FOCUS FAMILY

Schnittstellenhandbuch

REST/JSON, Webhooks, CMIS, XÖV, SCIM, Kalender und SIEM einrichten und betreiben

Version 1.3.0 · Stand November 2026 · Software Notion

Inhaltsverzeichnis

1. **Über dieses Handbuch**
    1. Grundsätze
2. **Überblick über die Schnittstellen**
    1. Adressen auf einen Blick
    2. Begriffe
3. **Rechte und Rollen**
4. **Freigabe-Workflow (Vier-Augen-Prinzip)**
    1. Status
    2. Ablauf
    3. Was eine erneute Freigabe auslöst
    4. Freigabepflicht abschalten
5. **Datenschutz-Voreinstellungen**
    1. Klarnamen und Pseudonymisierung
    2. Bereiche
    3. Offenlegungsprotokoll und Auskunft
6. **Netzwerk und Sicherheit der ausgehenden Verbindungen**
7. **REST/JSON-API**
    1. API-Client anlegen
    2. Token abrufen
    3. Scopes
    4. Ressourcen
    5. Konventionen
    6. Änderungs-Feed
8. **Webhooks**
    1. Einrichten
    2. Ereignisse
    3. Nachrichtenformat
    4. Signatur prüfen
    5. Zustellverhalten
9. **Eingehende Richtung**
    1. Dokumente einliefern
    2. Fall-Stammdaten ändern
    3. Posteingang und Prüfung
    4. Zurückziehen
10. **CMIS: Ablage im DMS oder in der E-Akte**
    1. Einrichten
    2. Ablagestruktur
    3. Eigenschaften
    4. Verbindungsprüfung
    5. Eingangsordner (Gegenrichtung)
11. **CMIS-Repository von Focus Family**
    1. Anmeldung und Rechte
    2. Aufbau
    3. Abfragen und Grenzen
    4. Dokumente ablegen
12. **XÖV und xdomea**
    1. Was übertragen wird
    2. Transporte
    3. Verzeichnis
    4. SFTP
    5. XTA 2
    6. FIT-Connect
13. **Benutzerbereitstellung mit SCIM 2.0**
    1. Einrichten
    2. Verhalten
    3. Hinweise zu den Anbietern
14. **Kalender-Abos (iCalendar)**

15. **SIEM-Weiterleitung (Syslog)**
16. **Manuelle Übergabe aus der Fallansicht**
17. **Konfiguration exportieren und importieren**
18. **Betrieb**
    1. Ablauf der Zustellung
    2. Übertragungsprotokoll und Wiederholungen
    3. Pausieren und Not-Aus
    4. Monitoring-Kennzahlen
    5. Audit-Ereignisse
    6. Konfigurationsparameter
19. **Fehlerbehebung**
    1. Fehlercodes der REST-API
20. **Glossar**
21. **Checkliste Inbetriebnahme**

Über dieses Handbuch

Dieses Handbuch richtet sich an die **technische Administration beim Träger** und an technische Dienstleister, die den Focus-Family-Server an Fachverfahren, Dokumentenmanagement, E-Akte, Jugendämter, Identitätsanbieter, Kalender und Sicherheitsmonitoring anbinden. Es beschreibt jede Schnittstelle mit Einrichtung, Referenz, Datenschutz-Voreinstellungen, Betrieb und Fehlersuche.

Installation, Absicherung und Betrieb des Servers selbst stehen im **Technischen Handbuch**, die fachliche Arbeit im Panel im **Handbuch für das Admin-Panel**. Die maschinenlesbare Beschreibung der REST-API (OpenAPI 3.1) steht im Panel unter **Schnittstellen → Dokumentation der Schnittstellen** zum Herunterladen bereit.

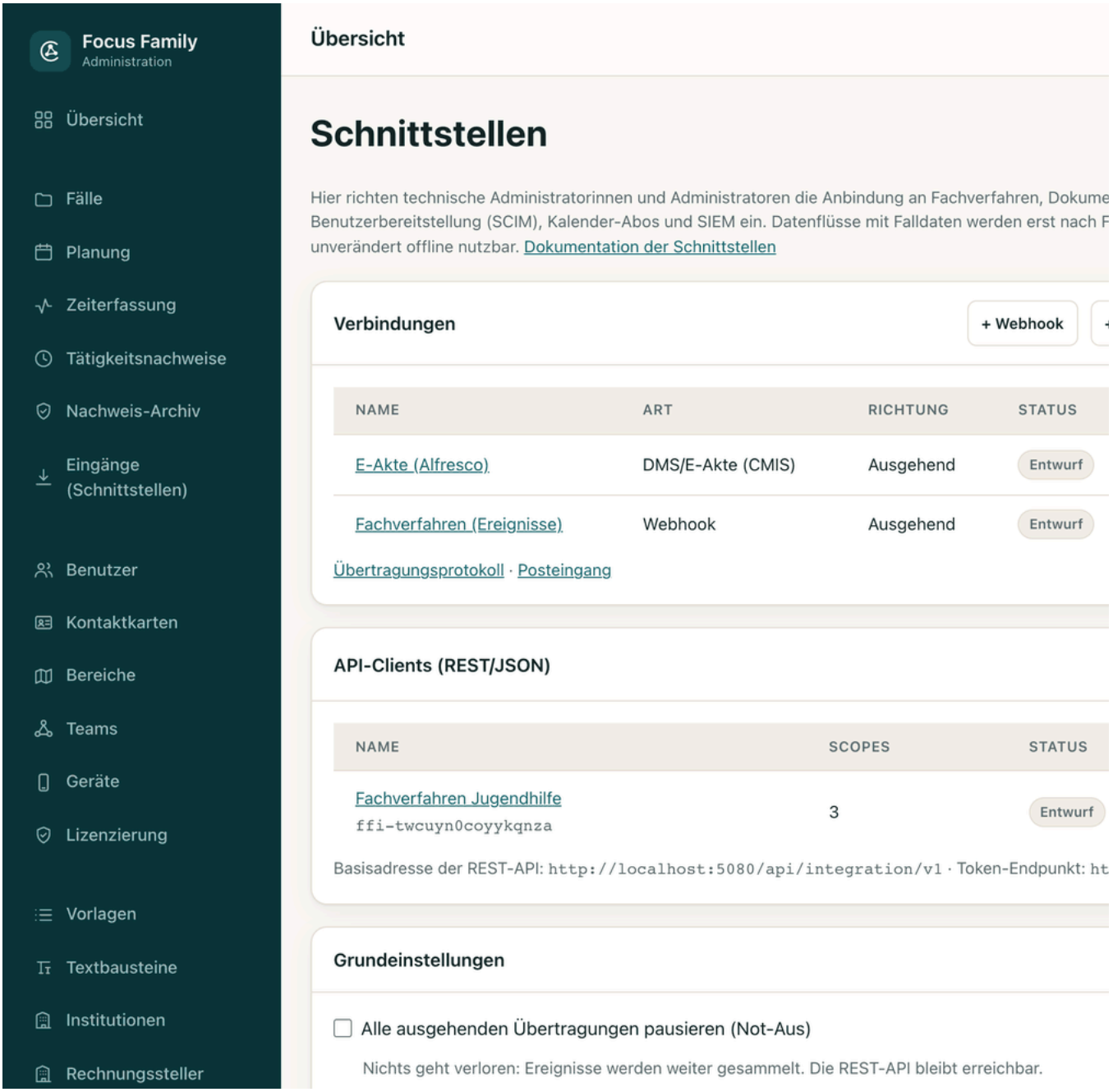
Vorausgesetzte Kenntnisse: HTTP und TLS, OAuth 2.0 (Client-Credentials-Flow), JSON und XML, Grundlagen des jeweiligen Zielsystems (DMS, Gateway, Identitätsanbieter, SIEM).

Grundsätze

- **Alles läuft im Träger-Server.** Apps und Desktop bleiben unverändert und vollständig offline nutzbar. Die Schnittstellen sehen nur Daten, die bereits zum Server synchronisiert sind.
- **Nichts ist von selbst aktiv.** Jede Verbindung und jeder API-Client entsteht als Entwurf. Datenflüsse mit Falldaten werden erst nach Freigabe durch die Datenschutzrolle aktiv (Vier-Augen-Prinzip).
- **Pseudonymisiert und minimal ist der Standard.** Klarnamen, Entwürfe, kennwortgeschützte Dokumente und vertrauliche Dokumenttypen verlassen den Server nur nach ausdrücklicher Einstellung und Freigabe.
- **Bidirektional nur per Konfiguration.** Jede eingehende Richtung ist aus, bis sie eingerichtet und freigegeben ist. Eingehende Löschungen gibt es nicht.
- **Standards statt Eigenformate:** OAuth 2.0, OpenAPI 3.1, RFC 9457, CloudEvents 1.0, Standard Webhooks, CMIS 1.1, xdomea 3.1.0 und 4.0.0, XTA 2, FIT-Connect, SCIM 2.0, iCalendar (RFC 5545), Syslog (RFC 5424/5425) und CEF.
- **Private und lokale Daten bleiben unsichtbar.** Private Fälle und Einträge, Fälle ausgeschiedener Fachkräfte mit privatem Besitzstand, gelöschte, zur Löschung vorgemerkte und in der Verarbeitung eingeschränkte Datensätze erreicht keine Schnittstelle.

Überblick über die Schnittstellen

Schnittstelle	Richtung	Zweck	Freigabe nötig
REST/JSON-API	Drittsystem ruft Focus Family auf (lesen und, wenn eingerichtet, schreiben)	Fachverfahren, Statistik, Abrechnung, eigene Werkzeuge	ja, sobald ein Scope mit Falldaten gewählt ist
Webhooks	ausgehend	Benachrichtigung bei Ereignissen, nur Kennungen	ja
CMIS (DMS/E-Akte)	ausgehend, optional eingehend	finale Dokumente, Nachweise und abgeschlossene Akten im DMS ablegen; Dokumente aus einem Eingangsordner übernehmen	ja
CMIS-Repository	Drittsystem ruft Focus Family auf	DMS oder E-Akte liest die Fallakten über CMIS 1.1 Browser Binding und legt Dokumente ab	über den API-Client
XÖV (xdomea)	ausgehend, optional eingehend	Aktenabgabe bei Fallabschluss, Import eingehender Abgaben mit Importbestätigung; Transport über Verzeichnis, SFTP, XTA 2 oder FIT-Connect	ja
SCIM 2.0	Identitätsanbieter ruft Focus Family auf	Fachkräfte-Konten anlegen, ändern, deaktivieren; Gruppen auf Teams abbilden	nein (keine Falldaten)
Kalender-Abos	Kalender-Programm ruft Focus Family auf	eigene Termine im Dienstkalender abonnieren	nein; mehr als „Belegt“ stellt nur die Datenschutzrolle ein
SIEM (Syslog)	ausgehend	Ereignisse der Audit-Kette an ein Sicherheitsmonitoring	nein (nur Kennungen)



Adressen auf einen Blick

Adresse	Inhalt
`https://<server>/api/integration/v1`	Basisadresse der REST-API
`https://<server>/connect/token`	Token-Endpunkt für API-Clients
`https://<server>/cmis/browser`	CMIS-Repository (Browser Binding), Repository-ID `focusfamily`
`https://<server>/scim/v2`	SCIM-Basisadresse für den Identitätsanbieter
`https://<server>/feeds/calendar/<token>.ics`	persönliches Kalender-Abo
`/admin/integrations`	Panel-Bereich **Schnittstellen**
`/admin/integrations/log`	**Übertragungsprotokoll**
`/admin/integrations/inbox`	**Eingänge (Schnittstellen)** für die fachliche Prüfung
`/admin/integrations/docs`	Handbuch und OpenAPI-Beschreibung zum Herunterladen
`/admin/calendar-feed`	eigenes **Kalender-Abo** erzeugen oder beenden

Die Seite **Schnittstellen** zeigt die Basisadresse der REST-API und den Token-Endpunkt der Installation zum Kopieren an.

Begriffe

- Eine **Verbindung** ist ein Zielsystem, das der Server selbst anspricht: Webhook, CMIS, XÖV oder SIEM. Sie hat eine Richtung (ausgehend, eingehend, beidseitig), Auslöser, Datenschutz-Einstellungen und einen eigenen Zustellstand.
- Ein **API-Client** ist ein Drittsystem, das sich mit eigenen Zugangsdaten an der REST-API oder am CMIS-Repository anmeldet. Was es sieht, bestimmen Scopes, Bereiche, IP-Liste und Datenschutz-Einstellungen.
- **Tokens** für SCIM und Kalender-Abos sind lange Zufallswerte, die nur einmal angezeigt und auf dem Server nur als SHA-256-Prüfsumme gespeichert werden.

Rechte und Rollen

Recht im Panel	Wirkung
Schnittstellen verwalten (REST-Clients, CMIS, XÖV, Webhooks, SCIM, SIEM) (`IntegrationManage`)	Bereich **Schnittstellen**: API-Clients und Verbindungen anlegen, prüfen, einreichen, pausieren, löschen; Secrets erneuern; SCIM-Tokens; Übertragungsprotokoll mit Wiederholen; Konfiguration exportieren und importieren. Im System-Admin enthalten.
Datenschutzbeauftragte:r (`DataProtection`)	Datenflüsse mit Falldaten freigeben oder zurückweisen, Richtlinie **Datenflüsse mit Falldaten erst nach Freigabe aktivieren** schalten, Kalender-Detailgrad über „Belegt“ hinaus erlauben, beim Import weiter geöffnete Datenschutz-Einstellungen übernehmen.
Eingänge aus Schnittstellen prüfen und übernehmen (`IntegrationInboxReview`)	Seite **Eingänge (Schnittstellen)**: Eingänge im eigenen Verwaltungsumfang prüfen und ablehnen; einem Fall zuordnen und übernehmen nur zusammen mit „Fälle bearbeiten“. Im Fach-Admin enthalten; „Fälle bearbeiten“ allein genügt nicht, weil im Posteingang auch Daten anderer Fachkräfte landen können.
Fälle bearbeiten (`CaseEdit`)	Schaltfläche **An Zielsystem übergeben** in der Fallansicht.
Sicherheits-Audit ansehen (`AuditView`)	Ereignisse `integration.*` in der Audit-Ansicht
Monitoring konfigurieren (`MonitoringConfigure`)	Zugriff auf `/metrics` mit den Kennzahlen `fokusfamilie_integration_*`

Lesend sehen die Seiten des Bereichs **Schnittstellen** alle Konten mit **Schnittstellen verwalten** oder **Datenschutz**. Konten nur mit Datenschutzrecht finden den Menüpunkt **Schnittstellen** in ihrem Bereich und können dort prüfen und freigeben, aber nichts anlegen oder ändern.

Heikle Aktionen verlangen eine **erneute Anmeldebestätigung** (Passwort und, falls eingerichtet, TOTP, oder Passkey): API-Client speichern, Client-Secret erneuern, Verbindung speichern, Signatur-Secret erneuern, SCIM-Token erzeugen, Konfiguration importieren, Freigeben oder Zurückweisen und die Freigabe-Richtlinie ändern. Freigaben sind nur mit einem **lokalen Konto** möglich, nicht mit einem SSO-Konto.

Freigabe-Workflow (Vier-Augen-Prinzip)

Status

Status im Panel	Bedeutung
Entwurf	angelegt oder zurückgewiesen; nichts wird übertragen, der API-Client erhält kein Token
Wartet auf Freigabe	eingereicht; Ereignisse werden nicht übertragen, bis die Datenschutzrolle entscheidet
Aktiv	Datenfluss läuft
Pausiert	von der technischen Administration oder nach wiederholten Fehlern automatisch angehalten; nichts geht verloren
Widerrufen	API-Client endgültig entzogen; die Zugangsdaten sind gelöscht

Ablauf

1. Die technische Administration legt den API-Client oder die Verbindung an. Zweck der Übermittlung und Rechtsgrundlage (Freitext, z. B. „§ 61 ff. SGB VIII, § 69 SGB X“) gehören dazu; beides erscheint im Freigabedialog, im Datenschutzprotokoll und im Verzeichnis der Empfänger.
2. Bei Verbindungen: **Verbindung prüfen** ausführen (siehe die Abschnitte der einzelnen Schnittstellen).
3. **Zur Freigabe einreichen.** Überträgt die Schnittstelle keine Falldaten oder ist die Freigabepflicht abgeschaltet, heißt die Schaltfläche **Aktivieren** und der Status wechselt sofort auf **Aktiv**.
4. Eine **andere** Person mit Datenschutzrecht prüft Empfänger, Zweck, Rechtsgrundlage, Datenumfang, Scopes bzw. Auslöser, Datenschutz-Einstellungen und Bereiche und wählt **Freigeben** oder **Zurückweisen** (mit Begründung). Wer die Schnittstelle angelegt oder zuletzt geändert hat (Anlegen und jedes Speichern), kann sie nicht selbst freigeben; diesen Personen zeigt die Statuskarte einen Hinweis auf das Vier-Augen-Prinzip. Beispiel: A legt an, P gibt frei, B (technische Administration und Datenschutz) ändert die Adresse; die Schnittstelle wartet wieder auf Freigabe, und weder B noch A können sie freigeben, eine andere Person mit Datenschutzrecht schon. Die Entscheidung gilt nur für den geprüften Stand: Das Formular trägt eine vom Server berechnete Revision (SHA-256 über die freigaberelevanten Einstellungen und den Zeitpunkt der letzten Änderung). Wurde die Schnittstelle nach dem Öffnen der Seite geändert, verweigert der Server die Entscheidung (`itg_err_changed`), und die Schnittstelle wartet weiter auf Freigabe. Freigeben, Bearbeiten und Einreichen sperren den Datensatz in einer Transaktion, sodass eine gleichzeitige Änderung nie einen ungeprüften Stand aktiviert.
5. Die Freigabe schreibt den Datenschutzeintrag `integration.recipient_approved` mit Name, Art, Richtung, Zweck und Rechtsgrundlage.

Ohne Falldaten und damit ohne Freigabe kommen aus: SIEM-Verbindungen, API-Clients nur mit `integration:billing.read`, `integration:catalogs.read`, `integration:catalogs.write`, `integration:directory.read` und `integration:inbox.read`, SCIM und Kalender-Abos.

Was eine erneute Freigabe auslöst

Ändert die technische Administration an einer aktiven, pausierten oder wartenden Schnittstelle mit Falldaten den Datenumfang, während die Freigabepflicht eingeschaltet ist, springt der Status zurück auf **Wartet auf Freigabe**:

- API-Client: Scopes, Bereiche, IP-Liste, Datenschutz-Einstellungen, eingehende Richtung, Zweck, Rechtsgrundlage.
- Verbindung: Richtung, Adresse, Auslöser, artspezifische Einstellungen (außer dem Abfrageintervall), Datenschutz-Einstellungen, eingehende Richtung, Bereiche, Zweck, Rechtsgrundlage.

Token-Laufzeit, Rate-Limit, Ablaufdatum und Geheimnisse von API-Clients sowie Anmeldung, Zugangsdaten, Zertifikate, Pins und der Schalter für unverschlüsselte Übertragung von Verbindungen lassen sich ohne neue Freigabe ändern.

Bis zur erneuten Freigabe wird nichts übertragen. Der Zustellstand bleibt erhalten; nach der Freigabe holt die Verbindung die Ereignisse seit dem letzten Stand nach.

Freigabepflicht abschalten

Unter **Datenschutz-Richtlinie für Schnittstellen** schaltet ein Konto mit Datenschutzrecht die Option **Datenflüsse mit Falldaten erst nach Freigabe aktivieren (Vier-Augen-Prinzip)** ab. Danach aktiviert die technische Administration Datenflüsse ohne zweite Prüfung; Datenschutz-Einstellungen weiter öffnen kann dann nur noch die Datenschutzrolle. Das ist nur für Träger ohne eigene Datenschutzrolle im Panel gedacht; die Änderung wird als `integration.settings_changed` mit `approval_off` auditiert.

Datenschutz-Voreinstellungen

Jede Verbindung und jeder API-Client hat eine Karte **Datenschutz**. Abweichungen vom Standard sind möglich, lösen aber die Freigabe aus. Weiter öffnen (Klarnamen, Entwürfe, kennwortgeschützte Dokumente, Freischalten gesperrter Bereiche oder Dokumenttypen) darf die Datenschutzrolle immer, die technische Administration nur bei eingeschalteter Freigabepflicht, weil dann die erneute Freigabe folgt. Ist die Freigabepflicht abgeschaltet, übernimmt der Server eine Ausweitung durch ein Konto ohne Datenschutzrecht nicht; die bisherigen Werte bleiben ohne Meldung stehen.

Einstellung	Standard	Wirkung
Klarnamen übertragen	aus	Ohne Haken erhält das Zielsystem Fallalias, Aktenzeichen und pseudonymisierte Titel und Dateinamen. Mit Haken liegen Sozialdaten im Zielsystem und unterliegen dort dessen Rechten und Löschfristen (§ 65 SGB VIII beachten).
Auch Entwürfe übertragen	aus	Standard: nur finale oder unterschriebene Dokumente
Auch kennwortgeschützte Dokumente übertragen	aus	Das Zielsystem kann diese Dateien ohne Kennwort weder lesen noch indizieren.
Gesperrte Bereiche der E-Akte	Notizen	Dokumente in markierten Bereichen verlassen den Server über diese Schnittstelle nie.
Gesperrte Dokumenttypen	Verlaufsdokumentation, Gesprächsnotiz, Telefonnotiz, Freier Text	Inhalte mit besonderem Vertrauensschutz bleiben im Server, solange sie nicht einzeln freigeschaltet sind.
Ordnervorlage im Zielsystem (CMIS)	`/{year}/{fileNumber}/{section}`	Platzhalter siehe *CMIS*

Klarnamen und Pseudonymisierung

Ohne Klarnamen (und ohne Scope `integration:sensitive`) gilt:

- Name und Kontakt der ASD-Fachkraft erscheinen als `[pseudonymisiert]`.
- Beteiligte Personen heißen „Kind“ oder „Person“ mit einer kurzen Kennung; Vor- und Nachname und Geburtsdatum fehlen.
- Dokumenttitel lauten `<Dokumenttyp> <Datum> v<Version>`, Dateinamen entsprechend; die Autorin bzw. der Autor ist geschwärzt.
- Tätigkeitsbeschreibungen in Zeiteinträgen fehlen.
- Unverändert bleiben Kennungen, Aktenzeichen, Fallalias, Status, Hilfeart, Zeiträume, Bewilligung und zuständiges Jugendamt.

Die Verzeichnis-Ressourcen (`integration:directory.read`) liefern Name und dienstliche E-Mail-Adresse der Mitarbeitenden immer im Klartext, aber nie Rechte oder Geräte.

Bereiche

Ist der Bereichsmodus eingeschaltet, begrenzt die Karte **Bereiche** eine Schnittstelle auf Fälle der Fachkräfte dieser Bereiche. Ohne Auswahl gilt die Schnittstelle organisationsweit.

Offenlegungsprotokoll und Auskunft

- Jede Freigabe erzeugt einen Datenschutzeintrag (`integration.recipient_approved`).
- Das Auskunftspaket nach Art. 15 DSGVO nennt je Fall die Empfänger: Verbindungen aller Arten einschließlich Webhooks, an die Daten des Falls übermittelt wurden (erstmals am, Anzahl der Übermittlungen, erneute Zustellungen gesondert gezählt), sowie freigegebene API-Clients mit Scopes für Falldaten als mögliche Empfänger.
- Grundlage für die Verbindungen ist das Offenlegungsverzeichnis: Jede erfolgreiche Zustellung zu einem Fall oder Datensatz hält Zeitpunkt, Kennungen, Ereignistyp sowie Name, Art, Zweck und Rechtsgrundlage der Verbindung zu diesem Zeitpunkt fest. Die Einträge enthalten keine Fallinhalte, bleiben beim Löschen der Verbindung und beim endgültigen Löschen eines Falls (nur Kennungen) erhalten und ändern sich nicht, wenn die Verbindung später umbenannt oder Zweck bzw. Rechtsgrundlage geändert werden.

- Löschungen in Focus Family löschen nie automatisch im Zielsystem. Mit dem Auslöser **Löschung eines Falls wird beantragt** erhält ein Webhook-Empfänger das Ereignis `de.fokusfamilie.case.erasure_requested` ohne Inhalt; die Löschung im Zielsystem verantwortet der Träger.
- Die endgültige Löschung eines Falls oder einzelner Datensätze in Focus Family löscht auch die Kopien in den Schnittstellen: Posteingangs-Einträge behalten nur technische Angaben (ID, Zustand, Quelle, Idempotenzschlüssel) und den Grund `erased`, Inhalt, Dateiname, Fallreferenz, externe ID und Dateiverweis werden entfernt; Fremdreferenzen werden gelöscht; das Zustellverzeichnis behält die Objekt-ID im Zielsystem, aber nicht den Ablagepfad, der Aktenzeichen oder Namen enthalten kann. Weil die Idempotenzangaben bleiben, legt eine wiederholte Einlieferung die gelöschten Daten nicht neu an.

Netzwerk und Sicherheit der ausgehenden Verbindungen

Webhooks, CMIS, XÖV (SFTP, XTA 2, FIT-Connect), OAuth-Token-Abrufe und SIEM laufen über einen gemeinsamen, abgesicherten Client.

- **Adressprüfung beim Verbindungsaufbau:** Der Server löst den Hostnamen auf und prüft **jede** Adresse unmittelbar vor dem Verbinden. Gesperrt sind Loopback, Link-Local (169.254.0.0/16, fe80::/10, damit auch Cloud-Metadatendienste), 0.0.0.0/8, Multicast, Broadcast und bekannte Metadatenadressen (100.100.100.200, fd00:ec2::/32). Interne Netze (10/8, 172.16/12, 192.168/16) sind erlaubt, weil DMS und Gateways meist im Intranet stehen.
- **Keine Weiterleitungen:** HTTP-Weiterleitungen werden nicht verfolgt; ein 3xx zählt als Fehler.
- **HTTPS ist Pflicht.** Unverschlüsseltes HTTP nur mit dem Schalter **Unverschlüsseltes HTTP erlauben (nur Testsysteme)**, Syslog über TCP nur mit **Unverschlüsseltes TCP erlauben (nur internes Netz)**. Das gilt auch für den **Token-Endpunkt** (OAuth 2.0): Er muss beim Speichern eine absolute `https://`-Adresse ohne Benutzerangaben sein, sonst meldet das Panel `itg_err_https` bzw. `itg_err_endpoint`; er darf auf einem anderen Host liegen als die Adresse der Verbindung (Identitätsanbieter). Zusätzlich verweigert der Server jede ausgehende Anfrage (Webhooks, CMIS, XTA, FIT-Connect, Token-Abrufe) ohne HTTPS (außer bei gesetztem Schalter) oder mit Zugangsdaten in der Adresse, bevor etwas gesendet wird.
- **Zertifikate:** Geprüft wird gegen die Zertifizierungsstellen des Containers, die Stellen aus `deploy/docker/ca/` (siehe Technisches Handbuch, *Interne Zertifizierungsstelle*) und je Verbindung **Zusätzliche vertrauenswürdige Zertifizierungsstelle (PEM)**. Ein Zertifikat für einen anderen Hostnamen wird immer abgelehnt.
- **Zertifikats-Pin:** Optional SHA-256 des öffentlichen Schlüssels (SPKI), Base64 oder Hex, mehrere durch Komma. Dann gilt die Verbindung nur, wenn ein Zertifikat der Kette genau diesen Schlüssel trägt. Ermitteln:

```
sh openssl s_client -connect dms.example.org:443 </dev/null 2>/dev/null \ | openssl x509 -pubkey -noout | openssl pkey -pubin -outform der \ | openssl dgst -sha256 -binary | base64
```

- **Client-Zertifikat (mTLS):** PKCS#12-Datei mit privatem Schlüssel und Kennwort (Pflicht für XTA 2). Datei und Kennwort werden gemeinsam geschützt gespeichert; das Kennwort darf beliebige Zeichen enthalten.
- **Proxy:** Ist `HTTPS_PROXY` gesetzt, läuft der Verkehr über den Proxy; die Adressprüfung erfolgt dann vor dem Senden. Interne Zielsysteme gehören in `NO_PROXY`, damit die Prüfung beim Verbindungsaufbau greift.
- **Grenzen:** 15 s Verbindungsaufbau, 30 s je Anfrage (Uploads an CMIS 600 s, XTA 2 und FIT-Connect 5 Minuten je Aufruf), Antworten höchstens 50 MB. Ein durch die Adressprüfung gesperrtes Ziel gilt als dauerhafter Fehler.
- **Geheimnisse** (Kennwörter, Tokens, OAuth-Secrets, SFTP-Schlüssel, Client-Zertifikate, Webhook-Secrets) liegen mit ASP.NET Data Protection verschlüsselt in der Datenbank (Schlüssel im Volume `dpkeys`). Das Panel zeigt sie nie wieder an, nur „gespeichert – leer lassen zum Behalten“. Sie erscheinen weder im Export noch in Protokollen oder im Audit.
- **Geändertes Ziel:** Ändern sich Adresse, Token-Endpunkt, XTA-Dienst, SFTP-Hostschlüssel, CA, Pin oder **Unverschlüsseltes HTTP erlauben** einer Verbindung, muss ein gespeichertes Kennwort bzw. Secret neu eingegeben oder entfernt und ebenso ein gespeichertes Client-Zertifikat neu hochgeladen oder entfernt werden; sonst lehnt das Panel das Speichern ab. Das Signatur-Secret von Webhooks ist davon nicht betroffen. OAuth-2.0-Zugriffstoken werden je Token-Endpunkt, Client-ID, Secret und Scope zwischengespeichert; eine Verbindung nutzt daher nur ein Token, das mit ihren eigenen Zugangsdaten abgerufen wurde.

Die Zielsysteme gehören in die Firewall-Freigabe für ausgehende Verbindungen.

REST/JSON-API

API-Client anlegen

Panel → **Schnittstellen** → **Neuer API-Client**:

1. **Allgemein:** Name, Beschreibung, **Zweck der Übermittlung**, **Rechtsgrundlage**.
2. **Anmeldeverfahren:** - **Signierte Client-Assertion (private_key_jwt, empfohlen):** Öffentlichen Schlüssel des Drittsystems als PEM (RSA ab 2048 Bit oder EC), X.509-Zertifikat oder JWKS hinterlegen. Auf dem Server liegt kein Geheimnis. - **Client-Secret (client_secret_basic):** Das Secret wird nach dem Speichern **einmal** angezeigt; gespeichert ist nur sein Hash. **Neues Secret erzeugen** macht das bisherige sofort ungültig.
3. **Berechtigungen (Scopes):** nur so viel wie nötig.
4. **Erlaubte Absender-IP-Adressen:** eine Adresse oder ein CIDR-Netz je Zeile. **Leer bedeutet kein Zugriff.** `*` erlaubt jede Adresse und ist nicht empfohlen. Hinter einem Reverse-Proxy zählt die weitergereichte Adresse; dafür muss `ReverseProxy:Enabled` gesetzt und der Proxy eingetragen sein.
5. **Gültig bis** (optional), **Token-Laufzeit (Sekunden)** 60–3600 (Standard 900), **Anfragen pro Minute** 1–6000 (Standard 120).
6. **Bereiche**, **Datenschutz** und **Eingehende Richtung** wie in den jeweiligen Abschnitten beschrieben.
7. Speichern (erneute Anmeldebestätigung), dann **Zur Freigabe einreichen**.

Die Client-ID beginnt mit `ffi-`. **Client widerrufen** entzieht den Zugang endgültig und löscht die Zugangsdaten.

Token abrufen

Client-Credentials-Grant gegen `https://<server>/connect/token`. Ohne Parameter `scope` erhält der Client alle zugewiesenen Scopes; mit `scope` (durch Leerzeichen getrennt) nur die angeforderten. Die Anforderung eines Scopes, der dem Client nicht zugewiesen ist, wird abgelehnt (`invalid_request`, unbekannte Scopes `invalid_scope`).

Mit Client-Secret:

```
curl -sS -u "ffi-…:<secret>" -d grant_type=client_credentials \
  -d scope="integration:cases.read integration:documents.read" \
  https://ff.traeger.example/connect/token
```

Mit private_key_jwt: Das Drittsystem signiert ein kurzlebiges JWT (RS256 oder ES256) mit `iss` und `sub` = Client-ID, `aud` = Basisadresse des Servers (z. B. `https://ff.traeger.example/`), eindeutiger `jti` und einer Laufzeit von wenigen Minuten, Typ `client-authentication+jwt`, und sendet es als `client_assertion` mit `client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer`.

Der Token-Endpunkt prüft zusätzlich Status **Aktiv**, Ablaufdatum, IP-Liste und die aktive Organisationslizenz. Eine Ablehnung kommt als `unauthorized_client` mit dem Fehlercode (z. B. `integration.ip_denied`) in `error_description`. Jede Anfrage an die API prüft dieselben Bedingungen erneut; Sperren, Pausieren und Widerrufen wirken spätestens nach 30 Sekunden auch auf bereits ausgestellte Tokens.

Scopes

Scope	Erlaubt
`integration:cases.read`	Fälle lesen (Stammdaten, Status, Bewilligung; pseudonymisiert)
`integration:sensitive`	Zusatz: Klarnamen und vertrauliche Felder statt Pseudonymen; gilt als Öffnung der Datenschutz-Einstellungen, hinzufügen dürfen ihn nur Konten, die diese öffnen dürfen
`integration:persons.read`	Beteiligte Personen eines Falls lesen
`integration:documents.read`	E-Akte lesen (Metadaten und Dateien)
`integration:documents.write`	Dokumente in die E-Akte einliefern und eigene Einlieferungen zurückziehen
`integration:cases.write`	freigegebene Feldgruppen von Fällen ändern, Fremdreferenz setzen
`integration:appointments.write`	Termine zu Fällen anlegen
`integration:time.read`	Zeiteinträge und Tätigkeitsnachweise lesen (auch im CMIS-Repository)
`integration:billing.read`	Entgeltvereinbarungen lesen
`integration:catalogs.read`	Kataloge lesen (Maßnahmen, Tätigkeitsarten, Einrichtungen, Textbausteine der Organisation)
`integration:catalogs.write`	Maßnahmen und Tätigkeitsarten pflegen
`integration:directory.read`	Mitarbeitende und Teams lesen (ohne Rechte und Geräte)
`integration:changes.read`	Änderungs-Feed lesen (nur Kennungen)
`integration:inbox.read`	Status eigener Einlieferungen abfragen

Schreibende Scopes wirken nur zusammen mit den Einstellungen der **Eingehenden Richtung**.

Ressourcen

Alle Pfade relativ zu `/api/integration/v1`.

Methode und Pfad	Scope	Inhalt
`GET /health`	gültiges Token	Verbindungstest: Client-Name, Scopes, Serverzeit
`GET /cases`	cases.read	Fallliste; Filter `updatedSince`, `status`, `helpType`, `areaId`; `cursor`, `limit` (Standard 50, höchstens 200)
`GET /cases/{caseId}`	cases.read	ein Fall mit `ETag`
`GET /cases/{caseId}/persons`	persons.read	Beteiligte mit Rollen
`GET /cases/{caseId}/documents`	documents.read	E-Akte-Einträge mit Dateien (Metadaten)
`GET /documents/{documentId}`	documents.read	ein Dokument mit `ETag`
`GET /documents/{documentId}/files/{index}/content`	documents.read	Dateiinhalt mit `Repr-Digest: sha-256=…`, Range-Abrufe möglich
`GET /cases/{caseId}/activity-reports`	time.read	archivierte Tätigkeitsnachweise des Falls
`GET /activity-reports`	time.read	alle sichtbaren Tätigkeitsnachweise
`GET /activity-reports/{reportId}/content`	time.read	PDF eines Nachweises
`GET /time-entries`	time.read	Zeiteinträge; Filter `from`, `to`, `caseId`, `userId`; `cursor`, `limit` (Standard 100, höchstens 200)
`GET /cases/{caseId}/rate-agreements`, `GET /rate-agreements`	billing.read	Entgeltvereinbarungen
`GET /catalogs/{catalog}`	catalogs.read	`measures`, `activity-types`, `institutions`, `text-snippets`
`PUT /catalogs/{catalog}/{externalId}`	catalogs.write	Maßnahme oder Tätigkeitsart anlegen oder ändern (`measures`, `activity-types`)
`GET /directory/users`, `GET /directory/teams`	directory.read	Mitarbeitende und Teams
`GET /changes`	changes.read	Änderungs-Feed
`POST /cases/{caseId}/documents`	documents.write	Dokument in die E-Akte eines Falls einliefern
`POST /documents`	documents.write	Dokument mit Fallbezug über `caseReference` einliefern
`PATCH /cases/{caseId}`	cases.write	freigegebene Feldgruppen ändern
`PUT /cases/{caseId}/external-reference`	cases.write	eigene Fremd-ID am Fall hinterlegen
`POST /cases/{caseId}/appointments`	appointments.write	Termin anlegen
`GET /inbox`, `GET /inbox/{itemId}`	inbox.read	Stand eigener Einlieferungen
`DELETE /inbox/{itemId}`	documents.write	eigene, noch unbearbeitete Einlieferung zurückziehen

Werte wie `status`, `helpType`, `approval.period` und die Terminart sind Namen der Aufzählungen (z. B. `Active`, `SocialPedagogicalFamilySupport`, `Month`); die OpenAPI-Beschreibung listet sie vollständig.

Beispiel `GET /cases/{caseId}` ohne Klarnamen:

```
{
  "id": "6f1c0e8a-4c6b-4f0e-9a51-0d2f3b8e2c11",
  "fileNumber": "51.2-2026-0142",
  "alias": "K-0142",
  "status": "Active",
  "helpType": "SocialPedagogicalFamilySupport",
  "startDate": "2026-03-01",
  "endDate": null,
  "approval": { "minutes": 480, "period": "Month", "from": "2026-03-01", "to": "2026-08-31" },
  "responsibleAuthority": "Jugendamt Musterstadt",
  "caseworker": { "name": "[pseudonymisiert]", "contact": "[pseudonymisiert]" },
  "areas": [ { "id": "…", "name": "Ambulante Hilfen Nord" } ],
  "externalReferences": { "client:…": "FV-2026-0815" },
  "revision": 57,
  "updatedAt": "2026-10-26T14:03:11+01:00"
}
```

Konventionen

- **JSON:** camelCase, Zeitstempel nach ISO 8601 mit Offset, Kennungen als UUID-Zeichenketten.
- **Fehler:** RFC 9457 (`application/problem+json`) mit dem Feld `code`, z. B. `integration.scope_missing`. Alle Codes stehen im Kapitel *Fehlerbehebung*.
- **Seiten:** opaker `cursor`; die Antwort enthält `items` und `nextCursor`, dazu einen Kopf `Link: <…>; rel="next"`. Den Cursor nicht selbst bauen.
- **ETags:** `GET /cases/{caseId}` und `GET /documents/{documentId}` liefern `ETag: "<revision>"`; mit `If-None-Match` antwortet der Server `304`.
- **Schreiben:** Dokument-Einlieferungen verlangen `Idempotency-Key` (sonst `428`), höchstens 200 Zeichen ohne Steuerzeichen; längere Schlüssel weist der Server mit `422` `integration.payload_invalid` ab, statt sie zu kürzen. Derselbe Schlüssel liefert je Client dieselbe Einlieferung zurück, auch bei

gleichzeitigen Wiederholungen (eindeutiger Datenbankindex; die Datei des doppelten Uploads wird verworfen). Eine bereits übernommene `externalId` ergibt `409 integration.idempotency_conflict`. `PATCH /cases/{caseId}` verlangt `If-Match` mit der Revision (sonst `428`, bei veralteter Revision `412`).

- **Ratenbegrenzung:** je Client die eingestellten Anfragen pro Minute; darüber `429` mit `Retry-After: 60`.
- **Audit:** Jede Anfrage schreibt `integration.api_access`, jede Ablehnung `integration.api_denied`.

Änderungs-Feed

`GET /changes?after=<sequence>&limit=<n>` (Standard 500, höchstens 1000) liefert `items` mit `sequence`, `kind` (`upserted` oder `deleted`), `entityType`, `entityId`, `caseId`, `occurredAt` und `next` für den nächsten Abruf. Enthalten sind nur Typen, für die der Client Lese-Scopes hat (Fälle, Personen, Dokumente, Zeiteinträge, Entgeltvereinbarungen), nur sichtbare Fälle und keine Inhalte. Jeden Eintrag außerhalb der Fälle prüft der Server gegen den aktuellen Stand: `upserted` nur, wenn der Datensatz noch existiert, nicht gelöscht, privat, eingeschränkt oder zur Löschung vorgemerkt ist und Dokumente die Dokumentfilter des Clients wie beim direkten Abruf bestehen; `deleted`, wenn der Datensatz ganz entfernt ist (nur die Kennung, zum lokalen Bereinigen) oder der verbliebene Datensatz weder privat noch eingeschränkt noch zur Löschung vorgemerkt ist und Dokumente die Filter bestehen. Eine Seite kann deshalb weniger Einträge als `limit` enthalten; `next` weiter folgen, bis es `null` ist. Liegt `after` vor dem Aufbewahrungsbeginn des Sync-Feeds, antwortet der Server `410` mit `integration.cursor_expired`: dann einmal über die Listen-Ressourcen vollständig abgleichen und mit der aktuellen Sequenz weitermachen.

Webhooks

Einrichten

Panel → **Schnittstellen** → **+ Webhook**:

1. Name, **Adresse** (HTTPS), Zweck, Rechtsgrundlage.
2. Optional Anmeldung beim Zielsystem (Basic, Bearer, OAuth 2.0 Client Credentials, Client-Zertifikat) und TLS-Einstellungen.
3. **Auslöser** und unter **Ereignisse** die Ereignistypen wählen; ohne Auswahl gehen alle ausgelösten Ereignisse hinaus.
4. Speichern: Das **Signatur-Secret** (`whsec_…`) wird erzeugt und **einmal** angezeigt. Beim Empfänger hinterlegen. **Neues Signatur-Secret** ersetzt es sofort.
5. **Verbindung prüfen** sendet das Ereignis `de.fokusfamilie.test`. Danach einreichen.

Ereignisse

Typ	Auslöser im Panel	Wann
`de.fokusfamilie.case.created`	Fall wird angelegt oder geändert	erste Fassung eines Falls
`de.fokusfamilie.case.updated`	Fall wird angelegt oder geändert	jede weitere Fassung
`de.fokusfamilie.case.closed`	Fall wird abgeschlossen (ganze Akte)	Status „Abgeschlossen“ oder „Archiviert“
`de.fokusfamilie.document.finalized`	Dokument wird final oder unterschrieben	nach Datenschutzfilter der Verbindung
`de.fokusfamilie.activity_report.closed`	Tätigkeitsnachweis wird abgeschlossen und archiviert	neuer archivierter Nachweis
`de.fokusfamilie.case.erasure_requested`	Löschung eines Falls wird beantragt	Löschantrag oder gelöschter Fall, ohne Inhalt
`de.fokusfamilie.inbound.accepted`	ohne Auslöser, über **Ereignisse** wählbar	ein Eingang wurde übernommen (direkt oder nach Prüfung)
`de.fokusfamilie.inbound.rejected`	ohne Auslöser, über **Ereignisse** wählbar	ein Eingang wurde bei der Prüfung abgelehnt
`de.fokusfamilie.inbound.conflict`	ohne Auslöser, über **Ereignisse** wählbar	Feldkonflikt beim Eingang im Posteingangs-Modus
`de.fokusfamilie.test`	Verbindungsprüfung	nur auf **Verbindung prüfen**

Die Ereignisse `de.fokusfamilie.inbound.*` gehen an jede aktive Webhook-Verbindung, die sie abonniert hat (oder keine Auswahl getroffen hat) und deren Bereiche den Fall abdecken; Eingänge ohne Fall erhalten nur Verbindungen ohne Bereichsbindung. Sie tragen `entityType IntegrationInbox`, die ID des Eingangs und den Link `/api/integration/v1/inbox/{id}`, aber keinen Ablehnungsgrund; den vollständigen Stand fragt der einliefernde API-Client über `GET /inbox/{id}` ab.

Nachrichtenformat

Jede Nachricht ist ein CloudEvent 1.0 im strukturierten Modus (`Content-Type: application/cloudevents+json`) und enthält **nur Kennungen und Links**. Die Daten holt der Empfänger mit seinem API-Client.

```
{
  "specversion": "1.0",
  "id": "3b0d2f0e-7c1a-4f7e-8d55-9a3c1e2b4f60",
  "source": "urn:fokusfamilie:organization:2c9a…",
  "type": "de.fokusfamilie.document.finalized",
  "time": "2026-10-28T09:12:44+00:00",
  "datacontenttype": "application/json",
  "subject": "8e41…",
  "data": {
    "entityType": "StoredDocument",
    "entityId": "8e41…",
    "caseId": "6f1c…",
    "links": {
      "case": "/api/integration/v1/cases/6f1c…",
      "document": "/api/integration/v1/documents/8e41…"
    }
  }
}
```

Signatur prüfen

Signiert wird nach **Standard Webhooks**: Kopfzeilen `webhook-id`, `webhook-timestamp` (Unix-Sekunden) und `webhook-signature` (`v1,<Base64>`, mehrere durch Leerzeichen). Signiert ist die Zeichenfolge `<webhook-id>.<webhook-timestamp>.<Rohkörper>` mit HMAC-SHA256; Schlüssel ist der Base64-Teil des Secrets nach `whsec_`.

```
import base64, hashlib, hmac, time

def verify(secret: str, headers: dict, body: bytes, tolerance: int = 300) -> bool:
    msg_id, ts = headers["webhook-id"], headers["webhook-timestamp"]
    if abs(time.time() - int(ts)) > tolerance:
        return False
    key = base64.b64decode(secret.removeprefix("whsec_"))
    mac = hmac.new(key, f"{msg_id}.{ts}.".encode() + body, hashlib.sha256).digest()
    expected = "v1," + base64.b64encode(mac).decode()
    return any(hmac.compare_digest(expected, s) for s in headers["webhook-signature"].split())
```

Nachrichten mit zu altem Zeitstempel ablehnen (Empfehlung: 5 Minuten) und verarbeitete `webhook-id`-Werte merken, damit eine abgefangene Nachricht nicht erneut wirkt. Wiederholungen derselben Zustellung tragen dieselbe `webhook-id`.

Zustellverhalten

- `2xx` gilt als zugestellt.
- `400`, `401`, `403`, `404`, `405`, `410`, `413` und `422` gelten als dauerhaft: Die Zustellung wird sofort **Endgültig fehlgeschlagen**.
- Alle anderen Antworten, Zeitüberschreitungen und Netzfehler werden wiederholt (siehe *Betrieb*).
- Dieselbe Fassung eines Objekts wird je Verbindung und Ereignistyp nur einmal eingeplant.
- Unmittelbar vor jedem Zustellversuch, auch vor Wiederholungen, prüft der Server erneut, ob der Fall im aktuellen Bereich der Verbindung sichtbar und das Dokument nach ihren Datenschutzeinstellungen freigegeben ist. Ist das nicht mehr der Fall, wird das Ereignis nicht gesendet, sondern mit dem Grund `not_visible` als **Übersprungen** markiert.
- Löschaufforderungen (`de.fokusfamilie.case.erasure_requested`) werden weiterhin gesendet, aber nur an Verbindungen, deren Bereich den Fall umfasst, und an organisationsweite Verbindungen.

Eingehende Richtung

Jede API-Client- und jede CMIS- oder XÖV-Verbindung hat die Karte **Eingehende Richtung**; Webhook- und SIEM-Verbindungen arbeiten nur ausgehend. Standardmäßig ist alles aus.

Einstellung	Standard	Wirkung
Dokumente in die E-Akte einliefern	aus	neue Dokumente als Eintrag der E-Akte, nur anfügen
Übernahme von Dokumenten	Posteingang	**Posteingang (prüfen und übernehmen)** oder **Direkt übernehmen**
Fall-Stammdaten ändern (API-Client)	aus	nur die gewählten **Erlaubten Feldgruppen**: Aktenzeichen; Zuständiges Jugendamt und ASD-Kontakt; Bewilligung (Umfang, Zeitraum); Status und Hilfeende
Übernahme von Feldänderungen	Posteingang	wie bei Dokumenten
Termine anlegen (API-Client)	aus	Termine zu sichtbaren Fällen; werden sofort angelegt
Kataloge pflegen (API-Client)	aus	Maßnahmen und Tätigkeitsarten über `PUT /catalogs/…`
Fallzuordnung	Fremdreferenz oder Aktenzeichen	**Nur über hinterlegte Fremdreferenz**, **Nur über Aktenzeichen** oder beides; ein Aktenzeichen muss eindeutig sein
Max. Dateigröße (MB)	25	1–2048
Max. Einlieferungen pro Stunde	200	1–100 000, je Client bzw. Verbindung
Erlaubte Dateitypen	PDF, PNG, JPEG, DOCX	MIME-Typen, einer je Zeile

Freitexte der Fachkräfte sind nie beschreibbar, Löschungen von außen gibt es nicht. Eingelieferte Dateien werden wie jeder Upload auf Schadsoftware geprüft, verschlüsselt gespeichert und erreichen die Geräte per Synchronisation.

Dokumente einliefern

`POST /cases/{caseId}/documents` als `multipart/form-data` mit dem Teil `metadata` (JSON) und dem Teil `file`:

```
curl -sS -H "Authorization: Bearer $TOKEN" -H "Idempotency-Key: fv-2026-0815-hpg" \
  -F 'metadata={"title":"Hilfeplan 2026","documentType":"imported","externalId":"FV-4711"};type=application/json' \
  -F 'file=@hilfeplan.pdf;type=application/pdf' \
  https://ff.traeger.example/api/integration/v1/cases/6f1c…/documents
```

- `title` ist Pflicht (höchstens 200 Zeichen); `documentType`, `externalId` und `createdAt` sind optional.
- Ohne bekannte Fall-ID: `POST /documents` mit `caseReference` in den Metadaten (Fremdreferenz oder Aktenzeichen, je nach **Fallzuordnung**). Findet sich kein eindeutiger Fall, landet das Dokument im Status **Fall zuordnen** im Posteingang; zuvor durchläuft es dieselben Prüfungen wie jede andere Einlieferung (Anhangsrichtlinie, Inhalt gegen den MIME-Typ, Virenscan).
- Antwort `202` mit dem Stand der Einlieferung und `Location` auf `/inbox/{id}`; bei **Direkt übernehmen** `201`.
- Übernommene Dokumente sind final, tragen den Namen der Schnittstelle als Autorin bzw. Autor und erscheinen im Verlauf des Falls mit der Quelle „Schnittstelle“.

Fall-Stammdaten ändern

`PATCH /cases/{caseId}` mit `If-Match: "<revision>"` und einem JSON-Objekt, das nur `fileNumber`, `responsibleAuthority`, `caseworker` (`name`, `contact`), `approval` (`minutes`, `period`, `from`, `to`), `status` und `endDate` enthalten darf. Felder außerhalb der freigegebenen Gruppen führen zu `403 integration.field_group_denied`.

Hat eine Fachkraft ein Feld seit der letzten Übernahme dieses Systems geändert, gewinnt die Fachkraft: Die Änderung landet als **Konflikt** im Posteingang. `PUT /cases/{caseId}/external-reference` hinterlegt die eigene Fremd-ID des Systems, über die spätere Einlieferungen den Fall finden.

Posteingang und Prüfung

Eingänge im Status **Zu prüfen**, **Konflikt** oder **Fall zuordnen** erscheinen auf der Seite **Eingänge (Schnittstellen)**. Dort prüfen Konten mit **Eingänge aus Schnittstellen prüfen und übernehmen** im eigenen Verwaltungsumfang und wählen **Übernehmen**, **Zuordnen** (Fall wählen) oder **Ablehnen**. Es gelten dieselben Regeln wie in der Fallansicht: Eingänge und die Fallauswahl zeigen nur Fälle, die nicht gelöscht, nicht zur Löschung vorgemerkt und nicht in der Verarbeitung eingeschränkt sind. Eingänge ohne Fall sehen nur Konten mit organisationsweitem Verwaltungsumfang. Erfüllt der Fall eines Eingangs oder der gewählte Zielfall diese Regeln nicht, verweigert der Server Übernehmen, Zuordnen und Ablehnen; wird ein Fall etwa in der Verarbeitung eingeschränkt, verschwinden seine Eingänge aus der Liste. Der Ablauf aus fachlicher Sicht steht im Handbuch für das Admin-Panel.

Übernehmen ist atomar: Zieldatensatz, Eintrag im Sync-Änderungs-Feed, Fremdreferenz und der Zustand „Übernommen“ entstehen in einer Transaktion. Übernimmt eine zweite Person dasselbe Element gleichzeitig, wartet ihre Übernahme und schlägt danach fehl, ohne eine Dublette anzulegen.

Zurückziehen

`DELETE /inbox/{itemId}` zieht eine eigene Einlieferung zurück, solange sie unbearbeitet ist: im Posteingang jederzeit, nach der Übernahme nur, solange niemand das Dokument geändert hat. Danach löscht nur ein Mensch in Focus Family.

CMIS: Ablage im DMS oder in der E-Akte

Focus Family legt Dokumente über **CMIS 1.1 Browser Binding** (JSON) in einem Dokumentenmanagement oder einer E-Akte ab, etwa Alfresco, Nuxeo oder Systeme mit CMIS-Aufsatz.

Einrichten

Panel → **Schnittstellen** → **+ DMS/E-Akte (CMIS)**:

1. **Adresse** des Browser Binding, z. B. `https://dms.example.org/alfresco/api/-default-/public/cmis/versions/1.1/browser`. Alle Aufrufe, auch an die vom Repository gemeldeten Adressen (`repositoryUrl`, `rootFolderUrl`), müssen bei Schema, Host und Port dieser Adresse bleiben; sonst bricht der Server ab, bevor Zugangsdaten gesendet werden (`permissionDenied` „… differs from the configured address“).
2. **Anmeldung beim Zielsystem:** Basic, Bearer, OAuth 2.0 Client Credentials (Client-ID als Benutzername, Secret, **Token-Endpunkt**, optional **Scope**) oder Client-Zertifikat.
3. **CMIS-Repository: Repository-ID** (leer: erstes Repository), **Basisordner**, **Dokumenttyp** und **Ordnertyp** (Standard `cmis:document` bzw. `cmis:folder`), **Secondary Types (Aspekte)**, **Eigenschaftszuordnung**, **Geänderte Dokumente als neue Version ablegen (Check-out/Check-in)**.
4. **Auslöser** (Standard alle): Dokument wird final oder unterschrieben (optional **Nur unterschriebene Dokumente** und eine Liste von Dokumenttypen), Tätigkeitsnachweis wird abgeschlossen und archiviert, Fall wird abgeschlossen (ganze Akte), Manuell aus der Fallansicht.
5. **Datenschutz**, **Ordnervorlage**, **Bereiche**, optional **Eingangsordner (Gegenrichtung)**.
6. Speichern, **Verbindung prüfen**, einreichen.

Ablagestruktur

Die **Ordnervorlage** bestimmt den Pfad unter dem Basisordner. Platzhalter: `{year}` (Jahr des Hilfebeginns), `{fileNumber}` (fällt auf den Fallalias zurück), `{alias}`, `{caseId}`, `{helpType}`, `{section}`. Bereiche der E-Akte heißen im Zielsystem „Verträge und Einwilligungen“, „Berichte und Dokumentation“, „Nachweise“, „Eingänge“, „Notizen“ und „Sonstiges“. Fehlende Ordner legt der Server an.

- **Dokument final:** Das Dokument wird abgelegt. Ändert es sich später, entsteht bei versionierbarem Typ eine neue Version, sonst ein weiteres Dokument mit Namenszusatz. Unveränderte Fassungen werden nicht erneut übertragen.
- **Fall abgeschlossen** und **manuelle Übergabe:** alle zulässigen Dokumente des Falls plus das Aktenverzeichnis `fokusfamilie-akte.json` im Fallordner (Format `fokusfamilie-case-file/1` mit Dokument-ID, Titel, Bereich, Version, SHA-256 und Objekt-ID im Zielsystem).
- **Tätigkeitsnachweis:** das archivierte PDF. Der Server prüft neue Nachweise in der Reihenfolge ihres Eingangs und rückt seinen Fortschritt erst vor, wenn der ganze Durchlauf samt aller Nachweise mit demselben Eingangszeitpunkt eingereiht ist; nach einem Abbruch wiederholt der nächste Durchlauf die Gruppe. Das Einreihen ist idempotent, es geht also nichts verloren und nichts wird doppelt übergeben.

Eigenschaften

Die **Eigenschaftszuordnung** enthält eine Zeile je Eigenschaft: `CMIS-Eigenschaft = Quelle`. Quellen: `fileNumber`, `alias`, `caseId`, `documentId`, `documentType`, `section`, `version`, `status`, `signed`, `createdAt`, `author`, `sha256`, `helpType`, `title`. Namen und Autor erscheinen nur mit **Klarnamen übertragen** im Klartext. Die Eigenschaften müssen im Dokumenttyp bzw. in einem eingetragenen Aspekt existieren.

Verbindungsprüfung

Verbindung prüfen zeigt jeden Schritt einzeln: Repository erreichbar, Dokumenttyp vorhanden, Ordnertyp vorhanden, Eigenschaftszuordnung gültig, Basisordner bereit, Testordner angelegt, Testdokument abgelegt, neue Version angelegt, Inhalt zurückgelesen, Testobjekte entfernt und gegebenenfalls Eingangsordner vorhanden. Fehlende Typen und Eigenschaften stehen im Klartext daneben.

Eingangsordner (Gegenrichtung)

Mit Richtung **Eingehend** oder **Beidseitig** und **Dokumente in die E-Akte einliefern** fragt der Server den **Eingangsordner** im **Abfrageintervall (Minuten)** (1–1440, Standard 5) ab:

- Unterordner des Eingangsordners benennen den Fall (Aktenzeichen oder Fremdreferenz). Dokumente direkt im Eingangsordner brauchen die Zuordnungszeile `inbox:caseReference = <CMIS-Eigenschaft>`.
- Übernommene Dokumente verschiebt der Server in den **Ordner für übernommene Dokumente**. Dokumente ohne passenden Fall bleiben liegen und erscheinen als **Fall zuordnen** im Posteingang.
- Von Focus Family selbst abgelegte Dokumente werden nicht zurückgeholt.
- Downloads sind schon beim Lesen auf die **Max. Dateigröße** der Verbindung begrenzt und brechen nach 10 Minuten ab; die Verbindung zeigt dann einen `413`- bzw. `408`-Fehler, der Abfragelauf endet und das Dokument bleibt im Ordner, bis es im DMS entfernt oder ersetzt wird. Von einer Prüfung abgewiesene Dokumente (Dateityp, Größe, Stundenlimit, Schadsoftware) bleiben im Ordner und werden bei der nächsten Abfrage erneut geprüft. Fehler beim Abfragen zählen nicht zur automatischen Pause.
- Wurde eine Version eines Dokuments übernommen, werden spätere Versionen derselben Versionsreihe abgewiesen (`integration.idempotency_conflict`) und bleiben im Eingangsordner. Ist der vom Server gebildete Idempotenzschlüssel länger als 200 Zeichen, verwendet er intern einen Hashwert.

CMIS-Repository von Focus Family

Umgekehrt kann ein DMS die Fallakten über `https://<server>/cmis/browser` lesen (CMIS 1.1 Browser Binding, Repository-ID `focusfamily`).

Anmeldung und Rechte

- Ein **API-Client** mit den Scopes `integration:cases.read` und `integration:documents.read`; zum Ablegen zusätzlich `integration:documents.write` und **Dokumente in die E-Akte einliefern**.
- Anmeldung entweder mit **Basic** (Client-ID und Client-Secret, nur bei Anmeldeverfahren Client-Secret) oder mit einem **Bearer-Token** vom Token-Endpunkt. Nach `RateLimiting:AuthPermitLimit` fehlgeschlagenen Basic-Anmeldungen (Standard 100) von einer IP-Adresse innerhalb einer Minute erhalten weitere Basic-Anfragen von dort für den Rest der Minute 429 `integration.rate_limited`.

- Der Ordner `Taetigkeitsnachweise` und seine Tätigkeitsnachweise sind nur mit dem zusätzlichen Scope `integration:time.read` sichtbar; ohne ihn antworten sie mit `objectNotFound`.
- Es gelten Status, Ablaufdatum (`integration.client_expired`), IP-Liste, Lizenz, Ratenbegrenzung, Bereiche und Datenschutz-Einstellungen des Clients wie bei der REST-API. Zugriffe und Ablehnungen werden wie dort als `integration.api_access` bzw. `integration.api_denied` auditiert.

Aufbau

```
/ (Focus Family)
├── Faelle
│   └── <Aktenzeichen oder Alias> (<Kurzkennung>)     Typ ff:caseFolder
│       └── <Bereich der E-Akte>
│           └── <Dokument>                            Typ ff:document
└── Taetigkeitsnachweise
    └── Taetigkeitsnachweis <Nummer>.pdf
```

Eigenschaften der eigenen Typen: `ff:caseId`, `ff:fileNumber`, `ff:alias`, `ff:documentType`, `ff:section`, `ff:status`, `ff:signed`, `ff:sha256`, `ff:source`. Unterstützte Abfragen: Repository-Info, `typeChildren`, `typeDefinition`, `query`, `contentChanges` (nur Objekt-IDs) sowie je Objekt `object`, `content`, `children`, `parent`, `parents`, `allowableActions` und `versions`. Nicht unterstützt: ACL, Renditions, Multifiling, Ordnerbäume, Join und Sortierung.

Abfragen und Grenzen

`query` versteht eine bewusst kleine Teilmenge von CMIS-SQL:

```
SELECT * FROM ff:document WHERE IN_FOLDER('case:…') AND cmis:lastModificationDate >= TIMESTAMP '2026-10-01T00:00:00Z'
```

- `FROM` nur `cmis:document`, `ff:document`, `cmis:folder` oder `ff:caseFolder`.
- `WHERE` nur `IN_FOLDER('<id>')` und Vergleiche `=`, `>=`, `>` mit einem Wert in Hochkommas, verknüpft mit `AND`.
- Höchstens 1000 Treffer je Abfrage; durchsucht werden höchstens 2000 Fälle bzw. 5000 Dokumente; `children` liefert höchstens 1000 Einträge je Seite.

Alles andere lehnt der Server mit `invalidArgument` ab.

Dokumente ablegen

`createDocument` (Formular mit `cmisaction=createDocument`, Datei im Teil `content`) ist nur in einem Fallordner erlaubt. Optional `ff:documentType` und `ff:externalId` als Eigenschaften und `Idempotency-Key` als Kopfzeile. Das Dokument durchläuft die eingehende Richtung wie eine REST-Einlieferung (Prüfung, Posteingang oder direkte Übernahme). `delete` zieht nur eigene, noch unbearbeitete Einlieferungen zurück.

XÖV und xdomea

Was übertragen wird

- **Ausgehend:** Bei Fallabschluss (oder manueller Übergabe) entsteht eine **xdomea-Abgabe** (Nachricht `0401`, Version **3.1.0** oder **4.0.0**) als ZIP-Paket `<Prozess-ID>_Abgabe.Abgabe.0401.zip`. Das Paket enthält die Nachricht und die Primärdokumente der zulässigen E-Akte-Einträge mit SHA-256-Prüfsumme, gegliedert als ein Vorgang je Bereich der E-Akte oder als ein Vorgang (**Gliederung der Akte**). Aufbewahrungsfrist (Jahre, Standard 10) und **Aussonderungsart** (A – archivwürdig, B – zu bewerten, V – vernichten; Standard B) gehen in die Metadaten. Jede Nachricht wird vor dem Versand gegen das amtliche xdomea-Schema geprüft; ein ungültiges Paket wird nicht versendet.
- **Bestätigung:** Eine eingehende Importbestätigung (`0402`) markiert die Abgabe im Übertragungsprotokoll als **Vom Empfänger bestätigt**; Fehlmeldungen einzelner Objekte stehen im Fehlertext.
- **Eingehend:** Eingehende Abgaben (`0401`) werden geprüft, ihre Dokumente laufen über die eingehende Richtung (Fallzuordnung über das Kennzeichen der Akte). Verlangt der Absender eine Importbestätigung, sendet der Server eine `0402` mit Erfolg oder Fehler je Objekt zurück.

Absender und Empfänger werden als Name und optional mit DVDV-Kennung eingetragen (**Absender (Name der Organisation)**, **Absender-Kennung (DVDV, optional)**, **Empfänger (z. B. Jugendamt)**, **Empfänger-Kennung (DVDV, optional)**).

Transporte

Transport	Adresse	Richtung	Hinweise
Verzeichnis	leer	beide	Übergabe an ein vorhandenes Gateway über ein Verzeichnis im Container
SFTP	`sftp://host:port`	beide	Hostschlüssel-Fingerprint Pflicht; Kennwort oder privater Schlüssel
XTA 2	URL des XTA-Webservice	beide	XTA 2 Version 4 (KoSIT), Client-Zertifikat Pflicht
FIT-Connect	Basis-URL der Submission API	nur ausgehend	OAuth 2.0 Client Credentials, Ende-zu-Ende-Verschlüsselung

Eingehende Pakete dürfen höchstens 200 MB groß sein. Der Server fragt den Eingang im Abfrageintervall der Verbindung ab; bei Verzeichnis und SFTP verarbeitet er je Abfrage bis zu 50 Pakete.

Verzeichnis

Ausgang und Eingang liegen unterhalb des XÖV-Stammverzeichnisses `/var/lib/fokusfamilie/xoev` (Einstellung `Integrations__Xoev__FolderRoot`), Standard `outbox` und `inbox`. Pfade außerhalb des Stammverzeichnisses lehnt der Server ab. Pakete werden zunächst als `.partial` geschrieben und dann umbenannt; gelesen werden nur `*.zip`, danach verschoben nach `inbox/processed` bzw. `inbox/failed`.

Das Stammverzeichnis ist im Standard-Stack **kein Volume**. Einzubinden ist ein Verzeichnis des Hosts, das auch das Gateway erreicht; es gehört dem Container-Benutzer (UID 1654):

```
services:
  app:
    volumes:
      - /srv/fokusfamilie/xoev:/var/lib/fokusfamilie/xoev
```

```
mkdir -p /srv/fokusfamilie/xoev/outbox /srv/fokusfamilie/xoev/inbox
chown -R 1654:1654 /srv/fokusfamilie/xoev
docker compose up -d --force-recreate app
```

SFTP

- **SFTP-Hostschlüssel (SHA256-Fingerprint)** ist Pflicht; ohne passenden Fingerprint baut der Server keine Verbindung auf, eine Abweichung steht mit dem vorgelegten Fingerprint im Fehlertext. Ermitteln: `ssh-keyscan host | ssh-keygen -lf -`.
- Anmeldung mit **Benutzername** und Kennwort oder privatem Schlüssel (PEM) im Feld **Geheimnis**.
- **Ausgangsordner** und **Eingangsordner** relativ zum SFTP-Konto (Standard `outbox`, `inbox`).
- Jeder SFTP-Vorgang ist zeitlich begrenzt: Verbindungsaufbau, Auflisten, Umbenennen, Löschen, Verschieben und Verbindungstest auf 60 Sekunden (`Integrations__Xoev__SftpOperationTimeoutSeconds`), Hoch- und Herunterladen eines Pakets auf 600 Sekunden (`Integrations__Xoev__SftpTransferTimeoutSeconds`). Eine Zeitüberschreitung gilt als vorübergehender Fehler: Ein Versand wird mit Wartezeit wiederholt und zählt zur automatischen Pause, eine fehlgeschlagene Eingangsabfrage wird bei der nächsten Abfrage wiederholt.
- Die Größengrenze für eingehende Pakete gilt für die tatsächlich empfangenen Bytes. Ein zu großes Paket bricht mit „Incoming package exceeds the size limit.“ ab und wird nach `inbox/failed` verschoben. Überschreitet ein Download das Zeitlimit, bleibt das Paket im Eingang und wird beim nächsten Abruf erneut versucht.

XTA 2

- **Dienst (Service-URI aus dem DVDV)**, **Kennungstyp** (Standard `xoev`), **Geschäftsszenario**, optional **Als Testnachricht kennzeichnen (TestMsg)**.
- Absender- und Empfänger-Kennung sind Autor und Leser des Transportauftrags und Pflicht.
- Das Client-Zertifikat (PKCS#12) des XTA-Kontos gehört unter **TLS, Zertifikate und Netz**.
- Hat das Gateway getrennte Ports, steht `{port}` in der Adresse für `management`, `send` bzw. `msgbox`.
- Versand mit `createMessageID` und `sendMessage` (MTOM), Eingang mit `getStatusList`, `getMessage` und `close`; die Verbindungsprüfung ruft `checkAccountActive`.
- Die Umsetzung folgt der Spezifikation und ist gegen einen Spezifikations-Mock geprüft. Vor dem Produktivbetrieb mit dem eigenen Gateway und dessen Testkonto testen.

FIT-Connect

- Anmeldung über **OAuth 2.0 Client Credentials** (Client-ID, Secret und **Token-Endpunkt** des FIT-Connect-Autorisierungsdienstes).
- **Zustellpunkt (Destination-ID)** als UUID, **Verwaltungsleistung (Leistungsschlüssel)**, **Bezeichnung der Leistung**, optional **Schema der Fachdaten**.
- Die xdomea-Nachricht geht als Fachdatensatz, die Primärdokumente als Anlagen, jeweils mit dem öffentlichen Schlüssel des Zustellpunkts verschlüsselt (JWE, RSA-OAEP-256 und A256GCM). Der Schlüssel muss RSA mit mindestens 4096 Bit sein und `wrapKey` erlauben; der Zustellpunkt muss die Leistung und das Schema anbieten. Vor dem Verschlüsseln prüft der Server die Zertifikatskette des Schlüssels (`x5c`): Der Schlüssel muss zum Blattzertifikat passen, das Blatt darf keine CA sein und muss Schlüsselverschlüsselung erlauben, und die Kette muss zu einer Wurzel der Verwaltungs-PKI führen (eingebettet PCA-1-Verwaltung-17, -20, -23 und -26; weitere Wurzeln über `Integrations__Xoev__FitConnectTrustedRootsPem` oder `…File`). Der Sperrstatus wird online geprüft (`Integrations__Xoev__FitConnectRevocationMode`, Standard `Online`). Ist nur der Sperrstatus nicht ermittelbar, wird die Übertragung mit Backoff wiederholt; widerrufene oder nicht vertrauenswürdige Zertifikate enden als **Endgültig fehlgeschlagen**.
- FIT-Connect ist eine reine Versandstrecke. Die Umsetzung ist gegen einen Spezifikations-Mock geprüft; vor dem Produktivbetrieb in der FIT-Connect-Testumgebung testen.

Benutzerbereitstellung mit SCIM 2.0

Der Identitätsanbieter (z. B. Microsoft Entra ID, Keycloak, Okta) legt Fachkräfte-Konten an, ändert und deaktiviert sie.

Einrichten

1. Panel → **Schnittstellen** → **Benutzerbereitstellung (SCIM 2.0)**: **SCIM-Bereitstellung erlauben** einschalten und speichern.
2. **SCIM-Zugangstokens** → **Neues Token erzeugen** (Bezeichnung, erneute Anmeldebestätigung). Das Token (`ffscim_…`) wird **einmal** angezeigt.
3. Im Identitätsanbieter als SCIM-Basisadresse `https://<server>/scim/v2` und das Token als Bearer-Token („Secret Token“) eintragen.
4. Optional **Gruppen** → **Teams**: eine Zeile je Zuordnung, `Gruppenname = Teamname`.
5. **Rechte neuer SCIM-Konten** wählen: **Keine – Rechte vergibt die Verwaltung** (Standard, empfohlen) oder **Rolle „Fachkraft“**. Auf **Rolle „Fachkraft“** umstellen darf nur, wer **Benutzer verwalten** hat.

Verhalten

- Neue Konten sind aktive Fachkräfte **ohne Lizenzplatz**; `userName` muss eine E-Mail-Adresse sein. Ist SSO aktiv, entstehen sie als SSO-Konten. Die Rechte richten sich nach **Rechte neuer SCIM-Konten**: Bei **Keine** bleibt die App-Anmeldung gesperrt, bis die Administration unter **Benutzer** Rechte vergibt

(Markierung „App-Login gesperrt“); bei **Rolle „Fachkraft“** erhalten sie sofort die Rechte für Fälle, Termine, Aufgaben, Zeiten und eigene Textbausteine, aber keine Verwaltungsrechte. Den Lizenzplatz vergibt die Administration im Panel.

- Ablauf: SCIM legt das Konto an → die Fachkraft meldet sich per SSO an; beim ersten Mal verknüpft Focus Family die SSO-Identität über die vom Anbieter bestätigte E-Mail-Adresse mit dem Konto → die App-Anmeldung gelingt, sobald das Konto fachliche Rechte hat.
- `active=false`, `PATCH` mit `active` oder `DELETE` **deaktivieren** das Konto und beenden seine Sitzungen; gelöscht wird nichts.
- Über SCIM sichtbar und änderbar sind nur Fachkräfte-Konten, deren Rechte innerhalb der Rolle „Teamleitung“ (Rolle „Fachkraft“ plus Teamleitungs-Rechte) oder reiner App-Rechte liegen. Jedes andere Recht (z. B. System-, Datenschutz- oder Fach-Admin-Rechte, Benutzer oder Teams verwalten, Kataloge verwalten) macht das Konto für SCIM unsichtbar (`404`) und nimmt es aus der Zählung; Rechte sind über SCIM nie änderbar.
- Gruppen wirken nur über die Zuordnung: Mitglieder einer zugeordneten Gruppe werden Mitglied des Teams (Rolle Fachkraft). SCIM erfasst je Gruppe und Teammitgliedschaft eine eigene Vergabe; sind mehrere Gruppen demselben Team zugeordnet, zählen ihre Vergaben unabhängig, und eine Mitgliedschaft endet erst, wenn keine Gruppe sie mehr vergibt. Beim Hinzufügen und Reaktivieren gilt die Bereichsprüfung wie im Panel: Ein Team mit Bereich nimmt nur Mitarbeitende dieses Bereichs auf. Übersprungene Mitglieder protokolliert der Server als `integration.scim_change` mit `members_skipped=N` (Ergebnis „Denied“).
- Bestand eine Mitgliedschaft schon, bevor SCIM sie zum ersten Mal vergibt, merkt sich der Server ihre Herkunft: Eine manuell vergebene aktive Mitgliedschaft bleibt nach dem Entzug der letzten SCIM-Vergabe bestehen, eine zuvor inaktive ist nur aktiv, solange eine Gruppe sie vergibt, und wird danach wieder inaktiv. Von SCIM angelegte Mitgliedschaften werden gelöscht.
- `replace` auf `members` und `PUT` gleichen vollständig ab (eine leere Liste entzieht alle Vergaben der Gruppe), `remove` und `DELETE` der Gruppe entziehen nur ihre eigenen Vergaben. `GET` auf eine Gruppe listet alle Mitglieder, denen sie eine aktive Mitgliedschaft im aktuell zugeordneten Team vergibt, auch ursprünglich manuell vergebene. Andere Gruppen haben keine Wirkung.
- Gleichzeitige Änderungen an derselben Teammitgliedschaft laufen nacheinander (Zeilensperre in der Datenbank innerhalb der Transaktion). Entfernt der Identitätsanbieter eine Person zeitgleich über mehrere Gruppen desselben Teams, bleibt keine aktive Mitgliedschaft ohne vergebende Gruppe zurück.
- Wird eine Gruppe umbenannt (`PATCH` auf `displayName` oder `PUT`) oder wird die Zuordnung **Gruppen → Teams** geändert und gespeichert, gleicht der Server ab: Vergaben in einem Team, das nicht mehr passt, werden entzogen, und die Mitglieder erhalten eine Vergabe im neu zugeordneten Team (mit Bereichsprüfung). Ist die Gruppe keinem Team mehr zugeordnet, werden ihre Vergaben nur entzogen. Das Speichern im Panel protokolliert `integration.scim_change` mit `group_map_reconciled skipped=N`.
- Unterstützt: `/ServiceProviderConfig`, `/ResourceTypes`, `/Schemas`, `/Users` und `/Groups` mit GET, POST, PUT, PATCH, DELETE; Filter nur `eq` auf `userName`, `emails.value`, `externalId`, `id` (Gruppen: `displayName`, `id`); höchstens 200 Einträge je Seite. Nicht unterstützt: Bulk, Sortierung, ETags, Passwortänderung.
- Jede Änderung schreibt `integration.scim_change`. **Widerrufen** beendet die Bereitstellung über ein Token sofort.

Hinweise zu den Anbietern

- **Microsoft Entra ID:** Unternehmensanwendung → Bereitstellung → Automatisch; „Mandanten-URL“ = SCIM-Basisadresse, „Geheimes Token“ = SCIM-Token. Zuordnung `userPrincipalName` oder `mail` auf `userName`.
- **Keycloak:** SCIM-Erweiterung mit Ziel-URL und Bearer-Token; Gruppen-Synchronisation nur für die zugeordneten Gruppen nötig.
- **Okta:** App mit SCIM 2.0, Authentifizierung „HTTP Header“ mit dem Token; „Push Groups“ für die zugeordneten Gruppen.

Kalender-Abos (iCalendar)

Fachkräfte abonnieren ihre Termine im Dienstkalender (Outlook, Thunderbird, iOS).

- **Einschalten:** Panel → **Schnittstellen** → **Kalender-Abos (iCalendar)** → **Kalender-Abos erlauben**.
- **Detailgrad** für alle Abos: **Nur „Belegt“ (empfohlen)**, **Terminart und Fallalias** oder **Terminart, Fallalias und Ort**. Mehr als „Belegt“ kann nur ein Konto mit Datenschutzrecht einstellen, weil Abos auf Servern Dritter (z. B. Microsoft 365) gespeichert werden; die Auswahl liegt auf derselben Seite und setzt zusätzlich **Schnittstellen verwalten** voraus. Private Termine und Termine privater Fälle erscheinen immer nur als „Belegt“, Namen nie.
- **Abo-Adresse:** jede Person selbst im Panel unter **Kalender-Abo** → **Abo-Adresse erzeugen**. Die Adresse `https://<server>/feeds/calendar/<token>.ics` wird nur einmal angezeigt, gilt ein Jahr und ist persönlich und geheim. **Neue Adresse erzeugen** macht die bisherige ungültig, **Abo beenden** widerruft sie.
- **Inhalt:** eigene Termine von 30 Tagen zurück bis 180 Tage voraus, Zeitzone aus `Organization__TimeZone` (Standard `Europe/Berlin`); Kalender-Programme dürfen höchstens alle 5 Minuten abrufen (`Cache-Control: private, max-age=300`).
- Ungültige, abgelaufene oder widerrufene Adressen, abgeschaltete Abos, deaktivierte Konten und Organisationen ohne Lizenz beantwortet der Server mit `404`.

SIEM-Weiterleitung (Syslog)

Ereignisse der Audit-Kette gehen an ein SIEM oder Informationssicherheits-Monitoring. Übertragen werden nur Kennungen, keine Falldaten; eine Freigabe ist nicht nötig.

- **Adresse:** `tls://host:port` (empfohlen, RFC 5425, üblich Port 6514) oder `tcp://host:port` mit **Unverschlüsseltes TCP erlauben (nur internes Netz)**. Zertifikate, Pin und Client-Zertifikat wie bei den übrigen Verbindungen.
- **Nachrichtenformat:** RFC 5424 mit strukturierten Daten oder CEF. Rahmung nach Oktettzählung.
- **Ereignisfilter:** Präfixe der Audit-Aktionen, einer je Zeile (z. B. `user.`, `sso.`, `integration.`, `privacy.`); leer bedeutet alle.
- Die Weiterleitung beginnt mit dem Zeitpunkt der Aktivierung (kein Nachsenden älterer Ereignisse) und läuft in Blöcken bis 500 Ereignisse. Bei Fehlern wiederholt der Server ab derselben Stelle.
- **Zeitgrenze:** Verbindungsaufbau, TLS-Handshake, Schreiben und Spülen eines Blocks sind zusammen auf 30 Sekunden begrenzt. Ein Empfänger, der nicht antwortet, ergibt den Fehler „The syslog endpoint did not complete the TLS handshake or the transfer within 30 seconds.“; der Versuch zählt als

Fehlversuch (automatische Pause nach 10 in Folge), die Stelle in der Audit-Kette bleibt erhalten, und die übrigen Schnittstellen laufen weiter. **Verbindung prüfen** nutzt dieselbe Grenze.

Beispiel RFC 5424 (Facility authpriv, Schweregrad 6 bei Erfolg, 4 bei Ablehnung, 3 bei Fehler):

```
<86>1 2026-10-28T09:15:02.123Z ffhost focusfamily – integration.approved [ff@32473 seq="18231" action="integration.approved" result="Success" actor="…" targetType="Integration" targetId="…" correlation="…" hash="…"] integration.approved Success
```

CEF: `CEF:0|SoftwareNotion|FocusFamily|<Version>|<Aktion>|<Aktion>|<Schwere>|rt=… act=… outcome=… suid=… cs1Label=targetType cs1=… cs2Label=targetId cs2=… cs3Label=correlation cs3=… cn1Label=sequence cn1=…` ; CR und LF in Kopf- und Erweiterungsfeldern werden zu Leerzeichen.

Manuelle Übergabe aus der Fallansicht

Hat eine aktive, ausgehende CMIS- oder XÖV-Verbindung den Auslöser **Manuell aus der Fallansicht**, zeigt die Fallansicht Konten mit **Fälle bearbeiten** die Schaltfläche **An Zielsystem übergeben**. Nach Auswahl des **Zielsystems** und Bestätigung überträgt der Server die Akte mit den freigegebenen Dokumenten wie bei einem Fallabschluss (CMIS: Dokumente und Aktenverzeichnis; XÖV: xdomea-Abgabe). Es gelten die Datenschutz-Einstellungen der Verbindung. Die Übergabe erscheint im Übertragungsprotokoll und im Audit (`integration.manual_handover`).

Neue Verbindungen beginnen „ab jetzt“: Bestehende Dokumente und abgeschlossene Fälle überträgt der Server nicht nachträglich. Für Bestandsakten dient die manuelle Übergabe.

Konfiguration exportieren und importieren

Unter **Konfiguration übertragen** exportiert **Konfiguration exportieren** API-Clients und Verbindungen als JSON-Datei (`focusfamily-schnittstellen-<Datum>.json`), etwa für einen Test- oder Zweitserver.

- Nie exportiert werden Geheimnisse, Client-Secrets und Client-Zertifikate. Öffentliche Schlüssel von private_key_jwt-Clients, CA-Zertifikate und Pins sind enthalten; Bereiche stehen mit ihrem Namen in der Datei.
- **Konfiguration importieren** (Datei höchstens 2 MB, erneute Anmeldebestätigung) legt alles als **Entwurf** an. Freigaben werden nicht übernommen, API-Clients erhalten neue Client-IDs.
- Einträge mit einem schon vorhandenen Namen werden übersprungen. Bereiche werden über den Namen zugeordnet; nennt ein Eintrag Bereiche, die auf dem Zielserver fehlen oder nicht eindeutig sind, wird er nicht importiert, weil er sonst weiter reichen würde als im Export. Dann die Bereiche anlegen bzw. eindeutig benennen und erneut importieren. Einträge ohne Bereichseinschränkung werden organisationsweit übernommen. Weiter geöffnete Datenschutz-Einstellungen und den Scope `integration:sensitive` übernimmt der Import nur, wenn ein Konto mit Datenschutzrecht importiert; sonst gelten die Standardwerte, und der Scope entfällt mit einer Warnung. Eingangsgrenzen außerhalb der zulässigen Bereiche (max. Dateigröße 1 KB bis 2 GB, Einlieferungen pro Stunde 1 bis 100 000) verhindern den Import des Eintrags.
- Nach dem Import nennt das Panel alles, was zu prüfen ist: neue Client-Secrets, neu einzutragende Geheimnisse und Zertifikate, zurückgesetzte Datenschutz-Einstellungen.

Betrieb

Ablauf der Zustellung

Ein Hintergrunddienst folgt alle 5 Sekunden dem Änderungs-Feed des Servers, plant passende Ereignisse je aktiver Verbindung ein und stellt sie zu. Zugestellt wird nur an aktive, ausgehende Verbindungen lizenzierter Organisationen, deren ausgehende Übertragungen nicht pausiert sind; jeder Durchlauf wird gleichmäßig auf diese Verbindungen verteilt, sodass eine pausierte oder stark belegte Verbindung die anderen nicht aufhält. Bei mehreren App-Instanzen arbeitet immer nur eine (PostgreSQL-Sperre). Eingangsordner und eingehende Pakete fragt er im Abfrageintervall der Verbindung ab, SIEM-Ereignisse leitet er im selben Takt weiter.

Eine Organisation gilt als lizenziert, wenn sie gesponserte Seats hat oder gekaufte Seats mit einem Abo, das aktiv ist, sich in der Kulanzfrist befindet oder ein Zahlungsproblem hat. Ohne Lizenz ruhen Zustellungen und Abfragen; Token-Endpunkt, REST-API, CMIS-Repository, SCIM und Kalender-Abos antworten ablehnend (`integration.license_required` bzw. `403` oder `404`). Die SIEM-Weiterleitung läuft weiter. Nach der Lizenzprüfung geht es ohne Datenverlust weiter. Der Server speichert den Lizenzstatus fünf Minuten zwischen; eine Ablehnung durch den Lizenzserver (Abo nicht aktiv, Organisation ungültig) gilt als „nicht lizenziert“. Nur solange der Lizenzserver nicht erreichbar ist, gilt eine zuvor bestätigte Lizenz bis zu 24 Stunden weiter.

Übertragungsprotokoll und Wiederholungen

Panel → **Schnittstellen** → **Übertragungsprotokoll**, filterbar nach Verbindung und Status:

Status	Bedeutung
Wartend	eingeplant
Übertragen	zugestellt; die Objekt-ID im Zielsystem steht unter **Objekt**
Fehlgeschlagen, wird wiederholt	nächster Versuch nach 1 min, 5 min, 30 min, 2 h, 6 h, 24 h
Endgültig fehlgeschlagen	dauerhafter Fehler oder nach dem siebten Versuch
Übersprungen	nicht zuständig, etwa nicht abonnierter Ereignistyp oder Fall bzw. Dokument zum Zeitpunkt der Zustellung für die Verbindung nicht mehr sichtbar (`not_visible`, `case_not_visible`)
Vom Empfänger bestätigt	xdomea-Importbestätigung eingegangen

Erneut versuchen stellt eine Zustellung neu ein, **Alle fehlgeschlagenen erneut versuchen** bis zu 1000 auf einmal; der Versuchszähler beginnt dabei von vorn. Die Übersicht zeigt je Verbindung **Fehlversuche in Folge**, **Letzte Übertragung** und **Warteschlange**; der letzte Fehlertext steht in der Verbindung.

Pausieren und Not-Aus

- **Pausieren** hält eine Verbindung oder einen API-Client an, **Fortsetzen** setzt den Fehlerzähler zurück; wartende Übertragungen gehen im nächsten Durchlauf hinaus, Übertragungen mit geplanter Wiederholung behalten ihren Zeitpunkt, endgültig fehlgeschlagene gehen nur über **Erneut versuchen** wieder hinaus.
- **Automatische Pause:** Nach 10 Fehlversuchen in Folge (Zustellungen oder SIEM-Weiterleitung; Einstellung `Integrations__Dispatch__FailingThreshold`) wechselt eine aktive Verbindung auf **Pausiert** mit dem Grund `auto:consecutive_failures`, auditiert als `integration.paused`. Die Statuskarte der Verbindung erklärt das. Ursache beheben, **Verbindung prüfen**, dann **Fortsetzen**.
- **Alle ausgehenden Übertragungen pausieren (Not-Aus)** unter **Grundeinstellungen** hält jede ausgehende Zustellung und die SIEM-Weiterleitung an. Ereignisse bleiben im Änderungs-Feed und werden nach dem Fortsetzen nachgeholt. Die REST-API bleibt erreichbar.
- **Verbindung löschen** entfernt Warteschlange und Zustellprotokoll der Verbindung. Bereits übertragene Daten im Zielsystem bleiben dort. Das Offenlegungsverzeichnis für Auskünfte nach Art. 15 DSGVO bleibt erhalten.
- Eine pausierte Verbindung holt nach, solange der Änderungs-Feed die Ereignisse noch enthält (Sync-Aufbewahrung, siehe Technisches Handbuch). Nach längeren Pausen fehlende Akten manuell übergeben.

Monitoring-Kennzahlen

`/metrics` (siehe Technisches Handbuch, *Monitoring*) enthält:

Kennzahl	Bedeutung
`fokusfamilie_integration_clients_active`	aktive API-Clients
`fokusfamilie_integration_connections_active`	aktive Verbindungen
`fokusfamilie_integration_connections_paused`	pausierte Verbindungen
`fokusfamilie_integration_connections_pending_approval`	Verbindungen und API-Clients, die auf die Freigabe warten
`fokusfamilie_integration_outbox_pending`	wartende und zu wiederholende Übertragungen
`fokusfamilie_integration_outbox_retrying`	Übertragungen, die mindestens einmal fehlschlugen
`fokusfamilie_integration_outbox_dead_lettered`	endgültig fehlgeschlagene Übertragungen – sollte 0 sein
`fokusfamilie_integration_outbox_oldest_pending_age_seconds`	Alter der ältesten offenen Übertragung
`fokusfamilie_integration_deliveries_24h`	Übertragungen der letzten 24 Stunden
`fokusfamilie_integration_inbox_pending_review`	Eingänge, die auf fachliche Prüfung warten

Sinnvolle Alarme: `outbox_dead_lettered > 0`, `outbox_oldest_pending_age_seconds > 86400`, `connections_pending_approval > 0` über mehrere Tage, `inbox_pending_review` dauerhaft steigend.

Audit-Ereignisse

Ereignis	Anlass
`integration.client_created`, `integration.client_changed`, `integration.client_secret_rotated`, `integration.client_revoked`	API-Clients
`integration.connection_created`, `integration.connection_changed`, `integration.connection_deleted`, `integration.connection_tested`	Verbindungen
`integration.submitted`, `integration.approved`, `integration.rejected`, `integration.paused`, `integration.resumed`	Freigabe und Betrieb
`integration.settings_changed`	Grundeinstellungen, Freigabe-Richtlinie
`integration.delivered`, `integration.delivery_failed`, `integration.delivery_retried`	Zustellungen
`integration.api_access`, `integration.api_denied`, `integration.token_issued`, `integration.token_revoked`	Zugriffe und Tokens
`integration.inbound_received`, `integration.inbound_accepted`, `integration.inbound_rejected`	eingehende Richtung
`integration.scim_change`, `integration.manual_handover`, `integration.config_exported`, `integration.config_imported`	SCIM, Übergabe, Konfiguration

Konfigurationsparameter

Die Standardwerte passen für die meisten Installationen. Abweichungen gehören in eine `docker-compose.override.yml` unter `services.app.environment`.

Einstellung	Standard	Bedeutung
`Integrations__Dispatch__Enabled`	`true`	Hintergrunddienst an oder aus
`Integrations__Dispatch__IntervalSeconds`	`5`	Takt des Hintergrunddienstes
`Integrations__Dispatch__ScanBatch`	`500`	Änderungen je Verbindung und Durchlauf
`Integrations__Dispatch__DeliveryBatch`	`25`	Zustellungen je Durchlauf
`Integrations__Dispatch__FailingThreshold`	`10`	Fehlversuche in Folge bis zur automatischen Pause
`Integrations__Network__TimeoutSeconds`	`30`	Zeitlimit je Anfrage
`Integrations__Network__UploadTimeoutSeconds`	`600`	Zeitlimit je CMIS-Upload
`Integrations__Network__MaxResponseBytes`	`52428800`	größte Antwort (50 MB)
`Integrations__Network__AllowLoopback`	`false`	Loopback-Ziele erlauben (nur Testumgebungen)
`Integrations__Network__AllowLinkLocal`	`false`	Link-Local-Ziele erlauben (nur Testumgebungen)
`Integrations__Xoev__FolderRoot`	`/var/lib/fokusfamilie/xoev`	XÖV-Stammverzeichnis
`Integrations__Xoev__MaxIncomingBytes`	`209715200`	größtes eingehendes Paket (200 MB)
`Integrations__Xoev__SftpOperationTimeoutSeconds`	`60`	Zeitlimit je SFTP-Vorgang (Verbindungsaufbau, Auflisten, Umbenennen, Löschen, Verschieben, Verbindungstest)
`Integrations__Xoev__SftpTransferTimeoutSeconds`	`600`	Zeitlimit je SFTP-Upload bzw. -Download eines Pakets
`Integrations__Xoev__FitConnectTrustedRootsPem`, `Integrations__Xoev__FitConnectTrustedRootsFile`	leer	zusätzliche Wurzelzertifikate für die Schlüsselprüfung bei FIT-Connect (z. B. Testumgebung)
`Integrations__Xoev__FitConnectRevocationMode`	`Online`	Sperrprüfung des FIT-Connect-Schlüssels
`RateLimiting__AuthPermitLimit`	`100`	fehlgeschlagene Basic-Anmeldungen je IP-Adresse und Minute am CMIS-Repository
`Organization__TimeZone`	`Europe/Berlin`	Zeitzone der Kalender-Abos

Fehlerbehebung

Symptom	Ursache	Abhilfe
Token-Abruf `unauthorized_client`, `integration.client_inactive`	Client nicht aktiv (Entwurf, wartet, pausiert, widerrufen)	einreichen, freigeben lassen bzw. fortsetzen
`integration.ip_denied`	Absender-IP nicht in der Liste oder Liste leer	IP-Liste ergänzen; hinter einem Proxy `ReverseProxy` prüfen
`integration.scope_missing`	Scope nicht zugewiesen oder beim Token-Abruf nicht angefordert	Scope ergänzen (löst Freigabe aus) oder ohne `scope` abrufen
Verbindung bleibt „Wartet auf Freigabe“	Datenschutzrolle hat noch nicht entschieden	Freigabe durch eine andere Person mit Datenschutzrecht
„Die Freigabe muss eine andere Person erteilen …“	Vier-Augen-Prinzip: Die eigene Person hat die Schnittstelle angelegt oder zuletzt geändert	Person mit Datenschutzrecht, die weder angelegt noch zuletzt geändert hat
„Die Konfiguration wurde seit dem Öffnen geändert. Bitte den aktuellen Stand neu laden und erneut prüfen.“	Die Schnittstelle wurde nach dem Öffnen der Seite geändert (oder die Anfrage enthielt keine Revision); die Freigabe gilt nur für den geprüften Stand	Seite neu laden, aktuellen Stand prüfen und erneut entscheiden
Import: „: not imported, area(s) … not found or ambiguous …“	Bereiche des Eintrags fehlen auf dem Zielserver oder sind nicht eindeutig	Bereiche anlegen bzw. eindeutig benennen, dann erneut importieren
„Freigaben sind nur mit einem lokalen Konto möglich …“	Anmeldung per SSO	mit lokalem Konto freigeben
Verbindungsprüfung: Adresse nicht erlaubt	Ziel löst auf Loopback, Link-Local oder Metadatenadresse auf	richtige Adresse eintragen; DNS prüfen
TLS-Fehler	interne Zertifizierungsstelle unbekannt, Pin passt nicht, falscher Hostname	CA unter TLS eintragen oder in `deploy/docker/ca/` ablegen; Pin neu ermitteln
Webhook „Endgültig fehlgeschlagen“ mit HTTP 401/403	Empfänger lehnt Anmeldung oder Signatur ab	Signatur-Secret beim Empfänger prüfen, ggf. neu erzeugen; dann **Erneut versuchen**
„redirects are not followed“	Empfänger antwortet mit Weiterleitung	Zieladresse direkt eintragen
CMIS: Dokumenttyp oder Eigenschaft fehlt	Typ oder Aspekt im DMS nicht angelegt	Typ anlegen oder Zuordnung anpassen; Verbindungsprüfung zeigt die Namen
xdomea validation …	Paket verstößt gegen das Schema (z. B. fehlende Pflichtangaben)	Absender und Empfänger, Aufbewahrung und Aktenzeichen prüfen; Fehlertext nennt Zeile und Element
SFTP „Host key mismatch“	Hostschlüssel geändert oder falsch eingetragen	Fingerprint neu ermitteln und mit dem Betreiber abgleichen
XÖV-Verzeichnis nicht beschreibbar	Stammverzeichnis nicht eingebunden oder falscher Besitzer	Bind-Mount einrichten, `chown 1654:1654`
SCIM `401`	Token falsch, abgelaufen oder widerrufen	neues Token erzeugen
SCIM `403`	SCIM-Bereitstellung nicht erlaubt oder keine Lizenz	**SCIM-Bereitstellung erlauben**
SCIM `404` für eine bekannte Person	Konto hat Rechte außerhalb der Rolle „Teamleitung“ und der reinen App-Rechte	Konto im Panel pflegen
Kalender-Abo `404`	Abo beendet, abgelaufen, Abos abgeschaltet, Konto deaktiviert oder keine Lizenz	neue Abo-Adresse erzeugen; Lizenz prüfen
SIEM erhält nichts	Filter zu eng, Not-Aus aktiv, TLS-Fehler	Filter leeren, **Verbindung prüfen**
Verbindung plötzlich **Pausiert** mit Grund `auto:consecutive_failures`	Zielsystem zehnmal in Folge nicht erreichbar oder abweisend	Fehlertext der Verbindung lesen, Ursache beheben, **Fortsetzen**
Ausweitung der Datenschutz-Einstellungen wird nicht gespeichert	Freigabepflicht abgeschaltet, Konto ohne Datenschutzrecht	Änderung durch die Datenschutzrolle vornehmen lassen

Fehlercodes der REST-API

Code	HTTP	Bedeutung
`integration.scope_missing`	403	Scope der Ressource fehlt
`integration.area_denied`	–	reserviert; Objekte außerhalb der Bereiche beantwortet der Server mit `integration.not_found`
`integration.ip_denied`	403	Absender-IP nicht erlaubt
`integration.client_inactive`	403	Client nicht aktiv
`integration.client_expired`	403	Gültigkeit abgelaufen (auch am CMIS-Repository)
`integration.license_required`	403	keine aktive Organisationslizenz
`integration.not_found`	404	Objekt unbekannt oder nicht sichtbar
`integration.cursor_invalid`	400	Cursor beschädigt
`integration.cursor_expired`	410	Änderungs-Feed hat den Stand nicht mehr
`integration.rate_limited`	429	Ratenbegrenzung
`integration.inbound_disabled`	403	eingehende Richtung für diese Art aus
`integration.field_group_denied`	403	Feldgruppe nicht freigegeben
`integration.payload_invalid`	400/422	Anfrage ungültig
`integration.file_too_large`	413	Datei über der Grenze
`integration.mime_type_denied`	415	Dateityp nicht erlaubt oder Inhalt passt nicht zum Typ
`integration.malware_detected`	422	Schadsoftware-Prüfung schlug an
`integration.precondition_required`	428	`If-Match` fehlt
`integration.precondition_failed`	412	Revision veraltet
`integration.idempotency_key_required`	428	`Idempotency-Key` fehlt
`integration.idempotency_conflict`	409	Schlüssel mit anderem Inhalt wiederverwendet
`integration.inbound_conflict`	–	Feldkonflikt; der Eingang wartet im Status **Konflikt** im Posteingang
`integration.inbound_quota_exceeded`	429	Einlieferungen pro Stunde oder Speicherkontingent erschöpft
`integration.withdraw_denied`	403	Einlieferung bereits bearbeitet
`integration.case_not_writable`	–	Fall inzwischen gelöscht, eingeschränkt oder privat; steht als Grund am Eingang

Glossar

Begriff	Erklärung
API-Client	Drittsystem mit eigenen Zugangsdaten für REST-API und CMIS-Repository
Änderungs-Feed	fortlaufend nummerierte Liste aller Änderungen auf dem Server; Grundlage von Sync und Schnittstellen
CloudEvents	Standard der CNCF für Ereignisnachrichten
CMIS	Content Management Interoperability Services (OASIS), Standard für den Zugriff auf Dokumentenmanagement
DVDV	Deutsches Verwaltungsdiensteverzeichnis, liefert Kennungen und Dienste für XTA
Fremdreferenz	Kennung eines Drittsystems, die am Fall oder Dokument hinterlegt ist
FIT-Connect	Übermittlungsinfrastruktur der FITKO für Anträge und Nachrichten an Verwaltungen
Idempotenz	Wiederholung derselben Anfrage wirkt nur einmal
mTLS	TLS mit Client-Zertifikat
Posteingang	Seite **Eingänge (Schnittstellen)** zur fachlichen Prüfung eingehender Inhalte
private_key_jwt	Anmeldung eines Clients mit signiertem JWT statt Secret (RFC 7523)
Pseudonymisierung	Ersetzen von Namen durch Alias, Kennung oder `[pseudonymisiert]`
SCIM	System for Cross-domain Identity Management (RFC 7643/7644)
Scope	Berechtigung eines API-Clients
SPKI-Pin	SHA-256 des öffentlichen Schlüssels eines Serverzertifikats
SSRF	Server-Side Request Forgery: Missbrauch des Servers, um interne Adressen anzusprechen
Standard Webhooks	offene Spezifikation für die Signatur von Webhooks
xdomea	XÖV-Standard für den Austausch und die Aussonderung von Schriftgut
XÖV	XML in der öffentlichen Verwaltung, Rahmenwerk der KoSIT
XTA 2	XÖV-Transportadapter, Webservice-Schnittstelle zu OSCI-Intermediären

Checkliste Inbetriebnahme

1. Konten festlegen: technische Administration mit **Schnittstellen verwalten**, mindestens eine **andere** Person mit Datenschutzrecht und lokalem Konto.
2. Ausgehende Firewall-Freigaben für die Zielsysteme; interne CAs in `deploy/docker/ca/` oder je Verbindung.
3. Für XÖV über Verzeichnis: Bind-Mount für `/var/lib/fokusfamilie/xoev` einrichten.
4. Verbindung bzw. API-Client anlegen, Zweck und Rechtsgrundlage eintragen, Datenschutz-Einstellungen minimal halten.
5. **Verbindung prüfen**, bis alle Schritte grün sind.
6. Einreichen und freigeben lassen.
7. Ersten Echtfall manuell übergeben bzw. erste API-Abfrage im Audit nachvollziehen.
8. Monitoring-Alarme für `fokusfamilie_integration_*` einrichten.
9. Konfiguration exportieren und mit der Betriebsdokumentation ablegen.

Focus Family · Schnittstellenhandbuch · Version 1.3.0 · Stand Oktober 2026