter	Wert
Zeichensatz (Eingang)	Aus MSH-18, ersatzweise UTF-8
Zeichensatz (Ausgang)	UTF-8, in MSH-18 als UNICODE UTF-8 angegeben
HL7-Version (Ausgang)	Die Version des beantworteten Auftrags, ersatzweise 2.4
Sendende Anwendung / Einrichtung	MSH-3 = FLOW, MSH-4 = IEM
Empfangende Anwendung / Einrichtung	MSH-5 und MSH-6 aus MSH-3 und MSH-4 des eingegangenen Auftrags, ersatzweise HIS und HOSPITAL
Untersuchungscodes ABDM (OBR-4)	ABPM, 24h-RR, 24h Blutdruckmessung
Untersuchungscodes Holter (OBR-4)	HOLTER, LZ-EKG, 24h Langzeit-EKG
Strenge Validierung	Abgeschaltet
Dateiname (Ausgang)	Die Nachrichtenkennung MSH-10 mit der Endung .hl7

Die empfangende Anwendung ist damit kein fester Wert: FLOW antwortet an die Anwendung, die den Auftrag geschickt hat. Nur wenn der eingegangene Auftrag dazu nichts sagt, werden die Ersatzwerte verwendet.

Anforderungen an den eingehenden Auftrag

Damit FLOW einen Auftrag annehmen und verwerten kann, muss die Nachricht die folgenden Bedingungen erfüllen. Ist eine davon verletzt, wird die Nachricht abgewiesen und in das Quarantäneverzeichnis verschoben.

- Der Nachrichtentyp in MSH-9 ist ORM^O01.
- Die in MSH-12 angegebene HL7-Version ist eine der unterstützten Versionen.
- Die Nachricht enthält genau einen Auftrag. Nachrichten mit mehreren Aufträgen werden abgewiesen.
- Die Auftragsart in ORC-1 ist NW (neuer Auftrag). Stornierungen (CA) und Änderungen (XO) werden abgewiesen.
- Die Auftragsnummer in ORC-2 oder OBR-2 ist gesetzt. Die Ergebnisnachricht gibt sie zurück; ohne sie kann das empfangende System das Ergebnis keinem Auftrag zuordnen.
- Der Untersuchungscode in OBR-4 ist einem der oben genannten Codes zugeordnet. FLOW vergleicht den Code und den Anzeigetext, ohne Berücksichtigung der Groß- und Kleinschreibung.

Aus der Nachricht liest FLOW die folgenden Felder:

Feld	Herkunft
Patientenkennung	PID-2, ersatzweise PID-3
Name, Vorname	PID-5.1, PID-5.2
Geburtsdatum	PID-7
Geschlecht	PID-8
Untersuchung	OBR-4 (Code und Anzeigetext)
Termin	OBR-36, ersatzweise TQ1-7
Auftragsnummer	ORC-2, ersatzweise OBR-2
Fallnummer	PV1-19

Feld	Herkunft
Anfordernder Arzt	ORC-12.2, ersatzweise OBR-16.2
Absender	MSH-3, MSH-4

Den Termin trägt FLOW beim Anlegen in das Feld ***Geplant für*** des Auftrags ein. Nennt die Nachricht keinen Termin, bleibt das Feld leer und kann in FLOW gesetzt werden. OBR-6 (gewünschter Zeitpunkt) und ORC-15 (Beginn der Gültigkeit) liest FLOW nicht als Termin: beide benennen keinen vereinbarten Zeitpunkt, und ORC-15 enthält bei vielen Absendern schlicht den Moment der Auftragserfassung.

Ein Zeitstempel darf seinen UTC-Versatz angeben (20260728093000+0200). Fehlt er, liest FLOW die Angabe als Ortszeit des Rechners, auf dem es läuft.

Zeichensatz

Der Zeichensatz des eingehenden Auftrags richtet sich nach dem Feld MSH-18. Dort stehen die Kennungen der HL7-Tabelle 0211, nicht die gebräuchlichen Namen der Zeichensätze. FLOW unterstützt die Werte ASCII, 8859/1, 8859/15, UNICODE und UNICODE UTF-8.

- Ist MSH-18 leer, verwendet FLOW UTF-8.
- Nennt MSH-18 einen Zeichensatz, den FLOW nicht kennt, wird die Nachricht abgewiesen und in die Quarantäne verschoben. Ein Ersatzzeichensatz würde Umlaute und Sonderzeichen unbemerkt verfälschen. Das gilt auch für UTF-8: die Kennung für UTF-8 lautet UNICODE UTF-8.

Die Ergebnisnachricht schreibt FLOW in UTF-8 und gibt das in MSH-18 als UNICODE UTF-8 an.

Strenge Validierung

Die strenge Validierung nach HL7-Spezifikation ist abgeschaltet. FLOW prüft stattdessen gezielt die Felder, die es für den Auftrag benötigt - siehe „Anforderungen an den eingehenden Auftrag".

Die Ergebnisnachricht

Ist ein Auftrag abgeschlossen und ein Bericht vorhanden, schreibt FLOW eine Nachricht vom Typ ORU^R01 in das Exportverzeichnis. Sie enthält die Auftragsnummer aus dem ursprünglichen Auftrag (OBR-2), die Patientendaten, die Fallnummer (PV1-19) und den Bericht:

- Im Dokumentmodus „Embedded" steht das PDF Base64-kodiert in OBX-5.
- Im Dokumentmodus „File Reference" kopiert FLOW das PDF in das Dokumentverzeichnis, und OBX-5 enthält nur den Pfad dorthin.

Jede Nachricht erhält eine eigene Kennung (MSH-10) und wird unter diesem Namen mit der Endung .hl7 abgelegt. FLOW schreibt die Datei zunächst mit der Endung .tmp und benennt sie anschließend um, sodass der Empfänger nie eine halb geschriebene Nachricht sieht. Eine Bestätigung (ACK) wird nicht erwartet.

Kann FLOW die Nachricht nicht schreiben - etwa weil das Exportverzeichnis nicht erreichbar ist -, bleibt der Auftrag zum Versand vorgemerkt und wird alle 20 Sekunden erneut versucht. Steht er länger als fünf Minuten an, meldet FLOW ihn in der Auftragsliste als fehlgeschlagene Übertragung.

Wird ein Auftrag erneut exportiert, entsteht eine weitere Datei mit einer eigenen Kennung. Eine zuvor geschriebene Nachricht wird dabei nicht überschrieben.

Quarantäne

Nachrichten, die FLOW nicht verarbeiten kann, werden nicht gelöscht, sondern in das Quarantäneverzeichnis verschoben. So bleibt die Schnittstelle für die folgenden Aufträge offen, und ein Auftrag verschwindet nicht unbemerkt. Den Grund führt FLOW im Anwendungsprotokoll auf.

FLOW räumt das Quarantäneverzeichnis zu keinem Zeitpunkt selbst auf. Prüfen Sie es regelmäßig, und lassen Sie Aufträge, die durch eine Fehlkonfiguration abgewiesen wurden, nach deren Behebung vom sendenden System erneut schicken.

Sicherheit und Pflichten des Betreibers

Die HL7-v2-Spezifikation definiert nur den Aufbau und die Semantik der Nachrichten, enthält jedoch keine Sicherheitsmechanismen wie Verschlüsselung, Authentifizierung oder Integritätsschutz. Der Datenaustausch erfolgt über gemeinsam genutzte Verzeichnisse (Import-, Export-, Quarantäne- und Dokumentverzeichnis). Der Betrieb und Schutz dieser Verzeichnisse liegt in der Verantwortung des Betreibers (z. B. der Arztpraxis oder des IT-Dienstleisters). Die Anwendung unterstützt den Datenaustausch streng innerhalb der HL7-v2-Spezifikation. End-to-End-Sicherheitsmechanismen (wie Verschlüsselung oder digitale Signaturen) sind nicht Teil des Standards und daher nicht implementiert.

Um einen sicheren und konformen Betrieb zu gewährleisten, muss der Betreiber folgende Maßnahmen ergreifen:

- Zugangskontrollmaßnahmen implementieren. Nur autorisierte Stellen dürfen auf die HL7-Schnittstelle und die dafür genutzten Verzeichnisse zugreifen.
- Die Integrität und Vertraulichkeit der übertragenen HL7-Nachrichten sicherstellen.
- Gespeicherte Informationen durch Verschlüsselung und technische Sicherheitsvorkehrungen schützen. Das gilt auch für das Quarantäneverzeichnis und - im Dokumentmodus „File Reference" - für das Dokumentverzeichnis: Beide enthalten Patientendaten bzw. vollständige Berichte.
- Die Protokollierung und Überwachung des HL7-Austauschs zur Rechenschaftspflicht aufrechterhalten.
- Angemessene Sicherungs- und Wiederherstellungsmechanismen bereitstellen, um die Verfügbarkeit der ausgetauschten Nachrichten zu gewährleisten.
- Das Quarantäneverzeichnis regelmäßig sichten und geordnet leeren. FLOW bewahrt dort jede Nachricht auf, die es nicht verarbeiten konnte, und löscht sie zu keinem Zeitpunkt selbst.
- Für die HL7-Schnittstelle ausschließlich eigene Verzeichnisse einrichten. FLOW verarbeitet jede reguläre Datei, die im Importverzeichnis erscheint; die vier Verzeichnisse dürfen sich daher weder untereinander noch mit den GDT-Austauschordnern überschneiden.

Hinweise zur Konfiguration des Empfangssystems

Das empfangende System muss die Ergebnisnachricht nach Verarbeitung bzw. Import aus dem Exportverzeichnis löschen. FLOW löscht dort nichts.

Im Dokumentmodus „File Reference" gilt das auch für die Berichte im Dokumentverzeichnis. Das empfangende System muss die PDF-Datei über den in OBX-5 genannten Pfad abholen, solange sie dort liegt.

Das sendende System sollte Aufträge atomar in das Importverzeichnis schreiben, also unter einem temporären Namen anlegen und anschließend umbenennen. FLOW überspringt Dateien mit den Endungen .tmp und .part; eine unvollständige Datei unter ihrem endgültigen Namen landet dagegen in der Quarantäne.