



DENTALXPAND LEARNING CENTER / WORK HUB

Use Video, Audio, and Screen Sharing

A complete guide to authorized Meeting launch, camera and microphone permissions, available screen sharing, audio and minimize behavior, invite links, Super Admin local capture safeguards, live-room connection states, tenant boundaries, troubleshooting, and verification.

VERSION	1.0	AUDIENCE	Authorized meeting participants and organizers
FORMAT	Website + PDF	UPDATED	July 2026

Every person, organization, provider, patient, meeting, participant, device, date, status, and count shown in this guide is fictional. Never use live patient, provider, employee, credential, password, token, recording, 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.

Use live communication from an authorized current meeting	3
Confirm current identity, organization, and meeting context	4
Start from a current Meeting card	5
Use camera and microphone permissions deliberately	6
Choose the smallest safe surface before sharing	7
Use audio, minimize, reconnect, and leave deliberately	8
Copy a current meeting invitation carefully	9
Understand current Super Admin local capture	10
Trace the current live-room connection without exposing secrets	11
Protect tenant and participant boundaries throughout the call	12
Resolve expected states without bypassing access	13
Verify that live communication is understood	14
Continue through DentalXpand learning	15
Related lessons	15

How to use this guide

Read access, current meeting context, and tenant boundaries first. Then practice meeting launch, media permissions, screen sharing, audio and lifecycle controls, invitations, local recording safeguards, safe troubleshooting, and completion verification.

01 / PURPOSE

Use live communication from an authorized current meeting

Area	Current role	Boundary
Meetings live room	Configured LiveKit room launched from a current Meeting card	Current identity, meeting context, server authorization, live service, and browser permissions matter.
Video meeting	Requests video plus audio for the live room	Device permission and available controls can differ by browser, hardware, and configuration.
Audio meeting	Keeps audio enabled without requiring a camera	Use approved device and private listening practices.
Messages call overlay	Separate implementation with its own explicit media and screen-share controls	Do not assume button location or behavior matches the Meetings room.
In-person meeting	Schedules people and time without creating a live room	Do not try to join it as video or audio.

Live communication is not the source record

Record operational actions in Tasks and patient, payer, provider, credentialing, financial, clinical, or compliance outcomes in their owning authorized module.

02 / ACCESS

Confirm current identity, organization, and meeting context

Check	Confirm before joining	Why it matters
Identity	Your own signed-in account and current session	Copied URLs, room labels, and another person's browser session are not credentials.
Organization/practice	Expected tenant, practice, and working context	Live communication must not bridge Guardian Connect or unrelated DentalXpand data.
Meeting record	Title, date, time, organizer, type, status, and participant state	A prior invitation or notification can be stale.
Role/membership	Legitimate organizer or participant relationship	Visible UI does not override API authorization or row-level policy.
Environment	Appropriate device, network, and private setting	Camera, microphone, display, and audio output are intentional permission decisions.

Do not infer encryption from a label

A security-oriented room label is not proof of the configured encryption model. Confirm the deployed live-service architecture, retention rules, and organization policy with platform administration.

[Review the Meetings guide](#) | [Review roles and permissions](#) | [Review organization context](#)

03 / JOIN

Start from a current Meeting card

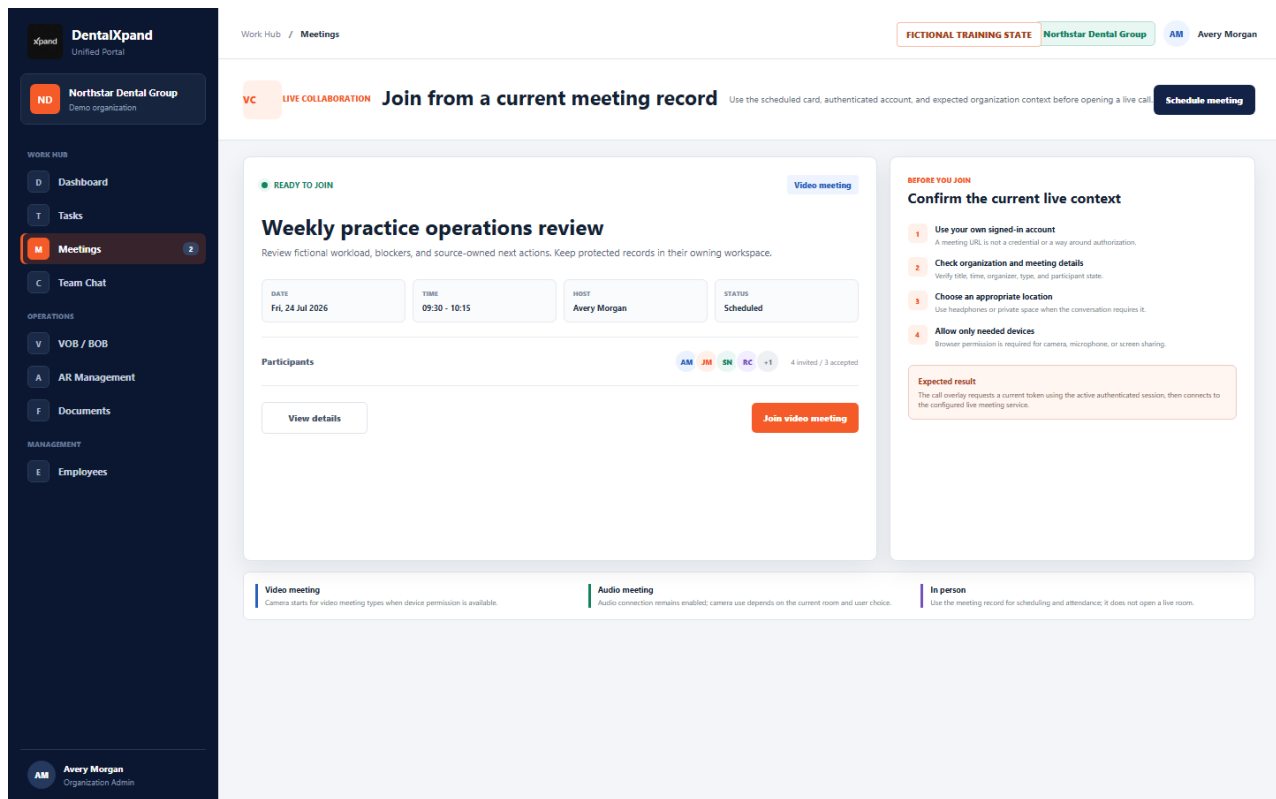


Figure 1. Fictional Meetings page with a current video meeting card, Join action, meeting details, participants, and a pre-join checklist.

- 1 Open the authorized Meetings workspace and confirm account, organization, practice, and meeting context.
- 2 Review title, type, date, time, organizer, participant state, and current status.
- 3 Join only a scheduled or in-progress live meeting.
- 4 Allow only the camera, microphone, and device permissions you require.
- 5 Wait for the configured live room to connect; do not share credentials or borrow another account after failure.

Expected result

The current overlay requests a room token using the active authenticated session, then connects to the configured live meeting service.

04 / MEDIA

Use camera and microphone permissions deliberately

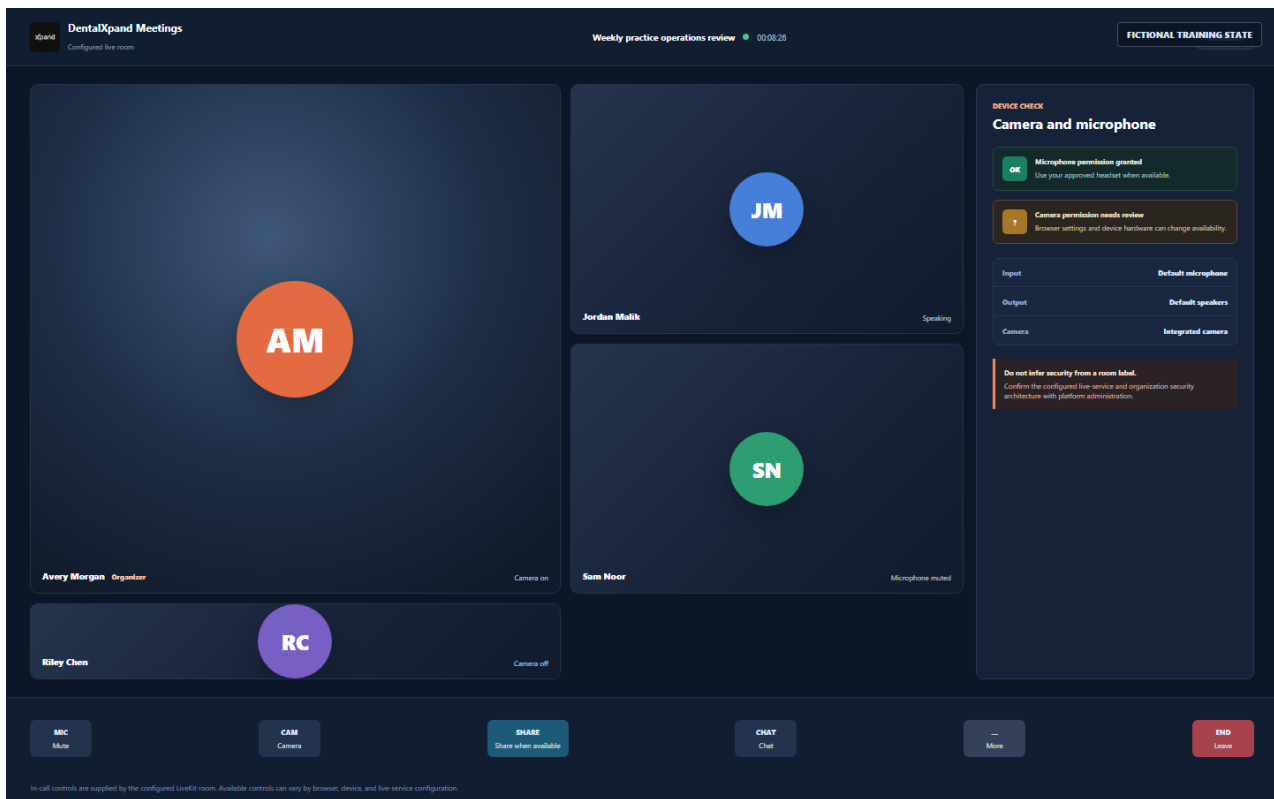


Figure 2. Fictional live room with participant tiles, camera and microphone controls, screen-share availability note, device checks, and Leave control.

State	What it means	Safe response
Video meeting	The current room starts with video and audio requested.	Allow only required devices and confirm the room is appropriate before enabling camera.
Audio meeting	Audio remains enabled while camera use is not required.	Use a suitable microphone, output device, and private environment.
Device denied	Browser, OS, hardware, privacy controls, or another application may block access.	Review local settings with your own account; do not use someone else's device session.
Controls differ	Configured LiveKit controls can vary by browser, device, and room configuration.	Verify the deployed experience before promising a button or workflow.

Keep the room appropriate

Do not show sensitive records merely because media is working. Verify who is present and keep discussion limited to the approved operational purpose.

05 / SCREEN SHARE

Choose the smallest safe surface before sharing

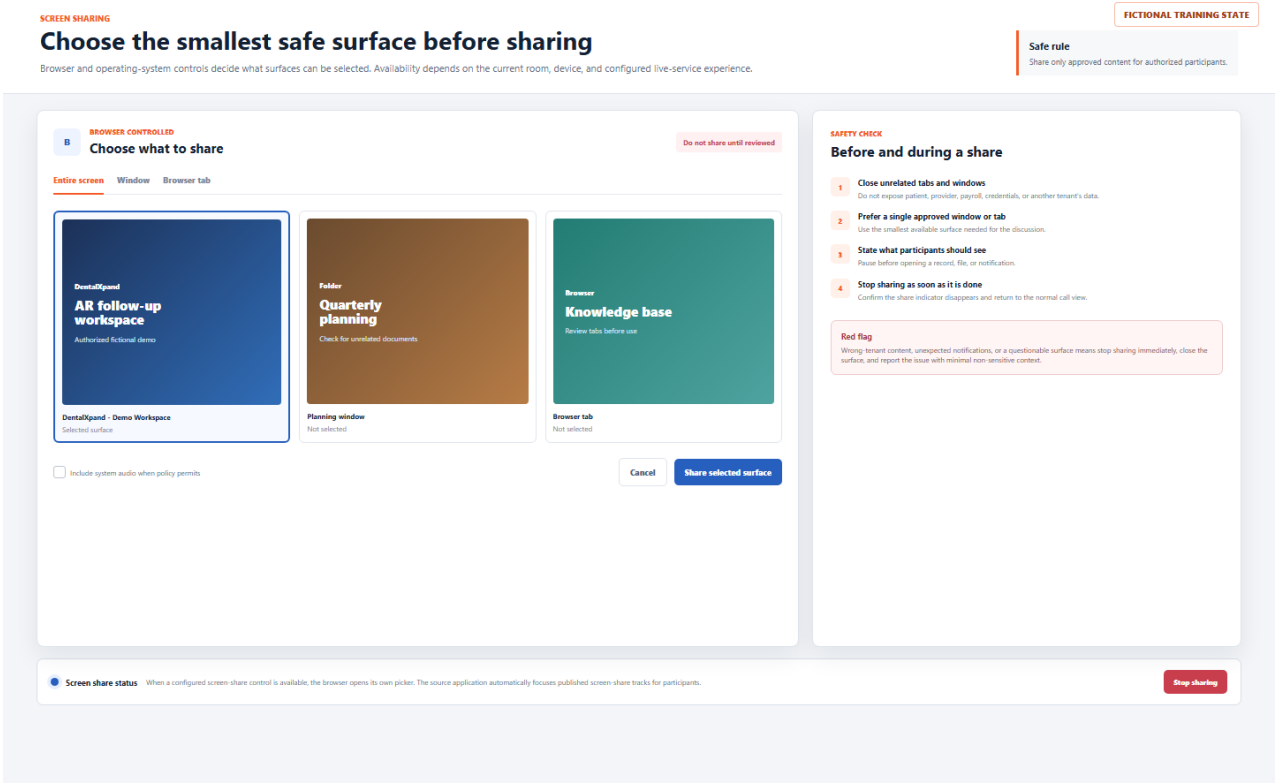


Figure 3. Fictional browser display picker with an approved demo workspace, safety checks, warning state, and stop-sharing control.

The current Meetings overlay renders the LiveKit VideoConference experience. It can present published screen-share tracks and automatically focus a published share for participants. The exact screen-share control is supplied by the configured component and live-service environment, so its visible behavior must be verified in the deployed browser.

Moment	Correct practice
Before opening the picker	Close unrelated windows, browser tabs, chat popups, notifications, private documents, credentials, payroll, patient information, provider data, and anything from another tenant.
Choose a surface	Prefer one approved tab or window over the entire desktop. Share the smallest surface that answers the operational question.
During the share	State what participants should see, pause before navigating, and confirm participant identity before showing a record.
After the share	Stop sharing immediately and verify the share indicator disappears before opening other work.
Unexpected content	Stop, close the surface, avoid further access, and report minimum non-sensitive context as a potential privacy or tenant incident.

06 / AUDIO

Use audio, minimize, reconnect, and leave deliberately

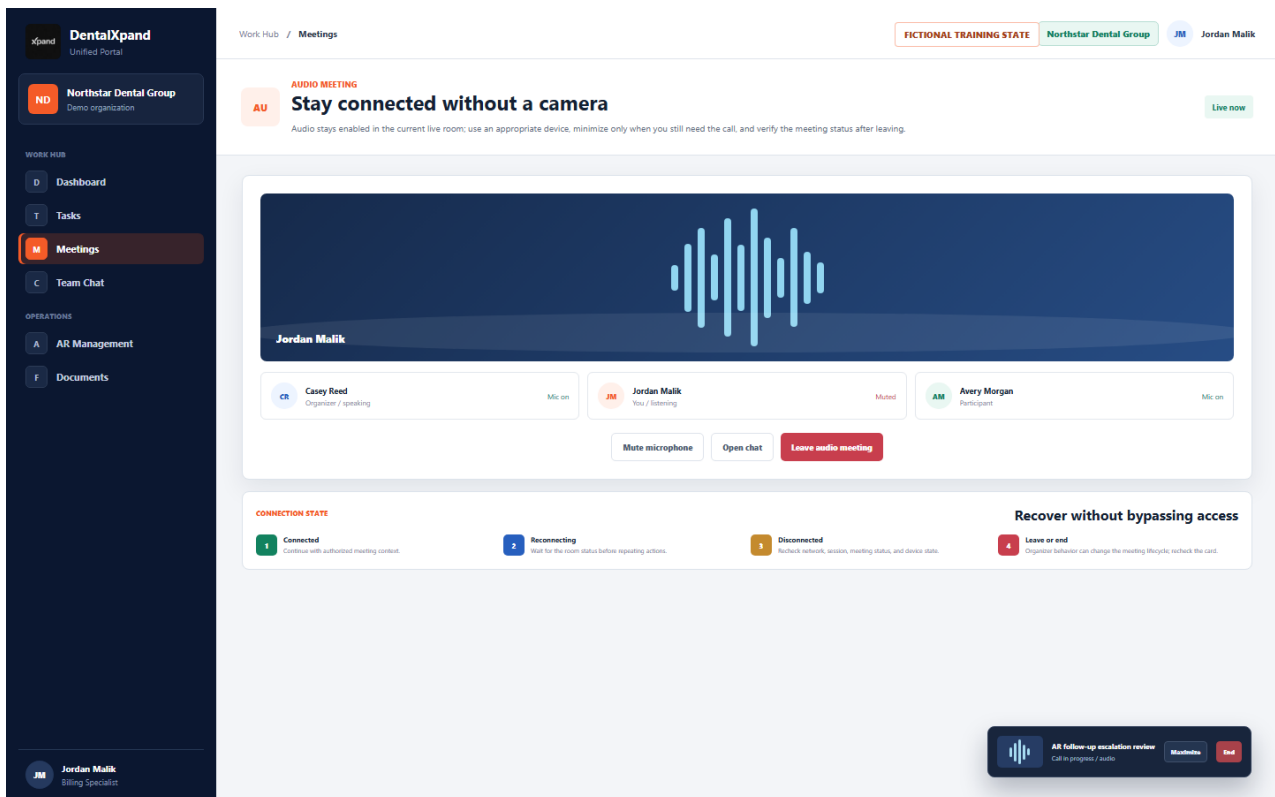


Figure 4. Fictional audio meeting with participant state, audio controls, recovery states, and a minimized in-progress call panel.

- 1 Use audio when a camera is unnecessary, and mute when you are not speaking.
- 2 Minimize only while the call remains needed; maximize when you must return to the room.
- 3 When reconnecting, wait for current state and check network, browser session, device permission, and meeting status.
- 4 Leave intentionally, then return to the Meeting card and confirm the saved status.

Organizer caution

The current Meetings page uses the same end handler after live-room disconnection. When the current user is the organizer, leaving or disconnecting can mark the meeting completed. Verify the card after leaving and schedule a new record when another conversation is required.

07 / INVITE

Copy a current meeting invitation carefully

INVITE AND RECORDING SAFEGUARDS

Share a current meeting invite carefully and understand local capture limits

A copied invite supports legitimate coordination only. Current recording behavior is a Super Admin browser display-capture flow that saves a local WebM file.

FICTIONAL TRAINING STATE

Do not send
Tokens, passwords, protected data, or another tenant's content.

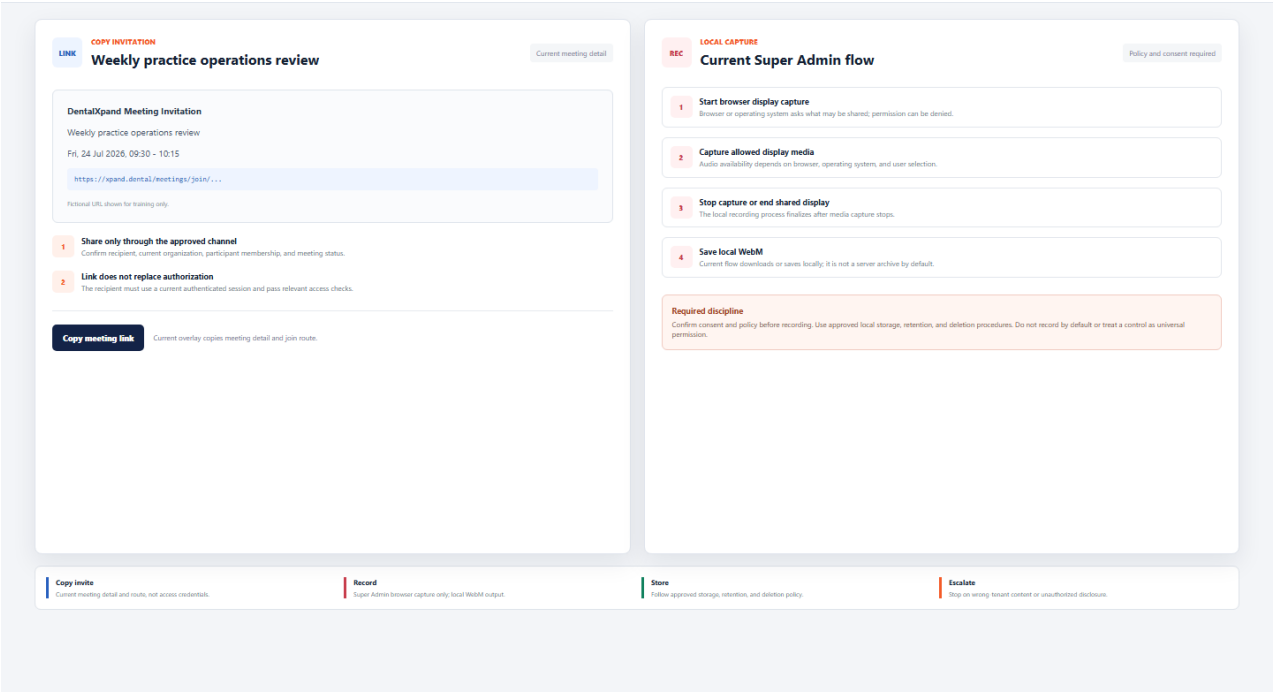


Figure 5. Fictional invitation copy and local recording safeguards view with current meeting details, display-capture flow, local WebM output, and policy discipline.

Action	Current behavior	Boundary
Copy invite	The overlay can copy meeting title, scheduled time, and current join route.	The route is an invitation aid, not a password, token, or entitlement.
Send invite	Share only through an approved communication path.	Confirm recipient, organization, participant membership, and current meeting status first.
Receive invite	Recipient uses their own current session.	Current server-side, tenant-aware, and room access checks remain authoritative.
Meeting changed	A link or notice can become stale after cancellation, completion, or material edit.	Open the current Meeting card before joining.

08 / RECORDING

Understand current Super Admin local capture

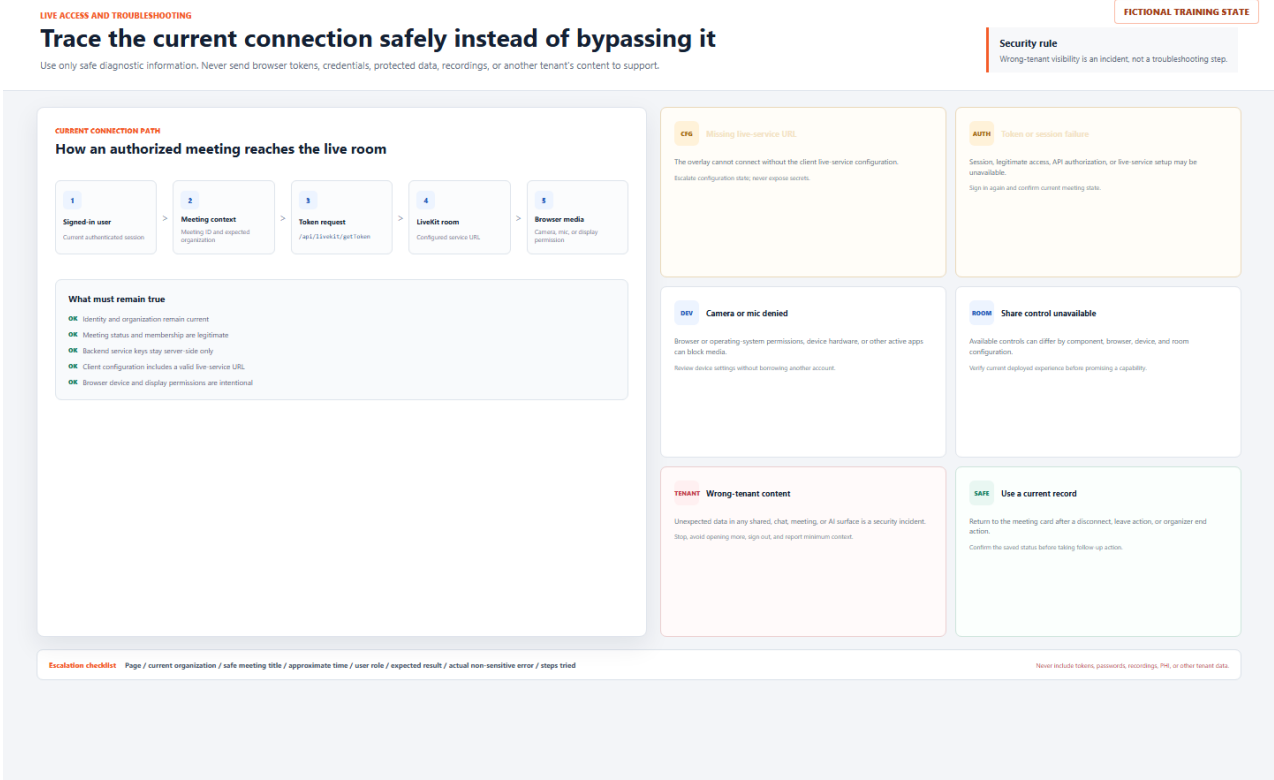
The current Meeting overlay conditionally shows recording to a Super Admin user. It requests browser display capture and uses MediaRecorder to create a local WebM file. It is not a server-side archive, a universal participant recording feature, a permanent record, or a replacement for a documented retention process.

Current behavior	Required discipline
Control visibility	Super Admin visibility does not equal universal authorization to record. Confirm legitimate purpose, consent, policy, and applicable law.
Browser display capture	The browser or operating system chooses what may be shared. Do not bypass denied permission with another person's device or account.
Audio request	Audio capture availability depends on browser, OS, and user-selected surface. Do not assume audio will be captured.
Local WebM output	Use approved storage, access control, retention, and deletion procedures. Do not assume central storage.
Capture end	Stopping recording or ending shared display finalizes local output. Review its location and handling immediately.

Never record by default
Do not record passwords, protected health information, unrelated applications, personal communications, unauthorized attendees, or another tenant's information. Close unrelated content before capture.

09 / CONNECTION

Trace the current live-room connection without exposing secrets



10 / BOUNDARIES

Protect tenant and participant boundaries throughout the call

Boundary	Correct behavior
Participant	Use the narrowest legitimate attendee list. Do not add someone because a live room is convenient.
Tenant	Never bridge Guardian Connect, DentalXpand, provider, practice, client, or unrelated organization data through a room, share, invite, recording, message, or AI surface.
Source record	Move decisions to Tasks or the correct authorized patient, payer, AR, credentialing, HR, finance, or operational module.
Support	Report only safe diagnostic context. Do not attach recordings, sensitive screenshots, browser tokens, credentials, or other tenant data.

Cross-tenant data is a security incident

If unexpected data appears in a meeting, participant list, screen share, recording, invitation, message, notification, or AI response: stop, do not open more, stop sharing, sign out, and report the incident immediately with minimum non-sensitive context.

Move operational follow-up to Tasks | Continue to Team Messages

11 / TROUBLESHOOT

Resolve expected states without bypassing access

What you see	Possible reason	Correct first response
Cannot join or no token	Session, meeting state, membership, API authorization, or live-service configuration.	Confirm current sign-in, context, meeting card, and safe error text. Do not share tokens or borrow access.
Missing live-service URL	Client configuration incomplete or unavailable.	Report configuration state to platform administration without sharing environment values or secrets.
Camera/mic denied	Browser or OS permissions, hardware, privacy setting, active application, or wrong device.	Review local device settings with your own authorized session.
Share control missing	Current component, browser, device, or room configuration differs.	Verify deployed behavior before promising the capability.
Unsafe surface in picker	Unrelated tabs, notifications, apps, or records are open.	Cancel, close unrelated content, and share only the smallest approved surface.
Status changed after leave	Organizer end or disconnect behavior changed lifecycle.	Return to current Meeting card and verify saved state.
Recording unavailable	Role, browser, device permission, or policy restriction.	Do not bypass. Confirm consent, policy, role, and approved process.
Other tenant data	Potential authorization, RLS, cache, link, notification, sharing, search, AI, or isolation failure.	Stop, avoid further access, sign out, and report an incident.

12 / COMPLETION

Verify that live communication is understood

- I can explain why account, organization, practice, meeting context, membership, current status, backend authorization, live service, and browser permission all matter before joining.
- I know a copied meeting invitation is not a credential or authorization bypass.
- I know the configured Meetings room and the Messages call overlay are separate implementations that can expose controls differently.
- I can handle camera, microphone, audio, minimize, reconnect, leave, and post-leave Meeting status safely.
- I use screen sharing only when available, choose the smallest approved surface, and stop it immediately when finished.
- I understand current Super Admin capture is a browser display-capture flow with local WebM output, not a server archive by default.
- I know consent, policy, approved storage, retention, and deletion rules apply before recording.
- I do not infer encryption configuration from UI labels alone.
- I know server-side membership, tenant scope, and live-room authorization must remain authoritative.
- I can identify safe troubleshooting information and keep tokens, secrets, recordings, PHI, and other tenant data out of support requests.
- I know wrong-tenant visibility is an immediate stop-and-report security incident.

Ready for team communication

Continue with Team Messages to learn direct and group conversations, attachments, voice notes, unread state, and safe discussion boundaries.

13 / CONTINUE

Continue through DentalXpand learning

Meetings guide	Team Messages guide	All resources
Meetings guide	Team Messages guide	All resources

Related lessons

- Use the Dashboard command center
- Understand roles, permissions, and access boundaries
- Understand organization and practice context
- Manage tasks, assignments, steps, and timers
- Schedule and manage meetings

Website guide: Use video, audio, and screen sharing

Support: support@xpand.dental

Website: xpand.dental