DENTALXPAND LEARNING CENTER / PROVIDER AND DSO

Control Provider and Practice Access

A security-first administrator guide to named identity, organization membership, role and scope, complete practice assignments, provider relationships, exact permissions, controlled changes, effective-access verification, tenant enforcement, and suspension.

VERSION	1.0	AUDIENCE	Organization administrators and approved access managers
FORMAT	Website + PDF	SCOPE	DentalXpand provider and practice boundaries

Fictional screenshots and minimum necessary data
All screenshots use fictional training data. Never put passwords, temporary keys, MFA codes, recovery material, patient records, full identifiers, another tenant, another Xpand product, or Guardian Connect data in access tickets, screenshots, PDFs, support messages, downloads, or AI prompts.

Contents

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

Never widen a role to fix a missing practice
Provider, Client, and External accounts are intentionally practice scoped. Fix the approved assignment or permission. Do not switch to an internal role, use direct SQL, guess IDs, borrow another session, or test against a real unrelated client.

01 / ACCESS MODEL

Separate every record that participates in authorization

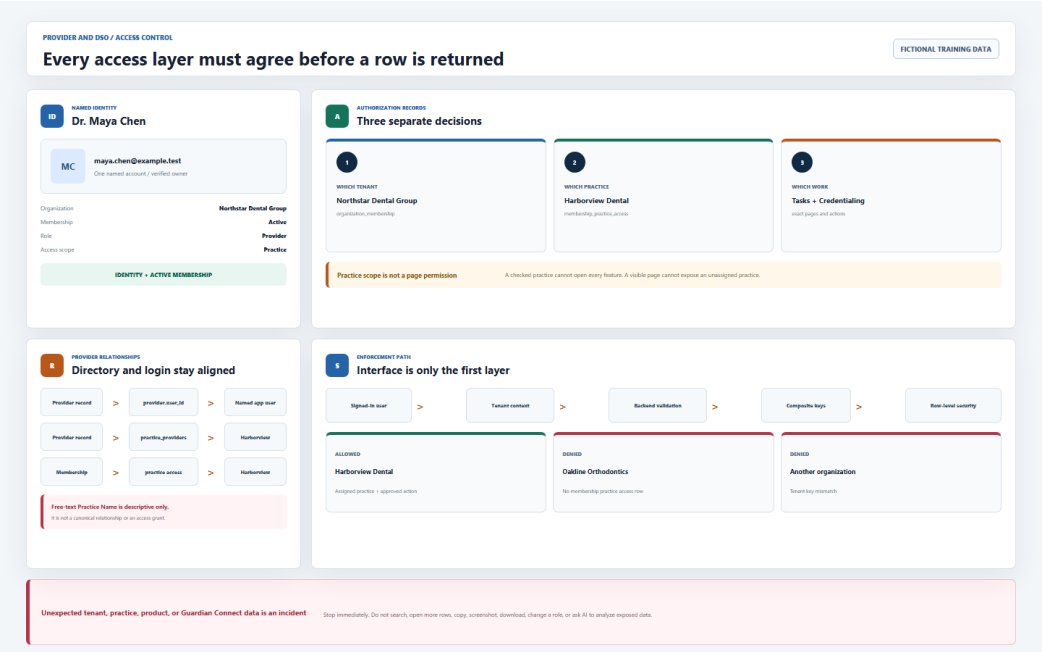

Figure 1. Fictional access-control model showing the named identity, active membership, practice assignment, exact permissions, provider relationships, backend validation, composite keys, and row-level security.

Layer	Purpose	Boundary
Application user	Named authenticated identity.	Never share one practice login between people.
Organization membership	Connects the user to one tenant with status, role, scope, and onboarding state.	Inactive, suspended, incomplete, or wrong-tenant membership is denied.
Role and scope	Provider, Client, and External are practice scoped; internal roles are organization scoped.	Role is not a workaround for missing assignment.
Practice access	Lists approved same-organization practices for an external membership.	Free-text Practice Name is not this record.
Page and action	Controls destinations and operations.	A checked practice does not grant every feature.
Provider relationship	Links the provider record to the user and canonical practices.	It remains separate from login practice access.

02 / CHANGE READINESS

Translate approval into one minimum-access target

Confirm	Required evidence	Stop when
Named user	Verified work email, identity, current account, and access owner.	The request is for a shared login or unmatched person.
Business purpose	Specific work, duration, and required destinations or actions.	The request says only 'full access'.
Organization	Exact active tenant that owns the user and practices.	The request mixes another client, product, or Guardian Connect.
Practice set	Canonical active practice records in the current organization.	A practice is archived, duplicated, missing, or from another tenant.
Role	Provider, Client, or External for external practice scope.	An internal role is requested only to clear an assignment error.
Permissions	Exact pages and actions required for the approved job.	The scope cannot be stated precisely.
Authority	Administrator using their own account and an auditable approval.	Approver, owner, or required second reviewer is absent.
Lifecycle	Current account is active, or explicit reactivation is approved.	The user is suspended and reactivation is not approved.

- Record the current role, scope, selected practices, exact permissions, lifecycle state, provider link, and open operational work before editing.
- Write the complete target state: every retained practice, every addition, every removal, and every page or action change.
- Require a second reviewer for multi-practice expansion, external-to-internal conversion, administrator access, or reactivation.
- Keep passwords, MFA, patient data, copied claims, and exposed records out of the request.

User Management	Practices	Roles
User Management	**Practices**	**Roles**

03 / CURRENT-STATE REVIEW

Read the whole account before touching a checkbox

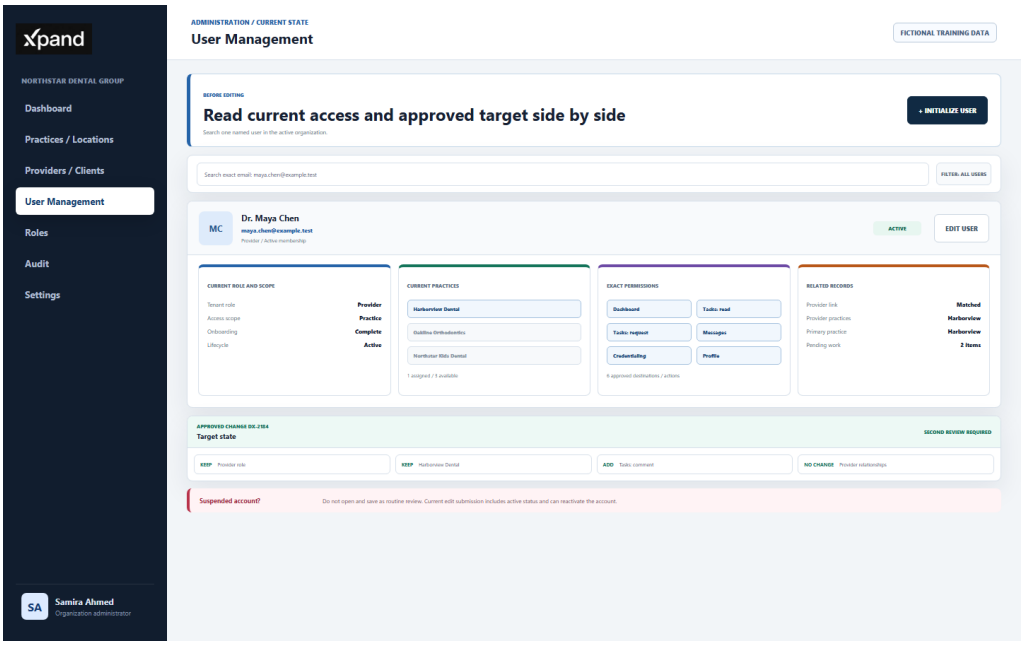

Figure 2. Fictional User Management review with identity, role, practice assignments, exact permissions, provider relationships, approved target, and suspended-account warning.

Review step	Administrator action	Why it matters
Organization	Confirm the active organization before searching.	A stale support or tenant tab can show the wrong context.
Identity	Search the exact email and verify the named person.	Repair the intended account instead of creating a duplicate.
Membership	Read role, status, onboarding, and access scope.	Role label alone does not show effective access.
Practices	Record every checked practice before making a change.	The submitted list replaces the current set.
Permissions	Record every exact page and action.	Role templates are not the authoritative saved list.
Suspension	Do not save routine edits on a suspended account.	The current edit payload includes active status and can reactivate it.

04 / ROLE AND PRACTICE SCOPE

Submit the complete approved practice list

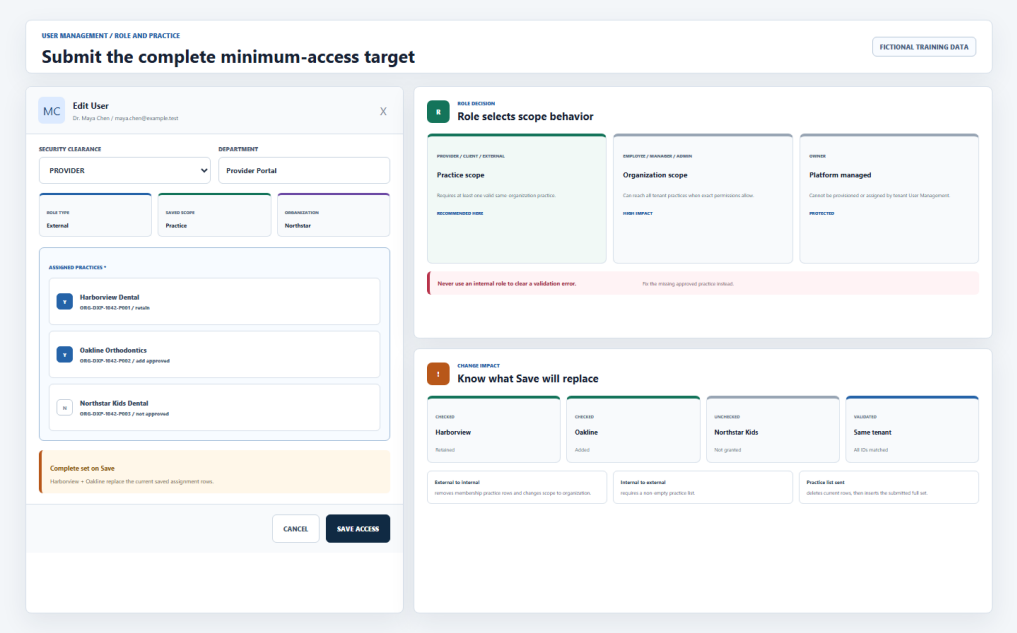

Figure 3. Fictional edit form showing Provider practice scope, retained and added practices, an unapproved practice, full-set replacement, role choices, and conversion impact.

Decision	Current behavior	Required control
Provider / Client / External	Membership uses practice scope and requires at least one valid practice.	Select the complete minimum same-organization set.
Internal role	Membership becomes organization scoped and practice access rows are removed.	Treat conversion as a high-impact expansion.
Owner	Provisioning and assignment are platform managed.	Tenant administrators cannot assign or terminate owner.
Checked practice	Included in the rebuilt membership practice set.	Keep every approved existing practice checked.
Unchecked practice	Absent after the saved set is rebuilt.	Remove only after handoff and explicit approval.
Practice ID	Backend verifies each ID belongs to the current organization.	Select through the UI; never paste or guess an ID.

Saving replaces the full set

The backend removes current membership practice access rows and inserts the submitted list. Read the final checkboxes against the approved target before Save.

05 / PROVIDER RELATIONSHIPS

Align directory identity, canonical practices, and login scope

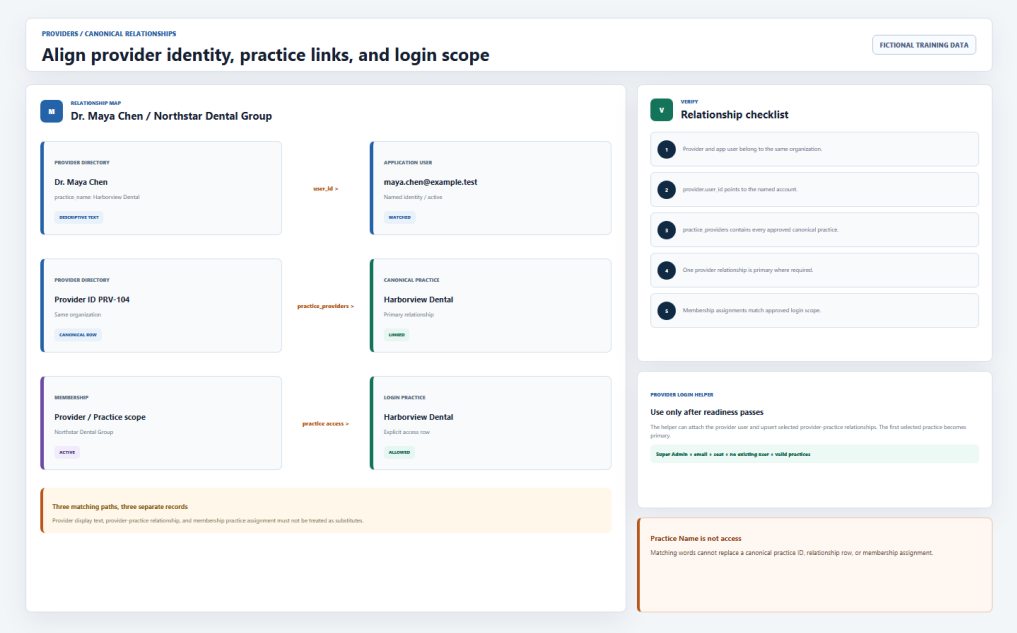

Figure 4. Fictional provider relationship map separating directory metadata, provider user linkage, canonical provider-practice rows, membership scope, and login practice access.

Record	Meaning	Verification
Provider practice_name	Descriptive directory text.	Never treat matching text as access.
Provider user_id	Links the provider row to the application user.	Confirm exact named account and same organization.
practice_providers	Canonical provider-to-practice relationships and primary marker.	Confirm every approved relationship separately.
membership_practice_access	Practices returned to the external login.	Review Assigned Practices and refreshed tenant context.
Provider Login helper	Can attach provider user and upsert selected provider-practice links; first selection is primary.	Use only after email, seat, authority, user, and practices pass readiness.
User Management edit	Updates membership role, practice set, identity fields, and permissions.	Do not assume it repairs every provider relationship.

Providers / Clients	User Management
Providers / Clients	**User Management**

06 / EXACT PERMISSIONS

Grant what the user can do inside the assigned practice

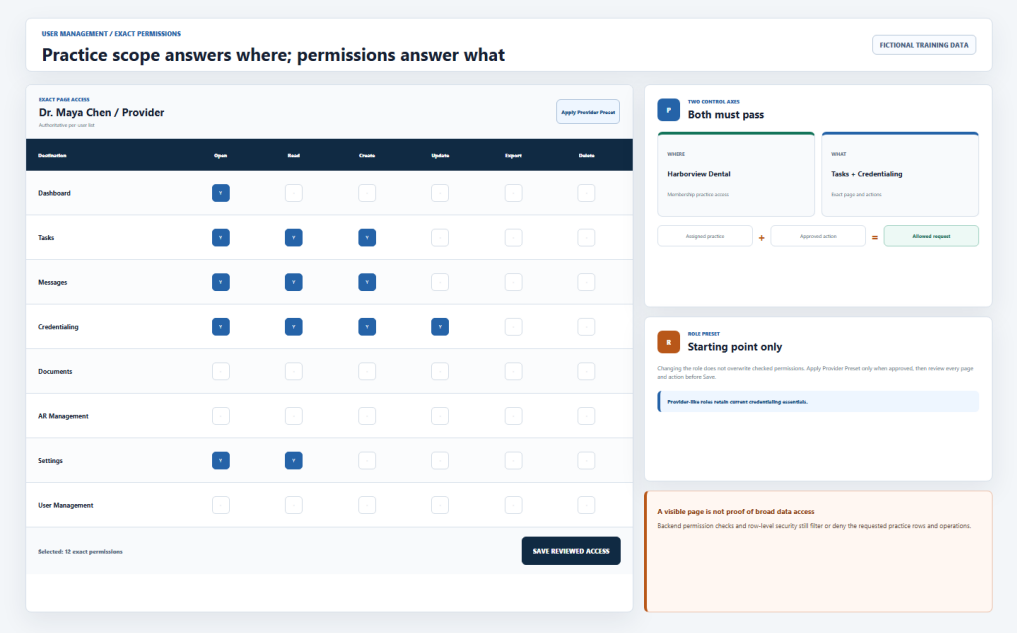

Figure 5. Fictional permission matrix separating practice scope from Dashboard, Tasks, Messages, Credentialing, Documents, AR, Settings, and User Management actions.

Control	Current behavior	Administrator rule
Saved permission list	Modern accounts reopen with their exact page permissions.	Start from the current list; compare every change.
Role selection	Changing role does not overwrite checked page permissions.	Role and permission review are separate steps.
Apply Role Preset	Pre-fills a role baseline when deliberately selected.	Treat as a starting point and inspect every page and action.
External credentialing baseline	Provider-like aliases retain current credentialing read, create, update, and page essentials.	Include this behavior in external-role approval.
Page permission	Controls whether a destination can open.	Grant only the minimum required page.
Action permission	Controls read, create, update, upload, send, manage, export, or delete where implemented.	Verify the exact approved action, not only page visibility.
RLS	Still filters returned rows by tenant and practice.	A visible page is not proof of broad data access.

07 / CONTROLLED CHANGE

Know every side effect before Save

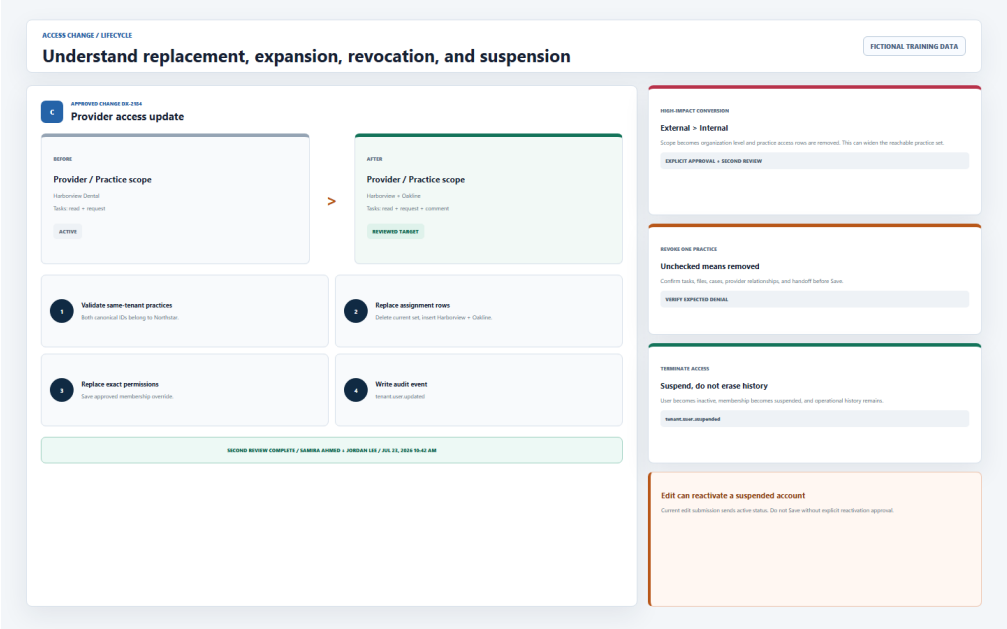

Figure 6. Fictional reviewed access update showing before and after state, assignment replacement, exact permissions, audit event, high-impact conversion, revocation, suspension, and reactivation warning.

Change	System effect	Required control
Add a practice	Final submitted set replaces current access rows.	Retain all approved existing practices.
Remove a practice	Unchecked practice is absent from the rebuilt set.	Complete work and data handoff first.
External to internal	Scope changes to organization and practice access rows are removed.	Explicit approval plus second review.
Internal to external	Scope changes to practice and requires at least one practice.	Select the complete approved minimum set before Save.
Permission edit	Submitted exact list updates user and membership override.	Compare old and new lists line by line.
Suspended account edit	Current edit submission includes active status.	Do not Save without explicit reactivation approval.
Successful update	Backend records tenant.user.updated.	Keep the request and verify effective access; audit alone is not a test.

08 / EFFECTIVE-ACCESS VERIFICATION

Test allowed work and expected denial from both sides

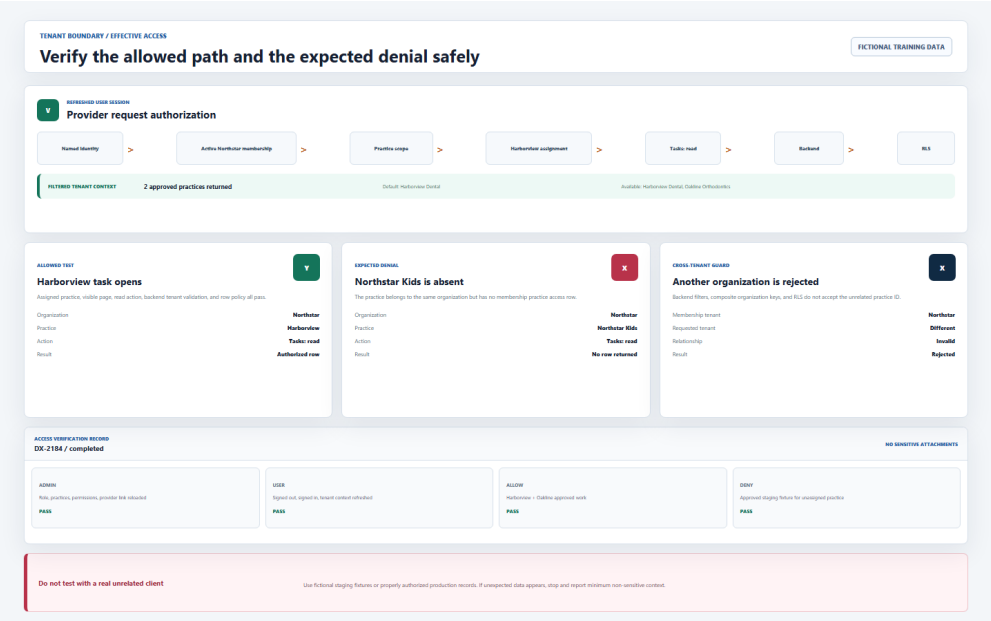

Figure 7. Fictional refreshed tenant context with approved practices, allowed Harborview task, expected same-tenant practice denial, cross-tenant rejection, and verification record.

Verification	Pass condition	Evidence
Admin state	Role, active status, exact practices, exact permissions, and provider link reload correctly.	Named tester and time; no secrets.
Fresh session	User signs out and in, then receives refreshed tenant context.	Expected organization and navigation.
Allowed practice	Approved fictional or authorized work opens and the exact action succeeds.	Practice, page, action, and result.
Expected denial	Approved staging fixture for an unassigned practice returns no row or safe denial.	Fixture ID or safe description, not real client data.
Cross-tenant guard	Unrelated organization relationship is rejected by normal checks.	Automated or approved staging test only.
Record result	Request contains tester, time, target state, passes, denials, and remediation.	No passwords, PHI, or exposed screenshots.

Do not test with a real unrelated client

Use fictional staging fixtures or properly authorized production records. If unexpected data appears, stop and report minimum non-sensitive context.

09 / TENANT ENFORCEMENT

Understand what protects the boundary after Save

Enforcement	Repository-backed behavior	Expected outcome
Tenant context	Practice-scoped memberships load membership access rows and filter active organization practices to those IDs.	Default practice is chosen only from the filtered list.
Tenant user routes	User reads and changes are restricted to the current organization.	Another tenant's user cannot be selected through the route.
Practice validation	Every submitted practice ID must exist in the current organization.	Invalid assignment request is rejected.
Composite foreign keys	Membership organization and practice organization must match.	Cross-organization practice access cannot be stored as valid.
can_access_practice	Organization scope can reach tenant practices; practice scope requires an explicit access row.	External user receives only assigned practice rows.
Write permission	Practice-aware write checks also require the corresponding table action permission.	Assigned practice without action permission remains read-only or denied.
Row-level security	Practice and tenant tables apply organization or practice predicates.	Typed routes, guessed UUIDs, and direct client requests do not widen access.
Acceptance tests	External fixture sees one assigned practice, no unassigned provider, no organization settings, and cross-organization keys are rejected.	Run approved staging tests after tenant-policy changes.

Isolation incident

If another provider, practice, organization, product, or Guardian Connect record appears, stop. Do not search, open more rows, copy, screenshot, download, change roles, send messages, or ask AI to analyze it. Report time, account, expected organization, route, safe action, and a non-sensitive symptom.

10 / SUSPENSION AND OFFBOARDING

Terminate login access while preserving operating history

1. Confirm the offboarding owner, effective time, and required handoff for tasks, cases, messages, documents, exports, and practice work.
2. Use Terminate access in User Management. The action requires approved authority, blocks self-deactivation, and protects the owner role.
3. Read the confirmation: user becomes inactive, membership becomes suspended, historical records remain, and tenant.user.suspended is recorded.
4. Review provider directory status and provider-practice relationships separately; login suspension does not automatically archive every related record.
5. Rotate or revoke payer portals, practice systems, mailboxes, recovery methods, API credentials, and downloaded data through their approved owners.
6. Verify the suspended membership no longer receives normal tenant context.
7. Do not open and save the account as a routine review; current edit submission can reactivate it.
8. Require a new explicit approval, target state, and full verification for any reactivation.

Protected action	Current behavior	Operator response
Deactivate self	Backend rejects the current actor's own account.	Use another authorized administrator and preserve separation of duties.
Edit owner	Tenant workflow treats owner as platform managed.	Use the approved DentalXpand platform process.
Delete history	Terminate access suspends rather than erasing operational records.	Retain records according to policy and legal requirements.
External credential rotation	Not automatically completed by DentalXpand suspension.	Coordinate separately with each system owner.

11 / TROUBLESHOOT AND COMPLETE

Fix the failed layer without broadening access

What you see	Likely layer	Correct first response
Assign at least one practice	External role has an empty set.	Select the minimum approved canonical practice; do not choose an internal role.
Practice assignment invalid	Submitted ID is not in the current organization.	Confirm organization and active practice through the normal UI.
User or provider not found	Wrong tenant, stale link, or mismatched identity.	Verify exact identity and tenant; do not recreate another account.
Page missing	Page permission is absent.	Grant only the narrow approved page or action.
Page visible, no rows	Assignment, relationship, row policy, or record ownership does not match.	Verify the specific layer; do not grant Admin.
Practice disappeared	Replacement set omitted it or practice was archived.	Review target and audit, then restore only when authorized.
Suspended user active	An edit Save submitted active state.	Suspend again if appropriate, preserve evidence, and review the change.
Wrong tenant or product	Isolation, session, context, query, cache, deployment, or policy failure.	Stop immediately and report without reproducing exposed data.

Completion check

- I can separate user, membership, role scope, practice access, exact permissions, and provider relationships.
- I record current state and one complete approved target before editing.
- I use external practice scope correctly and understand full-set replacement.
- I verify provider linkage and canonical practice relationships separately from login scope.
- I review every exact page and action and treat role presets as optional starting points.
- I require extra approval for internal-role conversion, multi-practice expansion, or reactivation.
- I verify refreshed admin and user state, an allowed action, and a safe expected denial.
- I understand backend, composite keys, and RLS protect the boundary beyond the interface.
- I suspend access while preserving history and handle related systems separately.
- I stop immediately at cross-tenant, cross-practice, cross-product, or Guardian Connect exposure.

Next lesson
Continue with Operate a DSO or multi-practice workspace for organization overview, practice switching, shared teams, scoped records, and comparison workflows. Also open the website guide, previous lesson, or all resources.