



DENTALXPAND LEARNING CENTER / WORK HUB

Manage Notifications, Reminders, and Push Alerts

A complete guide to the personal notification center, search and view controls, read-state and cleanup actions, current meeting/task/personal reminder behavior, browser and desktop delivery, Web Push conditions, privileged broadcasts, saved preference labels, tenant boundaries, and safe troubleshooting.

VERSION	1.0	AUDIENCE	Authorized DentalXpand users
FORMAT	Website + PDF	UPDATED	July 2026

Every person, organization, provider, patient, employee, client, task, meeting, notification, date, status, count, browser state, and device state shown in this guide is fictional. Never use live protected, credential, password, token, endpoint, recording, unredacted third-party, or another-tenant data in training material.

Contents

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

Use alerts to find current work, not as a substitute for source records	3
Confirm your identity, expected tenant, and safe device context	4
Read personal alerts and open the current linked work	5
Search, filter, and choose a view that supports the question	6
Acknowledge alerts without confusing inbox state with source-work state	7
Use near-term prompts to open current meeting, task, and personal work	8
Understand browser, desktop, and Web Push conditions	9
Use privileged communication and saved account labels with clear limits	10
Keep personal alerts, delivery, routes, and content in the intended scope	11
Resolve expected notification states without bypassing access	12
Verify safe notification handling	13
Continue through DentalXpand learning	14
Related lessons	14

How to use this guide

Read identity, tenant scope, alert privacy, and source-record discipline first. Then practice personal inbox controls, read states, cleanup, reminders, delivery layers, privileged broadcasts, saved preference labels, incident response, and completion verification.

01 / PURPOSE

Use alerts to find current work, not as a substitute for source records

Area	Current role	Boundary
Personal inbox	Current notification records for the signed-in user, ordered newest first.	It is not a complete historical archive or proof that every prior event is visible.
Unread activity	Unread count and navigation badges help prioritize attention.	Unread does not create an emergency classification, source change, or entitlement.
Linked route	An alert with a route can be opened from the inbox and may be marked read.	The destination must still enforce current account, role, tenant, practice, and record access.
Delivery surface	The same work context can appear in the inbox, overlay, native prompt, or supported Web Push alert.	A delivery surface never grants new permission or replaces the owning workflow.
Source record	Tasks, Meetings, Messages, and other authorized modules hold current operational state.	Do not approve, complete, RSVP, retain, or document a material outcome only in an alert.

An alert is a prompt
Open the current authorized source workflow and verify its live state before acting. A title, badge, browser banner, or push payload can be stale, dismissed, delayed, duplicated, deleted, or superseded.

02 / ACCESS

Confirm your identity, expected tenant, and safe device context

Check	Confirm	Why it matters
Identity	Your own active DentalXpand account and current session.	A shared browser, copied notification, screenshot, link, or another person's desktop profile is not permission.
Organization and practice	Expected DentalXpand tenant, organization, practice, and operating context.	Notifications must not bridge Guardian Connect and DentalXpand or unrelated organizations, providers, clients, patients, or employees.
Screen privacy	A private approved device and appropriate lock-screen visibility.	Notification text can be visible even when the application itself is protected.
Source workflow	The current linked record and legitimate action for your role.	An alert does not replace backend authorization, row-level policy, storage policy, tenant controls, or the owning record.
Content	Minimum necessary alert information only.	Never place passwords, tokens, protected data, sensitive finance/HR detail, or cross-tenant content in notification text.

Unexpected data is an incident

If another organization, Guardian Connect, patient, provider, client, practice, employee, or unrelated detail appears, stop. Do not open more alerts, follow links, copy, download, forward, or screenshot it. End the affected session according to policy and report minimum non-sensitive context.

[Review roles and permissions](#) | [Review organization and practice context](#)

03 / COMMAND CENTER

Read personal alerts and open the current linked work

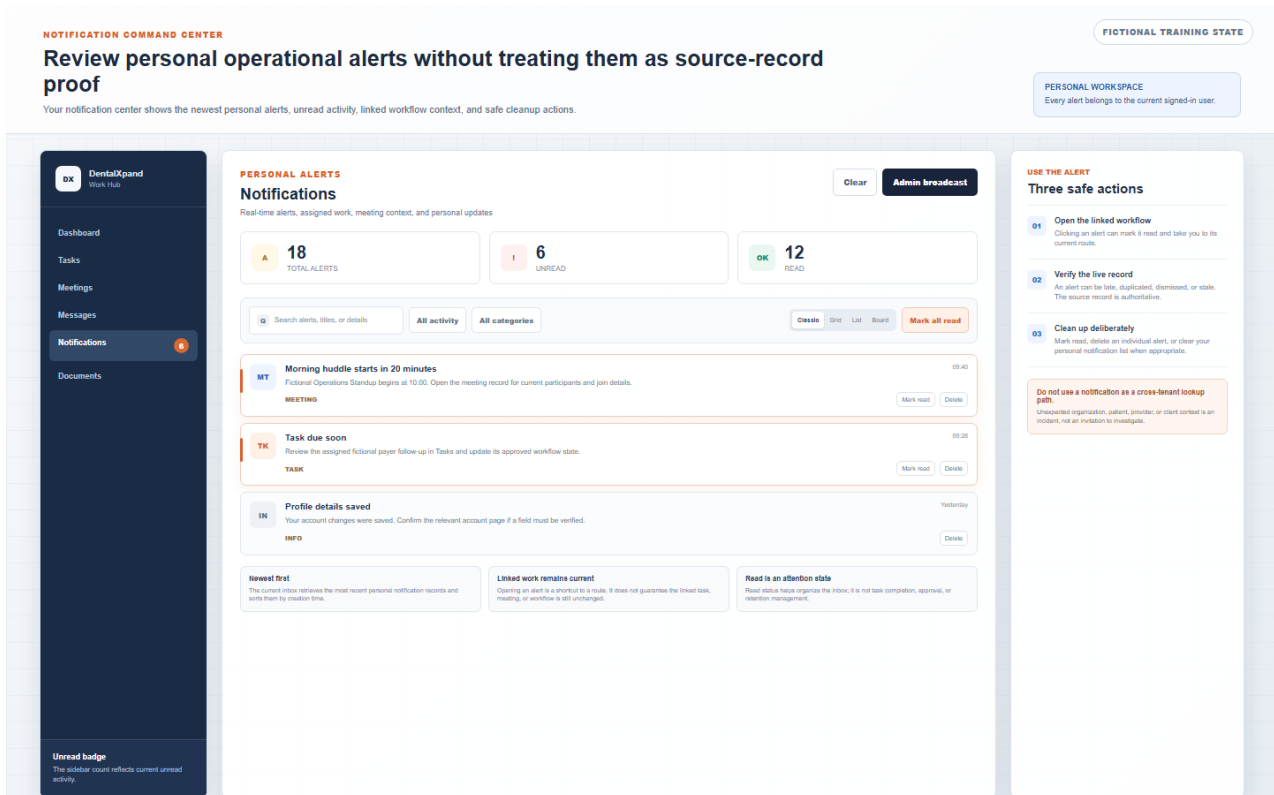


Figure 1. Fictional notification command center with personal total, unread and read counts, sidebar badge, linked meeting and task alerts, search controls, and cleanup guidance.

- 1 Open Notifications from the sidebar, header, dashboard, or the current personal route.
- 2 Read title, detail, type, and time as context only; do not assume the alert remains current.
- 3 Select a legitimate alert to follow its route. The reviewed page marks an unread alert read before navigating when a link is present.
- 4 Verify the source record: tasks need current owner, status, priority, steps, comments, and due date; meetings need current time, status, participants, and join details.
- 5 Return to the inbox and manage attention deliberately. Do not leave material decisions only in a notification title or badge.

04 / CONTROLS

Search, filter, and choose a view that supports the question

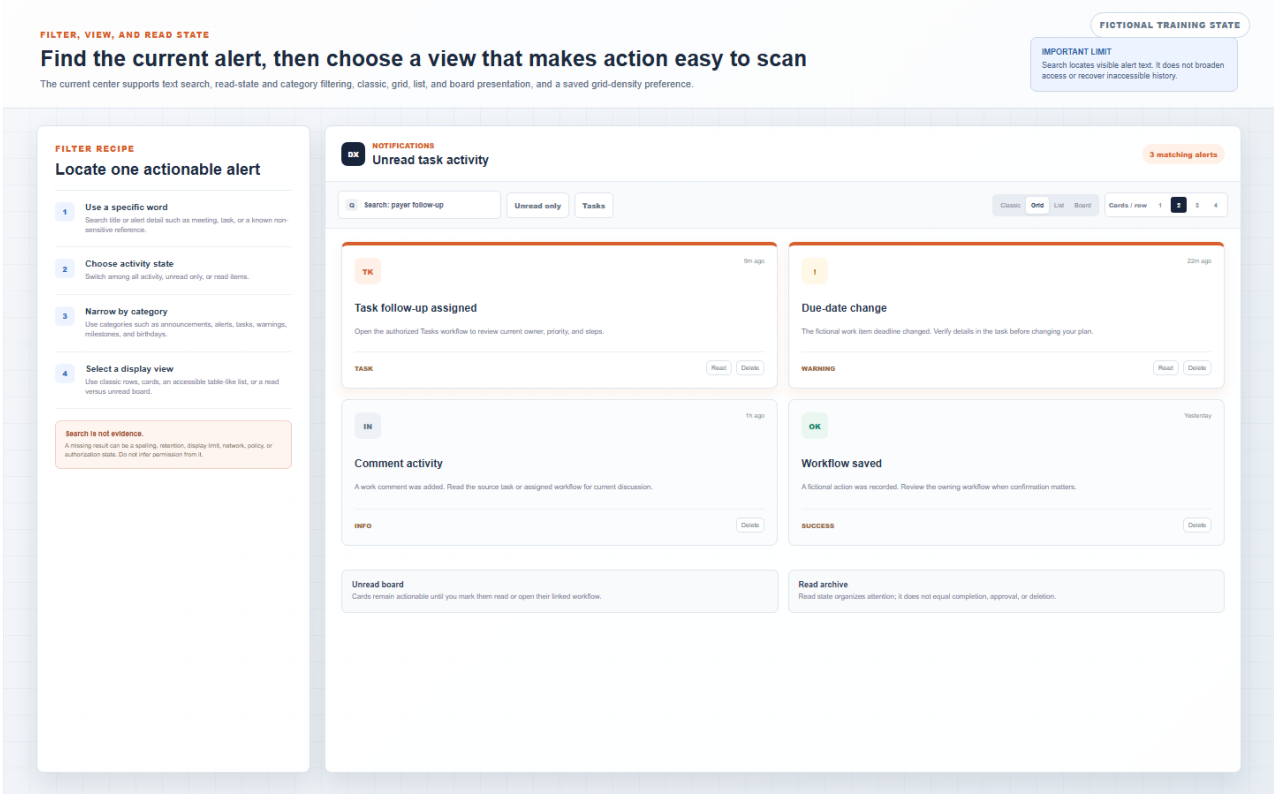


Figure 2. Fictional notifications controls showing text search, unread and task filtering, grid cards, card density, and read versus unread guidance.

Control	Use it for	Do not assume
Text search	Finding visible notification title and message text with a known non-sensitive term.	A result is access approval; a missing result means data should be exposed or is permanently absent.
Read state	Focusing on all, unread, or read activity.	Read equals task completion, approval, escalation, or correct retention.
Category	Narrowing to current exposed filters such as announcements, alerts, tasks, success, warnings, info, milestones, or birthdays.	A category label is a security label or a full priority policy by itself.
Views	Classic rows, grid cards, structured list, or read versus unread board.	Changing the view changes record access, ownership, or source truth.
Cards per row	Choosing a locally saved grid density that suits the current screen.	The setting follows the user across browsers or devices, or that it is a role control.

Search stays personal and scoped
Do not use a person, client, provider, organization, or task name to discover alert content outside your legitimate scope. Search is a navigation aid, not a data-discovery tool.

05 / READ STATE AND CLEANUP

Acknowledge alerts without confusing inbox state with source-work state

Action	Current reviewed behavior	Required discipline
Mark one read	Available per alert, or triggered when a linked unread alert is opened.	Read state organizes attention. It does not complete, approve, retain, or resolve the source work.
Mark all read	Updates unread notification records for the current user.	Use after review or intentional triage; do not make it a shortcut for unreviewed work.
Delete one	Removes the notification record from the personal inbox.	It does not delete the linked task, meeting, message, person, source record, or separate retention duty.
Clear all	Removes the current user's notification records from the inbox.	Treat as consequential housekeeping, not proof that related work or retention needs have disappeared.
Local display conflict	The UI can update before a later refresh confirms persistent state.	Refresh once, avoid repeated clicking, and report a non-sensitive symptom if the conflict persists.

Keep the record of work in the owning workflow
After acknowledging an alert, record material action, decision, completion, exception, or outcome in Tasks, Meetings, or the proper authorized module. A notification is not a shadow system of record.

[Continue to Tasks](#) | [Continue to Meetings](#)

06 / REMINDERS

Use near-term prompts to open current meeting, task, and personal work

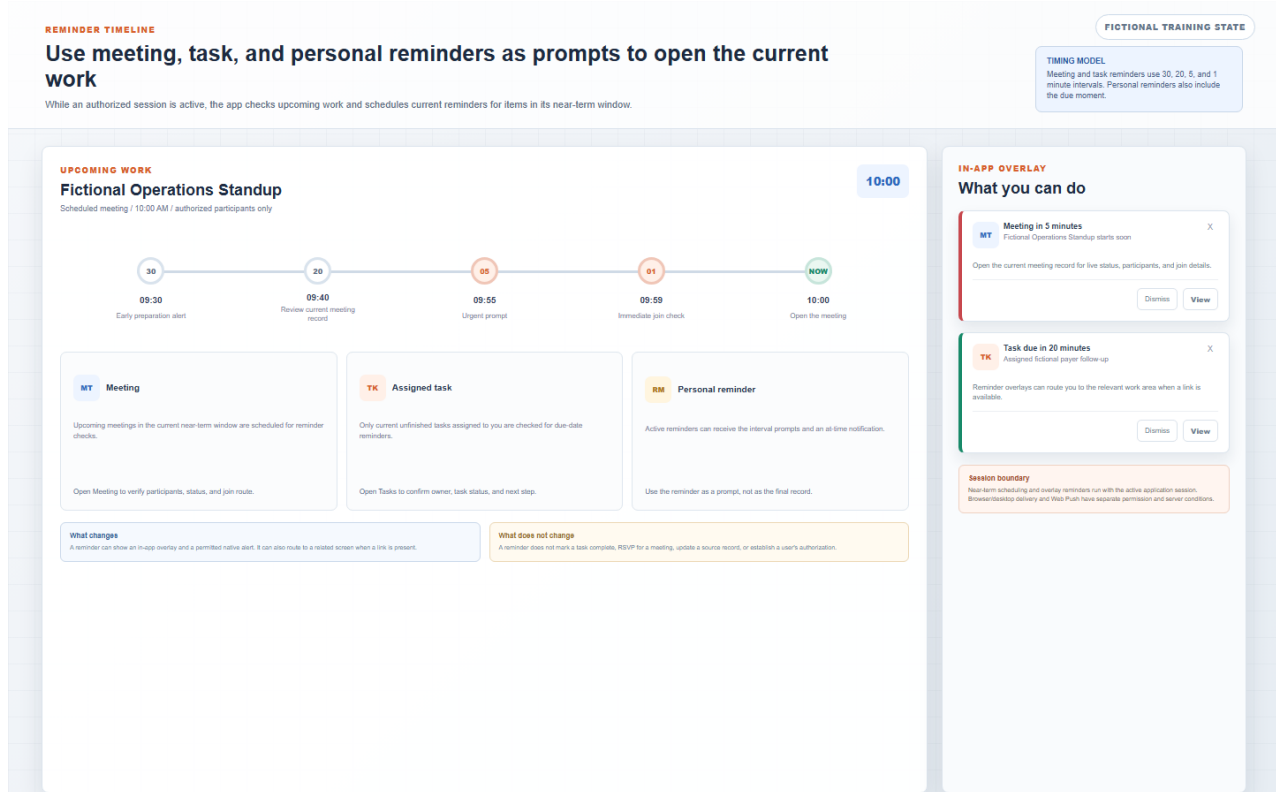


Figure 3. Fictional reminder timeline with 30, 20, 5, and 1 minute meeting prompts, task and personal reminder cards, in-app overlay actions, and session boundary guidance.

Reminder path	Reviewed current behavior	Correct action
Meeting	Future reminders are scheduled at 30, 20, 5, and 1 minutes before upcoming meetings returned in the near-term window.	Open the Meeting record to confirm current time, status, participants, and authorized join details.
Assigned task	Unfinished tasks assigned to the signed-in user in the near-term due-date window use the same four reminder intervals.	Open Tasks to verify assignment, due date, priority, status, steps, and current next action.
Personal reminder	Active personal reminders in the user's near-term window use those intervals plus an at-time reminder.	Use the prompt to revisit the intended work; it does not create an audit record or authorization decision.
Polling	The near-term check starts at sign-in and repeats each minute while the authorized application session is active.	Closed sessions, past intervals, sleep mode, permission, connectivity, and device behavior can change what appears.

07 / DELIVERY

Understand browser, desktop, and Web Push conditions

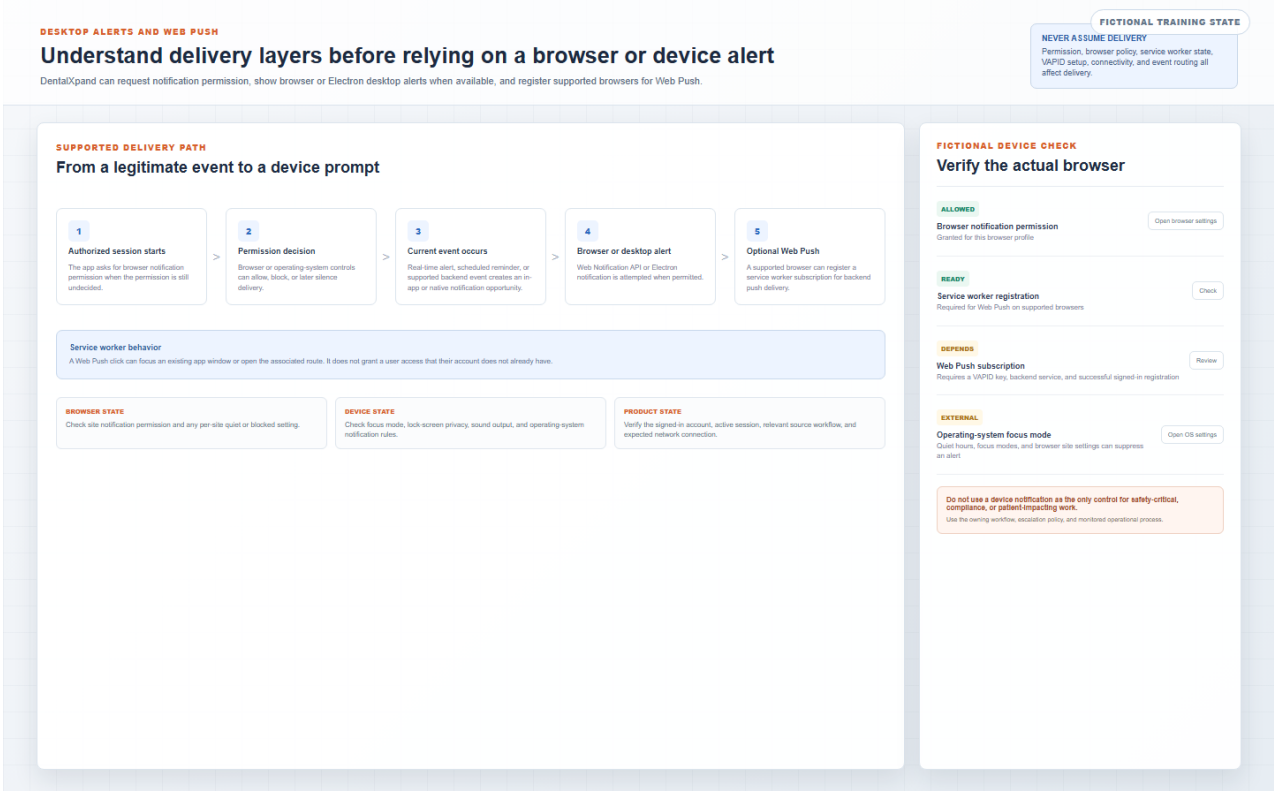


Figure 4. Fictional delivery path from authorized session and permission through a current event, browser or desktop alert, optional Web Push subscription, and device checks.

Layer	Current behavior	What to check
Permission	The app requests browser notification permission when the browser permission remains undecided at an eligible logged-in session.	Use browser site settings to allow or block on an approved private profile; do not borrow another person's profile.
Native alert	The service uses Web Notification API when granted and tries Electron notification first when its bridge is available.	Browser support, site permission, operating-system focus mode, lock-screen privacy, sound, and device policy.
Web Push registration	Supported browsers can register the service worker, obtain the public VAPID key, create or reuse a subscription, and send it to the authenticated backend.	Browser support, permission, service worker, VAPID configuration, authenticated API access, subscription, backend, and connectivity.
Push click	The service worker can focus an existing app window or open the route included in push data.	The route still needs current account, tenant, role, page, and record authorization.
Inactive app	Web Push can support a subscribed browser for backend-sent events; overlays and in-app polling need the active session.	Do not assume every alert or reminder arrives after the app closes.

08 / BROADCASTS AND PREFERENCES

Use privileged communication and saved account labels with clear limits

ADMIN BROADCASTS AND SAVED PREFERENCES

Use broadcast and settings controls only within their intended authority

The current Notifications screen exposes the broadcast control for admin and super-admin UI roles; Settings stores account-level notification preference labels separately from browser permissions.

FICTIONAL TRAINING STATE

ROLE BOUNDARY
Visible client controls are not the sole authorization layer. Deployment policy must enforce role and tenant access server-side.

ADMIN / SUPER ADMIN UI
System broadcast

BROADCAST TITLE
Fictional schedule update

CATEGORY
Announcement

MESSAGE
Use the current workspace for approved updates. Review your assigned work and meeting records for full operational detail.

Urgent protocol
Urgent styling can request a native alert for the active sender; it does not override recipient browser or operating-system settings.

Send broadcast

SETTINGS / NOTIFICATIONS
Saved account preferences

Email notifications
Preference label stored with the account settings record

Desktop notifications
Preference label; browser or OS permission remains separate

Task updates
Preference label for task-related updates

New messages
Preference label for conversation activity

Product updates
Preference label for feature updates

Save settings

BEFORE SENDING
Broadcast discipline

01 Use the right audience
Announcements are for legitimate operational information, not personal, clinical, financial, evidential, password, token, or cross-tenant content.

02 Keep the source record current
A broadcast points users to work. It does not replace the approved task, meeting, policy, or client record.

03 Expect normal delivery limits
Recipients still depend on their session, browser, device, permission, and push configuration states.

Do not use broadcast to bridge Guardian Connect and DentalXpand.
Each product and tenant must remain independently scoped.

Figure 5. Fictional privileged broadcast form with title, category, message, urgent state, saved preference labels, and broadcast safety guidance.

Control	Reviewed interface	Boundary
Broadcast	The Notifications UI exposes the broadcast control when the current UI role is admin or super admin; it accepts title, message, category, optional urgent state, and an AI text-polish action.	Use only for legitimate operational communication. Do not include protected records, credentials, tokens, sensitive HR/finance content, or cross-tenant data.
Audience	The reviewed client send flow creates notifications for active user records.	In multi-tenant deployment, server-side authorization and tenant targeting must restrict the audience to the intended organization. Visible client role UI is not enough.
Urgent	The current reviewed flow can request a native notification for the active sender.	It cannot override recipient browser permission, focus mode, device policy, session state, or tenant authorization.
Saved preference labels	Settings offers saved email, desktop, task, message, and product-update preference labels.	Those labels are separate from browser and operating-system permission and do not by themselves guarantee or suppress every delivery path.

09 / TENANT SECURITY

Keep personal alerts, delivery, routes, and content in the intended scope

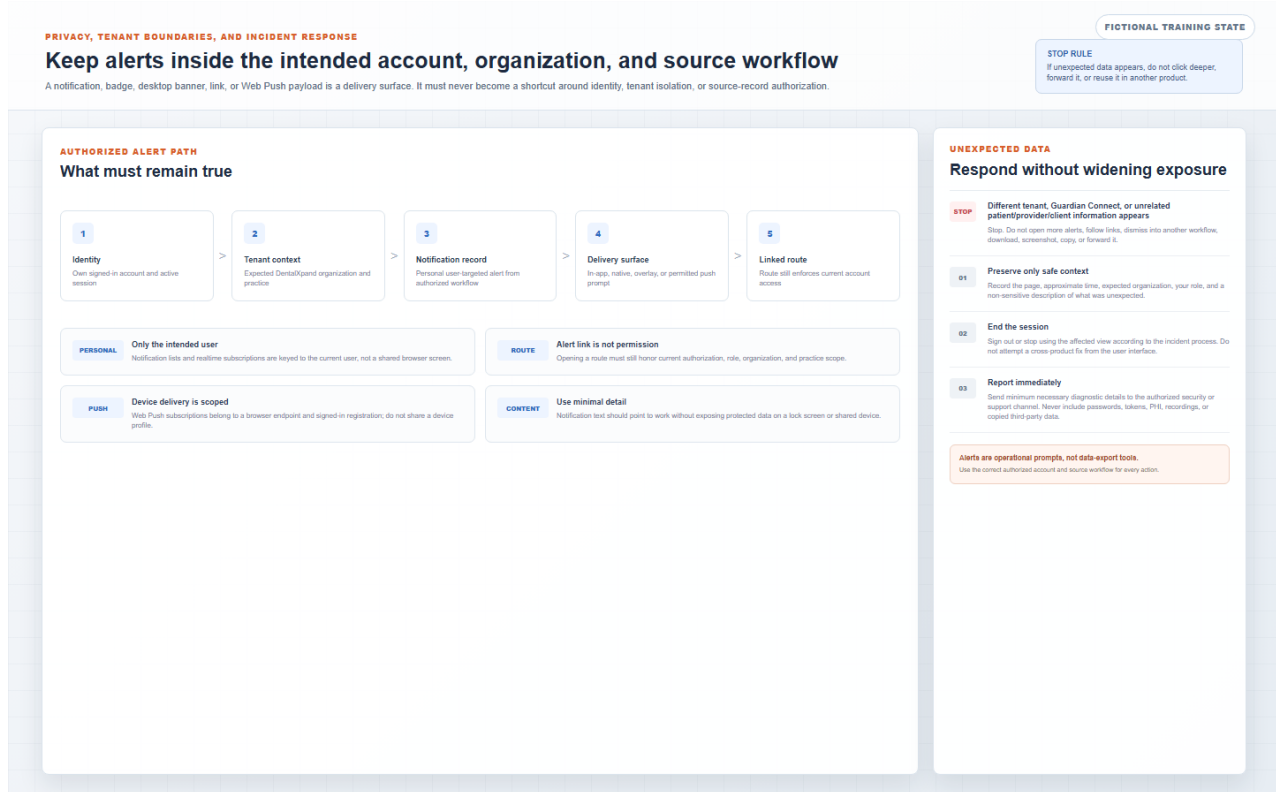


Figure 6. Fictional notification security view with identity, tenant context, personal alert ownership, delivery surface, linked route authorization, and incident response.

Boundary	What must remain true
Identity	The signed-in user acts through their own account and active session. Shared devices and copied browser profiles require separate care.
Notification ownership	Personal inbox and realtime delivery remain limited to the intended user's authorized notification records; badges, banners, and push endpoints must not expose another person's alerts.
Tenant context	Expected DentalXpand organization, practice, provider, client, and work context remain correct. Guardian Connect and unrelated tenant data must not appear.
Linked route	An alert route continues to enforce role, page, organization, practice, record, storage, and row-level authorization. A deep link is navigation, not entitlement.
Push subscription	The subscription belongs to the registered browser endpoint and authenticated setup. It is not a data-export channel and should not be shared across profiles.
Content	Title and message use minimum necessary detail and do not leak protected or cross-tenant data to lock screens, shared devices, screenshots, logs, or support tickets.

10 / TROUBLESHOOT

Resolve expected notification states without bypassing access

What you see	Possible reason	Correct first response
No permission prompt	Permission may already be granted or blocked, browser policy may prevent prompts, or the session may not be eligible.	Check the browser's site settings in your own approved profile. Do not keep clearing data or use another person's profile.
No desktop alert	Permission, browser support, Electron state, focus mode, device settings, sound, connection, event timing, or session state.	Open the inbox and source workflow first, then check browser and device settings using safe non-sensitive context.
No reminder	Item is outside the near-term window, past an interval, inactive, not assigned to current user, unavailable to session, or affected by permissions/connectivity.	Verify current task, meeting, or personal reminder data. Do not assume work is cancelled or completed because an alert was absent.
Push absent after close	Browser capability, permission, service worker, VAPID, backend, subscription, connection, device policy, or event sender can be missing.	Verify safe browser registration state and report the non-sensitive symptom. Do not expose VAPID keys, tokens, endpoint data, or another person's device details.
Alert route unavailable	Record changed, session stale, role/scope policy denies, or route no longer applies.	Respect the response, refresh your own session, confirm expected tenant and role, then contact the authorized administrator or support.
Unexpected tenant data	Potential policy, cache, storage, API, push, browser, or configuration isolation issue.	Stop immediately, avoid more exposure, end the session per process, and report minimum non-sensitive context.

[Review Team Messages](#) | [Review Tasks](#) | [Review Meetings](#)

11 / COMPLETION

Verify safe notification handling

- I can distinguish personal inbox records, unread badges, linked source routes, in-app overlays, native browser or desktop prompts, and Web Push delivery as separate surfaces.
- I confirm my own account, expected DentalXpand organization and practice context, and safe device environment before acting on an alert.
- I can search, filter by current read and category states, and choose classic, grid, list, or board view without treating those controls as authorization decisions.
- I know opening an alert may mark it read and navigate, but the destination still authorizes my account and the source record remains current authority.
- I can mark read, delete, or clear notifications without assuming any related task, meeting, record, retention, or compliance duty disappeared.
- I understand current near-term reminder timing and that in-app polling and overlays rely on the active authorized session.
- I know browser, Electron, and Web Push delivery need permission, device/browser support, service worker/VAPID setup, authenticated registration, connectivity, and a relevant event sender.
- I know privileged broadcasting must use server-side role and tenant-aware audience controls, and saved preference labels are separate from browser/OS permission.
- I stop and report if Guardian Connect, another tenant, patient, provider, client, practice, employee, or unrelated data appears unexpectedly.

Ready for the next workflow

Continue to Documents to learn how files, folders, previews, downloads, deletion, and storage boundaries should be handled with the same tenant-safe discipline.

12 / CONTINUE

Continue through DentalXpand learning

Tasks guide	Meetings guide	Documents guide	All resources
Tasks guide	Meetings guide	Documents guide	All resources

Related lessons

- Use the Dashboard command center
- Understand roles, permissions, and access boundaries
- Understand organization and practice context
- Use team messages, conversations, and attachments
- Manage documents, files, folders, and previews

Website guide: Manage notifications, reminders, and push alerts

Support: support@xpand.dental

Website: xpand.dental