FOCUS FAMILY

Admin Panel Handbook

Administration, management and data protection – explained step by step

Version 1.3.0 · November 2026 · Software Notion

Contents

1. **Welcome**
    1. What the panel is for
    2. What the panel deliberately is not
2. **Signing in and basics**
    1. Searching and filtering
3. **Roles and permissions**
    1. The two levels
    2. Individual permissions
    3. Management scope
4. **Managing users**
    1. Creating a user
    2. Granting permissions
    3. Accounts without permissions
    4. Editing, deactivating, changing passwords
    5. Setup by QR code
    6. Setting up two-factor sign-in (MFA)
    7. Passkey sign-in (passwordless)
    8. Sign-in through the organization (SSO)
5. **Teams and case assignment**
6. **Areas (area-based administration)**
    1. Basic rules
    2. Setting up
    3. Organisation pages in area mode
    4. Switching off
    5. Activity
7. **Cases**
    1. Creating and assigning a case
    2. Participants and addresses
    3. Roadmap, goals and review points
    4. Cover arrangements
    5. Transferring a case
    6. Appointments, tasks and media in a case
    7. Case history
8. **Interfaces: incoming items and handover**
    1. Reviewing incoming items
    2. Origin of delivered documents
    3. Handing over to a target system

    4. Calendar subscription

9. **Planning**
10. **Time tracking**
11. **Activity records**
    1. Closing and reopening
    2. Identification and record archive
12. **Devices**
    1. Licence seats
13. **Policies**
14. **Help & contact**
15. **Managed settings**
    1. Billing basis
16. **Invoice issuer**
17. **Templates and export profiles**
18. **Text snippets**
19. **Catalogues: institutions, measures, activity types**
    1. Institutions
    2. Measure catalogue
    3. Activity types
20. **Calendars & commitments in the case**
21. **Contact cards and cover arrangements**
    1. Who may do what?
    2. Provider contact details
    3. Practitioner contact cards
    4. Cover arrangements
22. **Deletion requests**
23. **Data protection: subject requests and documents**
    1. Setting it up
    2. Before the first request: create the documents
    3. Handling a request
24. **Security audit**
25. **Crash reports and desktop downloads**
26. **Data protection and the limits of the panel**
27. **Frequently asked questions**

Welcome

The **admin panel** is the web administration of your organisation's Focus Family server. You reach it in a browser at your server address followed by `/admin`.

This handbook is written for **administration, management and data protection officers**. It requires no technical knowledge. Setting up and operating the server itself is covered in the **technical handbook**.

What the panel is for

You manage the organisational side of your work here:

- practitioners, their access and permissions,
- teams and case assignment,
- shared planning (appointments and tasks),
- time tracking and activity records,
- devices, policies and central settings,
- templates, text snippets and catalogues,
- deletion requests and data protection cases.

What the panel deliberately is not

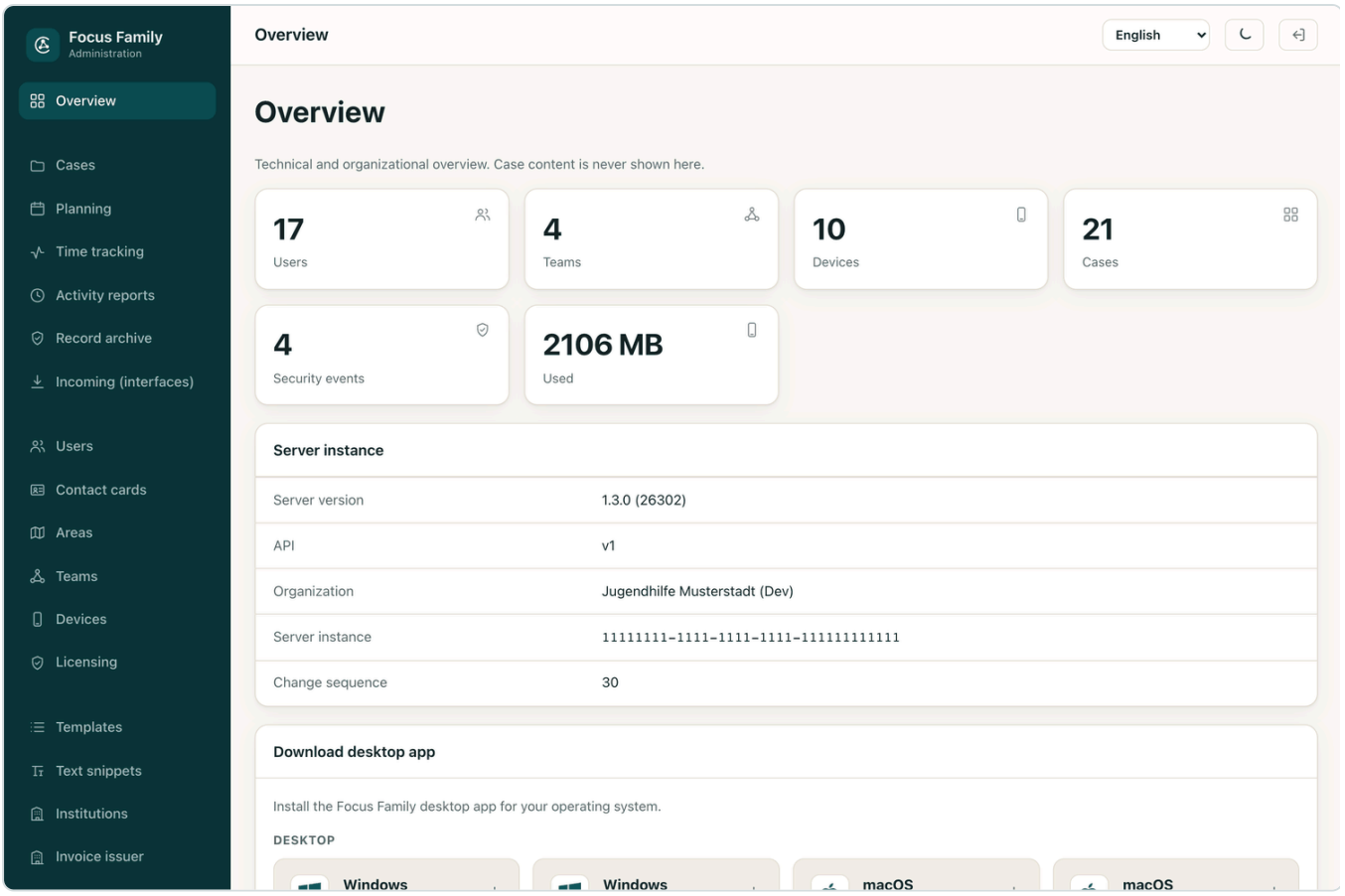
- It is **not a second case documentation**. The professional work – notes, assessments, progress – happens in the practitioners' app.
- Administrators do **not** see private content. Entries marked "private" stay hidden.
- **Technical administration** sees **no** cases and no appointments.

Signing in and basics

1. Open your server address with `/admin` in a browser.
2. Enter **e-mail** and **password** and click **Sign in**.
3. If two-factor sign-in (MFA) is active for your account or required by policy, the panel also asks for the **6-digit code** from your authenticator app.
4. If your account uses **passkey sign-in**, you confirm with fingerprint, face or a security key instead.
5. If your account still uses an **initial password** – for example the admin accounts created during installation, or after an admin set your password with a required change – **Change password** opens first. Enter the current password and the new one twice; no other page is reachable before that. When you sign in from the app, it continues the sign-in in the browser for this step.

At the top right you switch the **language** (Deutsch, English, Español, Français), toggle between **light and dark** appearance and sign out.

> **Important: Technical admin accounts cannot sign in to the apps.** Everyone who uses the app needs a **practitioner account**.



The overview shows key figures, details about the server instance and the desktop app downloads. The navigation on the left only lists what your permissions allow.

Searching and filtering

Every longer list has the same **filter bar** above its entries: a search field on the left and the matching selection fields next to it. Selections apply immediately; confirm search terms with **Filter** or the Enter key. **Reset filters** shows everything again. If nothing matches, the list says **No matches.** The filters are part of the address bar, so you can bookmark or share a filtered view. Filtering only ever works within what you are allowed to see anyway.

Page	Search	Filters
Cases	name, file number, tags, office, youth welfare officer	status, type of support, practitioner (owner or assigned), team
Planning	title, location, case, practitioner	practitioner, case; for appointments type, status, date range; for tasks status, priority, due (overdue, today, next 7 days, no date), date range
Time tracking	note, activity, case, practitioner	practitioner, case, type, billing status, date range
Users	name, email	status, account type
Devices	device name, person, version, IP	approval, platform
Audit	action, target, correlation	action, person, result, date range
Contact cards	name, role, phone, email	–
Crash reports	error type, context	device, version, platform

Text snippets, institutions, the measure catalogue, activity types, activity records and the data protection log have their own filters in the same bar.

Roles and permissions

Focus Family splits administration into two areas. IT can look after the technology without seeing case content – and professional management can administer the content side without touching server technology.

The two levels

Level	May	Sees
System admin (technical)	use and grant all technical permissions	no cases, no appointments
Professional admin	use and grant all professional permissions	case content, except private entries

Anyone holding both levels can grant everything.

Individual permissions

In addition, **individual permissions** can be granted. Two rules always apply:

- **"Edit" includes "view".**
- You can only grant permissions **from your own area**. The **general permissions** may be granted by professional and system admins.
- **Permission ceiling:** accounts holding permissions outside your own grant scope cannot be edited or deactivated, and their password, MFA, passkeys, setup QR code or sign-in method cannot be

changed. The panel then reports "This account holds permissions outside your own grant scope and cannot be changed here." Technical accounts can only be changed with *Manage technical admins*.

Professional permissions

Permission	Meaning
View / edit cases	see cases, or create and change them
View / edit calendar	see or manage appointments
View / edit tasks	see or manage tasks
View / record time	see time entries, or create and change your own
Manage records	edit time entries and records of **other** practitioners within your own management scope (includes "view time")
Close records	close past months/years and reopen them with a reason (includes "manage records")
View / edit managed settings	maintain central values that are locked in the app
Manage practitioners	create and maintain user accounts
Manage teams	maintain teams and members
Assign to others	assign cases to other people, create cover arrangements
Emergency access (break-glass)	time-limited exceptional access to a case
Manage templates & export profiles	maintain central DOCX templates and export profiles
View / create / manage text snippets	maintain central text snippets
See amounts	see monetary amounts in invoice drafts
Review deletion requests	decide about deleted data
Review and accept interface inbox items	use the page **Incoming (interfaces)**: review and reject items, and with **Edit cases** in addition assign them to cases and accept them (includes "View cases"; included in the professional admin)
Show setup QR	create a setup QR code for practitioners
Manage areas	switch area mode on and off, maintain areas, assign practitioners and teams, grant administrative scope (only with organisation-wide scope; included in professional admin)
Manage invoicing details	maintain the central invoice issuer for e-invoices (page *Invoice issuer*; included in professional admin)
Create e-invoices	app-only permission: create e-invoices in the app and receive the central invoicing details for it (grants no panel access; included in professional admin)

Technical permissions

Permission	Meaning
System configuration	basic technical settings
View / edit policies	maintain organisation policies
View / manage devices	see device connections, approve or block them
Manage technical admins	maintain IT administration – also governs **removing MFA and passkeys**
View security audit	inspect the security log
View system status	see technical load
Configure monitoring	switch the monitoring interface on, create the access key and restrict it to address ranges
View crash reports	see technical error reports from the apps
Manage crash reports	delete single or all crash reports (includes viewing)
Download desktop app	download installer packages in the panel
Manage single sign-on	set up, test and enforce sign-in through the organization's identity provider (included in system admin)
Manage interfaces (REST clients, CMIS, XÖV, webhooks, SCIM, SIEM)	set up connections to case management systems, document management, XÖV recipients, webhooks, SCIM, calendar subscriptions and SIEM (included in system admin; data flows with case data are approved by the data protection role)

> Removing two-factor sign-in or a passkey requires the permission **Manage technical admins**.

General permissions

Permission	Meaning
Manage licensing (assign)	assign seats to practitioners and revoke them, remove and reinstate licence devices
Purchase licensing	manage seats and subscription – buy more or fewer seats, change the billing interval, cancel (includes "manage")

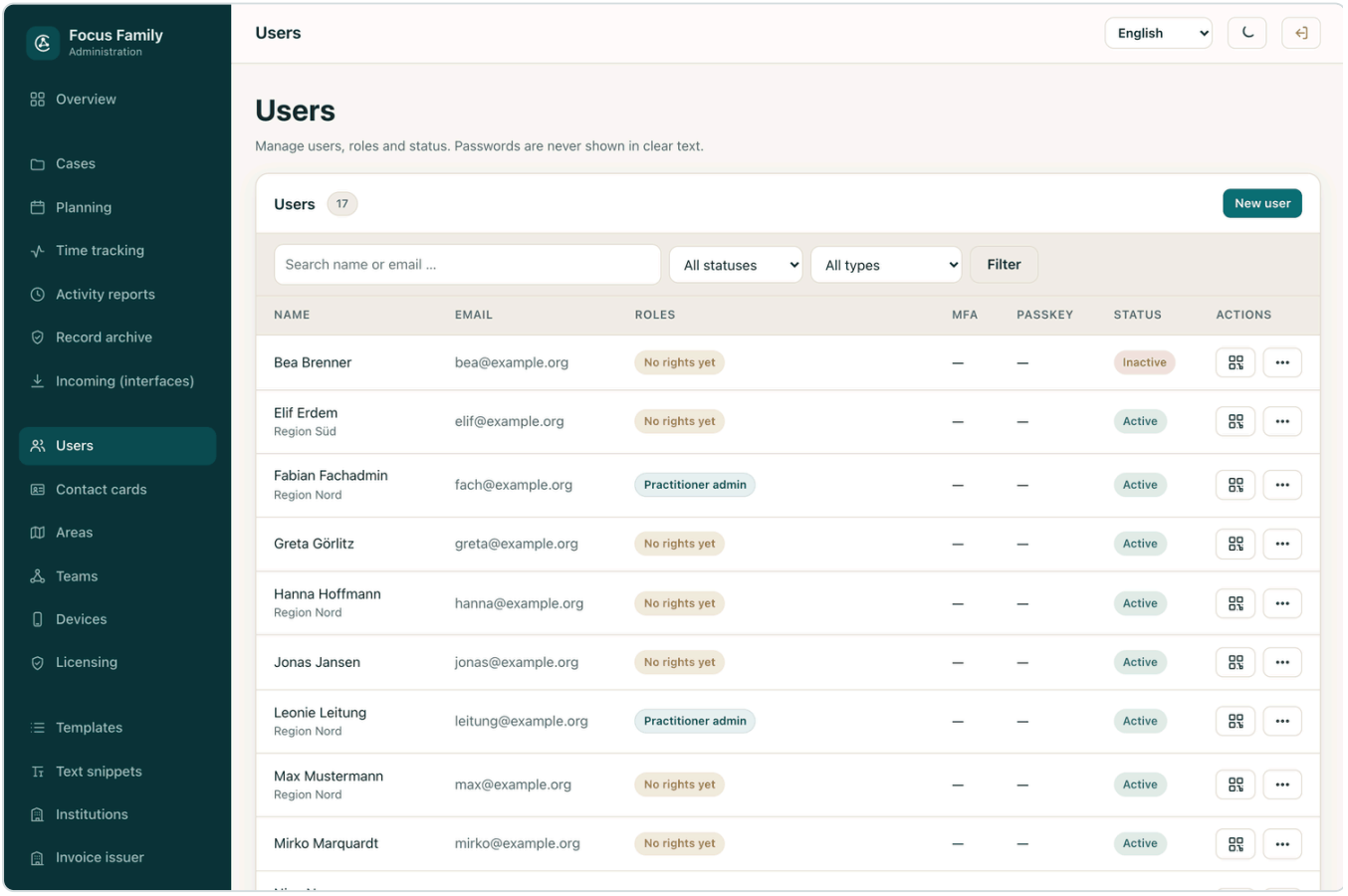
The professional and technical admins created during installation receive both licensing permissions. Ticking **Operations admin** or **System admin** in the permission dialog preselects them; they can be unticked if needed.

Management scope

The two record permissions only apply inside a person's **management scope**: the teams where they are listed as **team lead**, with those members and assigned cases. A **professional admin** automatically has the whole organisation as their scope; with area mode on, area-bound accounts are limited to their areas (see “Areas”). Reading stays organisation-wide for everyone with "view time".

Managing users

Menu item **Users** (permission *Manage practitioners*). Passwords are never shown in clear text.



The user list with name and areas, e-mail, roles, status and passkey state. The menu on the right holds every action for a person.

Creating a user

1. Click **New user**.
2. Enter **display name**, **e-mail** and a **password**. The password needs at least 12 characters with upper and lower case, a digit and a special character; **Generate password** fills both fields.
3. Optionally tick **Require a password change at the next sign-in** (off by default) – the person then replaces the password with their own at the first sign-in.
4. Set the **permissions** (see below). Whether the person may sign in to the app follows from the permissions: without professional permissions the account is administration only.
5. Click **Create**.

Granting permissions

1. Open the user and go to the **permissions** area.
2. Permissions are grouped into **professional**, **system / technical** and **data protection**. You only see the groups and permissions you are allowed to grant; a technical admin, for example, sees no professional permissions.
3. **Presets** tick several boxes at once: **Practitioner** and **Team lead** only appear if you may grant all permissions they contain; **Read only** covers the read permissions within your scope. **Reset** restores

the state when the dialog was opened – the current permissions of an existing account, none for a new account.

4. Tick the boxes and click **Save**.

Accounts without permissions

Accounts without any permission – typically after the first SSO sign-in with automatic account creation – carry the **No rights yet** badge in the user list. In the **Account type** selection, **Without rights** shows only these accounts.

As long as an account has no administration permissions (this includes practitioners with app-only permissions such as *read text snippets*), the person sees a **welcome page** after signing in: sign-in successful, no administration rights yet, own contact details can be maintained here. The menu only contains **Home**, **My contact details** and **Help & contact**, with language and sign-out at the top; local accounts also find **Account security** (MFA, passkey) on the welcome page. The server rejects every other page and action and shows **Access denied** with the link **Back to the start page**. MFA requirements and password changes apply as before. As soon as you grant permissions, the matching menu items appear on the next page load.

Editing, deactivating, changing passwords

- **Edit** – adjust display name and settings.
- **Activate / deactivate** – a deactivated account can no longer sign in. Access ends immediately: panel sessions and app sign-ins are revoked, and sync rejects the person's devices from their next contact. You cannot deactivate your own account.
- **Change password** – enter the new password twice. **Require a password change at the next sign-in** is preselected for other accounts; the person then chooses their own password at the next sign-in. Without the tick, the password you set stays valid. Existing panel sessions of that person end within a minute. For your **own** account the option is not ticked and you stay signed in; if you tick it, the panel signs you out and requires the change at your next sign-in.

Setup by QR code

So a new practitioner does not have to type the server address and credentials (permission *Show setup QR*):

1. Open the user and choose **Show setup QR**.
2. The QR code is **time-limited** and can be used **only once**. Issuing it replaces the current password with a one-time password in a single step.
3. The practitioner scans the code in the app under **Connect server**.
4. The app configures the connection and sign-in automatically; afterwards the person sets their own password.

> **Security note:** the setup QR is sensitive. Show it only to the right person, never send it over insecure channels and do not leave it lying around. It expires by itself after a short time.

Setting up two-factor sign-in (MFA)

The Focus Family app and the authenticator app usually run on the **same phone** – and a device cannot photograph its own screen. That is why you show the setup code in the panel on a second screen.

1. Open **Users** and choose **Set up MFA**.
2. A **QR code** and a **key** for manual entry appear.
3. The practitioner scans the code with their authenticator app (for example Google or Microsoft Authenticator).
4. Enter the displayed **6-digit code** in the **code** field and click **Confirm & activate**.

Whether MFA is **mandatory** is decided centrally under **Policies**. The requirement applies to apps **and** the admin panel.

Passkey sign-in (passwordless)

Alternatively an account can be switched to **passkeys** – sign-in with fingerprint, face recognition or a security key.

1. In the person's menu choose **Enable passkey sign-in**. The **passkey** column then shows **pending**.
2. At the next sign-in the person is guided to the **set up passkey** page. Afterwards the column shows **active**.
3. Once a passkey exists, **the password no longer works for that account**.
4. **Show passkeys** lists every registered passkey. Adding another one (for a second device, say) requires confirmation with an existing passkey.
5. While a passkey is active, **set password** and **set up MFA** are greyed out – they only take effect after a passkey reset.

> **Resetting passkeys** and removing individual passkeys – like removing MFA – require the permission **Manage technical admins**, for example after a lost device. Both immediately end the person's sessions; set a new password right afterwards.

Sign-in through the organization (SSO)

When single sign-on is set up (see the technical handbook), the sign-in page also shows the button **Sign in with …** (with the identity provider's name). Accounts that sign in this way carry the **SSO** badge in the user list; the MFA and passkey columns read **at identity provider**.

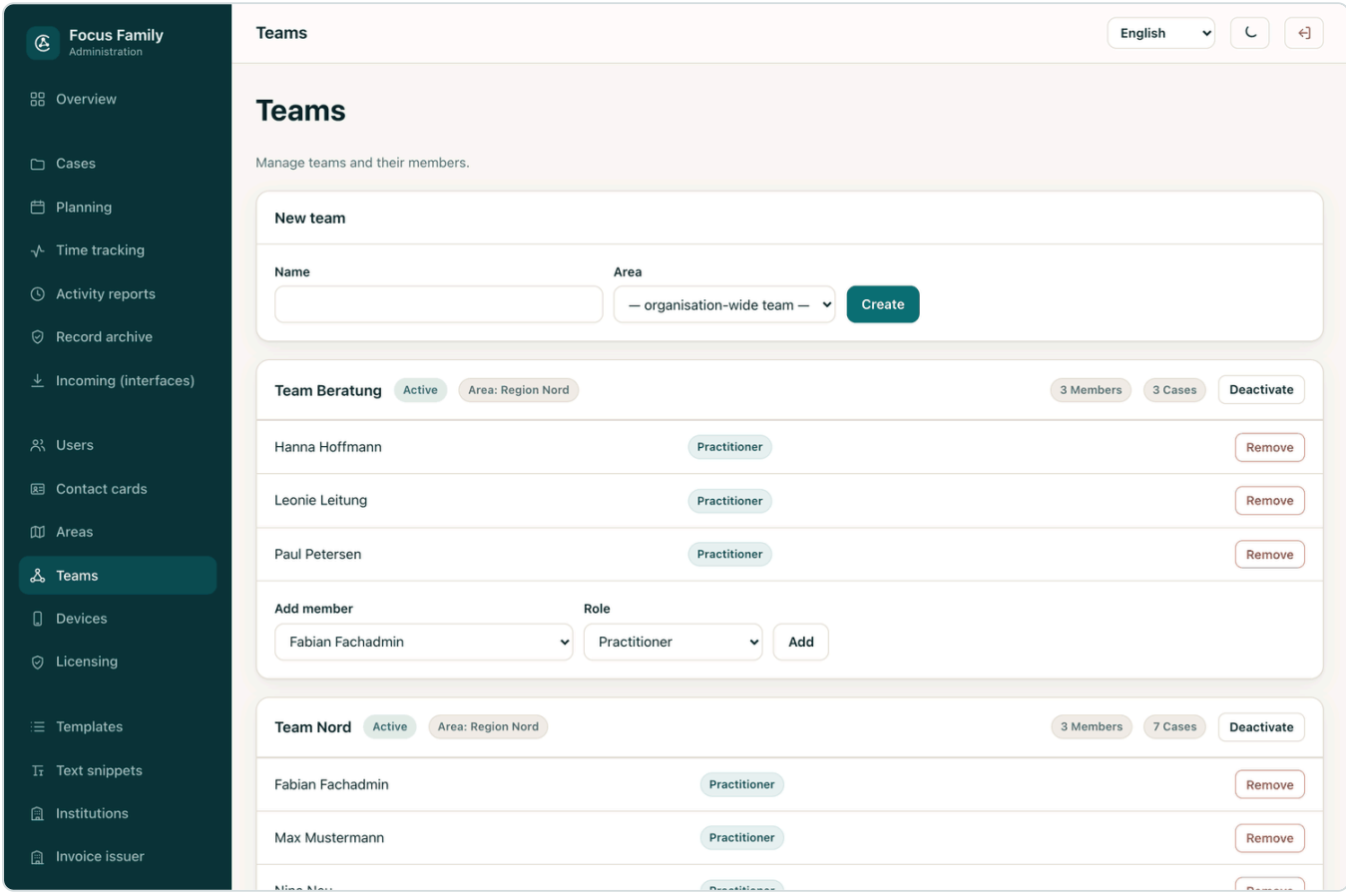
1. **New SSO account** creates an account without a password (name, email or UPN, permissions, area). You can assign permissions and a license seat right away. Until the first sign-in the badge reads **pending**; the account is then linked through the email address verified by the identity provider. If the provider does not verify the address, an administrator with the "Manage single sign-on" and user management permissions allows the first sign-in for 24 hours under **Single sign-on → Allow first sign-in**.
2. Switch existing accounts in the person's menu under **Sign-in method → Switch to SSO**. Password, MFA, passkeys and open QR codes are removed and all sessions end; permissions and seat are kept.

3. SSO accounts have no **Set password**, no **Set up MFA**, no passkeys and no setup QR code – the identity provider manages these.
4. **Remove link** helps after changing the identity provider; **Switch to local sign-in** turns the account back into a password account (then set a password).
5. With automatic account creation enabled, new people appear after their first sign-in without permissions and without a seat (badge **No rights yet**, filter **Without rights**). Until then they only reach the welcome page and **My contact details** in the panel (see *Accounts without permissions*). Assign permissions and a seat before they use the app.
6. When **Enforce SSO** is switched on, all local sessions and app sign-ins end at that moment. The app and the desktop then only offer **Sign in with organization account**; addresses from the SSO domains are always routed to the identity provider.

> You cannot switch your own sign-in method. At least one local system admin account with a password always remains (emergency access). Even with enforced SSO it signs in with its password – in the admin panel only, not in the apps.

Teams and case assignment

Menu item **Teams** (permission *Manage teams*). Teams bundle practitioners so cases can be assigned to several people at once.



Teams with their members. The role "team lead" also defines the management scope for the record permissions.

1. Create a **new team** and give it a name.
2. Use **Add member** to include practitioners and **Remove** to take them out.
3. The role **team lead** reaches beyond team administration: it defines the **management scope** for "manage records" and "close records".

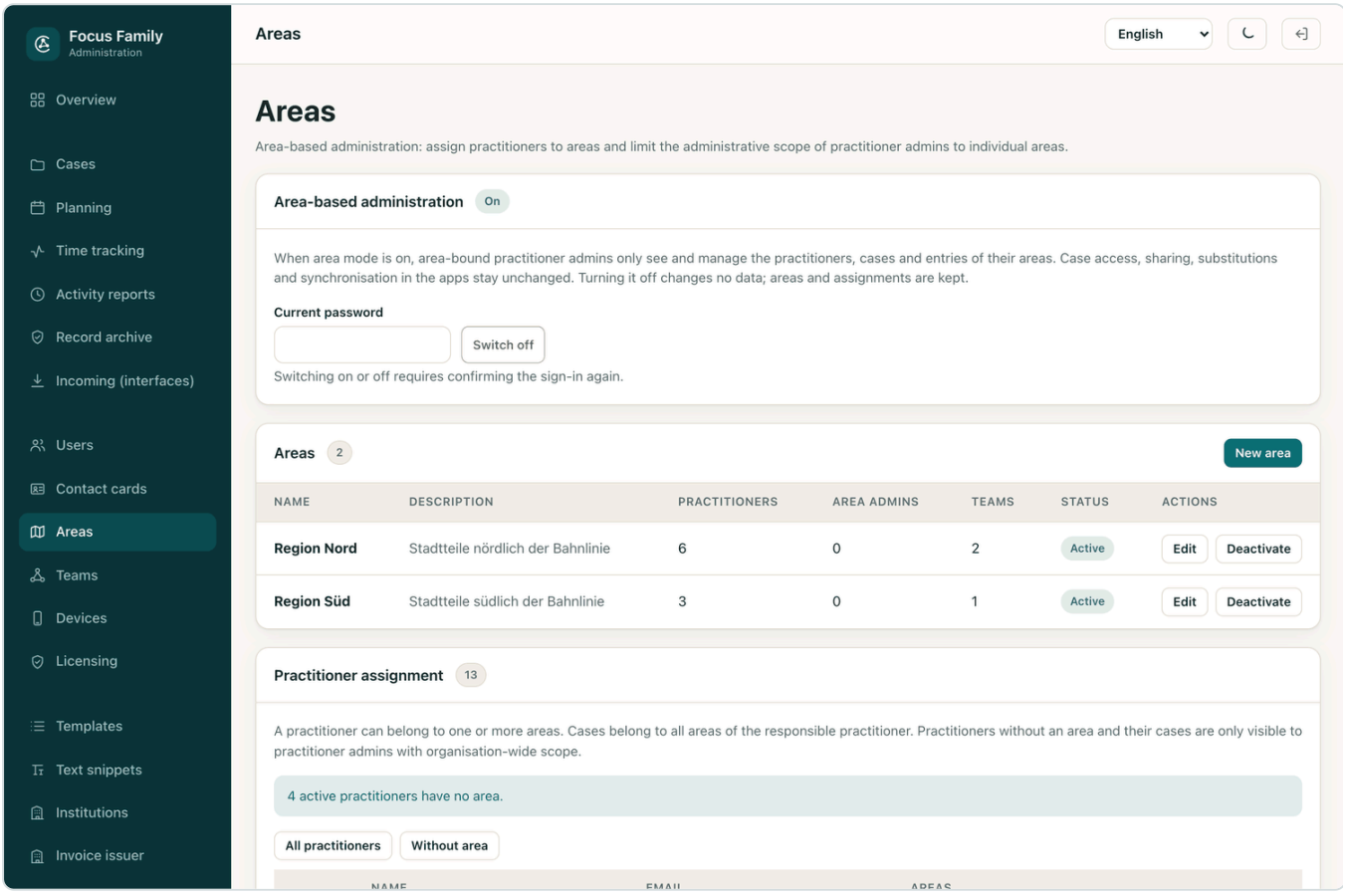
Cases can be assigned to a **team** or to individual **practitioners**. An app only ever shows the cases assigned to that person.

If **areas** are set up (see below), a team can belong to an area. Such an **area team** only accepts practitioners of the same area; teams without an area are organisation-wide teams. When creating a team, a full-scope admin may choose the area; an area-bound admin always creates teams in their own area.

> If you remove someone from a team, their device loses access at the **next sync** to cases it only reached through that team.

Areas (area-based administration)

Menu item **Areas** – visible to accounts with the **Manage areas** permission and **organisation-wide scope** (the permission is part of *Practitioner admin* and can also be granted on its own under **Areas** in the permission list). Large providers can group their practitioners into **areas** (for example regions, departments or sites) and limit practitioner admins to individual areas. An area is purely an **administrative boundary**: case access, sharing, substitutions and synchronisation in the apps do not change.



Area mode, areas and the assignment of practitioners; a practitioner can belong to several areas.

Basic rules

- **Area mode**: an organisation setting, **off by default**. While it is off, the panel behaves for every account as if there were no areas.
- **Practitioner**: belongs to **one or more** areas; one of them is the **primary area**. A **case** belongs to all areas of its **responsible practitioner**; transferring it to a practitioner of other areas moves the case along. The admins of each of these areas see the practitioner and their cases.
- **Administrative scope** of an account with casework administration permissions: **Full** (organisation-wide) or **one or more areas**. An area-bound account only sees the practitioners and cases of its areas (plus itself) in cases, case view, user list and dashboard; other records behave as if they did not exist. Actions on other targets are rejected as “not found” and recorded in the audit as “Access outside the area denied”.
- **Fail-closed**: practitioners without an area and their cases are only visible to full-scope admins. An account with administrative permissions but **no** scope sees no casework data; the panel shows a notice.
- **Area-bound admins** only change accounts whose areas and area-bound teams lie **entirely** within their own scope and that hold no permissions beyond their own; one shared area is enough for viewing. They never grant **professional admin** or **Manage areas** – only full-scope admins create professional admins.
- **Practitioners without an admin role** (neither professional nor system admin) who have panel permissions such as *View cases* and no administrative scope of their own are automatically responsible for their **own active areas**; without an area they see nothing either.
- Area-bound accounts **cannot** hold **audit log**, **licence** or **data protection** permissions. Technical admins and data protection admins without casework permissions are not affected by area mode.
- Pages not yet prepared for area mode are hidden with a notice for area-bound accounts.

Setting up

1. Create **areas** (**New area**; unique name, optional description). Edit, deactivate and delete are available in the list; only an area without practitioners, admins and teams can be deleted. A deactivated area no longer grants any scope.
2. Under **Practitioner assignment**, select practitioners, choose an area and click **Add to area** or **Remove from area** (the **Without area** filter shows practitioners still open). Adding is always possible; existing areas are kept. With area mode switched on, a person's areas can also be changed in the user dialog under **Edit** → **Areas**, where the **primary area** is chosen as well (without a choice, the area assigned first). If the person is an active or future member of teams of an area that is to be removed, the removal is rejected and the message names those teams. The option **End memberships in teams of removed areas** ends those memberships – including expired and future ones – in the same step (audited per membership); expired memberships do not block and no longer affect settings; cases only reachable through those teams disappear from the device at the next sync. Teams without an area are not affected.
3. **Switch on** in the **Area-based administration** card: this requires **confirming the sign-in again** (current password, plus the code if two-factor sign-in is active; passkey accounts confirm with the passkey). When switched on, **all** active accounts with administrative permissions that have no scope yet automatically get **Full** – so nothing changes for anyone at that moment. The card shows the number beforehand.

4. Under **Administrative scope of admins**, switch individual accounts to **Selected areas only** (several areas possible). Nobody can change their own scope; the last practitioner admin with full scope cannot be restricted.
5. Practitioners with panel permissions (e.g. *View cases* or *View time tracking*) keep the full scope after switching on. The bulk action **Limit to own area** in the same card moves all active practitioners who are assigned to at least one active area and hold only the full scope to their own areas in one step. The card lists number and names beforehand. Accounts holding the *Practitioner admin* or *Manage areas* permission and your own account stay unchanged.
6. Under **Teams**, optionally assign each team to an area or move it to another area. Members who do not yet belong to the new area are added to it (the page shows how many); their existing areas are kept.

With area mode switched on, the **New user** dialog offers an area choice (several possible, the first becomes the primary area); with area mode off it is hidden. New accounts created by an area-bound admin are placed in that admin's area automatically (with a required choice in the dialog if the admin has several areas). Accounts with administrative permissions get no scope when created; a full-scope admin assigns it.

Organisation pages in area mode

For area-bound accounts the organisation pages behave as follows:

- **Teams**: only teams of the own areas; new members only from the own area.
- **Contact cards and substitutions**: only cards of the own practitioners; substitutions appear when the absent person or the case belongs to the own area. A full-scope admin creates cross-area substitutions. Only a full-scope admin maintains the **organisation contact details**.
- **Managed settings**, **text snippets** and **templates**: organisation-wide entries are **read-only**; entries for the own areas, teams, practitioners and devices can be maintained.
- **Institutions**, **measure catalogue** and **activity types** apply organisation-wide and are **read-only**.
- **Devices**: only devices of the own practitioners.
- **Admin API** (`/api/v1/admin/…`): sign-ins of a user account are subject to the same scope; foreign targets answer "not found". The service client (client credentials) stays organisation-wide.

Switching off

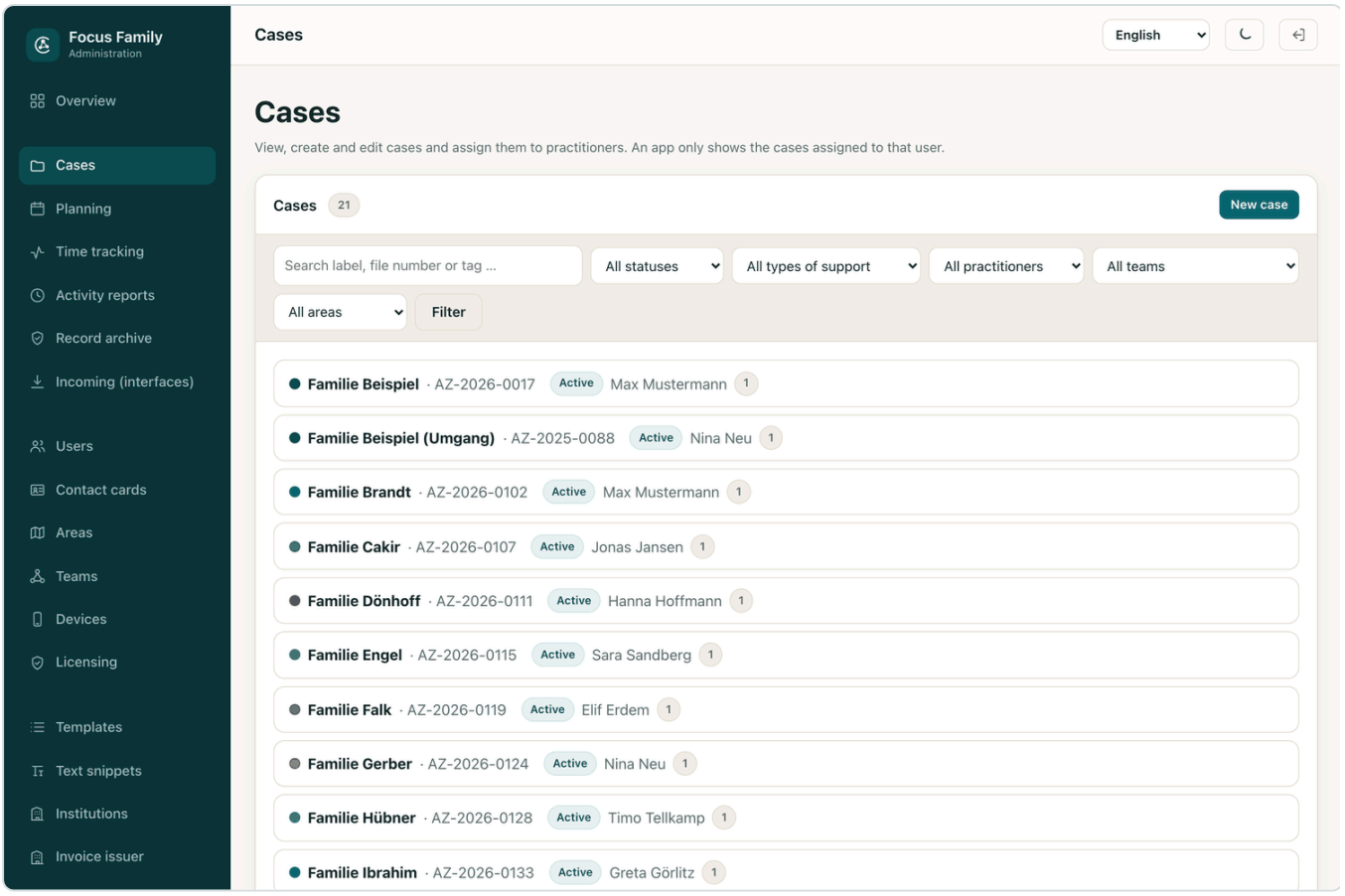
Switch off (also with sign-in confirmation) only resets the switch. Areas, assignments and scopes stay stored and apply again when switched back on; cases and entries are never changed.

Activity

The **Activity** list shows the latest area events (mode, areas, assignments, scopes, denied access) with time, acting person and target. The full log is in the **security audit**.

Cases

Menu item **Cases** (permission *View cases* or *Edit cases*). Remember: this is about administration and assignment, not about the professional case work.



The organisation's cases with status, type of support and assigned practitioners.

Creating and assigning a case

1. Click **Create new case** and fill in the fields: **name / alias**, **file number**, **status**, **type of support** (including **school accompaniment**), **responsible office**, **youth welfare officer**, **approved minutes** and **colour**.
2. Click **Create case**.
3. Under **assigned practitioners**, use **Assign** to add people.

The case form contains all professional fields – among them the responsible practitioner, a custom type of support, key information, resources and tags.

Use the filter bar of the case list to find cases by name or file number and to narrow them down by status, type of support, practitioner or team.

Participants and addresses

Inside a case, the card **Participants & addresses** lists everyone involved, grouped by their **address** (formerly "household"). An address groups the people living at the same place.

- **Add participant** opens the dialog with given and family name, **role**, **gender**, **date of birth**, **place of birth**, **date of death**, **nationality**, **marital status**, **health insurance**, **child benefit number** and **institution / office**. The date of death must not be before the date of birth.
- Besides child, parents, foster carer and network partners, the roles include **sibling, half-sibling, grandmother, grandfather, aunt, uncle, step-parent, partner of a parent, cousin, other relative**

and **youth welfare provider**. For half-siblings, grandparents, aunt, uncle and cousin an extra **family side** field (maternal/paternal) appears; the view then shows e.g. "Grandmother (maternal)".

- **Is a minor** marks children and young people; it is ticked automatically for the role "child".
- **Address** links the person to an existing address. **New address …** creates a new address with label and postal address in the same dialog; saving creates the address and the person together.
- While **Take over the address details** is ticked, the address of the linked address applies and the fields for an own address are hidden. Untick it to enter a different address.
- Phone numbers have the types **mobile (private)**, **landline (private)**, **landline (work)**, **mobile (work)** and **other**.

Fields the panel does not show (such as notes from the app) are kept unchanged when saving.

Roadmap, goals and review points

Two cards in the open case show how the support is progressing:

- **Roadmap** – a timeline from the start of the case until today: goal tracks, review points as markers and, below, the recorded time per week or month with the quota line.
- **Goals & review points** – the list of goals (status, target date, predecessor goal, achieved on) and review points (date, type, title, next appointment, status). With *Edit cases* you can create review points; changes sync to the devices.

Cover arrangements

Every case has the card **Cover (time-limited)**:

- Choose a **colleague**, set **from** and **to**, then **create cover**. Access starts and ends automatically; holiday cover can be planned in advance and ended early at any time.
- A cover arrangement grants normal read and write access for its duration. **Private entries stay protected**, permanent assignments remain unchanged.
- Every step (created, activated, ended, expired) is logged.

Transferring a case

When responsibility changes permanently, transfer the case completely to another practitioner. In the case, under **assigned practitioners**, **Transfer case** opens a dialog (permissions *Edit cases* and *Assign to others*):

1. Choose the **new responsible practitioner** (active practitioners of the organisation only).
2. Optionally tick **Previous practitioner keeps access** – the previous practitioner then stays on the case as a shared person.
3. Click **Transfer** and confirm.

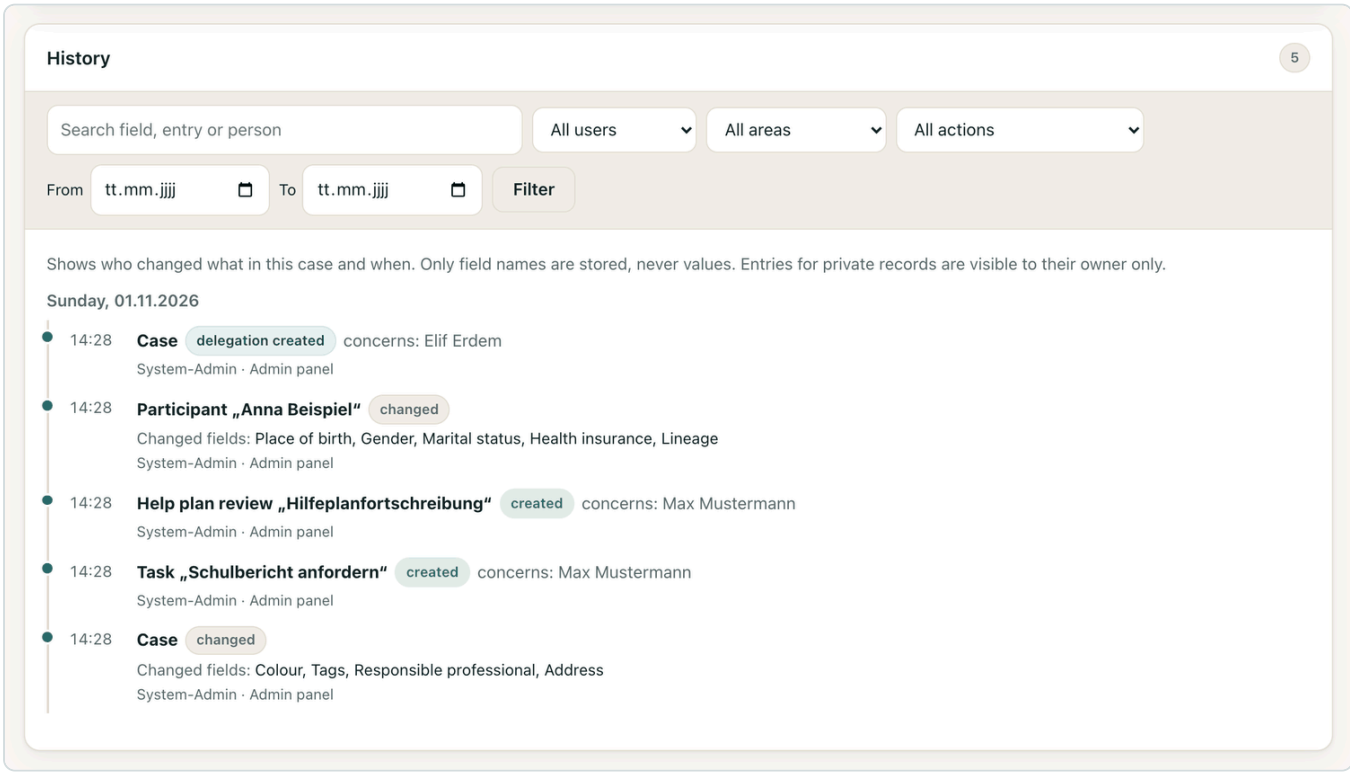
The new practitioner becomes the owner of the case and takes over every entry that belonged to the previous practitioner – including private and restricted entries and files. Time entries, signatures and closures stay assigned to the person who recorded them. Open cover arrangements for the previous practitioner end. Without "keeps access", the previous practitioner loses the case at the next sync unless a team still grants access. The transfer appears in the **audit** as "Case transferred".

In the app, only the current owner can transfer a case.

Appointments, tasks and media in a case

- **Add appointment** and **Add task** create both directly inside the case.
- The **media** area shows photos, videos, voice memos and sketches – but only if you are a professional admin or assigned to the case, and only **non-private** entries. If a file has not been transferred yet, the note "file not on the server yet" appears.
- The **e-file** lists the documents per section (e.g. contracts & consents) with creation, version, template and signatures. Clicking the title or **Open** loads the file; file name and size appear in the tooltip. In narrow windows the panel hides the template and signature columns.

Case history



The history lists time, affected entry, action, person, device and source for each change – field names only, never content.

At the bottom of the case view, the **History** area shows who changed what in the case and when – newest first, grouped by day. All paths are recorded: sync from the app and desktop (including the device), changes in the admin panel, the app functions share, remove sharing, cover arrangement and transfer, as well as deletion requests, retention decisions and processing restrictions. Purely technical records are not part of the history: activity record closures (period snapshots), imported person calendars and the external commitments taken over from them. Time entries, trips and signatures do appear, because they document work done in the case.

- Each entry shows the time, the area (e.g. "Participant "Anna B."", "Appointment dated 12.03.2026" or "Time entry dated 03.10.2026"), the action, the person or "System", the device and the source (e.g. "synced from app/desktop").
- For changes, only the **names of the changed fields** appear (e.g. "Date of birth, Primary address"). The history never stores contents, old or new values. Technical fields such as timestamps, versions or checksums do not count as changes.

- Entry names only appear if they are visible in the case view anyway; appointments, time entries and trips show their date instead. If neither is available (for example for private or deleted records), only the area is shown, e.g. "Phone number" – without a technical identifier.
- Use the filters to narrow down by person, area, action and period; the search covers area, field names and people. Each page shows 50 entries; **Older** and **Newer** turn the pages.
- You only see what you may also see in the case view: appointments only with the calendar right, tasks only with the task right, time entries and trips only with the time-tracking right, rate agreements only with the billing right, e-file and media only for professional admins and assigned people. Entries about private records are visible to their owner only. For a private case, others only see administrative steps such as sharing, transfers or cover arrangements.
- When a case is permanently deleted after the deletion review, its history disappears completely. For a single permanently deleted record only the note "permanently deleted" remains.

Interfaces: incoming items and handover

If the server is connected to case management systems, document management, an e-file or youth welfare offices, the technical administration sets this up; details are in the **Interfaces handbook**. In day-to-day work it shows in several places.

Reviewing incoming items

The page **Incoming (interfaces)** collects documents, master data changes and appointments from connected systems that need review. It is available to accounts with the permission **Review and accept interface inbox items** (included in the professional admin, under **Operational** in the permission list) and, like the case view, only shows items for cases within the own administrative scope that are not deleted, not marked for deletion and not restricted in processing; the case picker for assigning offers the same cases. **Assign** and **Accept** write into cases and only appear if the account also holds **Edit cases**; rejecting only needs the inbox permission. "Edit cases" alone does not open the page, because items assigned to another practitioner can also land here. If a case is restricted in processing, for example, its items disappear from the list and can no longer be accepted, assigned or rejected.

- Each row shows time, **Source** (name of the interface), **Type** (document, master data, appointment, catalog), **Content**, **Case** and **Status**.
- **To review: Accept** creates the document in the case file or enters the master data into the case. **Reject** discards the item.
- **Assign case:** the connected system did not name a unique case. Choose the case and click **Assign**. The file is then scanned for malware and becomes available under **To review**. Items without a case are only visible to accounts with organisation-wide administrative scope.
- **Conflict:** a practitioner changed a field since the last import from this system; the affected fields are listed below the status. **Accept** overwrites the practitioner's values only after a confirmation, **Reject** keeps them.
- Accepted and rejected items stay visible at the end of the list.
- If a case or record is finally deleted, its items keep only technical data; content, file name and the connected system's case reference and external ID are removed.

Depending on the setup the server also accepts documents directly; appointments from connected systems are always created directly in the case. No interface changes practitioners' free texts, and nothing is deleted from outside.

Origin of delivered documents

Accepted documents appear in the case's **case file** as final documents; the author is the name of the interface. The case **history** names "Interface" as the source. The documents reach the practitioners' devices with the next sync.

Handing over to a target system

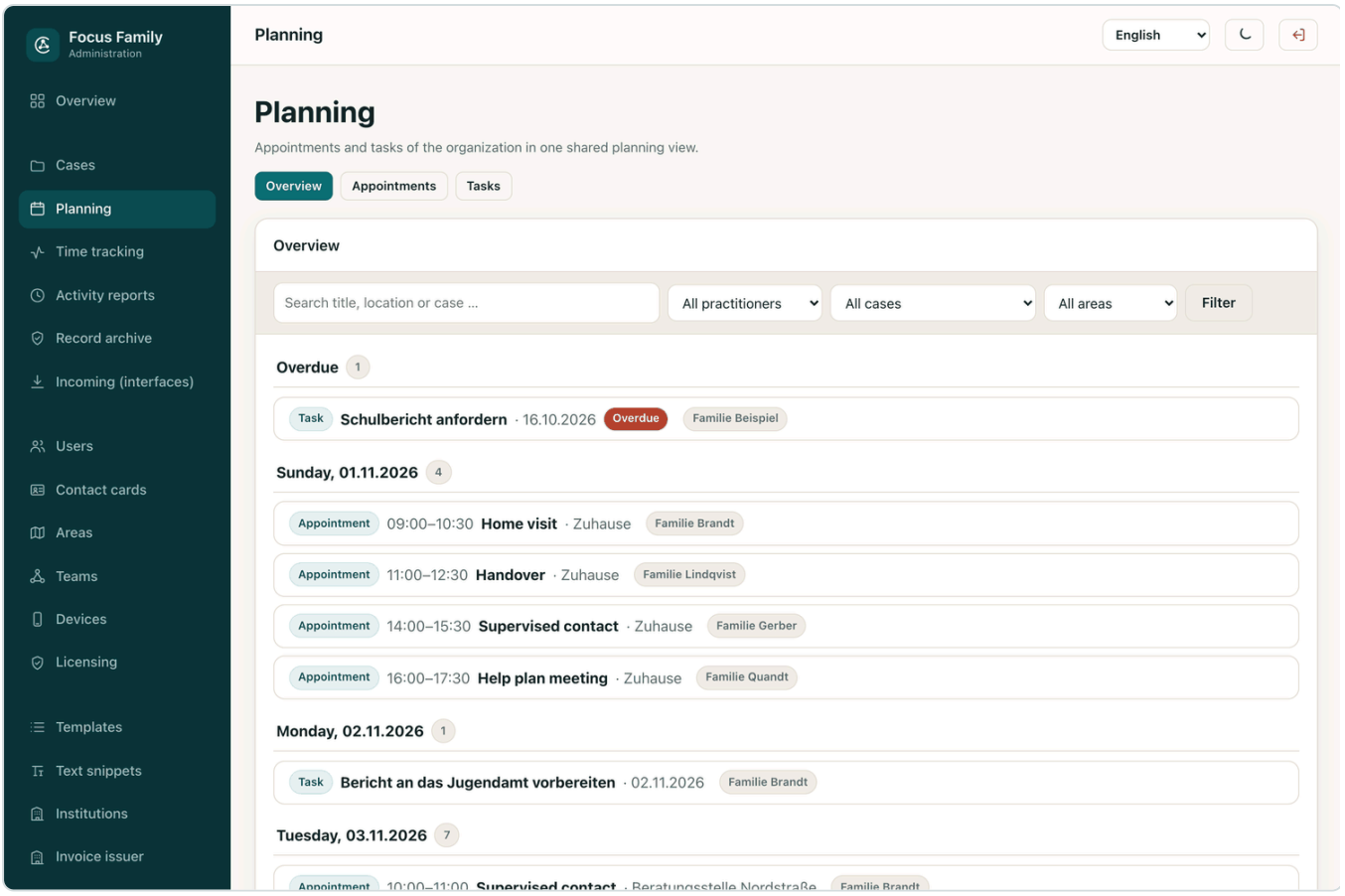
If an interface is set up for manual handover, the case view shows accounts with **Edit cases** the button **Hand over to target system**. Choose the **Target system** (e.g. the e-file or a youth welfare office via XÖV) and confirm with **Start handover**. The case file is handed over with the released documents. The interface's privacy settings apply; blocked document types and private entries stay behind. The handover appears in the technical administration's transfer log.

Calendar subscription

If calendar subscriptions are enabled, every person creates a personal subscription address for Outlook, Thunderbird or the iPhone calendar under **Calendar subscription**. The address is shown only once and is secret; **Create new address** invalidates the previous one, **End subscription** revokes it. How much an appointment shows in the subscription (only "Busy", appointment type and case alias, plus location) is set by the organisation; private appointments always appear only as "Busy".

Planning

Menu item **Planning** – one page with three views:



Overview, appointments and tasks for the whole organisation in one place.

- **Overview** – overdue tasks first, then appointments and tasks grouped by day, finally tasks without a date. Clicking an entry opens it under **Appointments** or **Tasks** for editing. Planned appointments whose end time has passed and tasks whose due date or due time has passed are overdue – on the same day, too – and carry the **Overdue** badge.
- **Appointments** (permission *View calendar*) – the organisation-wide appointment list. **New appointment** creates entries; the **repeat** section creates a **series** (daily, weekly with weekdays and "every N weeks", monthly; ending by date or count; at most 180 appointments over at most 3 years). Series occurrences carry a **series** badge; editing changes only that occurrence, while **delete series** removes the whole series. Past and documented appointments are preserved.
- **Tasks** (permission *View tasks*) – the organisation-wide task list with **New task**. Tasks without a case can be edited and removed; new tasks need a case.

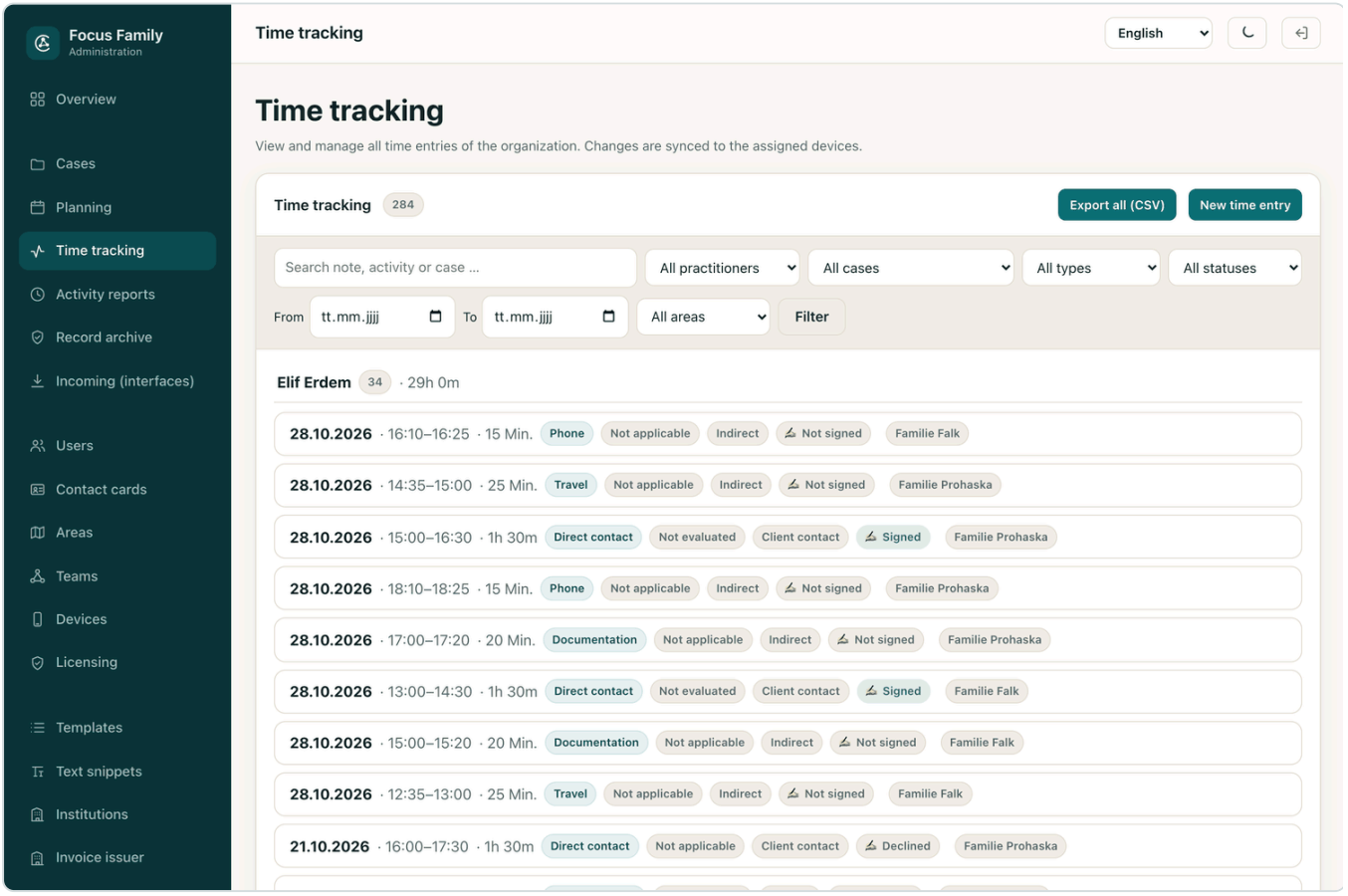
Editing and removing require the permissions *Edit calendar* and *Edit tasks*. Appointments with a signature, time entries or documentation cannot be removed; the panel names the reason. **Delete series** keeps such occurrences as well. If a change fails, the panel shows an error message instead of "Saved".

With the permission *Record time*, every appointment additionally offers **Create time entry** – at most one time entry per appointment.

Every view has a filter bar: search, practitioner and case everywhere, plus type, status and date range for **Appointments**, and status, priority, due date and date range for **Tasks**.

Time tracking

Menu item **Time tracking**.



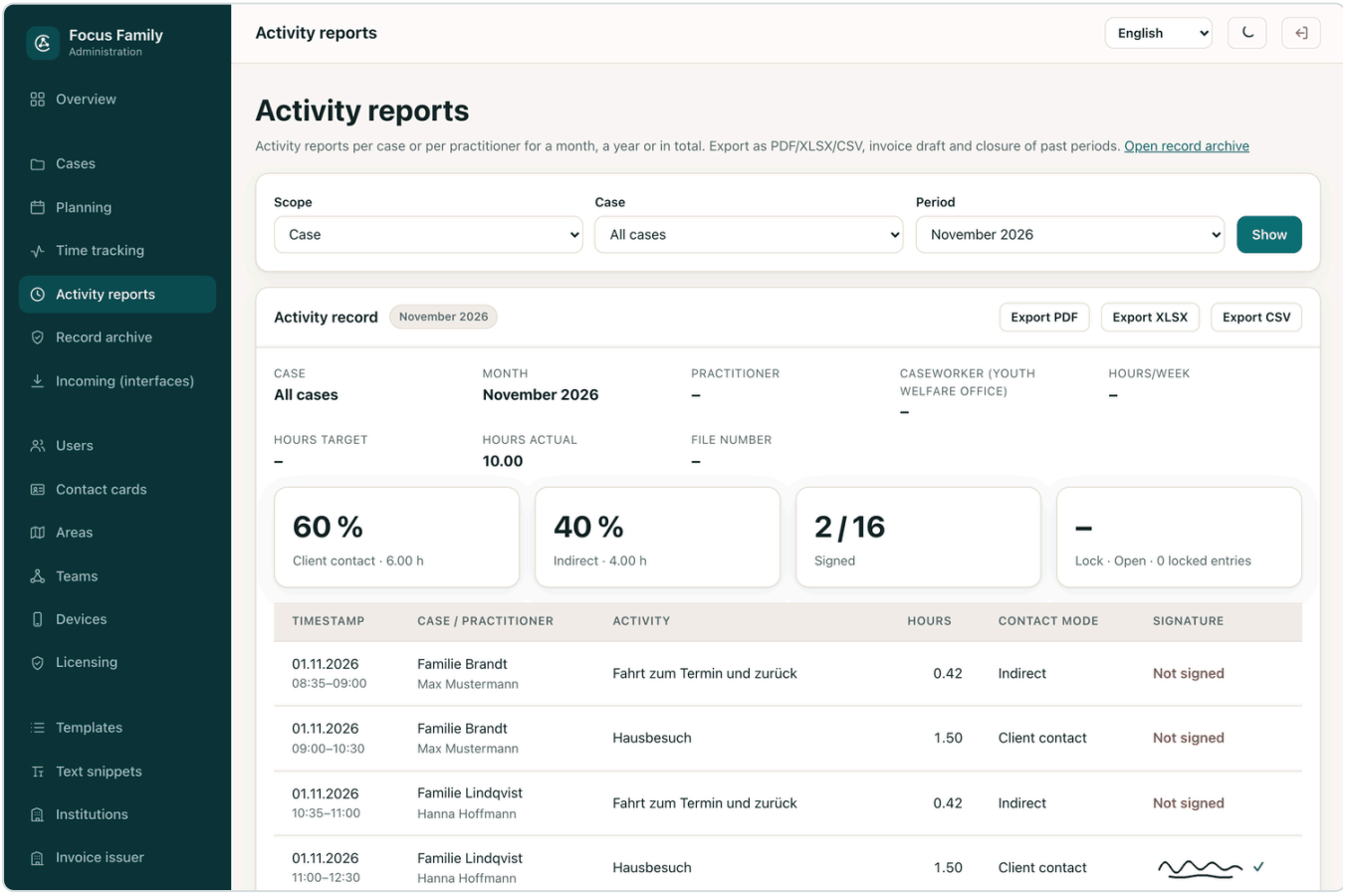
All time entries of the organisation with lock and signature status; filters narrow the list down to one practitioner.

- With **View time** you see all time entries of the organisation with date, duration, type and case, plus the columns **lock** (a padlock means the period is closed) and **signature** (signed, not signed, refused).
- With **Record time** you create your own entries via **New time entry**.
- Entries of **other** practitioners can only be changed or deleted with **Manage records** and only within your **management scope**. Such changes are logged as management corrections.
- The filter bar narrows the list by practitioner, case, type, billing status and date range or searches notes and activities; **Export all (CSV)** extracts the data for further processing.
- Trips recorded in the app with **Start trip now** and **Arrived** appear as a travel time entry with a kilometre badge. In the details, the section **Recorded trip** shows kilometres, duration, departure and arrival, destination and purpose plus a route sketch as evidence. The panel draws the sketch without a map service; the route points are movement data of the practitioner and are therefore not included in access requests and data exports for clients.

> No one can change another practitioner's time entries or signatures from a device. Management corrections are only possible here in the panel.

Activity records

Menu item **Activity records** (permission *View time*).



Records per case or practitioner with key figures, individual lines, exports and the closing of past periods.

1. Choose **case** or **practitioner** and the **period** (month, year, total), then **show**.
2. The page shows the **key figures**: hours, target/actual from the quota, share of client contact and indirect work, signature rate and lock status – followed by the table with date, case or practitioner, time, activity, hours, contact type and signature. Yearly and total records are grouped by month, practitioner records by case. **Private entries are never included.**
3. **Signatures** appear directly in the table with image, name, role and time. Next to each image sits a check symbol: - ✓ – the checksum matches the image and the frozen summary; the signature is unchanged. - ⚠ – the checksum does **not** match; image or summary were changed after signing or are damaged. Clarify this with the practitioner. A missing signature is **not an error** – it is voluntary.
4. **Export** as **PDF**, **XLSX** or **CSV**.
5. **Invoice draft** turns a case record into a JSON preparation with funding body, items per activity type and open signatures. Amounts only appear with the permission *See amounts*. The e-invoice itself (XRechnung or ZUGFeRD PDF) is created by the professionals in the app or on the desktop, because the invoice issuer details (tax number, IBAN, VAT treatment) are only maintained there.

Closing and reopening

This requires the permission *Close records*, and only within your own management scope.

- **Close** freezes a **past** month or year (optionally with a note). From then on all time entries of the period are **locked** on every device: changes, deletions and moving entries into the period are rejected; reading stays possible. The record receives a checksum and the complete state is stored.
- **Closed state:** opening a closed period shows the note "closed state (checksum secured)". Table and exports then come from the stored state. If the yellow warning **"attention: current data differs from the closed state"** appears as well, entries were changed after closing – for example because a device synced later. The closed state is still what is shown and exported.
- The **current month** and the **current year** can never be closed.
- **Reopen** lifts the lock and requires a **reason**. Both end up in the security audit.
- Practitioners cannot close or open anything themselves; they see locked entries with a padlock.

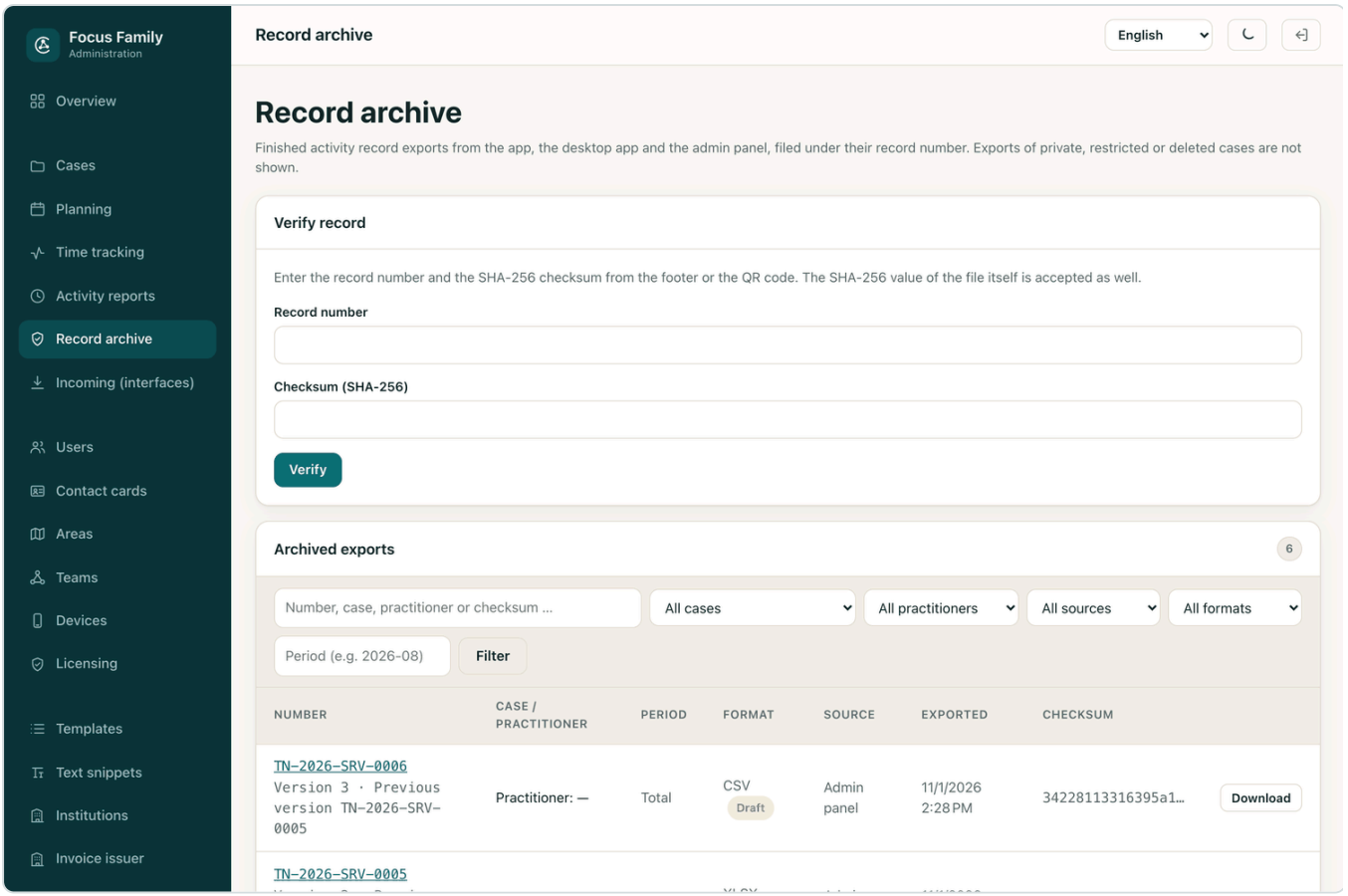
Identification and record archive

Every exported activity record – from the app, the desktop app or the panel, in any format – is uniquely identified:

- **Record number** in the format `TN-<year>-<device code>-<sequence>`, e.g. `TN-2026-7KQ2-M9XA-0042`. The eight-character device code is generated randomly once per device; the sequence counts per device and year. This way no duplicate numbers arise even offline on several devices of the same person. Panel exports get numbers with the code `SRV` (e.g. `TN-2026-SRV-0007`), issued consecutively by the server.
- **Export time** and **version**: if the same record (same case or practitioner and the same period) is exported again, the version increases and the document names the number of the previous version.
- **SHA-256 checksum** over the content of the record including number, version and export time. Any later change to the content yields a different value.
- **QR code** with number and checksum; on devices connected to the server it leads directly to the verification page.

PDF and Word show these details in the footer of every page, Excel on the **Identification** sheet and in the print footer, CSV in the **Identification** block at the end of the file (after a blank line; the column headings stay in the first line) and JSON in the `identification` section.

Archive: a device connected to the server uploads every export encrypted after saving – buffered while offline, as soon as a connection is available. Panel exports are filed immediately. The **Record archive** menu item (permission *view time tracking*) lists all archived exports with search and filters (case, practitioner, source, format, period) and offers the **download** of the original file. Exports that contain a private, restricted or deleted case are not shown.



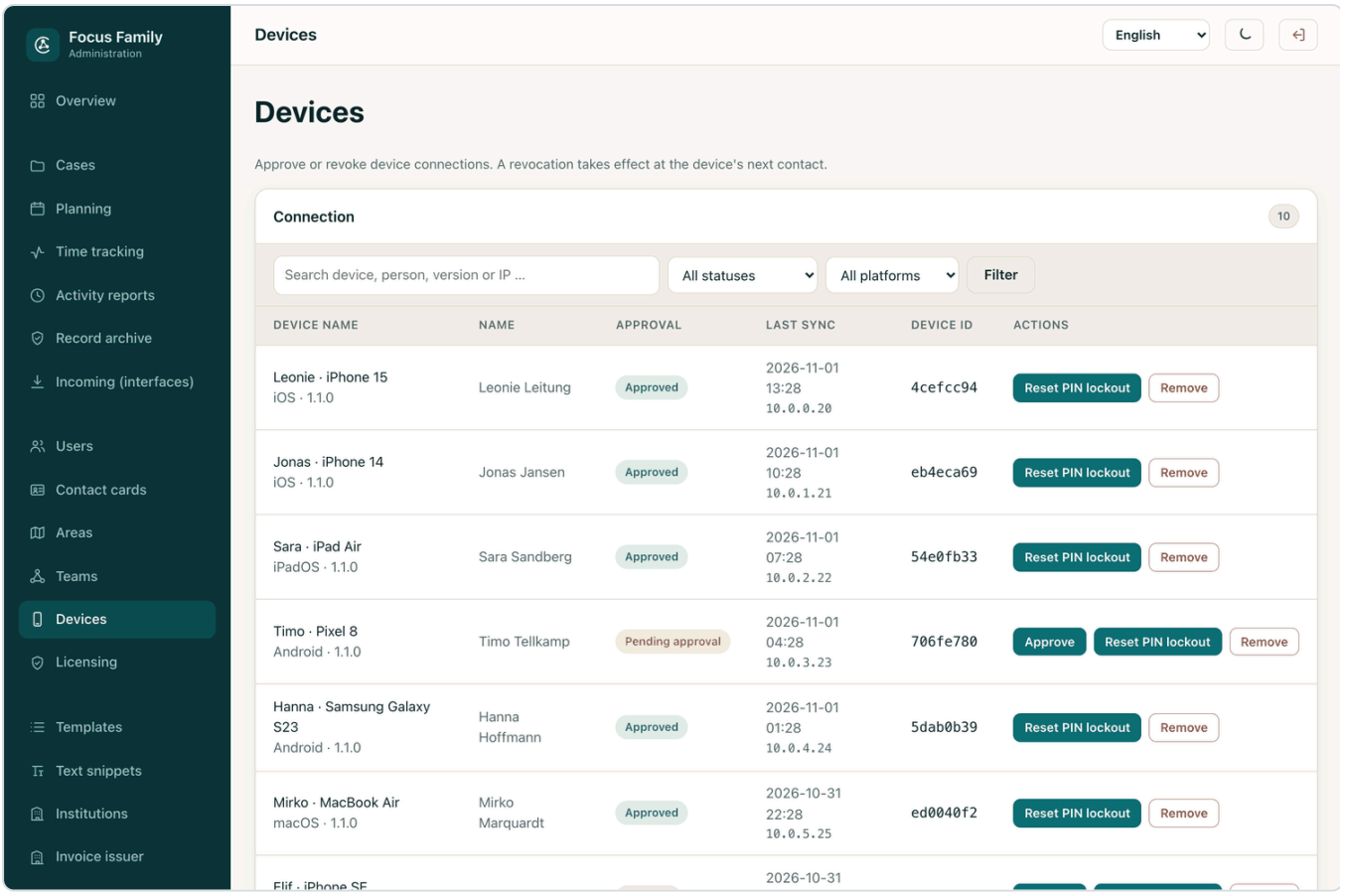
The record archive lists every stored export with record number, version, source, format and checksum.

Verify: under **Verify record** enter the record number and the checksum from the footer or QR code (the QR code opens the page directly after sign-in). The result is *Authentic*, *Mismatch* (the checksum does not match – the presented document was changed) or *Not found*. The SHA-256 value of the file can be entered instead of the content checksum. The page requires sign-in and shows no contents of blocked cases.

Deletion: if a contained time entry is deleted or a case is removed for good, the archived file is deleted as well. Number, version and checksums remain as evidence ("File deleted").

Devices

Menu item **Devices** (permission *View devices* or *Manage devices*).



Registered devices with platform, version, last sync and status. This is where you approve, block or disconnect devices.

The first line shows the device model, for example **iPhone Duo**. If the device has a name of its own, it appears in the line below. iPhones and iPads only report their name with Apple's approval; without it only the model is shown. Desktop devices show the computer name.

- **Approve / block** – a block takes effect the next time the device contacts the server.
- **Reset PIN lock** – if a practitioner locked themselves out or forgot the PIN, lift the app lock here. It is released at the next sync and the person sets a new PIN.
- **Remove** – disconnects the device from the server. It loses access and must be set up again; the **licence seat becomes free** again. Practitioners cannot disconnect themselves.
- **Re-enrolment code** – if a known device has to be set up again (after a reinstall, say), issue a code. The device reconnects to its existing registration without consuming a new seat.

Licence seats

Seats are assigned **exclusively by administration** – devices and practitioners cannot claim one themselves. Without a seat a device cannot sync. The menu item **Licensing** gives an overview of your organisation licence (permission *Manage licensing*); the button for managing seats and subscription only appears with the permission *Purchase licensing*.

The tile **Seats assigned** shows "assigned / total"; the total is the sum of purchased seats (while the subscription is running) and sponsored seats.

Sponsored seats: The vendor can grant an organisation additional free seats. They count towards the total and can be assigned like purchased seats, even without a subscription; the tile **Subscription** then shows

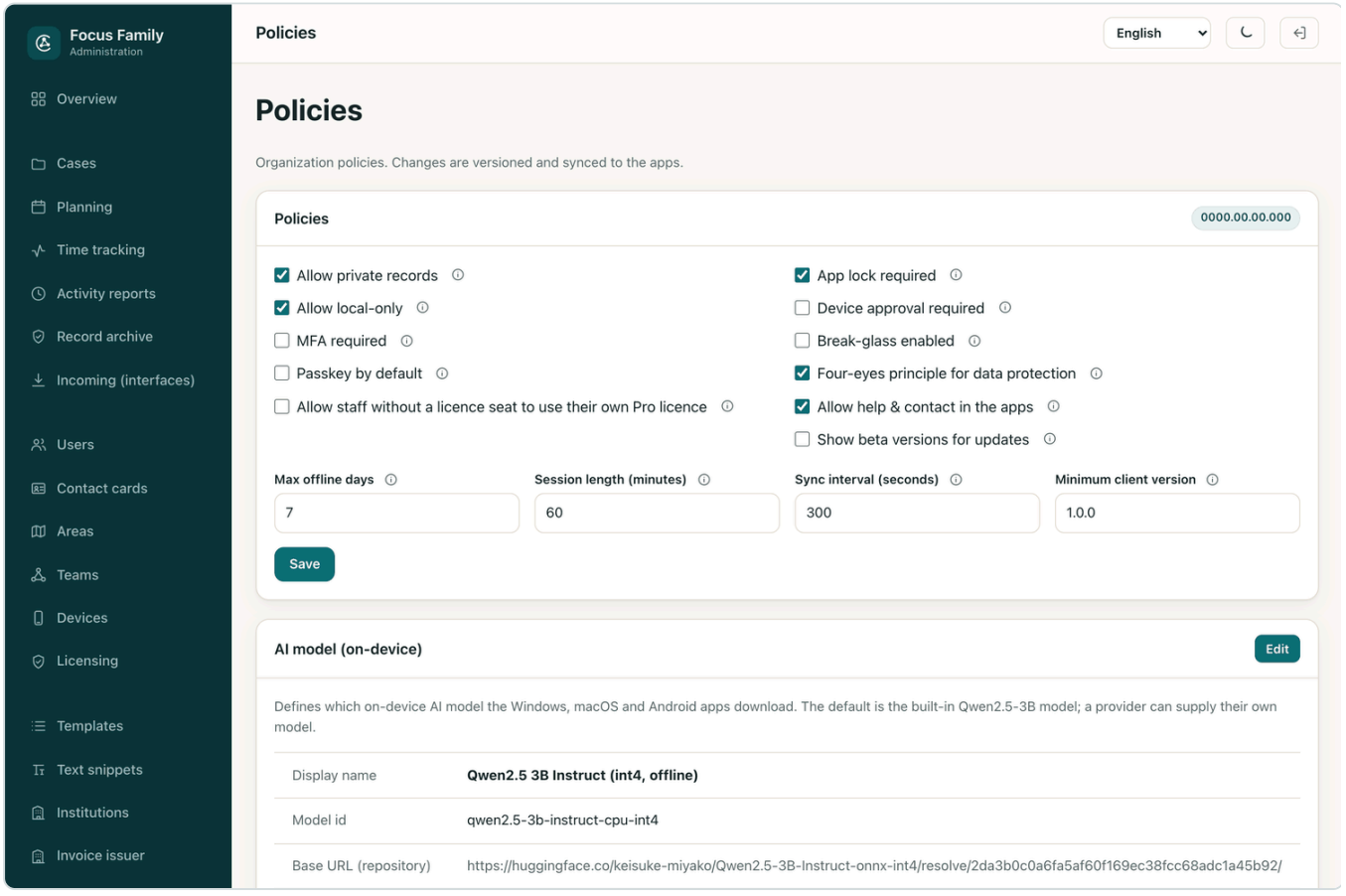
Sponsored. Below the tiles the note reads "Sponsored seats: *number* – free of charge and not part of billing (until *date*). They can be assigned like purchased seats but cannot be changed in the subscription." They cannot be added or removed in the admin panel. Buying or reducing purchased seats ignores them; purchased seats can be reduced down to the number of assigned seats minus the sponsored ones.

Assigned, unlicensed: if there is no running subscription and fewer sponsored seats than assignments (for example after a sponsorship ends), only the earliest assigned seats up to the number of sponsored seats are valid. The remaining practitioners carry the label **Assigned, unlicensed** in the list, and a note above states their number. They cannot sync until seats are purchased or assignments are revoked; a seat can be revoked at any time, even without a valid licence.

> **Licence reminders in the app:** paid licences must be confirmed online regularly. If that does not happen, the app reminds the practitioner from **day 3** at most once a day, from **day 5** hourly, and from **day 10** it requires confirmation (locked until the check succeeds – data stays untouched).

Policies

Menu item **Policies** (permission *View policies* or *Edit policies*). Policies apply organisation-wide, are **versioned** and distributed to all apps.



Organisation-wide rules – from mandatory app locks to the maximum offline period.

Policy	Meaning
Allow private records	practitioners may keep individual entries private
Allow local-only	content that deliberately stays on the device
MFA required	two-factor sign-in is mandatory (apps and panel)
App lock required	the app must be locked with a PIN or biometrics
Max. offline period (days)	how long a device may work without server contact
Session duration (minutes)	after this time without activity a new sign-in is needed
Sync interval (seconds)	how often the app syncs in the background
Minimum client version	older app versions are rejected during synchronisation
Device approval required	new devices must be approved first
Break-glass enabled	switch emergency access on or off
Four-eyes principle for data protection	release of subject access packages by a second person
Allow help & contact in the apps	practitioners can send bug reports, feature requests, general enquiries and security reports from the app and desktop to Software Notion – never with app data; when off, the area is hidden in the apps after the next sync and in the panel; in the panel only accounts with the *edit policies* permission keep it; on by default
Show beta versions for updates	visible to system administration only: the update notice also offers pre-release versions; recommended for test installations only, off by default

Break-glass (emergency access): in exceptional cases – acute risk to a child's welfare, for example – an authorised person can access a case for a limited time (at most 120 minutes), with two-factor confirmation and a logged reason, even without a regular assignment. Every access appears in the audit.

AI model: policies also decide which **language model** the apps use for local AI support. The model size determines the download in the app. The AI still runs entirely on the device.

Help & contact

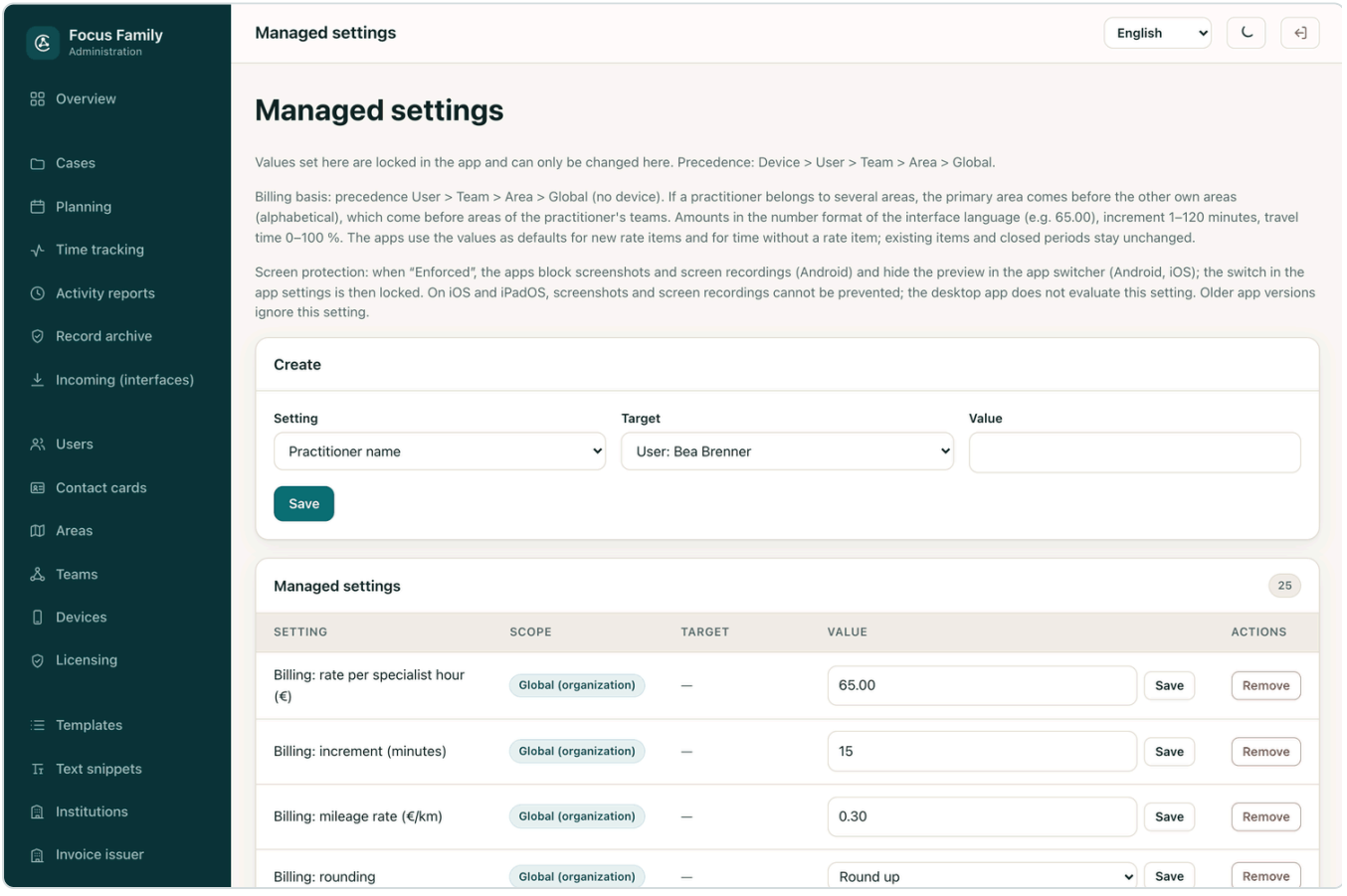
Menu item **Help & contact** (for every signed-in account while the policy **Allow help & contact in the apps** is on; accounts with the *edit policies* permission always see it). From here you send a **bug report**, a **feature request**, a **general enquiry** or a **security report** from the admin panel to Software Notion.

- **No data from the panel** is transmitted – no cases, appointments, tasks, documents or people. Please therefore describe the request as precisely as possible (page, steps, expected and actual result).
- **Check** examines the text for names and addresses from the database and removes phone numbers, e-mail addresses and similar details. The **preview** then shows exactly what will be sent: technical details (reference, panel version, licence type, Focus Family ID, server instance) plus the subject and text, both of which you can still correct. The text is checked again when you **send** it.
- Replies go to the e-mail address entered (prefilled with your account address).
- The panel sends the request itself over HTTPS to `software-notion.de`. If the server has no internet access, the page offers **Copy text** and **Send by e-mail**.
- Successfully sent requests appear in the security audit with type and reference – without the text.

Which data is transmitted and when it is deleted is described at focusfamily.software-notion.de/support. Whether practitioners also see the area in the apps is controlled by the policy **Allow help & contact in the apps**.

Managed settings

Menu item **Managed settings** (permission *View managed settings* or *Edit managed settings*).



Centrally set values appear locked in the app. Each value applies to a scope.

Here you define values that are **locked** in the app and can only be changed here – for example the **organisation name**, **address**, **contact**, the **practitioner name** or the **blob storage limit**.

Each value is set for a **scope**: **global (organisation)**, **area**, **team**, **user** or **device**. If more than one value applies to the same setting, precedence decides:

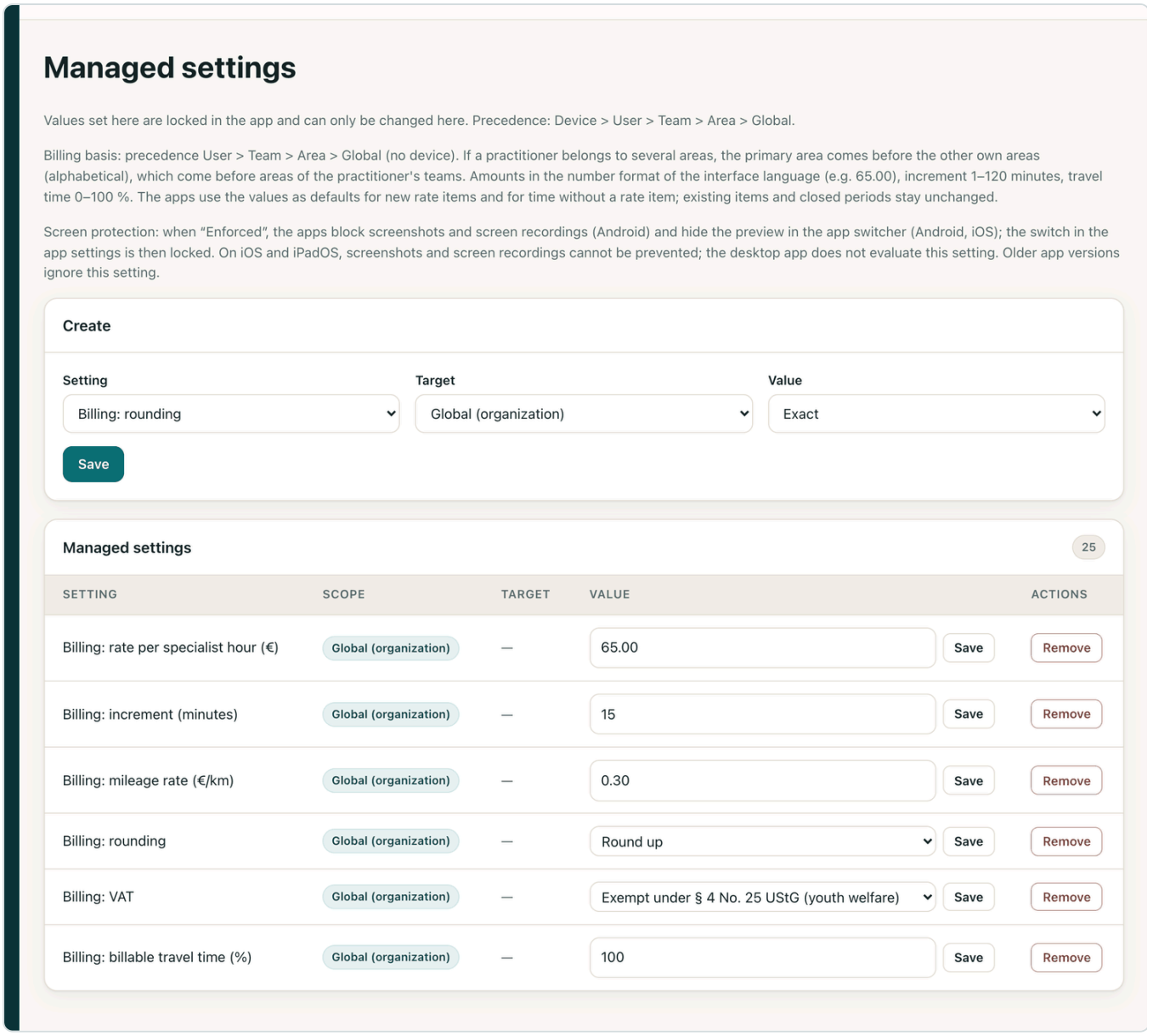
> **Device > user > team > area > global** – the more specific value wins.

A value for an **area** applies to the practitioners of that area and to the members of teams belonging to that area while the area is active. If values of several areas apply to a practitioner, the **primary area** wins, followed by the practitioner's other areas in alphabetical order, followed by areas that only apply through teams (also alphabetical). It applies regardless of whether area mode is switched on. Area-bound admins can only set values for their own areas, teams, practitioners and devices; they see global values read-only.

The **blob storage limit** is set in **MB** and applies **per practitioner** to all of their files on the server combined (not per day). 512 GB corresponds to the value `524288`. Under **System**, the tile "Storage limit per practitioner (global)" shows the global value.

Billing basis

The billing basis consists of six settings, each set **globally, per area, per team or per user** (not per device). Precedence is **user > team > area > global**; every setting is resolved on its own, so a team or area can override just the hourly rate and inherit everything else from the global values.



The six billing basis values; amounts appear in the number format of the interface language.

Setting	Default (industry standard)	Allowed values
Billing: rate per specialist hour (€)	65.00	greater than 0 up to 1000
Billing: increment (minutes)	15	1–120
Billing: rounding	Round up	Exact, round up, round down, round to nearest
Billing: mileage rate (€/km)	0.30	0 to 5
Billing: billable travel time (%)	100	0–100
Billing: VAT	Exempt under § 4 No. 25 UStG	Exempt § 4 No. 25, small business § 19, 19 %, 7 %

The defaults follow outpatient youth welfare services (e.g. SPFH). They are created once per organisation as global values and can be changed like any other value. Values that are already set are never overwritten; a deleted value is not created again. Rounding and VAT are chosen from a selection list. The panel shows

amounts in the number format of the interface language (English: `0.30`, German: `0,30`); input accepts comma and point, also with thousands separators (`1,000.00` or `1.000,00`). A single separator is always read as the decimal separator. The panel rejects invalid values.

How the apps use the billing basis:

- **New rate items** in rate agreements are prefilled with hourly rate, increment and rounding (with the mileage rate for the unit kilometre) and remain editable. This also applies to new items in the panel (case page → rate agreements, billing basis of the responsible practitioner).
- **Time without a matching rate item** is priced in the invoice draft and e-invoice as "Specialist hour (default)" or "Travel time (default)". Travel time uses the configured share of the hourly rate; at 0 % it is not billable.
- **Kilometres** from recorded trips are billed exactly once: in the trip's case, on the trip date, for the practitioner who owns the trip. If a kilometre item of the rate agreement applies on the trip date it is used, otherwise the "Mileage allowance (default)" from that practitioner's billing basis. Trips without a case are not billed.
- The **VAT** for e-invoices (XRechnung, ZUGFeRD) is locked in the apps and marked "Set by the provider".

Existing rate items remain authoritative. Closed periods keep the prices that applied when they were closed; later changes to the billing basis only affect open periods. Kilometres from trips and the mileage rate are recorded at closing as well, so the invoice draft yields the same amount before and after closing.

Invoice issuer

Menu item **Invoice issuer** in the configuration group (permission *Manage invoicing details*). This is where the details printed as the issuer on every e-invoice (XRechnung, ZUGFeRD) are maintained while the apps are connected to this server. There is exactly one record per organisation.

Section	Fields
Issuer and contact	name (required), contact person, phone, email, street, house number, postal code, town, country
Tax details	tax number, VAT ID
Bank details	IBAN, BIC, account holder
Invoice numbers and payment term	invoice-number prefix, payment term in days (0–365, default 30)

When saving, the panel checks the details: name present, address complete and postal code matching the country, valid email address, **IBAN with correct check digits**, **VAT ID in a valid format** (`DE` plus nine digits, other countries two letters plus 2–12 characters), BIC with 8 or 11 characters. IBAN, VAT ID and BIC are stored without spaces in upper case. A valid e-invoice also needs the tax number or the VAT ID; the app checks this when creating the invoice. Every change appears in the security audit as "Invoicing details changed" with the changed fields. Area-bound admins see the page read-only.

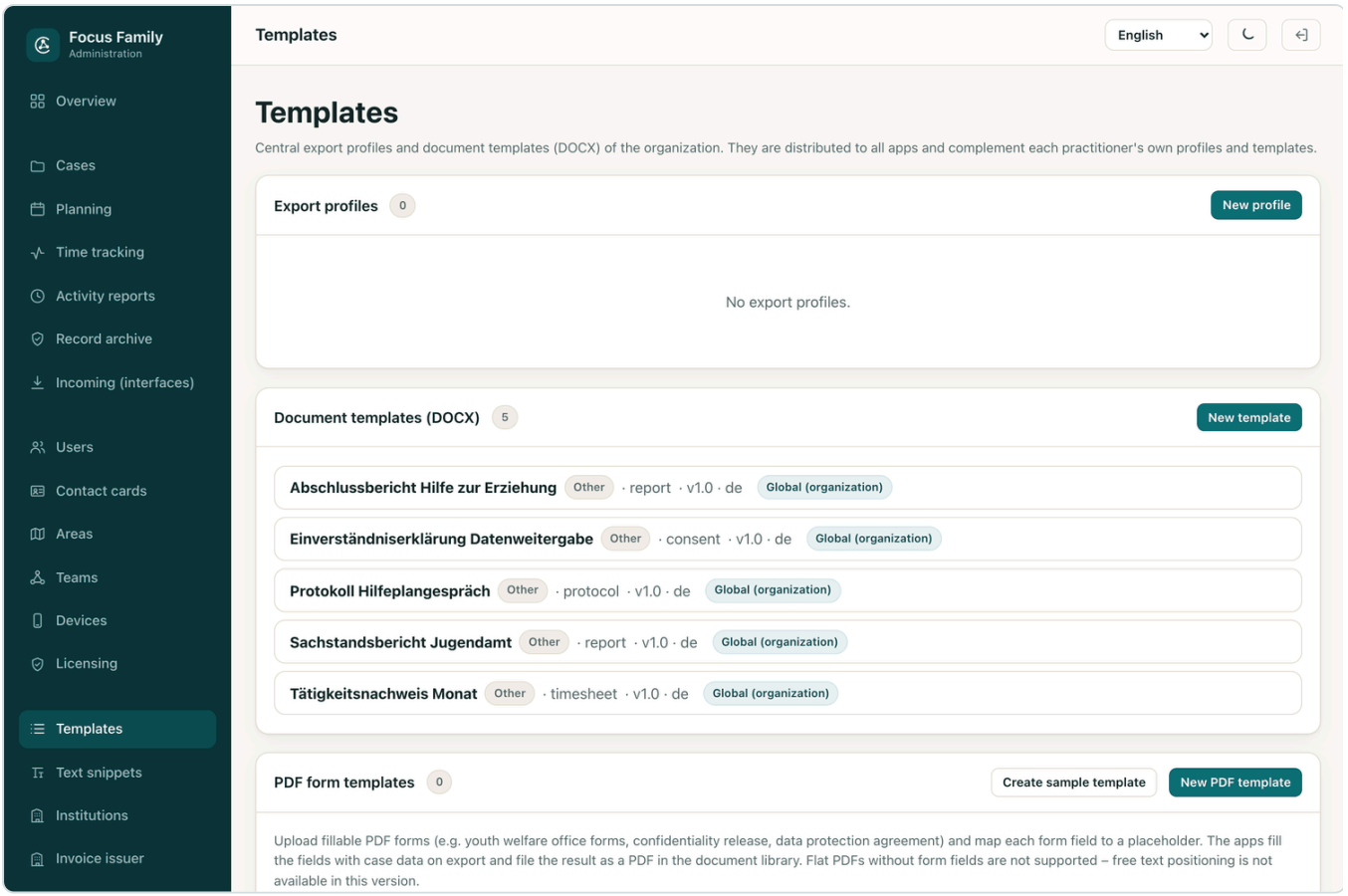
How the apps use the invoicing details:

- They are delivered **only to accounts holding the app permission *Create e-invoices*** – not through managed settings, which reach every device. The apps cache them encrypted, refresh them on every sync and delete them as soon as the permission is missing, the details were removed here or the device is disconnected from the server.
- In connected apps the local issuer settings are hidden; they can be neither viewed nor changed there.
- Without the permission the e-invoice button is hidden and the app shows "A permission is required for e-invoices." If no details have been entered here yet, the app reports "Invoicing details have not been set up yet."
- The prefix applies to all devices. Invoice numbers are unique across the organisation, even without a connection at creation time: on its first fetch of the invoicing details the server assigns each device a fixed **number series** (never reused, not even after a device is removed). Format: prefix + series (at least two digits) + `-` + four-digit counter, e.g. `TR-07-0001`, with the default prefix `RE-2026-07-0001`. The invoice number is assigned automatically from the device's series and cannot be edited by hand ("The invoice number is assigned automatically."). The device keeps the counter and the issued numbers encrypted; a number only counts as issued after a successful export – a cancelled or failed export does not use up a number. Before every export the app checks that the number belongs to its own series and has not been issued in that series before; an issued number is never reused, not even after a restart or when returning to an earlier series. The counter only moves forward and restarts at 1 only with a new series (e.g. after re-registration). Without an assigned series no e-invoices can be created ("Invoicing details have not been set up yet."). Permission and invoicing details are re-checked immediately before every export. VAT treatment still comes from the **billing basis**.

On the update from 1.0.0 all existing professional admins receive both new permissions; all other accounts get them as needed through the permission checklist (row "E-invoices").

Templates and export profiles

Menu item **Templates** (permission *Manage templates & export profiles*).



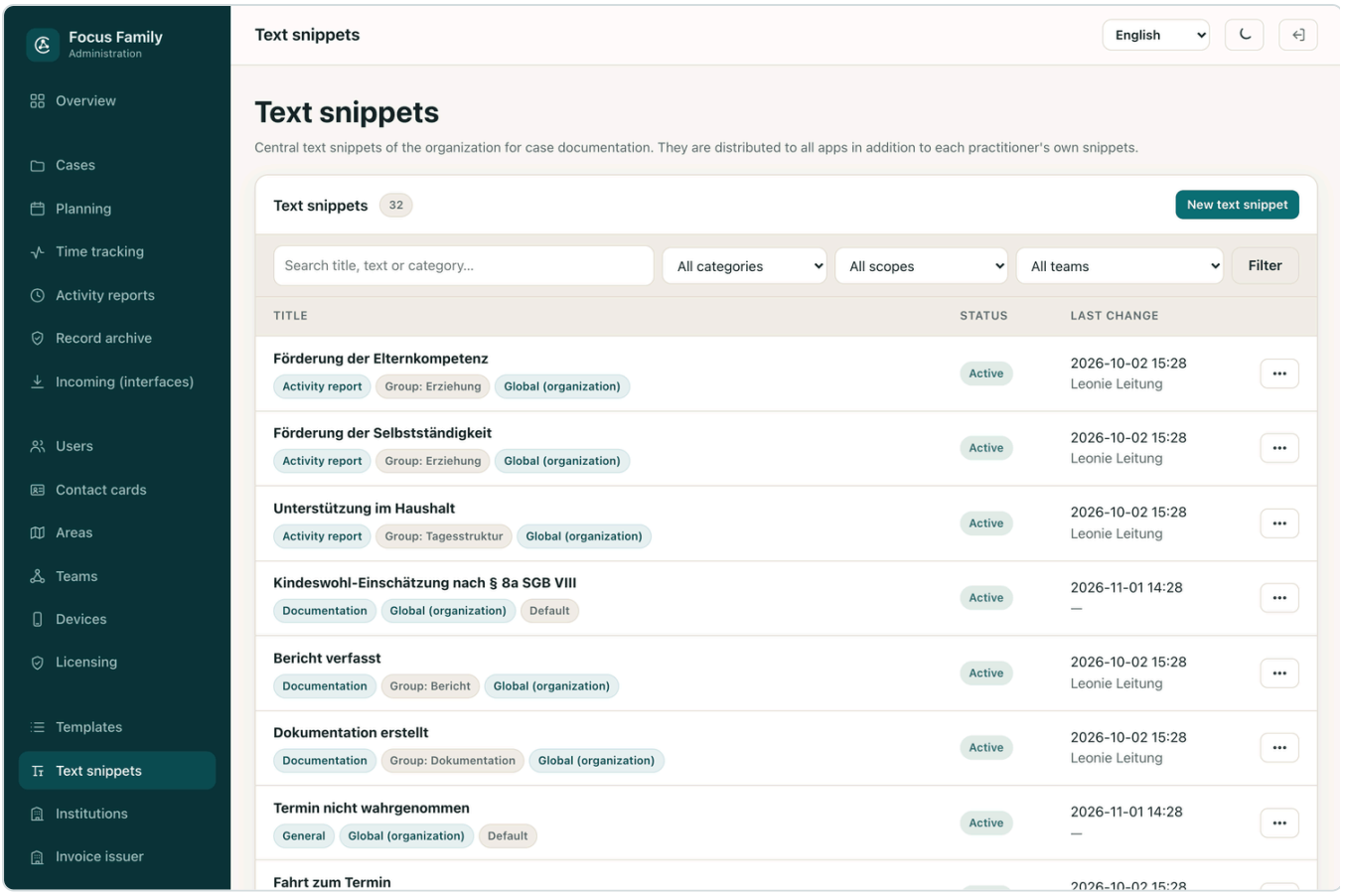
Central export profiles and Word templates are distributed to all apps.

- **Export profiles** – defaults for exporting: formats, cover page, logo, signature fields and data minimisation ("pseudonymise names", "remove address").
- **Document templates (DOCX)** – Word templates with placeholders, at most 5 MB each.
- **PDF forms** – fillable forms of your organisation that practitioners can complete on the device inside the case file. PDF files with permission restrictions (such as official forms that open without a password) are supported; PDF files that need a password to open are rejected on upload with a notice.

These central defaults are a **basis**; practitioners can still use their own profiles and templates.

Text snippets

Menu item **Text snippets** (permissions *View* / *create* / *manage text snippets*).



Snippets at organisation, team and personal level, with categories and built-in defaults.

Text snippets are reusable pieces of text for documentation and activity records. They are distributed to all apps and appear there in addition to the practitioners' own snippets.

- **New text snippet** creates one; **edit** adjusts it; **deactivate** takes it out of circulation.
- There are **organisation**, **team** and **personal** levels. Personal snippets belong to the practitioner and can only be changed by them.
- The server ships with **default text snippets** so you do not start from zero. They can be adjusted or deactivated.
- **Titles are unique:** within the organisation, a team and a practitioner's personal snippets every title may appear only once; letter case and extra spaces do not count as a difference. Organisation and team snippets may not share a title. **Duplicate** assigns consecutive titles ("(copy)", "(copy) 2" …). Titles that already occur twice are flagged in the list with **"Duplicate title – please rename"**; in the apps, snippets with the same title show their origin, e.g. "Greeting · Organisation".

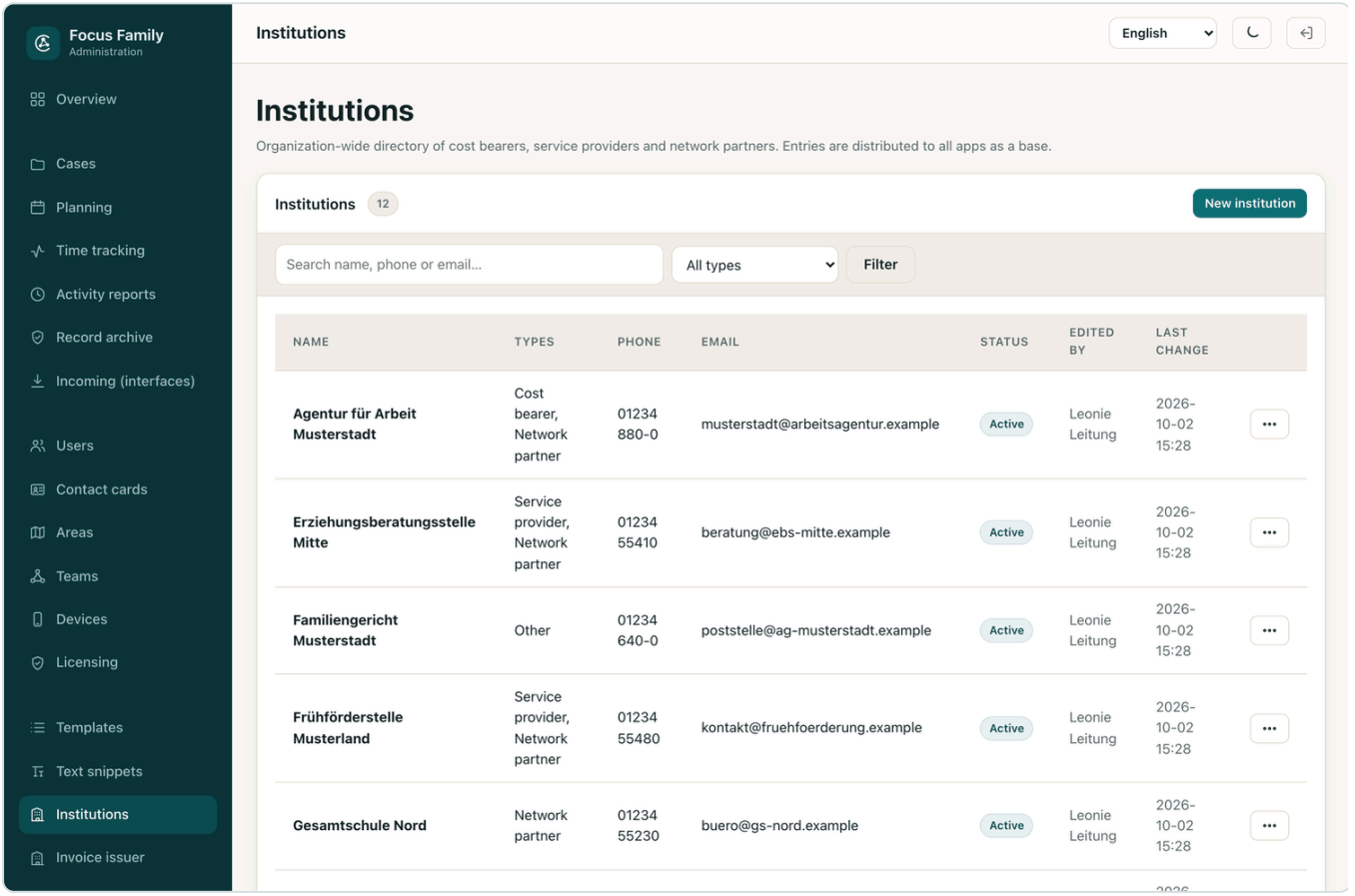
Catalogues: institutions, measures, activity types

Three catalogues make sure all practitioners use the same terms.

In all three catalogues the ⋯ menu of a row offers **edit**, **deactivate/activate** and **delete**. **Deactivate** removes an entry from selection but keeps it in the list; **delete** removes it for good. Activity types used in time entries or rate items cannot be deleted, only deactivated – devices keep them for existing entries. When a search or filter is active, **Reset filters** returns to the unfiltered list.

Addresses are checked: the country is a two-letter code (e.g. DE, AT), the postal code matches the country (Germany: five digits), a street needs a postal code and town, a house number needs a street. The same check applies to persons, addresses and contact cards.

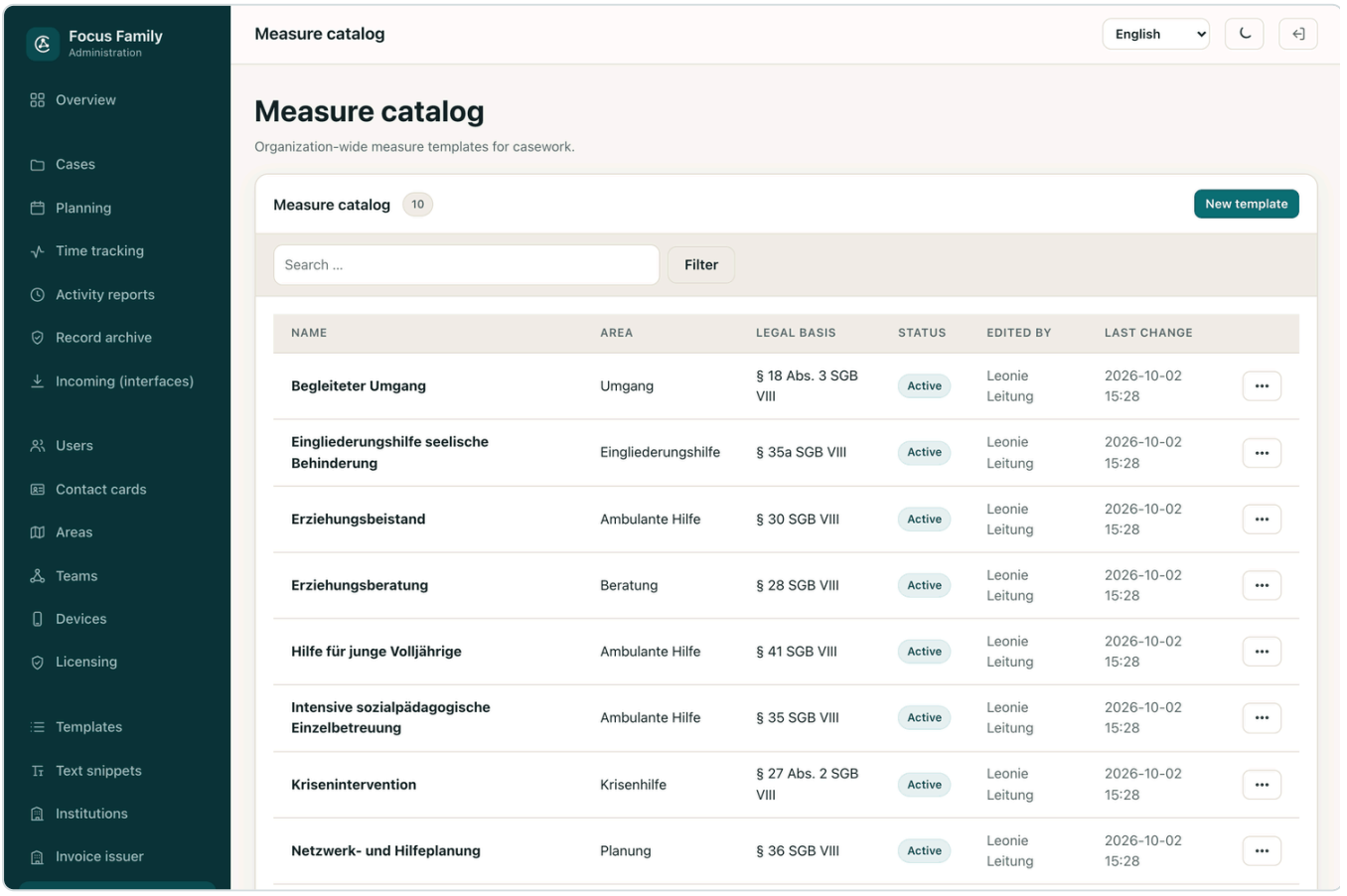
Institutions



Youth welfare offices, schools, day-care centres, counselling services and funding bodies maintained centrally.

The menu item **Institutions** holds the organisations you work with – with type, address and contact details. In the app they are offered when creating cases and network contacts.

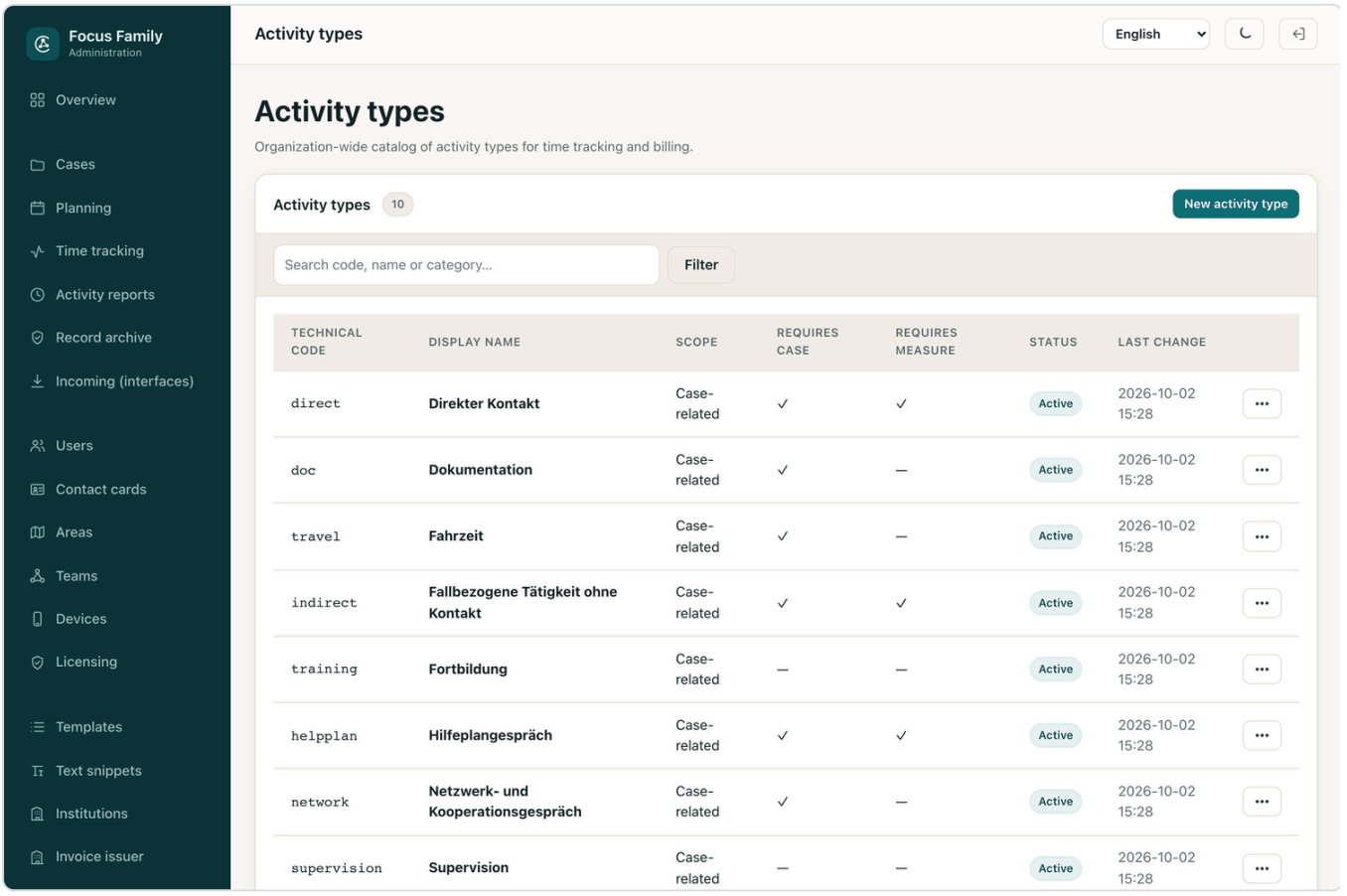
Measure catalogue



The types of support and services of your organisation – the basis for cases and billing.

The **measure catalogue** contains your organisation's types of support and services with name, abbreviation and the details needed for records and billing.

Activity types



Activity types govern how time is recorded and counted in the activity record.

Activity types determine which categories appear in time tracking – such as client contact (in person), travel time, documentation or phone calls – and whether an activity counts as **direct contact** or **indirect**. The activity record uses this to calculate the contact ratio.

Calendars & commitments in the case

When a practitioner reads in a shared calendar of a participant or records appointments that happen without them, it shows up on the case detail page under **Calendars & commitments**: per calendar the person, when it was read and how many entries it holds, below that the commitments with date, window and origin (recorded by hand or from a calendar). The section only appears when there are entries and requires the right to view the calendar.

Contact cards and cover arrangements

Menu item **Contact cards** – practitioners without extra permissions see it as **My contact details**.

This is the source of what practitioners hand to families in the app: their own availability and that of their cover.

Who may do what?

- **Every practitioner** maintains their **own** contact card – in the panel, in the app and on the desktop. No permission is needed for that.
- The permission *manage other practitioners' cards & cover arrangements* (part of **Fach-Admin**) adds the provider details, everyone's cards and the cover arrangements.

Provider contact details

Maintained centrally once – provider/organisation, phone, email, web, address and an emergency contact. These details apply to **every** contact card unless the practitioner fills in that field themselves. The switch **practitioners may edit their own contact card in the app** decides whether self-service is allowed; with it off, the cards are read-only in the app and on the desktop and are maintained here only.

Practitioner contact cards

The table lists every active practitioner with role, phone, mobile, email, availability and whether the card may be passed on. **Edit** opens the full card:

- **role**, **department / team**, **provider / organisation**
- **phone (work)**, **mobile**, **email**, **web**
- **address** for postal matters
- **availability**: up to two windows per weekday plus a free note
- **in an emergency**, **note** and the **card may be passed on** switch

Empty fields inherit the provider details. A card without any way to make contact is not offered for sharing in the app at all.

Cover arrangements

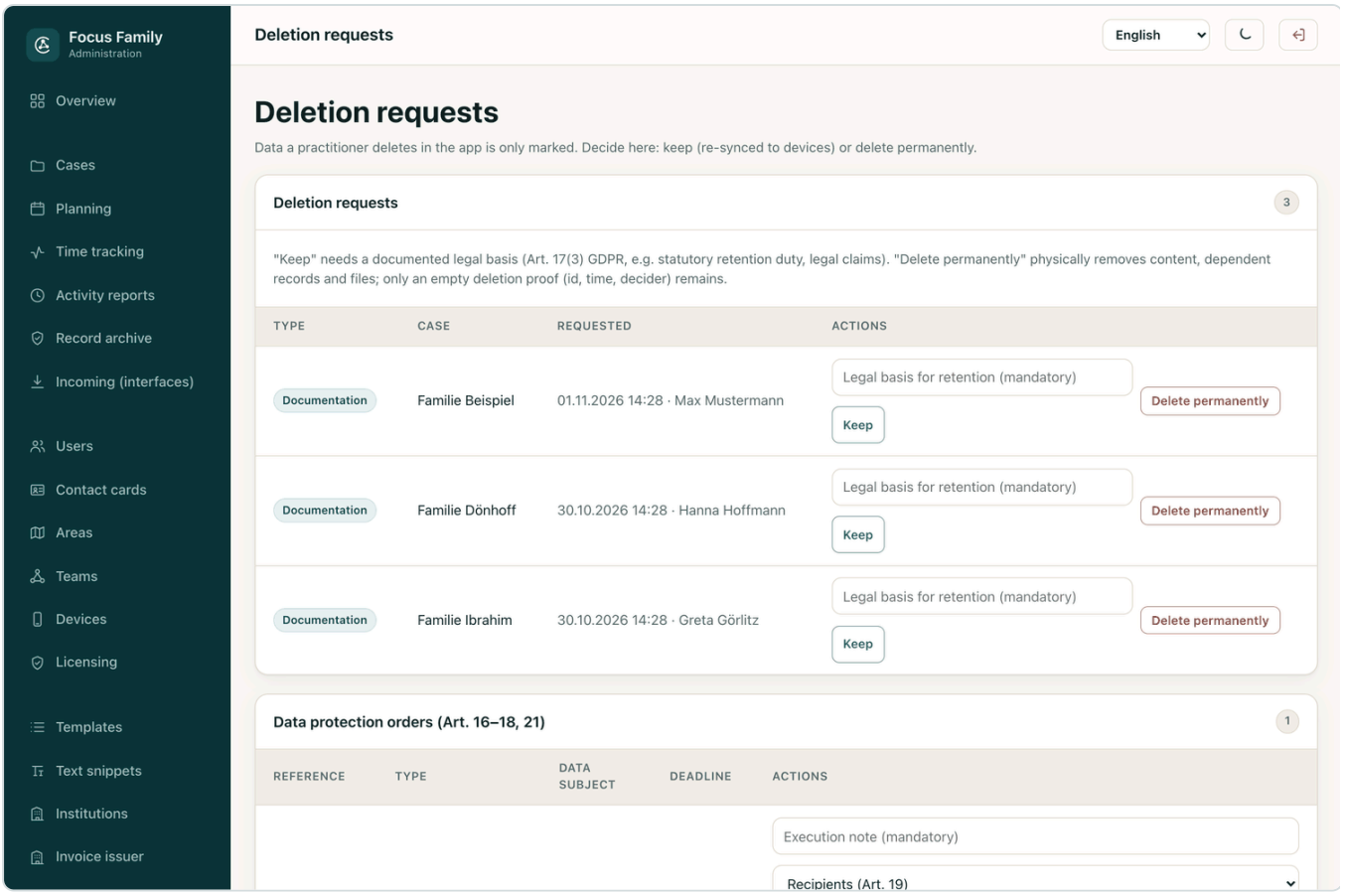
Add cover records who covers for whom and for how long, with an optional note (for example "annual leave"). The arrangement then shows up in the absent practitioner's app and can be passed on to families directly. Rules:

- Two different active practitioners; the period must lie in the future and cover at most one year.
- Overlapping arrangements for the same pair are refused.
- **End** stops a running arrangement immediately.
- The list also shows the **case delegations** made in the app. The **scope** column tells "whole organisation" apart from "case: …", and **end** works for both kinds. In the apps, case delegations only reach the practitioners of that case.

Every change to cards, provider details and cover arrangements is written to the audit log.

Deletion requests

Menu item **Deletion requests** (permission *Review deletion requests*).



Data deleted by practitioners is only marked at first and presented here for a decision.

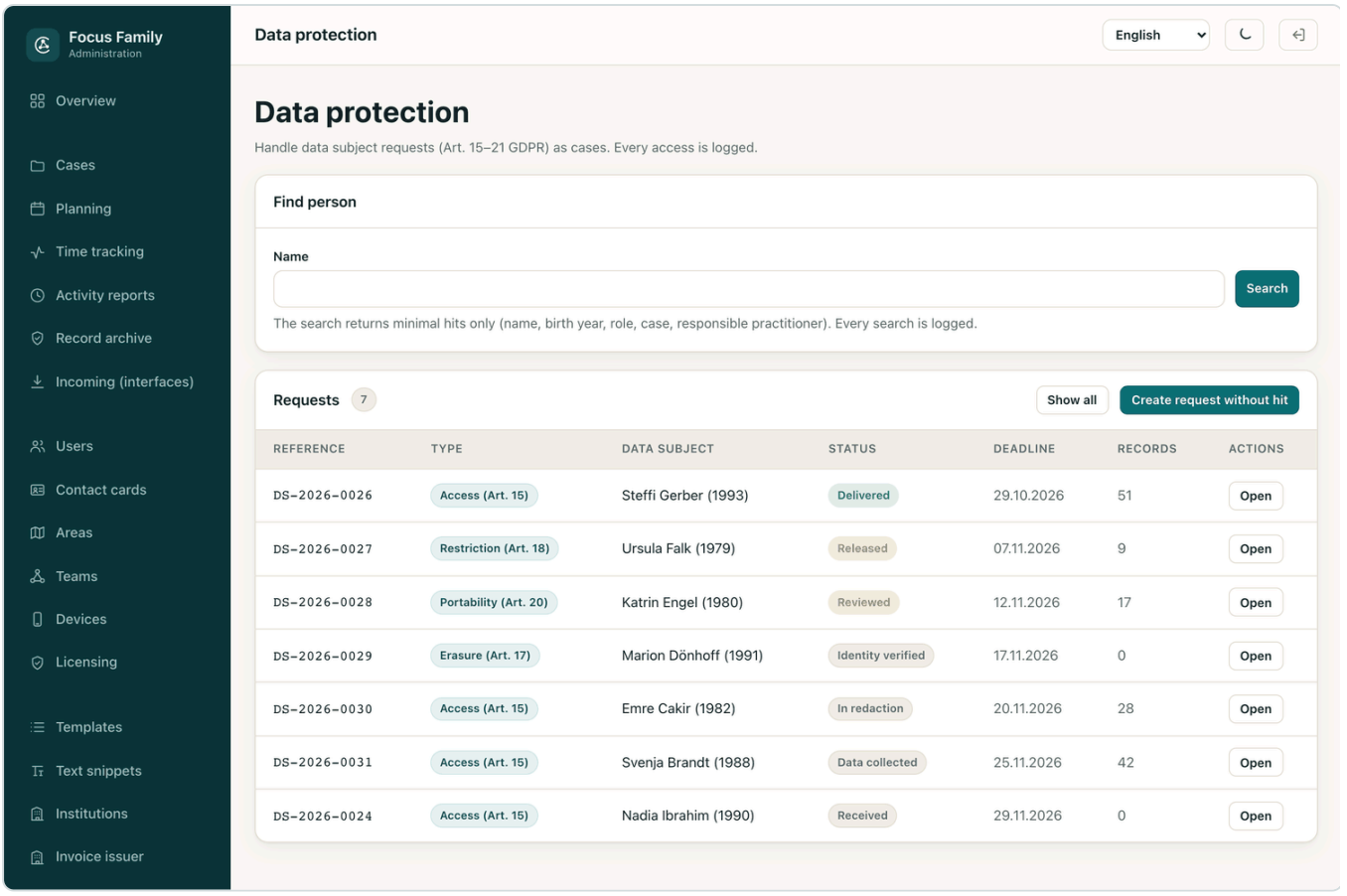
When a practitioner deletes data in the app, it is initially **only marked**. You decide per entry:

- **Keep** – the data remains and syncs back to the devices. You state the **legal basis** for keeping it (for example a statutory retention obligation or ongoing proceedings); it is stored with the record.
- **Delete permanently** – content, dependent records and files are removed **physically and irreversibly**; only an empty deletion receipt remains. For a case, the devices remove it at the next sync. A confirmation prompt appears.

The same page shows **restricted records** (Art. 18/21 GDPR). A restriction can only be lifted if you enter the **date and channel** of the prior information to the data subject and the **legal basis** for lifting it.

Data protection: subject requests and documents

The **data protection** area is for your data protection officer (DPO).



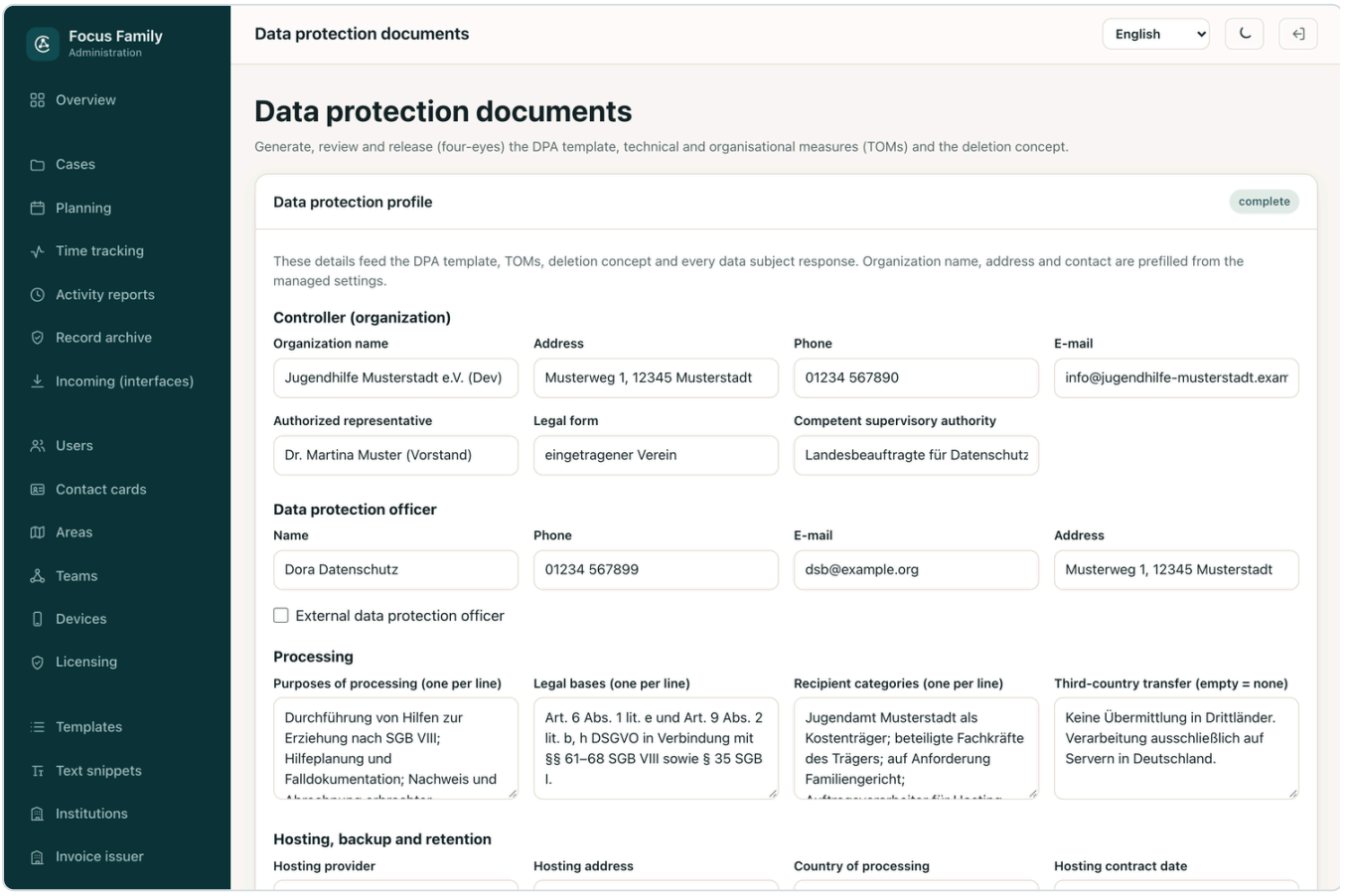
Cases for data subject rights – from identity verification through redaction to release.

Setting it up

Create the account with the type **data protection officer** and tick the permissions in the **data protection** block. Such an account **cannot sign in to the apps** unless it also holds professional permissions.

Because the final release is normally done by a **second person** (four-eyes principle), you need a second account with the permission **release (four eyes)**. Small organisations without a second person can switch the four-eyes principle off under **policies** – every step is still logged.

Before the first request: create the documents



The data protection profile plus the processing agreement template, technical and organisational measures and the deletion concept as draft, reviewed and final.

1. Open **data protection documents** and fill in the **data protection profile**: organisation, DPO contact, supervisory authority, purposes, legal bases, hosting and retention periods.
2. Generate the three documents: **processing agreement template**, **technical and organisational measures** and **deletion concept**.
3. Each document starts as a **draft** with a watermark, is marked as **reviewed** and is **finalised by a second person**. A new draft discards older, not yet finalised versions.

Only **final** versions are attached to subject access packages. If the documents no longer match the profile or the policies, the page shows "outdated" – a new finalisation is then required.

Handling a request

1. Open **data protection** and search for the person by name. You only see minimal matches (name, year of birth, role, case, responsible practitioner). **Create case** – the one-month deadline starts with the date of receipt you enter and can be extended once by two months for complex requests.
2. **Confirm identity** and record how you verified it.
3. **Collect data** – the panel assembles everything stored about that person. Other family members stay out of it.
4. **Redact** – open every record containing free text and remove details about third parties. The system marks possible mentions of other people; you decide: remove, exclude with a reason, or deliberately keep with a reason. Every view is logged.

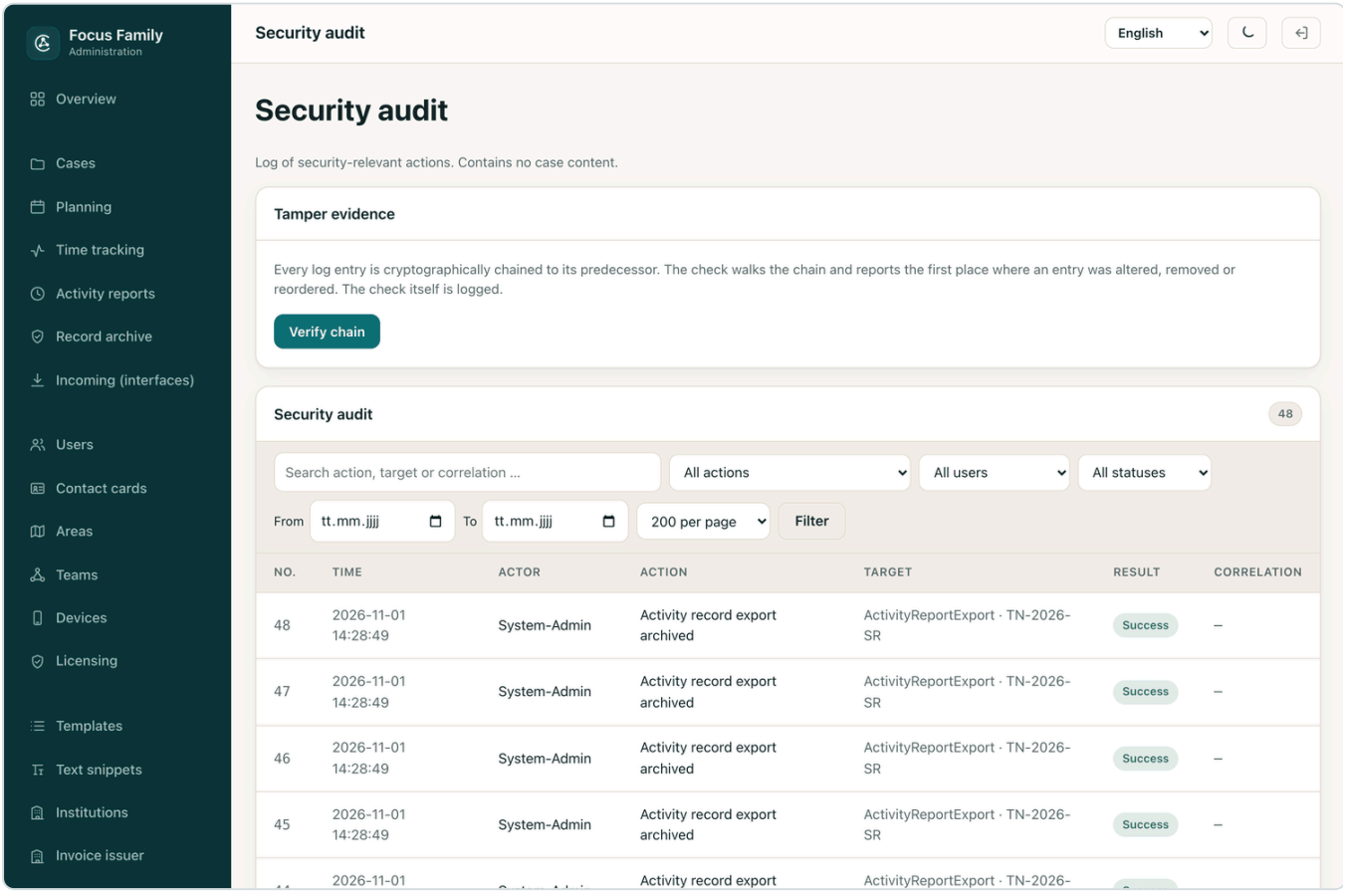
5. **Mark as reviewed** once the checklist is complete.
6. A **second person** releases it in the **release** tab. The panel produces the package (access information as PDF and DOCX, machine-readable JSON, the three documents and a checksum file) and shows the **password once**. Download the package immediately – the link works only once – and transmit the password **separately** (by phone or letter).
7. Mark the case as **handed over** and later as **closed**.

> Open the encrypted archive with 7-Zip, WinRAR, Keka or PeaZip – not with the built-in extractors of Windows and macOS.

Other data subject rights: restrictions (Art. 18) and upheld objections (Art. 21) immediately lock the selected records technically – no sync, no changes, storage remains. Rectifications (Art. 16) are carried out by professional administration on your instruction. A portability request (Art. 20) delivers the JSON export of the master data provided by the person themselves.

Security audit

Menu item **Security audit** (permission *View security audit*).



A log of security-relevant actions with time, action, target and result.

The audit records **who did what and when** – for example: user created, password reset, team member added or removed, case assigned, device approval changed, policy changed, emergency access opened or closed, storage cleaned, record closed or reopened, time entry changed by management.

> The audit contains **no case content**.

Crash reports and desktop downloads

Crash reports (permission *View crash reports*): after a crash an app can send a technical report to the server. You see the time, platform and technical details. Crash reports contain **no case data, names or notes**. With the permission *Manage crash reports* you remove reports immediately via **Delete report** (detail page) or **Delete all reports**; otherwise the server deletes them automatically after the configured retention period (default 90 days).

Download desktop app (permission *Download desktop app*): here you find the installer packages of the desktop application – **.pkg** for macOS (Apple Silicon and Intel) and the **MSI** installer for Windows (x64 and ARM64). Pass them on to your practitioners.

Data protection and the limits of the panel

- Administration sees **no private content**.
- **Technical administration** sees **no** cases and appointments.
- The panel is **administration, not case documentation**.
- Passwords are **never** shown in clear text; files are stored encrypted on the server.
- Security-relevant actions are traceable in the **audit**.

Frequently asked questions

A practitioner forgot their PIN. Open **Devices** and choose **Reset PIN lock** for that device. The lock is released at the next sync.

A practitioner lost their phone. Remove the device under **Devices** – this disconnects it and frees the licence seat. Reset MFA or passkeys if needed and issue a new setup QR.

Why can I not see a particular menu item? The navigation only shows what you are entitled to. Ask someone with the matching admin level to grant you the permission.

Why are entries missing from a record? Private entries are never included. Entries also only appear once the practitioner's device has synced.

A record shows the warning "data differs". Entries of the period arrived or changed after closing. Check them under **Time tracking** and decide whether the period needs to be reopened.

Can I lock out a practitioner remotely? Yes – deactivate the account under **Users** and/or block or remove their devices under **Devices**.

Who may remove MFA? Only accounts with the permission **Manage technical admins**.

Focus Family · Admin Panel Handbook · Version 1.3.0 · October 2026