DENTALXPAND LEARNING CENTER / START HERE

Roles, Permissions, and Access Boundaries

A complete guide to protected and custom roles, exact page and action permissions, authoritative per-user access, organization and practice scope, direct-route handling, backend authorization, row-level security, and controlled verification.

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

All product states and people in this guide are fictional. Never use live patient, provider, practice, employee, credential, password, token, or unredacted third-party 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.

Administrator reading path
Read the access model first, then follow the role and user workflows. Finish with both allowed and denied verification before closing a permission change.

01 / ACCESS MODEL

Understand defense in depth

DentalXpand does not treat a job title, menu item, or hidden button as the complete security decision.

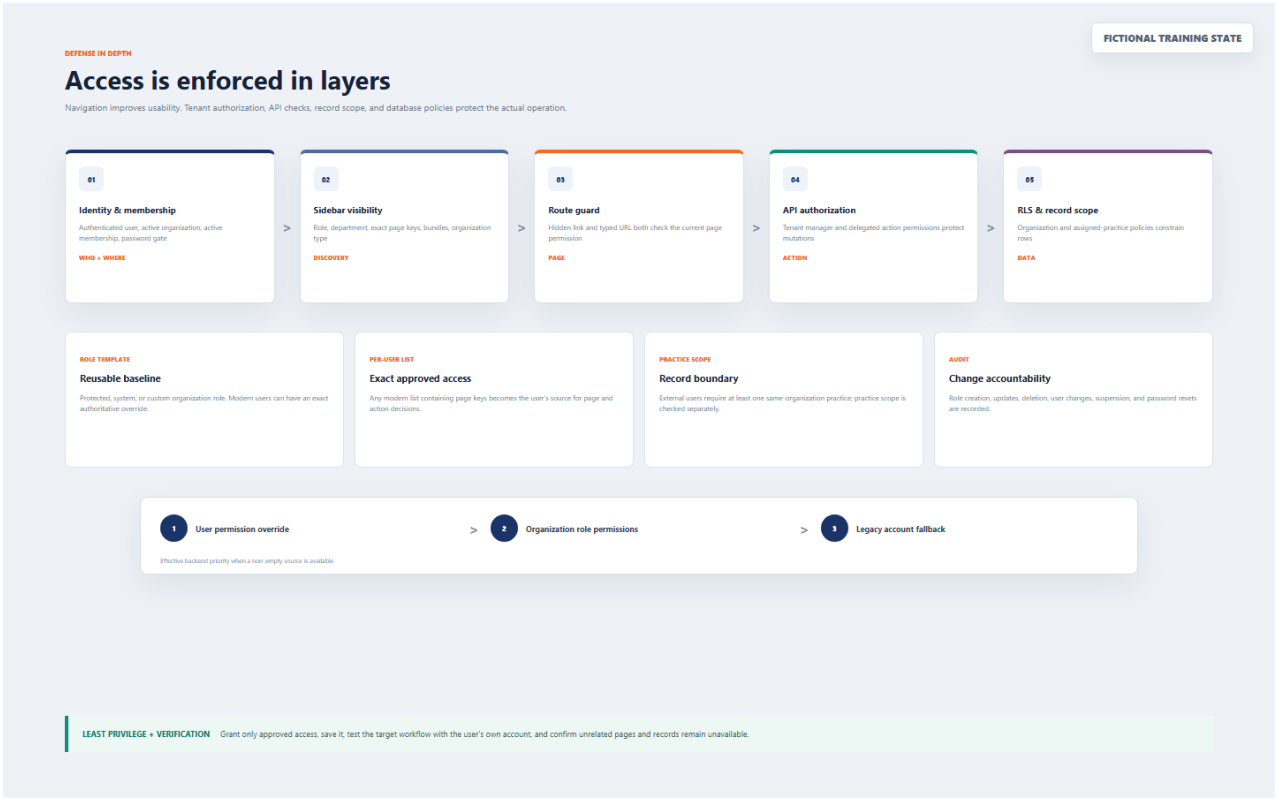

Figure 1. Fictional defense-in-depth map from identity and membership through page, API, practice, row-level, and audit controls.

> Navigation is not the security boundary
> A visible link does not grant unrestricted data access, and a hidden link is not permission to guess a direct URL.

01A / FIVE DECISIONS

Know the five access decisions

Layer	Decision	Boundary
1. Identity	Authenticated individual account	Shared or borrowed credentials are not acceptable
2. Membership	Active organization and membership, completed password gate	Suspended or unavailable context blocks normal access
3. Page	Exact page, qualifying bundle, role, or department route rule	Determines whether a protected destination opens
4. Action	View, create, update, approve, export, delete, reset, or admin grant	A visible page does not imply every operation
5. Record	Organization, practice, ownership, and database policy	A permitted module does not expose out-of-scope rows

Expected layered behavior
A user can open a page yet remain unable to approve, export, delete, or reach records outside the permitted scope.

02 / SEPARATE CONCEPTS

Separate role, department, designation, scope, and status

Concept	What it means	What it does not prove
Role	Reusable permission template and responsibility label	Does not automatically replace a modern exact user list
Department	Can qualify Billing, HR, or Marketing route families	Does not grant every page or action in the department
Designation	Job title and profile metadata	Not itself a security grant
Access scope	Organization-wide or assigned-practice records	Does not grant a feature page
Membership status	Invited, pending password, active, or suspended	Cannot be repaired by adding page keys
Support context	Explicit audited platform entry to a tenant	Not informal account switching or impersonation

Review organization and practice context

03 / ROLE TYPES

Know protected, system, and custom roles

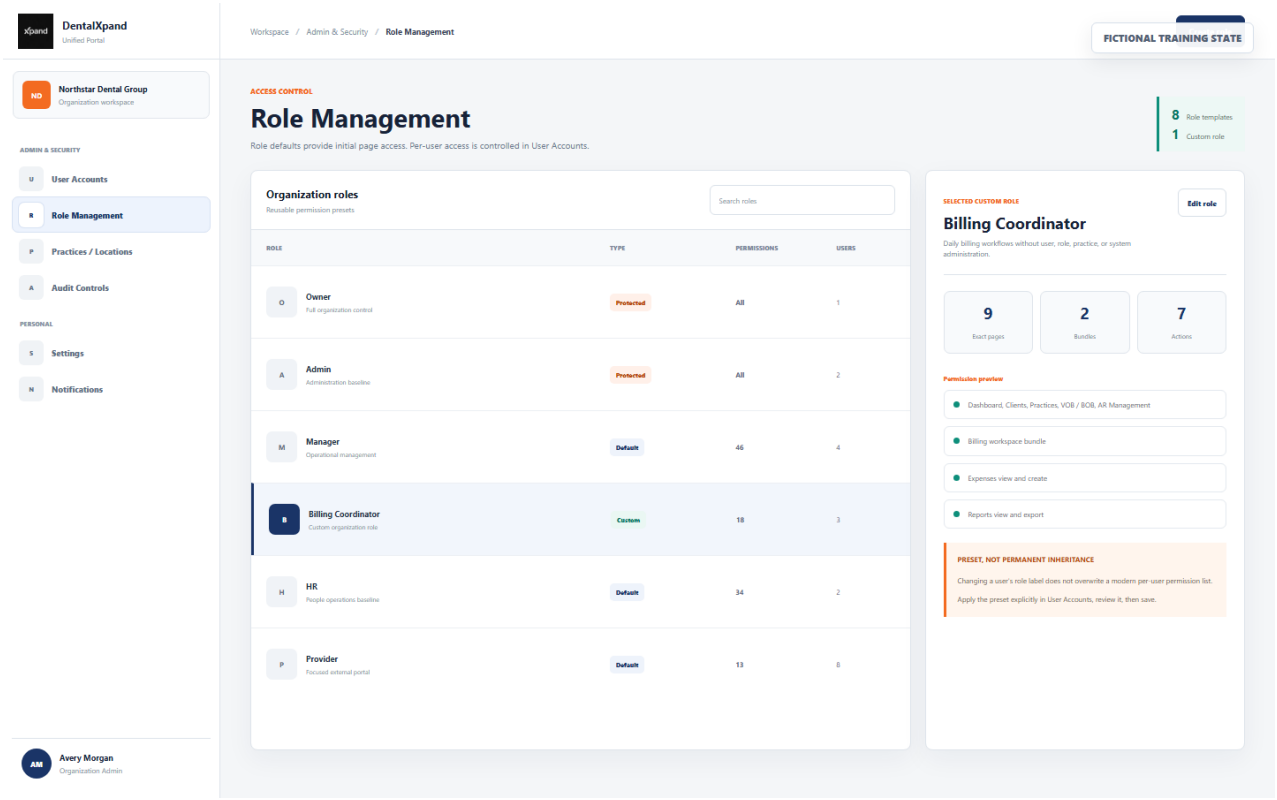

Figure 2. Fictional Role Management screen with protected Owner and Admin roles, default baselines, and a selected custom Billing Coordinator preset.

> Role is a preset, not permanent inheritance
> Changing a role label does not overwrite a modern user's exact page and action list.

03A / ROLE BOUNDARIES

Use each role type correctly

Role	Purpose	Important rule
Organization Owner	Protected full authority	Platform-provisioned; cannot be assigned in normal User Accounts
Admin	Protected privileged organization administration	Use only for real administrative responsibility
Manager / HR / Finance / Employee	System or default baselines	Review the actual per-user list
Provider / client / external	Focused portal baseline	Requires at least one same-organization practice
Guest	Minimal compatibility baseline	Do not use as a substitute for a reviewed custom role
Custom organization role	Reusable tenant-specific preset	Can be edited or deleted only under tenant authorization
Platform administrator	Separate SaaS control context	Tenant access requires an authorized support session

Do not promote for convenience

Admin and Owner are not shortcuts for resolving one missing operational page.

04 / PERMISSION MATRIX

Understand the permission matrix

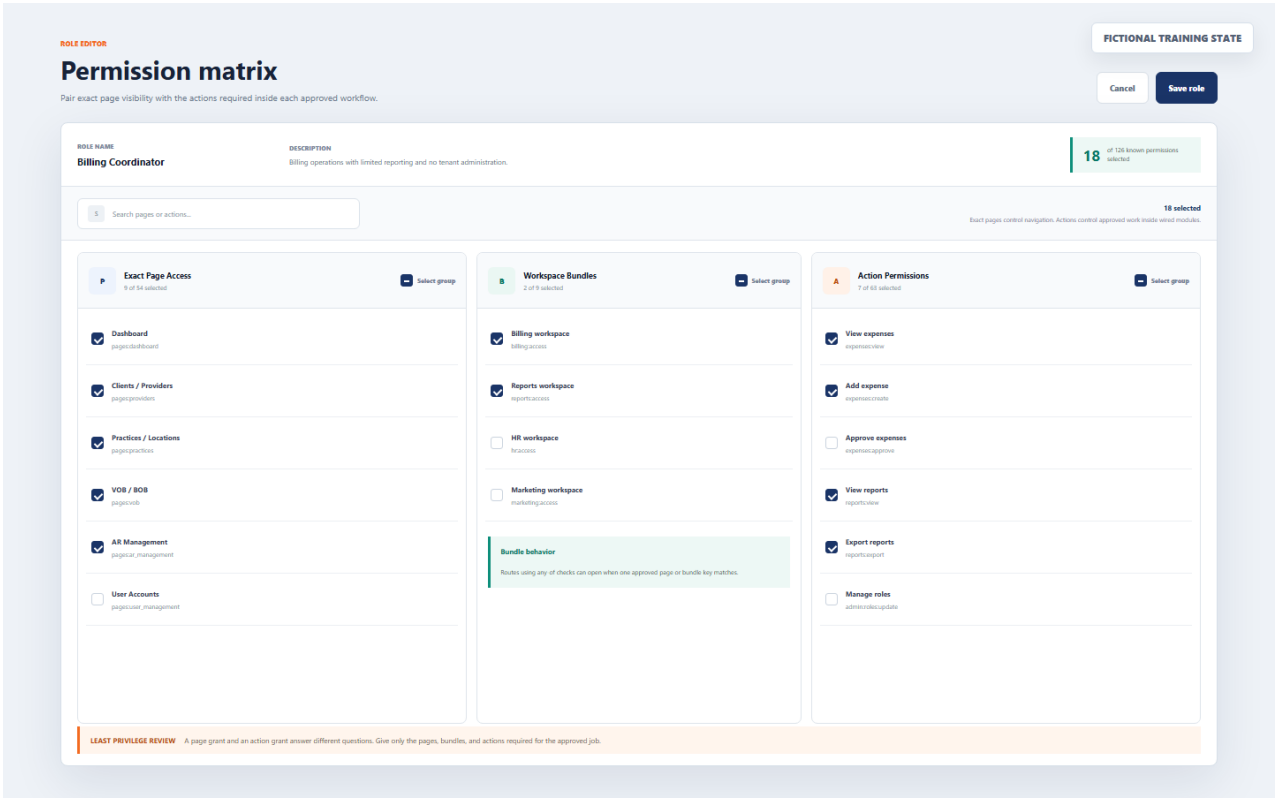

Figure 3. Fictional matrix separating Exact Page Access, Workspace Bundles, and Action Permissions.

> Search and count before saving
> Search can match a group, label, or key. An indeterminate group checkbox means only part of the group is selected.

04A / PERMISSION TYPES

Distinguish pages, bundles, actions, and wildcard

Type	Example	Purpose
Exact page	pages:dashboard, pages:vob, pages:roles	Protected destination and matching route guard
Workspace bundle	billing:access, reports:access	Can satisfy routes using an approved any-of rule
Action	expenses:create, reports:export	Operation inside an approved workflow
Administrative action	admin:roles:update, admin:users:reset_password	Narrow tenant administration operation
Wildcard	*	Protected full-access source; inappropriate for ordinary custom roles

Action enforcement is workflow-specific

Test the actual target control and API after a change. Do not assume every button in every module uses the same action key.

05 / NEW USER

Know the safe new-user starting point

Initial key	Destination	Purpose
pages:profile	My Profile	Own identity and profile context
pages:notifications	Notifications	Personal operational alerts
pages:settings	Settings	Permitted personal settings
pages:xpand_ai	Xpand AI	Page key only; availability and data boundaries still apply

A newly created account starts with the Employee role label and these four permission keys. An administrator then applies an approved preset or chooses exact operational access.

> Profile can be the correct landing page
> If Dashboard is not granted, DentalXpand can route a normal user to My Profile. Do not grant Dashboard only to change the landing screen.

06 / ROLE ADMINISTRATION

Get authorized for Role Management

Operation	Relevant authorization	Boundary
Open page	Role page access or admin:roles	Active organization only
Create	admin:roles or admin:roles:create	Tenant-scoped custom role
Update	admin:roles or admin:roles:update	Protected roles remain backend-protected
Delete	admin:roles or admin:roles:delete	Protected and assigned roles are rejected

Backend is the source of truth
A protected or cross-organization operation remains invalid even if a client-side control is manipulated.

07 / REVIEW AND CREATE

Review an existing role, then create carefully

1. Confirm the active organization before reading or changing a role.
2. Identify Protected, Default or system, and Custom labels.
3. Read the description, page count, bundle count, action count, and current assignments.
4. For a new role, use a responsibility name rather than a person's name.
5. Document required outcomes and exclusions before selecting permissions.
6. Start the custom role empty, add exact approved pages and actions, then save.
7. Test with one authorized demonstration account before broad assignment.

> A custom role begins empty
> The role name does not silently grant a department, page, action, organization, or practice.

08 / EDIT AND RETIRE

Edit or delete a custom role safely

1. Identify every user or membership that uses the custom role.
2. Compare current and proposed page, bundle, and action keys.
3. Use a per-user exception for one person's exceptional need instead of broadening the shared role.
4. Choose and approve a replacement before retiring a role.
5. Reassign each user and review their modern exact permissions.
6. Verify required and denied workflows for each affected responsibility.
7. Delete only after no memberships reference the custom role.

> Deletion can be blocked
> The backend rejects protected roles and custom roles still assigned to memberships. Reassign first, verify, then delete.

09 / USER ACCESS

Understand authoritative per-user access

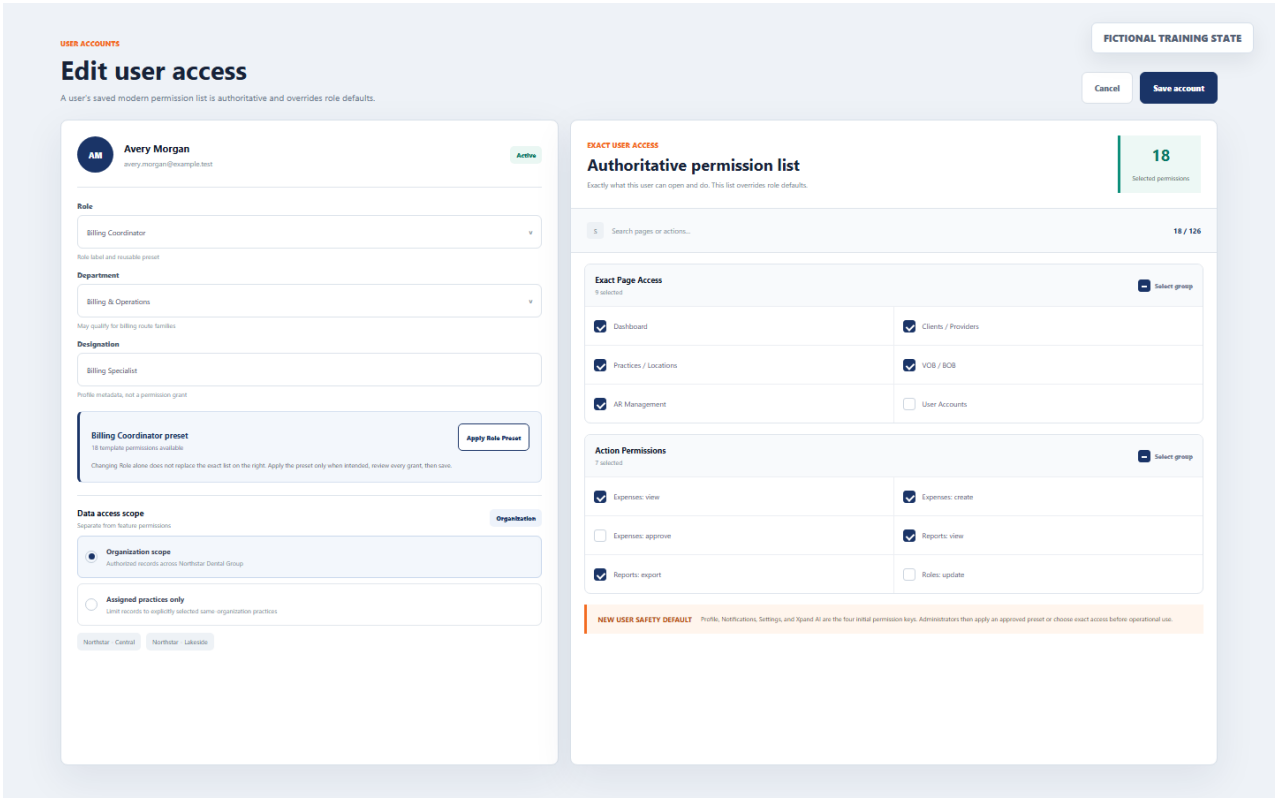

Figure 4. Fictional User Account editor showing role, department, designation, explicit preset action, exact permissions, and organization or practice scope.

> Changing Role alone does not rewrite access
> The role dropdown changes the responsibility label. The modern exact list remains unchanged until an administrator deliberately applies and saves a reviewed preset or edits the list.

09A / RESOLUTION RULES

Know how role and user permissions resolve

Saved state	Resolution	Administrator response
Modern list has any pages:* key	Exact user list is authoritative	Role defaults are not merged
Legacy list has no page key	Compatibility merge with role baseline	Next reviewed save creates a modern exact list
Role contains wildcard	Protected full access	Use only for approved privileged roles
Client/external alias	Focused portal essentials are normalized	Practice scope and same-organization validation still apply

Role edits are not automatic bulk updates

Review User Accounts and explicitly apply or adjust intended exact lists for affected modern users.

10 / APPLY PRESET

Apply a role preset intentionally

1. Open User Accounts with permission to update the user and manage permissions.
2. Confirm user name, email, status, organization, and current scope.
3. Choose the intended role; remember this changes the label only.
4. Select Apply Role Preset to prefill the template plus personal defaults.
5. Review every exact page, bundle, and action; remove unnecessary grants.
6. Review organization or assigned-practice scope separately.
7. Save the account and confirm the update succeeds.
8. Use the target user's own account and a fresh sign-in for verification.

> Preset is an explicit prefill
> Applying the preset is optional and reversible before save. It is not final until the account update succeeds.

11 / PAGE AND ACTION

Pair a destination with only the required operations

Requirement	Page	Review actions	Avoid
Enter expenses	Expenses page	View + create	Approve, delete, export
Approve expenses	Expenses page	View + approve	User or role administration
Read reports	Reports page or bundle	View	Export without need
Export reports	Reports destination	View + export	Broad finance administration
Manage roles	Role Management	Create/update/delete as assigned	Full Admin for one operation
Reset password	User Accounts	Reset-password action	Create, deactivate, or manage permissions

Page and action answer different questions
When a page opens but an approved action fails, inspect that action and its API. Do not grant the entire permission group.

12 / PRACTICE SCOPE

Configure provider and client practice access

1. Select the approved provider, client, customer, practice, client-provider, or external role.
2. Assign at least one practice from the same active organization.
3. Review focused portal pages such as credentialing, AR, tasks, chat, AI, notifications, profile, and settings.
4. Grant only required upload, edit, export, or workflow actions.
5. Save, then verify each assigned practice and one intentionally unassigned practice.
6. Stop and report if any other organization's practice or records appear.

> Feature access cannot defeat practice scope
> Tenant API and row-level policies still restrict records to the active organization and approved practice assignments.

Continue to practices, locations, and assignments

13 / UNAUTHORIZED

Handle Access denied correctly

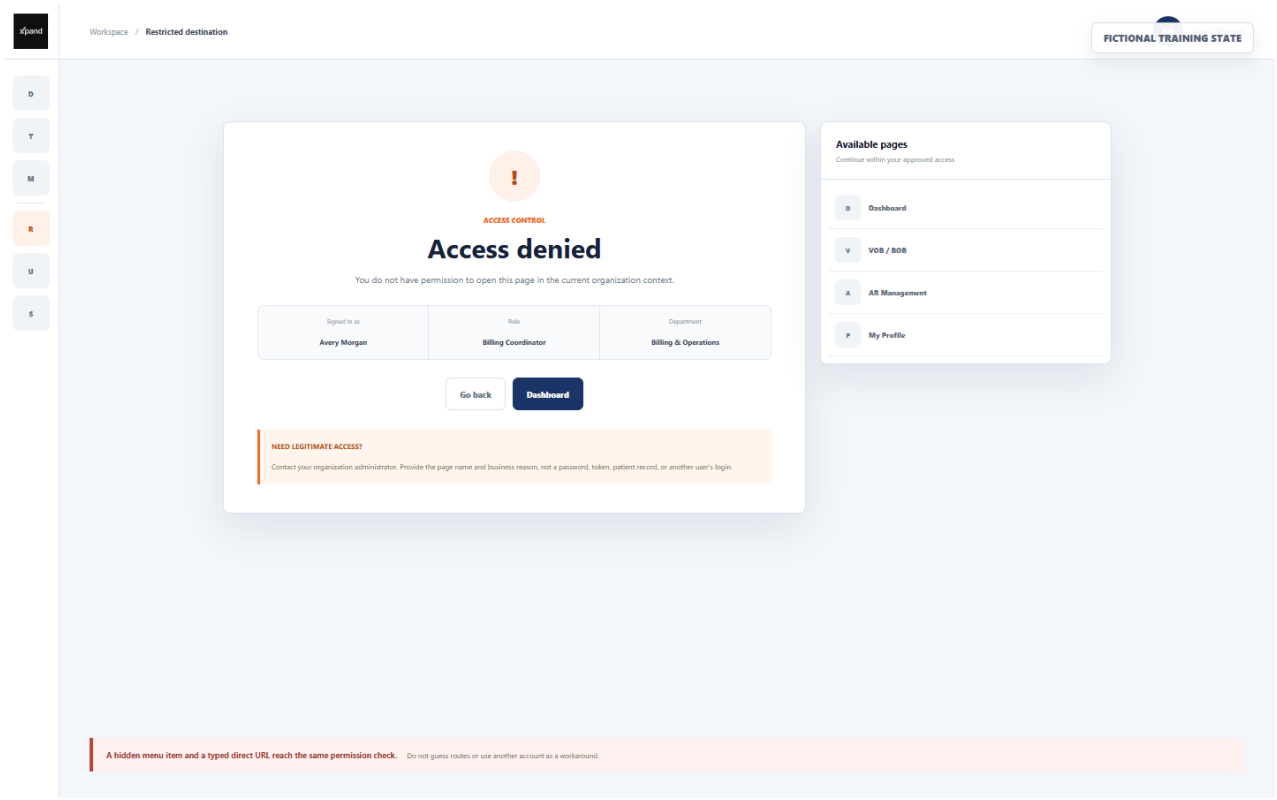

Figure 5. Fictional Access denied screen with user, role, department, safe navigation, available pages, and an administrator request path.

A typed URL uses the same check

A hidden menu item and a manually entered protected route reach the same page-permission decision.

13A / SAFE RESPONSE

Respond without bypassing controls

Step	Correct action
Read context	Confirm page name, user, role, department, and organization
Return safely	Use Go back, Dashboard, My Profile, or another available page
Request review	Provide page name, business reason, and required action to an authorized admin
Protect secrets	Do not send passwords, tokens, PHI, or sensitive screenshots
Re-test	After approval, use the user's own account and verify allowed and denied behavior

Never use a workaround
Do not borrow an administrator account, alter browser storage, guess routes, or request Admin for one missing task.

14 / BACKEND ENFORCEMENT

Understand API, organization, practice, and RLS controls

Layer	Decision	Example protection
Tenant context	Active organization and membership; password gate complete	Blocks suspended or unavailable workspaces
Frontend route	Exact page, bundle, role, or department	Redirects unauthorized direct routes
Tenant API	Manager authority or delegated action key	Protects role and user mutations
Organization validation	User, role, and practice belong to active tenant	Rejects cross-organization assignments
Practice scope	Record belongs to an assigned practice	Blocks unassigned practice rows
Database RLS	Table, action, tenant, and practice policy	Protects rows behind application requests
Audit	Administrative event recorded	Supports review and accountability

Client-side success is not enough

A rendered button does not prove the API or database will authorize the operation. Confirm the saved response and actual workflow result.

14A / EFFECTIVE SOURCE

Know the backend permission-source priority

Priority	Source	Condition
1	Membership permission override	Used when a non-empty override exists
2	Organization role permissions	Used when the role has a non-empty permission set
3	Account custom permissions	Compatibility fallback for the app user

The normal tenant User Account workflow saves the exact permission list to the account and membership override so frontend and backend decisions stay aligned.

> Data scope remains separate
> Even a matching action permission cannot authorize another organization or an unassigned practice row.

15 / CHANGE CONTROL

Apply a controlled permission change

1. Document requester, approver, reason, organization, practices, pages, actions, start date, and review date.
2. Inspect current role, department, designation, status, exact permissions, and scope.
3. Choose the narrowest change: per-user exception for one person, custom role for repeatable responsibility.
4. Save once and confirm the account or role update succeeds.
5. Refresh authorization through a fresh sign-in when practical.
6. Test the required page and action with fictional or non-sensitive data.
7. Test unrelated pages, high-risk actions, organizations, and practices remain unavailable.
8. Record the result, exception, rollback, and next review date.

> Authorization refresh
> The app refreshes role and permission profile after sign-in, when the window regains focus, and periodically. A fresh sign-in is the clearest verification.

16 / VERIFY BOTH SIDES

Test approved and denied behavior

Area	Allowed test	Denied test
Identity	Correct individual account and organization	Another user's login is never used
Navigation	Approved page appears when expected	Unrelated admin and department pages remain hidden
Direct route	Approved URL opens	Unapproved URL redirects to Unauthorized
Action	Required create/update/approve/export succeeds	Unapproved high-risk action is blocked
Practice	Assigned practice records are available	Unassigned practice is unavailable
Organization	Current tenant data is available	Another tenant never appears
Audit	Expected administrative event is recorded	No unexplained changes remain

Verification result

The user can complete the approved job while unrelated pages, actions, organizations, practices, and sensitive exports remain unavailable.

17 / TROUBLESHOOT

Troubleshoot page and role behavior

Symptom	Likely reason	Correct response
Page missing	Page, bundle, role, department, portal, or org rule	Inspect authoritative user list
Direct URL denied	Route guard rejected page decision	Return safely; request least privilege
Role changed, menu did not	Modern exact list was not overwritten	Apply preset, review, save, re-test
Preset appears ineffective	Account not saved or state not refreshed	Save, fresh sign-in, verify
Page opens, action fails	Action/API/record scope rejected	Inspect exact action and row context
Profile is landing page	Dashboard not granted	Confirm intent before adding Dashboard

Continue to page permissions and direct-route security

17A / TROUBLESHOOT SCOPE

Troubleshoot practice, status, and protected roles

Symptom	Likely reason	Correct response
External user will not save	No same-organization practice	Assign at least one valid practice
Custom role will not delete	Memberships still reference it	Reassign and verify users first
Protected role rejected	Owner or protected system role	Use a custom role or platform process
Wrong practice data	Scope error or security incident	Stop, sign out, report immediately
User remains suspended	Membership status is a separate gate	Use authorized lifecycle workflow
Action differs by module	Different wired permission or API	Test exact workflow; report safe error text

Protect incident details
Never email passwords, setup links, tokens, patient data, or unredacted sensitive screenshots while troubleshooting.

18 / COMPLETION

Verify that this lesson is complete

- I can separate role, department, designation, scope, and membership status.
- I understand protected Owner and Admin responsibilities.
- I can distinguish exact pages, bundles, actions, and wildcard access.
- I know the four initial permission keys for a new user.
- I understand why a modern pages:* list is authoritative.
- I know changing the role dropdown alone does not rewrite exact access.
- I can apply, review, save, and verify a role preset.
- I can pair a page with only the required actions.
- I can configure and test same-organization practice scope.
- I know how to respond to Access denied without bypassing controls.
- I understand API, RLS, practice, and audit enforcement behind the interface.
- I can verify both approved and intentionally denied behavior.

Ready for feature training
The next lesson explains the Dashboard command center and its role-specific operational signals.

19 / CONTINUE

Continue through DentalXpand learning

Previous lesson	Next lesson	All resources
Previous lesson	Next lesson	All resources

Related administrator lessons

- Manage user accounts and lifecycle
- Create and manage roles
- Configure page permissions and direct-route security
- Manage practices, locations, and assignments
- Understand organization and practice context

Website guide: Roles, permissions, and access boundaries
Support: support@xpand.dental
Website: xpand.dental