DENTALXPAND LEARNING CENTER / TENANT CONTEXT

Understand Organization and Practice Context

A complete guide to active organization identity, practice scope, organization types, user assignments, role and permission boundaries, tenant safeguards, files and integrations, wrong-context incident response, unavailable workspaces, and audited platform support.

VERSION	1.0	AUDIENCE	All users and administrators
FORMAT	Website + PDF	UPDATED	July 2026

Every product state in this guide is fictional. Never include patient, provider, practice, employee, credential, token, API key, or unredacted third-party data in training or support material.

Contents

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

01 / ACCESS MODEL

Understand the layers behind every workspace decision

Authentication identifies an account. It does not independently grant every organization, practice, page, action, or record.

Layer	Question	Access decision
1	Authenticated identity	The sign-in session identifies one application user.
2	Organization membership	The account must belong to an active DentalXpand organization.
3	Practice scope	The membership is organization-wide or limited to assigned practices.
4	Role and permissions	The tenant role and granted actions decide which tools can be used.
5	Status and security gates	Organization, membership, password-change, and platform-MFA state can block access.

Five checks, one result
A familiar logo, working password, visible menu item, copied URL, or previous access is not enough on its own. Every applicable context layer must agree.

Stop on an unexpected organization
Do not open, search, copy, edit, upload, export, summarize, or ask AI about unexpected records. Sign out and report the mismatch without disclosing sensitive data.

02 / ORGANIZATION

Confirm the active organization after every fresh sign-in

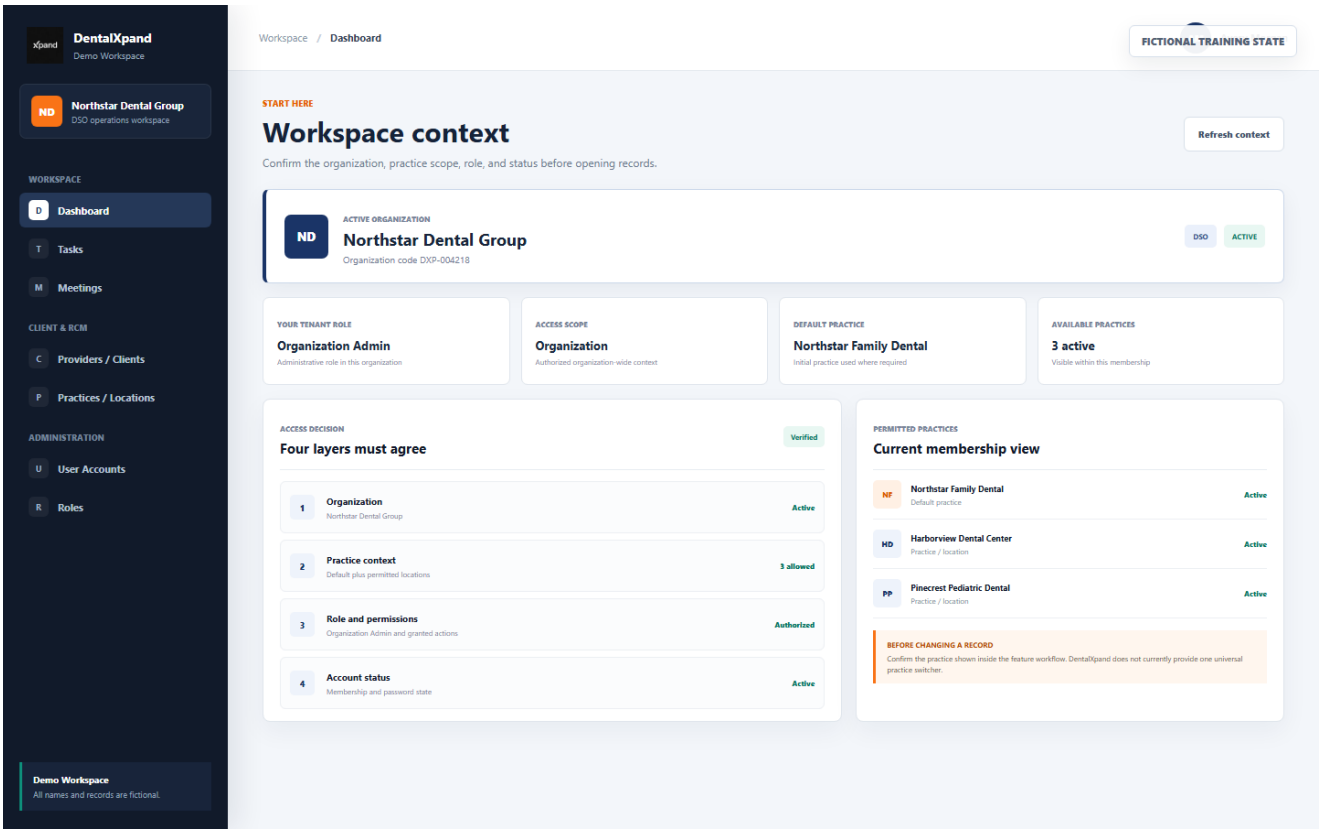

Figure 1. Fictional workspace context showing organization identity, membership scope, role, default practice, permitted practices, and status.

Read the expanded sidebar identity

The account area displays the organization loaded for the current membership. Confirm that name before opening records or following a deep link.

02A / ORGANIZATION CHECK

Complete the organization check

The intended destination may be Dashboard, My Profile, or another permitted page depending on page permissions.

1. Read the organization name shown for the signed-in account.
2. Confirm whether the expected workspace is a single practice, DSO, or billing company.
3. Confirm that you are using your own individual account.
4. Confirm the expected first page and available navigation for your role.
5. Stop and sign out if the organization, practice names, providers, clients, counts, or records are unexpected.
6. Report only non-sensitive context through the approved support or security channel.

> Branding is not proof
> A shared DentalXpand logo, familiar colors, or a similar practice name does not prove that the active tenant is correct. Confirm the organization context itself.

03 / ORGANIZATION TYPES

Understand the supported organization models

Organization type	Practice model	Navigation label
Single practice	One default organization-owned practice; expansion remains subject to plan and administration	Practice
DSO	Multiple practices or locations inside one organization tenant	Practices / Locations
Billing company	Client practices represented as organization-owned practice records	Clients / Practices

The organization is the top-level tenant boundary. A practice is a location or client record inside that organization; it is not a second independent DentalXpand organization.

> Labels adapt, boundaries do not
> Practice, Practices / Locations, and Clients / Practices use the same organization-owned practice model.
> Organization and practice IDs remain the security-relevant context.

04 / PRACTICE CONTEXT

Understand default, allowed, and feature-specific practice context

Term	Meaning
Default practice	Organization-owned practice marked default and preferred for initial context when accessible
Allowed practices	Active, non-archived practices returned for the membership or support session
Feature-selected practice	Practice field or filter on a particular record, queue, report, or export
Practice-scoped membership	Explicit membership-to-practice rows limiting the available practice set

Tenant context prefers the first allowed default practice; when none is available, it uses the first allowed practice. A practice-scoped user receives only assigned practices.

> No universal global practice switcher
> The current global layout does not provide one workspace-wide practice selector. Verify the default or assigned context, then use the feature's own practice selector or filter where implemented.

05 / ACCESS SCOPE

Compare organization-wide and assigned-practice access

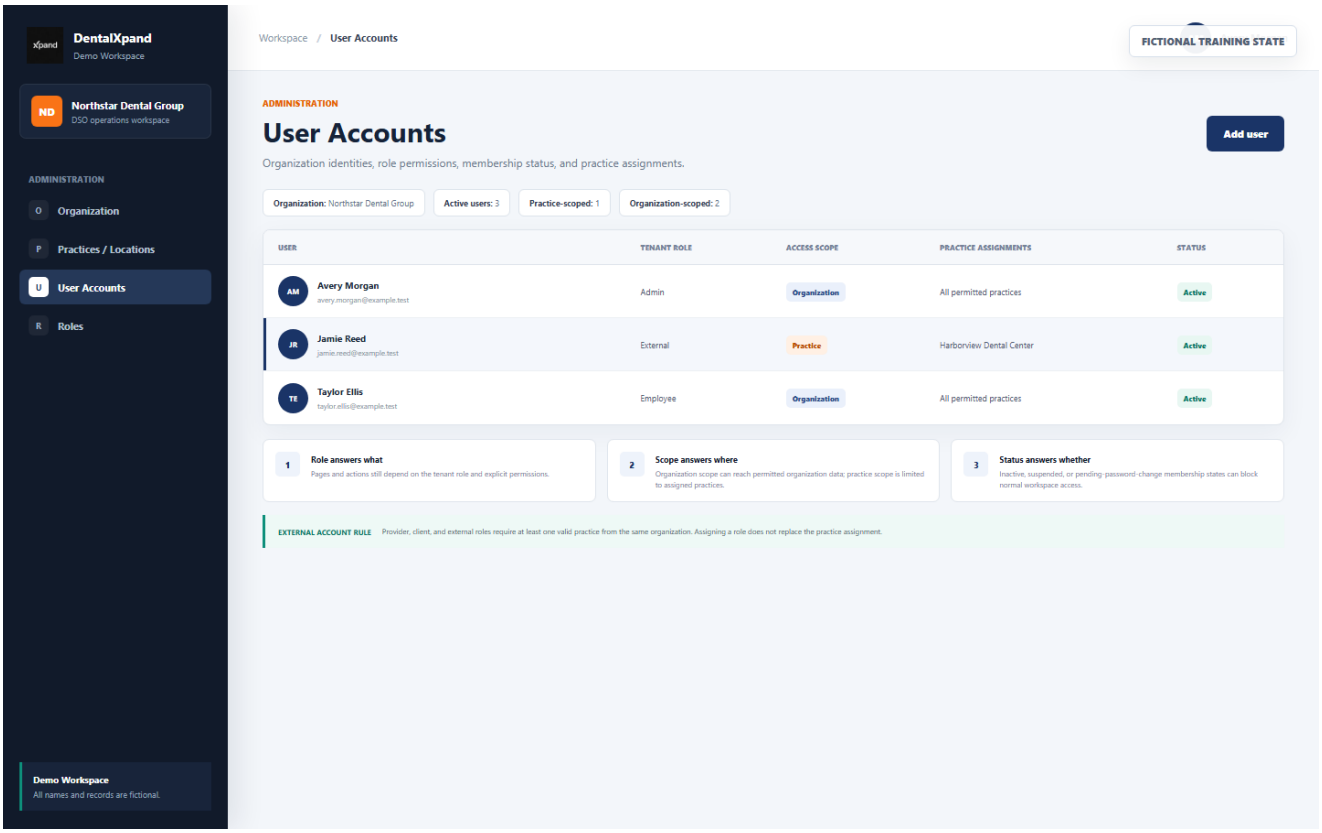

Figure 2. Fictional User Accounts state comparing organization-scoped and practice-scoped memberships.

> Role, scope, and status are different
> Role answers what responsibility and permissions apply. Scope answers where. Status answers whether normal access is currently allowed.

05A / SCOPE RULES

Apply organization and practice scope correctly

Scope	Practice visibility	Common use	Important limit
Organization	Active practices available through organization context	Internal owner, administrator, employee, or manager	Permissions still limit pages and actions
Practice	Only explicitly assigned same-organization practices	Provider, client, or external user	At least one valid assignment is required at creation

- A practice-scoped user may have one or several assigned practices.
- An assignment must never reference a practice from another organization.
- Organization scope is not automatic full administration.
- Changing a role and changing practice assignments are separate authorization decisions.
- Password setup or reset must not change scope, role, permissions, or assignments.

06 / PRE-ACTION CHECK

Verify context before sensitive work

Check	Layer	Question to answer
1	Organization	Matches the authorized request or assignment
2	Practice	Record, form, queue, report, or export shows the intended practice/client
3	User and role	You are signed in as yourself with the intended responsibility
4	Permission	The required view, create, update, approve, delete, upload, or export action is granted
5	Record ownership	The record belongs to the expected organization and practice
6	Output destination	Files, messages, integrations, AI requests, and reports remain inside approved context

Repeat after context-changing events

Repeat after sign-in, account changes, deep links, notifications, new browser profiles, bulk actions, exports, file uploads, integration calls, and AI-assisted work.

07 / PRACTICE DIRECTORY

Manage practices, locations, and client records

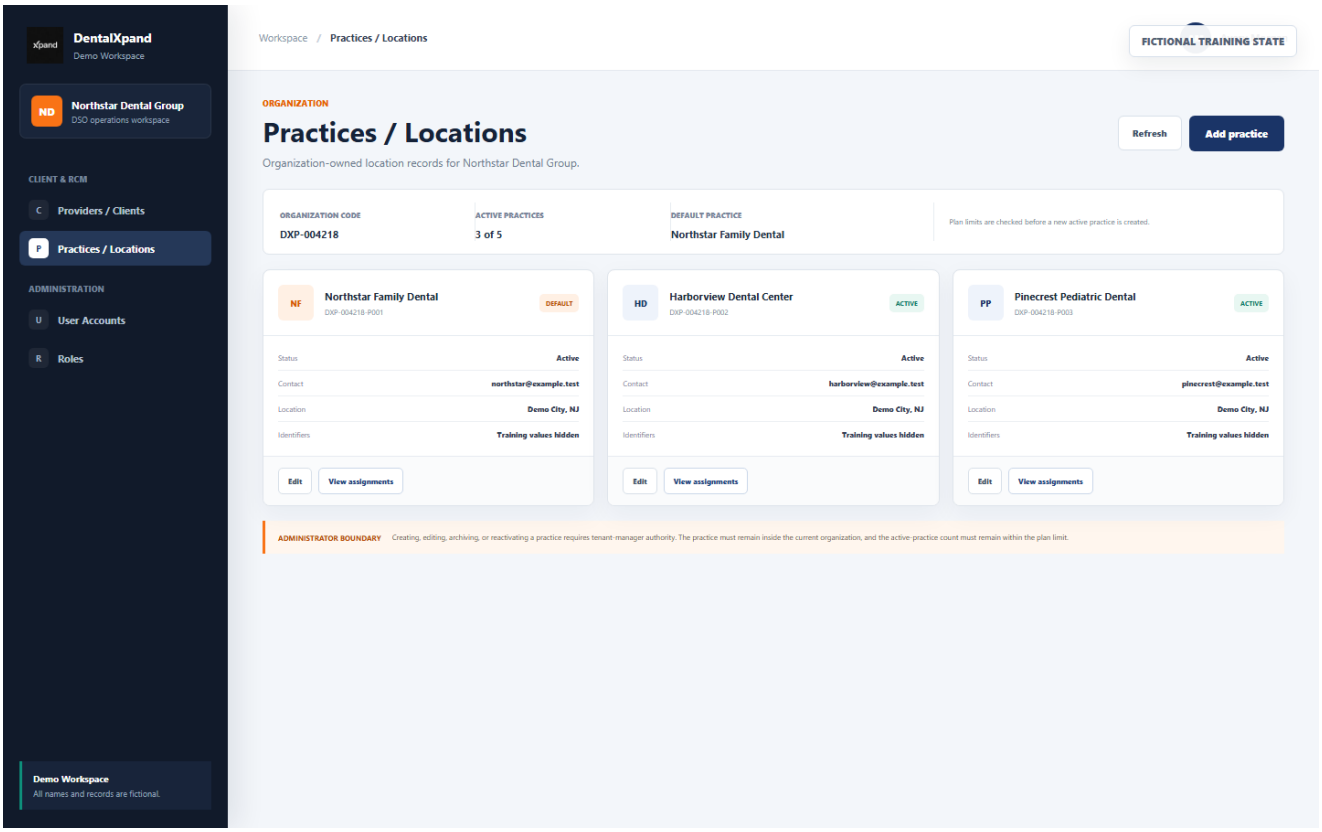

Figure 3. Fictional DSO Practices / Locations view showing organization code, active count, default practice, and organization-owned location records.

Plan-aware creation

DentalXpand checks the active practice count against the subscription override or plan limit before creating another active practice.

07A / PRACTICE WORKFLOW

Create or update a practice safely

1. Confirm organization name and code before adding or editing.
2. Review active count and plan limit before creating another practice.
3. Use the generated practice code and exact name to avoid similarly named locations.
4. Maintain approved name, legal name, contact, identifiers, status, and address fields.
5. Archive or reactivate only under an approved procedure and review dependent assignments.
6. Refresh and verify count, status, default marker, organization, and related user/provider assignments.

Tenant-manager authority
Practice creation and updates require owner, admin, platform support, wildcard authority, or delegated tenant settings permission. A default practice receives additional deletion protection.

Continue to practices, locations, and assignments

08 / USER ASSIGNMENTS

Assign accounts to the least-privilege scope

Decision	Administrator check	Outcome
Internal role	Confirm role and only required page/action permissions	Organization scope; permissions still limit tools
Provider/client/external	Select at least one active practice in the current organization	Practice scope with explicit mappings
Change external assignments	Validate every selected practice before saving	Approved list replaces existing mappings
Change external to internal	Review business need and broader permissions	Organization scope; obsolete mappings removed
Suspend user	Confirm identity, tenant, reason, and downstream sessions	Normal tenant access is blocked
Organization owner	Use platform owner-management workflow	Protected owner cannot be assigned by tenant admin

Password recovery is separate
A reset must not silently add organizations, practices, roles, pages, actions, provider links, or client relationships.

Continue to the user account lifecycle guide

09 / AUTHORIZATION

Separate role, permission, scope, and status

Authorization element	What it controls
Tenant role	Responsibility model such as owner, admin, employee, provider, client, or external
Permissions	Role permissions, wildcard access, or membership overrides for pages and actions
Access scope	Organization or practice boundary applied independently from feature permissions
Membership status	Invited, pending password change, active, or suspended state

DentalXpand uses permission-aware navigation and route guards. A hidden sidebar item is a usability cue; protected direct URLs are checked before the page renders.

> Avoid broad shortcuts
> Do not make every user an administrator, add all practices to solve one assignment, use organization scope to solve a page permission, borrow another login, or treat hidden navigation as the only control.

Review roles, permissions, and access boundaries

10 / TENANT ISOLATION

Understand the safeguards that keep organizations apart

The current tenancy foundation applies multiple controls together; no UI label is treated as the whole boundary.

Safeguard	Purpose
Tenant context API	Loads organization, membership, role, permissions, subscription, branding, and allowed practices
Server-side filtering	Scopes tenant users, practices, assignments, and operations to the active organization/support context
Tenant columns	Organization identifiers on tenant records and practice identifiers on practice-specific records
Row-level security	Evaluates organization, practice, role/permission, membership status, and password-change state
Composite constraints	Rejects relationships combining memberships, users, roles, or practices across organizations
Isolation tests	Covers independent tenants, guessed IDs, practice scope, pending-password access, and write attempts

Layered controls, not an absolute promise

Isolation depends on correctly deployed migrations, policies, API configuration, credentials, storage rules, integrations, and ongoing tests. Investigate unexpected data as a security incident.

11 / FILES AND INTEGRATIONS

Keep storage, exports, integrations, and AI in context

Operation	Confirm	Do not assume
File upload/download	Organization, practice, record, storage path, and recipient	Filename or folder label proves ownership
CSV/PDF export	Filters, organization, practice, period, rows, and destination	A previous filter survived a new session
Email/PMS/API/webhook	Tenant configuration, credentials, endpoint, payload, and response ownership	One shared credential is safe for every tenant
Xpand AI or other AI	Tenant ID, practice scope, source collection, retrieval filters, output, logs, and retention	Visual app context isolates an independent external AI store

External systems require their own tenant controls

Database row-level security does not automatically isolate a separate AI index, vector store, email system, file service, or third-party API.

Never combine Guardian Connect and DentalXpand sources without explicit tenant namespaces, authorization filters, separate credentials or stores where appropriate, and cross-tenant tests.

12 / INCIDENT RESPONSE

Respond safely when the wrong context appears

1. Stop without opening additional records or testing whether edits are possible.
2. Sign out without copying, exporting, uploading, messaging, or sending data to AI.
3. Report date, time zone, application address, account email, expected organization/practice, unexpected label, route, and last safe action.
4. State whether any record was opened, changed, uploaded, downloaded, exported, messaged, or sent to AI.
5. An authorized administrator contains sessions and reviews membership, assignments, integrations, logs, and tenant configuration.
6. Preserve factual timestamps and audit evidence; do not delete records merely to hide the mismatch.
7. Retest with approved fictional or non-sensitive records before normal work resumes.

> Do not expand exposure to prove it
> Do not include passwords, tokens, cookies, setup URLs, patient data, provider identifiers, employee records, claim details, or complete unredacted screens in the report.

13 / UNAVAILABLE ACCESS

Handle a suspended, inactive, or unverifiable workspace

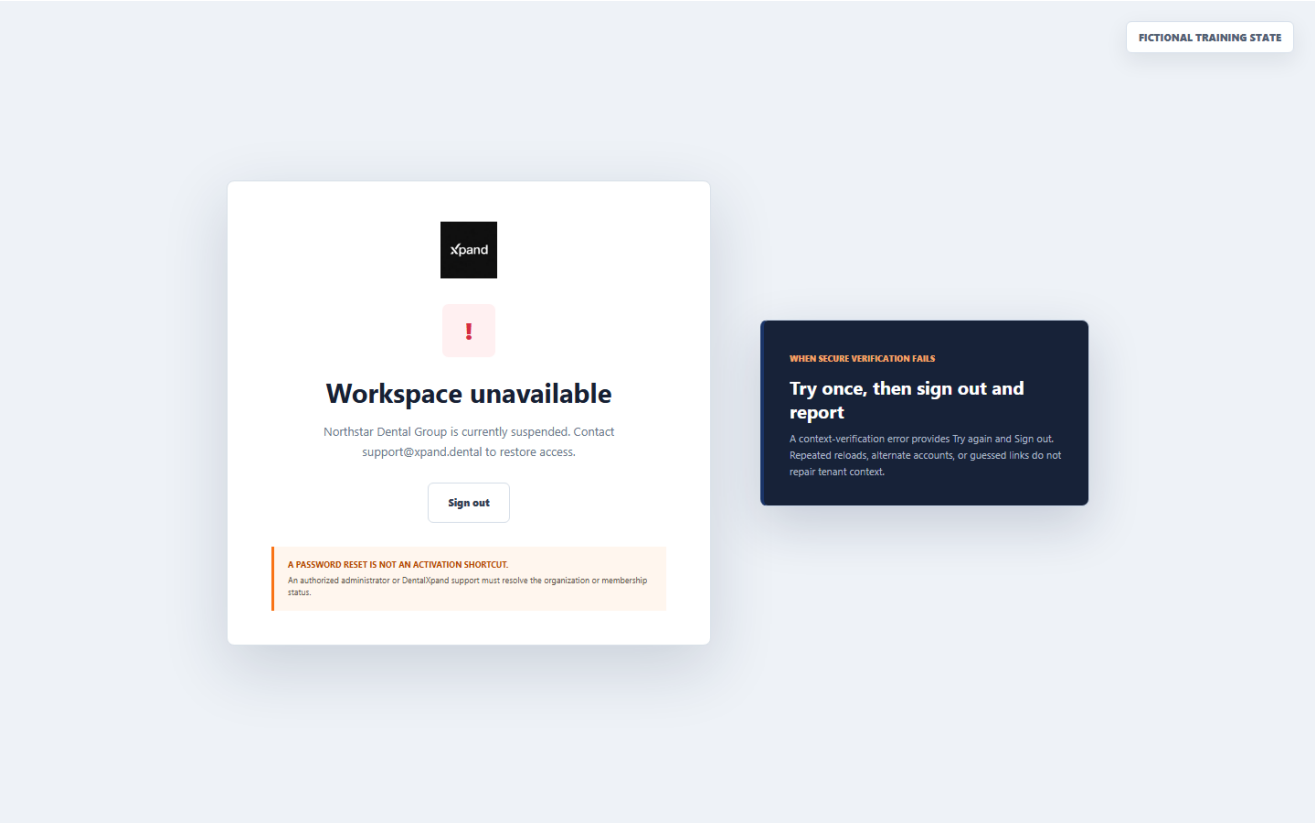

Figure 4. Fictional Workspace unavailable state. An inactive organization or suspended membership blocks normal tenant access.

> Password reset is not activation
> An authorized administrator or DentalXpand support must resolve the organization or membership status. Do not create a duplicate account or borrow another login.

13A / ACCESS STATES

Choose the correct response to each blocked state

State	System behavior	User response
Secure context not verified	Workspace unavailable with Try again and Sign out; one automatic retry	Try once, then sign out and report
Organization inactive/suspended	Normal tenant routes blocked and organization status shown	Sign out; contact authorized admin/support
Membership suspended	Normal access blocked even when organization is active	Same-organization admin reviews membership
Pending password change	Required password workflow appears before tenant data	Complete approved temporary-password flow

Do not bypass the gate

Do not alter browser storage, guess routes, repeatedly refresh, use another person's account, or change roles merely to remove the message.

14 / ADMINISTRATION

Verify and correct access without broadening it casually

1. Match the exact application user, authentication email, and organization membership without asking for a password.
2. Review organization lifecycle status, subscription, plan, and enabled context.
3. Review membership status and the must-change-password flag.
4. Confirm protected/custom role and current permissions.
5. Confirm organization versus practice scope and list every assigned practice.
6. Validate that each practice is active and belongs to the same organization.
7. Review provider links, files, integrations, AI source configuration, and open sessions where relevant.
8. Make the smallest authorized correction and preserve the audit reason.
9. Have the user perform a fresh sign-in and verify the expected organization, practices, navigation, and records.

> Never request the user's credential
> Use logs, tenant administration, approved support tooling, and the user's own verification. Platform entry into a tenant requires an explicit support session.

15 / PLATFORM SUPPORT

Use time-limited, audited support context

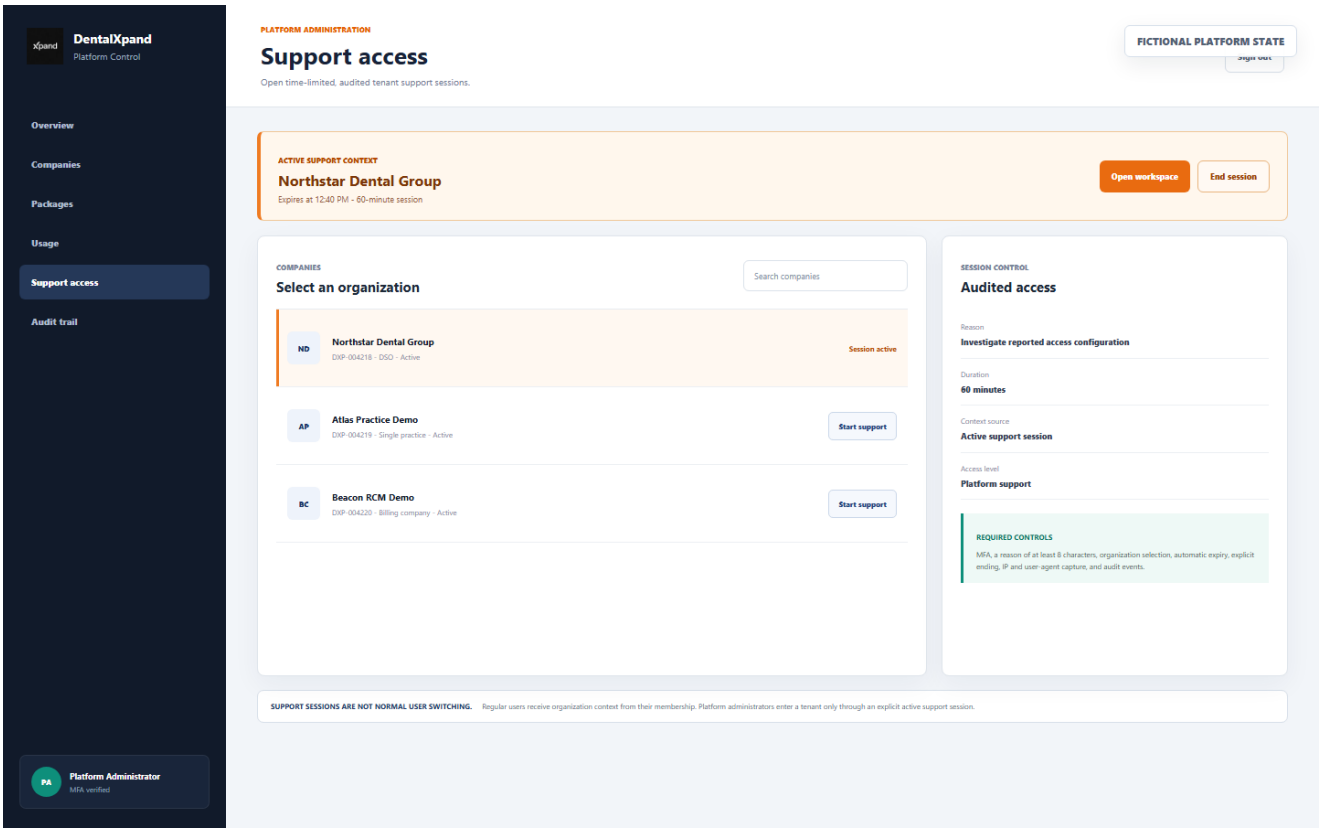

Figure 5. Fictional Platform Administration state with an active 60-minute support context and explicit end control.

> Support is not normal user switching
> Regular users receive tenant context from membership. Platform administrators receive tenant context only from an active audited support session.

15A / SUPPORT WORKFLOW

Start, minimize, and end a platform support session

1. Verify the approved platform administrator identity and MFA where configured.
2. Select the exact organization by name and code.
3. Enter a meaningful non-sensitive reason of at least eight characters.
4. Start the session; any prior active session for that administrator is ended.
5. Open only the required workspace and perform only approved support work.
6. End the session explicitly instead of relying only on the 60-minute expiry.
7. Confirm the support banner disappears and review applicable audit events.

Audited control	Captured context
Identity	Platform administrator and organization target
Purpose	Required reason and support-session identifier
Timing	Start, expiry, explicit end, and status
Environment	Starting IP and user-agent metadata
Audit	Supported actions carry support-session context; start and end are recorded

16 / TROUBLESHOOT

Troubleshoot organization and practice context

What you see	Likely context	Correct action
Wrong organization	Unexpected account, membership, or support context	Stop, sign out, report
Practice missing	Assignment absent, practice inactive/archived, or stale context	Admin validates status and mapping
Extra practice	Overbroad scope or wrong assignment	Do not inspect; report immediately
Sidebar page missing	Role, permission, organization type, or external navigation	Confirm need and permission
Direct URL blocked	Route permission or tenant state rejected	Use authorized administration
Workspace unavailable	Verification, organization, or membership problem	Try once, sign out, resolve status
Password screen	Pending-password-change membership	Complete approved setup
Practice limit	Plan/subscription active-practice limit	Review plan and practice status
External create fails	No valid same-organization practice	Assign intended practice
File path rejected	Organization/practice conflicts with context	Correct context; keep validation
AI shows other tenant	Shared/wrong source, credentials, index, or filter	Disable, contain, investigate
Support context remains	Session not ended or expired	End it in Platform and verify

17 / VERIFY

Verify that organization and practice context is understood

All-user verification

- I can identify the organization loaded after sign-in and know when to stop.
- I understand the difference between a tenant organization and its practices, locations, or clients.
- I understand that role, permissions, scope, and status answer different access questions.
- I verify feature-specific practice context before records, uploads, exports, messages, integrations, or AI.
- I can report an unexpected organization or practice without disclosing sensitive data.
- I know that password recovery does not repair a wrong or suspended tenant context.

Administrator verification

- Users have the intended organization membership, role, permissions, scope, status, and assignments.
- External accounts have at least one valid same-organization practice and no unrelated practices.
- Files, exports, integrations, provider links, and AI sources preserve tenant context.
- Suspension, password, route-guard, and cross-tenant tests behave as expected.
- Platform support is justified, time-limited, minimized, ended, and audited.

PREVIOUS	NEXT	CURRICULUM
Password setup, reset, and change	**Navigation and pinned items**	**All resources**

Website guide: Organization and practice context
Support: support@xpand.dental