DENTALXPAND LEARNING CENTER / START HERE

Understand the DentalXpand Workspace

A complete first-session guide to secure sign-in, organization and practice scope, role-based navigation, permissions, daily security, and the correct learning path.

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

Uses fictional demonstration screenshots. Do not use live patient, provider, employee, payer, or financial data in training materials without authorization.

Contents

Select any section in supported PDF viewers. Every content page includes a clickable Contents link in the upper-right corner.

How to use this guide
Read sections 1 through 8 before feature training. Then choose the role-based path in section 9. Finish with troubleshooting and the completion checklist.

01 / PREPARE

Before you begin

Use an individual account created by an authorized organization administrator. Shared accounts are not appropriate for DentalXpand access.

- Have your individual organization email address and temporary password or password-setup invitation.
- Use only the application URL supplied by your organization.
- Know the organization, DSO, billing company, or practice you expect to enter.
- Use a private device or trusted organization-managed workstation.
- Confirm unexpected invitations with your administrator or support@xpand.dental.

> Stop if the invitation looks wrong
> Confirm the sender, company name, and destination URL before opening a password link.

02 / ACCESS

Sign in safely

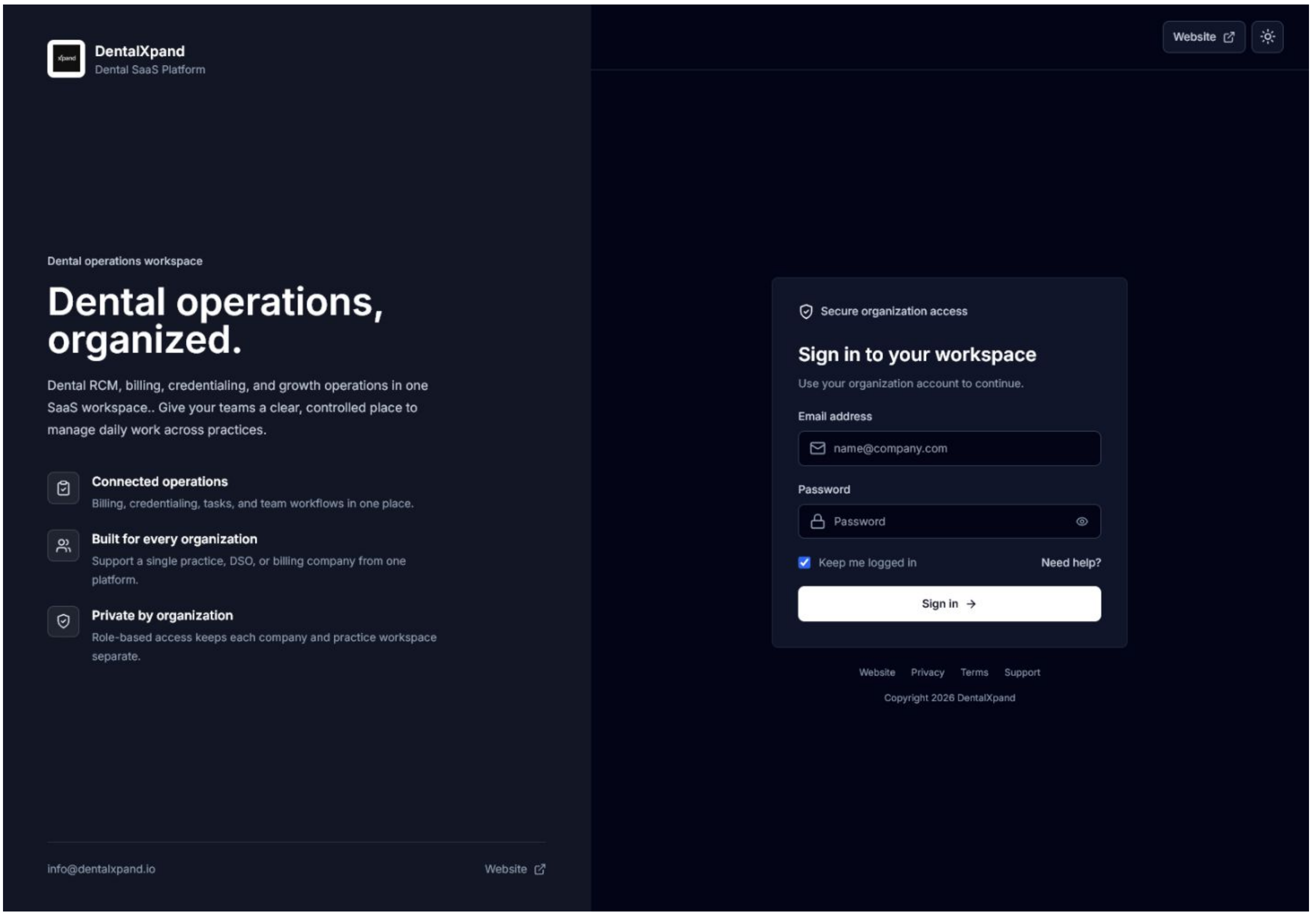


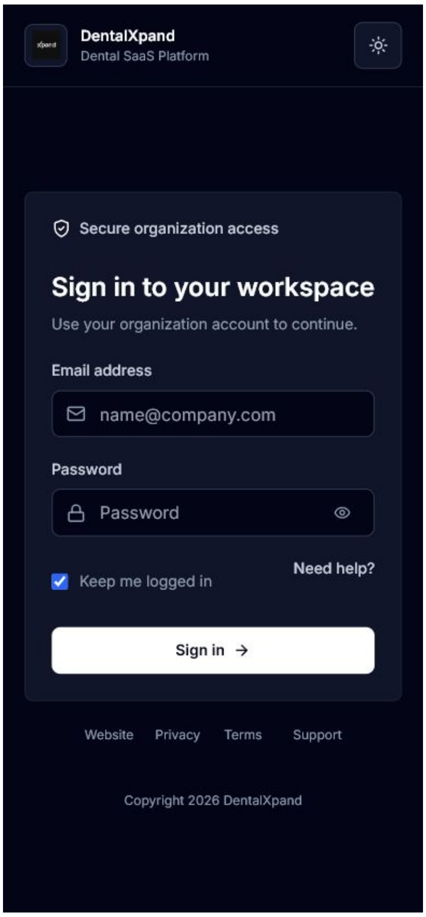
Figure 1. Desktop sign-in screen with organization access, email, password, session preference, help, and sign-in controls.

1. Open the approved application URL and confirm the domain.
2. Enter the exact email attached to your DentalXpand membership.
3. Enter your password; reveal it only when nobody else can view the screen.
4. Use Keep me logged in only on a private or organization-managed device.
5. Select Sign in once and allow account and tenant context to load.
6. When password setup is required, create at least eight characters and enter matching confirmation.

> Repeated failed sign-ins
> Wait for any displayed countdown instead of retrying. A persistently blocked account requires an administrator-assisted reset.

02A / MOBILE

Mobile sign-in uses the same controls



Mobile checklist

1. Confirm the DentalXpand logo and secure organization access heading.

2. Enter your email and password.

3. Leave Keep me logged in off on a shared phone or tablet.

4. Use Need help? for the approved support route.

5. Sign in once and wait for the workspace to load.

Open the current website version of this guide

03 / SCOPE

Confirm the correct workspace context

After authentication, DentalXpand loads the organization membership, plan, branding, permitted practices, and access scope for the account.

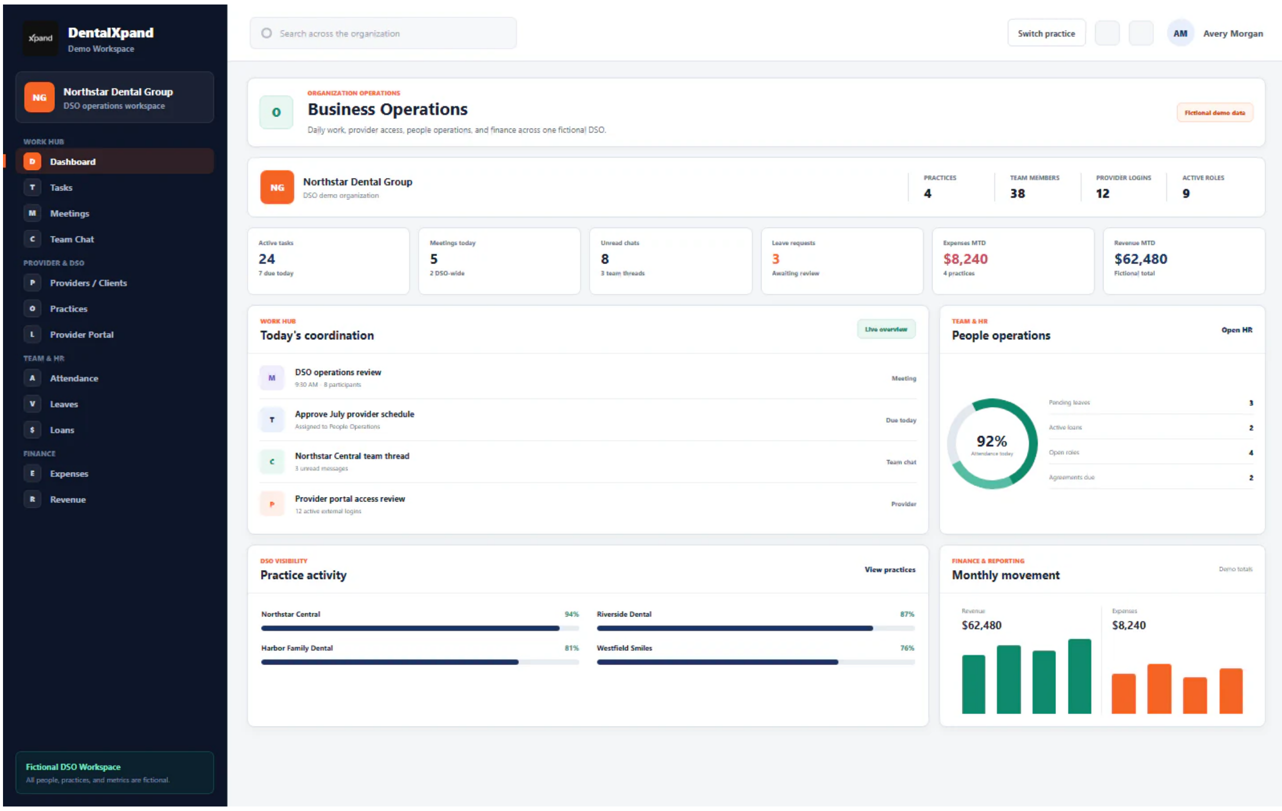


Figure 2. Fictional DSO workspace demonstrating organization-wide and practice-aware context.

Context	Meaning
Organization	The company-level data boundary, such as a practice group, DSO, or billing company.
Practice	A dental location or client practice. Access may be limited to selected practices.
Membership	Your active role, status, permissions, access scope, and password requirements.
Role	A baseline access profile such as admin, HR, finance, employee, provider, or an organization-defined role.
Support session	Explicit, audited temporary workspace access for authorized platform support.
Platform admin	A SaaS-level operator who remains outside a client workspace unless an authorized support session exists.

Data-boundary check
If the organization, practice, client, provider, employee, or patient context is unexpected, do not open, edit, export, copy, or discuss the record. Sign out and report the mismatch immediately.

04 / NAVIGATE

Understand the workspace screen

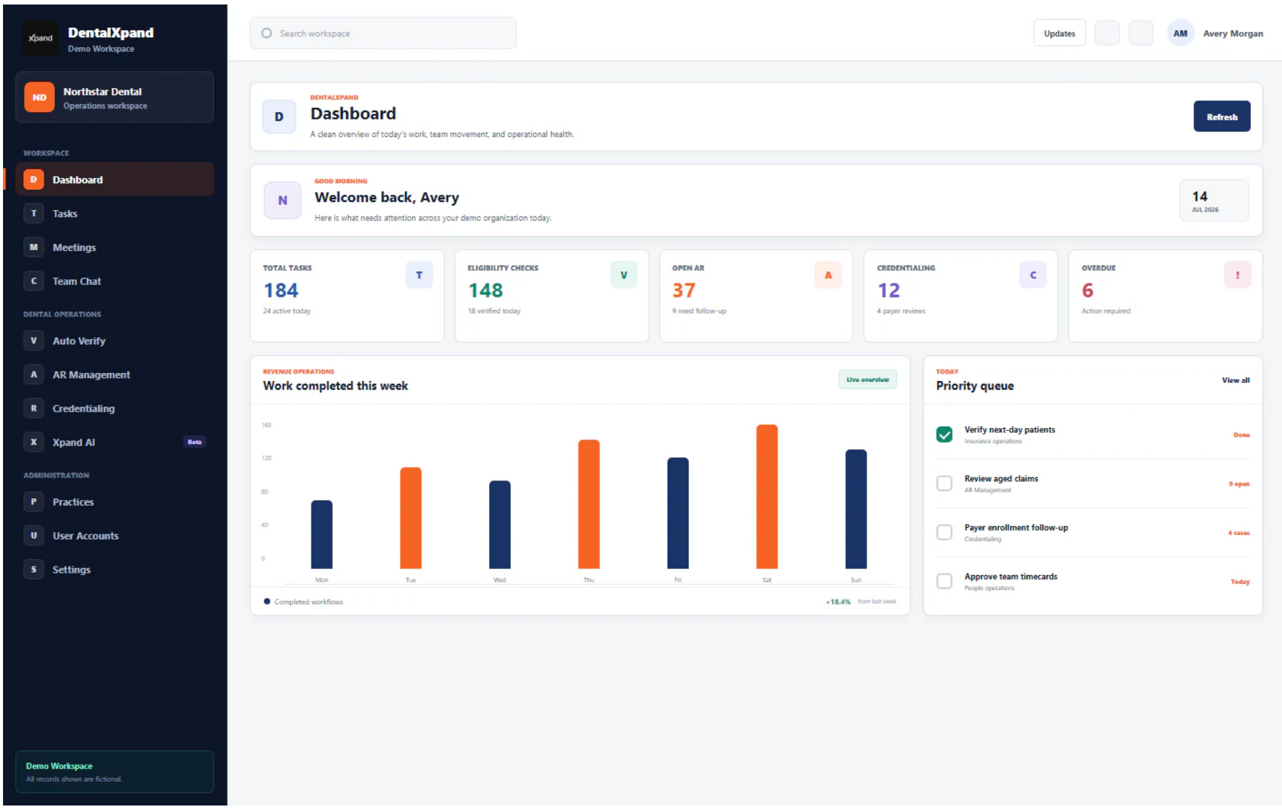


Figure 3. Fictional dashboard showing the stable sidebar, header, summary, and priority areas.

Area	Purpose
1. Organization identity	Confirms the active company or workspace.
2. Role-aware sidebar	Shows permitted groups and pages. It collapses on desktop and opens as a drawer on mobile.
3. Current page trail	Names the current page before you change data.
4. Search	Supports workspace or feature-level discovery where implemented.
5. Utilities	Updates, Settings, theme mode, and Notifications.
6. User menu	Profile, Settings, displayed identity, and Logout.

05 / PLATFORM MAP

Know where each type of work belongs

The sidebar is intentionally filtered. A user is not expected to see every module.

Learning track	Included work
Work Hub	Dashboard, Tasks, Meetings, Messages, Notifications, Documents, Profile, Support, and Xpand AI.
Client and RCM	Providers or Clients, Practices, Client Agreements, AR Follow Up, AR Management, and Medical Billing OS.
Dental RCM	Client Instructions, VOB or BOB, Auto Verify, Auto AR, and VOB Auto-Fill.
Credentialing	Provider portal, Provider Data, payer workflow, and client-facing reports.
Marketing and Growth	Lead Generation, Leads Directory, Cold Calling CRM, Email Outreach, and Marketing Scraper.
Team and HR	Teams, Attendance, Leaves, Loans, Directory, Recruitment, Agreements, and Employee Notices.
Finance and Reports	Authorized Expenses, Revenue, approvals, exports, and management reporting.
Admin and Security	Employees, User Accounts, Roles, Practices, Data Intelligence Vault, and platform controls.
AI and Automation	Permission-aware Xpand AI, approved knowledge, continuous learning, and NATO Phonetics.
System	Personal and organization settings, downloads, branding, integrations, and configuration.

06 / PERMISSIONS

Understand page access and action permissions

Access is checked at sign-in, tenant, page, action, and record-scope levels.

Step	Access layer	Decision
1	Authenticated account	A valid user session must exist.
2	Active tenant context	Organization and membership status must allow access.
3	Page permission	The role or individual user must receive the page.
4	Action permission	Create, edit, approve, export, delete, and administration actions may require separate grants.
5	Record scope	The record must belong to the permitted organization, practice, team, or owner context.

- Admins and super admins pass standard workspace checks but still operate inside the active tenant boundary.
- HR, billing or operations, and marketing routes can use department membership or explicit permission.
- Provider and client roles receive focused portal navigation and essential portal permissions.
- Restricted users may land on My Profile when Dashboard is unavailable.
- Unauthorized means access was not granted. Request least-privilege access instead of borrowing another account.

07 / FIRST SESSION

Complete the first-session checklist

1. Confirm your displayed name and email in the user menu.
2. Confirm the organization and, when applicable, the practice or client context.
3. Check that the sidebar contains only the pages required for your work.
4. Verify department, designation, and contact information in My Profile.
5. Review unread operational alerts in Notifications.
6. Choose a preferred theme in Settings.
7. Open Dashboard when permitted and verify that the summary belongs to the expected workspace.
8. Locate Support Hub and record the approved escalation method.
9. Sign out once and confirm you can return through the approved sign-in page.

Expected result
You can identify your account, organization, role, page access, security controls, and next training track without opening live operational records.

08 / SECURITY

Protect the workspace during daily use

DO	DO NOT
Use only your own account. Confirm context before changing data. Lock the device when stepping away. Use Logout on shared devices. Report unexpected access or AI responses.	Share passwords or invitations. Save credentials in unapproved tools. Copy PHI into personal services. Capture live records for training without approval. Use AI across organization boundaries.

09 / LEARNING ORDER

Choose the correct learning path

Role	Begin with	Continue to
Every user	Start Here, Sign-in, Navigation, Profile, Notifications	Granted Work Hub modules
Provider or client	Provider portal and practice context	Credentialing, Tasks, Messages, permitted AR
Billing or operations	Client context and Dental RCM map	VOB, Auto Verify, AR, Medical Billing, Credentialing
HR	Teams, Directory, Employees, Attendance	Leave, Loans, Recruitment, Agreements, Notices
Finance	Organization and practice context	Expenses, Revenue, Reports, approvals, exports
Marketing	Lead ownership and outreach rules	Lead Generation, CRM, Calling, Email, Scraper
Organization admin	Tenant boundary and least privilege	Practices, Employees, Users, Roles, Settings
Platform admin	Platform scope and audited support	Organizations, provisioning, plans, support, import or export
AI user	Underlying manual workflow and data boundary	Xpand AI, approved knowledge, review, automation

10 / RECOVER

Troubleshoot access without creating risk

What you see	Meaning	Correct action
Invalid email or password	Credentials were not accepted.	Check the exact email and keyboard state. Do not guess repeatedly.
Wait before trying again	A temporary sign-in pause is active.	Stop and wait for the full displayed countdown.
Account temporarily blocked	Persistent failures require admin help.	Request an administrator-assisted password reset.
Password link expired or used	The one-time setup grant is invalid.	Request a new link; do not forward the old link.
Account unavailable	Organization or membership is inactive or blocked.	Contact the organization administrator.
Unauthorized page	The page permission is missing.	Return to an allowed page and request least-privilege access.
Wrong organization or records	Workspace context may be incorrect.	Stop, do not interact, sign out, and report immediately.
Workspace keeps loading	Tenant context or connectivity did not finish.	Wait once, refresh, then contact support with non-sensitive error text.

11 / VERIFY

Verify that Start Here is complete

You are ready for feature training when every statement below is true.

- I can identify the approved DentalXpand sign-in URL.
- I know when Keep me logged in is appropriate.
- I can confirm my organization, practice, role, and displayed identity.
- I understand that sidebar visibility and direct routes use the same page-access model.
- I know the difference between page permission, action permission, and record scope.
- I can locate Profile, Settings, Notifications, Support, and Logout.
- I know what to do if I see the wrong organization or unauthorized data.
- I selected the learning track that matches my responsibilities.

NEXT LESSON	FULL CURRICULUM
Sign in and access your account	**Browse all DentalXpand resources**

Support: support@xpand.dental | Website: xpand.dental