RadioWeb

Administrationshandbuch

Version 1.1.10, 2026-11-24

Inhalt

Übersicht 1
- Die Kapitel im Überblick 1
- Begriffe 1

Installation 2
- Systemanforderungen 2
- Ersteinrichtung 3

Anmeldung und Übersicht 6
- Anmelden 6
- Navigation 6
- Übersicht (Dashboard) 6

Anmeldung & Sicherheit 8
- Zweiten Faktor einrichten 8
- Backup-Codes 12
- Anmelden mit zweitem Faktor 13
- Faktoren verwalten 14
- Gerät verloren 14
- Anmeldefaktoren eines Benutzers zurücksetzen 14
- Notfall: kein Administrator kann sich anmelden 15
- Hinweise für den Betrieb 15

Stammdaten 17
- Kunden 17
- Überweiser 18
- Benutzer 20

Tokens 23
- Integrations-Tokens 23
- QR-Code-Import 24
- Freigaben 25

Admin 28
- Import Status 28
- Ausdruck-Vorlagen 28
- Sprachverwaltung 42
- Audit-Log 44
- Archive 45
- HL7-Kommunikation 46
- DirectView 56
- Lizenz & Module 61
- Einstellungen 63

Customer-Bereich 65
- Freigaben 65

Zugangscodes erstellen 66
Voraufnahmen hochladen (Upload) 67
Portal Import (DLX) 68
ZIP-Upload 68
Fortschritt verfolgen 68
Einrichtung 69
Betrieb 69
Integration 71
Overview 71
PACS: VEPRO 72
RIS: Mesalvo 74
GDT/HL7: gdt-hl7-bridge 76
Portal-Launch 103

Übersicht

Dieses Handbuch richtet sich an Administratoren des Patientenportals und an Customer (Praxis oder Klinik), die das Portal für ihre Überweiser und Patienten betreiben.

Die Kapitel im Überblick

Installation

Systemanforderungen und das Formular für die Ersteinrichtung.

Anmeldung und Übersicht

Anmeldung, Aufbau der Navigation und das Dashboard mit den wichtigsten Kennzahlen.

Stammdaten

Kunden, Überweiser und Benutzer mit Rollen.

Tokens

Integrations-Tokens für Fremdsysteme, QR-Code-Import und die Freigaben-Verwaltung.

Admin

Import Status, Ausdruck-Vorlagen, Sprachverwaltung, Audit-Log, Archive und Einstellungen.

Customer-Bereich

Funktionen für Praxen und Kliniken.

Integration

Anbindung von PACS (VEPRO), RIS (Mesalvo) und PVS (gdt-hl7-bridge, Portal-Launch).

Begriffe

Begriff	Bedeutung
Kunde (Customer)	Radiologische Praxis/Klinik oder Standort, für den das Portal betrieben wird
Überweiser (Referrer)	Überweisende Ärztin, überweisender Arzt oder Praxis
Freigabe / Zugangscode (Token)	Zeitlich begrenzter Zugang zu Untersuchungen im Format `XXXX-XXXX-XXXX`, meist mit QR-Code
Integrations-Token	Langlebiger Zugangsschlüssel für ein Fremdsystem (PACS, PVS)
DICOM-Wert	Wert in den DICOM-Bilddaten, über den Kunden (InstitutionName) und Überweiser (ReferringPhysicianName) ihren Studien zugeordnet werden

Installation

Systemanforderungen

Hier finden Sie die empfohlenen Systemanforderungen für das Patientenportal, basierend auf der Anzahl der gleichzeitigen Nutzer und dem gewählten Betriebsmodus.

Hardware-Szenarien

Die Hardware-Anforderungen richten sich primär nach der Anzahl der gleichzeitigen Nutzer.

Szenario	Gleichzeitige Nutzer	RAM	CPU
Klein	5–10	8 GB	4 vCPU
Mittel	10–20	16 GB	6–8 vCPU
Höher	20–50	32 GB	12–16 vCPU

Speicherbedarf

Modus: Query/Retrieve (Empfohlen)

Generell wird empfohlen, dass das Patientenportal im **Query/Retrieve (Q/R)** Modus arbeitet. Dabei werden alle Daten bei Bedarf direkt vom PACS abgefordert.

- **Speicherbedarf**: Dient nur als Cache.
- **Empfehlung**: ca. **1 TB** (500 GB System + 500 GB Cache).

Modus: DICOM Store (Datenhaltung im Portal)

Wenn die Daten aktiv an das Patientenportal gesendet und dort gespeichert werden sollen, gelten folgende Schätzwerte für den Speicherbedarf.

Vorhaltezeit 3 Monate (~90 Tage)

Größe	Datenaufkommen	Rohdaten (90 Tage)	Empfohlene SSD (ca.)
Klein	5–10 GB/Tag	450–900 GB (0,45–0,9 TB)	**2 TB**
Mittel	20–50 GB/Tag	1,8–4,5 TB	**6 TB**
Groß	50–100 GB/Tag	4,5–9 TB	**12 TB**

Vorhaltezeit 6 Monate (~180 Tage)

Größe	Datenaufkommen	Rohdaten (180 Tage)	Empfohlene SSD (ca.)
Klein	5–10 GB/Tag	900–1.800 GB (0,9–1,8 TB)	**4 TB**
Mittel	20–50 GB/Tag	3,6–9 TB	**12 TB**
Groß	50–100 GB/Tag	9–18 TB	**24 TB**

Ersteinrichtung

Bitte füllen Sie das folgende Formular für die Ersteinrichtung des Patientenportals aus.

1. Netzwerkdaten

Netzwerkdaten für das Patientenportal im lokalen Netz:

Parameter	Wert
IP-Adresse	
Subnetzmaske	
Gateway	
DNS-Server	

2. DICOM Parameter / Betriebsmodi

DICOM Dienste (Store / ECHO)

Parameter	Standardwert	Ihr Wert
TCP Port für DICOM-Dienste vom Portal	4104	

AET für Patientenportal

Parameter	Standardwert	Ihr Wert
AET Title	RADIOWEB	

Betriebsmodi

Bitte wählen Sie den gewünschten Betriebsmodus (a oder b).

a) Query/Retrieve (Empfohlen)

Das Portal ruft Bilder aktiv vom PACS ab.

Parameter	Wert
IP-Adresse (Remote PACS)	

Port (Remote PACS)	
AET (Remote PACS)	

b) DICOM Store

Das PACS sendet Bilder aktiv an das Portal.

Parameter	Wert
AET für DICOM Store (Remote PACS)	

3. Mail-Einstellungen

Für den Versand von E-Mails (z.B. Token-Versand) werden folgende SMTP-Daten benötigt:

Parameter	Beschreibung	Ihr Wert
`email.smtp.host`	SMTP Server Hostname (z.B. smtp.gmail.com)	
`email.smtp.port`	SMTP Server Port (z.B. 587)	
`email.smtp.username`	SMTP-Benutzername	
`email.smtp.password`	SMTP-Passwort	
`email.from.address`	Absender-E-Mail-Adresse	
`email.from.name`	Absendername	

4. Token Sicherheit

Konfiguration der Berechtigungen für die Erstellung von Zugriffs-Tokens.

Berechtigungen

Wer darf erzeugen?	Überweiser	Patient	Studie	Keine
PACS Anwender (Customer)	☐	☐	☐	☐
Überweiser (Referrer)	☐	☐	☐	☐
Patient	☐	☐	☐	☐
Studienzugang (Study)	☐	☐	☐	☐

Legende:

- **Überweiser**: Alle Patienten und Studien von einem Überweiser
- **Patient**: Alle Studien eines Patienten (ohne für jede Studie eine neue Freigabe erzeugen zu müssen)
- **Studie**: Freigabe auf Studienebene
- **Keine**: Darf keine weiteren Freigaben erzeugen

Konfigurationsoptionen

Für jeden Token-Typ (Patient, Überweiser, Studie) können folgende Parameter eingestellt werden:

Patient

Einstellung	Editierbar (Anwender entscheidet)	Fester Standardwert (wenn nicht editierbar, bitte nur EINE Option wählen)
Authentifizierung	☐ Ja	☐ Geburtsdatum ☐ Passwort ☐ Keine
Standard Gültigkeitsdauer	☐ Ja	☐ Unbegrenzt ☐ 7 Tage ☐ 14 Tage ☐ 30 Tage ☐ 60 Tage ☐ 90 Tage ☐ 180 Tage ☐ 365 Tage

Überweiser (Referrer)

Einstellung	Editierbar (Anwender entscheidet)	Fester Standardwert (wenn nicht editierbar, bitte nur EINE Option wählen)
Authentifizierung	☐ Ja	☐ Passwort ☐ Keine
Standard Gültigkeitsdauer	☐ Ja	☐ Unbegrenzt ☐ 7 Tage ☐ 14 Tage ☐ 30 Tage ☐ 60 Tage ☐ 90 Tage ☐ 180 Tage ☐ 365 Tage

Studie (Study)

Einstellung	Editierbar (Anwender entscheidet)	Fester Standardwert (wenn nicht editierbar, bitte nur EINE Option wählen)
Authentifizierung	☐ Ja	☐ Geburtsdatum ☐ Passwort ☐ Keine
Standard Gültigkeitsdauer	☐ Ja	☐ Unbegrenzt ☐ 7 Tage ☐ 14 Tage ☐ 30 Tage ☐ 60 Tage ☐ 90 Tage ☐ 180 Tage ☐ 365 Tage

Beispiel: Ein Patient möchte eine Studie teilen. Er erstellt einen `Study`-Token. Das System prüft `security.group.patient.allowedtokens` (enthält `study`). Die Authentifizierungsmethode wird durch `token.type.study.authentication` bestimmt (z.B. `BIRTHDATE` fordert das Geburtsdatum des Patienten zur Verifizierung). Die Gültigkeit wird durch `token.type.study.validity_days` voreingestellt.

Anmeldung und Übersicht

Anmelden

Administratoren melden sich auf der Anmeldeseite im Bereich **Anmelden** mit **E-Mail** und **Passwort** an (zeigt die Anmeldeseite nur den Zugangscode, über den Link **Mit Login anmelden** unter der Karte) und bestätigen die Anmeldung mit einem zweiten Faktor (Passkey, Authenticator-App oder Backup-Code, siehe Anmeldung & Sicherheit). Bei der ersten Anmeldung richten Sie diesen zweiten Faktor ein. Das erste Administratorkonto wird bei der Installation angelegt (siehe Installationsanleitung in der Entwicklerdokumentation); weitere Konten legen Sie unter Benutzer an.

Navigation

Die Kopfzeile fasst die Verwaltungsfunktionen in drei Menüs zusammen:



Abbildung 1. Kopfzeile im Admin-Bereich

Menü	Einträge
Stammdaten	Kunden, Überweiser, Benutzer
Tokens	Integrations-Tokens, QR-Code-Import, Freigaben
Admin	Import Status, Ausdruck-Vorlagen, Sprachverwaltung, Audit-Log, Archive, Einstellungen

Außerdem erreichen Sie über **Download** die Desktop- und Integrations-Apps, Beispiel-Vorlagen und die Handbücher.

Rechts in der Kopfzeile stehen vier Symbole:

- **Hilfe** (Fragezeichen): Kurzanleitung, FAQ, Handbücher und Kontakt,
- **Kontomenü** (Personen-Symbol): Ihre E-Mail-Adresse, Anmeldung & Sicherheit und **Logout**,
- **Sprache** (Flagge) und **Hell/Dunkel**.

Impressum und Datenschutz finden Sie am Ende jeder Seite, die Versionsnummer (mit Link zu den Versionshinweisen) oben rechts über der Kopfzeile.

Übersicht (Dashboard)

Nach der Anmeldung sehen Sie die **Übersicht** mit den wichtigsten Kennzahlen.

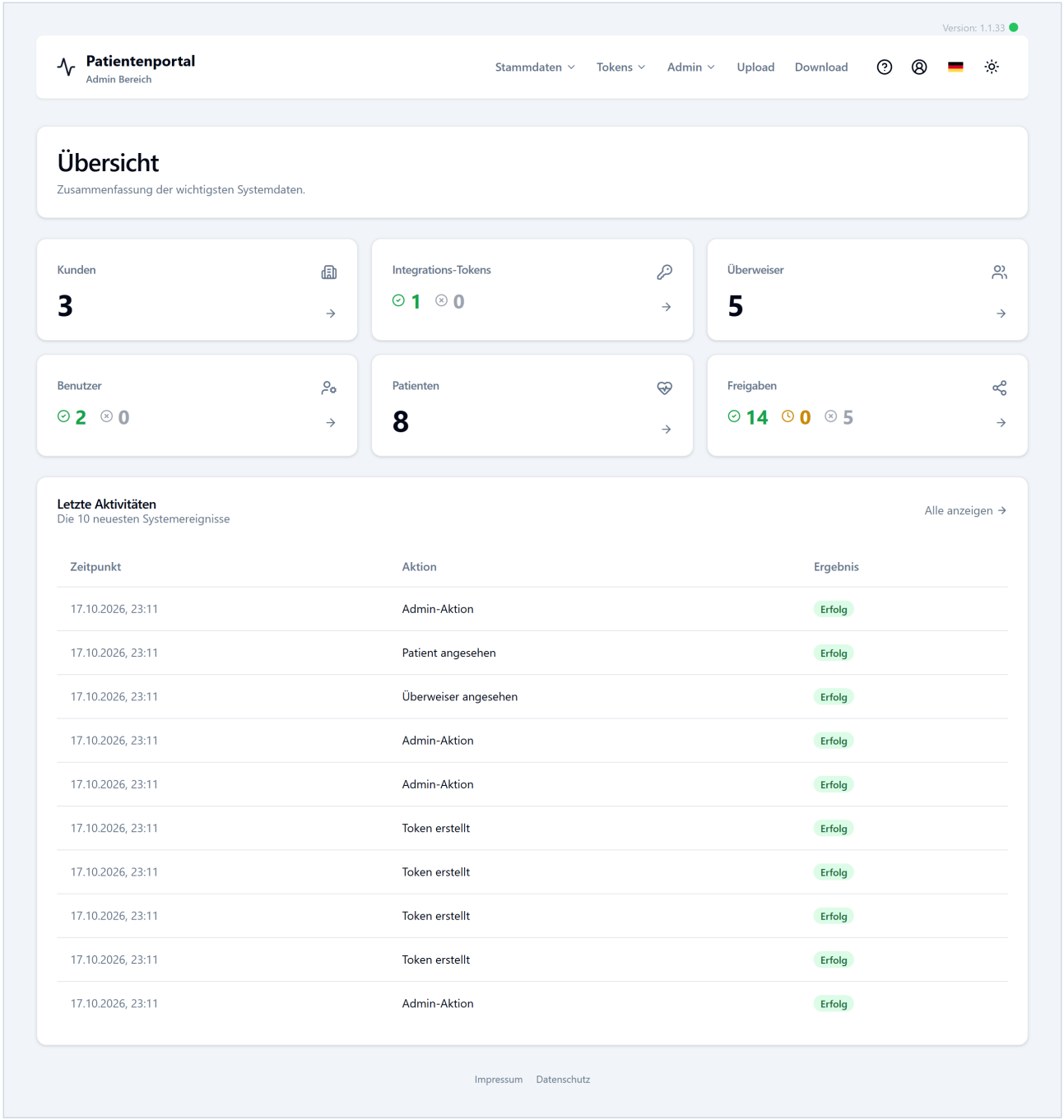


Abbildung 2. Übersicht nach der Anmeldung

- Die Kacheln zeigen die Anzahl der **Kunden**, **Überweiser**, **Patienten**, **Benutzer**, **Integrations-Tokens** und **Freigaben** – bei Tokens, Benutzern und Freigaben aufgeteilt in aktiv (grün), abgelaufen (gelb) und widerrufen bzw. inaktiv (grau). Ein Klick auf eine Kachel öffnet die zugehörige Verwaltung.
- **Letzte Aktivitäten** listet die zehn neuesten Einträge des Audit-Logs; **Alle anzeigen** öffnet das vollständige Protokoll.

Anmeldung & Sicherheit

Alle Anmeldungen mit E-Mail-Adresse und Passwort – Administratoren, Customer-Logins der Praxen sowie dauerhafte Logins von Überweisern und Patienten – erfordern einen zweiten Faktor (NIS2, Art. 21 Abs. 2j). Anmeldungen mit Zugangscode, Studienfreigabe oder Integrations-Token sind keine Benutzerkonten und davon nicht betroffen.

Zum Schutz der Gesundheitsdaten reicht für die Anmeldung mit **E-Mail und Passwort** das Passwort allein nicht aus: Jedes Konto braucht einen **zweiten Faktor**. Wer Ihr Passwort kennt, kann sich damit noch nicht anmelden.



Die Anmeldung mit einem **Zugangscode** (Freigabecode, Token) ist davon nicht betroffen und funktioniert wie bisher.

Als zweiter Faktor stehen zur Wahl:

Passkey (empfohlen)

Die Anmeldung wird mit Fingerabdruck, Gesichtserkennung oder der PIN Ihres Geräts bestätigt – ohne Code abzutippen und ohne zusätzliche App. Passkeys funktionieren mit aktuellen Smartphones, Tablets und Computern (Windows Hello, Apple Touch ID/Face ID, Android) sowie mit Sicherheitsschlüsseln. Sie können mehrere Passkeys anlegen, zum Beispiel für Smartphone und Arbeitsplatz-PC.

Passkeys gelten als besonders sicher, weil sie gegen Phishing geschützt sind: Ein Passkey funktioniert nur auf der echten Adresse des Portals und kann deshalb nicht über eine gefälschte Webseite abgegriffen werden – anders als ein Passwort oder ein abgetippter Code. Fingerabdruck und Gesichtsbild dienen nur dazu, den Passkey auf Ihrem Gerät freizugeben; sie verlassen das Gerät nicht und werden nicht an das Portal übertragen.

Authenticator-App

Eine kostenlose App auf dem Smartphone erzeugt alle 30 Sekunden einen neuen 6-stelligen Code, den Sie bei der Anmeldung eingeben. Das Portal empfiehlt **Microsoft Authenticator** und **Google Authenticator**; jede andere App nach dem gängigen Standard (TOTP) funktioniert ebenso.

Zusätzlich erhalten Sie beim ersten Faktor zehn **Backup-Codes** für den Notfall.

Zweiten Faktor einrichten

Bei der ersten Anmeldung mit E-Mail und Passwort öffnet das Portal automatisch die Seite **Anmeldung & Sicherheit** mit dem Hinweis **Bitte richten Sie einen zweiten Anmeldefaktor ein**. Er erklärt kurz, warum das nötig ist, und stellt die beiden Möglichkeiten vor. Solange kein zweiter Faktor eingerichtet ist, sind alle anderen Bereiche gesperrt. Später erreichen Sie die Seite jederzeit über das Kontomenü (Personen-Symbol oben rechts) unter **Anmeldung & Sicherheit**.

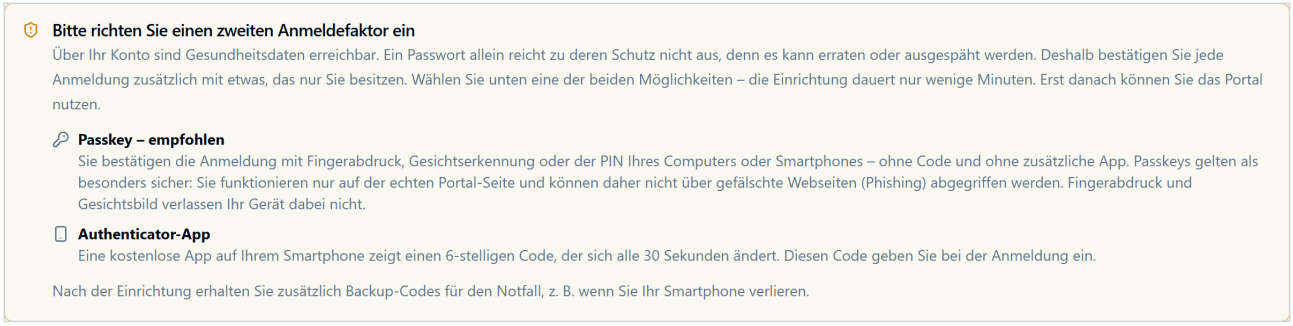


Abbildung 3. Hinweis bei der ersten Anmeldung

Richten Sie einen der beiden Faktoren ein – oder beide, dann haben Sie eine Ausweichmöglichkeit.

Passkey hinzufügen

1. Öffnen Sie **Anmeldung & Sicherheit** auf dem Gerät, mit dem Sie sich künftig anmelden möchten (Computer, Smartphone oder Tablet).
2. Klicken Sie unter **Passkeys** auf **Passkey hinzufügen**.
3. Übernehmen oder ändern Sie den vorgeschlagenen Namen (zum Beispiel „Laptop Büro“) – er hilft Ihnen später, die Passkeys auseinanderzuhalten. Geben Sie Ihr aktuelles Passwort ein und klicken Sie auf **Passkey erstellen**.

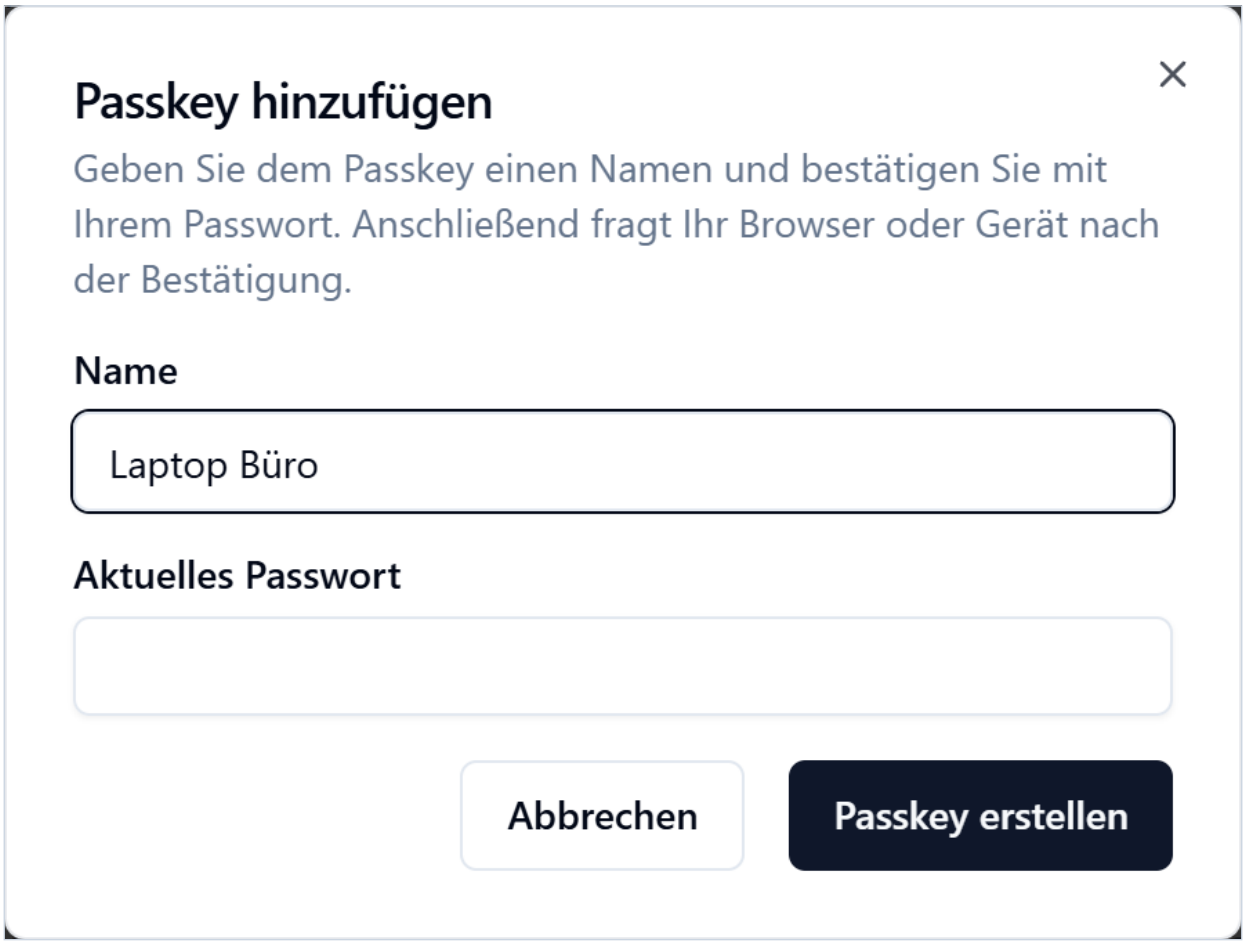


Abbildung 4. Passkey hinzufügen

4. Ihr Browser bzw. Betriebssystem öffnet nun ein eigenes Fenster. Je nach Gerät:

- **Windows:** Bestätigen Sie mit Windows Hello (Gesicht, Fingerabdruck oder Windows-PIN).
- **Mac, iPhone, iPad:** Bestätigen Sie mit Touch ID, Face ID oder dem Gerätecode. Der Passkey wird im iCloud-Schlüsselbund gespeichert.
- **Android:** Bestätigen Sie mit Fingerabdruck, Gesicht oder Displaysperre. Der Passkey wird im Google Passwortmanager gespeichert.
- **Passkey auf dem Smartphone speichern, obwohl Sie am Computer sitzen:** Wählen Sie im Fenster „Anderes Gerät verwenden“ bzw. „Smartphone oder Tablet“ und scannen Sie den angezeigten QR-Code mit dem Smartphone.

5. Der neue Passkey erscheint in der Liste. Die Kennzeichnung **synchronisiert** bedeutet, dass er über Ihr Apple- oder Google-Konto auch auf Ihren anderen Geräten verfügbar ist.

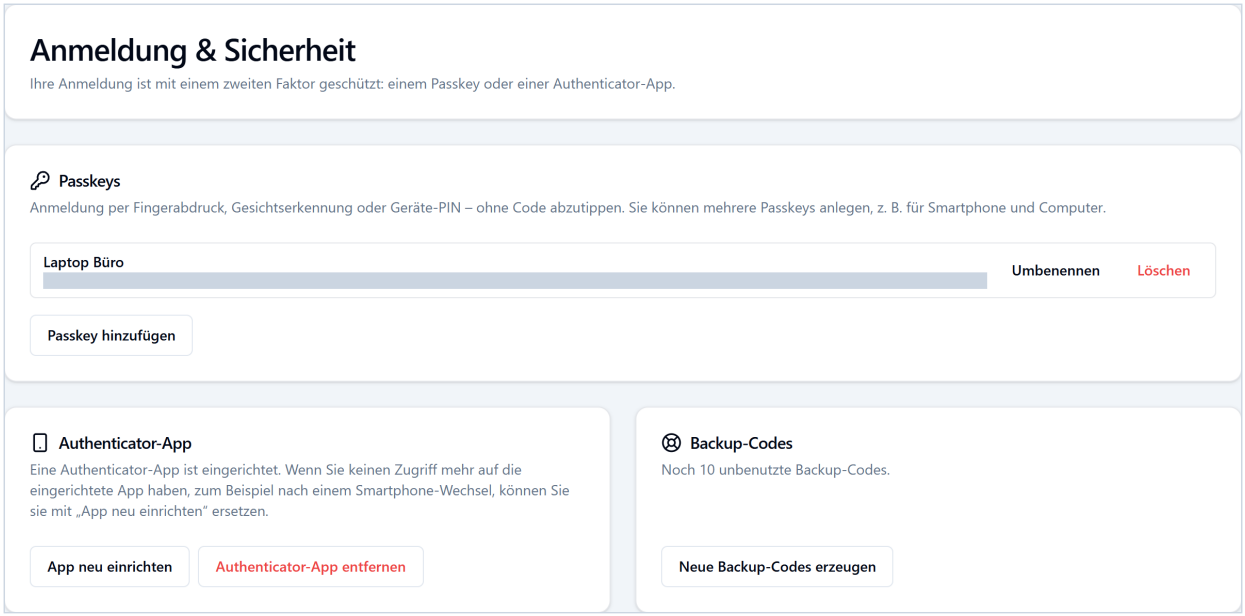


Abbildung 5. Passkeys, Authenticator-App und Backup-Codes auf der Seite Anmeldung & Sicherheit

Legen Sie für jedes Gerät, mit dem Sie sich regelmäßig anmelden, einen eigenen Passkey an – oder nutzen Sie einen synchronisierten Passkey. Fragt der Browser nach dem Speicherort, ist der Passwortmanager Ihres Geräts für die meisten Nutzer die einfachste Wahl.

Authenticator-App einrichten

1. Klicken Sie unter **Authenticator-App** auf **Authenticator-App einrichten** und geben Sie Ihr aktuelles Passwort ein. Die Einrichtung führt Sie in drei Schritten durch den Vorgang.



Abbildung 6. Einrichtung der Authenticator-App (QR-Code und Schlüssel sind hier verdeckt)

2. **App installieren:** Das Portal empfiehlt zwei kostenlose Apps, die es für Android und iPhone gibt: **Microsoft Authenticator** und **Google Authenticator**. Wählen Sie Ihr Smartphone (Android oder iPhone) und scannen Sie den QR-Code der gewünschten App mit der Kamera Ihres Smartphones – er öffnet die App im Google Play Store bzw. App Store. Öffnen Sie das Portal auf dem Smartphone selbst, führen die Links direkt in den Store. Eine bereits vorhandene Authenticator-App können Sie weiterverwenden.
3. **Konto hinzufügen:** Tippen Sie in der App auf „+“ bzw. „Konto hinzufügen“ und scannen Sie den QR-Code im Portal. Lässt sich der Code nicht scannen, tragen Sie den darunter angezeigten Schlüssel in der App von Hand ein. Auf dem Smartphone öffnet **Direkt in der Authenticator-App öffnen** die App ohne Scannen. Die App zeigt danach den Eintrag „RadioWeb Patientenportal“.
4. **Code eingeben:** Geben Sie den 6-stelligen Code ein, den die App gerade anzeigt, und klicken Sie auf **Bestätigen**. Der Code wechselt alle 30 Sekunden – nehmen Sie einfach den aktuellen.



Wählen Sie eine App mit Sicherungsfunktion (bei Microsoft und Google über Ihr Konto), dann bleiben die Einträge auch bei einem neuen Smartphone erhalten.

Backup-Codes

Nach dem ersten Faktor zeigt das Portal einmalig zehn Backup-Codes an (Format `XXXXX-XXXXX`). Mit einem Backup-Code können Sie sich anmelden, wenn Sie Passkey und App gerade nicht verwenden können – zum Beispiel nach dem Verlust des Smartphones.

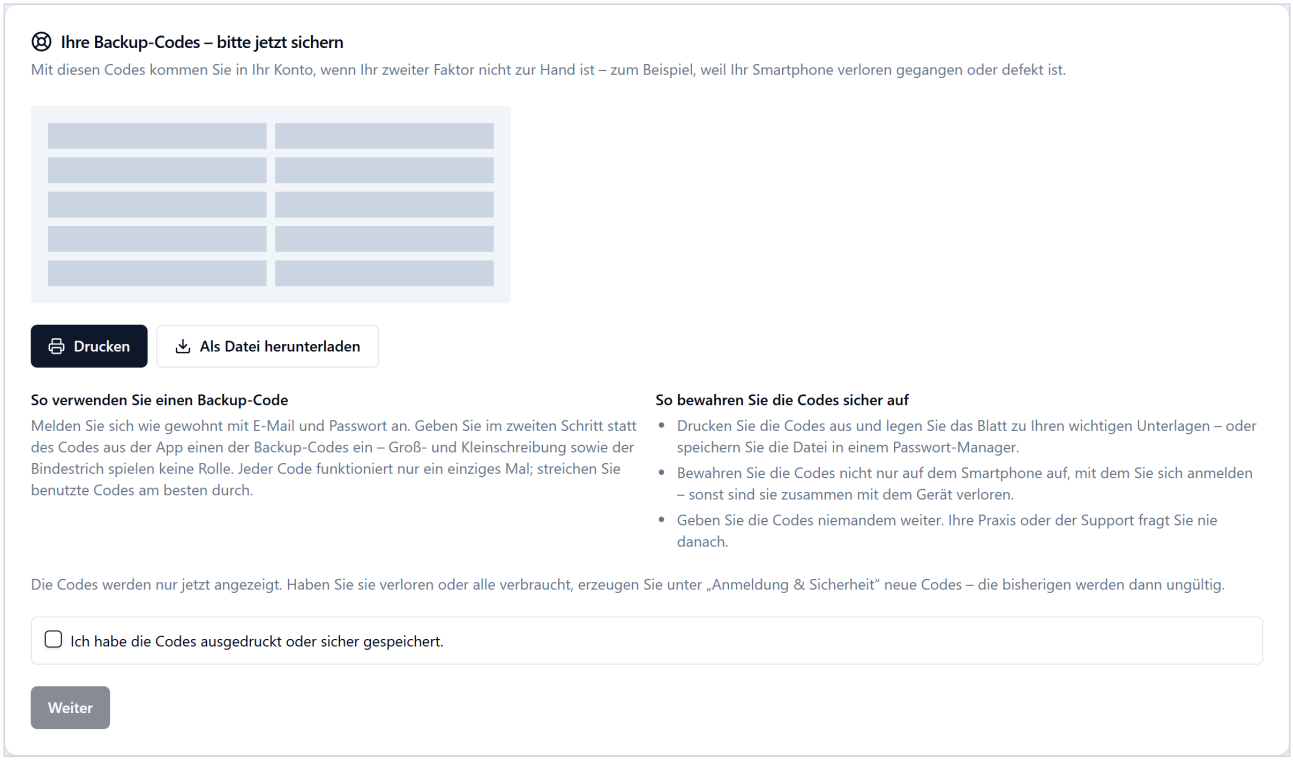


Abbildung 7. Backup-Codes nach der Einrichtung (Codes hier verdeckt)

Backup-Code verwenden

Melden Sie sich wie gewohnt mit E-Mail und Passwort an und geben Sie im zweiten Schritt statt des App-Codes einen Backup-Code ein. Groß- und Kleinschreibung sowie der Bindestrich spielen keine Rolle. Jeder Code funktioniert genau einmal – streichen Sie benutzte Codes am besten durch.

Backup-Codes sicher aufbewahren

- Klicken Sie auf **Drucken** und legen Sie das Blatt zu Ihren wichtigen Unterlagen – oder laden Sie die Codes mit **Als Datei herunterladen** herunter und speichern Sie die Datei in einem Passwort-Manager. Ausdruck und Datei enthalten auch eine kurze Anleitung.
- Bewahren Sie die Codes nicht nur auf dem Smartphone auf, mit dem Sie sich anmelden – sonst sind sie zusammen mit dem Gerät verloren.
- Geben Sie die Codes niemandem weiter. Die Praxis oder der Support fragt nie nach Ihren Backup-Codes.

Erst wenn Sie bestätigen, dass Sie die Codes ausgedruckt oder sicher gespeichert haben, geht es mit **Weiter** zurück zur Übersicht. Die Seite zeigt danach an, wie viele unbenutzte Codes Sie noch haben. Über **Neue Backup-Codes erzeugen** erhalten Sie einen neuen Satz; die bisherigen Codes werden dabei ungültig.

Anmelden mit zweitem Faktor

1. Geben Sie wie gewohnt E-Mail-Adresse und Passwort ein und klicken Sie auf **Anmelden**.
2. Im Schritt **Bestätigung erforderlich** klicken Sie auf **Passkey verwenden** und bestätigen die Abfrage Ihres Geräts – oder geben Sie den Code aus der Authenticator-App bzw. einen Backup-Code ein und klicken Sie auf **Bestätigen**.

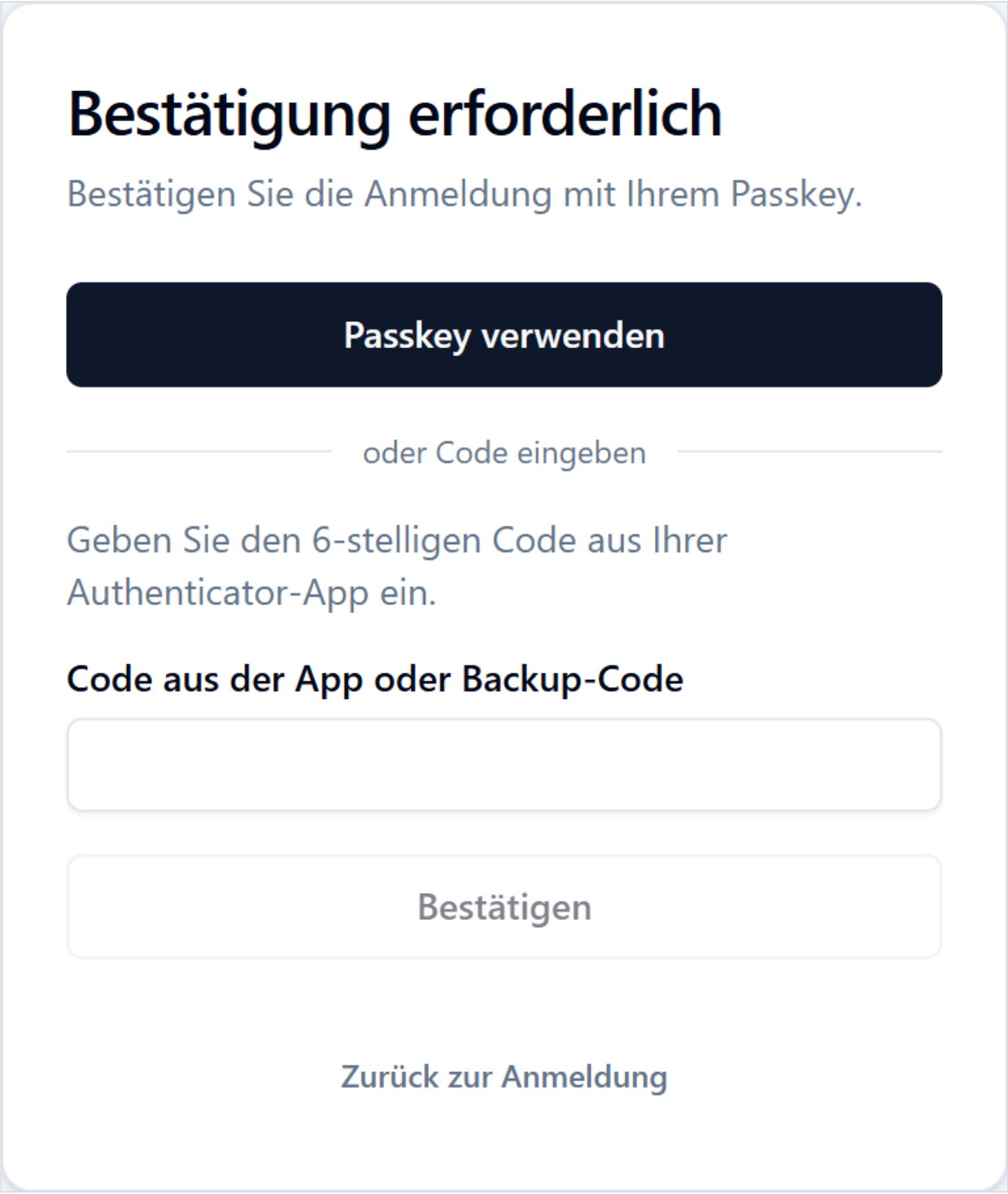


Abbildung 8. Zweiter Schritt der Anmeldung

Mit einem Passkey geht es auch ohne Passwort: Klicken Sie auf der Anmeldeseite auf **Mit Passkey anmelden** oder wählen Sie den Passkey direkt im Vorschlag des E-Mail-Felds aus. Liegt der Passkey

auf Ihrem Smartphone, Sie melden sich aber am Computer an, wählen Sie im Fenster des Browsers „Anderes Gerät verwenden“ und scannen den QR-Code mit dem Smartphone.

Nach fünf fehlgeschlagenen Versuchen (falsches Passwort oder falscher Code) wird das Konto vorübergehend gesperrt: zunächst für 15 Minuten, bei weiteren Fehlversuchen länger (höchstens 4 Stunden).

Faktoren verwalten

- **Umbenennen** und **Löschen** einzelner Passkeys sowie **Authenticator-App entfernen** finden Sie auf der Seite **Anmeldung & Sicherheit**.
- Der letzte verbleibende Faktor kann nicht entfernt werden – richten Sie zuerst einen weiteren ein. So ist Ihr Konto nie nur durch das Passwort geschützt.
- **App neu einrichten** ersetzt die Authenticator-App, zum Beispiel nach einem Smartphone-Wechsel. Die Einrichtung läuft wie beim ersten Mal; die bisherige App bleibt gültig, bis Sie den Code der neuen App bestätigt haben. Danach gelten nur noch Codes der neuen App, und Ihre Anmeldungen auf anderen Geräten werden beendet.
- Änderungen an den Faktoren erfordern Ihr Passwort. Liegt Ihre letzte Bestätigung mehr als zehn Minuten zurück, fragt das Portal zusätzlich nach einem Passkey oder Code (**Identität bestätigen**).
- Wird ein Faktor entfernt, werden alle anderen Sitzungen Ihres Kontos beendet.
- Über jede Änderung erhalten Sie zur Sicherheit eine E-Mail – in der Sprache, in der Sie sich zuletzt angemeldet haben. Haben Sie die Änderung nicht selbst vorgenommen, wenden Sie sich umgehend an Ihre Praxis bzw. den Administrator.

Gerät verloren

1. Melden Sie sich mit E-Mail, Passwort und einem **Backup-Code** an.
2. Öffnen Sie **Anmeldung & Sicherheit** und ersetzen Sie den verlorenen Faktor:
    - **Authenticator-App:** Klicken Sie unter **Authenticator-App** auf **App neu einrichten** und richten Sie die App auf dem neuen Smartphone ein. Codes des verlorenen Smartphones gelten danach nicht mehr.
    - **Passkey:** Legen Sie zuerst einen neuen Passkey an (oder richten Sie eine Authenticator-App ein) und löschen Sie dann den Passkey des verlorenen Geräts.
3. Prüfen Sie, wie viele Backup-Codes Sie noch haben, und erzeugen Sie bei Bedarf neue.

Haben Sie keinen Backup-Code mehr, kann der Administrator des Portals Ihre Anmeldefaktoren zurücksetzen. Bei der nächsten Anmeldung richten Sie dann einen neuen zweiten Faktor ein.

Ändert jemand anderes Ihre Faktoren, erhalten Sie eine E-Mail – wenden Sie sich dann umgehend an Ihre Praxis bzw. den Administrator.

Anmeldefaktoren eines Benutzers zurücksetzen

Hat ein Benutzer Gerät und Backup-Codes verloren, setzen Sie unter Benutzer seine Anmeldefaktoren

zurück:

1. Prüfen Sie die Identität der Person auf einem zweiten Weg (zum Beispiel Rückruf unter der bekannten Telefonnummer).
2. Klicken Sie in der Zeile des Benutzers auf das Schild-Symbol **Anmeldefaktoren zurücksetzen** und bestätigen Sie.

Alle Passkeys, die Authenticator-App und die Backup-Codes werden entfernt, laufende Sitzungen enden sofort. Bei der nächsten Anmeldung muss der Benutzer einen neuen zweiten Faktor einrichten. Die Spalte **Zweiter Faktor** der Benutzerliste zeigt, welche Faktoren ein Benutzer eingerichtet hat; Konten ohne Faktor sind mit **keiner** markiert. Der Vorgang wird im Audit-Log protokolliert (**Anmeldefaktoren zurückgesetzt**).

Notfall: kein Administrator kann sich anmelden

Haben alle Administratoren ihren zweiten Faktor und ihre Backup-Codes verloren, setzt der Betreiber die Faktoren eines Administrators direkt in der Datenbank zurück. Ersetzen Sie `admin@example.de` durch die E-Mail-Adresse des Administrators:

```
-- docker compose exec postgres psql -U postgres -d patientenportal
SET search_path TO patientenportal;
BEGIN;
DELETE FROM user_passkey      WHERE user_id = (SELECT id FROM users WHERE email =
'admin@example.de');
DELETE FROM user_backup_codes WHERE user_id = (SELECT id FROM users WHERE email =
'admin@example.de');
UPDATE users SET two_factor_method = 'NONE', totp_secret = NULL,
two_factor_confirmed_at = NULL,
                 token_version = token_version + 1
 WHERE email = 'admin@example.de';
COMMIT;
```

Bei der nächsten Anmeldung richtet der Administrator einen neuen zweiten Faktor ein.

Hinweise für den Betrieb

- **Passkeys sind an die Domain gebunden**, unter der das Portal aufgerufen wird. Sie wird über `WEBAUTHN_RP_ID` (Domain) und `WEBAUTHN_ORIGINS` (Adresse inklusive `https://`) festgelegt; ohne diese Angaben gilt der erste Eintrag aus `CORS_ALLOWED_ORIGINS`. Wechselt die Domain später, funktionieren die bisherigen Passkeys nicht mehr – die Benutzer melden sich dann mit Authenticator-App oder Backup-Code an und legen neue Passkeys an.
- Die Secrets der Authenticator-Apps werden mit `FIELD_ENCRYPTION_KEY` verschlüsselt gespeichert (das Installationsskript erzeugt den Schlüssel automatisch). Bewahren Sie den Schlüssel zusammen mit der Datensicherung auf – ohne ihn sind die eingerichteten Authenticator-Apps nach einer Wiederherstellung unbrauchbar.
- Sicherheitshinweise per E-Mail (Faktor hinzugefügt, entfernt, zurückgesetzt) werden über den in

den Einstellungen konfigurierten E-Mail-Versand verschickt.

Stammdaten

Kunden

Ein **Kunde** (Customer) ist eine radiologische Praxis oder Klinik bzw. ein Standort, für den das Portal Untersuchungen bereitstellt. Kunden bündeln Überweiser, Benutzer, Freigaben, Integrations-Tokens und eigene Ausdruck-Vorlagen.

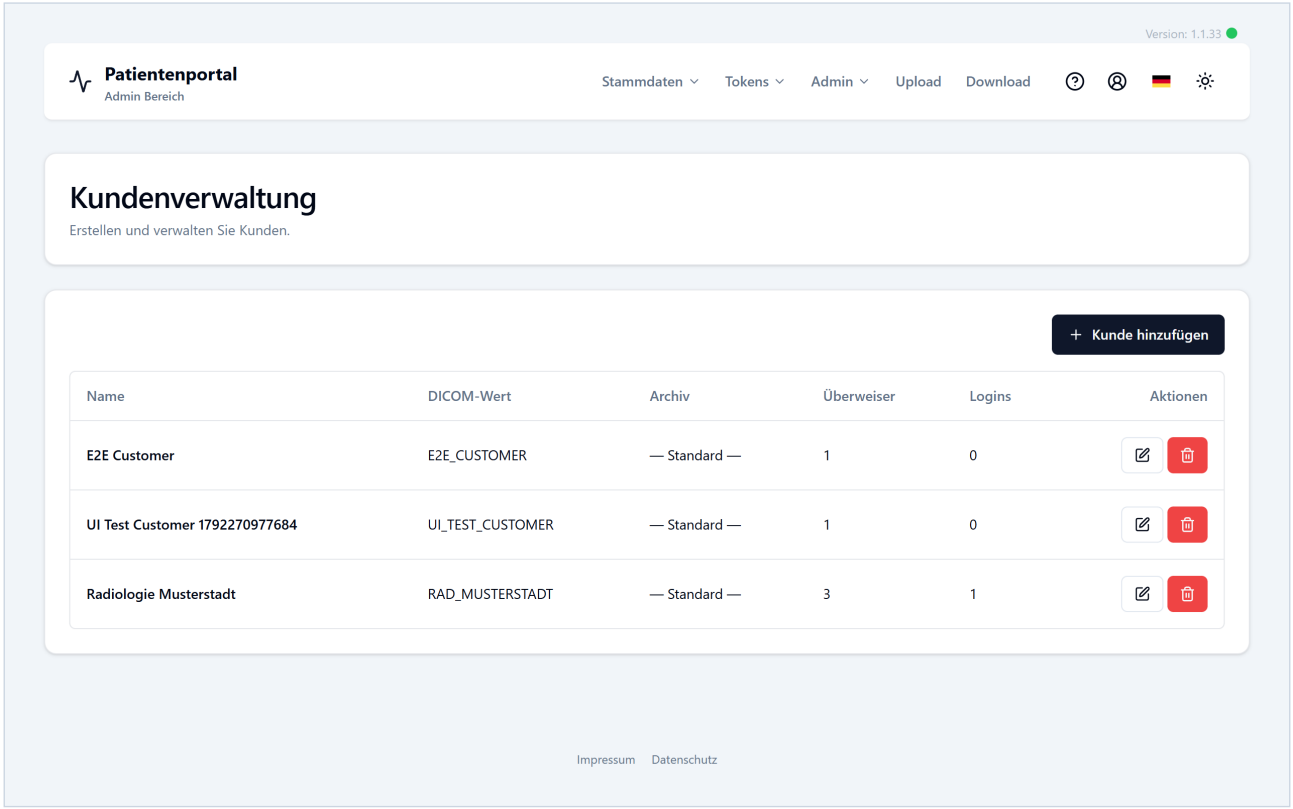


Abbildung 9. Kundenverwaltung

Die Tabelle zeigt für jeden Kunden Name, DICOM-Wert, zugeordnetes Archiv sowie die Anzahl der Überweiser und Logins.

Kunden anlegen und bearbeiten

1. Klicken Sie auf **Kunde hinzufügen** (bzw. bei einem vorhandenen Kunden auf das Stift-Symbol).
2. Füllen Sie die Felder aus:

Feld	Bedeutung
Kundenname	Anzeigename, z. B. „Radiologie Musterstadt“.
DICOM-Wert	Wert des DICOM-Attributs **InstitutionName** (0008,0080), mit dem die Studien dieses Kunden im PACS gekennzeichnet sind. Er wird u. a. als Filter für PACS-Abfragen verwendet und muss exakt dem Eintrag in den Bilddaten entsprechen.

Feld	Bedeutung
Archiv	PACS-Archiv, aus dem die Studien dieses Kunden abgerufen werden. — *Standard* — verwendet das Standard-Archiv aus der Archiv-Verwaltung.

3. Speichern Sie.



Wie viele Kunden angelegt werden können, legt die Lizenz fest (ohne Lizenz ein Kunde). Ist das Kontingent erreicht, ist **Kunde hinzufügen** gesperrt; bestehende Kunden bleiben nutzbar.

Kunden löschen

Klicken Sie auf das rote Papierkorb-Symbol und bestätigen Sie die Sicherheitsabfrage.



Prüfen Sie vor dem Löschen, ob dem Kunden noch Überweiser, Benutzer oder Integrations-Tokens zugeordnet sind.

Überweiser

Überweiser (Zuweiser) sind die überweisenden Ärztinnen, Ärzte und Praxen. Sie greifen über das Zuweiserportal auf die Untersuchungen ihrer Patientinnen und Patienten zu (siehe Zuweiserhandbuch).



Das Zuweiserportal ist ein lizenzpflichtiges Modul. Ist es nicht aktiv, ist der Menüpunkt **Stammdaten** → **Überweiser** ausgeblendet.

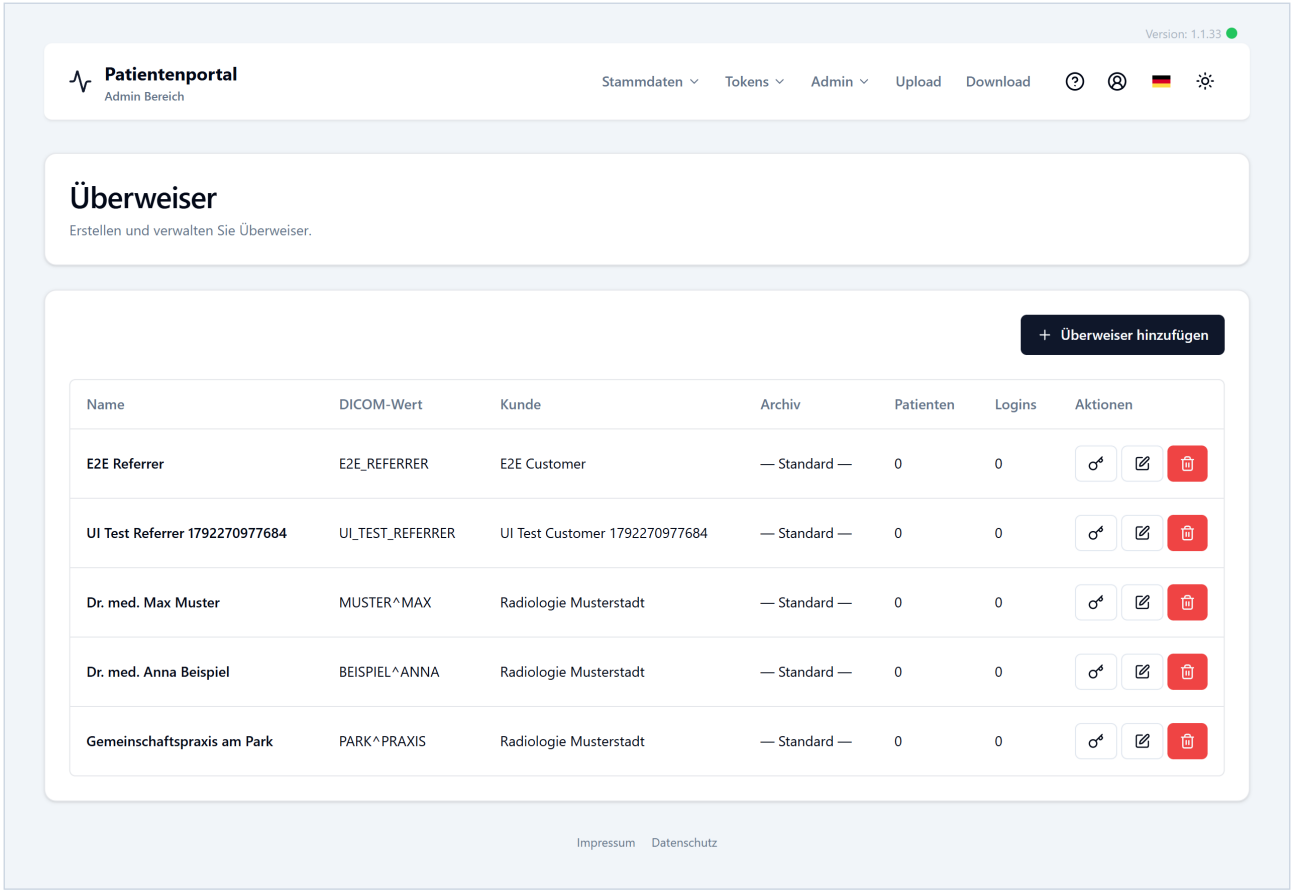


Abbildung 10. Überweiser-Verwaltung

Die Tabelle zeigt Name, DICOM-Wert, Kunde, Archiv sowie die Anzahl der Patienten und Logins.

Überweiser anlegen und bearbeiten

1. Klicken Sie auf **Überweiser hinzufügen** (bzw. auf das Stift-Symbol).
2. Füllen Sie die Felder aus:

Feld	Bedeutung
Überweiser Name	Anzeigename, z. B. „Dr. med. Anna Beispiel“.
DICOM-Wert	Wert des DICOM-Attributs **ReferringPhysicianName** (0008,0090), so wie er im RIS/PACS bei den Untersuchungen dieses Überweisers eingetragen wird (z. B. `BEISPIEL^ANNA`). Die PACS-Ansicht des Überweisers zeigt **nur** Studien mit genau diesem Wert.
Kunde	Praxis/Klinik, zu der der Überweiser gehört.
Archiv	PACS-Archiv für die Abfragen dieses Überweisers; — *Standard* — übernimmt das Archiv des Kunden bzw. das Standard-Archiv.

3. Speichern Sie.

Findet ein Überweiser in seiner PACS-Ansicht keine Patienten, ist fast immer der DICOM-Wert nicht identisch mit dem Eintrag in den Bilddaten. Prüfen Sie

> Schreibweise, Reihenfolge und Trennzeichen (^).

Zugang für einen Überweiser erzeugen

Über das Schlüssel-Symbol (**Token erzeugen**) erstellen Sie einen Zugangscode für den Überweiser:

1. Wählen Sie die **Gültigkeit (Tage)** und den **Authentifizierungstyp** (*Keine* oder *Passwort*, dann Passwort eingeben).
2. Klicken Sie auf erzeugen und kopieren Sie den **erzeugten Token**.
3. Übergeben Sie den Code dem Überweiser. Mit dem Code kann er sich anmelden und anschließend selbst einen dauerhaften Login mit E-Mail und Passwort einrichten (sofern in den Einstellungen erlaubt).

Überweiser löschen

Klicken Sie auf das Papierkorb-Symbol und bestätigen Sie die Sicherheitsabfrage.

Benutzer

Unter **Benutzer** verwalten Sie alle Konten, die sich mit E-Mail und Passwort anmelden. Zugänge über Zugangscodes (Tokens) erscheinen hier erst, wenn daraus ein dauerhafter Login eingerichtet wurde.

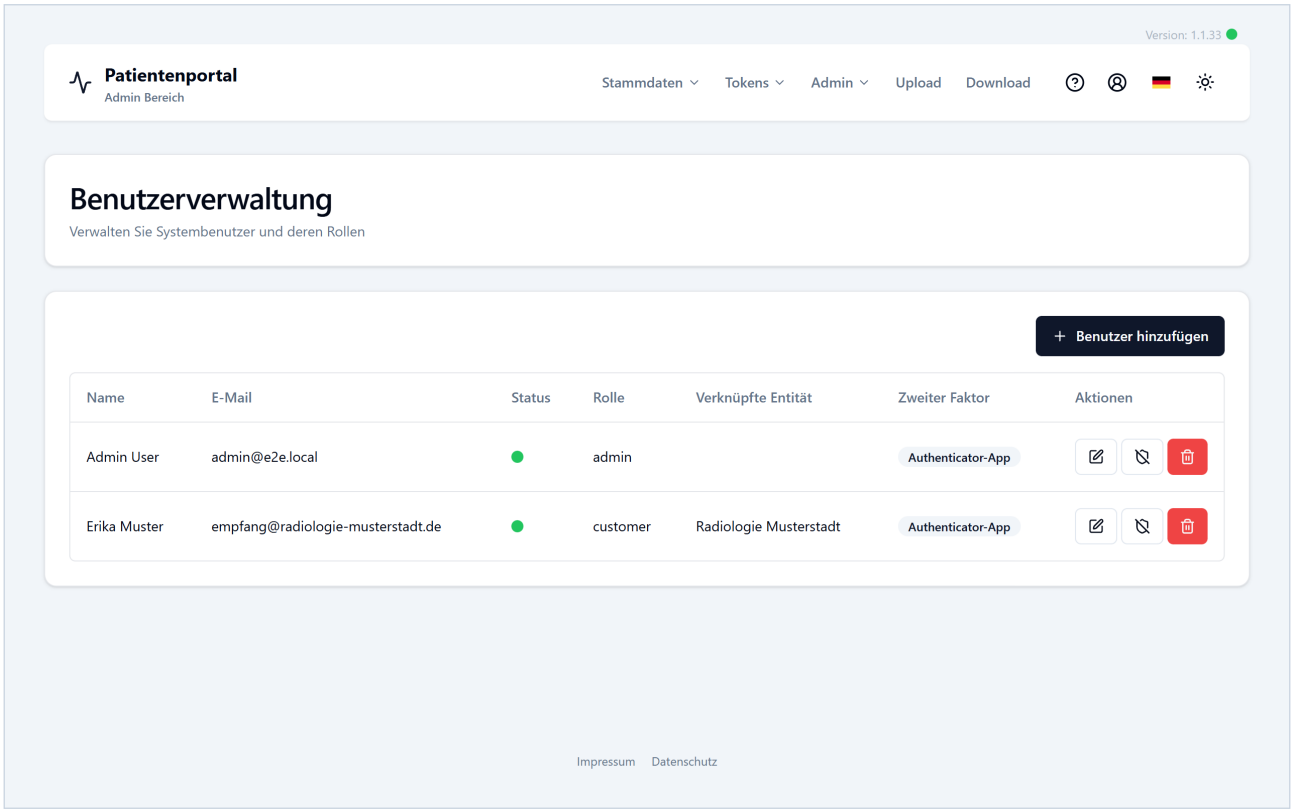


Abbildung 11. Benutzerverwaltung

Die Tabelle zeigt Name, E-Mail, Status (grün = aktiv), Rolle und die verknüpfte Entität (Kunde, Überweiser oder Patient).

Rollen

Rolle	Zugriff
`admin`	Vollzugriff auf alle Verwaltungsfunktionen und Einstellungen.
`customer`	Praxis/Klinik: Freigaben des eigenen Kunden, Upload und Downloads (siehe Customer-Bereich). Muss mit einem Kunden verknüpft sein.
`referrer`	Überweiser: PACS-Ansicht der eigenen Patienten, Freigaben, Upload, Downloads. Muss mit einem Überweiser verknüpft sein.
`patient`	Patient: eigene Untersuchungen ansehen, herunterladen und teilen. Muss mit einem Patienten verknüpft sein.

Benutzer anlegen und bearbeiten

1. Klicken Sie auf **Benutzer hinzufügen** (bzw. auf das Stift-Symbol).
2. Geben Sie **Vorname**, **Nachname**, **E-Mail** und ein **Passwort** ein. Beim Bearbeiten lassen Sie das Passwort leer, um das bisherige beizubehalten.
3. Wählen Sie die **Rolle**. Eine Rolle ist nicht vorausgewählt; beim Bearbeiten zeigt das Feld die gespeicherte Rolle.
4. Wählen Sie je nach Rolle in **Mit Kunde verknüpfen**, **Mit Überweiser verknüpfen** oder **Mit Patient verknüpfen** den passenden Eintrag. Die Felder sind Suchfelder: Tippen Sie einen Teil des Namens ein, bei Patienten auch Geburtsdatum oder Patienten-ID. Die Trefferliste zeigt bei Patienten Geburtsdatum und Patienten-ID, um Namensgleiche zu unterscheiden. Für Kunde, Überweiser und Patient ist die Verknüpfung Pflicht; ohne sie lässt sich der Benutzer nicht speichern.
5. Über **Aktiv** sperren oder entsperren Sie das Konto.
6. Speichern Sie.

Jeder Benutzer richtet bei der ersten Anmeldung einen zweiten Faktor ein (Anmeldung & Sicherheit). Die Spalte **Zweiter Faktor** zeigt den Stand; über das Schild-Symbol setzen Sie die Faktoren eines Benutzers zurück, zum Beispiel nach dem Verlust seines Geräts (siehe Anmeldefaktoren zurücksetzen). Ein vom Administrator gesetztes neues Passwort beendet alle laufenden Sitzungen des Benutzers.



Die Passwortregeln (Mindestlänge, Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen) legen Sie in den Einstellungen im Bereich **Sicherheit** fest.

E-Mail-Adressen und Groß-/Kleinschreibung

Bei der Anmeldung spielt die Groß-/Kleinschreibung der E-Mail-Adresse keine Rolle: `Max.Muster@Praxis.de` und `max.muster@praxis.de` führen zum selben Konto. Das Portal speichert E-Mail-Adressen deshalb immer kleingeschrieben. Eine Adresse, die sich von einem bestehenden Konto nur in der Schreibweise unterscheidet, gilt als bereits vergeben.

Beim Update mit dieser Änderung wurden bestehende Adressen einmalig automatisch kleingeschrieben. Davon ausgenommen sind Konten, deren Adressen sich nur in der Groß-

/Kleinschreibung unterscheiden, zum Beispiel `Max@praxis.de` und `max@praxis.de`. Diese Konten bleiben unverändert, und das Konto mit Großbuchstaben kann sich nicht mehr anmelden. Das Backend meldet solche Konten bei jedem Start im Log mit `Email case collision between user ids: …`.

So lösen Sie eine solche Dublette auf:

1. Suchen Sie die Konten über die im Log genannten IDs bzw. die E-Mail-Adresse in der Tabelle **Benutzer**.
2. Klären Sie, welches Konto weiter genutzt wird.
3. Löschen Sie das nicht mehr benötigte Konto oder geben Sie ihm eine andere E-Mail-Adresse.
4. Öffnen Sie das verbleibende Konto und speichern Sie es. Dabei wird seine Adresse kleingeschrieben.

Tokens

Integrations-Tokens

Integrations-Tokens sind langlebige Zugangsschlüssel für Fremdsysteme, z. B. eine PACS-Workstation (VEPRO VIM), ein PVS über Portal-Launch oder die gdt-hl7-bridge. Sie ermöglichen eine automatische Anmeldung ohne Passwort-Dialog und sind immer einem Kunden zugeordnet.

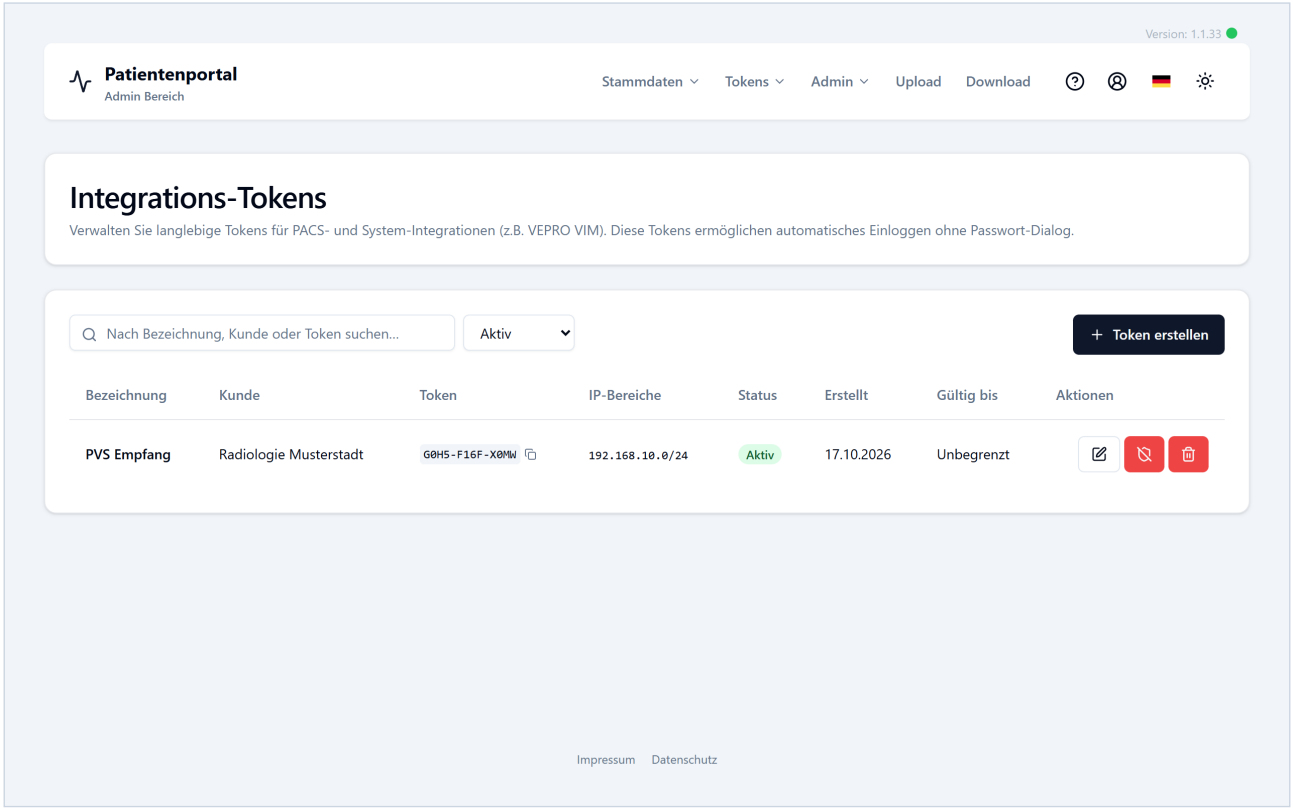


Abbildung 12. Integrations-Tokens

Über das Suchfeld filtern Sie nach Bezeichnung, Kunde oder Token, über die Auswahl nach Status.

Token erstellen

1. Klicken Sie auf **Token erstellen**.
2. Füllen Sie die Felder aus:

Feld	Bedeutung
Bezeichnung	Wofür der Token verwendet wird, z. B. „VEPRO Workstation 1“ oder „PVS Empfang“.
Kunde	Der Kunde, in dessen Namen das Fremdsystem arbeitet.
Erlaubte IP-Bereiche (CIDR)	Kommagetrennte IPv4- oder IPv6-Adressen bzw. Netzbereiche (CIDR), aus denen der Token verwendet werden darf, z. B. `192.168.2.0/24, 10.0.0.5, 2001:db8:10::/48`. Einzelne Adressen gelten als `/32` (IPv4) bzw. `/128` (IPv6). Ungültige Einträge lehnt das Portal beim Speichern ab.

Feld	Bedeutung
Gültigkeit (Tage)	Leer lassen für unbegrenzte Gültigkeit.

3. Klicken Sie auf erstellen. Der Token wird angezeigt – kopieren Sie ihn sofort; er wird nur einmal vollständig angezeigt. Für VBS-basierte Integrationen wird zusätzlich eine Beispielkonfiguration angezeigt.



Lassen Sie die IP-Bereiche nur in Ausnahmefällen leer. Ein Token ohne IP-Beschränkung ist von überall nutzbar; das Portal warnt beim Erstellen.

Token bearbeiten, widerrufen, löschen

- **Stift-Symbol** – Bezeichnung, IP-Bereiche oder **Ablaufdatum** ändern.
- **Widerrufen** (Schild-Symbol) – der Token ist sofort ungültig, bleibt aber zur Nachvollziehbarkeit sichtbar (Status *Inaktiv*).
- **Löschen** (Papierkorb) – entfernt den Token endgültig.

QR-Code-Import

Mit dem **QR-Code-Import** übernehmen Sie Zugangscodes, die ein Fremdsystem (z. B. das PACS beim Befunddruck) bereits erzeugt und auf Ausdrucke gedruckt hat. Patientinnen und Patienten können sich dann mit diesen Codes am Portal anmelden.

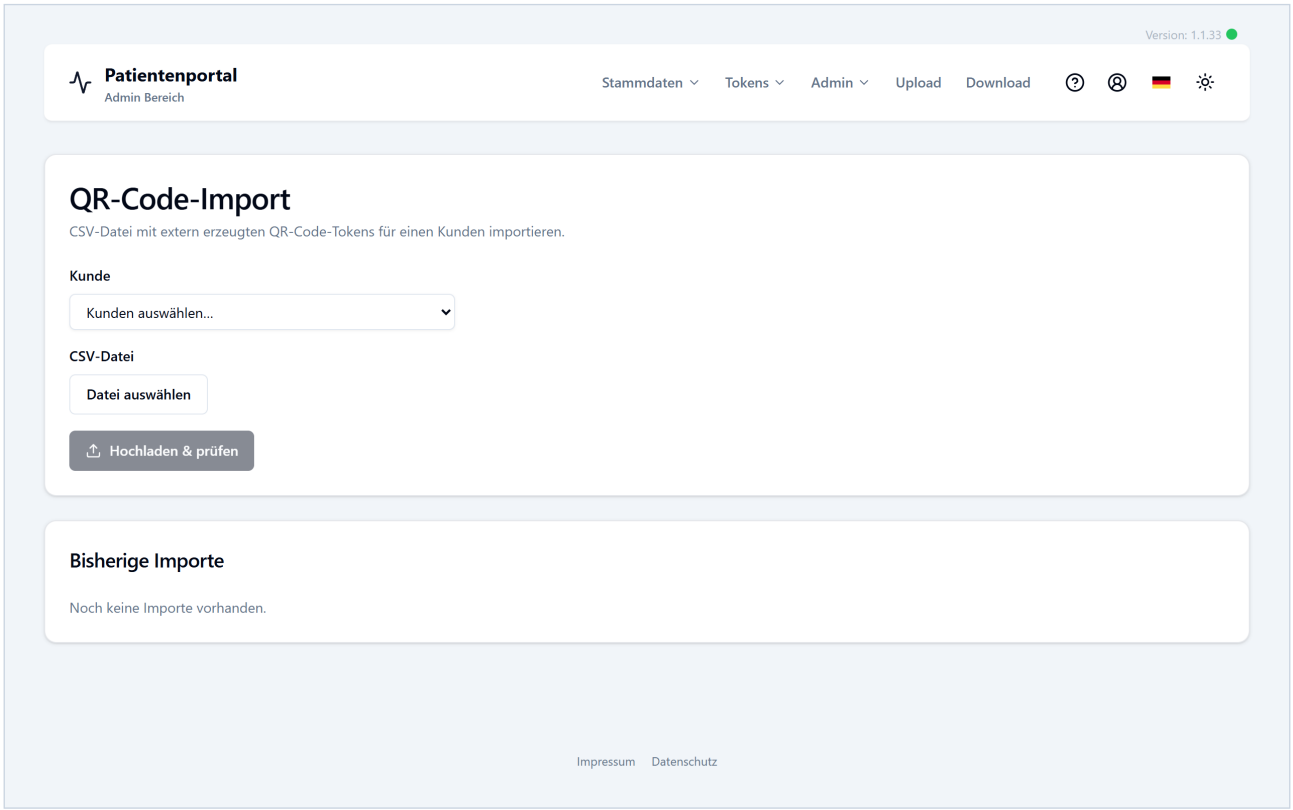


Abbildung 13. QR-Code-Import

CSV-Format

Die CSV-Datei enthält pro Zeile einen Code, getrennt durch Semikolon:

```
code;expirationdate;studyuid
ABCD-EFGH-JKLM;20270131;1.2.840.113619.2.55.3.1234.1
```

- `code` – der aufgedruckte Zugangscode
- `expirationdate` – Ablaufdatum im Format `JJJJMMTT`
- `studyuid` – StudyInstanceUID der freigegebenen Untersuchung

Eine Kopfzeile ist optional und wird automatisch erkannt.

Import durchführen

1. Wählen Sie den **Kunden** und die **CSV-Datei** und klicken Sie auf **Hochladen & prüfen**.
2. Das Portal prüft jede Zeile (Format, doppelte Codes in der Datei und in der Datenbank, Existenz der Studie im PACS). Den Fortschritt sehen Sie unter **Bisherige Importe**.
3. Öffnen Sie den Import über **Ansehen**: Die Details zeigen gültige und fehlerhafte Zeilen mit Grund.
4. Klicken Sie auf **Import durchführen**, um die gültigen Codes zu übernehmen.

Laufende Importe lassen sich **abbrechen** und später **fortsetzen**; abgeschlossene oder fehlgeschlagene Importe können Sie **löschen**.

Freigaben

Die **Freigaben-Verwaltung** zeigt alle erteilten Patienten- und Untersuchungs-Freigaben (Zugangscodes) – unabhängig davon, wer sie erstellt hat (Praxis, Überweiser, Patient).

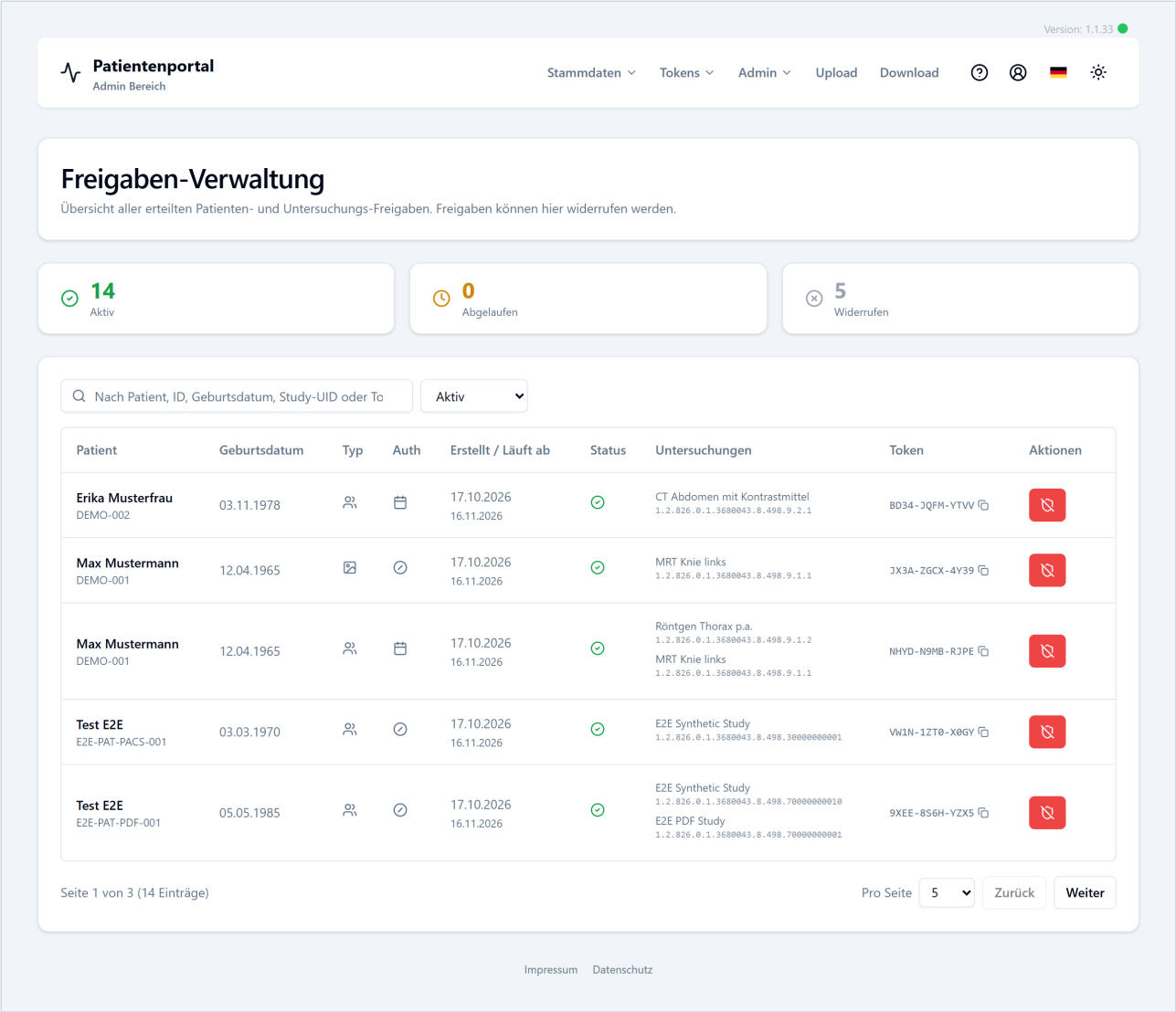


Abbildung 14. Freigaben-Verwaltung

- Die Kacheln oben zählen **aktive**, **abgelaufene** und **widerrufene** Freigaben.
- Über das Suchfeld finden Sie Freigaben nach Patient, Patienten-ID, Geburtsdatum, Study-UID oder Token; die Auswahl daneben filtert nach Status.
- Die Spalten zeigen Patient, Geburtsdatum, **Typ** (Symbol: Patienten- oder Untersuchungs-Freigabe), **Auth** (Absicherung: keine, Geburtsdatum, Passwort), Erstellungs- und Ablaufdatum, Status, enthaltene Untersuchungen und den Token (mit Kopier-Symbol).

Freigabe widerrufen

Klicken Sie auf das rote Symbol in der Spalte **Aktionen** und bestätigen Sie. Der Zugang ist sofort ungültig.



Das ist der schnellste Weg, wenn ein Ausdruck mit Zugangscode verloren gegangen ist oder an die falsche Person übergeben wurde.

Freigabe erneut drucken

Bei aktiven Freigaben öffnet das Drucker-Symbol in der Spalte **Aktionen** die Druckansicht mit QR-Code und Zugangslink, mit derselben Druckvorlage wie beim Erstellen. Als Gültigkeit steht dort die verbleibende Laufzeit bis zum Ablaufdatum.



Ein Passwort, mit dem die Freigabe abgesichert ist, wird nur verschlüsselt gespeichert und erscheint deshalb nicht im Nachdruck. Geben Sie es dem Patienten auf anderem Weg weiter.

Jeder Nachdruck wird im Audit-Log als `TOKEN_REPRINTED` protokolliert.

Freigabe im Audit-Log prüfen

Das Protokoll-Symbol in der Spalte **Aktionen** öffnet das Audit-Log, gefiltert auf diese Freigabe als Akteur und ohne Zeitraum-Einschränkung, also mit allen Einträgen zu dieser Freigabe. Anmeldungen mit dem Zugangscode und alles, was danach geschieht (Ansicht, Download), sind mit der ID der Freigabe als Akteur-ID protokolliert. So sehen Sie zum Beispiel, ob über genau diese Freigabe schon Untersuchungen heruntergeladen wurden.

Das Symbol erscheint nur für Administratoren, weil nur sie das Audit-Log sehen dürfen.

Customer sehen die Freigaben ihres eigenen Kunden unter Freigaben im Customer-Bereich.

Admin

Import Status

Studien, die über den Upload (DLX-Import oder ZIP-Upload) ins Portal gelangen, können automatisch an ein **Fremdbild-Archiv** weitergeleitet werden (DICOM C-STORE). **Import Status** zeigt diese Übertragungen.

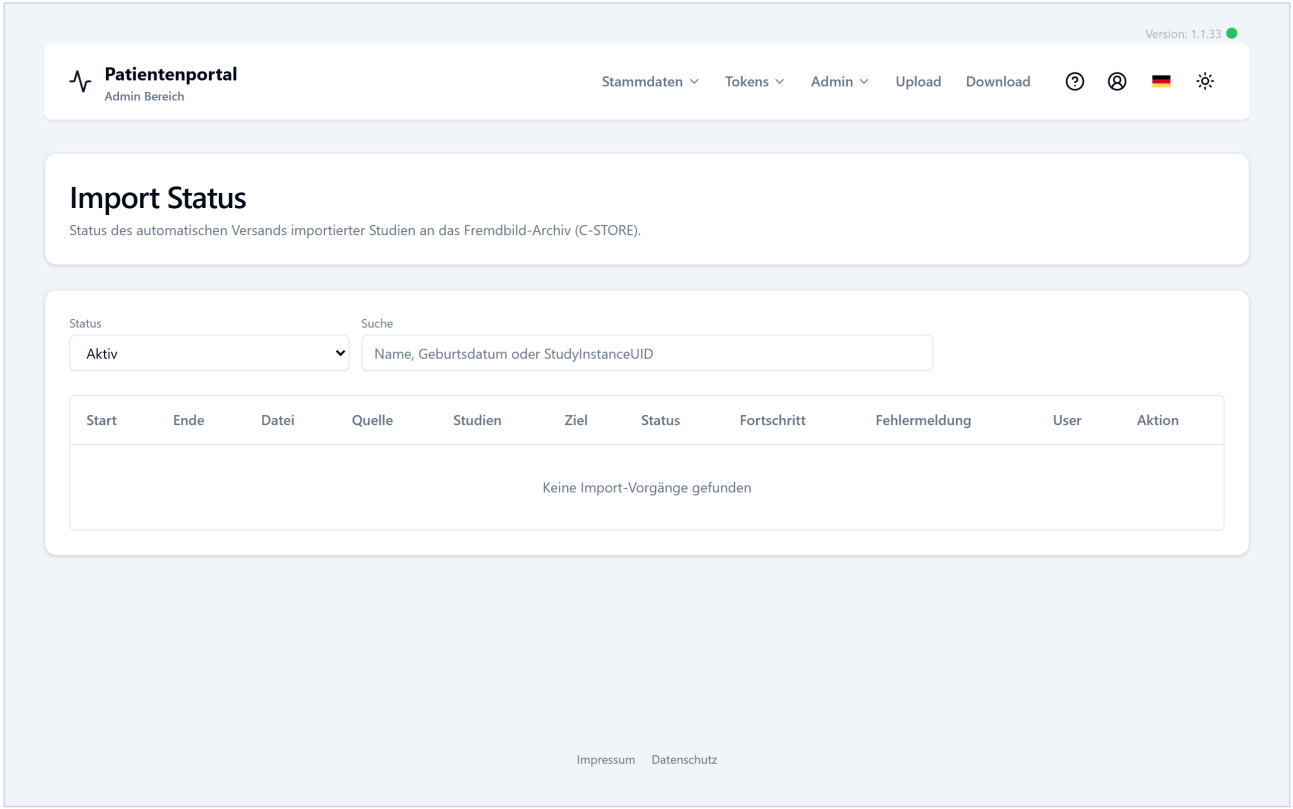


Abbildung 15. Import Status

- **Status**-Filter: aktive, abgeschlossene oder fehlgeschlagene Vorgänge.
- **Suche** nach Name, Geburtsdatum oder StudyInstanceUID.
- Die Tabelle zeigt Start und Ende, Datei, Quelle (DLX, ZIP), Anzahl der Studien, Ziel, Status, Fortschritt, Fehlermeldung und den auslösenden Benutzer. Fehlgeschlagene Übertragungen können über die Spalte **Aktion** erneut gestartet werden.

Für welche Nutzergruppen der DLX-Import und die automatische Weiterleitung aktiv sind, legen Sie in den Einstellungen im Bereich **Import** fest.

Ausdruck-Vorlagen

Diese Anleitung beschreibt, wie Sie Druck-, PDF- und E-Mail-Vorlagen für Zugangslinks sowie die System-Mails (dauerhafter Login, Sicherheitshinweise) an das Corporate Design (CI) einer Praxis oder eines Kunden anpassen. Sie richtet sich an Administratoren mit grundlegenden HTML- und CSS-Kenntnissen.

Überblick

Wann immer das Portal einen Zugangslink ausgibt (Ausdruck mit QR-Code, PDF über die Freigabe-API, Versand per E-Mail), wird eine HTML-Vorlage mit der Template-Engine Handlebars gerendert. Jede Vorlage besteht aus zwei Teilen:

- **HTML-Template** – das Layout mit Platzhaltern wie `{{patient.lastName}}` und Texten wie `{{i18n "common.title"}}`.
- **Vorlagen-Übersetzungen (JSON, optional)** – nur Texte, die es ausschließlich in dieser Vorlage gibt.

Alle Standardtexte (Titel, Betreff, Einleitung, Feldbezeichnungen …) liegen zentral im Übersetzungs-Namespace `templates`. Sie werden über die Sprachpakete in alle installierten Sprachen übersetzt und lassen sich unter **Admin → Sprachverwaltung** per Override anpassen – ohne die Vorlage zu ändern (siehe Übersetzungen).

Dazu kommen **Assets** (Logo, Stylesheet, Bilder, Schriften), die zentral hochgeladen und in allen Vorlagen verwendet werden.

Die Verwaltung erfolgt unter **Admin → Ausdruck-Vorlagen** (`/admin/print-templates`).

Vorlagen-Typen

Eine Vorlage wird einem oder mehreren Vorlagen-Typen (Template-Keys) zugeordnet:

Kontext	Typ	Verwendung
Patient	`patient_print`	Ausdruck im Browser nach Erzeugen eines Patienten-Tokens (Token-Generator).
	`patient_pdf`	PDF der Freigabe-API bei Aufruf mit `patid`. Fehlt es, wird `patient_print` verwendet.
	`patient_email`	E-Mail-Versand eines Patienten-Tokens.
Studie	`study_print`	Ausdruck im Browser nach Erzeugen eines Studien-Tokens.
	`study_pdf`	PDF der Freigabe-API bei Aufruf mit `studyuid` oder `accnbr`. Fehlt es, wird `study_print` verwendet. Wird auch als PDF-Anhang von E-Mails genutzt.
	`study_email`	E-Mail-Versand eines Studien-Tokens.
Überweiser	`referrer_print`	Ausdruck eines Überweiser-Zugangs (Überweiserverwaltung, Token-Generator).
	`referrer_pdf`	Derzeit ohne Verwendung (reserviert).
	`referrer_email`	E-Mail-Versand eines Überweiser-Tokens.
System-Mails	`account_activation`	Bestätigungs-Mail nach dem Anlegen eines dauerhaften Logins (Patienten und Überweiser), siehe System-Mails.
	`account_welcome`	Willkommens-Mail nach der Aktivierung des dauerhaften Logins.

Kontext	Typ	Verwendung
	`account_security`	Sicherheits-Mail an alle E-Mail-Logins (Administratoren, Praxis, Überweiser, Patienten), wenn sich ein Anmeldefaktor ändert.



Überweiser-Typen und Patient/Studie-Typen schließen sich in der Oberfläche gegenseitig aus, da sie unterschiedliche Daten erhalten. Eine Vorlage kann aber z. B. gleichzeitig `patient_print` und `study_print` abdecken. System-Mails erhalten eigene Daten: Eine Vorlage deckt genau eine System-Mail ab.

Auflösungsreihenfolge

Für einen Vorlagen-Typ wird die erste passende, **aktive** Vorlage in dieser Reihenfolge verwendet:

1. **Kunden-Vorlage** – für den Kunden (Customer), dem der Token zugeordnet ist.
2. **System-Vorlage** – unter **Default Templates** angelegt, gilt für alle Kunden ohne eigene Vorlage.
3. **Eingebaute Vorlage** – `backend/src/main/resources/templates/default-<typ>.html`.

Assets werden ebenfalls geschichtet: System-Assets bilden die Basis, Kunden-Assets mit gleichem Schlüssel überschreiben sie. Ein System-Logo unter dem Schlüssel `logo` wird also automatisch durch das Kunden-Logo `logo` ersetzt.



Pro Kunde (bzw. auf Systemebene) darf je Vorlagen-Typ **nur eine aktive Vorlage** existieren. Mehrere aktive Vorlagen mit demselben Typ führen beim Auflösen zu einem Serverfehler. Deaktivieren Sie alte Versionen, bevor Sie eine neue aktivieren.

Schritt für Schritt: CI-Vorlage anlegen

1. **Assets hochladen.** Wählen Sie unter **Ausdruck-Vorlagen** den Kunden (oder **Default Templates** für alle Kunden) und laden Sie im Bereich **Assets** hoch:
   - `logo` – Praxislogo (PNG, SVG, WebP oder JPEG), mit Alt-Text.
   - `css` – optionales Stylesheet für Druck/PDF (siehe Farben und Stylesheet).
   - weitere Bilder oder Schriften unter frei wählbaren Schlüsseln (z. B. `stamp`, `font_regular`).

   In der Asset-Liste öffnet das Augen-Symbol (Spalte **Vorschau**) Bilder (PNG, JPEG, WebP, SVG) in einem Vorschaufenster. Der Stift (Spalte **Aktionen**) bearbeitet ein vorhandenes Asset: Der Alt-Text lässt sich bei jedem Asset ändern, bei CSS und SVG zusätzlich der Inhalt im Code-Editor (SVG mit Live-Vorschau) – ohne die Datei neu hochzuladen.

2. **Neue Vorlage anlegen. Neue Vorlage** → Bezeichnung vergeben, Vorlagen-Typ(en) wählen und mit **Standardvorlage laden** die eingebaute Vorlage des ersten gewählten Typs als Ausgangspunkt übernehmen (siehe Editor).
3. **Farben, Schrift und Layout anpassen** (siehe CI-Elemente umsetzen).
4. **Vorschau prüfen.** Die Live-Vorschau rechts im Editor rendert mit Beispieldaten in jeder

installierten Sprache (siehe Testen).

5. **Aktivieren und speichern.** Mehrere Vorlagen lassen sich auch direkt in der Vorlagenliste gemeinsam schalten: per Checkbox auswählen und **… Vorlagen aktivieren** bzw. **… Vorlagen deaktivieren** wählen. Pro Vorlagen-Typ kann nur eine Vorlage aktiv sein – bisher aktive Vorlagen derselben Typen werden dabei deaktiviert und im Hinweis genannt; zwei ausgewählte Vorlagen desselben Typs lassen sich nicht gemeinsam aktivieren.
6. **Alle Ausgabewege real testen** – Ausdruck, PDF und E-Mail verhalten sich unterschiedlich (siehe Unterschiede je Ausgabeweg).

CI-Elemente umsetzen

Logo

```
{{#if assets.logo}}
<img class="logo" src="{{assets.logo.url}}" alt="{{assets.logo.alt}}" />
{{/if}}
```

Alternativ liefert der Helper `{{assetUrl "logo"}}` nur die URL. Umschließen Sie Assets immer mit `{{#if ...}}`, damit die Vorlage auch ohne hochgeladenes Asset funktioniert.



SVG oder PNG mit ausreichender Auflösung (mind. 2× der Anzeigegröße) verwenden – der Ausdruck und das PDF werden sonst unscharf.

Farben und Stylesheet

Für Druck- und PDF-Vorlagen gibt es zwei Möglichkeiten:

- **CSS direkt im Template** in einem `<style>`-Block – am einfachsten, wenn die Vorlage nur für einen Kunden gilt.
- **CSS als Asset** (Schlüssel `css`, Typ `text/css`) – sinnvoll, wenn eine System-Vorlage für alle Kunden gilt und jeder Kunde nur sein eigenes Stylesheet hochlädt.

Die eingebauten Vorlagen nutzen bereits das Muster „Kunden-CSS, sonst Standard-CSS“:

```
{{#if assets.css}}
<style>{{{assets.css.content}}}</style>
{{else}}
<style>
  /* Standard-Styles */
</style>
{{/if}}
```



CSS-Inhalte müssen mit **drei** geschweiften Klammern (`{{{assets.css.content}}}`) eingebunden werden. Mit zwei Klammern wird der Inhalt HTML-escaped und das

> Stylesheet ist unwirksam.

Empfehlung: Definieren Sie CI-Farben als CSS-Variablen am Anfang des Stylesheets, damit sie an einer Stelle gepflegt werden:

```
:root {
  --ci-primary: #004f9f;
  --ci-accent:  #e30613;
  --ci-text:    #1a1a1a;
}
h1         { color: var(--ci-primary); }
.header    { border-bottom: 3px solid var(--ci-accent); }
```

Schriften



Schriften dürfen **nicht** von externen Servern geladen werden (z. B. Google Fonts). Das Portal unterliegt der DSGVO; jeder externe Abruf überträgt die IP-Adresse des Patienten an Dritte. Laden Sie Schriften als `font/woff2`-Asset hoch oder verwenden Sie einen System-Font-Stack.

Die URL einer hochgeladenen Schrift steht nur im HTML-Template zur Verfügung, nicht innerhalb eines CSS-Assets (dessen Inhalt wird nicht von Handlebars verarbeitet). Die `@font-face`-Regel gehört daher in den `<style>`-Block des Templates:

```
<style>
  {{#if assets.font_regular}}
  @font-face {
    font-family: "PraxisSans";
    src: url("{{assets.font_regular.url}}") format("woff2");
  }
  {{/if}}
  body { font-family: "PraxisSans", Arial, Helvetica, sans-serif; }
</style>
```

In E-Mails werden Web-Fonts von vielen Clients (Outlook, Gmail) ignoriert – geben Sie immer eine Fallback-Schrift an.

Seitenformat für Druck und PDF

```
@page { size: A4; margin: 2cm; }
@media screen { body { padding: 1.5rem; } }
```

Das PDF wird mit Chromium im Format A4 mit Hintergrundfarben erzeugt; `@page`-Regeln werden berücksichtigt. Der Browser-Ausdruck rendert die Vorlage in einem isolierten `iframe` – die Styles des

Portals beeinflussen die Vorlage nicht.

Impressum und Kontaktdaten

Statt Adressen fest in die Vorlage zu schreiben, verwenden Sie die Einstellungen (siehe Einstellungen in Vorlagen). So bleibt eine System-Vorlage für alle Kunden gültig:

```
<div class="footer">
  {{settings.legal.group.company.name}}
  {{#if settings.legal.group.company.street}}·
{{settings.legal.group.company.street}}{{/if}}
  {{#if settings.legal.group.company.city}}· {{settings.legal.group.company.zip}}
{{settings.legal.group.company.city}}{{/if}}
  {{#if settings.legal.group.contact.phone}}·
{{settings.legal.group.contact.phone}}{{/if}}
</div>
```

Übersetzungen

Alle sichtbaren Texte werden über `{{i18n "…"}}` mit ihrem **vollständigen Pfad** ausgegeben – nie direkt ins HTML geschrieben. Die Sprache wird beim Ausdruck über die Sprachauswahl, beim E-Mail-Versand über die gewählte Sprache und beim PDF über den Parameter `lang` der Freigabe-API bestimmt; möglich ist jede installierte Sprache.

Namespace `templates`

Die Standardtexte aller Vorlagen liegen im Übersetzungs-Namespace `templates`. Gemeinsame Texte stehen unter `common`, nur Betreff, Einleitung und Button-Text unterscheiden sich je Zielgruppe:

Pfad	Text (de)
`common.title`	Ihr Zugangslink
`common.scan_qr`	QR-Code scannen oder Link öffnen
`common.access_type_label`	Zugangstyp
`common.access_type.PATIENT` / `.REFERRER` / `.STUDY`	Patientenzugang / Überweiserzugang / Untersuchungszugang
`common.verification_label`	Zugangsschutz
`common.verification_type.NONE` / `.BIRTHDATE` / `.PASSWORD`	Kein Passwort / Geburtsdatum / Passwort
`common.validity`, `common.unlimited`	Gültig bis, Unbegrenzt
`common.patient`, `common.referrer`	Patient, Überweiser
`common.included_studies`	Enthaltene Untersuchungen
`common.image_count` (Plural)	1 Bild / 5 Bilder

Pfad	Text (de)
`common.series`	Serie
`common.generated_on`	Erstellt am
`common.date_format`	`{{day}}.{{month}}.{{year}}` – Format für `formatDate`
`patient.subject`, `referrer.subject`, `study.subject`	Betreffzeile der E-Mail
`patient.intro`, `referrer.intro`, `study.intro`	Einleitungstext der E-Mail
`patient.open_link_button`, `referrer.open_link_button`, `study.open_link_button`	Beschriftung des Link-Buttons

Beispiele:

```
<h1>{{i18n "common.title"}}</h1>
<p>{{i18n "referrer.intro"}}</p>
{{i18n "common.verification_type" token.verificationType}}   {{!-- Argumente werden
mit "." verbunden --}}
{{i18n "common.image_count" count=instanceCount}}            {{!-- Pluralform
passend zur Sprache --}}
{{i18n audience "intro"}}                                    {{!-- Vorlage für
mehrere Zielgruppen --}}
```

`audience` enthält die Zielgruppe des gerade gerenderten Vorlagen-Typs (`patient`, `referrer` oder `study`). Deckt eine Vorlage z. B. `patient_email` und `study_email` ab, liefert `{{i18n audience "subject"}}` jeweils den passenden Text. Der Betreff von E-Mails ist immer `<zielgruppe>.subject`.

Texte anpassen

Standardtexte passen Sie **nicht** in der Vorlage an, sondern unter **Admin → Sprachverwaltung** als Override im Namespace `templates` (z. B. Schlüssel `referrer.intro`). Der Override gilt sofort für Ausdruck, PDF und E-Mail aller Vorlagen und lässt sich je Sprache setzen.

Vorlagen-Übersetzungen

Für Texte, die nur eine Vorlage benötigt, schreiben Sie einen eigenen Schlüssel ins HTML, z. B. `{{i18n "custom.footer"}}`. Der Editor legt unbekannte Schlüssel automatisch im Übersetzungs-JSON der Vorlage an – leer und für **jede installierte Sprache** (bei `count=` mit allen Pluralformen der Sprache). Noch leere Einträge zeigt der Editor als Warnung und in der Vorschau als `⟦custom.footer⟧` an.

```
{
  "de": { "custom.footer": "Bitte bringen Sie diesen Ausdruck zum nächsten Termin
mit." },
  "en": { "custom.footer": "Please bring this printout to your next appointment." }
```

```
}
```

Eine Vorlagen-Übersetzung mit einem Pfad aus dem Namespace (z. B. `common.title`) überschreibt den Standardtext nur für diese Vorlage.

Auflösungsreihenfolge

Für jeden Schlüssel gilt der erste nicht leere Text aus:

1. Vorlagen-Übersetzung der Sprache,
2. Override bzw. Sprachpaket der Sprache (Namespace `templates`),
3. eingebauter Standardtext der Sprache,

jeweils entlang der Sprachkette **gewählte Sprache** → **Fallback des Sprachpakets** → `en` → `de`. Fehlt ein Schlüssel überall, wird der Schlüssel selbst ausgegeben.



Übersetzungen dürfen kein HTML enthalten – die Ausgabe ist je Kanal unterschiedlich escaped.

Verfügbare Daten

Allgemein

Platzhalter	Inhalt
`{{lang}}`	Aktuelle Sprache (z. B. `de`, `en`, `ro`), z. B. für `<html lang="{{lang}}">`.
`{{audience}}`	Zielgruppe des Vorlagen-Typs: `patient`, `referrer` oder `study`.
`{{link}}`	Vollständiger Zugangslink.
`{{qrDataUrl}}`	QR-Code des Links als `data:`-URL, verwendbar als `<img src="{{qrDataUrl}}">`.
`{{token.value}}`	Token-Wert.
`{{token.type}}`	`PATIENT`, `REFERRER` oder `STUDY`.
`{{token.verificationType}}`	`NONE`, `BIRTHDATE` oder `PASSWORD`.
`{{token.validUntil}}`	Ablaufdatum als `JJJJ-MM-TT` (leer bei unbegrenzter Gültigkeit) – mit `formatDate` ausgeben.
`{{token.validityDays}}`	Gültigkeit in Tagen (leer bei unbegrenzter Gültigkeit).
`{{token.generatedAt}}`	Erstellungsdatum als `JJJJ-MM-TT` – mit `{{formatDate token.generatedAt}}` ausgeben.
`{{patient.firstName}}`, `{{patient.lastName}}`, `{{patient.externalId}}`	Patientendaten (nur Patient/Studie).
`{{referrer.name}}`	Name des Überweisers (nur Überweiser).

Platzhalter	Inhalt
`{{#each studies}}`	Liste der enthaltenen Studien (siehe unten).
`{{assets.<schlüssel>.url}}`, `.alt`, `.content`	Assets; `content` nur bei CSS.
`{{settings.<pfad>}}`	Einstellungen (siehe Einstellungen in Vorlagen).



Geben Sie `patient.birthDate` nicht in Vorlagen aus. Das Geburtsdatum ist bei `BIRTHDATE`-Tokens das Zugangsgeheimnis – ein Ausdruck oder eine E-Mail mit Link **und** Geburtsdatum hebt den Zugangsschutz auf.

Studien

Innerhalb von `{{#each studies}}` stehen zur Verfügung:

Feld	Inhalt
`description`	Studienbeschreibung (kann leer sein).
`studyDate`	Studiendatum als `JJJJ-MM-TT` – mit `{{formatDate studyDate}}` ausgeben.
`studyTime`	Uhrzeit der Studie (`HH:MM:SS`).
`modalities`	Modalitäten, z. B. `CT` oder `MR / CT`.
`modalitiesList`	Modalitäten als Liste, z. B. `{{#each modalitiesList}}…{{/each}}`.
`accessionNumber`, `studyuid`	Kennungen.
`seriesCount`, `instanceCount`	Anzahl Serien bzw. Bilder.
`{{#each series}}`	Serien mit `seriesuid`, `modality`, `description`, `instanceCount`, `seriesTime` (im Browser-Ausdruck abschaltbar über `display.group.print.show_series`).

Die Anzahl der gedruckten Studien lässt sich über die Einstellung `display.group.print.maxstudies` begrenzen.

Unterschiede je Ausgabeweg

Die Vorlagen werden an drei Stellen mit unterschiedlichen Daten gerendert. Robuste Vorlagen prüfen optionale Felder daher immer mit `{{#if ...}}`.

Merkmal	Druck (Browser)	PDF	E-Mail
Renderer	Handlebars (JS) im Browser	Handlebars (Java), Chromium	Handlebars (Java)
Sprache	wählbar	Parameter `lang` (Standard `de`)	beim Versand gewählt

Merkmal	Druck (Browser)	PDF	E-Mail
Asset-URLs	relativ (`/api/…`)	eingebettet als `data:`-URL	absolut (`frontend.url` + Pfad)
`studies[].series`, `studyTime`, `modalitiesList`, `instanceCount`	ja	ja	ja
`patient`	Patient/Studie	ja	Patient/Studie
`referrer.name`	nur aus Überweiserverwaltung	nein	ja

Einstellungen in Vorlagen

Unter `settings` stehen alle **nicht verschlüsselten** System- und Kundeneinstellungen mit den Präfixen `display.`, `frontend.`, `app.` und `legal.` zur Verfügung. Kundeneinstellungen überschreiben Systemeinstellungen. Punkte im Schlüssel werden zu Verschachtelungen, aus `legal.group.company.name` wird `{{settings.legal.group.company.name}}`.

Häufig genutzt:

- `legal.group.company.name`, `.street`, `.zip`, `.city`, `.country`, `.representative`
- `legal.group.contact.phone`, `.email`, `.privacy_email`
- `legal.group.medical.responsible_name`, `.responsible_specialty`
- `legal.group.dataprivacy.dpo_name`, `.dpo_contact`
- `app.support_email`
- `frontend.url`

Helper-Referenz

Helper	Beschreibung
`{{i18n "pfad"}}`	Übersetzung für die aktuelle Sprache (siehe Übersetzungen). Mehrere Argumente werden mit `.` verbunden: `{{i18n "common.access_type" token.type}}`. Mit `count=` wird die Pluralform gewählt und `{{count}}` ersetzt.
`{{formatDate datum}}`	Formatiert `JJJJ-MM-TT` gemäß `common.date_format`. Andere Formate werden unverändert ausgegeben.
`{{assetUrl "key"}}`	URL eines Assets (leer, wenn nicht vorhanden).
`eq`, `ne`, `gt`, `lt`, `gte`, `lte`	Vergleiche als Unterausdruck: `{{#if (eq token.type "PATIENT")}}…{{/if}}`.
`{{#and a b}}…{{/and}}`, `{{#or a b}}…{{/or}}`	Logische Verknüpfung – nur als **Block**-Helper verwenden, nicht als Unterausdruck in `#if`.

Helper	Beschreibung
`#if`, `#unless`, `#each`, `#with`, `@index`, `@first`, `@last`	Standard-Handlebars.



Der Browser-Ausdruck nutzt Handlebars für JavaScript, PDF und E-Mail nutzen Handlebars für Java. Beschränken Sie sich auf die hier genannten Helper und vergleichen Sie mit `eq` nur Werte gleichen Typs (Zahl mit Zahl, Text mit Text).

System-Mails

Neben den Zugangslinks versendet das Portal drei System-Mails rund um das Konto. Es gibt jede nur einmal – für Patienten und Überweiser gemeinsam. Sie werden genauso aufgelöst (Praxis → System → eingebaute Vorlage) und gestaltet wie die `_email`-Vorlagen und stehen im Editor in der Gruppe `*System-Mails`:

Typ	Anlass und Daten
`account_activation`	Ein Patient oder Überweiser hat einen dauerhaften Login angelegt. Daten: `link` (Bestätigungslink), `expiresInHours` (Gültigkeit, 24).
`account_welcome`	Die E-Mail-Adresse ist bestätigt, der Login aktiv. Daten: `link` (Anmeldeseite).
`account_security`	Ein Anmeldefaktor wurde geändert. Daten: `event`, `detail` (z. B. Name des Passkeys), `message` (fertiger Satz zum Ereignis), `occurredDate`, `occurredTime`, `link` (Seite **Anmeldung & Sicherheit**).

Alle System-Mails erhalten außerdem `email`, `user.firstName`/`user.lastName`, `accountType` (`patient`, `referrer`, `customer` oder `admin`), `lang`, `audience`, `assets` und `settings`. Mit `accountType` lassen sich Texte je Empfänger unterscheiden:

```
{{#if (eq accountType "referrer")}}<p>Ihre Zuweisungen finden Sie unter
⋯</p>{{/if}}
```

Welche Praxis-Vorlage gilt?

- Überweiser und Praxis-Logins: die Praxis des Kontos.
- Patienten: die Praxis des zuletzt erzeugten Zugangscodes des Patienten.
- Administratoren: immer die System-Vorlage.

Sprache

- Bestätigungs- und Willkommens-Mail: die Oberflächensprache bei der Registrierung des Logins.
- Sicherheits-Mail: die Oberflächensprache der letzten Anmeldung mit E-Mail und Passwort.
- Möglich ist jede installierte Sprache; fehlt ein Text, greift die Fallback-Kette (siehe Übersetzungen).

Ereignisse der Sicherheits-Mail

Die Variable `event` hat einen dieser Werte; der Text steht in `account.security.events.<EVENT>` und lässt

sich wie jeder Vorlagentext überschreiben: `TOTP_ADDED` (Authenticator-App eingerichtet), `TOTP_REPLACED` (App neu eingerichtet), `TOTP_REMOVED` (App entfernt), `PASSKEY_ADDED` und `PASSKEY_REMOVED` (mit Passkey-Name als `{{name}}`), `BACKUP_CODES_REGENERATED`, `FACTORS_RESET` (Administrator hat alle Faktoren zurückgesetzt).

```
<p>{{i18n "account.security.events" event name=detail}}</p>
{{#if (eq event "FACTORS_RESET")}}<p>Bitte richten Sie bei der nächsten Anmeldung
einen neuen Faktor ein.</p>{{/if}}
```

In der Vorschau des Editors wählen Sie das Ereignis über das Menü **Ereignis**.

Texte (Namespace `templates`)

`account.activation.`, `account.welcome.` und `account.security.*` – jeweils mit `subject` (Betreff) sowie Überschrift, Text und Button. Die Gültigkeit des Bestätigungslinks ist eine Pluralform: `{{i18n "account.activation.validity" count=expiresInHours}}`.

Besonderheiten für E-Mail-Vorlagen

E-Mail-Clients (insbesondere Outlook) unterstützen nur einen Teil von HTML und CSS. Die eingebauten `*_email`-Vorlagen folgen daher bewährten Regeln – behalten Sie diese bei:

- Layout mit `<table role="presentation">` statt Flexbox/Grid, feste Breite von 600 px.
- Alle Styles **inline** im `style`-Attribut; `<style>`-Blöcke und CSS-Assets werden von vielen Clients entfernt.
- Buttons als `<a>` mit Hintergrundfarbe und Innenabstand; darunter den Link zusätzlich als Text ausgeben.
- Keine CSS-Variablen, keine Web-Fonts ohne Fallback.
- Den QR-Code (`qrDataUrl`) **nicht** in E-Mails einbinden – `data:`-Bilder werden von vielen Clients blockiert.
- Logo-URLs werden automatisch absolut gemacht; die Einstellung `frontend.url` muss dafür korrekt gesetzt sein, und der Asset-Endpunkt muss vom Internet aus erreichbar sein.

Ist die Einstellung `token.group.email.appendpdf` aktiv, wird zusätzlich ein PDF (Typ `*_pdf` bzw. `*_print`) angehängt – dafür gelten die Regeln für Druck/PDF.

Editor

Der Editor nimmt nahezu das ganze Browserfenster ein: links Quellcode und Vorlagen-Übersetzungen (Tabs), rechts die Live-Vorschau. Er schließt sich nur über **Abbrechen** oder **Speichern** – ein Klick neben das Fenster schließt ihn nicht; bei ungespeicherten Änderungen fragt **Abbrechen** (auch `Esc`) nach.

- `{{` öffnet die Auswahl der **Systemvariablen** und der **Funktionen**. Über der Liste steht die Beschreibung des markierten Eintrags inklusive Beispielwert aus den Vorschaudaten. Innerhalb von `{{#each studies}}`/`{{#each series}}` werden die Felder des Listenelements angeboten, Systemvariablen dort als `@root.⋯`.

- `{{i18n "` öffnet die Auswahl der **Übersetzungen**: Vorlagen-Übersetzungen und Standardtexte aus dem Namespace `templates`, jeweils mit dem Text in der Vorschausprache.
- **Assets:** Hochgeladene Assets erscheinen in der `{{`-Auswahl als `assets.<schlüssel>.url`/`.alt` (Bilder, mit Vorschaubild), `.url` (Schriften) bzw. `.content` (CSS). **Asset einfügen** (über dem Quellcode) setzt das passende Snippet an der Cursorposition ein, z. B. `{{#if assets.logo}}<img src="{{assets.logo.url}}" alt="{{assets.logo.alt}}" />{{/if}}`, für CSS einen `<style>`-Block, für Schriften eine `@font-face`-Regel.
- **Übersetzungen als Tabelle:** Der Tab **Übersetzungen** zeigt die Vorlagen-Übersetzungen als Tabelle – eine Zeile je Schlüssel, eine Spalte je installierter Sprache. Graue Platzhalter sind die Standardtexte (leere Zelle = Standardtext), gelb markierte Zellen haben weder Text noch Standardtext. Unter der Tabelle lassen sich Schlüssel hinzufügen (mit Vorschlägen aus dem Namespace, um einen Standardtext nur für diese Vorlage zu überschreiben); Zeilen, die die Vorlage nicht verwendet, sind gekennzeichnet. Über **JSON** ist das Rohformat weiterhin editierbar.
- **Bearbeiten:** Fährt die Maus über einen Platzhalter, erscheinen Beschreibung bzw. Text und Aktionen: **Variable ersetzen** (öffnet die Auswahl für die markierte Variable), **Übersetzung bearbeiten** (Dialog mit einem Feld je installierter Sprache; der Standardtext steht als Platzhalter, leer lassen = Standardtext) und bei unbekannten Variablen **Als Übersetzung übernehmen**. Ein **Doppelklick** führt die jeweils erste Aktion aus.
- **Neue Texte:** Schreiben Sie z. B. `{{hinweis}}`, markiert der Editor die unbekannte Variable. **Als Übersetzung übernehmen** (Hover, Doppelklick oder Quick-Fix der Warnung) macht daraus `{{i18n "hinweis"}}`, legt den Schlüssel für alle Sprachen an und öffnet den Übersetzungsdialog.
- Unbekannte Variablen und Syntaxfehler werden im Quellcode markiert; leere Übersetzungen im Übersetzungs-Tab (die Zahl am Tab zeigt, wie viele fehlen). Beim Speichern verhindert ein Syntaxfehler das Speichern, bei unbekannten Variablen fragt der Editor nach.
- **Vorschau und Quellcode verbunden:** Ein Klick auf ein Element in der Vorschau markiert sein Start-Tag im Quellcode und scrollt dorthin (auch aus dem Tab **Übersetzungen** heraus); beim Überfahren mit der Maus ist das Element gestrichelt umrandet. Umgekehrt hebt der Cursor im Quellcode das zugehörige Element in der Vorschau hervor – bei `{{#each}}`-Schleifen alle Wiederholungen. Text aus `{{i18n ⋯}}` oder Variablen führt zum umschließenden Element.
- **Standardvorlage laden** (über dem Quellcode) übernimmt die eingebaute Standardvorlage des ersten gewählten Typs; vorhandener Quellcode wird erst nach Rückfrage ersetzt.

Vorlagen exportieren und importieren

Vorlagen lassen sich zwischen Installationen übertragen (z. B. von einer Test- in die Produktivumgebung) – einzeln oder mehrere zusammen in einer Datei:

- **Export:** In der Vorlagenliste lädt das Download-Symbol einer Zeile die Vorlage als JSON-Datei herunter – Name, Vorlagen-Typen, HTML und Vorlagen-Übersetzungen. Für mehrere Vorlagen diese per Checkbox auswählen (die Checkbox im Tabellenkopf wählt alle) und **… Vorlagen exportieren** wählen; alle ausgewählten Vorlagen landen in einer Datei, gemeinsam genutzte Assets nur einmal. Mit **Assets einschließen** werden zusätzlich die Assets mitgeliefert, die die Vorlage verwendet (`assets.<schlüssel>⋯`, `assetUrl "<schlüssel>"`); bei Kunden-Vorlagen gilt dabei dieselbe Schichtung wie beim Rendern (Kunden-Asset vor System-Asset).
- **Import: Vorlagen importieren** übernimmt eine Exportdatei in die gerade gewählte Ebene (Kunde

oder **Default Templates**). Enthält die Datei mehrere Vorlagen, listet der Dialog sie auf; alle sind vorausgewählt und lassen sich einzeln abwählen. Optional werden die Assets importiert, die die ausgewählten Vorlagen verwenden; vorhandene Assets mit gleichem Schlüssel bleiben unverändert, außer **Vorhandene Assets mit gleichem Schlüssel überschreiben** ist gewählt.

- **Aktivieren:** Ohne weitere Option werden die Vorlagen **inaktiv** angelegt – prüfen Sie sie im Editor und aktivieren Sie sie dann (vorher die bisher aktive Vorlage des Typs deaktivieren). Mit **Nach dem Import aktivieren** sind sie sofort aktiv; die bisher aktiven Vorlagen derselben Typen auf dieser Ebene werden dabei automatisch deaktiviert (nicht gelöscht). Haben mehrere ausgewählte Vorlagen denselben Typ, ist das nicht möglich – der Dialog weist darauf hin.

Exportdateien früherer Versionen (eine Vorlage je Datei) lassen sich weiterhin importieren.

Beim Import gelten dieselben Prüfungen wie beim Anlegen im Editor (erlaubte Vorlagen-Typen, Format der Übersetzungen, Asset-Typen PNG/JPEG/WebP/SVG/CSS/WOFF2, max. 2 MB je Asset); eine ungültige Datei wird vollständig abgelehnt.

Beispiel-Vorlagen

Als Ausgangspunkt für eigene Vorlagen gibt es ein Paket mit importierbaren Beispiel-Vorlagen. Es enthält vier Designs: **Standard** (die eingebauten Vorlagen), **Modern**, **Professionell** (Briefbogen) und **Klinisch** (minimal, kontrastreich). Jedes Design umfasst vier Vorlagen – Patient/Untersuchung und Überweiser, jeweils für Druck/PDF und für E-Mail – mit Platzhalter-Logo, Stylesheet und deutschen/englischen Texten. Patienten- und Untersuchungszugang teilen sich eine Vorlage; die Unterschiede (Texte, Serienliste) regelt sie über die Variable `audience`.

- **Bezug:** für Administratoren auf der Download-Seite des Portals (Karte **Beispiel-Vorlagen**, Download mit SHA-256-Prüfsumme wie bei den Anwendungen), als `sample-templates-<version>.zip` auf `download.radioweb.de`, im Integrationspaket eines Releases (Ordner `Sample-Templates/`) und im Repository unter `integration/sample_templates/`
- **Import:** je Design eine Datei – `<design>/import/<design>.json` mit allen vier Vorlagen und den Assets – wie oben beschrieben importieren, auf Wunsch direkt mit **Nach dem Import aktivieren**
- **Logo:** ist auf der Ebene ein Asset `logo` vorhanden, verwenden alle Designs dieses Logo statt des Platzhalters
- **Lizenz:** alle Vorlagen und Grafiken sind selbst erstellt und stehen unter CC0 – auch kommerziell frei verwendbar

Die `README.md` des Pakets beschreibt Import und Anpassung im Detail.

Testen

Die Live-Vorschau rendert mit Beispieldaten sowie den Assets und Einstellungen des gewählten Kunden – in jeder installierten Sprache (Auswahl **Sprache**) und bei Vorlagen für mehrere Zielgruppen je Zielgruppe. Die Texte werden genauso aufgelöst wie beim Versand. Sie ersetzt trotzdem keinen echten Test der Ausgabewege.

PDF-Vorschau: In der Vorlagenliste lädt das Symbol in der Spalte **Vorschau** eine Druck-/PDF-Vorlage als PDF mit Testdaten herunter – auch eine noch inaktive Vorlage. Das PDF wird wie bei der PDF-

Auslieferung im Backend erzeugt (Seitenformat, Seitenumbrüche, eingebettete Assets) und verwendet die Assets und Einstellungen der gewählten Ebene sowie die aktuelle Oberflächensprache. Bei Vorlagen für Patient und Untersuchung wird die Zielgruppe im Menü gewählt; E-Mail-Vorlagen haben keine PDF-Vorschau. Vorschau und PDF-Vorschau zeigen auch bei inaktiven Vorlagen die echten Praxisdaten (Einstellungen) und Assets des Kunden; die Beispiel-Praxisdaten erscheinen nur, wenn auf der Ebene keine Einstellungen hinterlegt sind.

Checkliste vor dem Aktivieren:

- ▢ Ausdruck über den Token-Generator in **allen** genutzten Sprachen geprüft.
- ▢ PDF über die Freigabe-API (siehe Entwicklerdokumentation) erzeugt (sofern genutzt) – Logo sichtbar, Umlaute korrekt.
- ▢ Test-E-Mail an Outlook und einen Webmail-Client gesendet.
- ▢ Vorlage ohne Studien, mit einer und mit vielen Studien geprüft (Seitenumbruch).
- ▢ Keine externen URLs (Schriften, Bilder, Skripte) im HTML.
- ▢ Keine fest eingetragenen Texte – alles über `i18n`.
- ▢ Nur eine aktive Vorlage je Typ und Kunde.

Einschränkungen

- Assets: PNG, JPEG, WebP, SVG, CSS, WOFF2; maximal 2 MB je Datei.
- JavaScript in Vorlagen wird nicht unterstützt und darf nicht verwendet werden.
- Vorlagen und Assets werden ausschließlich von Benutzern mit Administratorrechten gepflegt.

Sprachverwaltung

Das Portal ist auf Deutsch und Englisch verfügbar. In der **Sprachverwaltung** installieren Sie zusätzliche Sprachen und passen einzelne Texte dauerhaft an.

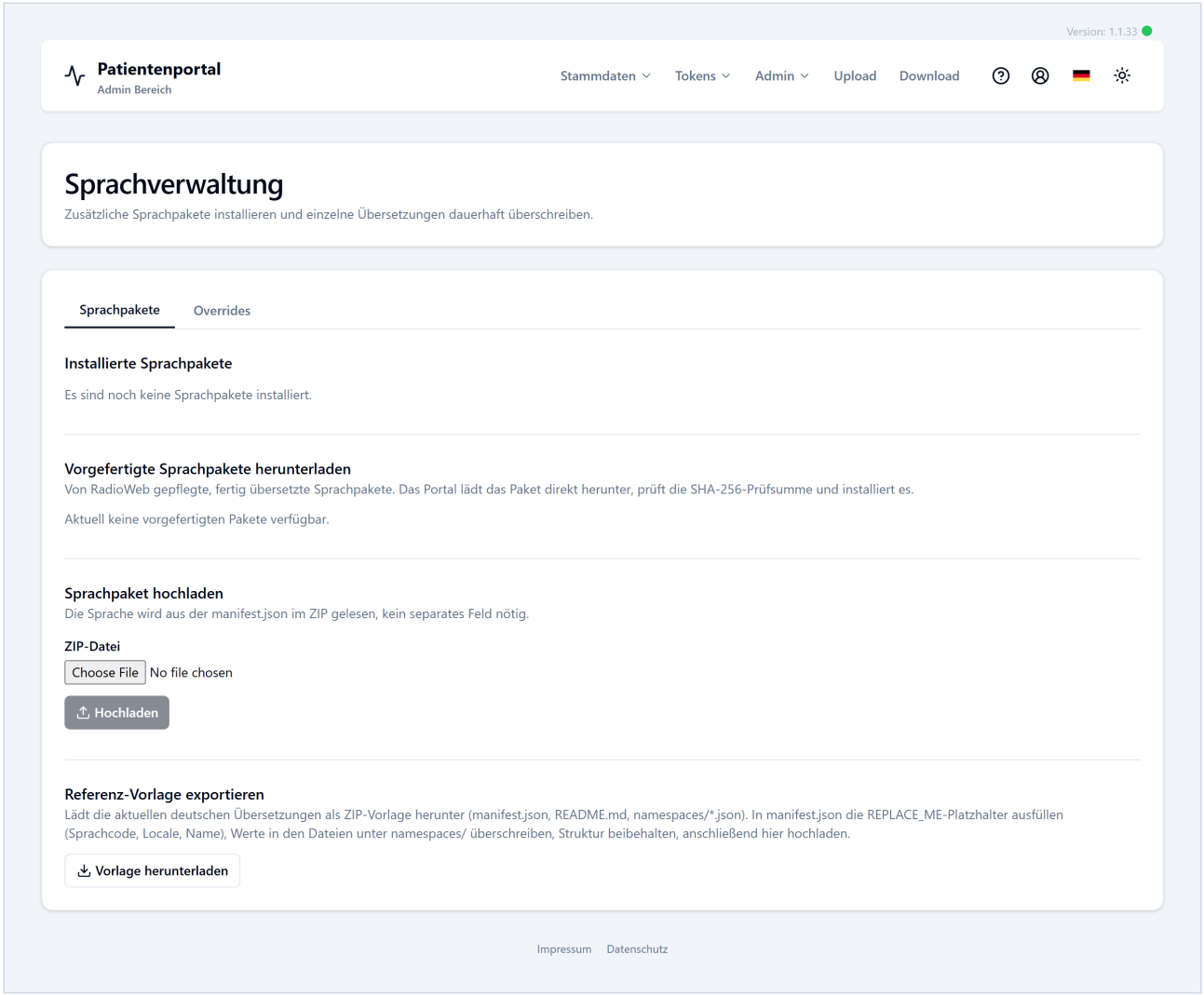


Abbildung 16. Sprachverwaltung, Reiter Sprachpakete

Sprachpakete

Installierte Sprachpakete

Liste der installierten Sprachen mit Version und Abdeckung; Pakete lassen sich aktualisieren oder entfernen.

Vorgefertigte Sprachpakete herunterladen

Von RadioWeb gepflegte, fertig übersetzte Pakete (z. B. Polnisch, Rumänisch, Russisch, Türkisch, Ukrainisch). Nach Bestätigung lädt das Portal das Paket selbst von `download.radioweb.de`, prüft die SHA-256-Prüfsumme und installiert es. Ist der Download-Server vom Portal aus nicht erreichbar, können Sie das Paket im Browser herunterladen und anschließend hochladen.

Sprachpaket hochladen

Eine ZIP-Datei mit `manifest.json` und den Übersetzungsdateien hochladen; die Sprache wird aus dem Manifest gelesen.

Referenz-Vorlage exportieren

Lädt die aktuellen deutschen Texte als ZIP-Vorlage für eine eigene Übersetzung herunter. Platzhalter `REPLACE_ME` in `manifest.json` ausfüllen, Texte unter `namespaces/` übersetzen, Struktur

beibehalten, anschließend hochladen.

Overrides

Im Reiter **Overrides** überschreiben Sie einzelne Texte einer Sprache dauerhaft – zum Beispiel, um Bezeichnungen an die Sprache Ihrer Praxis anzupassen. Overrides bleiben bei Updates des Portals erhalten.



Auch die Texte der Ausdruck-Vorlagen (Namespace `templates`) lassen sich hier anpassen.

Audit-Log

Das **Audit-Log** protokolliert alle sicherheitsrelevanten Zugriffe und Aktionen im Portal: Anmeldungen, Token-Prüfungen, das Ansehen von Patienten und Studien, Downloads, Freigaben und Verwaltungsaktionen. Die Einträge sind gegen nachträgliche Veränderung geschützt (HMAC-Signatur) und dienen dem Nachweis gegenüber Datenschutzbehörden und Patienten.

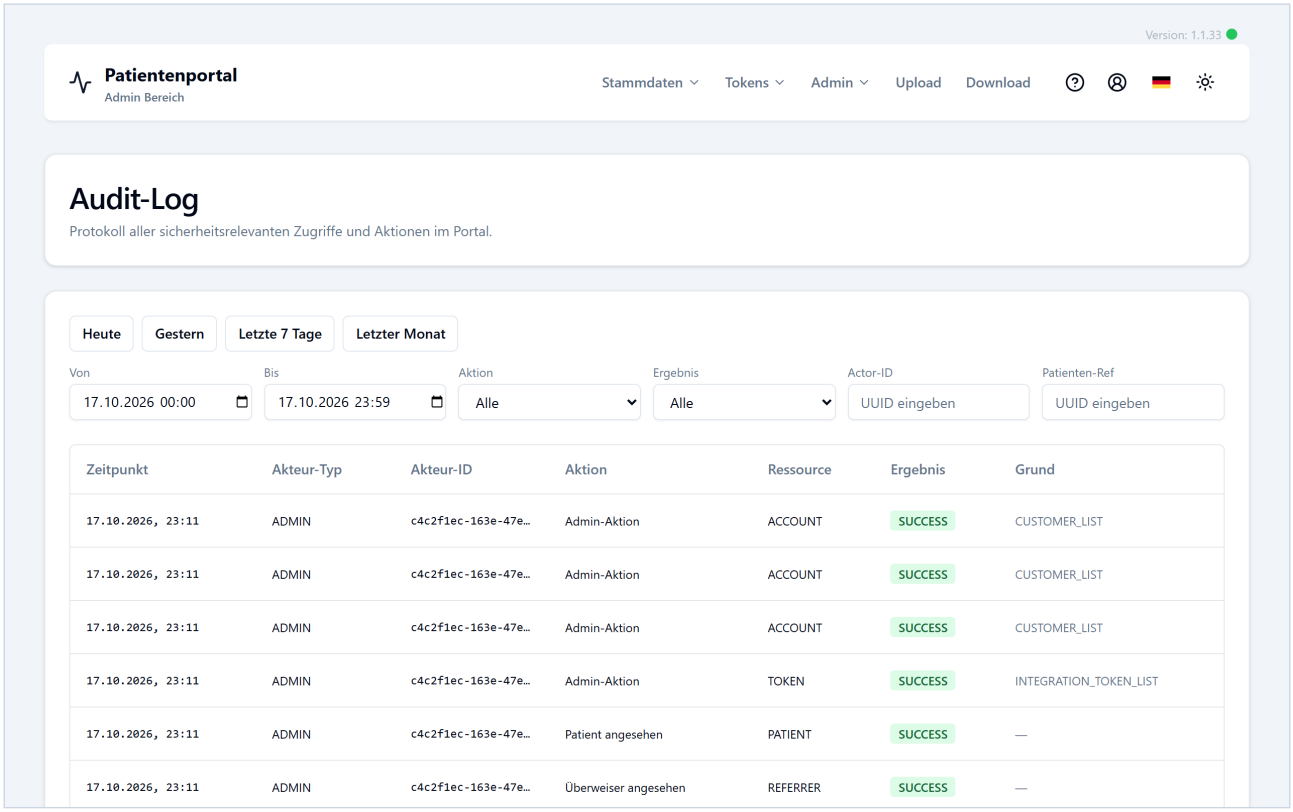


Abbildung 17. Audit-Log

Filtern

- **Schnellauswahl**: *Heute*, *Gestern*, *Letzte 7 Tage*, *Letzter Monat*, *Alle* (ohne Zeitraum-Einschränkung)
- **Von** / **Bis**: freier Zeitraum
- **Aktion** (z. B. „Studie angesehen“, „Token-Login erfolgreich“) und **Ergebnis** (Erfolg/Fehler)
- **Actor-ID**: alle Aktionen eines bestimmten Benutzers oder Tokens

- **Patienten-Ref**: alle Zugriffe auf einen bestimmten Patienten – z. B. zur Beantwortung eines Auskunftsersuchens nach Art. 15 DSGVO

Spalten

Spalte	Bedeutung
Zeitpunkt	Datum und Uhrzeit
Akteur-Typ	`ADMIN`, `CUSTOMER`, `REFERRER`, `PATIENT`, `STUDY` oder `ANONYMOUS` (vor der Anmeldung)
Akteur-ID	Interne Kennung des Benutzers bzw. Tokens
Aktion	Was geschah
Ressource	Betroffenes Objekt (z. B. `STUDY`, `TOKEN`, `ACCOUNT`)
Ergebnis	`SUCCESS` oder Fehler
Grund	Zusätzliche Information, z. B. `CUSTOMER_CREATE` oder `PACS_QUERY_CACHED`

Archive

Unter **Archive** verwalten Sie die PACS-Archive, aus denen das Portal Untersuchungen per DICOM Query/Retrieve abruft. Kunden und Überweiser ohne eigene Zuordnung verwenden automatisch das **Standard**-Archiv.

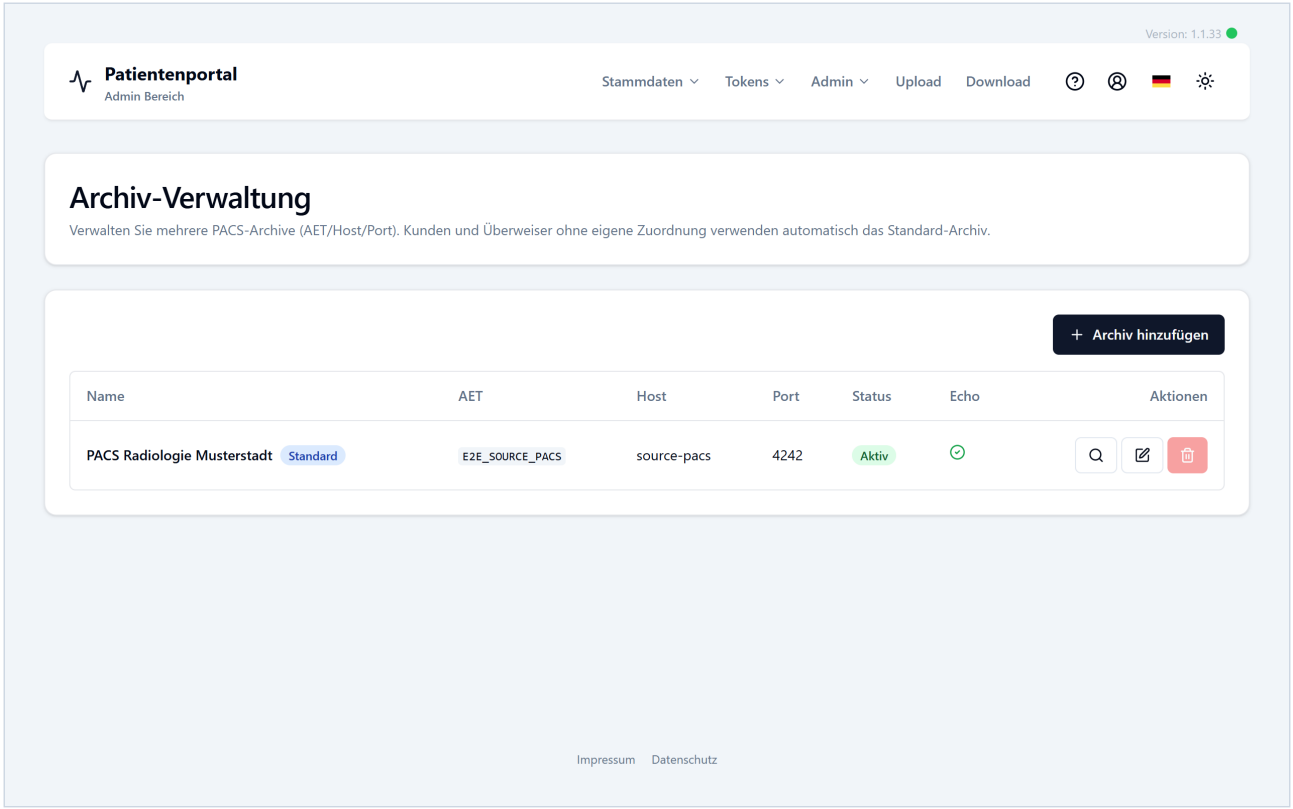


Abbildung 18. Archiv-Verwaltung

Die Tabelle zeigt Name, AET, Host, Port, Status und das Ergebnis des letzten Verbindungstests (**Echo**).

Archiv anlegen und bearbeiten

1. Klicken Sie auf **Archiv hinzufügen** (bzw. auf das Stift-Symbol).
2. Geben Sie **Name**, **AET** (AE-Title des PACS), **Host / IP** und **Port** ein, optional eine **Beschreibung**; über **Aktiv** schalten Sie das Archiv ein oder aus.
3. Prüfen Sie mit **Verbindung testen** (C-ECHO) die Erreichbarkeit und speichern Sie.



Damit das Portal Bilder abrufen darf, muss es im PACS als DICOM-Knoten eingetragen sein – mit dem AE-Title und Port des Portals (siehe Ersteinrichtung).

Query-Test

Über das Lupen-Symbol führen Sie eine Testabfrage gegen das Archiv aus: Suchen Sie nach Patienten-ID, Name, Study-UID oder Accession-Nr., optional mit Zeitraum. So prüfen Sie, ob ein Patient im PACS gefunden wird und mit welchen DICOM-Werten (z. B. für die Zuordnung von Überweisern).



Das Standard-Archiv kann nicht gelöscht werden.

PACS-Abfrage

Unter `/admin/pacs` steht Administratoren zusätzlich eine **PACS-Abfrage** zur Verfügung: Auswahl des Archivs, Zeitraum, Kunde und Überweiser – mit Patienten-, Studien- und Serienliste. Damit prüfen Sie, welche Daten ein bestimmter Kunde oder Überweiser zu sehen bekommt.

DirectView

Im Abschnitt **DirectView** des Archiv-Dialogs geben Sie ein Archiv für die Einbettung des Bildbetrachters in andere Anwendungen frei und legen Reihenfolge, Fremdarchiv und das DICOM-Attribut der Fallnummer fest. Die Spalte **DirectView** der Tabelle zeigt die Freigabe. Details: DirectView.

HL7-Kommunikation

Das Portal tauscht HL7-v2-Nachrichten per MLLP mit einem RIS/KIS aus – ohne die gdt-hl7-bridge. Es sendet die Zugangskarte eines Zugangscodes als **MDM^T02** (PDF als Base64 in OBX-5), storniert sie beim Widerruf mit **MDM^T11**, nimmt Aufträge (**ORM^O01**) entgegen, aus denen sofort ein Zugangscode entsteht, und übernimmt Patientenänderungen (**ADT^A08/A31**, **ADT^A40/A18/A34/A36**, **ADT^A47/A46**).



HL7 ist ein lizenzpflichtiges Modul. Ist es nicht aktiv, ist **Admin** → **HL7** ausgeblendet, eingehende Nachrichten werden mit `AR` beantwortet und es werden keine Nachrichten versendet. Bereits erstellte Nachrichten bleiben in der Warteschlange.

Alles liegt unter **Admin** → **HL7** mit den Reitern **Partner**, **Nachrichten**, **Mapping Eingang**, **Mapping Ausgang** und **Events**. Die Verarbeitung folgt immer derselben Kette:



Freigaben entstehen auch ohne HL7-Auftrag (Token-Generator im Browser, PDF-Endpunkt, HL7-Endpunkt). Sie lösen dieselben Events aus; die Event-Abos entscheiden, wer welche Nachricht bekommt. Ohne passendes Abo sendet das Portal nichts.

Beispiel: Auftrag aus dem RIS, Zugangskarte zurück

1. **Partner** anlegen: Host/Port des RIS, **Anwendung** `RIS` (MSH-3 der Aufträge, MSH-5 der Antworten), **Kunde** der Praxis. Unter **Erweitert** ist für `ORM^O01` das Mapping **ORM Standard** vorbelegt.
2. **Events** → Abo „Zugangskarte an RIS“: Ereignis **Freigabe erstellt**, Quelle **Auftrag (ORM)**, Empfänger **Absender des Auftrags**, Mapping **MDM^T02 Standard**.
3. Zweites Abo „Storno an RIS“: Ereignis **Freigabe widerrufen**, Quellen **Freigabe widerrufen** und **Auftrag storniert/ersetzt**, Empfänger **Absender des Auftrags**, Mapping **MDM^T11 Standard**.
4. **Einstellungen** → **HL7** → **Empfang** einschalten und den Port freigeben (siehe Empfang einrichten).

Ein `ORC|NW` erzeugt jetzt einen Zugangscode und schickt die Zugangskarte als MDM^T02 an das RIS zurück; `ORC|CA` widerruft ihn und sendet MDM^T11. Beides steht unter **Nachrichten**.

Partner

Ein Partner ist ein Kommunikationspartner (RIS/KIS, ePA-Konnektor, Dokumentenarchiv). Es gibt beliebig viele.

Allgemein

Feld	Bedeutung
Host / Port	MLLP-Empfänger (TCP). TLS wird noch nicht unterstützt.
Anwendung / Einrichtung	Kennung des Partners, nur einmal einzutragen: beim **Senden** MSH-5/MSH-6, beim **Empfang** die erwartete MSH-3/MSH-4 (Einrichtung leer = jede). Komponenten mit `^` trennen.
Kunde	Kunde der Zugangscodes, die aus Aufträgen dieses Partners entstehen.
Aktiv	Inaktive Partner pausieren den Versand; Nachrichten bleiben in der Warteschlange und werden nach dem Reaktivieren zugestellt. Von inaktiven Partnern wird nichts angenommen.

Die eigene Kennung des Portals (MSH-3/MSH-4 aller gesendeten Nachrichten und Quittungen) steht unter **Einstellungen** → **HL7** → **Absender** (`hl7.group.sender.application`, `hl7.group.sender.facility`).

Erweitert – mit Vorbelegung, meist nicht zu ändern:

Feld	Bedeutung
HL7-Version	MSH-12 (Standard 2.5)

Feld	Bedeutung
Zeichensatz	UTF-8 oder ISO-8859-1; wird so übertragen und in MSH-18 angegeben. Zeichen, die ISO-8859-1 nicht kennt, werden ohne Akzent übertragen.
Verarbeitungskennung	MSH-11: P (Produktion), T (Schulung), D (Fehlersuche)
Timeouts	Verbindungsaufbau (10 000 ms) und Warten auf die Empfangsbestätigung (30 000 ms)
Empfang	Nachrichten von diesem Partner annehmen (Standard an) und erlaubte Absenderadressen (IP/CIDR)
Eingangs-Mapping je Nachrichtentyp	z. B. `ORM^O01` → **ORM Standard**. Ohne Mapping wird der Typ mit `AR` abgelehnt.

Die Schaltfläche in der Spalte **Verbindung** testet den TCP-Verbindungsaufbau (es wird keine Nachricht gesendet). Partner mit Event-Abos oder Nachrichten können nicht gelöscht, nur deaktiviert werden.

Nachrichten

Der Reiter listet alle gesendeten und empfangenen Nachrichten mit Partner, Kunde, Patient, Quelle, Status und Versuchen (Filter nach Status, Partner, Quelle, Richtung, Typ; Suche nach Control-ID oder Patienten-ID). Aktionen:

- **Details**: Nachricht (der Base64-Inhalt ist gekürzt), Ereignis, Event-Abo und Mapping, Empfangsbestätigung, Fehler, SHA-256-Prüfsumme, PDF herunterladen
- **Jetzt erneut versuchen**: wartende Nachricht sofort zustellen (z. B. nachdem der Partner wieder erreichbar ist)
- **Abbrechen**: wartende Nachricht nicht weiter zustellen
- **Erneut senden**: abgeschlossene Nachricht als **neue** Nachricht (neue Control-ID, gleiche Dokumentnummer, gleiches Mapping) aus dem Zugangscode neu erzeugen – bei Dokumenten nur, solange der Zugangscode gültig ist

Warteschlange und Zustellung

Jede Nachricht wird zusammen mit dem auslösenden Vorgang gespeichert und danach zugestellt. Die Empfangsbestätigung (ACK, MSA-1) wird ausgewertet:

- `AA`/`CA` → **Zugestellt**
- `AR`/`CR` → **Fehlgeschlagen** (keine Wiederholung)
- `AE`/`CE` → **Fehlgeschlagen**; mit der Einstellung `hl7.group.retry.ack_ae` stattdessen erneuter Versuch
- keine oder unlesbare Bestätigung, Timeout, Verbindungsfehler → **Erneuter Versuch geplant**: nach 30 s, 1 min, 2 min … bis höchstens `hl7.group.retry.max_backoff_minutes`; nach `hl7.group.retry.max_attempts` Versuchen **Fehlgeschlagen**.

Automatische Wiederholungen senden dieselbe Nachricht mit derselben Control-ID (MSH-10). Kann eine Nachricht nicht erzeugt werden (z. B. PDF-Fehler oder ein Mapping, das keine gültige Nachricht

ergibt), steht sie mit Status **Fehlgeschlagen** und dem Grund in der Historie; der Zugangscode bzw. das PDF entsteht trotzdem.

Alle Vorgänge stehen im Audit-Log (`HL7_MESSAGE_*`, `HL7_DOCUMENT_CANCEL_QUEUED`, `HL7_INBOUND_*`, `HL7_PARTNER_*`, `HL7_MAPPING_*`, `HL7_SUBSCRIPTION_*`).

Aufbewahrung (Datenschutz)

Nachrichten enthalten Patientendaten und die Zugangskarte. Der Inhalt abgeschlossener Nachrichten wird nach `hl7.group.retention.payload_days` (Standard 30) gelöscht; Status und Prüfsumme bleiben. Nach `hl7.group.retention.message_days` (Standard 365) wird der Eintrag ganz gelöscht. Wartende Nachrichten werden nie gelöscht. Beim Löschen eines Patienten werden seine HL7-Nachrichten mitgelöscht; eine dabei ausgelöste Stornomeldung bleibt bis zur Zustellung erhalten.

Events

Ein Event-Abo legt fest, welches Ereignis welche Nachricht an welchen Empfänger auslöst. Ein Ereignis kann mehrere Abos haben (z. B. an das RIS **und** an ein Archiv), und mehrere Quellen können dasselbe Mapping nutzen.

Feld	Bedeutung
Ereignis	**Freigabe erstellt** (`SHARE_CREATED`, Nachricht mit Zugangskarte), **Freigabe widerrufen** (`SHARE_REVOKED`, Storno), **Patient geändert** (`PATIENT_UPDATED`) oder **Patienten zusammengeführt** (`PATIENT_MERGED`)
Quellen	Wodurch das Ereignis entstand (siehe unten); mindestens eine
Kunde	Nur Freigaben dieses Kunden (bei Patienten-Events: Patienten mit einem Zugangscode dieses Kunden), leer = alle
Empfänger	**Fester Partner** oder **Absender des Auftrags** (der Partner, von dem der ORM kam; nur für Freigaben aus Aufträgen). Patienten-Events gehen nur an feste Partner, nie an den Absender der ADT-Nachricht.
Ausgangs-Mapping	Baut die Nachricht: **Freigabe erstellt** → MDM^T02, **Freigabe widerrufen** → MDM^T11, **Patient geändert** → ADT^A08, **Patienten zusammengeführt** → ADT^A40 oder ADT^A47.
Sprache	Sprache der Zugangskarte; leer = Sprache der Anfrage bzw. aus dem Auftrag

Ereignis	Quelle	Wann
Freigabe erstellt	Token-Generator	Zugangscode im Browser erzeugt – gesendet im Hintergrund, ohne Rückfrage an den Anwender (z. B. für ePA oder Dokumentenarchiv)
Freigabe erstellt	PDF-Endpunkt	Abruf über `/api/reports/pdf`. **Nicht** zusammen mit dem HL7-Versand der gdt-hl7-bridge nutzen, sonst erhält das RIS jedes Dokument doppelt.

Ereignis	Quelle	Wann
Freigabe erstellt	HL7-Endpunkt	`/api/reports/hl7` (Schnittstellenbeschreibung im Entwicklerhandbuch unter **Schnittstellen → HL7-Endpunkt**). Ohne Abo lehnt der Endpunkt ab und erzeugt keinen Code.
Freigabe erstellt	Auftrag (ORM)	Zugangscode aus einem ORM-Auftrag
Freigabe widerrufen	Freigabe widerrufen	Widerruf in der Freigaben-Übersicht (Admin, Kunde, Patient)
Freigabe widerrufen	Auftrag storniert/ersetzt	ORM-Storno (`CA`, `OC`, `DC`, `DR`) oder wiederholter Auftrag mit `repeat` = `REPLACE`
Freigabe widerrufen	Patient gelöscht	Patient samt Freigaben gelöscht
Patient geändert	Patientendaten (ADT)	ADT^A08/A31 oder ein Auftrag (ORM) hat Name oder Geburtsdatum eines bekannten Patienten geändert
Patienten zusammengeführt	Patientendaten (ADT)	ADT^A40/A18/A34/A36 oder ADT^A47/A46 hat die Patienten-ID geändert bzw. zwei Patienten zusammengeführt

Storno beim Widerruf (MDM^T11)

Beim Widerruf erhält jeder Empfänger eines Abos **Freigabe widerrufen** für jedes Dokument, das **er** zu diesem Zugangscode bekommen hat, eine Stornomeldung mit derselben **Dokumentnummer** (TXA-12) und Verfügbarkeit `CA` (TXA-19), ohne PDF:

- einmal pro Dokument – auch wenn es mehrfach gesendet wurde; ein erneuter Widerruf sendet nichts;
- Partner, die kein Dokument des Codes erhalten haben, bekommen kein Storno;
- noch wartende Dokumente des Codes werden nicht mehr zugestellt (Status **Abgebrochen**), unabhängig von den Abos.

TXA-12 enthält eine eindeutige Dokumentnummer (`RW⋯`, die Control-ID der ersten Sendung). Die Auftragsnummer bzw. Patienten-ID steht im Event-Feld `document.orderNumber`, die Accession in TXA-14.

Mapping Ausgang

Ein Ausgangs-Mapping baut aus den Daten eines Events eine Nachricht. Eingebaut sind **MDM^T02 Standard** (Zugangskarte), **MDM^T11 Standard** (Storno) sowie **ADT^A08/A40/A47 Standard (out)** (weitergeleitete Patientenänderung); sie werden vom Portal gepflegt und sind schreibgeschützt. Zum Anpassen **Kopieren** und die Kopie im Event-Abo wählen.

- Jede Zeile schreibt einen Wert in ein HL7-Feld: Ziel ist ein Pfad (`PID-5-1`, `OBX(2)-5`, `PID-3[2]-1`), Quelle ein **Event-Feld** (z. B. `patient.lastName`) oder ein **fester Wert**. Mehrere Quellen: die erste mit Wert zählt.
- Werte werden automatisch HL7-maskiert (`|` → `\F\`, `^` → `\S\` …); Komponenten und Wiederholungen

ergeben sich aus dem Pfad.

- **MSH** und **EVN** füllt das Portal: Absender aus den Einstellungen, Empfänger = Anwendung/Einrichtung des Partners, Zeitstempel, Nachrichtentyp, Control-ID, Version, Zeichensatz.
- Ein Segment wird nur geschrieben, wenn mindestens ein Wert aus dem Event darin gelandet ist – so entfallen z. B. die OBX-Segmente eines Stornos ohne PDF, obwohl sie feste Werte enthalten.
- Links zeigt der Editor alle Event-Felder mit Beispielwerten, unten die gerenderte Nachricht samt Strukturprüfung (HAPI).

Event-Felder: `customer.`, `patient.externalId/lastName/firstName/birthDate`, `token.`, `link`, `study.` (erste Studie, `study.count`), `order.` (Auftragsnummer, Accession, Study-UID), `visitNumber`, `document.id` (Dokumentnummer, TXA-12), `document.orderNumber`, `document.title`, `document.filename`, `document.pdfBase64`, `document.completionStatus`, `document.availability` (`AV`/`CA`), `event`, `source`, `lang`.

Event-Felder der Patienten-Events: `patient.externalId/lastName/firstName/birthDate` (neuer Stand), `prior.externalId` (bisherige ID, nur beim Zusammenführen; MRG-1), `action`, `event`, `source`. ADT^A08 enthält immer ein PV1-Segment (Patientenklasse `N`).



Die Standard-Mappings setzen Name und Geburtsdatum in die HL7-konformen Felder PID-5/PID-7. Die Vorlage der gdt-hl7-bridge verwendet PID-6/PID-8 – ein RIS, das auf die Bridge eingestellt ist, braucht ggf. eine angepasste Kopie.

Mapping Eingang

Ein Eingangs-Mapping macht aus einer empfangenen Nachricht ein **Verarbeitungsobjekt**. Der Partner wählt unter **Erweitert** pro Nachrichtentyp eines aus. Eingebaut sind **ORM Standard** und je ein **ADT^... Standard** für A08, A31, A40, A18, A34, A36, A47 und A46.

- Pro Zielfeld werden die Quellen der Reihe nach geprüft; die erste mit Wert zählt. Eine Quelle ist ein HL7-Pfad (`SEG-Feld-Komponente-Subkomponente`, z. B. `PID-3-1`; `OBR(2)-4` = zweites OBR; `PID-3[2]-1` = zweite Wiederholung; `PID-3[PI]-1` = die Wiederholung mit der Identifier-Art `PI` in Komponente 5, siehe Mehrere IDs in PID-3 / MRG-1; Z-Segmente wie jedes andere) oder ein fester Wert.
- Transformationen je Quelle, in Reihenfolge: Leerzeichen entfernen, Groß-/Kleinbuchstaben, **Wertetabelle** (z. B. `NW=CREATE`, mit Wert für alles andere), Standardwert, Datum (HL7 → ISO), Text voranstellen/anhängen.
- Im Editor eine Beispielnachricht einfügen (z. B. aus 7edit): Sie erscheint als Baum (Segment → Feld → Komponente). Eine Quelle auswählen und im Baum auf einen Pfad klicken übernimmt ihn. Darunter steht das Verarbeitungsobjekt, das das Mapping aus der Beispielnachricht ergibt.

Aufträge (ORM^O01)

Verarbeitungsobjekt und Standardbelegung (**ORM Standard**):

Feld	Standard	Bedeutung
`action`	`ORC-1` → Wertetabelle	`CREATE` (`NW`, `SN`), `UPDATE` (`XO`, `SC`, `XX`, `SS`), `CANCEL` (`CA`, `OC`, `DC`, `DR`), sonst `IGNORE` (quittiert, nichts passiert)

Feld	Standard	Bedeutung
orderNumber	ORC-2-1, OBR-2-1	Auftragsnummer, eindeutig je Partner
fillerOrderNumber	ORC-3-1, OBR-3-1	
patient.id	PID-3-1	Patient wird angelegt bzw. aktualisiert
patient.lastName / patient.firstName	PID-5-1 / PID-5-2	
patient.birthDate	PID-7-1 → Datum	Pflicht, wenn der Code per Geburtsdatum geschützt ist
accession	OBR-18, ORC-3-1, OBR-3-1	
studyUid	ZDS-1-1	
visitNumber	PV1-19-1	Fallnummer, geht als Event-Feld visitNumber in die Antwort (PV1-19)
scope	fest PATIENT	Gewünschte Freigabeebene PATIENT, ACCESSION oder STUDY
scopeFallback	–	Ausweich-Ebenen, kommagetrennt (z. B. ACCESSION,PATIENT)
maxScope	–	Weiteste erlaubte Ebene
lang	–	Sprache der Zugangskarte
repeat	– (= KEEP)	Wiederholter Auftrag, siehe unten

Beispiel Ebene aus einem Z-Segment: scope ← ZRW-1 mit Wertetabelle P=PATIENT, A=ACCESSION, S=STUDY.

Ablauf:

- **CREATE:** Zugangscode sofort, Event **Freigabe erstellt** (Quelle **Auftrag**). Ist die Auftragsnummer schon bekannt und ihr Code aktiv, entscheidet repeat (siehe unten). Studien, die noch nicht existieren, ergänzt das Portal beim Login mit dem Code (Abfrage am PACS per Accession bzw. Study-UID) und sobald die Bilder im Portal eintreffen – nur Studien desselben Patienten.
- **Patientendaten:** Name und Geburtsdatum aus PID werden übernommen. Ändern sie einen bekannten Patienten, folgt wie bei ADT^A08 die lokale Orthanc-Kopie (Fehler → AE, nichts übernommen) und das Event **Patient geändert** wird ausgelöst (nie zurück an den Absender).
- **UPDATE:** Accession, Study-UID und Patientendaten werden übernommen, der Code bleibt; ein unbekannter Auftrag (oder einer ohne aktiven Code) wird wie **CREATE** behandelt.
- **CANCEL:** alle Zugangscodes des Auftrags widerrufen, Event **Freigabe widerrufen** (Quelle **Auftrag storniert/ersetzt**).
- **Kunde:** der Kunde des Partners (**Allgemein**); ohne Kunde wird der Auftrag mit AR abgelehnt.

Wiederholter Auftrag: Ein Auftrag ist bekannt, wenn Partner und Auftragsnummer (orderNumber, ersatzweise fillerOrderNumber) übereinstimmen. Ein neuer Code entsteht immer, wenn der Auftrag

storniert oder sein Code widerrufen wurde. Hat der Auftrag noch einen aktiven Code, bestimmt `repeat`, was ein erneutes **CREATE** bewirkt:

`repeat`	**Verhalten**
`KEEP` (Standard, auch leer)	Auftrag aktualisieren (Accession, Study-UID), Code und Ebene bleiben. Quittung „Order already known, access code unchanged“.
`REPLACE`	Alten Code widerrufen (Storno an seine Empfänger über die Quelle **Auftrag storniert/ersetzt**), neuen Code mit neu bestimmter Ebene erzeugen und als **Freigabe erstellt** senden.
`NEW`	Zusätzlichen Code erzeugen; der alte bleibt gültig. Ein späteres Storno widerruft alle Codes des Auftrags.

`repeat` kann fest im Mapping stehen (gilt dann für alle Aufträge des Partners) oder aus der Nachricht kommen, z. B. `ZRW-2` mit Wertetabelle `N=NEW`, `R=REPLACE` und `KEEP` für alles andere. Eine Auftragsnummer gehört immer zu einem Patienten: Kommt sie mit einer anderen Patienten-ID, wird die Nachricht mit `AR` abgelehnt („Order number already used for another patient“) und nichts geändert.

Freigabeebene – die Regel selbst ist fest, das Mapping liefert nur die Werte:

1. **Gewünschte Ebene** `scope` (leer = `PATIENT`; ein anderer Wert als die drei Ebenen → Ablehnung).
2. **Maximalebene:** die engere aus `maxScope` und `token.pdf.max_scope` des Kunden. Eine weitere gewünschte Ebene wird auf sie reduziert.
3. **Nötige ID vorhanden?** Studie braucht die Study-UID, Accession die Accession-Nummer. Fehlt sie, werden die Ebenen aus `scopeFallback` der Reihe nach versucht (jeweils innerhalb der Maximalebene). Ohne passende Ausweich-Ebene wird der Auftrag mit `AR` abgelehnt.

Die Quittung (MSA-3) und die Historie zeigen, welche Ebene wie entstanden ist, z. B. „Access code created (ACCESSION): level STUDY; Study Instance UID missing for level STUDY → fallback ACCESSION“.

Patientendaten (ADT)

Das RIS meldet Patientenänderungen per ADT. Das Quell-PACS bekommt dieselben Nachrichten vom RIS und bleibt führend; das Portal zieht nach: seinen Patienten-Datensatz, die daran hängenden Freigaben und die lokale Orthanc-Kopie der Studien. Für jeden Typ gibt es ein eingebautes Eingangs-Mapping (**ADT^A08 Standard**, **ADT^A31 Standard** …); beim Partner unter **Erweitert** die Typen auswählen, die das RIS/KIS sendet, sonst wird der Typ mit `AR` abgelehnt.

Nachricht	`action`	**Verhalten**
ADT^A08	`UPDATE`	Name und Geburtsdatum aus PID übernehmen. **Achtung:** Das Geburtsdatum ist der zweite Faktor beim Login mit Geburtsdatum – nach einer Korrektur gilt das neue Datum.
ADT^A47	`CHANGE_ID`	Der Patient `prior.id` (MRG-1) bekommt die ID `patient.id` (PID-3).

Nachricht	action	Verhalten
ADT^A40	MERGE	Wie A47; gibt es die neue ID im Portal schon, werden Studien, Freigaben, Patientenkonto, Aufträge und HL7-Verlauf auf diesen Patienten umgehängt und der bisherige Datensatz gelöscht.
ADT^A31	UPDATE	Personendaten aktualisieren (Master Patient Index); wie A08. Viele KIS senden A31 statt A08.
ADT^A18	MERGE	Zusammenführung (alt, bis v2.3); wie A40.
ADT^A34	MERGE	Zusammenführung, nur Patienten-ID (alt); wie A40.
ADT^A36	MERGE	Zusammenführung, Patienten-ID und Fallnummer (alt); wie A40, die Fallnummer (MRG-5) wird ignoriert.
ADT^A46	CHANGE_ID	Patienten-ID ändern (alt, Vorgänger von A47); wie A47.

A18, A34, A36 und A46 sind seit HL7 v2.3.1 bzw. v2.4 abgekündigt, werden aber von vielen Systemen noch gesendet; das Portal verarbeitet sie wie ihre Nachfolger.

Bewusst **nicht** verarbeitet (mit AR abgelehnt): A23/A29 (Löschen – Freigaben werden nicht automatisch widerrufen), A41/A42/A44/A45/A49/A50 (Fall, Konto, Besuch – kennt das Portal nicht), A24/A37 (Verknüpfen/Trennen), A01/A04/A05 (Aufnahme/Registrierung). A30/A39 (wie Zusammenführung) und A28 (wie Aktualisierung) können bei Bedarf eines konkreten RIS ergänzt werden.

- Nur Patienten, die das Portal schon kennt, werden geändert; ADT legt keine Patienten an. Unbekannte Patienten werden mit AA quittiert („unknown … nothing to update“).
- **Lokale Orthanc-Kopie:** Die Studien des Patienten (und Studien, die noch die alte ID tragen) werden umgeschrieben (PatientID, Name, Geburtsdatum). Study-, Series- und SOP-Instance-UIDs bleiben gleich, nur die Orthanc-interne ID ändert sich. Schlägt das fehl, ändert das Portal nichts und quittiert mit AE; der Partner kann die Nachricht erneut senden.
- **PACS-Ansicht der Zuweiser:** Nach erfolgreicher Verarbeitung übernimmt das Portal Name, Geburtsdatum und Patienten-ID auch in den PACS-Cache aller Zuweiser (Einträge mit der neuen oder alten ID und die bekannten Studien des Patienten). Zuweiser sehen die Änderung sofort, die Suche nach dem neuen Namen findet die Studie, und der Abruf aller Studien des Patienten fragt mit der neuen ID ab – ohne erneute PACS-Abfrage. Ein Fehler dabei wird nur protokolliert und ändert die Quittung nicht; das gilt ebenso für Patientenänderungen per Auftrag (ORM). Änderungen, die nur im PACS gemacht werden (ohne ADT), erscheinen nach spätestens 30 Tagen (ältere Studien) bzw. 24 Stunden (letzte Woche) oder sofort über **Aktualisieren** in der PACS-Ansicht.
- Haben beim Zusammenführen **beide** Patienten ein Patientenkonto (Login), wird die Nachricht mit AR abgelehnt („Both patients have a portal account“); das muss ein Admin klären.
- Wiederholungen sind unschädlich: Ein bereits zusammengeführter Patient ergibt AA „already merged“.
- **Mehrere Paare in einer Nachricht:** A40 (und die alten Zusammenführungen) darf die PID/MRG-Gruppe wiederholen. Das Portal verarbeitet alle Paare nacheinander in einer Transaktion: Scheitert ein Paar (Konflikt → AR, Orthanc-Fehler → AE), wird **nichts** übernommen; die Quittung nennt das

Paar („Pair 2: …“). Bei Erfolg nennen Quittung und Historie die Anzahl, z. B. „2 patient pairs processed: 1) Patients merged; 2) Patient id changed“. Das Mapping wird auf jedes Paar einzeln angewendet – `PID-3-1` und `MRG-1-1` meinen immer das gerade verarbeitete Paar (in eigenen Mappings kein `PID(2)-⋯` verwenden). Die Vorschau im Mapping-Editor zeigt das erste Paar.

- Danach lösen die Änderungen die Events **Patient geändert** bzw. **Patienten zusammengeführt** aus (siehe Events) – nie zurück an den Partner, von dem die Änderung kam.
- Audit-Log: `PATIENT_UPDATE` bzw. `PATIENT_MERGE`.

Beispiele: `backend/samples/hl7/adt/`.

Mehrere IDs in PID-3 / MRG-1

Die Standard-Mappings nehmen die erste Wiederholung (`PID-3-1`, `MRG-1-1`). Sendet ein KIS mehrere Patienten-IDs (z. B. KIS- und RIS-ID: `PID|1||K-100^^^KIS^PI~R-200^^^RIS^MR|⋯`), und das Portal bzw. das PACS kennt nur eine davon, das Mapping kopieren (**Mapping Eingang** → **Kopieren**) und in der Kopie die richtige ID wählen:

- **Nach Position:** `patient.id` ← `PID-3[2]-1`, `prior.id` ← `MRG-1[2]-1`. Nur geeignet, wenn das KIS die IDs immer in derselben Reihenfolge sendet.
- **Nach Identifier-Art (empfohlen):** `patient.id` ← `PID-3[MR]-1`, `prior.id` ← `MRG-1[MR]-1`. Gewählt wird die erste Wiederholung, deren Komponente 5 (Identifier Type Code, z. B. `PI`, `MR`, `PT`) passt; Groß-/Kleinschreibung egal. Fehlt sie, ist der Wert leer.
- Als zweite Quelle kann `PID-3-1` stehen bleiben, falls ein Absender die Identifier-Art nicht mitschickt.

Danach beim Partner unter **Erweitert** die Kopie statt des Standard-Mappings wählen – für jeden Typ, den das KIS sendet (auch ORM). Die Auswahl nach Identifier-Art gibt es nur beim Lesen (Eingang); im Ausgangs-Mapping sind Wiederholungen nur per Nummer möglich.

Empfang einrichten

Partner senden per MLLP an das Portal (TCP-Port 2575 im Backend-Container).

1. **Port freigeben:** In der `.env` `HL7_INBOUND_PORT` setzen, z. B. `HL7_INBOUND_PORT=2575` (Standard: nur `127.0.0.1`), Stack neu starten und die Firewall für die Adresse des RIS öffnen.
2. **Empfang einschalten: Einstellungen** → **HL7** → **Empfang** `hl7.group.inbound.enabled`. Ausgeschaltet schließt das Portal jede Verbindung sofort, ohne Quittung.
3. **Partner einrichten: Anwendung** (= MSH-3 des Partners), optional **Einrichtung** (MSH-4); unter **Erweitert** Empfang an, erlaubte Absenderadressen und ein Eingangs-Mapping je Nachrichtentyp.

Verhalten:

- Eine Nachricht wird dem Partner über MSH-3 (und MSH-4, falls eingetragen) zugeordnet; die Absenderadresse muss in den erlaubten Bereichen liegen. Unbekannte Absender erhalten `AR` und werden nur im Audit-Log (`HL7_INBOUND_REJECTED`) und im Backend-Log vermerkt.
- Nachrichtentypen ohne Eingangs-Mapping beim Partner werden mit `AR` abgelehnt.
- Jede Nachricht eines bekannten Partners steht in der Historie (Richtung **Empfangen**) samt

gesendeter Quittung, Status **Verarbeitet** (`AA`) oder **Abgelehnt** (`AR`/`AE`), mit dem Kunden des erzeugten Zugangscodes bzw. des Partners.

- Sendet der Partner eine bereits **verarbeitete** Nachricht mit derselben Control-ID (MSH-10) erneut, erhält er dieselbe Quittung; sie wird nicht ein zweites Mal verarbeitet. Eine **abgelehnte** Nachricht hat nichts verändert und wird bei erneutem Senden neu verarbeitet (z. B. nach einer Korrektur der Einstellungen).
- Zeichensatz: laut MSH-18 (`UNICODE UTF-8`, `8859/1`), sonst der Zeichensatz des Partners. Die Quittung wird im selben Zeichensatz gesendet.



Erlaubte Absenderadressen eintragen. Ohne Eintrag nimmt das Portal Nachrichten mit der passenden MSH-3 von jeder Adresse an.

DirectView

DirectView bettet den HTML5-Bildbetrachter des Portals in eine andere Anwendung ein und zeigt dort Archivdaten direkt an. Die **aufrufende Anwendung** kann z. B. ein KIS, ein RIS, eine Software zur Wunddokumentation, eine Praxissoftware oder eine Anwendung aus der Veterinärmedizin sein. Sie bettet dazu die Adresse `/directview` des Portals in einem iframe ein.

Das Portal holt die Bilder per DICOM Query/Retrieve in seinen Bildspeicher (Orthanc) und zeigt sie mit dem eingebauten Bildbetrachter. Patienten und Studien werden dabei **nicht** in der Portal-Datenbank angelegt. Die Bilder bleiben nur so lange im Bildspeicher, wie sie gebraucht werden.

DirectView ist ein lizenzpflichtiges Modul (siehe Lizenz & Module). Der Menüpunkt **Admin → DirectView** erscheint, sobald das Modul aktiv ist.

Ablauf eines Aufrufs

1. Die aufrufende Anwendung öffnet `/directview` mit einem Einmal-Code (empfohlen) oder einem DirectView-API-Key und genau einem Suchparameter (z. B. der Study Instance UID).
2. Das Portal sucht die Untersuchung im **Primärarchiv**. Sie muss genau einem Patienten gehören, sonst werden aus Sicherheitsgründen keine Bilder angezeigt.
3. Die aufgerufene Untersuchung wird Serie für Serie geladen; der Bildbetrachter öffnet sich, sobald sie vollständig ist.
4. Anschließend werden die **Voruntersuchungen** geladen, die die Regeln auswählen, zuerst aus dem Primärarchiv, danach aus den weiteren Archiven in ihrer Reihenfolge.
5. In der Kopfzeile meldet die Anzeige weitere geladene Studien; **anzeigen** lädt den Bildbetrachter mit ihnen neu. In der Studienliste kann der Nutzer Studien, die keine Regel ausgewählt hat, einzeln **laden**.

Der Nutzer sieht ausschließlich Studien des Patienten aus dem Aufruf.

Voraussetzungen

Modul einschalten

Schalten Sie DirectView unter Lizenz & Module ein.

Archive freigeben

Unter Archive legen Sie je Archiv im Abschnitt **DirectView** fest:

- **Für DirectView freigeben**: Nur freigegebene Archive werden abgefragt.
- **Reihenfolge**: Archive werden aufsteigend abgefragt. Das erste freigegebene Archiv, das kein Fremdarchiv ist, ist das **Primärarchiv**.
- **Fremdarchiv**: Archiv mit eigenen Patienten-IDs (z. B. externe oder ältere Bilder). Hier wird der Patient über Nachname, ersten Vornamen und Geburtsdatum zugeordnet, bei vorhandenem Geschlecht auch darüber. Schreibweisen mit Umlauten, Bindestrich oder Groß-/Kleinschreibung werden angeglichen. Studien von dort werden in der Anzeige als „Zuordnung über Name/Geburtsdatum“ gekennzeichnet.

  Das Verfahren ist bewusst für Fremdbildarchive gewählt: Deren Daten stammen aus zuweisenden Einrichtungen mit eigenen Patienten-IDs und werden meist nach etwa 30 Tagen wieder gelöscht (FIFO). Dass dort in diesem Zeitraum zwei verschiedene Patienten mit gleichem Namen und Geburtsdatum liegen, ist für ein regionales Krankenhaus so unwahrscheinlich, dass das Restrisiko vertretbar ist. Für Archive mit dauerhaftem, umfangreichem Bestand sollte die Option nicht verwendet werden.

- **DICOM-Attribut der Fallnummer**: welches Attribut beim Aufruf mit Fallnummer abgefragt wird (Standard `AdmissionID`).

API-Key anlegen

Unter **Admin** → **DirectView** → **API-Keys** legen Sie für jede aufrufende Anwendung einen eigenen Schlüssel an. Ein DirectView-API-Key öffnet ausschließlich DirectView, keine anderen Funktionen des Portals (anders als Integrations-Tokens).

- Der Schlüssel wird **nur einmal** beim Anlegen angezeigt; das Portal speichert ihn nicht im Klartext. Hinterlegen Sie ihn sofort in der aufrufenden Anwendung.
- **Erlaubte IP-Bereiche** sind Pflicht: die Netze der Geräte, auf denen die Anwendung läuft, und, beim Launch-Code, ihres Servers.
- **Aufrufe pro Minute** begrenzen die Last auf Archiv und Bildspeicher, falls ein Schlüssel missbraucht wird.
- **Benutzername erforderlich** lehnt Aufrufe ohne Benutzername der aufrufenden Anwendung ab.
- **Widerrufen** beendet auch laufende Sitzungen dieses Schlüssels sofort.

Einbettung erlauben

Der Betreiber trägt die Adresse der einbettenden Anwendung in die Variable `DIRECTVIEW_FRAME_ANCESTORS` ein (siehe Betrieb), sonst blockiert der Browser die Einbettung.

Aufruf aus der Anwendung

Empfohlen: Launch-Code (Server-zu-Server)

Der Server der Anwendung fordert mit dem API-Key einen Einmal-Code an und zeigt nur die zurückgegebene Adresse im iframe an. Der Schlüssel gelangt so nie in den Browser, und der Benutzername gilt im Audit-Log als bestätigt.

```
POST https://portal.klinik.de/api/directview/launch
X-DirectView-Key: <API-KEY>
Content-Type: application/json

{"studyuid": "1.2.276.123.456.789", "user": "<BENUTZER>"}
```

Antwort: `{"url": "https://portal.klinik.de/directview?launch=<CODE>", "expiresAt": "…"}`. Der Code gilt 60 Sekunden und genau einmal.

Alternative: API-Key in der iframe-Adresse

Nur wenn die Anwendung keine Server-Aufrufe kann:

```
https://portal.klinik.de/directview?apikey=<API-
KEY>&studyuid=1.2.276.123.456.789&user=<BENUTZER>
```

Der Schlüssel ist dann im HTML der Anwendung und im Browser sichtbar; der Benutzername gilt im Audit-Log als **nicht bestätigt**. Das Portal entfernt den Schlüssel sofort aus der Adresse und maskiert ihn in seinen Protokollen.

Parameter

Parameter	Bedeutung
`launch`	Einmal-Code aus `/api/directview/launch`
`apikey`	DirectView-API-Key (nur Alternative ohne Launch-Code)
`studyuid`	Study Instance UID der aufgerufenen Studie
`accnbr`	Accession Number der Untersuchung
`caseid`	Fallnummer (DICOM-Attribut je Archiv einstellbar)
`patid`	Patienten-ID im Primärarchiv; angezeigt wird die neueste Studie
`user`	optional: Benutzername in der aufrufenden Anwendung, wird im Audit-Log protokolliert

Genau einer der Parameter `studyuid`, `accnbr`, `caseid` oder `patid` muss angegeben sein. Platzhalter (`*`, `?`) sind nicht erlaubt.

Ein Aufruf ist so lange gültig, wie unter **Einstellungen** angegeben (Standard: 60 Minuten), und nur auf

dem Gerät, das ihn geöffnet hat (IP-Adresse und Browser). Das Zugriffstoken liegt nur im Arbeitsspeicher der Seite: Nach einem Neuladen oder nach Ablauf öffnet der Nutzer die Bilder erneut aus der aufrufenden Anwendung.

Regeln für Voruntersuchungen

Unter **Admin** → **DirectView** → **Regeln** legen Sie fest, welche Studien zusätzlich zur aufgerufenen geladen werden.

- **Auslöser**: Die Regel greift, wenn die aufgerufene Studie passt, z. B. Modalität `CT` und Studienbeschreibung `thorax`. Leere Felder passen immer.
- **Auswahl**: Welche Studien desselben Patienten geladen werden: Modalitäten (`SAME` = gleiche wie die aufgerufene Studie), Studienbeschreibung, Körperregion (beliebig, gleiche oder passend zu einem Ausdruck), Höchstalter in Monaten, höchstens so viele Studien und für welche Archive.
- Beschreibung und Körperregion werden als **reguläre Ausdrücke** ohne Beachtung der Groß-/Kleinschreibung geprüft, z. B. `thorax|lunge`. Die Körperregion stammt aus dem DICOM-Attribut `BodyPartExamined` der Serien (z. B. `CHEST`, `KNEE`). Es gilt die RE2-Syntax (lineare Laufzeit): Rückverweise wie `\1` und Lookaround wie `(?!…)` sind nicht erlaubt.

Alle aktiven Regeln, deren Auslöser passt, werden angewendet; die Einstellung **Höchstens automatisch geladene Voruntersuchungen** begrenzt die Gesamtzahl. Passt keine Regel, werden keine Voruntersuchungen automatisch geladen.

Mit **Regeln testen** sehen Sie für eine Study Instance UID oder Patienten-ID, welche Studien im Primärarchiv ausgewählt würden. Dabei werden keine Bilder abgerufen.

Einstellungen

Einstellung	Bedeutung
Gültigkeit eines Aufrufs	Minuten, die der Nutzer nach dem Öffnen aus der Anwendung Bilder ansehen kann (Standard 60)
Aufbewahrung im Bildspeicher	Stunden nach der letzten Nutzung, nach denen DirectView-Bilder gelöscht werden (Standard 24)
Höchstens automatisch geladene Voruntersuchungen	Obergrenze je Aufruf (Standard 20)
Gleichzeitige Abrufe	gleichzeitige C-MOVE-Abrufe aller Aufrufe zusammen (Standard 2)

Aufrufe, Bildspeicher und Audit-Log

- **Aufrufe** zeigt die letzten 100 Aufrufe mit Zeitpunkt, Art, Benutzer der Anwendung und Status.
- **Bildspeicher** zeigt Anzahl und Größe der DirectView-Bilder; **Jetzt aufräumen** löscht nicht mehr benötigte Bilder sofort. Studien, die das Portal selbst verwendet (z. B. für eine Freigabe), bleiben erhalten.
- Das Audit-Log protokolliert jeden Aufruf (Benutzer der Anwendung), jede abgerufene Studie (mit

Patienten-ID aus dem PACS) und verworfene Fremdarchiv-Treffer.

Betrieb

`DIRECTVIEW_FRAME_ANCESTORS` in der `.env` enthält die Adressen der Anwendungen, die DirectView einbetten dürfen, durch Leerzeichen getrennt, nur `https`, ohne Pfad:

```
DIRECTVIEW_FRAME_ANCESTORS=https://kis.klinik.de https://visite.klinik.de
```

Der CheckMK-Check `env_plausibility` meldet ungültige Einträge. Die Einbettungserlaubnis gilt nur für `/directview` und den Bildbetrachter.

Chrome und Edge prüfen zusätzlich den Zugriff auf das lokale Netz (**Local Network Access**): Läuft die einbettende Anwendung unter einer öffentlichen Adresse und das Portal unter einer Adresse im Kliniknetz, blockiert der Browser die Einbettung (`ERR_BLOCKED_BY_LOCAL_NETWORK_ACCESS_CHECKS`) oder fragt den Nutzer um Erlaubnis. Betreiben Sie beide im selben Netz, oder die Anwendung muss das iframe mit `allow="local-network-access"` einbetten.

Der Bildbetrachter läuft für DirectView unter einer eigenen Adresse (`/directview-viewer/`); der normale Bildbetrachter des Portals (`/viewer/`) bleibt gegen Einbettung geschützt.

Das Portal maskiert API-Keys, Launch-Codes und Zugangstokens in seinen eigenen Protokollen (nginx, Caddy). Vorgelagerte Proxys der Klinik (z. B. Pangolin oder ein Klinik-Reverse-Proxy) protokollieren die vollständige Adresse womöglich weiterhin – nutzen Sie daher möglichst den Launch-Code oder schalten Sie die Protokollierung von Query-Parametern dort ab.

Fragen an den Hersteller der aufrufenden Anwendung

Für die Anbindung klären Sie mit dem Hersteller der Anwendung (z. B. Telekom Healthcare für das KIS iMedOne / iMedOne Mobile):

1. Kann die Anwendung vor dem Öffnen des iframes einen Server-Aufruf (`POST` mit eigenem Header) machen und die zurückgegebene Adresse anzeigen? Dann den Launch-Code verwenden.
2. Welche Parameter stehen beim Aufruf zur Verfügung (Study Instance UID, Accession Number, Fallnummer, Patienten-ID, Benutzername)?
3. Von welchen Adressen kommen Server-Aufrufe und die Browser der Geräte, auf denen sie läuft (für die erlaubten IP-Bereiche)?
4. Unter welcher Adresse (Origin) läuft die Oberfläche, die das iframe einbettet (für `DIRECTVIEW_FRAME_ANCESTORS`)?
5. Läuft die Oberfläche der Anwendung im selben Netz wie das Portal? Falls sie aus dem Internet kommt: Kann das iframe mit `allow="local-network-access"` eingebettet werden?
6. Werden Zertifikate und Inhaltsrichtlinien (CSP) der eingebetteten Seite unterstützt, und wird das iframe mit `allow="fullscreen; local-network-access"` eingebettet?

Lizenz & Module

Einige Funktionen des Portals sind **lizenzpflichtige Module**:

Modul	Funktion
DirectView	Einbettung des HTML5-Bildbetrachters in andere Anwendungen zur direkten Anzeige von Archivdaten, ohne Speicherung im Portal (siehe DirectView)
HL7	HL7-Kommunikation mit RIS und KIS: Zugangscodes aus Aufträgen (ORM), Patientendaten (ADT), Versand und Storno der Zugangskarten (MDM) (siehe HL7-Kommunikation)
Zuweiserportal	Anmeldung und PACS-Ansicht für Überweiser (siehe Überweiser)
Mandanten (Kunden)	Anzahl der Kunden, die angelegt werden können

Ein Modul ist nur **aktiv**, wenn es **lizenziert** und **eingeschaltet** ist. Unter **Admin → Lizenz & Module** sehen Sie den Lizenzstatus und schalten lizenzierte Module ein oder aus. Menüpunkte und Seiten eines nicht aktiven Moduls (**Stammdaten → Überweiser**, **Admin → HL7**, **Admin → DirectView**) sind ausgeblendet.



Ab dieser Version benötigen auch Zuweiserportal und HL7 eine Lizenz. Installieren Sie die Lizenzdatei direkt nach dem Update. Bis dahin werden Anmeldungen von Überweisern abgelehnt, HL7-Nachrichten mit `AR` beantwortet und keine HL7-Nachrichten versendet. Daten und Einstellungen bleiben erhalten.

Lizenzdatei installieren

1. Öffnen Sie **Admin → Lizenz & Module**.
2. Klicken Sie auf **Lizenzdatei hochladen** und wählen Sie die von RadioWeb erhaltene Datei (`.json`).
3. Das Portal prüft die Signatur und die Portal-Adresse und zeigt anschließend Lizenznehmer, Gültigkeit und die lizenzierten Module.

Eine neue Lizenzdatei ersetzt die bisherige. Der Upload ist für Installationen ohne RadioWeb Manager gedacht (offline).

Zentral verwaltete Lizenz (RadioWeb Manager)

Bei Installationen über den RadioWeb Manager stellt RadioWeb die Lizenz im Manager aus. Der Updater spielt sie automatisch ein und tauscht sie bei einer Verlängerung aus, ohne Neustart des Portals. Die Seite zeigt dann als Quelle **Zentral verwaltet** und den Hinweis, dass kein Upload nötig ist.

- Eine zentral verwaltete Lizenz hat Vorrang vor einer hochgeladenen Lizenz. Solange sie gültig installiert ist, lehnt das Portal Uploads ab.
- Die Module schalten Sie weiterhin hier ein und aus.
- Fehlt die Lizenzdatei oder ist sie ungültig, gilt wieder eine zuvor hochgeladene Lizenz.

Technisch liegt die Datei als `license.json` im Lizenzverzeichnis des Servers (`/etc/<produkt>/license`, im Container `/run/radioweb/license`). Ohne Manager können Betreiber die Datei auch selbst dorthin legen.

Portal-Adresse

Die Lizenz gilt für bestimmte Portal-Adressen (Hostnamen). Maßgeblich ist die Einstellung **Frontend URL** (`frontend.url`). Passt sie nicht zur Lizenz, wird die Lizenz als **Ungültig** angezeigt und die Module sind nicht aktiv.

Status

Status	Bedeutung
Gültig	Lizenz in Ordnung
Läuft bald ab	weniger als 30 Tage bis zum Ende
Abgelaufen – Übergangsfrist	abgelaufen, das Modul läuft noch 14 Tage weiter
Abgelaufen	Modul ist abgeschaltet
Ungültig	Signatur, Schlüssel oder Portal-Adresse passen nicht
Nicht lizenziert	Modul ist nicht Teil der Lizenz

Läuft eine Lizenz ab, werden nur die Module abgeschaltet. Konfiguration und Daten bleiben erhalten und sind nach Einspielen einer neuen Lizenz sofort wieder verfügbar. Bereits erstellte HL7-Nachrichten bleiben in der Warteschlange und werden versendet, sobald das Modul wieder aktiv ist.

Module ein- und ausschalten

In der Tabelle **Module** schalten Sie jedes lizenzierte Modul über **Eingeschaltet** ein oder aus. Nicht lizenzierte Module lassen sich nicht einschalten. DirectView ist nach der Installation ausgeschaltet, die übrigen Module sind eingeschaltet.

Anzahl der Kunden (Mandanten)

Das Modul **Mandanten (Kunden)** hat keinen Schalter. Die Lizenz legt fest, wie viele Kunden angelegt werden können:

- **Ohne Lizenz** für das Modul (oder nach Ablauf der Übergangsfrist) ist **ein** Kunde erlaubt.
- **Mit Lizenz** gilt die lizenzierte Anzahl (mindestens 1) oder, ohne Anzahl, eine unbegrenzte Zahl.

Die Tabelle zeigt, wie viele Kunden angelegt sind und wie viele erlaubt sind. Ist das Kontingent erreicht, ist **Kunde hinzufügen** in der Kundenverwaltung gesperrt. Bestehen mehr Kunden, als die Lizenz erlaubt (z. B. nach Ablauf der Lizenz), bleiben alle bestehenden Kunden voll nutzbar; nur neue Kunden können nicht angelegt werden.

Überwachung

Der CheckMK-Check `license_status` warnt 30 Tage vor dem Ende der Lizenz oder eines eingeschalteten Moduls und bei eingeschalteten, aber nicht lizenzierten Modulen. Ab dem Ablauf meldet er kritisch, auch während der 14-tägigen Übergangsfrist, in der das Modul noch funktioniert. Die Restlaufzeit in Tagen liefert er als Messwert `days_remaining`. Alle Änderungen an Lizenz und Modulen stehen im Audit-Log.

Einstellungen

Unter **Einstellungen** (Menü **Admin**) konfigurieren Sie das Verhalten des Portals. Die Einstellungen sind in Reiter gegliedert; jede Einstellung zeigt Bezeichnung, technischen Schlüssel (z. B. `app.support_email`), Beschreibung und Ebene (`SYSTEM`).

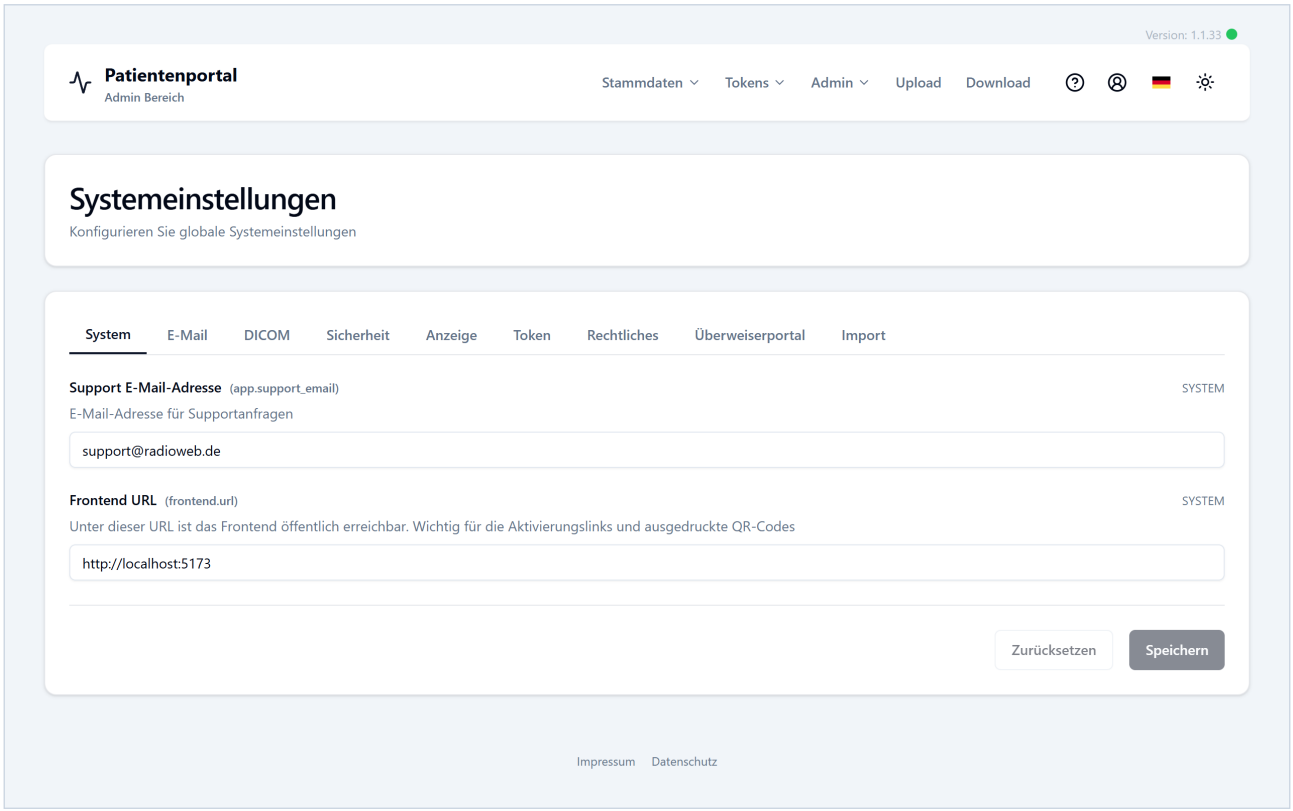


Abbildung 19. Systemeinstellungen

Reiter	Typische Einstellungen
System	Support-E-Mail-Adresse
E-Mail	SMTP-Server, Zugangsdaten und Absender für Aktivierungs-E-Mails und den Versand von Zugangslinks
DICOM	Betriebsmodus des Archivs: *Query/Retrieve* (Bilder bei Bedarf aus dem PACS abrufen, empfohlen) oder *Store* (Daten werden ins Portal gesendet und dort gehalten)
Sicherheit	Passwortregeln, Sitzungs-Timeouts je Rolle, welche Rollen welche Zugangscodes erstellen, welche Konten anlegen und welche Daten herunterladen dürfen, dauerhafter Login für Patienten

Reiter	Typische Einstellungen
Anzeige	Standardsprache, Datumsformat, Farbschema (hell/dunkel/System), **Anmeldeseite**: welche Anmeldeformulare (Zugangscode, E-Mail/Passwort) angezeigt werden und ob sie nebeneinander oder untereinander stehen
Token	Je Token-Typ (Patient, Studie, Überweiser): aktiv ja/nein, Absicherung (keine, Geburtsdatum, Passwort), Standard-Gültigkeit und wählbare Gültigkeitsdauern
Rechtliches	Angaben für Impressum und Datenschutzerklärung: Betreiber, Kontakt, Datenschutzbeauftragte(r), Aufsichtsbehörde, Ärztekammer, Registerangaben (werden im Portal unter **Impressum** / **Datenschutz** angezeigt)
Überweiserportal	Einstellungen der PACS-Ansicht für Überweiser
Import	DLX-Import und automatische Weiterleitung je Nutzergruppe, Ziel-Archiv (AE-Title, Host, Port) für Fremdaufnahmen – global oder je Nutzergruppe; Importliste der Upload-Seite: maximale Anzahl Einträge je Karte (Standard 20) und Zeitraum in Stunden (Standard 24)

Ändern Sie die gewünschten Werte und klicken Sie auf **Speichern**; **Zurücksetzen** verwirft ungespeicherte Änderungen.

Zeigt die Anmeldeseite nur die Anmeldung mit Zugangscode (*Nur Zugangscode*), wechseln Administratoren und Praxis-Logins über den Link **Mit Login anmelden** unter der Karte zur Anmeldung mit E-Mail und Passwort; direkt erreichbar ist sie auch über `/login?form=password`. Umgekehrt zeigt `/login?form=token` die Zugangscode-Anmeldung; Links und QR-Codes mit Zugangscode funktionieren unabhängig von der Einstellung.

Eine vollständige Liste aller Einstellungen mit Standardwerten enthält die Referenz „Systemeinstellungen“ in der Entwicklerdokumentation.

Customer-Bereich

Benutzer mit der Rolle `customer` sind Mitarbeiterinnen und Mitarbeiter einer Praxis oder Klinik (eines Kunden). Sie melden sich mit E-Mail und Passwort an; das Konto legt ein Administrator unter Benutzer an und verknüpft es mit dem Kunden.

Die Navigation enthält:

Menüpunkt	Funktion
Freigaben	Alle Freigaben (Zugangscodes) des eigenen Kunden mit Status, Suche und der Möglichkeit, Freigaben erneut zu drucken oder zu widerrufen.
Upload	Voraufnahmen per DLX-Import oder ZIP-Upload übermitteln (sofern für Customer freigeschaltet), siehe Voraufnahmen hochladen.
Download	Desktop- und Integrations-Apps (RadioWeb Bridge, gdt-hl7-bridge, Portal-Launch) und das Administrationshandbuch als PDF.

Freigaben

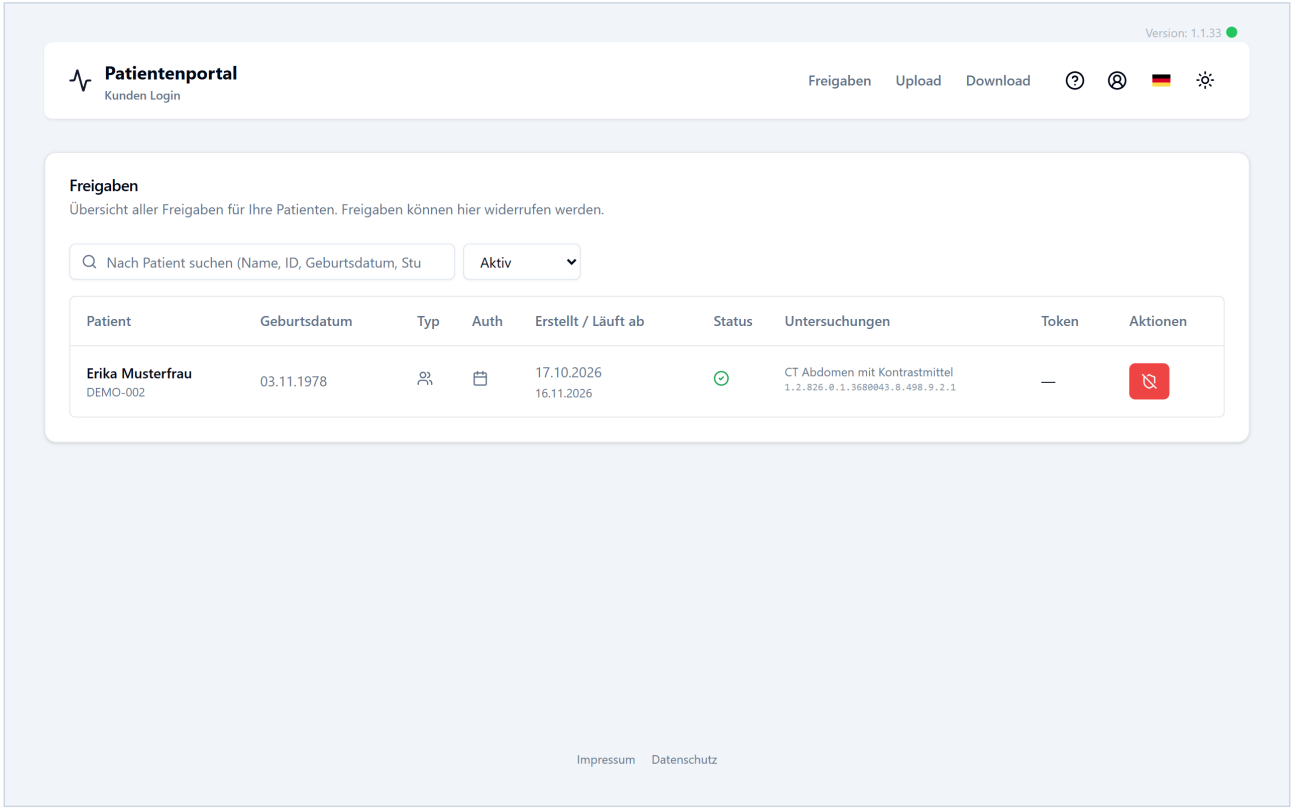


Abbildung 20. Freigaben im Customer-Bereich

Die Ansicht entspricht der Freigaben-Verwaltung der Administratoren, zeigt aber nur Freigaben des eigenen Kunden. Über das rote Symbol widerrufen Sie eine Freigabe sofort, über das Drucker-Symbol drucken Sie eine aktive Freigabe erneut (siehe Freigabe erneut drucken).

Zugangscodes erstellen

Customer dürfen – je nach Einstellung **Sicherheit** – Zugangscodes für Überweiser, Patienten und Studien erstellen. In der Praxis geschieht das meist direkt aus dem PACS bzw. PVS über die Integrationen (QR-Code beim Befunddruck, Portal-Launch).

Voraufnahmen hochladen (Upload)

Über **Upload** (`/import/upload`) übermitteln Benutzer Aufnahmen aus anderen Einrichtungen an das Portal: per **Portal Import** (DLX) direkt aus einem anderen Portal oder als **ZIP-Upload** von CD bzw. aus einem Download. Die Studien werden im Portal gespeichert, als Fremdaufnahme gekennzeichnet und – sofern eingerichtet – automatisch an ein Fremdbild-Archiv weitergeleitet (siehe Import Status).

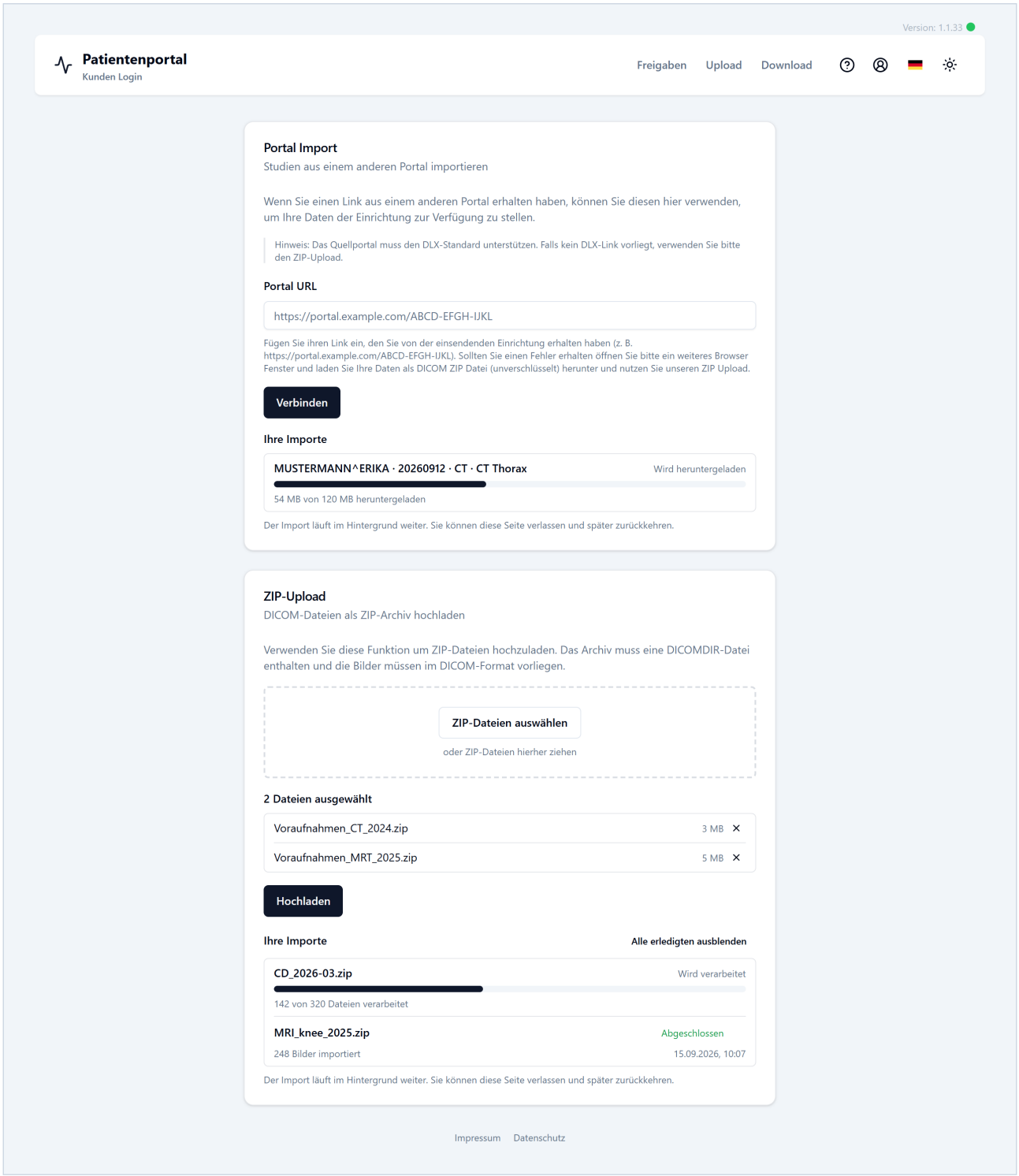


Abbildung 21. Die Upload-Seite mit laufenden und abgeschlossenen Importen

Portal Import (DLX)

Wenn Sie aus einem anderen Portal einen Freigabelink erhalten haben, kann das Patientenportal die Studien direkt von dort abholen. Voraussetzung ist, dass das andere Portal den Standard **DLX** (DICOM Link Exchange) unterstützt.

1. Fügen Sie den Link in das Feld **Portal URL** ein und klicken Sie auf **Verbinden**.
2. Beantworten Sie gegebenenfalls die Sicherheitsfragen des anderen Portals (zum Beispiel das Geburtsdatum) und klicken Sie auf **Verifizieren**.
3. Wählen Sie die Studien aus und klicken Sie auf **Studien importieren**.

Das Portal lädt die ausgewählten Studien anschließend selbst vom anderen Portal herunter; Sie sehen den Fortschritt unter **Ihre Importe** (siehe Fortschritt verfolgen).

Erkennt das Portal unter der Adresse kein DLX-Portal, erscheint ein Hinweis: Öffnen Sie den Link dann selbst, laden Sie die Daten dort als (unverschlüsseltes) DICOM-ZIP herunter und nutzen Sie den ZIP-Upload.

ZIP-Upload

1. Klicken Sie auf **ZIP-Dateien auswählen** und wählen Sie ein oder mehrere Archive aus – oder ziehen Sie die ZIP-Dateien mit der Maus in das gestrichelte Feld.
2. Prüfen Sie die Liste der ausgewählten Dateien; mit **×** entfernen Sie eine Datei wieder.
3. Klicken Sie auf **Hochladen**.

Mehrere Dateien werden nacheinander hochgeladen; jede Datei erscheint danach als eigener Eintrag unter **Ihre Importe**. Dateien, die keine ZIP-Dateien sind, werden ignoriert. Schlägt das Hochladen einer Datei fehl, werden die übrigen trotzdem hochgeladen; die fehlgeschlagene Datei bleibt ausgewählt, sodass Sie es erneut versuchen können.

Das ZIP-Archiv muss Bilder im DICOM-Format enthalten – so, wie es die meisten Patienten-CDs und Portale beim Download liefern. Die Bilder dürfen auch in Unterordnern oder in weiteren ZIP-Dateien innerhalb des Archivs liegen. Eine einzelne Datei darf höchstens 512 MB groß sein, sofern Ihre Praxis keine andere Grenze eingestellt hat. Größere Datenmengen teilen Sie auf mehrere ZIP-Dateien auf.

Fortschritt verfolgen

Während des Hochladens zeigt ein Balken an, wie viel bereits übertragen ist (bei mehreren Dateien: „Datei 2 von 5 …“). Danach verarbeitet das Portal die Daten im Hintergrund. Unter **Ihre Importe** sehen Sie für jeden Import den aktuellen Stand:

- **Wartet** – der Import beginnt in Kürze.
- **Wird heruntergeladen** – nur beim Portal Import: Die Studie wird vom anderen Portal abgeholt.
- **Wird verarbeitet** – die Bilder werden gespeichert, der Balken zeigt, wie viele Dateien bereits verarbeitet sind.
- **Abgeschlossen** bzw. **Fehlgeschlagen** – mit der Anzahl importierter Bilder oder dem Grund des

Fehlers.

Sie müssen nicht warten, bis ein Import abgeschlossen ist: Sie können die Seite verlassen und später zurückkehren. Die Importe der letzten 24 Stunden bleiben sichtbar (Zeitraum und Anzahl sind einstellbar).

Erledigte Einträge können Sie selbst ausblenden: Fahren Sie mit der Maus über einen Eintrag und klicken Sie auf das × (auf Tablets und Smartphones ist es immer sichtbar), oder klicken Sie auf **Alle erledigten ausblenden**. Laufende Importe bleiben dabei immer sichtbar.

Einrichtung

Alle Einstellungen finden Sie unter Einstellungen in der Kategorie **Import**.

Einstellung	Standard	Bedeutung
Nutzergruppen mit DLX-Import (`dlximport.enabled_groups`)	Admin, Customer, Überweiser	Für welche Rollen die Karte **Portal Import** angezeigt wird.
Nutzergruppen mit ZIP-Import (`zipimport.enabled_groups`)	Admin, Customer, Überweiser	Für welche Rollen die Karte **ZIP-Upload** angezeigt wird. Ist für eine Rolle keiner der beiden Wege aktiv, fehlt der Menüpunkt **Upload**.
Auto-Routing (`dlximport.autorouting_groups`, `zipimport.autorouting_groups`)	–	Rollen, deren Uploads automatisch an das Fremdbild-Archiv weitergeleitet werden (Ziel: `import.foreign_studies.*`).
Upload-Seite: maximale Anzahl Importe (`import.foreign_studies.upload_history.max_entries`)	20	Wie viele Importe die Liste **Ihre Importe** je Karte höchstens zeigt (1–200).
Upload-Seite: Zeitraum in Stunden (`import.foreign_studies.upload_history.window_hours`)	24	Importe der letzten X Stunden werden angezeigt (1–720).

Betrieb

- Jeder Import läuft als Hintergrund-Job. Bis zu zwei Imports werden gleichzeitig verarbeitet, weitere warten mit dem Status **Wartet**.
- Erledigte Imports werden nachts nach 7 Tagen gelöscht – bzw. nach dem eingestellten Zeitraum, falls dieser länger ist. Benutzer können sie vorher selbst ausblenden.
- Wird der Server während eines Imports neu gestartet, setzt das Portal den Import nach dem Start fort. Ist die hochgeladene Datei nicht mehr vorhanden (z. B. weil der Container neu erstellt wurde), endet der Import mit einem Hinweis auf den Neustart; der Benutzer muss ihn dann erneut starten.
- Eine einzelne Upload-Datei darf standardmäßig höchstens 512 MB groß sein. Die Grenze legt der Betreiber der Installation mit `UPLOAD_MAX_SIZE_MB` fest. Ist sie überschritten, meldet das Portal das

beim Hochladen.

- Die Weiterleitung an das Fremdbild-Archiv verfolgen Sie unter Import Status.

Integration

Overview

Dieses Dokument beschreibt die Integration externer Systeme in das Patientenportal.

Das Patientenportal kann mit bestehenden Systemen einer radiologischen Praxis verbunden werden. Die Integrationsskripte und -anwendungen befinden sich im Workspace `integration/` des Monorepos und sind nach System und Hersteller gegliedert.

```
integration/
├──── apps/
│    └──── gdt-hl7-bridge/   # GDT- und HL7-Integration (Windows-Anwendung)
├──── pacs/
│    └──── vepro/            # VEPRO PACS
└──── ris/
     └──── mesalvo/          # Mesalvo RIS
```

PACS

VEPRO

Schaltflächen zur Studienweitergabe und QR-Code-Erstellung direkt aus dem VEPRO Archive Manager.

RIS

Mesalvo RadCentre

Linkaufruf aus dem RIS RadCentre zum Patientenportal, z. B. um einen QR-Code für den Patienten zu erzeugen.

GDT / HL7

gdt-hl7-bridge

Windows-Anwendung, die ein GDT-Eingangsverzeichnis überwacht, PDF-Befunde aus dem Portal abruft, GDT-Antwortdateien erzeugt und HL7-MDM^T02-Nachrichten per MLLP/TCP sendet. Ermöglicht die Einbindung des Patientenportals in beliebige GDT-2.1-fähige Praxissoftware.

portal-launch

Windows-Programm, das das Patientenportal direkt aus PVS oder RIS heraus öffnet – ohne separate Anmeldung.

REST-API

Freigabe-API (generate-share)

Für eigene Integrationen: REST-Endpunkt zum serverseitigen Erzeugen einer Patienten- oder Studienfreigabe inklusive QR-Code, authentifiziert über ein Integrations-Token. Für Fälle, die nicht

durch VEPRO, `gdt-hl7-bridge` oder `portal-launch` abgedeckt sind. Die Schnittstelle ist in der Entwicklerdokumentation (Abschnitt „Schnittstellen“) beschrieben.

PACS: VEPRO

Overview

Die VEPRO-Integration ermöglicht es, direkt aus dem VEPRO Archive Manager heraus Studien oder Patienten im Patientenportal freizugeben und einen QR-Code für den Patienten zu erzeugen.

Enthaltene Komponenten

Datei	Beschreibung
`VIM/VIM.INI`	Konfiguration der zusätzlichen Schaltflächen im VEPRO Archive Manager
`VIM/Scripts/VMedView.vbs`	VBScript, das beim Klick auf die Schaltflächen ausgeführt wird und den Browser mit dem Patientenportal öffnet

Weiterführende Seiten

- Installation – Einrichtung der Schaltflächen in VEPRO
- QR-Code erstellen – Schritt-für-Schritt-Anleitung für Anwender

Installation

Voraussetzungen

- VEPRO ist installiert und läuft
- Das Patientenportal ist erreichbar (URL bekannt)
- Ein Integrations-Token wurde im Admin-Bereich des Patientenportals unter **Integrations-Tokens** erstellt

Schritt 1 – Skript ablegen

Kopieren Sie die Datei `VMedView.vbs` aus dem Workspace `integration/pacs/vepro/VIM/Scripts/` in das VIM-Skriptverzeichnis von VEPRO, typischerweise:

```
C:\VIM\Scripts\VMedView.vbs
```

Schritt 2 – Skript konfigurieren

Öffnen Sie `VMedView.vbs` in einem Texteditor und passen Sie die drei Konstanten am Anfang der Datei an:

```
Const PORTAL_BASE_URL   = "https://ihr-portal.beispiel.de/generate-token"
```

```
Const BROWSER_PATH      = """C:\Program Files
(x86)\Google\Chrome\Application\chrome.exe"""
Const INTEGRATION_TOKEN = "XXXX-XXXX-XXXX"  '①
```

① Den Integrations-Token aus dem Admin-Bereich des Patientenportals eintragen.

Schritt 3 – Schaltflächen in VIM.INI eintragen

Öffnen Sie die Datei `VIM.INI` (im VEPRO-Konfigurationsverzeichnis) und fügen Sie folgende Zeilen im Abschnitt `[VIMConfig]` ein:

```
ArchiveManagerButtonCustom1 = Studie freigeben,
CALL_SCRIPT_METHOD(SendStudyToPatientPortal), Studie ins Patientenportal senden
ArchiveManagerButtonCustom2 = Patient freigeben,
CALL_SCRIPT_METHOD(SendPatientToPatientPortal), Patient ins Patientenportal senden
```

Die fertige `VIM.INI` aus dem Workspace `integration/pacs/vepro/VIM/` kann als Vorlage verwendet werden.

Schritt 4 – VEPRO neu starten

Starten Sie VEPRO neu. Im Archive Manager erscheinen anschließend die beiden neuen Schaltflächen **Studie freigeben** und **Patient freigeben**.

Ergebnis

Nach erfolgreicher Installation können Anwender direkt aus VEPRO heraus QR-Codes für Patienten oder einzelne Studien erzeugen.

Weiter: QR-Code erstellen

QR-Code erstellen

Diese Anleitung beschreibt, wie ein Anwender in VEPRO einen QR-Code für einen Patienten oder eine einzelne Studie erzeugt und ausdruckt.

Voraussetzungen

- VEPRO ist geöffnet und der Anwender ist angemeldet
- Die Integration wurde eingerichtet (Installation)

Ablauf

Schritt 1 – Datensatz auswählen

Wählen Sie im **Archive Manager** den gewünschten Datensatz aus:

- **Studie freigeben** – klicken Sie zuerst auf eine Studie in der Liste

- **Patient freigeben** – es genügt, eine beliebige Studie des Patienten auszuwählen

Schritt 2 – Schaltfläche klicken

Klicken Sie auf eine der beiden Schaltflächen in der Werkzeugleiste:

Schaltfläche	Wirkung
Studie freigeben	Gibt genau die ausgewählte Studie frei. Der Patient erhält Zugriff nur auf diese eine Untersuchung.
Patient freigeben	Gibt alle Studien des Patienten frei. Der Patient erhält Zugriff auf alle seine Untersuchungen im Portal.

Ein Browserfenster öffnet sich automatisch mit dem Token-Generator des Patientenportals.

Schritt 3 – Zugriffsparameter festlegen (je nach Konfiguration)

Je nach Portaleinstellungen werden eine oder mehrere der folgenden Optionen angeboten:

Option	Bedeutung
Typ	Art der Freigabe, z. B. Studie oder Patient
Authentifizierung	Legt fest, ob der Patient beim Öffnen des QR-Codes zusätzlich sein Geburtsdatum eingeben muss
Gültigkeitsdauer	Zeitraum, für den der QR-Code gültig ist (z. B. 7 Tage, 30 Tage)



Wenn das Portal so konfiguriert ist, dass Standardwerte verwendet werden, entfällt dieser Schritt und der QR-Code wird direkt angezeigt.

Schritt 4 – QR-Code anzeigen und drucken

Nach dem Bestätigen der Parameter erscheint der QR-Code im Browserfenster.

1. Wählen Sie die gewünschte **Drucksprache** (Deutsch / Englisch)
2. Klicken Sie auf **Drucken**
3. Das Druckdialogfenster des Browsers öffnet sich – wählen Sie den gewünschten Drucker und bestätigen Sie

Der ausgedruckte Beleg enthält den QR-Code sowie einen kurzen Erklärungstext für den Patienten.

Ergebnis

Der Patient kann den QR-Code mit seinem Smartphone scannen und gelangt direkt zu seinen Bildern im Patientenportal – ohne Benutzername oder Passwort.

RIS: Mesalvo

Overview

Die Mesalvo-Integration ermöglicht es, direkt aus dem RIS RadCentre heraus einen Linkaufruf zum Patientenportal zu hinterlegen und so z. B. einen QR-Code für den Patienten zu erzeugen.

Weiterführende Seiten

- Linkaufruf im RadCentre anlegen – Schaltfläche in MedDoku oder Befund-/Untersuchungsmodul einrichten

Linkaufruf anlegen

Einleitung

In dieser Anleitung wird beschrieben, wie ein Linkaufruf-Button im RadCentre an verschiedenen Stellen angelegt wird, um z. B. den QR-Code-Generator des Patientenportals direkt aus dem RIS heraus aufzurufen.

Anlage in der MedDoku

1. RadCentre starten und mit einem Admin-Benutzer anmelden.
2. Einen Testpatienten auswählen.
3. Doppelklick auf einen Auftrag – es öffnet sich das Auswahlfenster.
4. Im Auswahlfenster **SHIFT + F6** drücken, um das Kaskadenfenster zu öffnen. Anschließend den Button **Neuer Eintrag** betätigen.
5. Es erscheint ein neuer Eintrag (im Beispiel Zeile D, blau unterlegt). Dort den Namen des neuen Kaskadeneintrags eingeben – auf ggf. vorhandene Nummerierung achten (Bsp.: A., B., C. → dann D. „neuer Name").
   Bei **Aktion** die Befehlskette eingeben und mit **Übernehmen** bestätigen. Abschließend **Speichern** drücken.

   > Befehlskette für den QR-Code-Aufruf des Patientenportals:
   > `y_shellexec("open", "https://pp.kesrbtz.de/generate-token?patid="+alltrim(oGapPatient:Nr))`
   > Für andere Befehlsketten kann Unterstützung durch Mesalvo erforderlich sein.

6. RadCentre beenden und neu starten, damit die Änderung übernommen wird.
7. Zur Kontrolle Schritte 2 und 3 wiederholen – der neue Eintrag muss nun in der Liste erscheinen.

Anlage im Untersuchung- oder Befundmodul

1. RadCentre starten und mit einem Admin-Benutzer anmelden.
2. Das **Befund-** oder **Untersuchungsmodul** auswählen.
3. Im unteren rechten Bereich auf die **drei Punkte** klicken – es öffnet sich ein Fenster.
4. Den Button **Neu** drücken.

5. Bei **Bezeichnung** den gewünschten Linknamen eintragen. Bei **Typ** „External" oder „URL" wählen, anschließend den gewünschten Link eintragen. Falls nötig einen Platzhalter über den Button **Platzhalter** einfügen. Abschließend **Speichern** drücken.
6. RadCentre neu starten, wieder einloggen und das Untersuchungsmodul erneut aufrufen.
7. Den Button **+/-** drücken, **Hinzufügen** wählen und bei dem neu erschienenen Button den gerade erstellten Linkaufruf auswählen.

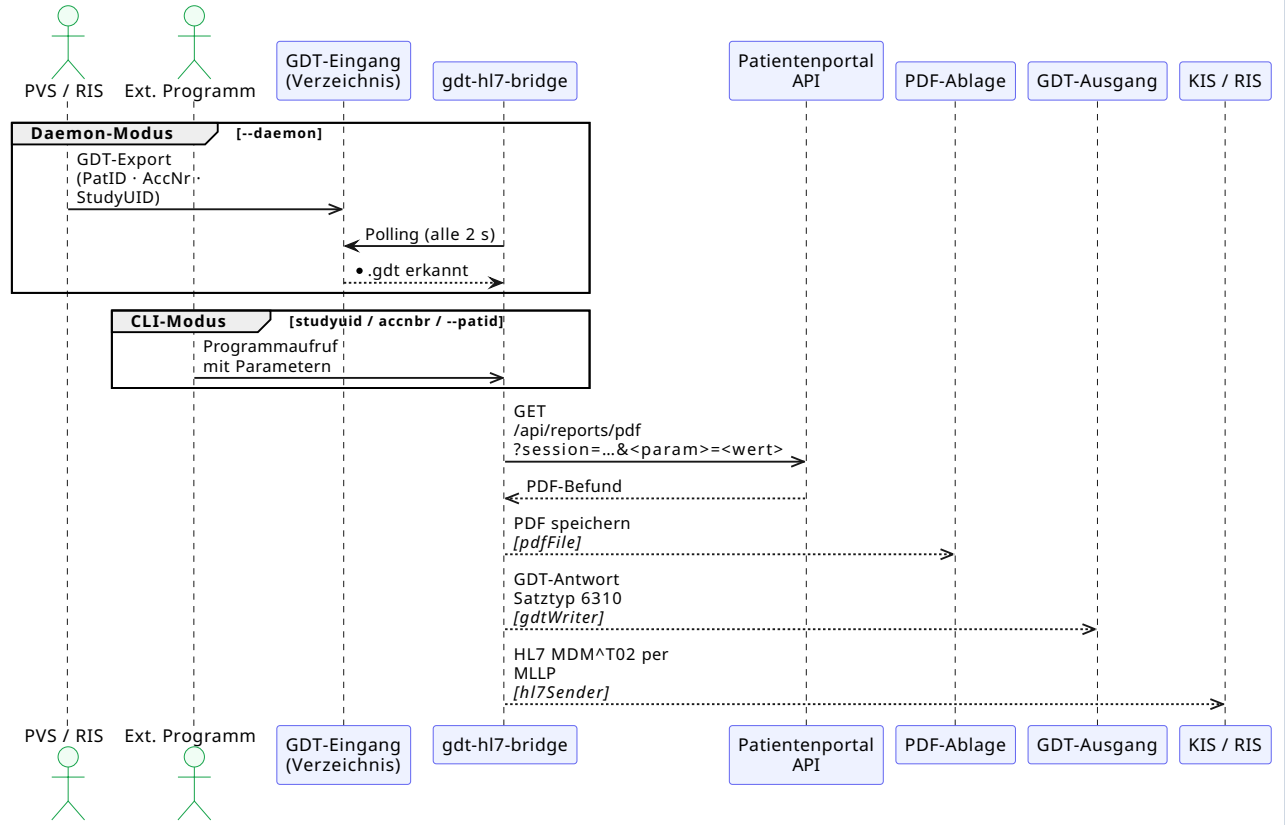
GDT/HL7: gdt-hl7-bridge

Overview

`gdt-hl7-bridge` ist eine Windows-Anwendung, die PDF-Befunde aus dem Patientenportal abruft und wahlweise eine GDT-Antwortdatei sowie eine HL7-MDM^T02-Nachricht erzeugt. Die Anwendung unterstützt zwei Aufrufmodi:

- **Daemon-Modus** (`--daemon`): Läuft im Hintergrund und überwacht ein GDT-Verzeichnis. Jede eingehende GDT-Datei der Praxissoftware löst automatisch den Abruf aus.
- **CLI-Modus** (ohne `--daemon`): Einmaliger Aufruf mit direkten Parametern (`--studyuid`, `--accnbr`, `--patid`). Ermöglicht die Integration in beliebige externe Programme ohne GDT-Schnittstelle.

Ablauf



Aufrufmodi

Daemon-Modus

```
gdt-hl7-bridge.exe --daemon
```

Startet den GDT-Polling-Dienst. Läuft dauerhaft im Hintergrund und verarbeitet alle eingehenden `*.gdt`-Dateien in `gdtImport.gdtInputDir` automatisch. Geeignet für den Betrieb als Windows-Dienst oder Autostart-Aufgabe.

CLI-Modus

```
gdt-hl7-bridge.exe --studyuid 2.25.186760260011452398476108131496539831798
gdt-hl7-bridge.exe --accnbr 186B7928
gdt-hl7-bridge.exe --patid 3209648408 --nachname Müller --vorname Max
```

Führt die Pipeline einmalig aus und beendet sich mit Exit-Code `0` (Erfolg) oder `1` (Fehler). Eignet sich für die direkte Integration aus RIS, PACS oder Worklist-Systemen heraus, ohne dass die rufende Software GDT-Dateien schreiben muss.

Hilfe

```
gdt-hl7-bridge.exe
gdt-hl7-bridge.exe --help
```

Zeigt die Hilfe an. Wird auch ohne jegliche Parameter ausgegeben.

Verzeichnisstruktur

```
gdt-hl7-bridge.exe
config/
  config.json          ①
  config.json.example  ②
templates/
  gdt-output.template  ③
  mdm-output.template  ④
nssm.exe             ⑤
install.bat
uninstall.bat
```

① Aktive Konfigurationsdatei (nicht eingecheckt, enthält API-Token)

② Vorlage mit allen verfügbaren Feldern

③ Handlebars-Template für die GDT-Antwortdatei

④ Handlebars-Template für die HL7-MDM^T02-Nachricht

⑤ Windows-Dienst-Wrapper (Non-Sucking Service Manager)

Module

Die Ausgabe-Module können in `config.json` unabhängig aktiviert werden. Beide Aufrufmodi nutzen dieselben aktivierten Module.

Modul	Funktion
`pdfFile`	PDF-Befund aus dem Portal herunterladen und lokal speichern
`gdtImport`	GDT-Eingangsverzeichnis überwachen (nur Daemon-Modus)
`gdtWriter`	GDT-Antwortdatei (Satztyp 6310) erzeugen
`hl7Sender`	HL7-MDM^T02-Nachricht per MLLP/TCP senden und/oder als Datei speichern

Weiterführende Seiten

Installation

Einrichtung unter Windows, Autostart-Konfiguration.

Konfiguration

Vollständige Referenz der `config.json` – alle Module, Feldmapping, Prioritätslogik und Dateinamen-Templates.

Betrieb

Verarbeitungsablauf, CLI-Parameter-Referenz, Fehlerbehandlung und Logging.

HL7 MDM^T02

Protokollübersicht, MLLP-Transport und Template-Referenz für die MDM^T02-Nachricht.

Installation

Lieferumfang

`gdt-hl7-bridge` wird als ZIP-Paket bereitgestellt und enthält folgende Dateien:

```
gdt-hl7-bridge.exe        ← Ausführbare Datei (standalone, kein .NET / Java
erforderlich)
config\
  config.json.example     ← Konfigurationsvorlage
templates\
  gdt-output.template     ← GDT-Antwort-Template (GDT 2.1, Satztyp 6310)
  mdm-output.template     ← HL7 MDM^T02-Template (nur bei aktiviertem hl7Sender)
nssm.exe                  ← Non-Sucking Service Manager (Windows-Dienst-Wrapper)
install.bat               ← Dienst installieren (als Administrator ausführen)
uninstall.bat             ← Dienst deinstallieren (als Administrator ausführen)
samples\
  input-patid.gdt         ← Testdatei: Suche per Patientennummer
  input-accnbr.gdt        ← Testdatei: Suche per Auftragsnummer
```

```
  input-studyuid.gdt      ← Testdatei: Suche per DICOM Study UID
```

Das Paket steht unter *Patientenportal → Download → GDT / HL7 Schnittstelle* zum Download bereit.

Voraussetzungen

- Windows 10 oder neuer (64-bit)
- Netzwerkzugang zum Patientenportal (HTTPS, Standard-Port 443)
- Wenn `hl7Sender.enabled: true`: Netzwerkzugang zum HL7-Empfänger (TCP, konfigurierter Port)
- API-Token des Kunden — wird im Portal-Admin unter *Einstellungen → Integration* erzeugt
- Schreibrechte der Praxissoftware auf `gdtImport.gdtInputDir`, Leserechte auf `gdtWriter.gdtOutputDir`



Falls eine Firewall zwischen dem Installationsrechner und dem Patientenportal bzw. dem HL7-Empfänger betrieben wird, müssen folgende ausgehenden Verbindungen freigegeben werden:

Ziel	Port / Protokoll	Zweck
Patientenportal-Host	443 / HTTPS (oder kundenspezifischer Port)	PDF-Abruf über die Portal-API
HL7-Empfänger (KIS / RIS)	konfigurierter TCP-Port (z.B. 2333)	MLLP-Nachrichtenversand (nur wenn `hl7Sender.enabled: true`)

Verzeichnisstruktur anlegen

Entpacken Sie das ZIP-Paket in ein Verzeichnis Ihrer Wahl, z.B. `C:\RadioWeb\`. Die resultierende Struktur:

```
C:\RadioWeb\
 ├──── gdt-hl7-bridge.exe
 ├──── nssm.exe
 ├──── install.bat
 ├──── uninstall.bat
 ├──── config\
 │     ├──── config.json.example
 │     └──── config.json           ①
 ├──── templates\
 │     ├──── gdt-output.template
 │     └──── mdm-output.template   ②
 └──── samples\
       ├──── input-patid.gdt
```

```
    ├──── input-accnbr.gdt
    └──── input-studyuid.gdt
```

① Muss manuell aus `config.json.example` erstellt werden (enthält API-Token, nicht im Lieferumfang)

② Nur erforderlich, wenn `hl7Sender.enabled: true` oder `hl7Writer.enabled: true`



Der genaue Installationspfad ist frei wählbar. Alle Verzeichnisse werden in `config.json` als absolute Pfade angegeben.

Konfiguration anlegen

1. Kopieren Sie `config\config.json.example` nach `config\config.json`.
2. Öffnen Sie `config\config.json` in einem Texteditor.
3. Tragen Sie mindestens die folgenden Pflichtfelder ein:

```
{
  "portalUrl": "https://portal.ihre-praxis.de",   ①
  "apiToken":  "XXXX-XXXX-XXXX",                  ②

  "gdtImport": {
    "enabled":      true,
    "gdtInputDir":  "C:\\RadioWeb\\GDT\\Input"     ③
  },

  "gdtWriter": {
    "enabled":      true,
    "gdtOutputDir": "C:\\RadioWeb\\GDT\\Output",   ④
    "senderId":     "RadioWeb"
  },

  "pdfFile": {
    "enabled": true,
    "pdfDir":  "C:\\RadioWeb\\PDFs"                ⑤
  }
}
```

① URL des Patientenportals (ohne abschließenden Schrägstrich)

② Integrations-Token — vom Portal-Administrator unter *Einstellungen → Integration* erzeugen

③ GDT-Eingangsverzeichnis: Hier legt die Praxissoftware ihre GDT-Exportdateien ab

④ GDT-Ausgangsverzeichnis: Hier liest die Praxissoftware die GDT-Antwortdateien ein

⑤ Verzeichnis für lokal gespeicherte PDF-Befunde

Alle weiteren Optionen (HL7, Logging, Feldmapping) sind in Konfiguration beschrieben. Nicht benötigte Module können mit `"enabled": false` deaktiviert bleiben.



Verzeichnisse werden beim ersten Bedarf automatisch angelegt — sie müssen nicht vorab erstellt werden.

Als Windows-Dienst einrichten (empfohlen)

Die bevorzugte Methode ist die Installation als Windows-Dienst über den mitgelieferten **NSSM** -Wrapper. Der Dienst startet automatisch beim Systemstart und wird vom Windows-Dienstmanager überwacht.

1. Öffnen Sie eine **Eingabeaufforderung als Administrator** (`cmd.exe → rechte Maustaste → Als Administrator ausführen`).
2. Wechseln Sie in das Installationsverzeichnis:

   ```
   cd C:\RadioWeb
   ```

3. Führen Sie das Installationsskript aus:

   ```
   install.bat
   ```

Das Skript installiert den Dienst `GDT-HL7-Bridge` und startet ihn sofort.

Aktion	Befehl (als Administrator)
Dienst starten	`net start GDT-HL7-Bridge`
Dienst stoppen	`net stop GDT-HL7-Bridge`
Dienststatus prüfen	`sc query GDT-HL7-Bridge`
Dienst deinstallieren	`uninstall.bat`

Alternative: Aufgabenplaner einrichten

Falls kein Administratorzugriff für die Dienst-Installation vorhanden ist, kann der Aufgabenplaner als Alternative genutzt werden.

1. Öffnen Sie den **Aufgabenplaner** (`taskschd.msc`).
2. Erstellen Sie eine neue **Aufgabe** (nicht einfache Aufgabe):
   - **Allgemein**: *Ausführen unabhängig von der Benutzeranmeldung* aktivieren
   - **Trigger**: Beim Systemstart
   - **Aktion**: Programm starten
     - Programm/Skript: `C:\RadioWeb\gdt-hl7-bridge.exe`
     - Argumente: `--daemon` ← **Pflicht — ohne diesen Parameter startet kein Daemon**
     - Starten in: `C:\RadioWeb\`

- **Einstellungen**: *Aufgabe so bald wie möglich nach einem verpassten Start ausführen* aktivieren

Erster Start / Konfiguration prüfen

Starten Sie die Anwendung zunächst manuell über die Eingabeaufforderung, um die Konfiguration zu prüfen:

```
C:\RadioWeb\gdt-hl7-bridge.exe --daemon
```

Bei erfolgreicher Konfiguration erscheint (abhängig von den aktivierten Modulen):

```
gdt-hl7-bridge gestartet [--daemon]
  Input:     C:\RadioWeb\GDT\Input
  GDT Out:   C:\RadioWeb\GDT\Output
  PDFs:      C:\RadioWeb\PDFs
  HL7 TCP:   ris-server:2333
  HL7 Queue: queue/hl7 (retry 60000ms)
  Interval:  2000 ms
```

Mit `Strg+C` beenden Sie die Anwendung wieder. Anschließend können Sie den Dienst/die Aufgabe starten.

Schlägt der Start mit einer Fehlermeldung fehl, prüfen Sie:

Fehlermeldung	Ursache / Lösung
`config/config.json not found`	Konfigurationsdatei fehlt oder liegt nicht im Unterverzeichnis `config\` neben der `.exe`
`config.json missing "portalUrl"`	Pflichtfeld `portalUrl` in der Konfiguration nicht gesetzt
`config.json "gdtImport.gdtInputDir" missing`	`gdtImport` ist aktiviert, aber `gdtInputDir` fehlt
`--daemon erfordert gdtImport.enabled: true`	`gdtImport.enabled` ist auf `false` gesetzt; im Daemon-Modus muss mindestens `gdtImport` aktiv sein
`Template not found: templates/…`	Template-Datei fehlt oder `templateFile`-Pfad in der Konfiguration zeigt auf eine nicht vorhandene Datei
`Failed to compile template`	Syntaxfehler im Handlebars-Template

Installation testen

Nach dem erfolgreichen Start kann die Installation mit einer der mitgelieferten Testdateien geprüft werden.

Voraussetzung

Die Testdateien enthalten Beispielwerte (Patienten-IDs, Auftragsnummern). Stellen Sie sicher, dass im

Portal ein passender Patient bzw. eine passende Studie für die verwendeten Werte existiert, oder passen Sie die Testdatei entsprechend an.

Ablauf

1. Öffnen Sie einen Datei-Explorer und navigieren Sie zu `C:\RadioWeb\samples\`.
2. Kopieren Sie `input-patid.gdt` in das konfigurierte `gdtImport.gdtInputDir` (z.B. `C:\RadioWeb\GDT\Input\`).
3. Warten Sie bis zu einem Polling-Zyklus (Standard: 2 Sekunden).

Erwartetes Ergebnis:

- Die Datei verschwindet aus `GDT\Input\` und erscheint in `GDT\Input\done\`
- Im konfigurierten `pdfDir` liegt eine neue PDF-Datei
- Im konfigurierten `gdtOutputDir` liegt eine neue `.gdt`-Antwortdatei

Im Fehlerfall:

- Die Datei liegt in `GDT\Input\error\` mit Timestamp-Suffix (z.B. `input-patid_20260701-143052.gdt`)
- Daneben liegt eine `.err`-Datei mit der Fehlermeldung

Typische Fehler beim ersten Test:

Fehlermeldung in .err	Ursache
`HTTP 401`	API-Token ungültig oder nicht aktiv
`HTTP 400 [TOKEN_NOT_FOUND]`	API-Token nicht im Portal hinterlegt
`HTTP 400 [TOKEN_EXPIRED]`	Gültigkeit des API-Tokens abgelaufen — unter *Einstellungen → Integration* verlängern oder neuen Token erzeugen
`HTTP 400 [TOKEN_IP_RESTRICTED]`	Der API-Token ist auf IP-Bereiche beschränkt, und die öffentliche IP des Installationsrechners liegt nicht darin
`HTTP 400 [PATIENT_ID_MISMATCH]`	Die gefundene Studie gehört zu einem anderen Patienten als dem in Feld 3000 — Patientennummer der Praxissoftware und PatientID im PACS stimmen nicht überein
`HTTP 400 [STUDY_NOT_FOUND]`	Für die Patienten-ID in der Testdatei existiert keine Studie im Portal
`HTTP 503 [ORTHANC_CONNECTION_ERROR]`	PACS ist nicht erreichbar (nur bei PACS-gebundenen Anfragen)
`ECONNREFUSED` / `ETIMEDOUT`	Portal-URL nicht erreichbar — Netzwerk oder Firewall prüfen

Konfiguration

Die gesamte Konfiguration von `gdt-hl7-bridge` erfolgt über die Datei `config\config.json`. Eine Vorlage mit allen verfügbaren Feldern liegt als `config\config.json.example` bei.

Die Konfiguration ist modular aufgebaut: Jeder Funktionsblock wird durch ein eigenes Objekt mit

einem `enabled`-Flag gesteuert. Nicht benötigte Module können deaktiviert werden, ohne die Konfiguration entfernen zu müssen.

Vollständiges Beispiel

```
{
  "portalUrl": "https://portal.ihre-praxis.de",
  "apiToken":  "Kann die Praxissoftware kein Feld für die Freigabeebene
befüllenKann die Praxissoftware kein Feld für die Freigabeebene befüllen-Kann die
Praxissoftware kein Feld für die Freigabeebene befüllenKann die Praxissoftware kein
Feld für die Freigabeebene befüllen-Kann die Praxissoftware kein Feld für die
Freigabeebene befüllenKann die Praxissoftware kein Feld für die Freigabeebene
befüllen",

  "pdfFile": {
    "enabled":     true,
    "pdfDir":      "C:\\RadioWeb\\PDFs",
    "pdfFileName":
"{{patid}}_{{nachname}}_{{vorname}}_{{accnbr}}_{{timestamp}}.pdf"
  },

  "gdtImport": {
    "enabled":       true,
    "gdtInputDir":   "C:\\RadioWeb\\GDT\\Input",
    "pollIntervalMs": 2000,
    "mapping": {
      "patid":        "3000",
      "nachname":     "3101",
      "vorname":      "3102",
      "geburtsdatum": "3103",
      "accnbr":       "8402",
      "fallnummer":   "8402",
      "studyuid":     "8410"
    },
    "required": ["patid"],
    "priority":  ["studyuid", "accnbr", "patid"]
  },

  "gdtWriter": {
    "enabled":      true,
    "templateFile": "templates/gdt-output.template",
    "gdtOutputDir": "C:\\RadioWeb\\GDT\\Output",
    "gdtFileName":  "{{patid}}_{{accnbr}}_{{timestamp}}.gdt",
    "senderId":     "RadioWeb"
  },

  "hl7Sender": {
    "enabled":      true,
```

```
    "templateFile": "templates/mdm-output.template",
    "host":         "ris-server",
    "port":         2333,
    "queue": {
      "enabled":         true,
      "dir":             "queue/hl7",
      "retryIntervalMs": 60000
    }
  },

  "hl7Writer": {
    "enabled":      false,
    "templateFile": "templates/mdm-output.template",
    "hl7OutputDir": "C:\\RadioWeb\\HL7\\Output",
    "hl7FileName":  "{{patid}}_{{accnbr}}_{{timestamp}}.hl7"
  },

  "log": {
    "enabled":  true,
    "level":    "info",
    "file":     "logs/gdt-hl7-bridge-%DATE%.log",
    "maxSize":  "10m",
    "maxFiles": "30d"
  },

  "vars": {
    "institute": "Dres. Müller Schmidt",

    "doc6302": "",
    "doc6304": "Radiologischer Befund",

    "SF2":  "Dres. Müller Schmidt",
    "SF3":  "Albrechtstraße 1",
    "SF6":  "00000 Musterstadt",
    "SF7":  "Germany",
    "SF16": "+49 0815 4711"
  }
}
```

Verbindung

Feld	Pflicht	Beschreibung
`portalUrl`	ja	Basis-URL des Patientenportals, z.B. `https://portal.ihre-praxis.de`. Ohne abschließenden Schrägstrich.
`apiToken`	ja	Integrations-Token des Kunden. Wird im Portal-Admin unter *Einstellungen → Integration* erzeugt und serverseitig validiert.

Modul: `pdfFile`

Steuert den Download und die lokale Speicherung des PDF-Befunds.

Feld	Pflicht	Standard	Beschreibung
`enabled`	nein	`false`	Modul aktivieren. Wenn `false`, wird kein PDF heruntergeladen.
`pdfDir`	ja (wenn enabled)	–	Verzeichnis, in das heruntergeladene PDF-Befunde gespeichert werden. Wird bei Bedarf automatisch angelegt.
`pdfFileName`	ja (wenn enabled)	–	Dateiname der gespeicherten PDF. Handlebars-Template, siehe Template-Variablen.

Modul: `gdtImport`

Steuert die Überwachung des GDT-Eingangsverzeichnisses und das Einlesen der GDT-Felder.

Feld	Pflicht	Standard	Beschreibung
`enabled`	nein	`false`	Modul aktivieren. Ohne dieses Modul überwacht die Anwendung kein Verzeichnis.
`gdtInputDir`	ja (wenn enabled)	–	Verzeichnis, das auf eingehende `*.gdt`-Dateien überwacht wird. Wird beim Start automatisch angelegt.
`pollIntervalMs`	nein	`2000`	Prüfintervall in Millisekunden.
`mapping`	ja (wenn enabled)	–	Objekt: Mapping-Schlüssel → GDT-Feldkennung. Beschreibung: Feldmapping (`gdtImport.mapping`).
`required`	ja (wenn enabled)	–	Array der Mapping-Schlüssel, die in der Eingangsdatei zwingend vorhanden sein müssen.
`priority`	ja (wenn enabled)	–	Array der Mapping-Schlüssel in absteigender Priorität für den Portal-API-Aufruf.
`scope`	nein	Portal-Einstellung	Freigabeebene des erzeugten Zugangscodes: `patient`, `accession`, `study` oder `auto`. Siehe Freigabeebene (`gdtImport.scope`).
`scopeValues`	nein	–	Übersetzt Werte des GDT-Felds `mapping.scope` in Freigabeebenen, z.B. `{"P": "patient", "A": "accession"}`.

Modul: `gdtWriter`

Erzeugt eine GDT-Antwortdatei (Satztyp 6310) mit dem lokalen PDF-Pfad.

Feld	Pflicht	Standard	Beschreibung
`enabled`	nein	`false`	Modul aktivieren.

Feld	Pflicht	Standard	Beschreibung
`templateFile`	nein	`templates/gdt-output.template`	Pfad zum Handlebars-Template (relativ zum Anwendungsverzeichnis oder absolut).
`gdtOutputDir`	ja (wenn enabled)	–	Verzeichnis für die GDT-Antwortdateien. Wird bei Bedarf automatisch angelegt.
`gdtFileName`	ja (wenn enabled)	–	Dateiname der GDT-Antwortdatei. Handlebars-Template, siehe Template-Variablen.
`senderId`	nein	`RadioWeb`	Kennung der sendenden Anwendung in der GDT-Antwortdatei (Feld 8316).

Modul: `hl7Sender`

Sendet eine HL7-MDM^T02-Nachricht per MLLP/TCP an einen HL7-Empfänger.

Eine vollständige Beschreibung des HL7-Nachrichtenformats finden Sie unter HL7 MDM^T02.

Feld	Pflicht	Standard	Beschreibung
`enabled`	nein	`false`	Modul aktivieren.
`templateFile`	ja (wenn enabled)	–	Pfad zum Handlebars-Template für die HL7-Nachricht.
`host`	ja (wenn enabled)	–	Hostname oder IP-Adresse des MLLP-Listeners.
`port`	ja (wenn enabled)	–	TCP-Port des MLLP-Listeners.
queue – Nachrichten-Queue bei Sendefehler			
`queue.enabled`	nein	`false`	Queue aktivieren. Bei Verbindungsfehlern wird die Nachricht in `queue.dir` gespeichert statt verloren zu gehen. Vollständige Beschreibung: HL7-Nachrichten-Queue.
`queue.dir`	ja (wenn queue.enabled)	–	Verzeichnis für zwischengespeicherte HL7-Nachrichten. Wird automatisch angelegt.
`queue.retryIntervalMs`	nein	`60000`	Intervall in Millisekunden, in dem der Daemon die Queue leert. Im CLI-Modus wird die Queue bei jedem Aufruf sofort geleert.

Modul: `hl7Writer`

Schreibt die HL7-MDM^T02-Nachricht als Textdatei in ein lokales Verzeichnis. Nützlich für Tests oder nachgelagerte dateibasierte Verarbeitung. Kann unabhängig von `hl7Sender` aktiviert werden.

Feld	Pflicht	Standard	Beschreibung
`enabled`	nein	`false`	Modul aktivieren.

Feld	Pflicht	Standard	Beschreibung
`templateFile`	ja (wenn enabled)	–	Pfad zum Handlebars-Template für die HL7-Nachricht.
`hl7OutputDir`	ja (wenn enabled)	–	Ausgabeverzeichnis für HL7-Dateien. Wird bei Bedarf automatisch angelegt.
`hl7FileName`	ja (wenn enabled)	–	Dateiname der HL7-Ausgabedatei. Handlebars-Template, siehe Template-Variablen.

Modul: `log`

Schreibt alle Laufzeitausgaben in eine täglich rotierende Logdatei. Die Konsolenausgabe bleibt unverändert aktiv — das Modul ergänzt sie durch eine persistente Protokolldatei.

Feld	Pflicht	Standard	Beschreibung
`enabled`	nein	`false`	Dateiprotokollierung aktivieren.
`level`	nein	`info`	Minimaler Log-Level: `error`, `warn`, `info`, `verbose`, `debug`.
`file`	nein	`logs/gdt-hl7-bridge-%DATE%.log`	Pfad zur Logdatei (relativ zum Anwendungsverzeichnis oder absolut). `%DATE%` wird durch das aktuelle Datum (`YYYY-MM-DD`) ersetzt. Das Verzeichnis wird automatisch angelegt.
`maxSize`	nein	`10m`	Maximale Dateigröße pro Logdatei. Einheiten: `k` (KB), `m` (MB), `g` (GB).
`maxFiles`	nein	`30d`	Aufbewahrungsdauer. Suffix `d` = Tage (z.B. `30d`), ohne Suffix = maximale Dateianzahl (z.B. `14`).

`vars` – Globale Template-Variablen

Das `vars`-Objekt definiert frei belegbare Variablen, die in *allen* Templates (GDT und HL7) verfügbar sind. Typisch sind Praxis- oder Institutionsdaten, die sich selten ändern.

```
"vars": {
  "institute": "Dres. Müller Schmidt",
  "SF2":  "Dres. Müller Schmidt",
  "SF3":  "Albrechtstraße 1",
  "SF6":  "00000 Musterstadt",
  "SF7":  "Germany",
  "SF16": "+49 0815 4711"
}
```

Die Schlüssel können frei gewählt werden und sind im Template direkt als `{{institute}}`, `{{SF2}}` usw. zugreifbar.

Zwei Schlüssel haben im Standard-GDT-Antwort-Template eine besondere Bedeutung:

Schlüssel	Bedeutung
`doc6302`	GDT-Feld 6302 (Befundanforderungskennung / Marker). Wenn leer oder nicht gesetzt, wird das Feld weggelassen.
`doc6304`	GDT-Feld 6304 (Dokumentenname / Titel des Befunds). Wenn leer oder nicht gesetzt, wird das Feld weggelassen.

Feldmapping (`gdtImport.mapping`)

Das `mapping`-Objekt ordnet logischen Bezeichnern (Mapping-Schlüssel) die entsprechenden GDT-Feldkennungen zu. Alle gemappten Felder werden aus der Eingangsdatei ausgelesen und stehen als Template-Variablen zur Verfügung.

Schlüssel	GDT-Feldkennung	Bedeutung
`patid`	`3000`	Patientennummer
`nachname`	`3101`	Nachname des Patienten
`vorname`	`3102`	Vorname des Patienten
`geburtsdatum`	`3103`	Geburtsdatum (GDT-Format TTMMJJJJ)
`accnbr`	`8402`	Auftragsnummer / Accession Number
`fallnummer`	`8402`	Fallnummer (Alias für `accnbr`, selbe Feldkennung)
`studyuid`	`8410`	DICOM Study UID (Belegung ist herstellerabhängig)
`scope`	frei wählbar (optional)	Freigabeebene pro Aufruf, siehe Freigabeebene (`gdtImport.scope`). Nur eintragen, wenn die Praxissoftware ein Feld frei befüllen kann.



Die GDT-Feldkennungen können angepasst werden, wenn die sendende Praxissoftware abweichende Feldkennungen verwendet.

Pflichtfelder (`gdtImport.required`)

Das `required`-Array enthält die Mapping-Schlüssel, die in der Eingangsdatei zwingend vorhanden sein müssen. Fehlt ein Pflichtfeld, wird die Datei mit einer Fehlermeldung nach `error/` verschoben.

```
"required": ["patid"]
```

Priorität (`gdtImport.priority`)

Das `priority`-Array bestimmt, welcher Wert für den API-Abruf verwendet wird, wenn mehrere gemappte Felder vorhanden sind. Es wird genau der erste Schlüssel verwendet, für den ein Wert in der Eingangsdatei gefunden wurde.

```
"priority": ["studyuid", "accnbr", "patid"]
```

Tabelle 1. Beispiele

Vorhandene Felder in der GDT	Verwendeter Parameter	Abfrage
`studyuid` + `patid`	`studyuid`	`?studyuid=2.25.186…`
`accnbr` + `patid`	`accnbr`	`?accnbr=186B7928`
nur `patid`	`patid`	`?patid=3209648408`

Freigabeebene (`gdtImport.scope`)

Beim PDF-Abruf erzeugt das Portal einen Zugangscode. Die Freigabeebene legt fest, welche Studien dieser Zugangscode freigibt.

Wert	Freigabe
`patient`	Alle Studien des Patienten (Patientenfreigabe).
`accession`	Alle Studien der Auftragsnummer. Beim Abruf per `studyuid` sind das alle Studien mit derselben Auftragsnummer wie diese Studie.
`study`	Nur die angefragten Studien (Studienfreigabe): beim Abruf per `studyuid` genau diese Studie, beim Abruf per `accnbr` alle Studien der Auftragsnummer.
`auto`	`accession`, wenn die GDT-Datei eine Auftragsnummer oder Study UID enthält, sonst `patient`.

Die Ebene wird in dieser Reihenfolge ermittelt:

1. GDT-Feld `mapping.scope`, falls es in der Eingangsdatei befüllt ist. Werte werden über `scopeValues` übersetzt, sonst direkt verwendet.
2. `gdtImport.scope` (im Profil oder in der Vorlage, siehe Profile (`profiles`)).
3. Ohne Angabe gilt die Portal-Einstellung **Freigabeebene PDF-Zugangscode** (`token.pdf.max_scope`, Standard `PATIENT`).

Die Portal-Einstellung ist zugleich die weiteste erlaubte Ebene: Ist dort z.B. `ACCESSION` eingestellt, lehnt das Portal Anfragen mit `patient` ab.

In folgenden Fällen wird die Eingangsdatei mit einer `.err`-Datei nach `error/` verschoben, und es wird kein Zugangscode erzeugt:

- ungültiger Wert im GDT-Feld,
- `accession` oder `study` ohne Auftragsnummer und Study UID in der Datei (`SHARE_SCOPE_REQUIRES_STUDY`),
- Ebene weiter als im Portal erlaubt (`SHARE_SCOPE_NOT_ALLOWED`).

Im CLI-Modus wird die Ebene mit `--scope patient|accession|study|auto` angegeben.

Freigabeebene über ein GDT-Feld (z.B. 6200)

```
"mapping": {
  "patid":  "3000",
  "accnbr": "8402",
  "scope":  "6200"
},
"scopeValues": { "P": "patient", "A": "accession", "S": "study" },
"scope": "auto"
```

Profile (`profiles`)

Mit Profilen betreibt eine Bridge-Installation mehrere unabhängige Abläufe, z.B. einen pro Button in der Praxissoftware. Jedes Profil hat ein eigenes Eingangsverzeichnis und kann alle Module abweichend konfigurieren, etwa die Freigabeebene, einen anderen HL7-Port oder einen zusätzlichen `hl7Writer`.

- **Ohne** `profiles` ist die gesamte Konfiguration das einzige Profil (`default`). Bestehende Konfigurationen funktionieren unverändert.
- **Mit** `profiles` ist alles außerhalb von `profiles` nur noch Vorlage und läuft selbst nicht mit. Es laufen ausschließlich die Profile.
- Ein Profil enthält nur die Abweichungen von der Vorlage:
  - Objekte werden zusammengeführt, d.h. `"hl7Sender": { "port": 2334 }` ändert nur den Port.
  - Arrays und Einzelwerte ersetzen den Vorlagenwert (z.B. `priority`).
  - `null` entfernt einen Vorlagenwert.
- `"enabled": false` direkt im Profil schaltet das ganze Profil ab.
- `log` gilt global und darf in Profilen nicht vorkommen. Logzeilen enthalten den Profilnamen, z.B. `Processing [accession]: …`.
- `portalUrl` und `apiToken` können pro Profil abweichen, z.B. für eine zweite Praxis mit eigenem Integrations-Token.
- Schlüssel, die mit `_` beginnen, gelten als Kommentar und werden ignoriert.

```
{
  "portalUrl": "https://portal.ihre-praxis.de",
  "apiToken":  "XXXX-XXXX-XXXX",
  "log":       { "enabled": true, "level": "info", "file": "logs/gdt-hl7-bridge-
%DATE%.log" },

  "pdfFile":   { "enabled": true, "pdfDir": "C:\\RadioWeb\\PDFs", "pdfFileName":
"{{patid}}_{{accnbr}}_{{timestamp}}.pdf" },
  "gdtImport": {
    "enabled":  true,
    "mapping":  { "patid": "3000", "accnbr": "8402", "studyuid": "8410" },
```

```
    "required": ["patid"],
    "priority": ["studyuid", "accnbr", "patid"]
  },
  "gdtWriter": { "enabled": true, "gdtOutputDir": "C:\\RadioWeb\\GDT\\Output",
"gdtFileName": "{{patid}}_{{timestamp}}.gdt" },
  "hl7Sender": {
    "enabled": false, "templateFile": "templates/mdm-output.template", "host":
"ris-server", "port": 2333,
    "queue": { "enabled": true, "dir": "queue/hl7" }
  },
  "hl7Writer": { "enabled": false, "templateFile": "templates/mdm-output.template",
"hl7OutputDir": "C:\\RadioWeb\\HL7\\Output", "hl7FileName":
"{{patid}}_{{timestamp}}.hl7" },

  "profiles": {
    "patient": {
      "gdtImport": { "gdtInputDir": "C:\\RadioWeb\\GDT\\Patient", "scope":
"patient" }
    },
    "accession": {
      "gdtImport": { "gdtInputDir": "C:\\RadioWeb\\GDT\\Accession", "scope":
"accession" },
      "hl7Sender": { "enabled": true, "port": 2334, "queue": { "dir": "queue/hl7-
accession" } },
      "hl7Writer": { "enabled": true }
    }
  }
}
```

Im Beispiel erzeugt `patient` eine Patientenfreigabe und eine GDT-Antwort. `accession` gibt nur die Auftragsnummer frei, sendet zusätzlich HL7 an Port 2334 und legt die HL7-Nachricht auch als Datei ab.

Regeln, die beim Start geprüft werden

- Alle Pflichtfelder werden pro Profil geprüft (nach dem Zusammenführen). Fehlermeldungen nennen das Profil, z.B. `"profiles.accession.hl7Sender.host" missing`.
- Jedes Profil braucht ein eigenes `gdtImport.gdtInputDir`.
- Profile, deren HL7-Nachrichten an verschiedene Empfänger (`host:port`) gehen, brauchen jeweils ein eigenes `hl7Sender.queue.dir`. Die Queue eines Verzeichnisses wird immer an genau einen Empfänger zugestellt.

Im CLI-Modus wählen Sie das Profil mit `--profile <name>`. Gibt es nur ein Profil, ist die Angabe nicht nötig.



Mit `gdt-hl7-bridge --print-profiles` prüfen Sie nach jeder Änderung, was jedes Profil tatsächlich tut. Die Ausgabe zeigt die zusammengeführten Werte und markiert mit `*`, was aus dem Profil stammt.

Template-Variablen

Die folgenden Variablen stehen in den Dateinamen-Templates (`pdfFileName`, `gdtFileName`, `hl7FileName`) zur Verfügung. Alle im `mapping` definierten Schlüssel stehen ebenfalls zur Verfügung, sofern das entsprechende Feld in der Eingangsdatei vorhanden ist.

Variable	Inhalt
`{{patid}}`	Patientennummer (GDT-Feld 3000)
`{{nachname}}`	Nachname (GDT-Feld 3101)
`{{vorname}}`	Vorname (GDT-Feld 3102)
`{{geburtsdatum}}`	Geburtsdatum im Format TTMMJJJJ (GDT-Feld 3103)
`{{accnbr}}`	Auftragsnummer / Accession Number (GDT-Feld 8402)
`{{fallnummer}}`	Fallnummer – identisch mit `accnbr` (GDT-Feld 8402)
`{{studyuid}}`	DICOM Study UID (GDT-Feld 8410, herstellerabhängig)
`{{scope}}`	Ermittelte Freigabeebene (`patient`, `accession`, `study`; leer, wenn die Portal-Einstellung gilt)
`{{timestamp}}`	Unix-Zeitstempel in Millisekunden
`{{date}}`	Aktuelles Datum im Format `JJJJ-MM-TT`
`{{time}}`	Aktuelle Uhrzeit im Format `HH-MM-SS`
`{{inputFile}}`	Dateiname der Eingangsdatei ohne Dateiendung
`{{<key>}}`	Jede Variable aus `vars` steht direkt unter ihrem Schlüsselnamen zur Verfügung

GDT-Antwort-Template

Das Template `templates\gdt-output.template` steuert den Aufbau der erzeugten GDT-Antwortdatei im Format GDT 2.1. Es verwendet Handlebars-Syntax.

Der Helper `{{gdtLine "FFFF" "Inhalt"}}` erzeugt eine korrekt formatierte GDT-Zeile inklusive Längenprefix und CRLF.

Standard-Template

```
{{~gdtLine "8000" "6310"~}}
{{~gdtLine "9206" "2.10"~}}
{{~gdtLine "8316" senderId~}}
{{~#if (lookup fields "8316")~}}{{gdtLine "8315" (lookup fields "8316")}}{{~/if~}}
{{~#if (lookup fields "8402")~}}{{gdtLine "8310" (lookup fields "8402")}}{{~/if~}}
{{~#if (lookup fields "3000")~}}{{gdtLine "3000" (lookup fields "3000")}}{{~/if~}}
{{~#if (lookup fields "3101")~}}{{gdtLine "3101" (lookup fields "3101")}}{{~/if~}}
{{~#if (lookup fields "3102")~}}{{gdtLine "3102" (lookup fields "3102")}}{{~/if~}}
{{~#if (lookup fields "3103")~}}{{gdtLine "3103" (lookup fields "3103")}}{{~/if~}}
{{~#if (lookup fields "3104")~}}{{gdtLine "3104" (lookup fields "3104")}}{{~/if~}}
```

```
{{~#if pdfPath~}}{{~#if doc6302~}}{{gdtLine "6302" doc6302}}{{~/if~}}{{gdtLine
"6303" "PDF"}}{{~#if doc6304~}}{{gdtLine "6304" doc6304}}{{~/if~}}{{gdtLine "6305"
pdfPath}}{{~/if~}}
```

Template-Kontext

Variable	Inhalt
`fields`	Alle GDT-Felder der Eingangsdatei, zugreifbar per Feldkennung: `(lookup fields "3000")`
`pdfPath`	Absoluter lokaler Pfad zur heruntergeladenen PDF-Datei (leer, wenn `pdfFile.enabled: false`)
`senderId`	Wert aus `gdtWriter.senderId`
`doc6302`	Wert aus `vars.doc6302` – optionaler Befundanforderungsmarker (Feld 6302)
`doc6304`	Wert aus `vars.doc6304` – optionaler Dokumentenname (Feld 6304)
`{{<key>}}`	Alle weiteren Variablen aus `vars`

Erzeugte GDT-Felder

Feldkennung	Bedeutung
`8000`	Satztyp: `6310` (Daten einer Untersuchung)
`9206`	GDT-Version: `2.10`
`8316`	ID des Senders (`senderId`)
`8315`	ID des Empfängers – aus Eingabefeld 8316 (Kennung der einsendenden Praxissoftware), nur wenn vorhanden
`8310`	Auftragsnummer des Einsenders – aus Eingabefeld 8402 (Accession Number), nur wenn vorhanden
`3000` / `3101` / `3102` / `3103` / `3104`	Patientendaten aus der Eingangsdatei (nur wenn vorhanden)
`6302`	Befundanforderungsmarker (aus `vars.doc6302`, optional)
`6303`	Dateiformat: `PDF` (immer gesetzt, wenn `pdfPath` vorhanden)
`6304`	Dokumentenname (aus `vars.doc6304`, optional)
`6305`	Verweis auf die Datei – lokaler Pfad zur PDF-Datei

HL7 MDM^T02

Das Modul `hl7Sender` sendet nach jedem verarbeiteten GDT-Auftrag eine HL7-Nachricht vom Typ **MDM^T02** (*Medical Document Management – Original Document Notification*). Die Nachricht enthält den PDF-Befund als Base64-kodierten Anhang sowie DICOM-Metadaten aus dem GDT-Eingangsauftrag.

Damit können nachgelagerte Systeme (KIS, RIS) den Befund automatisch empfangen, ohne auf das GDT-Antwortprotokoll angewiesen zu sein.



Das Portal kann MDM^T02-Nachrichten auch selbst senden (Partner und Event-Abos, persistente Warteschlange, Historie mit erneutem Senden), siehe HL7-Kommunikation. Nicht beide Wege für denselben Auftrag aktivieren (`hl7Sender` der Bridge und ein Event-Abo mit Quelle **PDF-Endpunkt** im Portal), sonst erhält das RIS jedes Dokument doppelt.

Übertragungsmodi

Beide Ausgabewege können unabhängig voneinander aktiviert werden und gleichzeitig aktiv sein.

Modus	Aktivierung	Beschreibung
MLLP/TCP	`hl7Sender.enabled: true`	Nachricht wird per MLLP-Protokoll an einen HL7-Listener gesendet. Wartet auf ACK (MSA-Segment), Timeout 10 Sekunden.
Dateiausgabe	`hl7Writer.enabled: true`	Nachricht wird als UTF-8-Textdatei in `hl7Writer.hl7OutputDir` gespeichert. Nützlich für Tests oder nachgelagerte Datei-basierte Verarbeitung.

Nachrichtenformat

Die Nachricht entspricht HL7 v2.3.1, Nachrichtentyp MDM^T02:

Segment	Inhalt
`MSH`	Message Header – Sender `RADIOWEB|PORTAL`, Timestamp, Nachrichten-ID
`EVN`	Event Timestamp
`PID`	Patientendaten (ID, Name, Geburtsdatum)
`PV1`	Visit-Informationen (Fallnummer)
`TXA`	Document Announcement (Typ `RAD`, Status `AU|AV`)
`OBX[1]`	PDF-Befund als Base64-Anhang (`ED`-Typ, MIME `AP/PDF`)
`OBX[2]`	Dokumentbeschreibung (Modalität, Studienbezeichnung aus `vars`)

MLLP-Protokoll

MLLP (*Minimum Lower Layer Protocol*) ist das Standard-Transportprotokoll für HL7-Nachrichten über TCP. `gdt-hl7-bridge` rahmt jede Nachricht wie folgt:

```
0x0B  ← Start Block (Vertical Tab)
<HL7-Nachricht als UTF-8-Text>
0x1C  ← End Data (File Separator)
0x0D  ← Carriage Return
```

Der MLLP-Listener des Empfängers muss dieses Framing verstehen (Standard bei allen gängigen HL7-Engines).

Konfiguration

Beispiel

```
"hl7Sender": {
  "enabled":      true,
  "templateFile": "templates/mdm-output.template",
  "host":         "ris-server",
  "port":         2333,
  "queue": {
    "enabled":         true,
    "dir":             "queue/hl7",
    "retryIntervalMs": 60000
  }
},

"hl7Writer": {
  "enabled":      false,
  "templateFile": "templates/mdm-output.template",
  "hl7OutputDir": "C:\\RadioWeb\\HL7\\Output",
  "hl7FileName":  "{{patid}}_{{accnbr}}_{{timestamp}}.hl7"
}
```

Felder

`hl7Sender` – MLLP/TCP-Versand

Feld	Pflicht	Standard	Beschreibung
`enabled`	nein	`false`	MLLP/TCP-Versand aktivieren.
`templateFile`	ja (wenn enabled)	–	Pfad zum Handlebars-Template für die MDM^T02-Nachricht (relativ zum Anwendungsverzeichnis oder absolut).
`host`	ja (wenn enabled)	–	Hostname oder IP-Adresse des HL7-Empfängers (MLLP-Listener).
`port`	ja (wenn enabled)	–	TCP-Port des MLLP-Listeners.
queue – Nachrichten-Queue bei Sendefehler			
`queue.enabled`	nein	`false`	Queue aktivieren. Schlägt der Versand fehl (Verbindung abgelehnt, Timeout), wird die Nachricht in `queue.dir` gespeichert statt verloren zu gehen.

Feld	Pflicht	Standard	Beschreibung
`queue.dir`	ja (wenn queue.enabled)	–	Verzeichnis für zwischengespeicherte HL7-Nachrichten. Wird automatisch angelegt. Im Daemon-Modus wird die Queue periodisch geleert, sobald der Empfänger wieder erreichbar ist.
`queue.retryIntervalMs`	nein	`60000`	Intervall in Millisekunden, in dem der Daemon versucht, die Queue zu leeren. Nur im Daemon-Modus aktiv.

`hl7Writer` – Dateiausgabe

Feld	Pflicht	Standard	Beschreibung
`enabled`	nein	`false`	Dateiausgabe aktivieren. Unabhängig von `hl7Sender`.
`templateFile`	ja (wenn enabled)	–	Pfad zum Handlebars-Template (kann identisch mit `hl7Sender.templateFile` sein).
`hl7OutputDir`	ja (wenn enabled)	–	Ausgabeverzeichnis für HL7-Dateien. Wird bei Bedarf automatisch angelegt.
`hl7FileName`	ja (wenn enabled)	–	Dateiname der HL7-Ausgabedatei. Handlebars-Template, siehe Template-Variablen.

Template (`mdm-output.template`)

Das Template steuert den exakten Aufbau der MDM^T02-Nachricht und verwendet Handlebars -Syntax.

Standard-Template

```
MSH|^~\&|RADIOWEB|PORTAL|SCN|RIS|{{now}}||MDM^T02|{{msgId}}|P|2.3.1|
EVN||{{now}}
PID|||{{patientId}}||||{{patientName}}||{{birthDate}}
PV1||O|||||||||||||||||{{fallnr}}
TXA|1|RAD||{{now}}|||||||||{{docId}}||||{{filename}}|AU||AV
OBX|1|ED|18748-4^Diagnostic Imaging
Report^LN||qr2mdm^AP^PDF^Base64^{{pdfBase64}}||||||F|||||||{{studyUid}}
OBX|2|ST|^Document Description||VEPRO QR Code {{modality}} {{studyDescription}}
```

Template-Variablen

Variable	Quelle	Inhalt
`{{now}}`	automatisch	HL7-Timestamp im Format `JJJJMMTTHHmmss` (z.B. `20260628143022`)

Variable	Quelle	Inhalt
`{{msgId}}`	automatisch	Eindeutige Nachrichten-ID (Base-36-kodierter Unix-Timestamp)
`{{patientId}}`	GDT-Feld 3000	Patientennummer
`{{patientName}}`	GDT-Felder 3101, 3102	Name im HL7-Format `Nachname^Vorname`
`{{birthDate}}`	GDT-Feld 3103	Geburtsdatum im HL7-Format `JJJJMMTT` (automatisch konvertiert aus GDT-Format TTMMJJJJ)
`{{fallnr}}`	GDT-Feld 8402	Fallnummer
`{{studyUid}}`	GDT-Feld 8410	DICOM Study UID
`{{docId}}`	GDT-Feld 8402 oder 3000	Dokument-ID (Auftragsnummer, Fallback: Patientennummer)
`{{filename}}`	automatisch	Dateiname der lokal gespeicherten PDF (ohne Pfad)
`{{pdfBase64}}`	automatisch	PDF-Datei Base64-kodiert. Das PDF wird immer heruntergeladen, wenn `hl7Sender` oder `hl7Writer` aktiv sind – unabhängig von `pdfFile.enabled`.
`{{<key>}}`	`vars`	Alle Variablen aus `config.json` → `vars`, z.B. `{{modality}}`, `{{studyDescription}}`



`{{modality}}` und `{{studyDescription}}` sind nicht aus dem GDT-Auftrag ableitbar und müssen bei Bedarf über `vars` in der Konfiguration gesetzt werden.



GDT kodiert Geburtsdaten im Format `TTMMJJJJ`; HL7 erwartet `JJJJMMTT`. Die Konvertierung für `{{birthDate}}` erfolgt automatisch.

Verbindung testen

Zum Testen des MLLP-Empfängers kann ein einfacher TCP-Listener verwendet werden:

```
# Linux/macOS
nc -l 2333

# Windows (PowerShell, benötigt ncat oder ähnliches)
ncat -l 2333
```

Nach dem Verarbeiten einer GDT-Testdatei erscheint die MLLP-gerahmte HL7-Nachricht im Terminal. Der Listener muss kein ACK senden – `gdt-hl7-bridge` schließt die Verbindung nach Erhalt von `FS CR` oder bei Verbindungsabbau.

Betrieb

CLI-Referenz

Aufruf

```
gdt-hl7-bridge.exe [--daemon] [--studyuid <uid>] [--accnbr <nr>] [--patid <id>]
                   [--nachname <name>] [--vorname <name>]
                   [--geburtsdatum <TTMMJJJJ>] [--fallnummer <nr>]
                   [--help]
```

Parameter

Parameter	Modus	Beschreibung
`--daemon`	Daemon	Startet den GDT-Polling-Dienst. Läuft dauerhaft im Hintergrund.
`--studyuid <uid>`	CLI	DICOM Study UID als Suchparameter für den PDF-Abruf.
`--accnbr <nr>`	CLI	Auftragsnummer / Accession Number als Suchparameter.
`--patid <id>`	CLI	Patientennummer als Suchparameter.
`--scope <ebene>`	CLI	Freigabeebene des Zugangscodes: `patient`, `accession`, `study` oder `auto`. Ohne Angabe gilt `gdtImport.scope`, sonst die Portal-Einstellung. Siehe Freigabeebene.
`--profile <name>`	CLI	Profil, dessen Einstellungen verwendet werden. Pflicht, wenn mehrere Profile konfiguriert sind. Siehe Profile.
`--print-profiles`	Kontrolle	Gibt alle Profile so aus, wie die Bridge sie verwendet (Vorlage und Profil zusammengeführt): Eingangsverzeichnis, GDT-Felder, Suchreihenfolge, Freigabeebene und alle Ausgaben. Im Profil gesetzte Werte sind mit * markiert, das Integrations-Token wird maskiert. Mit `--profile <name>` nur ein Profil. Ruft das Portal nicht auf und legt keine Verzeichnisse an.
`--nachname <name>`	CLI	Nachname – optional, für Dateinamen-Templates und HL7-Kontext.
`--vorname <name>`	CLI	Vorname – optional, für Dateinamen-Templates und HL7-Kontext.
`--geburtsdatum <TTMMJJJJ>`	CLI	Geburtsdatum im GDT-Format – optional, wird für HL7 automatisch nach JJJJMMTT konvertiert.
`--fallnummer <nr>`	CLI	Fallnummer – optional, für Dateinamen-Templates und HL7 (PV1-Segment).
`--help` / `-h`	beide	Hilfe anzeigen und beenden. Wird auch ohne Parameter ausgegeben.

Sind mehrere Suchparameter angegeben, bestimmt `gdtImport.priority` (Standard: `studyuid → accnbr → patid`), welcher für den API-Aufruf verwendet wird.

Exit-Codes (CLI-Modus)

Code	Bedeutung
`0`	Pipeline erfolgreich abgeschlossen
`1`	Fehler (kein Suchparameter, HTTP-Fehler, MLLP-Timeout, o.ä.)

Beispiele

```
# PDF per Study UID abrufen, HL7 MDM senden
gdt-hl7-bridge.exe --studyuid 2.25.186760260011452398476108131496539831798

# PDF per Auftragsnummer, mit Patientendaten für HL7-Kontext
gdt-hl7-bridge.exe --accnbr 186B7928 --patid 3209648408 --nachname Müller --vorname
Max

# Aufruf aus einem Batch-Skript mit Fehlerprüfung
gdt-hl7-bridge.exe --studyuid %STUDYUID%
if errorlevel 1 echo FEHLER beim PDF-Abruf
```

Verzeichnisstruktur im laufenden Betrieb

`gdt-hl7-bridge` verwaltet drei Unterverzeichnisse unterhalb von `gdtImport.gdtInputDir`:

```
gdtInputDir/
 ├──── *.gdt                    ← Neue Eingangsdateien (werden von der
Praxissoftware abgelegt)
 ├──── done/
 │     └──── *.gdt               ← Erfolgreich verarbeitete Dateien
 └──── error/
     ├──── *_YYYYMMDD-HHmmss.gdt      ← Fehlgeschlagene Dateien (mit Zeitstempel im
Namen)
     └──── *_YYYYMMDD-HHmmss.gdt.err  ← Fehlermeldung als Textdatei (gleicher Name)
```

Die Unterverzeichnisse `done/` und `error/` werden beim ersten Bedarf automatisch angelegt.

Verarbeitungsablauf

Für jede gefundene `*.gdt`-Datei läuft folgender Ablauf:

1. **Stabilitätsprüfung** – Dateien, die in den letzten 500 ms geändert wurden, werden übersprungen (Schutz vor noch laufenden Schreibvorgängen der Praxissoftware).
2. **GDT-Parsing** – Die Eingangsdatei wird im Format GDT 2.1 (ISO-8859-1) gelesen. Sowohl das kompakte Format (ohne Leerzeichen) als auch das Standard-Format werden unterstützt.
3. **Feldauflösung** – Alle im `gdtImport.mapping` definierten Felder werden aus der Datei extrahiert.
4. **Pflichtfeldprüfung** – Fehlende Pflichtfelder aus `gdtImport.required` führen zu einem Fehler.

5. **Prioritätsauswahl** – Der erste Schlüssel aus `gdtImport.priority`, für den ein Wert vorliegt, bestimmt den API-Parameter.
6. **Freigabeebene** – Aus dem GDT-Feld `mapping.scope` bzw. `scope` des Profils wird die Freigabeebene ermittelt (siehe Freigabeebene).
7. **PDF-Abruf** – Die PDF wird vom Portal unter `/api/reports/pdf?session=…&<param>=<wert>&scope=<ebene>` heruntergeladen. HTTP-Weiterleitungen (301, 302, 307) werden automatisch verfolgt. *(wenn `pdfFile.enabled`)*
8. **PDF speichern** – Die PDF wird unter `pdfFile.pdfDir/<pdfFileName>` abgelegt. *(wenn `pdfFile.enabled`)*
9. **GDT-Antwort schreiben** – Die Antwortdatei wird unter `gdtWriter.gdtOutputDir/<gdtFileName>` erzeugt. *(wenn `gdtWriter.enabled`)*
10. **HL7-MDM^T02 senden/speichern** – Die HL7-Nachricht wird per MLLP/TCP gesendet *(wenn `hl7Sender.enabled`)* und/oder als Datei abgelegt *(wenn `hl7Writer.enabled`)*. Schlägt der Versand fehl und ist `hl7Sender.queue.enabled`, wird die Nachricht in die Queue geschrieben statt die Verarbeitung abzubrechen.
11. **Aufräumen** – Die Eingangsdatei wird nach `done/` verschoben.

Gleichzeitige Verarbeitung

Mehrere GDT-Dateien im Eingangsverzeichnis werden gleichzeitig (parallel) verarbeitet. Jede Datei wird intern als separater Job geführt; eine bereits in Bearbeitung befindliche Datei wird beim nächsten Poll-Zyklus übersprungen.

Fehlerbehandlung

Tritt während der Verarbeitung ein Fehler auf (z.B. HTTP-Fehler beim PDF-Abruf, fehlendes Pflichtfeld, MLLP-Timeout, ungültige GDT-Datei), wird:

1. Die Fehlermeldung in der Konsole ausgegeben.
2. Eine Textdatei `<dateiname>.gdt.err` mit der Fehlermeldung in `error/` angelegt.
3. Die Eingangsdatei nach `error/<dateiname>.gdt` verschoben.

Beispiel nach einem HTTP-400-Fehler

```
error/
 ├──── input-accnbr_20260701-141203.gdt
 └──── input-accnbr_20260701-141203.gdt.err   ← Inhalt: "HTTP 400 von
https://portal.../api/reports/pdf?session=*** [STUDY_NOT_FOUND]: Die angeforderte
Untersuchung wurde nicht gefunden."
```

Beispiel nach MLLP-Timeout

```
error/
 ├──── eingabe_20260701-141203.gdt
 └──── eingabe_20260701-141203.gdt.err   ← Inhalt: "MLLP timeout after 10000ms
```

```
connecting to ris-server:2333"
```

HL7-Nachrichten-Queue

Wenn `hl7Sender.queue.enabled: true` konfiguriert ist, gehen HL7-Nachrichten bei einem Verbindungsfehler nicht verloren.

Situation	Verhalten
Empfänger nicht erreichbar (ECONNREFUSED, Timeout)	Nachricht wird als `.hl7`-Datei in `queue.dir` gespeichert. Verarbeitung gilt als erfolgreich — GDT-Datei wandert nach `done/`.
Daemon-Modus	Alle `queue.retryIntervalMs` Millisekunden (Standard: 60 s) wird versucht, die Queue zu leeren. Beim ersten Fehlschlag wird abgebrochen und beim nächsten Intervall erneut versucht.
CLI-Modus	Nach der Verarbeitung wird die Queue sofort einmalig geleert. Der nächste Aufruf wiederholt dies.
Empfänger wieder erreichbar	Gespeicherte Nachrichten werden in chronologischer Reihenfolge nachgesendet und nach erfolgreichem ACK aus der Queue gelöscht.

```
queue/hl7/
 ├──── 1751111295123-a4f2b.hl7   ← ausstehende Nachricht
 └──── 1751111301456-c9d1e.hl7   ← ausstehende Nachricht
```

Logging

Die Anwendung schreibt alle Meldungen auf die Standardausgabe (`stdout`). Zusätzlich kann über das `log`-Modul in `config.json` eine rotierende Logdatei aktiviert werden — siehe Modul: log.

Die Logdatei rotiert täglich und enthält Zeitstempel:

```
2026-06-28 13:48:15 [INFO] gdt-hl7-bridge gestartet [--daemon]
2026-06-28 13:48:15 [INFO]   Input:    C:\RadioWeb\GDT\Input
2026-06-28 14:12:03 [INFO] Processing: eingabe.gdt
2026-06-28 14:12:03 [INFO]   HL7:    send failed (connect ECONNREFUSED ...) —
queued as 1751111295123-a4f2b.hl7
2026-06-28 14:13:03 [INFO] Queue: 1 message(s) pending — retrying ris-server:2333
2026-06-28 14:13:03 [INFO] Queue: sent and removed 1751111295123-a4f2b.hl7
```



Das `log`-Modul übernimmt Rotation und Aufbewahrung automatisch. Eine manuelle Umleitung der Konsolenausgabe ist nicht mehr notwendig.

Typische Konsolenausgabe

Daemon-Modus – normaler Betrieb

```
gdt-hl7-bridge gestartet [--daemon]
  Input:     C:\RadioWeb\GDT\Input
  GDT Out:   C:\RadioWeb\GDT\Output
  PDFs:      C:\RadioWeb\PDFs
  HL7 TCP:   ris-server:2333
  HL7 Queue: queue/hl7 (retry 60000ms)
  HL7 Out:   C:\RadioWeb\HL7\Output
  Interval:  2000 ms
Processing: eingabe.gdt
  Lookup: patid=3209648408
  PDF:    C:\RadioWeb\PDFs\3209648408__1719475200000.pdf
  GDT:    C:\RadioWeb\GDT\Output\3209648408__1719475200000.gdt
  HL7:    sending to ris-server:2333
  HL7:    sent
  HL7:    C:\RadioWeb\HL7\Output\3209648408__1719475200000.hl7
  Done
```

Daemon-Modus – Empfänger nicht erreichbar, Queue läuft

```
Processing: eingabe.gdt
  Lookup: patid=3209648408
  HL7:    sending to ris-server:2333
  HL7:    send failed (connect ECONNREFUSED 10.0.0.1:2333) – queued as
1751111295123-a4f2b.hl7
  Done
Queue: 1 message(s) pending – retrying ris-server:2333
Queue: sent and removed 1751111295123-a4f2b.hl7
```

CLI-Modus

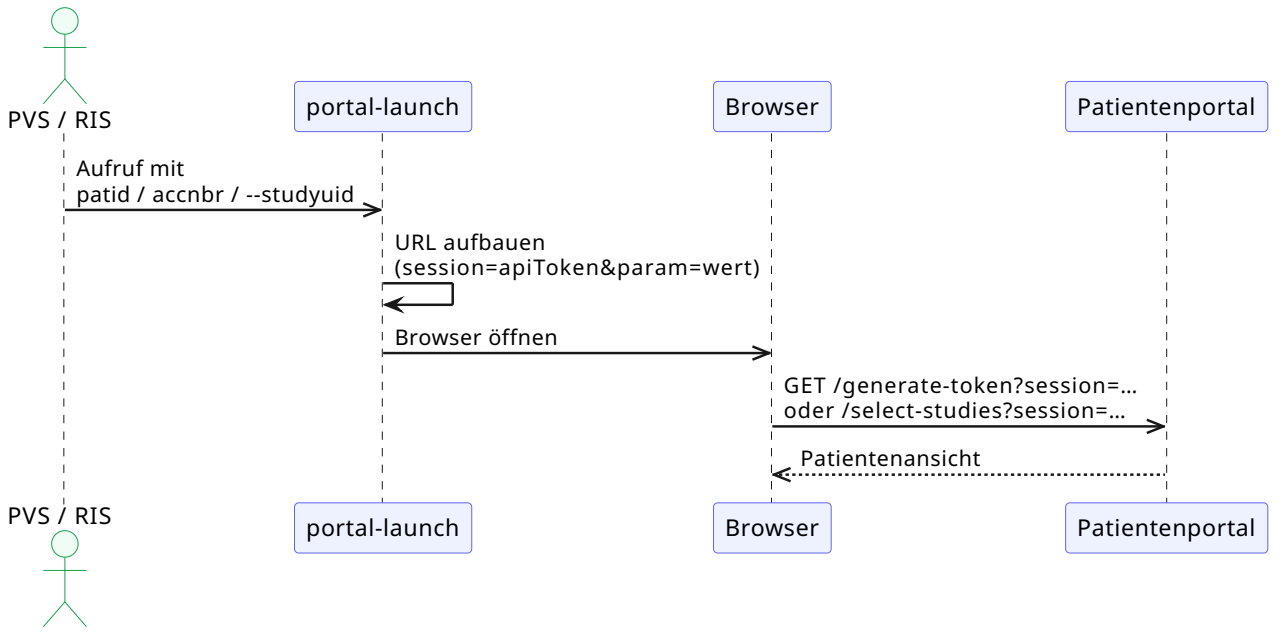
```
gdt-hl7-bridge [CLI]
  Lookup: studyuid=2.25.186760260011452398476108131496539831798
  PDF:    C:\RadioWeb\PDFs\3209648408__1719475200000.pdf
  HL7:    sending to ris-server:2333
  HL7:    sent
Fertig.
```

Portal-Launch

`portal-launch` ist ein Windows-Kommandozeilenprogramm, das das Patientenportal direkt aus der Praxisverwaltungssoftware (PVS), dem RIS oder einem anderen Arbeitsprogramm heraus im Standard-Browser (oder einem konfigurierten Browser) öffnet.

Die Anwendung erzeugt die korrekte Portal-URL mit Session-Token und übergibt sie an den Browser — der Benutzer ist ohne separate Anmeldung direkt auf der richtigen Seite.

Ablauf



Aufruf

```
portal-launch.exe --patid 3209648408
portal-launch.exe --accnbr 186B7928
portal-launch.exe --studyuid 2.25.186760260011452398476108131496539831798
```

Je nach übergebenem Parameter öffnet das Portal:

Parameter	Portal-Route	Verhalten
`--patid`	`/select-studies`	Zeigt alle Studien des Patienten zur Auswahl
`--accnbr`	`/generate-token`	Öffnet direkt die Studie zur übergebenen Auftragsnummer
`--studyuid`	`/generate-token`	Öffnet direkt die Studie zur übergebenen Study UID

Alle Parameter

Parameter	Alias	Beschreibung
`--patid <id>`	`-p`	Patientennummer (externe ID)
`--accnbr <nr>`	`-a`	Auftragsnummer (DICOM AccessionNumber)
`--studyuid <uid>`	`-s`	DICOM Study UID
`--config <pfad>`	`-c`	Pfad zur `config.json` (Standard: `config\config.json` neben der `.exe`)

Parameter	Alias	Beschreibung
`--help`	`-h`	Hilfetext anzeigen und beenden

Mindestens einer der Parameter `--patid`, `--accnbr` oder `--studyuid` muss angegeben werden. Die Anwendung beendet sich mit Exit-Code `0` bei Erfolg und `1` bei einem Fehler.

Voraussetzungen

- Windows 10 oder neuer
- Netzwerkzugang zum Patientenportal (HTTPS, Standard-Port 443)
- API-Token des Kunden — wird im Portal-Admin unter *Einstellungen* → *Integration* erzeugt
- Ein installierter Browser (Standard-Browser wird verwendet, wenn `browser.executable` nicht konfiguriert ist)

Installation

Entpacken Sie das ZIP-Paket in ein Verzeichnis Ihrer Wahl, z.B. `C:\RadioWeb-Launch\`. Die Verzeichnisstruktur nach dem Entpacken:

```
C:\RadioWeb-Launch\
 ├──── portal-launch.exe
 └──── config\
     └──── config.json.example
```

Konfiguration anlegen

1. Kopieren Sie `config\config.json.example` nach `config\config.json`.
2. Öffnen Sie `config\config.json` in einem Texteditor.
3. Tragen Sie mindestens die Pflichtfelder ein:

```
{
  "portalUrl": "https://portal.ihre-praxis.de",  ①
  "apiToken":  "XXXX-XXXX-XXXX"                  ②
}
```

① URL des Patientenportals (ohne abschließenden Schrägstrich)

② Integrations-Token — vom Portal-Administrator unter *Einstellungen* → *Integration* erzeugen

Browser konfigurieren (optional)

Ohne `browser`-Konfiguration wird der Standard-Browser des Betriebssystems verwendet. Soll ein bestimmter Browser in einem Fenster definierter Größe geöffnet werden:

```
{
  "portalUrl": "https://portal.ihre-praxis.de",
  "apiToken":  "XXXX-XXXX-XXXX",

  "browser": {
    "executable": "C:\\Program Files\\Google\\Chrome\\Application\\chrome.exe",  ①
    "width":       1280,
②
    "height":      900
②
  }
}
```

① Absoluter Pfad zum Browser-Executable

② Fenstergröße beim Öffnen (nur wenn `executable` angegeben)

Integration in PVS / RIS

`portal-launch.exe` kann direkt als externes Programm oder Makro in der Praxisverwaltungssoftware aufgerufen werden. Übergeben Sie die Patientennummer oder Auftragsnummer als Parameter.

Beispiel-Aufruf aus einem RIS-Makro (Windows):

```
"C:\RadioWeb-Launch\portal-launch.exe" --accnbr %ACCESSION_NUMBER%
```

Die genaue Syntax für den Aufruf externer Programme ist von der jeweiligen Software abhängig. Konsultieren Sie die Dokumentation Ihrer PVS/RIS-Software.

Konfigurationsreferenz

Feld	Pflicht	Standard	Beschreibung
`portalUrl`	ja	–	URL des Patientenportals. Kein abschließender Schrägstrich.
`apiToken`	nein	–	Integrations-Token. Wird als `session`-Parameter in der URL übergeben. Ohne Token muss sich der Benutzer manuell anmelden.
`browser.executable`	nein	–	Absoluter Pfad zu einem Browser-Executable (z.B. Chrome, Edge). Ohne dieses Feld wird `start` (Standard-Browser) verwendet.
`browser.width`	nein	–	Fensterbreite in Pixeln. Nur wirksam, wenn `browser.executable` gesetzt ist.
`browser.height`	nein	–	Fensterhöhe in Pixeln. Nur wirksam, wenn `browser.executable` gesetzt ist.

Fehlerbehandlung

Die Anwendung gibt Fehlermeldungen auf der Standardfehlerausgabe aus und beendet sich mit Exit-Code 1.

Fehlermeldung	Ursache / Lösung
`ERROR: At least one of --studyuid, --patid, or --accnbr is required.`	Kein Such-Parameter angegeben. Mindestens einen der drei Parameter übergeben.
`ERROR: Config file not found: …`	`config\config.json` fehlt. Aus `config.json.example` erstellen und Pflichtfelder eintragen.
`ERROR: config/config.json must contain "portalUrl".`	Pflichtfeld `portalUrl` fehlt in der Konfiguration.
`ERROR: Failed to parse …`	`config.json` enthält ungültiges JSON. Syntaxfehler beheben.
`ERROR: Failed to open browser: …`	Browser konnte nicht gestartet werden. Pfad zu `browser.executable` prüfen oder Feld entfernen, um den Standard-Browser zu verwenden.