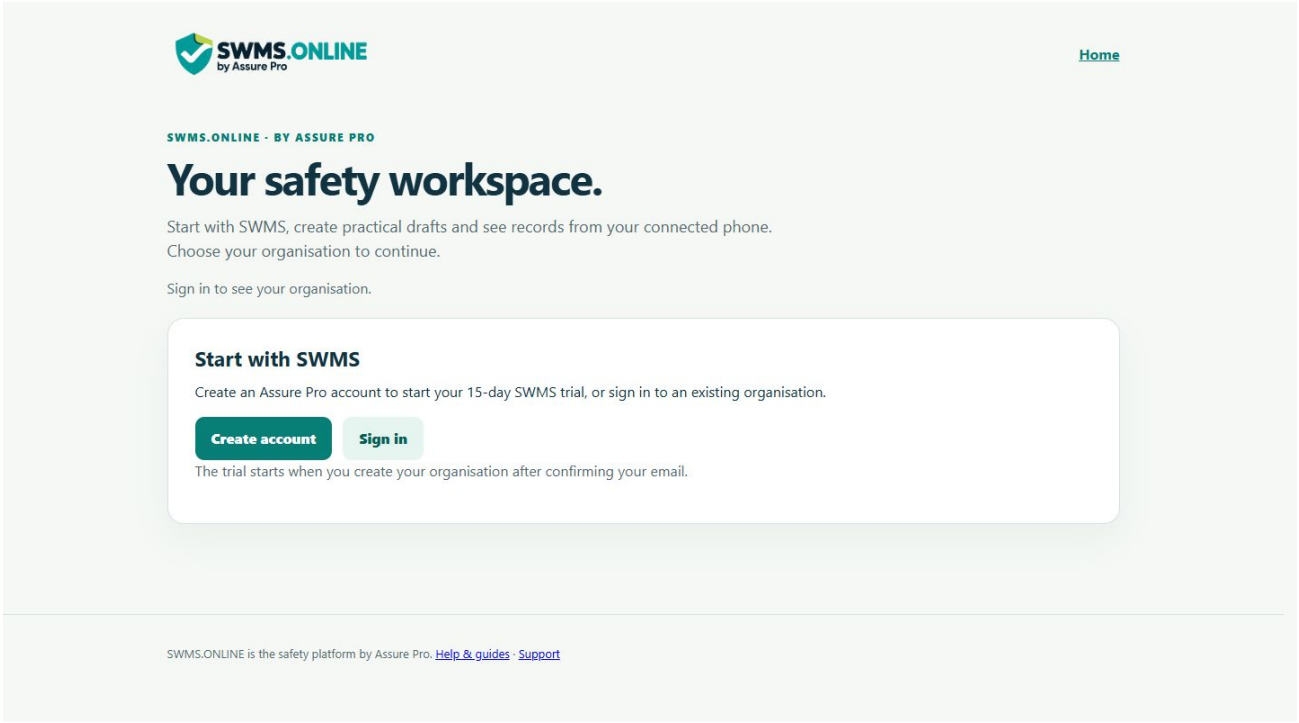
Owner & user guide

SWMS.ONLINE is the platform. Assure Pro is the company behind it. This guide explains account setup, everyday safety work, the Android app and troubleshooting.

Updated 24 October 2026 for Android 0.6.22 and the shared template library. QR signing, expanded team roles and per-person module/reporting controls are available on the deployed cloud service. Physical-device, recovery and security acceptance are separate from this guide.

Start here: app.assurepro.au/app.html. Support: support@assurepro.au. Keep your own sign-in; do not share an owner password.

Contents: 2 Owner setup; 3 Team access; 4 Web and phone; 5 Everyday records; 6 Imports, photos and voice; 7 Acknowledgements and QR; 8 Contractors and inductions; 9 Module guide; 10 Confidential access; 11 Troubleshooting; 12 Owner handover and recovery. Appendices: editable templates; expanded team controls.



Account entry screen. Screenshot captured 23 October 2026; labels may change as releases are deployed.

1. Set up the business owner

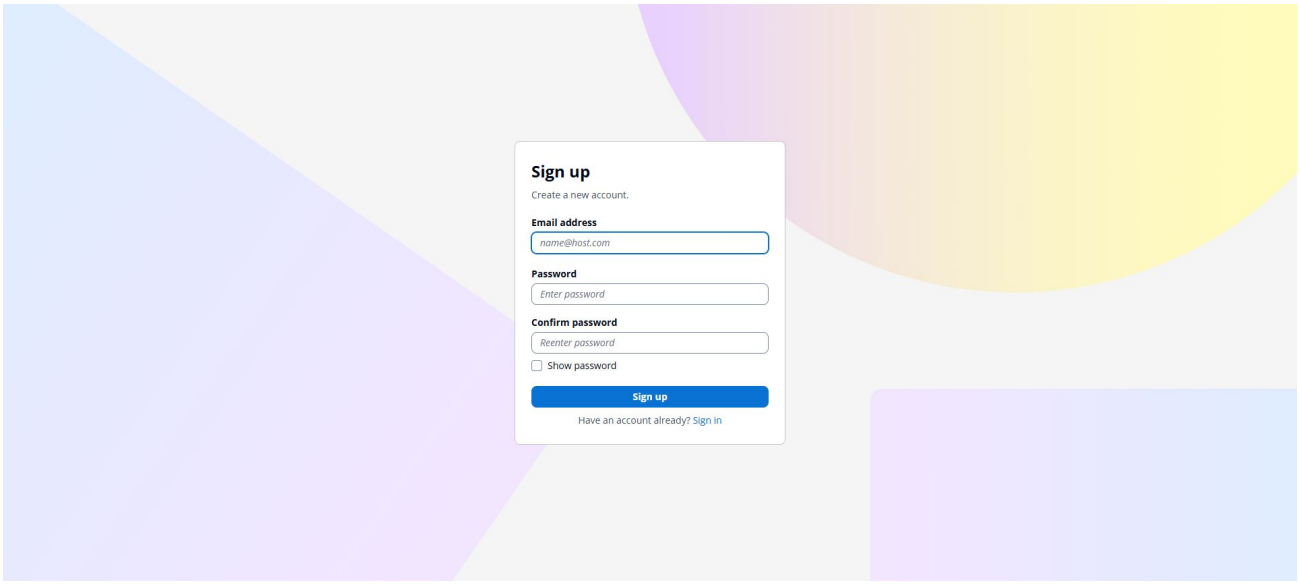
1. Open Client sign in and choose Create account. Use the nominated owner’s own work email. If the owner already has an account, choose Sign in.

2. Set the password privately and enter the email verification code on the sign-in page. Do not send passwords or codes to Assure Pro staff.

3. Enter the agreed business name and start the 15-day SWMS trial. The verified account creating the organisation becomes its owner. One account can start one new trial.

4. Select the correct organisation. Check its name and your owner role before entering information. Your account is the sign-in; the organisation is the business; a workspace groups the business’s workplaces and records.

5. Agree modules, payment and the operational start with Assure Pro. First clients use manual invoices. Website module prices are monthly AUD, including GST. A download code controls the installer; it does not grant a subscription.



Use your own work email. Verification is completed in the account flow.

2. Give the team access

1. Sign in, select the organisation and open Invite someone to this organisation.

2. Enter a recognisable name. Choose Standard user, Supervisor, Manager or View only. Under Modules & reporting, select the modules they need and whether reports, analytics and bulk exports are allowed. New invitations start with SWMS only and no reporting access.

3. Create one invitation per person and send it privately. A link works once and expires after 48 hours. Anyone holding it can claim the role after signing in, so do not put it on a public page or group noticeboard.

4. The recipient signs into their own account and opens the invitation. Refresh team to confirm the right person joined. Cancel unused or misdirected links under Invitation links.

5. Under People with access, choose a role and Modules & reporting, then Save access. To remove someone, choose Remove access and Confirm remove access. Restore access restores the selected permissions. Only an owner can grant or manage an Administrator.

An organisation owner manages their own company. Owner transfer and billing activation need Assure Pro assistance. Removing cloud access does not erase downloaded offline copies; apply your device-return and data-retention process. Do not create a duplicate organisation to work around a missing invitation.

3. Open the same work on web & phone

1. On the web, select the organisation and go to Connected workspaces. Open the existing team workspace, or create one with its first workplace.

2. Install the supplied Android update over the existing app. Do not uninstall or clear app data. The private-signed candidate supports Android 9 and later; confirm the released package before distribution.

3. On a new or empty phone workspace, open Menu → App & files → Assure Pro cloud. Sign in, choose the organisation and select Open company workspace. Choose the same workspace name as the web.

4. If the phone already contains the intended business's work, use Connect this phone workspace. Its synced workspace then appears on the web. Do not connect fictional demonstration records to a client organisation.

5. Save a fictional test record and photo. Confirm cloud receipt, open it on the web, then edit a harmless field and confirm the phone receives it. Complete this check before the client's operational start.

Saved locally means work is on this device. Saved to Assure Pro cloud means a matching cloud receipt was received. Photos and files can remain pending after record details arrive. A connection badge alone does not prove every attachment has uploaded.

4. Do the safety work

1. Choose the workplace and job. Open the relevant module and select the record or create a new one. A dashboard count opens its relevant records; check the selected workplace and filters if the list differs from your expectation.

2. Enter the actual task, hazards, controls and responsible people. The platform manages record references, timestamps and revisions. Focus on what the crew must do.

3. Unfinished supported forms autosave on the current device. Use the form’s save action to create or update the record and queue cloud sync. An unfinished browser draft is not a shared cloud record.

4. Check required fields and the record’s review or issue action. Imported drafts require a comparison with the original. A saved record, cloud receipt or signature is not by itself an approval.

5. For issued or locked work, use the available revision action when the task or controls change. Review the new version and collect fresh acknowledgements where required.

6. In reports and analysis, set your start and end dates. The range includes both dates. Current overdue-action totals describe the current situation and can differ from activity within the selected period.

If devices changed the same record, use Review sync changes. Compare both copies before selecting which to keep. Do not repeatedly overwrite or reinstall to resolve a conflict.

5. Import, photograph & dictate

Import a SWMS, risk assessment, incident or emergency plan: open the module’s upload/import action, choose the original PDF, Word document, image or supported text file, and wait for extraction. Create a draft for review.

Compare the draft with the original. Check names, dates, task steps, hazards, controls, contacts and any table rows. Correct missing or misread information, then confirm extraction was checked. The original and extracted text stay attached; extraction never approves or issues the record.

For photos, open the record’s attachment action and choose the camera or an existing image when offered. Allow camera access on your own device. Reopen the saved attachment, then confirm it is also available on another connected device.

On Android, select the text field before using voice entry. Review the transcript before inserting it. Correct names, numbers and safety terms. Recognition availability depends on the phone and its installed speech service; the app asks before using network recognition when on-device recognition is unavailable.

If reading a file fails, keep the original. Try a clearer scan or enter the fields manually. If an upload stalls, keep the app installed, save your work and retry on a stable connection. Never assume a local photo has reached the cloud until its receipt and downloaded copy are confirmed.

6. Collect acknowledgements

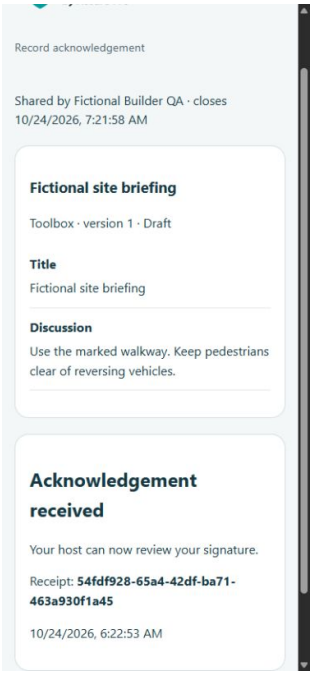
On this device: open the record, enter the signer’s full name, ask them to draw their signature and choose Record acknowledgement. A SWMS must be issued before people can acknowledge it.

QR signing: open QR signing session after syncing the record. Review the exact text, choose the duration and confirm sharing. The link exposes only the displayed record to its holder; attachments are not included.

Attendees scan the code, read the record, enter their name, draw and send their acknowledgement. They do not need an account. Their identity is self-declared. The host sees the count as receipts arrive.

Close session & review when attendees have finished. Inspect each name and signature, then choose Reviewed - add acknowledgement. A changed record cannot receive an acknowledgement from an older snapshot. Previous sessions on the same device remain reviewable.

Keep the receipt if the connection is uncertain. Retry saved acknowledgement reuses the submission ID instead of creating a duplicate. QR signing needs internet. Offline nearby/Bluetooth signing is not part of this release; use on-device signing when offline.



Fictional local acceptance test, 24 October 2026. Receipt screen; not evidence of a production signing session.

7. Contractors, visitors & inductions

1. From the organisation account, open Onboarding & inductions. An organisation administrator needs the relevant enabled module to create links or induction content.

2. Select the workplace and intended audience. Prepare employee, contractor or visitor induction content, or upload your own induction material using the available content/upload controls.

3. Create the intended person’s onboarding link and send it privately. Ask the person to complete their own details, required documents and individual induction. Do not use an editor invitation as a substitute for contractor onboarding.

4. Review submitted evidence, work scope, insurance or licence dates, and every linked worker’s induction and competency. An uploaded document or completed form does not automatically clear a contractor for work.

5. In the connected safety workplace, choose Get reviewed onboarding, select the linked workplace and choose Import reviewed handover. Close the panel to allow cloud sync. Check the business, workplace, records and evidence on the phone after syncing.

6. Returning visitors and contractors can use their personal pass where configured. Check arrival status and record departure. Changed work scope, induction content or expired evidence can require another review.

Phone users open the online onboarding portal from App & files. Offline local contractor records and online submitted applications are separate until the reviewed handover has been completed.

8. Pick the right module

All modules follow the same pattern: choose workplace/job, create or open, record the facts, attach evidence, save, then complete the required review or status action. Available modules depend on the organisation’s subscription.

SWMS	Task steps, hazards, controls, review, issue and worker acknowledgement.
Risks / hazards	Assess the exposure, controls and follow-up work.
Incidents	Record facts, evidence, investigation and corrective actions.
Emergency plans	Site arrangements, contacts, response instructions and reviews.
Toolbox / consultation	Briefings, feedback, attendance and agreed actions.
Inductions / training	Audience-specific learning, completion and competency evidence.
Prestarts / inspections	Checks, defects and actions before or during work.
Plant / maintenance	Asset information, condition, service and defects.
Permits	Scope, responsible people, time window and authorisation.
Contractors	Businesses, workers, documents, review and site attendance.
Audits / obligations	Review findings, duties, evidence and follow-up.
Actions / diary / documents	Supporting work included with the SWMS base subscription.
Psychosocial	Work-related risks and controls; restrict private person-level case material.
Confidential injury & recovery	Per-case restricted injury, recovery and related records.

9. Keep sensitive work restricted

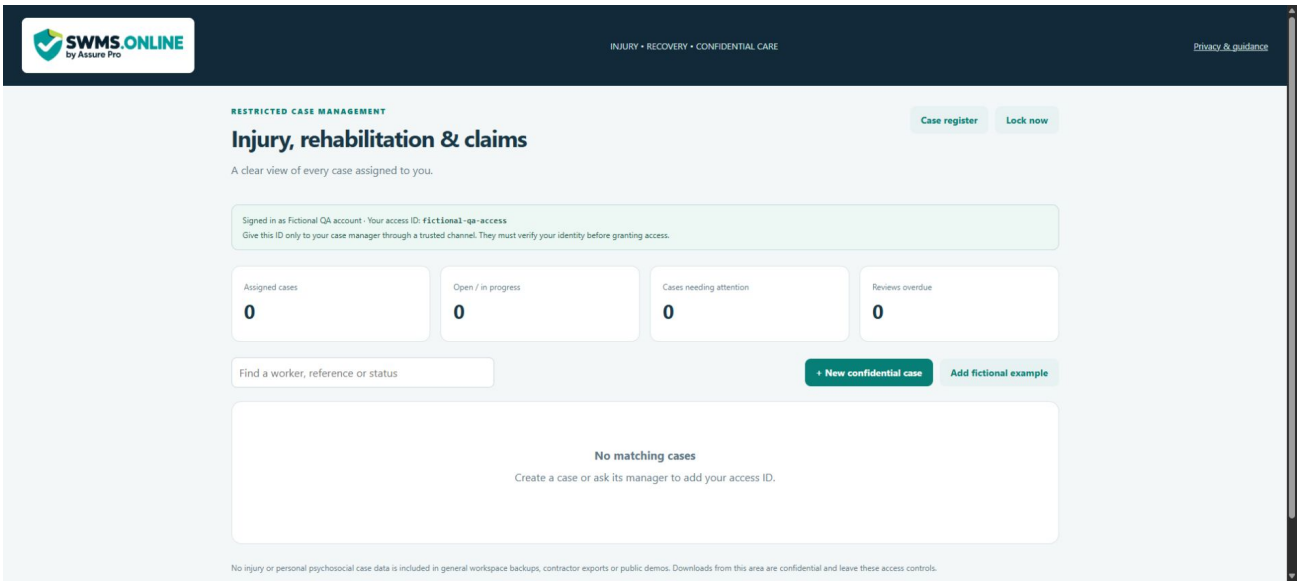
From Connected workspaces, choose Enterprise documents & actions or Confidential injury & recovery. These areas require internet and your Assure Pro account.

Enterprise: an organisation administrator can create a workspace. Other people provide the access ID shown after signing in; the administrator assigns the appropriate workspace role.

Confidential cases: choose Unlock case area. Give your access ID to the case manager. Company membership alone does not reveal a case. Access depends on the role assigned to that case.

Use Lock now when leaving the confidential area. Account & sign out returns to the account controls for full sign-out. On shared devices, do not leave downloaded documents or open sessions unattended.

Records from the previous sign-in system require a controlled migration. Do not recreate private cases in a general module or copy them into a different company to work around access.



Fictional test register. The case area uses additional access controls beyond company membership.

10. Troubleshoot without losing work

No organisation after sign-in	Use the owner setup or your private invitation. Do not create a duplicate business.
Phone says Offline	Check network, sign-in and company/workspace. Retry; keep the app and local backup.
Record is present but photo is missing	Check pending file status. Reconnect, retry sync and reopen the downloaded attachment.
Unfinished text is missing	Return to the same device/profile/account/workspace and the unfinished-form recovery control.
Conflicting versions	Open Review sync changes. Compare both copies before choosing the retained version.
Module locked / subscription ended	Check company and contact Assure Pro about the enabled module and paid term.
QR unavailable or record changed	Ask the host for the current session. Never sign an outdated copy to bypass the message.
Signature name already exists	Review the existing acknowledgement and remote receipt. Do not rename someone to force a duplicate.
Android reports incompatible signature	Stop. Keep the installed app and backup; contact support. Do not uninstall to bypass it.
Import misread the source	Correct the draft against the original and confirm the extraction review before release.
Cannot see a confidential case	Ask its case manager for the correct case role; membership alone is insufficient.

11. Owner handover & recovery

Before the first crew starts: confirm the company name, named owner, enabled modules and invoice term. Complete one invite/accept/revoke test with a second account and one phone → cloud → web → phone record-and-photo check using fictional information.

Confirm the crew knows where to see local save and cloud sync status, how to continue an unfinished form, and whom to contact. Have the safety lead review your actual templates and operating process.

Export a complete backup from App & files and keep it in your organisation’s approved secure storage. Test opening it in a separate controlled recovery workspace; do not overwrite the live workspace for a restore drill. A backup may contain personal and safety information.

For a lost device, remove or restrict the person’s cloud access and follow the business’s device-management process. Cloud revocation does not remotely erase already downloaded records. Contact Assure Pro before moving the recovered workspace to another company or account.

For support, provide the organisation, app version, device/browser, time, record title and exact error. Do not send passwords, verification codes, private QR/invitation links or sensitive records in the first email.

Assure Pro release acceptance includes live access-isolation tests, a real-device/network check, backup/restore verification, operational monitoring and safety-professional review. Those checks are separate from this guide. Do not describe the complete product as independently security-certified.

Editable templates and toolbox talks

1. Choose the workplace, then open SWMS, Risk assessments or Toolbox talks. Choose Browse templates and search for the topic, or Create from scratch for a blank record.

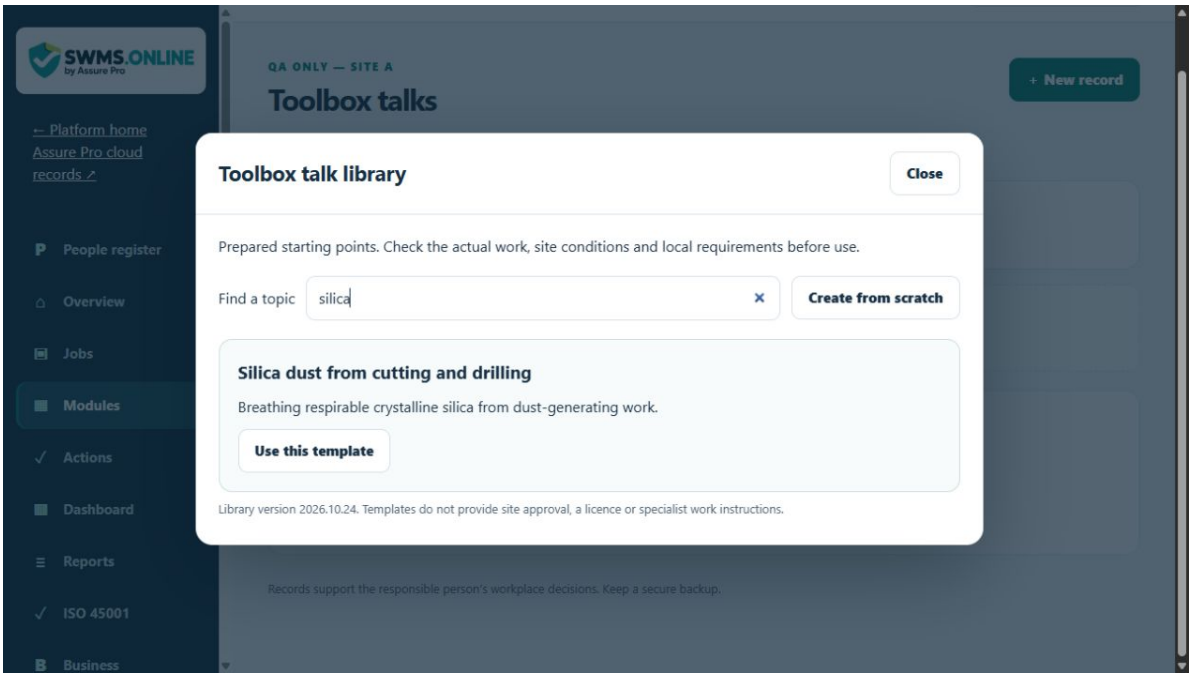
2. Use this template opens your own editable draft. Change the task, steps, hazards, controls, location and briefing points to match the actual work. The original library remains unchanged.

3. Complete Make this template site-specific, including what changed and who checked it. Enter actual risk ratings and responsible people. These fields are deliberately not fabricated for you.

4. Save draft, then reopen it to continue editing. Normal review and issue requirements still apply. A selected template is not an approved safe method.

5. For toolbox talks, record the real discussion, worker questions, attendees, signatures and agreed follow-up. Twenty prepared topics cover high-risk and common site hazards.

Safety training & competencies is available under Modules. Record courses, licences, competency evidence, completion, verification and expiry/refresher dates. It is a register, not an accredited learning course.



Local fictional workflow: searchable toolbox topics with an editable-copy or blank-record choice.

Expanded team controls

Open the organisation portal after signing in. Expanded role and module controls are available to organisation owners and administrators. Refresh the page if an older screen remains open.

1. The organisation owner or administrator opens People with access. Choose Standard user, Supervisor, Manager or View only as appropriate. Only the owner can grant or manage an Administrator.

2. Expand Modules & reporting. Select the modules the person needs and whether they may use reports, analytics and bulk exports. Save access. The organisation must also have an active subscription for each paid module.

3. Remove access requires an explicit second click. Restore access reactivates the selected role and permissions. Owners and your own account are protected against changes through this screen.

Standard users capture drafts and everyday checks. Supervisors review safety records. Managers can also manage workplaces. Administrators manage organisation access. Confidential cases still require separate case permissions.

Module assignments apply across the organisation’s sites. This release does not implement per-site private access boundaries. Removing cloud access does not erase copies already downloaded to a device.

Access is checked again by the cloud service. A changed permission can leave local work waiting rather than discard it. Contact your administrator; do not reinstall the app to resolve an access restriction.