



DENTALXPAND LEARNING CENTER / WORK HUB

Use the Support Hub, Complaints, and Help Tools

A detailed guide to the persistent Quick Hub, focused employee messaging, compact Xpand AI, safe screen snapshots, feedback and support submissions, full ticket tracking, anonymous identity boundaries, manager resolution, tenant enforcement, and safe troubleshooting.

VERSION	1.0	AUDIENCE	All authorized users, managers, and support administrators
FORMAT	Website + PDF	SCOPE	DentalXpand Quick Hub and Support Hub

Fictional screenshots and minimum-necessary support

Every screenshot uses fictional training data. Never place passwords, tokens, secret keys, patient records, copied client data, another practice, Guardian Connect data, or unrelated records into a ticket, message, AI prompt, or screen snapshot.

Contents

Select a section in supported PDF viewers. Use the Contents link in the upper-right corner of every content page to return here.

Choose the correct help surface inside the authorized workspace	3
Open, move, and recover the persistent launcher	4
Find an authorized coworker and open a focused chat	5
Ask for workflow help with only the minimum safe context	6
Choose channel, category, priority, content, and identity mode	7
Read summary counts, search, filter, expansion, and realtime updates correctly	8
Resolve or dismiss only with authorized role, purpose, and response	9
Keep convenience controls behind durable authorization	10
Recover expected failures without changing identity, policy, or data	11
Verify safe Support Hub use	12

How to use this guide

Confirm account, organization, practice, route, and service access first. Then use the smallest appropriate help surface, protect screenshot and ticket content, understand anonymous follow-up, track status, and complete only authorized management actions.

01 / PURPOSE AND ACCESS

Choose the correct help surface inside the authorized workspace

Surface	Reviewed purpose	Boundary
Quick Hub	Persistent launcher for Messages, Ask Xpand AI, Feedback, and unread notifications while using standard signed-in pages.	Hidden when signed out and not mounted in platform-only mode. Its presence does not grant every linked route or service.
Quick Messages	Search authorized employee identities and open a global chat popup for a linked user account.	Employee lookup, conversation access, and tenant scope remain enforced by their services and database policies.
Ask Xpand AI	Ask about the current workflow, select model and thinking level, and attach one optional screen image.	A model or route label does not expand authorization. The operator must review and minimize every prompt and screenshot.
Quick Feedback	Create a suggestion, support request, or issue with category, priority, subject, description, and optional anonymity.	Required fields and convenience controls do not replace tenant-bound insert policy or approved incident handling.
Full Support Hub	Create, search, filter, expand, track, resolve, or dismiss support tickets according to role.	The /support route requires page permission. Database row policy must enforce equal or stricter user, role, and tenant access.

Stop at unexpected data
If another person, organization, practice, Guardian Connect workspace, or unrelated record appears, stop. Do not search, expand, message, screenshot, copy, or test more records. Report minimum non-sensitive context.

Open Support Hub	Roles and access	Organization context
Open Support Hub	Roles and access	Organization context

02 / QUICK HUB

Open, move, and recover the persistent launcher

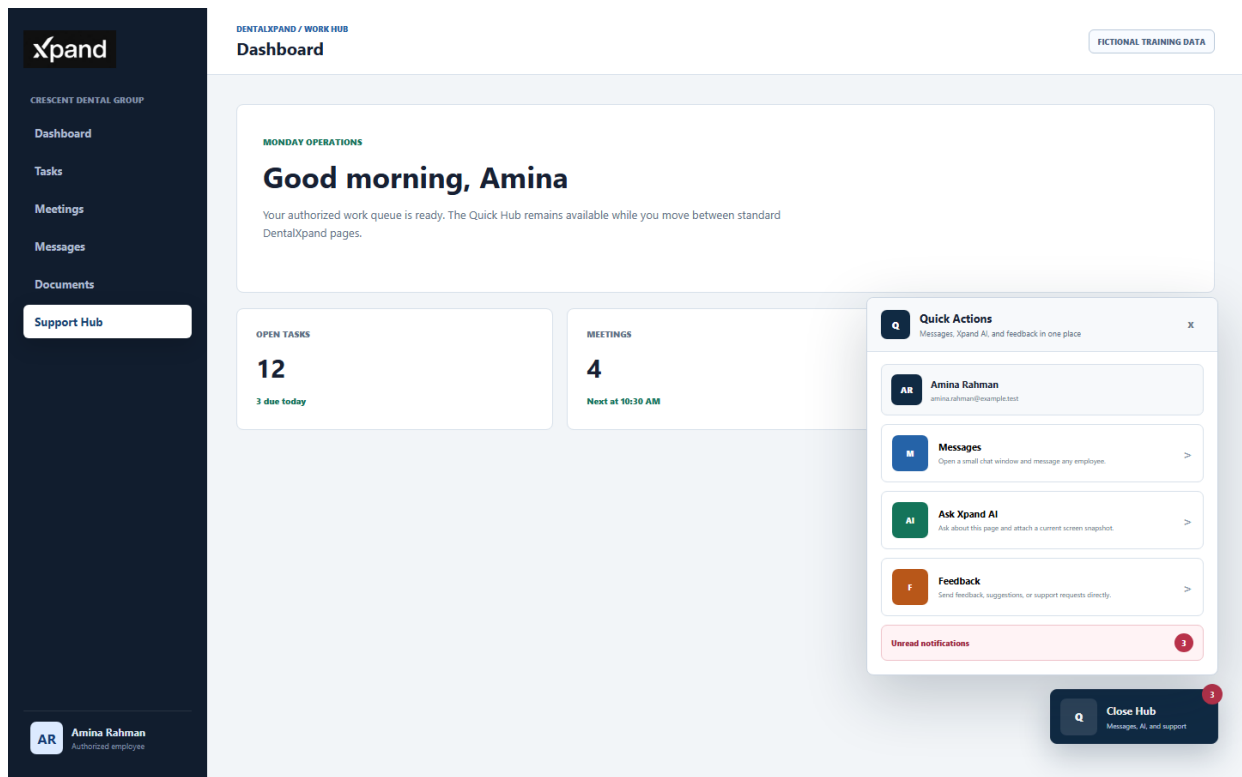


Figure 1. Fictional standard workspace with the Quick Hub launcher, operator identity, Messages, Ask Xpand AI, Feedback, and unread notification actions.

Action	Current behavior	Safe practice
Open or close	Click toggles the panel; opening returns to Quick Actions. Route changes close the panel and reset it to the menu.	Use the main menu rather than manipulating component or route state.
Drag	Pointer movement above the click threshold repositions the launcher and saves corrected coordinates.	Place it where it remains visible and does not cover required controls. Do not drag while trying to click.
Resize	Saved coordinates are clamped on load and resize with a screen margin and larger bottom safe area.	Resize once if the launcher appears too low or offscreen. Do not edit browser storage to impersonate access.
Mobile	Small screens use a 56-pixel compact button instead of the 196-pixel desktop pill.	Expect reduced label detail, but the same authorized actions and boundaries apply.
Unread badge	A count appears on the launcher and menu only when unread notifications are greater than zero.	Open Notifications for complete alert handling and read-state controls.

03 / QUICK MESSAGES

Find an authorized coworker and open a focused chat

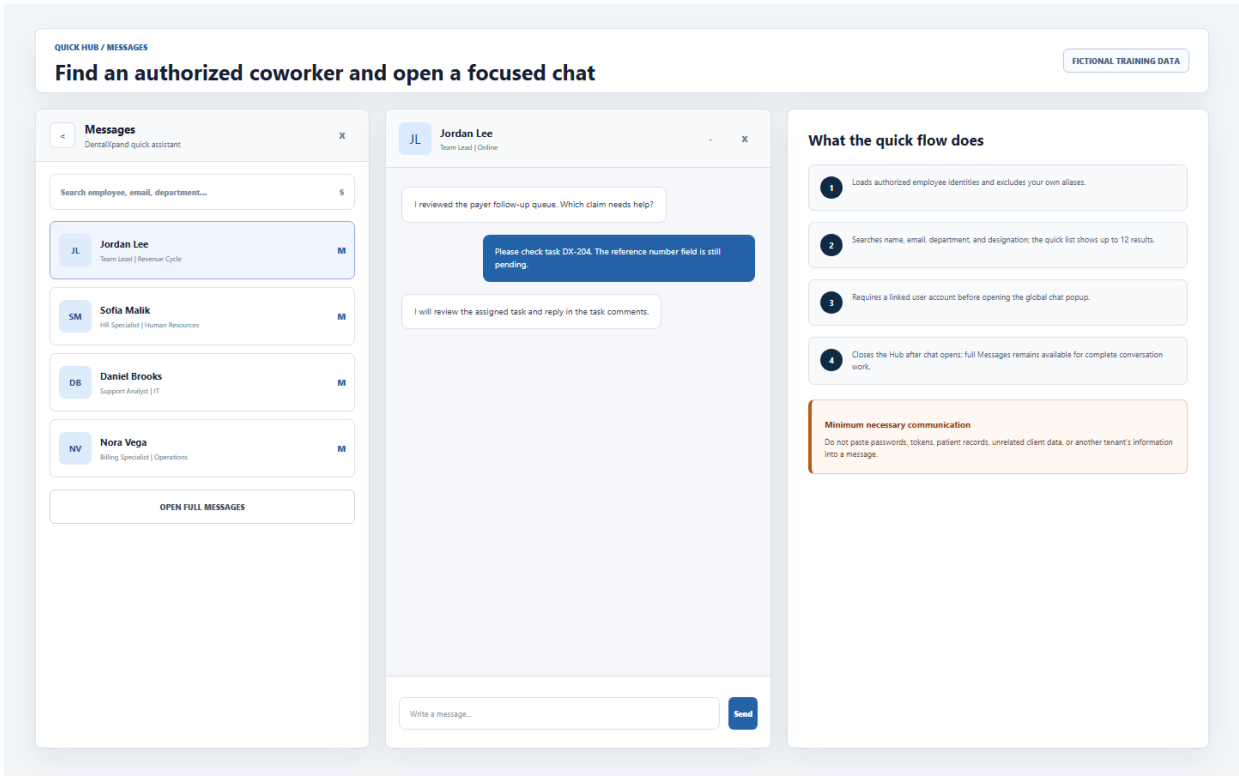


Figure 2. Fictional Quick Messages employee search, selected coworker, global chat popup, full Messages link, and communication boundary.

Step	Reviewed behavior	Required discipline
Load users	The panel requests employee identities and current-user aliases, then excludes the signed-in user's own accounts.	Use only identities returned in the current authorized scope. Do not enumerate or query employee IDs directly.
Search	Name, email, department, and designation are matched; the quick list displays up to 12 results.	Search only for a legitimate assignment and the minimum person needed.
Select	A linked user_id is required before the global chat popup can open.	If no user account exists, request an authorized mapping review. Never borrow or substitute another account.
Use popup	The Hub closes and the requested conversation opens or restores in the global popup.	Keep the exchange focused; never paste credentials, patient data, unrelated client records, or exposed cross-tenant content.
Open full Messages	Navigates to /messages for complete conversation work.	Use full Messages for history, search, group conversations, attachments, voice notes, mentions, and unread state.

Open Messages	Messages lesson	Support guide
Open Messages	Messages lesson	Support guide

04 / XPAND AI AND SCREEN CAPTURE

Ask for workflow help with only the minimum safe context

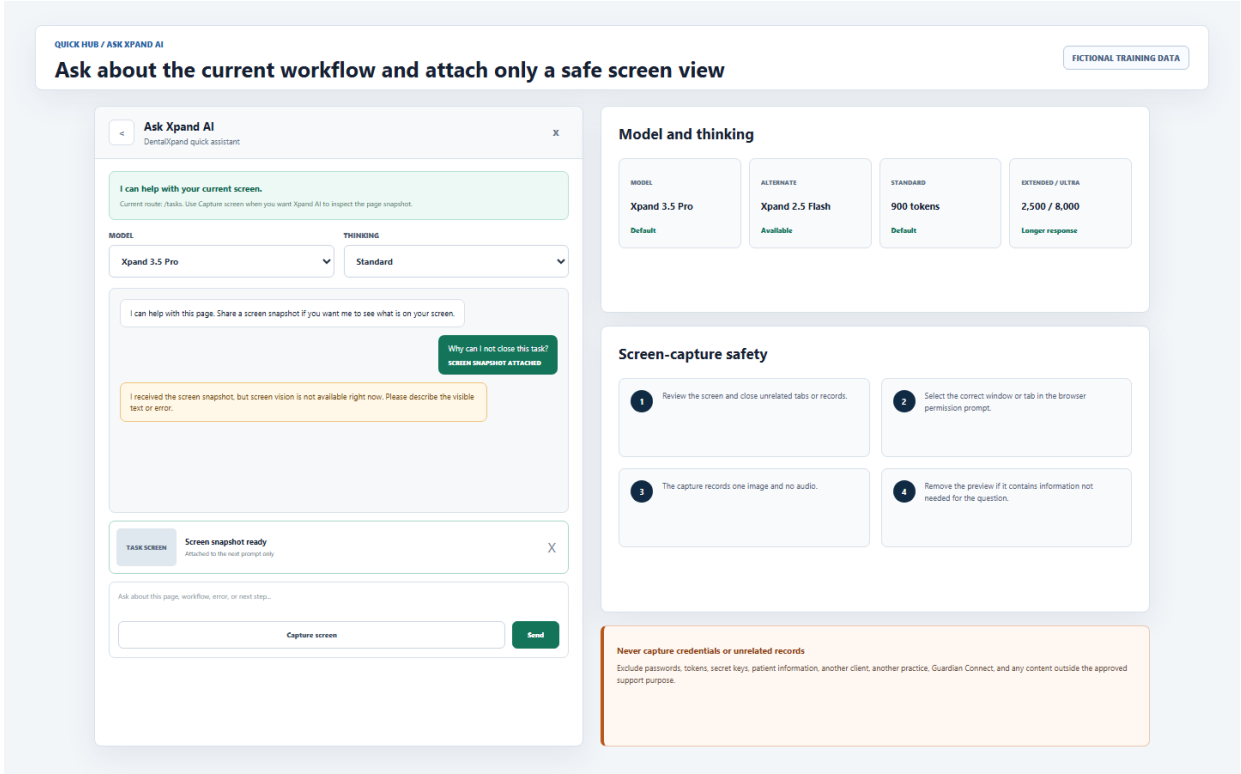


Figure 3. Fictional compact Xpand AI panel with current route, model and thinking controls, prompt, screenshot preview, vision fallback, and capture-safety guidance.

Control	Current behavior	Boundary
Model	Xpand 3.5 Pro is default; Xpand 2.5 Flash is available as an alternate.	Model choice does not change role, organization, practice, source access, or permission.
Thinking	Standard, Extended, and Ultra request about 900, 2,500, and 8,000 maximum response tokens.	Longer output does not justify adding more sensitive input.
Prompt	Enter sends and Shift+Enter adds a line. A prompt or attached snapshot is required.	Describe the exact button, field, safe ID, expected result, actual result, and non-sensitive error.
Capture	The browser selects a display source, records one PNG image without audio, and shows a removable preview.	Close unrelated records first, select the correct window or tab, review the preview, and remove it when too broad.
Vision warning	When extraction or vision is unavailable, the assistant confirms receipt and asks for visible text or a description.	Type the safe text. Do not keep attaching larger screenshots.

Never capture credentials or unrelated records

Exclude passwords, codes, tokens, keys, patient information, claim or eligibility records, another client or practice, Guardian Connect, private messages, inboxes, and screens outside the approved support purpose.

05 / SUPPORT SUBMISSIONS

Choose channel, category, priority, content, and identity mode

SUPPORT / NEW SUBMISSION

Choose the right channel, category, priority, and identity mode

FICTIONAL TRAINING DATA

QUICK HUB FEEDBACK

Fast submission

Suggestion

Support

Issue

CATEGORY

IT

PRIORITY

High

SUBJECT

Task status button is unavailable

DESCRIPTION

On task DX-204, the status control remains disabled after every required step is complete.

SUBMIT ANONYMOUSLY

NO

SUPPORT PAGE

SUBMIT

FULL SUPPORT PAGE

New Support Submission

Complaint

Suggestion

Support

DEPARTMENT UNIT

General Intelligence

SUBMIT ANONYMOUSLY

YES

PRIORITY LEVEL

Low

Medium

High

Urgent

SUBJECT

Workspace notification behavior

DESCRIPTION

Please review the notification sequence described here. No patient or client details are included.

CANCEL

SUBMIT TICKET

Use the fields deliberately

Complaint / Issue

Report a workplace or product problem that needs review.

Suggestion

Submit an improvement idea with expected benefit and context.

Support

Request help with an authorized Dentalxpand workflow.

Priority

Use urgent only when the issue truly needs immediate operational attention.

Anonymous

Identity linkage is removed from the ticket. Do not identify yourself inside subject or description.

Figure 4. Fictional Quick Feedback and full Support Submission forms with channels, category, priority, safe subject and description, and anonymous identity mode.

Field	Quick Feedback	Full Support Hub	Selection rule
Default channel	Suggestion	Complaint	Use Complaint or Issue for a problem, Suggestion for an improvement idea, and Support for help.
Category	General, IT, HR, Billing, Operations	General, HR, IT, Facility, Finance	Choose the closest owning unit; never add unrelated records to explain routing.
Priority	Low, Medium, High, Urgent; Medium default	Low, Medium, High, Urgent; Medium default	Use Urgent only for real immediate impact; follow the incident route when required.
Subject	Required	Required	Name the page or workflow and safe symptom without credentials or protected data.
Description	Required	Required	Include time, expected and actual behavior, safe ID, attempts, and exact non-sensitive error.
Anonymous	Checkbox	Toggle	Current create flow stores no employee ID. Do not identify yourself inside the text when anonymity matters.

DentalXpand Learning Center

Page 7

06 / TRACK THE SUPPORT QUEUE

Read summary counts, search, filter, expansion, and realtime updates correctly

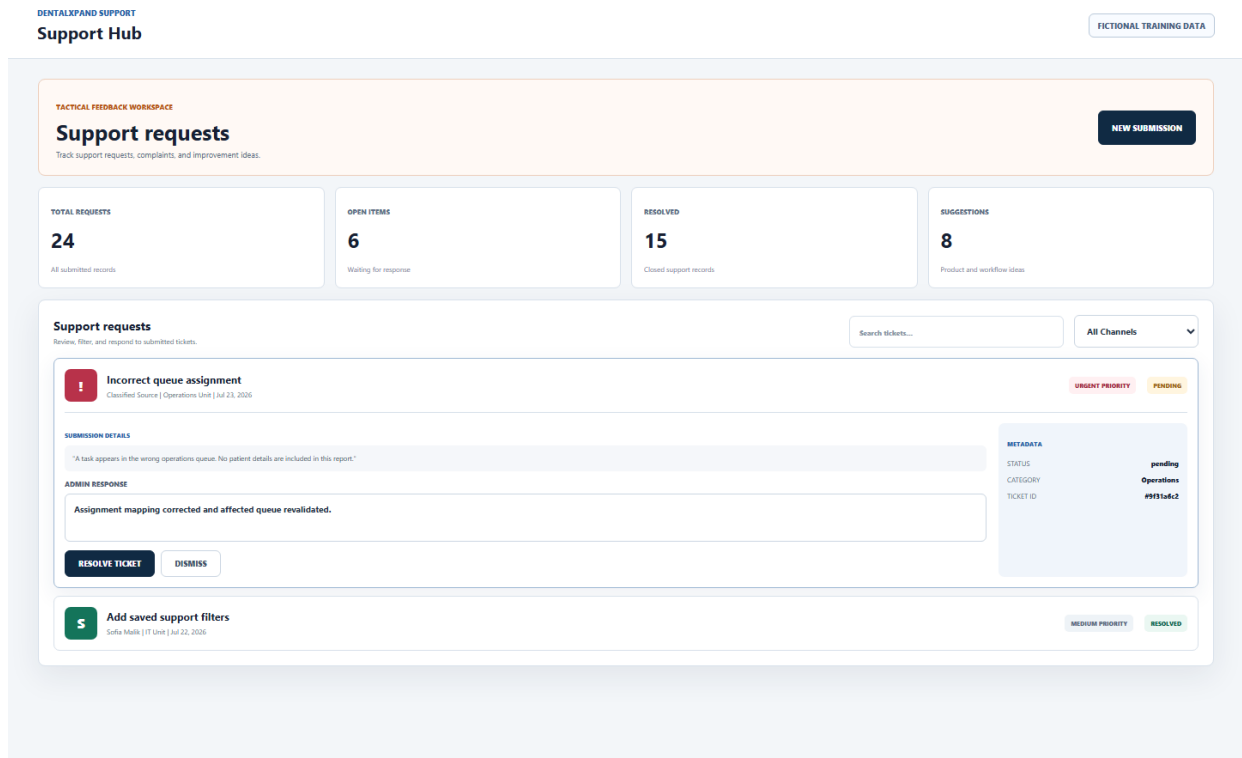


Figure 5. Fictional Support Hub queue with summary metrics, search, channel filter, expanded anonymous ticket, metadata, manager response, Resolve, Dismiss, and a resolved item.

Control	Reviewed behavior	Interpretation
Total	Counts rows returned to the current page.	It reflects the authorized query result, not automatically every ticket in the organization.
Open	Counts status exactly equal to pending.	The card response UI also treats under_review as actionable, but the current open summary does not count it.
Resolved	Counts resolved rows; dismissed rows are separate.	Read status and official resolution rather than inferring outcome from total counts.
Suggestions	Counts suggestion type across returned statuses.	The count is not limited to open ideas.
Search and filter	Matches subject, description, or linked employee name and filters complaint, suggestion, or support type.	Use only for a legitimate support purpose. Anonymous records display Classified Source.
Expand	Shows description, resolution, resolver, dates, status, category, and shortened ticket ID when available.	Open only the record required for assigned work; do not browse private complaints or infer anonymous identity.
Realtime	Complaint and employee-table events silently refresh the queue.	Re-read the current status before duplicating work or submitting a resolution.

07 / MANAGER RESOLUTION

Resolve or dismiss only with authorized role, purpose, and response

Step	Reviewed page behavior	Required control
Confirm access	Admin, super admin, or manager application roles see response actions for pending or under-review records.	Visible controls are not final authorization; route, service, policy, tenant, and management purpose must agree.
Review	The expanded record exposes description and metadata; a prior official resolution can also appear.	Use minimum necessary access. Do not correlate an anonymous source or expose private workplace details.
Write response	Resolve and Dismiss remain disabled until resolution text is entered.	State verified action, outcome, owner, and safe next step without investigation secrets, patient data, or unrelated employee information.
Resolve	Stores resolved status, response, current resolver employee ID, resolved time, and updated time.	Use only after a verified disposition or completed action.
Dismiss	Stores dismissed status with the entered response and resolution metadata.	Use only under approved dismissal policy and explain the alternate route when applicable.
Confirm	The page refreshes and can also receive realtime updates.	Verify the status and official resolution; do not repeatedly click while the first request is processing.

Anonymous identity must remain protected

Do not search messages, timing, employee activity, network logs, or other systems to guess who created an anonymous support record unless a formally approved legal or security process requires and authorizes it.

08 / PRIVACY AND TENANT ENFORCEMENT

Keep convenience controls behind durable authorization

SUPPORT / ACCESS, PRIVACY, AND TROUBLESHOOTING
Request help without bypassing account, tenant, or data boundaries
FICTITONAL TRAINING DATA

A
AUTHORIZED CONTEXT
Every support action stays scoped

Signed in account
Organization
Practice
Page permission
Ticket or message

The Quick Hub is a convenient entry point, not an access override. Route permissions, service authorization, database row policy, storage rules, and product isolation must still agree.

R
MINIMUM NECESSARY
Safe ticket content

Include
Page, time, expected result, actual behavior, safe ticket or task ID, and exact non-sensitive error.

Exclude
Passwords, tokens, secret keys, patient data, copied records, signed URLs, and unredacted client details.

Anonymous is not invisible everywhere
The current ticket removes employee linkage. Network, server, audit, and test metadata may still exist; never identify yourself inside the description when anonymously matters.

1
SAFE FIRST RESPONSE
Troubleshoot without bypassing controls

Quick Hub is missing
Confirm you are signed in and using the standard workspace. Review errors do not alter browser storage to improve access.

Button is offscreen
Resize the window so the saved position is changed. Do not edit local storage coordinates unless an authorized technical owner directs it.

Employee cannot open chat
The person may lack a linked user account or may not be returned to your authorized scope. Use full Messages or ask an administrator.

Submission fails
Keep the exact safe error, verify required fields and connectivity, then retry once. Do not disable SSL or insert ticket once manually.

Wrong tenant or product data appears
Stop immediately. Do not investigate with more searches, screenshots, messages, or ticket expansions.

Cross-tenant, cross-practice, or Guardian Connect data is an incident
Stop exposure and report only minimum non-sensitive content through the approved incident route. Do not attach the exposed record or repeat its contents in a ticket, message, or AI prompt.

Figure 6. Fictional support scope, safe-content, anonymity, troubleshooting, and cross-product incident workflow.

Layer	Reviewed implementation	Production requirement
Hub visibility	Signed-in standard-workspace UI check.	Does not grant linked route, employee, ticket, AI source, notification, or management access.
Employee lookup	Client excludes current aliases and requires a linked user ID.	Service and database must return only identities authorized for the active account, organization, practice, and role.
Ticket list	Regular application users add current employee_id; admin and manager roles request a broader list.	Row-level security must enforce equal or stricter tenant and role boundaries. Client filters cannot secure broad data.
Ticket insert	Named records resolve employee ID; anonymous records store null; status is forced to pending.	Authenticated tenant-bound insert policy must constrain accepted rows and fields. Never insert manually.
Resolution	Role-based UI controls call an update service that stores resolver and timestamps.	Backend and row policy must enforce management authorization; hidden buttons are not a security boundary.
AI image	One screen PNG can accompany the next compact assistant request.	The operator must minimize content. Route label and model choice do not protect an incorrect attachment.
Product isolation	Support tools belong to DentalXpand.	Guardian Connect data must never appear in DentalXpand support, messages, AI, or screenshots, and vice versa.

09 / TROUBLESHOOT

Recover expected failures without changing identity, policy, or data

What you see	Possible reason	Correct first response
Quick Hub missing	Signed out, platform-only mode, or global layout problem.	Confirm your own session and standard workspace, then refresh once. Do not alter auth or role state.
Launcher offscreen	Old saved coordinates or viewport change.	Resize once so supported clamping runs; report viewport and symptom if it remains missing.
Employees unavailable	Message service, aliases, mapping, tenant policy, or connectivity failed.	Try full Messages if authorized and report the safe error. Do not query employee IDs directly.
Chat will not open	Selected employee has no linked user account or is outside current scope.	Request an authorized mapping review; never substitute another account.
Capture fails	Browser support, permission, or selected source problem.	Use a supported browser or type safe visible text; never capture the broader desktop as a workaround.
Vision unavailable	Backend screenshot extraction is unavailable.	Describe exact non-sensitive text; do not attach repeated or broader images.
Submission fails	Required field, mapping, schema, connectivity, or row policy rejected the request.	Keep the safe error, verify fields, retry once, then escalate. Never disable RLS or insert rows manually.
Anonymous ticket absent	The ticket has no employee link and regular retrieval filters by current employee ID.	Use the approved anonymous follow-up path; do not reveal identity or submit duplicates.
Resolve action missing	Role, status, route permission, or deployed policy does not authorize it.	Respect the response and escalate to the assigned manager; do not change role or status values.
Wrong tenant or product	Session, mapping, query, row policy, cache, deployment, or isolation failure.	Stop immediately and report minimum non-sensitive context without investigating further.

10 / COMPLETION

Verify safe Support Hub use

- I can distinguish the Quick Hub, Quick Messages, Ask Xpand AI, Quick Feedback, full Support Hub, Notifications, and their owning records.
- I confirm my own account, standard workspace, organization, practice, route permission, and related service access before sending or reading support content.
- I can open, close, drag, and recover the Quick Hub without changing identity, role, route, or browser storage to force access.
- I search only authorized coworkers, require a linked user account, use focused popup chat, and move complete work to full Messages.
- I choose the appropriate Xpand model and thinking level and attach only one reviewed minimum-necessary screen image.
- I choose the correct channel, category, and honest priority and write an actionable subject and description without protected data.
- I understand anonymous submission removes the current employee link but does not guarantee absence of technical metadata.
- I know an anonymous ticket may not appear in a regular user's employee-filtered list and I use the approved follow-up route.
- I use search, filters, expansion, status, resolution, and realtime refresh only for a legitimate support purpose.
- I resolve or dismiss only with authorized management access and a complete non-sensitive response.
- I never include credentials, patient data, unrelated client records, signed URLs, another tenant, or Guardian Connect content in support tools.
- I never fix errors by changing IDs, borrowing accounts, editing role or status, disabling RLS, inserting rows, or investigating exposed data.
- I stop and report wrong-person, cross-tenant, cross-practice, or cross-product data without opening or copying more information.

Continue safely

The Work Hub foundation is now complete. Continue with the Provider and DSO learning track, beginning with managing providers and clients, while preserving the same account, tenant, permission, and minimum-necessary rules.

Website guide	Open Support Hub	All resources
Website guide	Open Support Hub	All resources