DENTALXPAND LEARNING CENTER / PASSWORD SECURITY

Set Up, Reset, and Change a Password

A complete guide to first-password setup, temporary credentials, self-service changes, failed-attempt recovery, authorized administrator resets, owner boundaries, secure delivery, and verification.

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

All product states are fictional. Never place a real password, temporary credential, setup URL, access token, recovery session, or patient information 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 / CHOOSE

Choose the correct password workflow

The safest path depends on whether the user has a valid session, knows the current password, received an invitation, or needs authorized administrator assistance.

Situation	Correct workflow	Who acts
Create password email	Open the newest one-time setup link	Invited user
Temporary password	Sign in, replace it, then sign in again	User
Signed in and knows current password	My Profile or Settings > Security	User
Forgotten password or persistent block	Authorized administrator reset	Tenant administrator
Organization owner recovery	Send owner password-setup email	Platform administrator
Unexpected organization or records	Stop, sign out, report tenant-context incident	User and security admin

Never disclose a current password
Administrators reset access without reading the user's existing password. Do not send credentials, setup URLs, or tokens in email, chat, screenshots, tickets, or comments.

Review sign-in and account access

02 / CREATE

Create a secure password

DentalXpand currently requires at least eight characters. Eight is a technical minimum, not a recommendation for a weak password.

Property	Correct practice
Unique	Use only for DentalXpand; never reuse email, banking, social, PMS, or other workplace credentials.
Long	Prefer a long passphrase or a password-manager-generated value.
Policy compliant	Follow stronger organization length or complexity rules when they apply.
Different	Do not reuse the temporary or current password, or make a predictable variation.
Protected	Store only in an approved password manager on a private or managed device.

Show password control
Reveal a password only when the screen is private and is not being shared, recorded, photographed, or watched.

- Do not use names, birthdays, practice names, phone numbers, or email fragments.
- Do not save passwords in notes, spreadsheets, screenshots, task comments, or tickets.
- Do not type a real password into a training or support screen.
- Report suspected exposure and reset the credential immediately through an approved path.

03 / INVITE

Use a one-time Create password link

1. Confirm the message was expected and sent to the exact account email.
2. Open only the newest invitation yourself; do not forward or paste it elsewhere.
3. Wait while DentalXpand matches the recovery session, user, and one-time grant.
4. Complete the current 10-minute setup window after the secure link is opened.
5. Enter and confirm a new password of at least eight characters.
6. Return to normal sign-in after the recovery session ends.

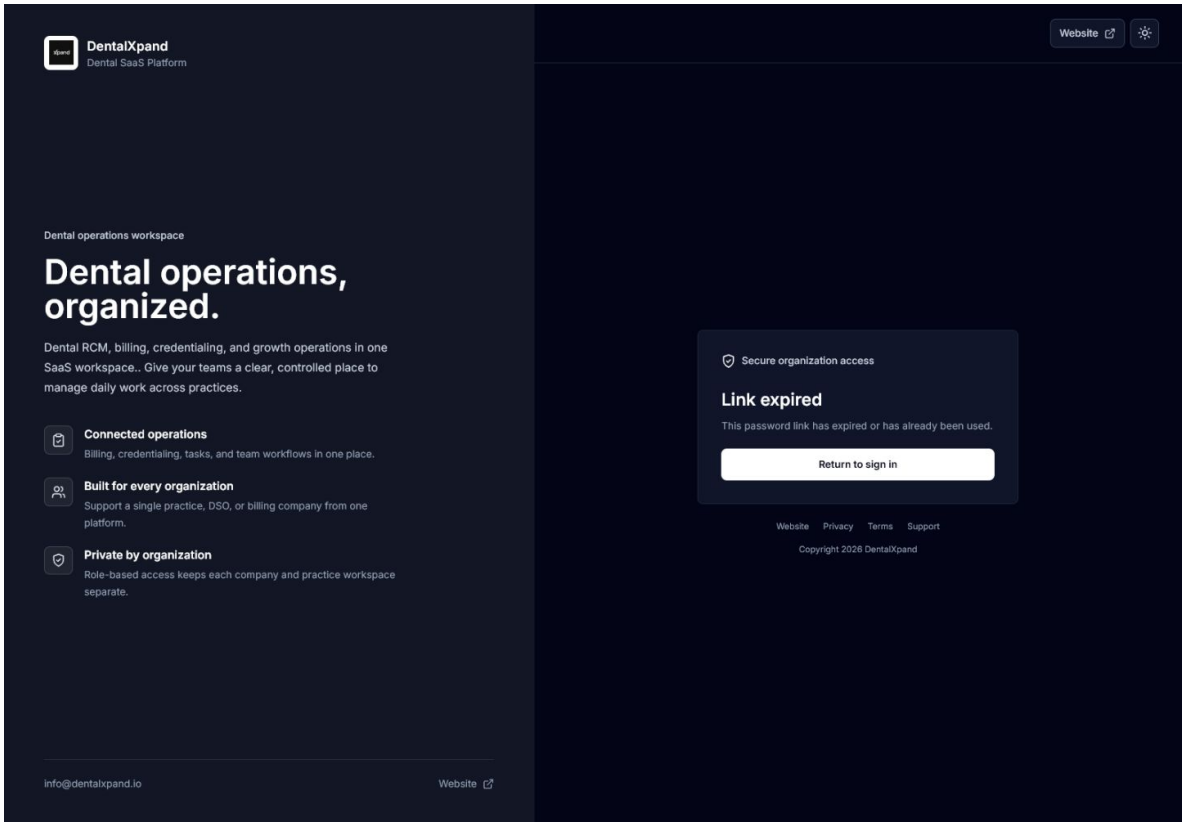

Figure 1. An invalid, expired, already-used, incomplete, or mismatched setup URL cannot create a password.

When a link fails
Close old invitations and recovery tabs, request one new setup email, and open only the newest message.
Never edit callback parameters or reuse a copied URL.

04 / REPLACE

Replace a temporary password before workspace access

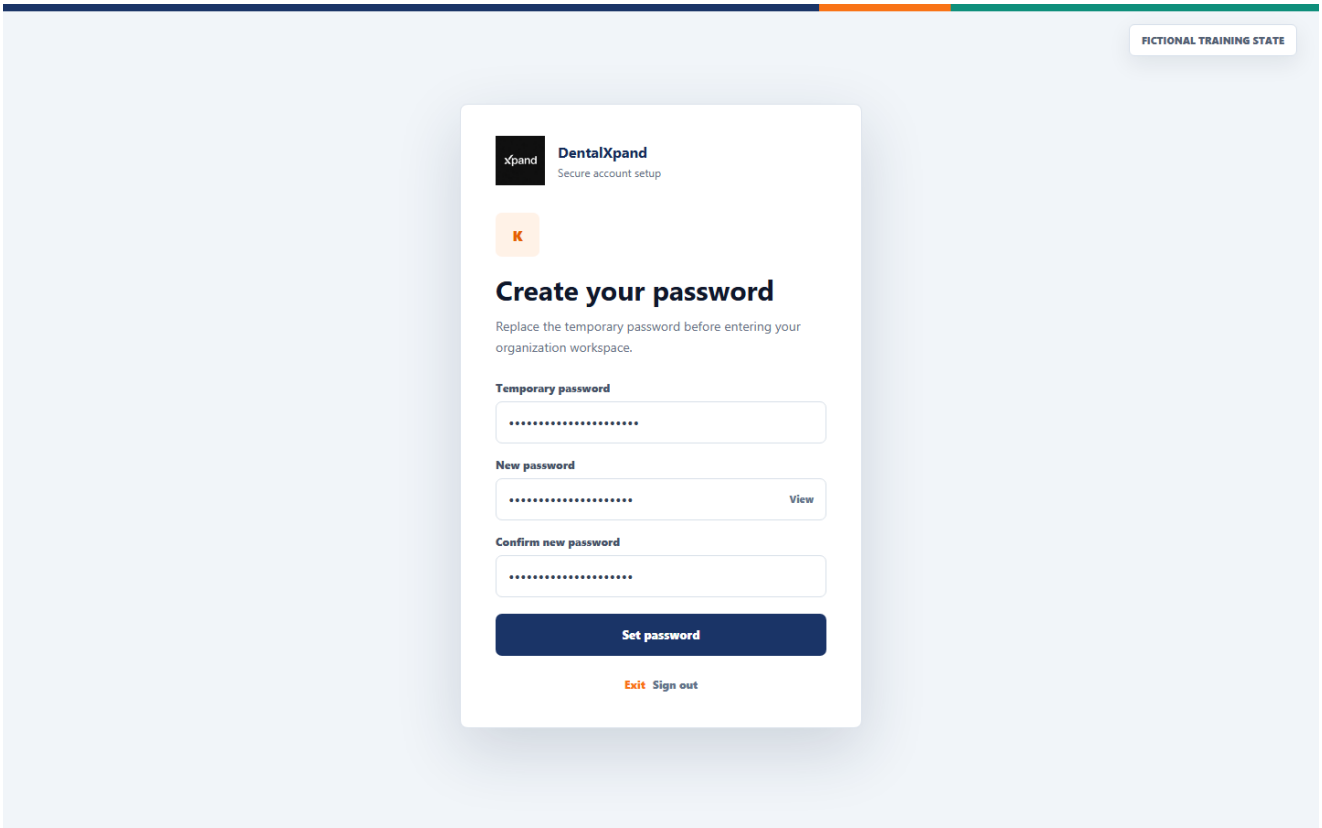

Figure 2. Source-accurate fictional training state. A pending-password-change membership is routed here before the workspace opens.

1. Enter the one-time value in Temporary password.
2. Enter a different New password with at least eight characters.
3. Enter the exact same value in Confirm new password.
4. Select Set password once and wait for the result.
5. After success, sign in again with the account email and new password.

> Temporary means one use
> Do not keep, reuse, forward, or store the temporary password after the new password succeeds.

05 / SELF-SERVICE

Change your own password while signed in

Use this path only when you know the current password. The self-service endpoint verifies the signed-in account and cannot be used to change another user's password.

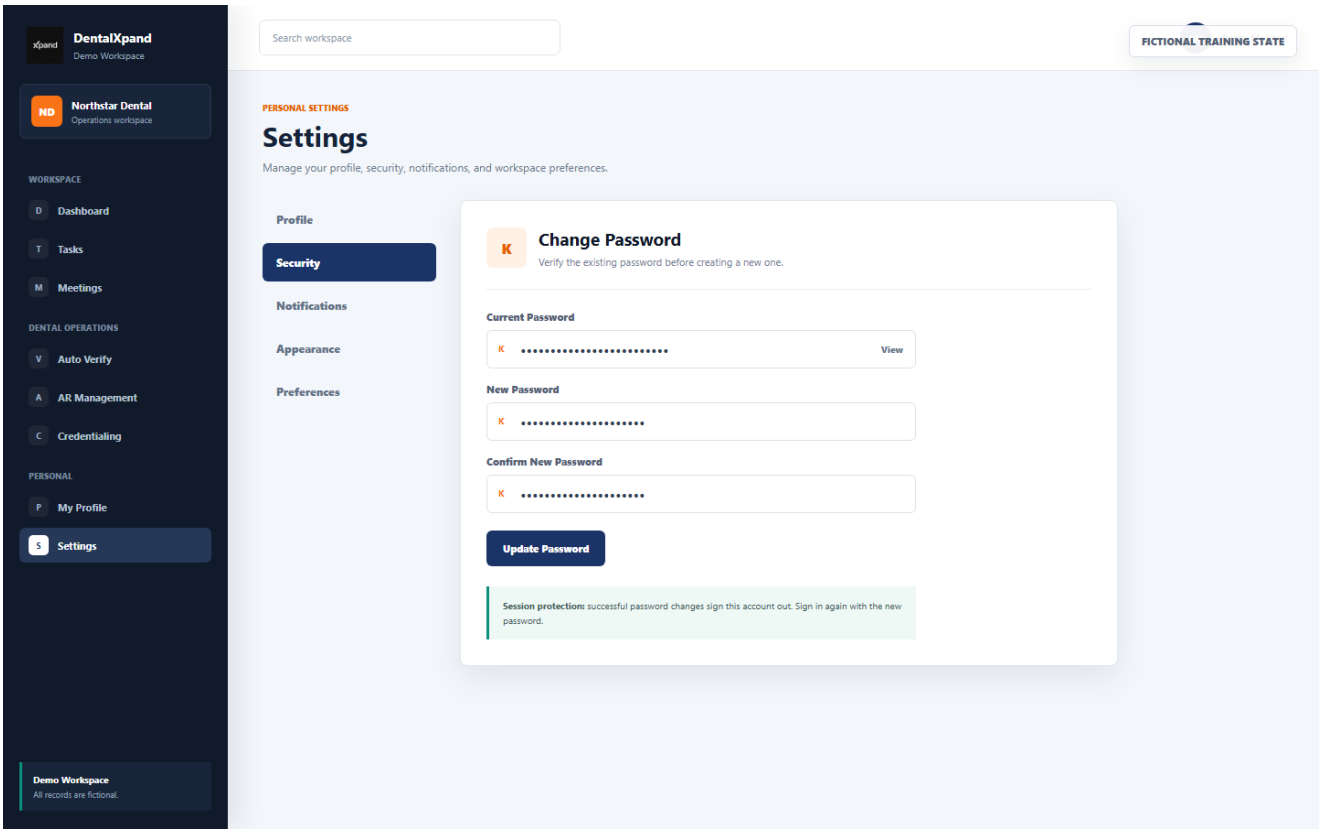

Figure 3. Source-accurate fictional Settings Security state. My Profile provides an equivalent security form.

1. Open My Profile or Settings, then the Security area.
2. Enter Current Password for the authenticated account.
3. Enter a unique New Password with at least eight characters.
4. Enter matching confirmation and select Update Password once.
5. Sign in again and verify the correct organization, role, practice scope, and destination.

06 / SESSION

Understand sign-out and account status changes

Step	Layer	Result
1	Credential verification	Current or temporary password must belong to the signed-in account.
2	Authentication update	The secure auth identity receives the new password.
3	Membership activation	Pending-password-change state clears when applicable.
4	Session termination	Local authentication clears and global sign-out is requested where supported.
5	Fresh access decision	Organization, practice, role, permissions, and status load again.

Save planned work first

A password change signs the user out. Save permitted work before a routine self-service change, but never delay an urgent security reset merely to preserve a session.

Fresh sign-in is part of verification

Do not treat the password-change success message as the final check. Confirm the new password and correct tenant context through a new sign-in.

07 / ADMIN CREATE

Create a user with the correct onboarding method

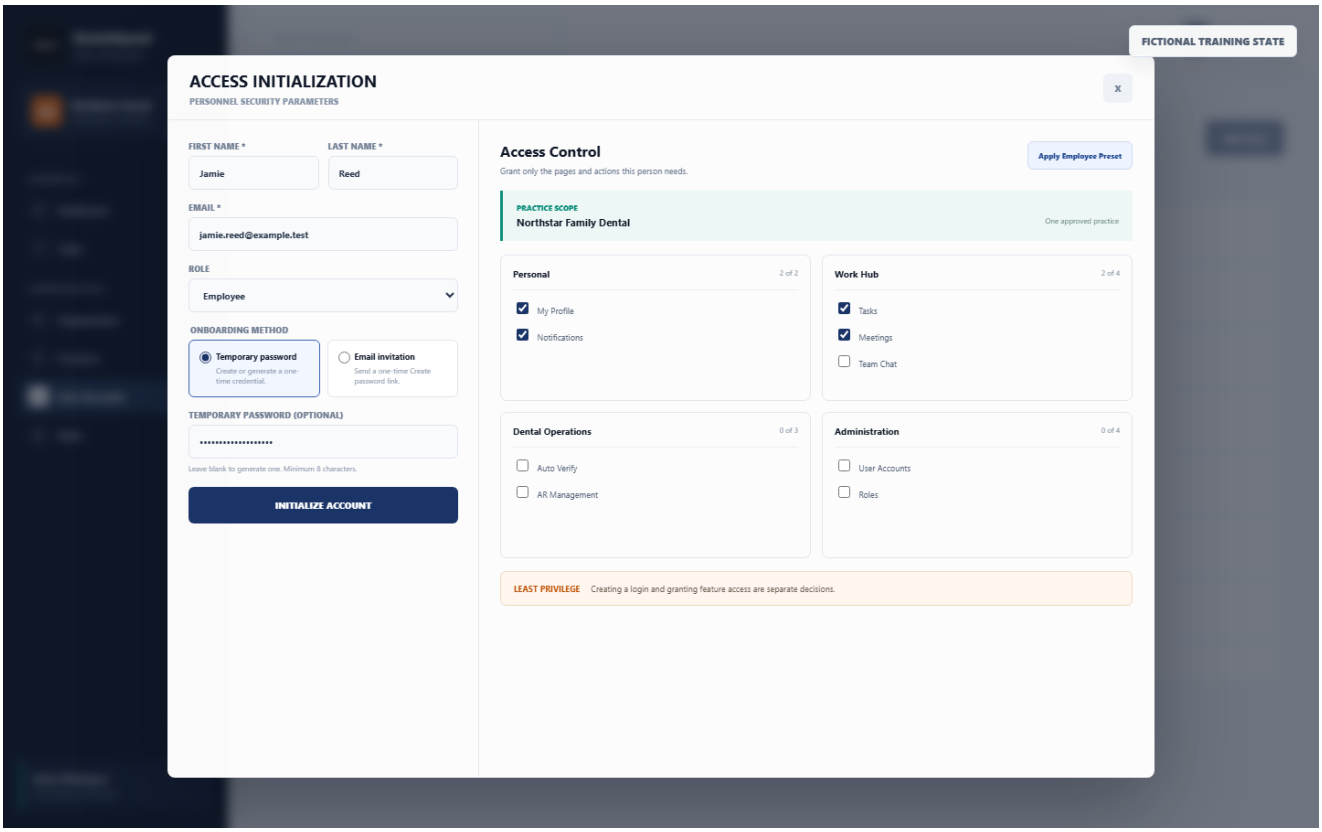

Figure 4. Source-accurate fictional Access Initialization state with onboarding method, practice scope, and least-privilege permissions.

Method	Use when	Result
Temporary password	Approved administrator will securely deliver a one-time credential	Pending password change; user must replace it at next sign-in
Email invitation	User controls the invited inbox and should create the first password	One-time setup email; no temporary password is displayed

07A / ADMIN CHECK

Review identity, role, permissions, and practice scope

Creating a login, granting feature pages, selecting a role, and assigning practices are separate decisions.

1. Confirm first name, last name, and the exact individual email.
2. Search for an existing application or authentication account before creating a duplicate.
3. Select the intended organization role without using it as a shortcut for broad permissions.
4. For provider, client, or external accounts, assign at least one valid practice.
5. Grant only required pages and actions, then review the permission matrix.
6. Choose temporary-password or invitation onboarding and initialize once.
7. Verify resulting account status, practice scope, and least-privilege destination.

> Duplicate authentication identity
> If an auth account already exists for the email, locate and update or reset the existing user. Do not create a second identity as a workaround.

Review roles, permissions, and access boundaries

08 / DELIVER

Deliver a one-time credential safely

DentalXpand displays a generated temporary password once. It is not retained for later display.

1. Verify the intended recipient and exact account email through an approved identity check.
2. Use the organization's approved secure credential-delivery method.
3. Do not place account address, temporary password, and application link together in an unprotected message.
4. Require the user to replace the temporary value immediately.
5. Confirm successful access without asking the user to send the password back.
6. Remove temporary notes or messages according to policy after activation.
7. Reset immediately when exposure, forwarding, loss, or uncertainty is suspected.

> Never record a password in the audit trail
> Record the action, authorized actor, target account, organization, reason, result, and time without including any credential.

09 / ADMIN RESET

Reset an organization user's password

The requester needs User Accounts password-reset permission. DentalXpand confirms the target belongs to the same organization and prevents tenant administrators from resetting the owner.

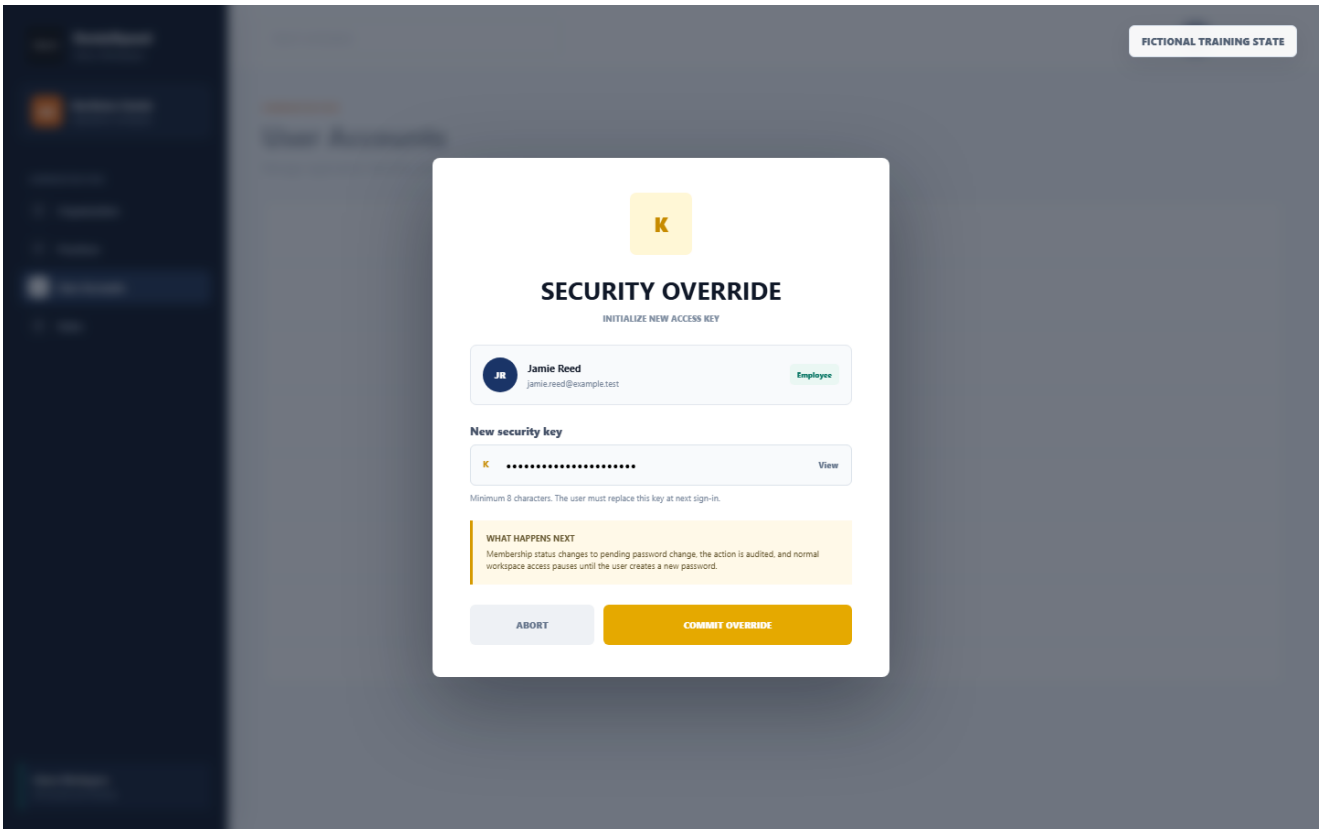

Figure 5. Source-accurate fictional Security Override state. The new access key is temporary and forces a new password at next sign-in.

> Reset does not change authorization
> Do not add roles, pages, actions, practices, provider links, or organization access as part of password recovery.

09A / RESET STEPS

Complete and verify the administrator reset

1. Verify the user's identity, organization, account email, and reset reason without asking for the old password.
2. Open User Accounts and select the existing target user.
3. Confirm name, email, role, and organization before entering a new security key.
4. Create a temporary value of at least eight characters.
5. Commit the override once; the membership becomes pending password change and the action is audited.
6. Deliver the one-time credential through the approved secure channel.
7. Have the user replace it, sign in again, and confirm the expected workspace only.

> Same-organization boundary
> An organization administrator cannot use this reset flow for a user outside the active tenant, and an owner account remains platform-managed.

Continue to the user account lifecycle guide

10 / ACCOUNT TYPES

Handle employee, provider, external, and owner accounts

Account	Authorized path	Boundary
Employee with login	Employee or User Accounts reset permission	Use at least eight characters even if an older dialog shows a shorter placeholder
Employee without login	Approved employee account-create or User Accounts path	Account creation does not justify extra feature permissions
Provider, client, external	Tenant user create or reset	At least one practice on creation; reset must not alter scope
Organization administrator	Different authorized same-tenant administrator	Requester still needs explicit reset permission
Organization owner	Platform sends owner setup email	Tenant administrators cannot edit or reset the owner
Platform administrator	Approved platform identity-security procedure	Do not use support sessions as a password workaround

Review organization provisioning and owner access

11 / RECOVER

Recover from failed sign-in attempts safely

What you see	Meaning	Correct response
Current password is incorrect	Self-service verification failed	Stop guessing; use authorized reset when unknown
Too many failed attempts	Short timed pause	Wait for the complete displayed countdown
Persistent local block	Repeated failures	Use administrator assistance; do not clear security state
Link expired	Old, used, incomplete, timed-out, or mismatched URL	Request one new invitation
Account inactive	User or membership status blocks access	Resolve status through authorized administration
Wrong organization	Tenant context is unexpected	Stop, sign out, and report immediately

Do not bypass a pause

Do not clear browser storage, switch accounts, create duplicates, or use another person's credentials to avoid failed-attempt protection.

12 / SECURE

Apply security, least-privilege, and audit controls

USER RESPONSIBILITIES	ADMINISTRATOR RESPONSIBILITIES
Use an individual account and unique password. Protect password-manager, device, and email access. Sign out on shared or reassigned devices. Report suspicious resets or tenant mismatch. Reject unsolicited password requests.	Require explicit reset permission. Verify target identity and organization. Never retrieve, request, log, or retain a password. Keep audit events credential-free. Keep owner operations platform-managed. Review authorization separately.

Security incident triggers

Escalate suspected credential exposure, an unsolicited reset, unexpected owner action, or cross-organization access according to the organization's incident procedure.

Review organization, practice, and tenant context

13 / TROUBLESHOOT

Troubleshoot password setup, change, and reset

What you see	Likely cause	Correct action
Minimum 8 characters	Value is too short	Create a longer unique password
Passwords do not match	New and confirmation differ	Clear and re-enter both fields
Choose a different password	New equals temporary/current	Create a different value
Current password incorrect	Self-service verification failed	Stop guessing; request reset
Link expired	Old, used, incomplete, or timed out	Request one new setup email
Auth account already exists	Duplicate creation attempted	Locate existing user; update or reset
Permission denied	Requester lacks reset action	Use an authorized administrator
Owner platform-managed	Tenant admin selected owner	Use platform owner setup email
Account inactive	Status blocks access	Resolve account or membership status
New password fails	Old value, wrong email, stale page, or wrong URL	Open approved sign-in and retry once
Unexpected workspace	Tenant, practice, role, or scope is wrong	Stop, sign out, report

14 / VERIFY

Verify that the password workflow is complete

The workflow is complete only when the new credential and the resulting access context are both correct.

User verification

- I used the correct invitation, temporary-password, or self-service workflow.
- I created a unique password and did not disclose it.
- I can sign in with the exact account email and new password.
- The temporary or old credential no longer provides expected access.
- I reach the correct organization, practice scope, role, and permitted destination.
- I can report failed attempts or unexpected access safely.

Administrator verification

- The target was the intended same-organization user and the requester had explicit authority.
- The reset did not change permissions, practices, or tenant scope.
- The user replaced any temporary credential at first sign-in.
- The action is auditable without containing a password.
- Any suspected exposure or tenant mismatch was escalated.

PREVIOUS	NEXT	CURRICULUM
Sign in and account access	**Organization and practice context**	**All resources**

Website guide: Password setup, reset, and change
Support: support@xpand.dental