

Admin_Guide

Administrator guide - Actuarial Closing Platform 3.2

Last verified against build: dev_rc1_20261005 (development copy, release candidate 3.2.0-RC1, store design), 2026-10-05.

For the platform Administrators of the Actuarial Closing department and for IT. How the platform works inside: Technical_Guide. The monthly procedure: Closing_Manual and the role guides (docs/guides). Store recovery: docs/guides/STORE_RUNBOOK.md. IT prerequisites and the go-live checklist: docs/guides/IT_PREREQUISITES.md, docs/guides/GO_LIVE_CHECKLIST.md.

1. What an Administrator does

- Installs the platform and runs Setup; runs it again when a folder or the platform location changes.
- Manages users and roles, command permissions and administrator passwords (Users and roles).
- Maintains the administrator tables: Parameters, ColumnMap, DimCompany, FX, currency aliases, RefData, Threshold_Register, KPI_Catalog, DecisionRegister and AdminConfig. Editing them needs the administrator sign-in; after an edit of RefData or Threshold_Register run Refresh reference data.
- Owns the store: Backfill at installation, the column-map lock, Rebuild store, Verify log.
- Handles exceptions: re-open of a closed month, manual FX, stale lock files, security reviews, store recovery.
- Records every structural change with Add changelog entry.

An Administrator does not prepare or close months by virtue of the role; a person who also prepares or reviews holds the Preparer or Reviewer role as well, and the segregation of duties still applies (the user who submitted a month can never close it).

2. Installation

1. **Excel.** Excel for Microsoft 365 on Windows (Data Model, CUBE functions, dynamic arrays and VBA are required).
2. **Folders.** IT creates the platform folder on the shared network drive (for example \\fileserver\ActuarialClosing\Platform) and grants the permissions of section 6. The source folder, where the companies deliver their files, is usually elsewhere.
3. **Workbook.** Copy Actuarial_Closing_Platform.xlsm into the platform folder. Keep one platform file; every other copy shows the COPY banner and cannot change data.
4. **Macros.** IT makes the platform folder a Trusted Location for the users, or signs the VBA project (DecisionRegister D37). Without macros a user sees only the Start sheet, which explains this.
5. **Privacy levels.** The workbook uses "Ignore the privacy levels" (Data > Get Data > Query Options > Current Workbook) and the platform re-sets it at every open; only dates leave the workbook, to the CBRT (D34). A machine policy that enforces privacy levels for every file stops the refresh: check it first (GO_LIVE_CHECKLIST, item 1).
6. **Setup.** The first Administrator opens the platform file; Setup starts by itself (section 3).

3. Setup

Setup is a sequence of dialogs; each step shows what it found, and Cancel stops at any time. Every change is logged with its old and new value.

1. **Administrator.** On a platform without users you are asked whether you want to become the first Administrator. This can be done once. You set your administrator password now (section 5); the claim is logged with severity HIGH. On later runs you sign in with your password.
2. **Source folder.** Pick the folder with the company payment files (sub-folders are read). A mapped drive letter is stored as its UNC path.
3. **Platform folders.** Yes = Archive (the store, its inbox and the controls files), Log, Export and src are created in the workbook folder (stored as .\Archive etc.). No = pick each folder.
4. **Validation.** Each folder must exist and be reachable; Archive, Log, Export and src must be writable (a probe file is written and deleted), the source folder readable, and the workbook folder writable (for ACP_Settings.ini and ACP.lock). Archive, Log and Export must not lie inside the source folder, and no folder may be a web address or a OneDrive / SharePoint synchronised folder (section 17). A local path (C:...) is accepted with a warning, because other users cannot reach it. On a failure you can pick the folders again.
5. **Discovery.** The file-name parser lists every file of the source folder (sheet STG_Discovery). Setup proposes the new companies (added to DimCompany with ExpectedFromPeriod = the first period found and SourceMode FOLDER, or CUMULATIVE for a company that delivers one ALL file; enter their name and type afterwards on sheet DimCompany), ArchiveStartPeriod (the earliest period found) and ActivePeriod (the earliest period not yet stored). Near-miss files (they break the name pattern, or their company ID differs from a listed one only by leading zeros) and unrecognised files are listed; fix or move them. A zero-padded twin is never proposed as a company.
6. **Users and roles.** Add users as DOMAIN\logon with their roles (section 4). Setup warns while fewer than two Administrators exist: only another Administrator can reset a lost password.
7. **FX check.** One CBRT bulletin request. If the CBRT cannot be reached, FXAutoFetch is set to N and the rates are entered by hand (section 8).
8. **Finish.** ACP_Settings.ini is written next to the workbook, the genesis event PLATFORM_INITIALISED (or SETUP_UPDATED) is logged, the first Refresh runs and the Home banner shows the next action. Then lock the approved column map (section 15) and, if the source folder holds several past months, store them with Backfill history (section 10).

The settings file (ACP_Settings.ini, UTF-8, one key=value per line) holds SourceFolder, PlatformFolder, ArchiveFolder, LogFolder, ExportFolder, SourceCodeFolder, PlatformHomePath, SetupCompletedOn and SetupCompletedBy. Relative paths are relative to the workbook folder. Change it only through Setup; VBA writes the resolved UNC paths into tblParameters at every open and before every refresh, where Power Query reads them.

Setup without dialogs (a desktop front end or an installation script): Application.Run "Api_SetSilent", True, then Application.Run "Cmd_Setup",
 "claim=Y|displayName=|password=|source=|platform=.\archive=.\Archive|log=.\Log|export=.\Export|src=.\src|addCompanies=Y|archiveStart=|active=|users=DOMAIN\u1:Name One:Preparer;DOMAIN\u2:Name Two:Reviewer+Analyst|fx=test". The password is used once and never logged.

4. Users and roles

Roles (a user may hold several; everyone not listed is a Viewer):

Role	May do
Viewer	read what is visible; export the Dashboard PDF
Analyst	Viewer + show and export the lines of a company and month (DataView)
Preparer	Analyst + Refresh, reconciliation totals, nil returns, check explanations, Submit for review
Reviewer	Analyst + Refresh, Reject submission, Close period, closing pack, archive notes
Administrator	Setup, users and roles, re-open, ColumnID verification, source export, log verification, changelog entries, staging sheets, lock clearing, Refresh, and the administrator tables - after signing in

The exact rights are the table tblCommandPermission (sheet Security, very hidden): Command x Role = Y / N.

Home > Users and roles (Cmd_ManageUsers; administrator sign-in needed):

Choice	What it does
1 Add a user or role	DOMAIN\logon (the domain may be left out for your own domain), display name, roles (comma separated)
2 Remove a role	The role row is set inactive with ValidTo = today; rows are never deleted. The last active Administrator cannot be removed
3 Reset another administrator's password	The user sets a new password at the next sign-in (severity HIGH)
4 Change your own password	New password twice
5 Change a command permission	Command (e.g. Cmd_RefreshAll, Edit_Recon) and Role=Y or Role=N
6 Accept the security tables	Only after a review, when the banner says the role table was modified outside the application (section 9)

Every change logs a SECURITY event with the old and new value, the list of active Administrators and the checksum of the security tables. Keep at least two Administrators.

5. Administrator password

- Each Administrator has an own password; there are no shared role passwords. Sign-in = Windows identity + that password.
- Rules: at least 12 characters, not containing the logon name, not one repeated character. Keep it in a password manager.
- Storage: only a salted, iterated hash (PBKDF2-HMAC-SHA256, 600,000 iterations, 16-byte random salt per Administrator) in tblAdminCredential. The password itself is never stored, never written into code or documentation and never logged.
- Five wrong passwords lock the sign-in for 30 minutes. Every attempt, successful or not, is logged.
- A sign-in lasts 30 minutes and is renewed by every administrator action; Administrator sign-out ends it.
- Switching FourEyesRequired off asks for the password once more and is logged with severity HIGH.
- **Recovery.** Another Administrator resets the password (Users and roles > 3); the user sets a new one at the next sign-in. If no other Administrator can sign in, IT restores the platform folder from backup. There is no master password and no other way in.

6. IT request - folder permissions

Send this to IT when the platform is installed or a user joins or leaves. It assumes four directory groups; the roles inside the workbook are still assigned per user in Users and roles.

Subject: Actuarial Closing Platform - folder permissions

Please create the groups ACP-Users (every platform user), ACP-Preparers, ACP-Reviewers and ACP-Admins, and set these NTFS permissions (inheritance to sub-folders and files):

Folder	ACP-Users	ACP-Preparers	ACP-Reviewers	ACP-Admins
Source folder (company files)	Read & execute	Read & execute	Read & execute	Read & execute
Platform folder (workbook, ACP_Settings.ini)	Read & execute	Modify	Modify	Modify
Platform\Archive	Read & execute	Read & execute + Write (no Delete)	Read & execute + Write (no Delete)	Modify
Platform\Log	Read & execute + Create files (no Delete, no overwrite)	Read & execute + Write (no Delete)	Read & execute + Write (no Delete)	Modify
Platform\Export	Modify	Modify	Modify	Modify
Platform\src	-	-	-	Modify

Delete in Archive and Log is granted to ACP-Admins only. Please make the platform folder a Trusted Location for the members of ACP-Users (Excel Trust Center, "Allow Trusted Locations on my network"), or sign the VBA project with the organisation's code-signing certificate. Please back up the platform folder daily and keep the backups of Archive and Log for at least ten years.

Notes for the Administrator:

- Modify on the platform folder is needed by everyone who changes the platform: Excel saves through a temporary file, and long commands write and remove ACP.lock there.
- Create files for all users on Log: the platform writes one read-only file per event, including the denied attempts of Viewers and Analysts, who open the workbook read-only. If IT allows only Read for ACP-Users on Log, those events stay in the users' sessions and are not kept.
- Setup checks the access of the Administrator who runs it. For the other roles, test once with a Preparer and a Reviewer account: the banner must not say read-only, and Refresh must answer OK.

7. Moving the platform

1. Ask the users to close the file. Copy the whole platform folder (workbook, ACP_Settings.ini, Archive with STORE_PAY.csv, Inbox and the controls files, Log, Export, src) to the new share. Relative paths (.\Archive) keep working. Compare the SHA-256 of STORE_PAY.csv before and after the copy.
2. Open the workbook at the new place. The red COPY banner appears.
3. Home > Setup. Answer Yes to "Has the platform been moved here?", check the folders (pick the source folder again if it moved) and finish. The new PlatformHomePath is logged.
4. Make the old folder read-only and keep it as evidence; never delete the old Log folder before the new one holds all ACT_*.csv files.

8. FX manual mode

When the CBRT bulletins cannot be reached (FX_FETCH REVIEW, or Setup's FX check failed):

1. Sign in. Parameters: FXAutoFetch = N.
2. Sheet FX, tblFXRate: add one row per business day and currency - RateDate, CurrencyCode (ISO), RateToTRY (TRY per 1 unit, the CBRT forex buying rate), Source ("CBRT ForexBuying bulletin (manual,)"). Source: www.tcmb.gov.tr/kurlar.
3. Refresh. FX_FETCH reports that the automatic fetch is off; FX_RATES must be OK.
4. When the connection works again, set FXAutoFetch = Y: the next Refresh fetches every bulletin after the last stored rate.

9. Security review (red banner)

"Role table modified outside the application - Administrator must review" means the security tables differ from the last signed state, or the ActivityLog chain is broken. Everyone is a Viewer until it is resolved.

1. Sign in (only the Administrators of the last signed state can).
2. Users and roles > 6 shows the reason and the current users. Compare them with the last SECURITY event in the external log folder (the ACT_*.csv files are authoritative).
3. If the tables are right: accept (logged with severity HIGH). If not, or if the ActivityLog chain is broken: do not accept; IT restores the platform folder from the last good backup.

10. Other administrator tasks

- **Re-open a closed month.** Home > Re-open period, month (YYYYMM) and reason. The month's batch stays in the store (append-only) and its ArchiveLog row becomes SUPERSEDED; the controls file moves to Archive\Superseded (never deleted); ActivePeriod becomes that month. The month is then prepared and closed again by a Preparer and a Reviewer, which appends batch -2. Only the CURRENT batch of a month is read.
- **Adding a company.** Setup proposes new companies from the file names; otherwise add a DimCompany row (CompanyID exactly as in the file name, name, type, ExpectedFromPeriod, SourceMode). Refresh, classify its new headers (below) and ask the Preparer to add its Recon rows. A company that delivers one cumulative file: docs/guides/CUMULATIVE_COMPANY.md.
- **Classifying a new header.** Refresh; STG_DQ lists every UNMAPPED HEADER (Show staging). Sign in and unlock the column map (section 15); on ColumnMap add one row per header: SourceHeader (exact spelling), CanonicalName (an existing field, or a new one), ColumnID (from the schema reference), DataType, IncludeInModel, PersonalData (ask the Data Protection Officer when in doubt; blank means personal), Group, Notes. Refresh; MAPPING_DQ must be OK; lock the map again (and Rebuild store if a model field was added). Verify the ColumnIDs with Verify selected ColumnIDs once they are checked against the schema reference.
- **Past months (backfill).** When the source folder holds months before go-live, Setup proposes the earliest one as ArchiveStartPeriod and ActivePeriod. Rather than closing each of them with four-eyes, lock the column map, sign in and run Home > Backfill history once: every month before the newest one is stored as found by the bulk build (BulkChunkMonths months per refresh, default 12; one batch, one ArchiveLog row and one SignOff BACKFILL row per month, files copied to the inbox, the workbook saved after each chunk; about 25 minutes for 119 months at rehearsal volume, P3-102). Type BACKFILL to confirm. Files that fail the whitelist gate are listed in the result and never stored. The newest month stays open and is closed normally by a Preparer and a Reviewer. If the run stops, fix the cause and run it again: stored months are skipped (D61, P3-87, P3-95).
- **Stale lock.** A lock file older than 2 hours (a crashed session): Home > Clear lock (logged with severity HIGH).
- **Changelog.** Home > Add changelog entry: version, what, why, components, breaking changes. Your name and DOMAIN\logon are stamped; typing in tblChangelog is reverted.
- **Source export.** Home > Export source code writes src\pq, src\vba and src\contract into SourceCodeFolder. The VBA part needs "Trust access to the VBA project object model" and an unlocked project (unlock it for the session in the VBA editor); otherwise it is skipped with a note.
- **Drill-through limit.** Double-clicking a Data Model pivot value lists at most 1,000 rows; the governed way to list lines is DataView. The limit can be raised by hand: Data > Queries & Connections > ThisWorkbookDataModel > Properties > Usage (D49).

11. Locking the VBA project (owner)

The VBA project is locked for viewing after the source export of a release. The password is chosen by the owner and never stored in the workbook, the source export, the documentation or any log. There is no scripted way to set it; do it by hand:

1. Make sure nobody else has the platform file open. Open it with macros enabled.
2. Press Alt+F11 (VBA editor). Tools > VBAProject Properties > tab Protection.
3. Tick "Lock project for viewing", type the password twice, OK.
4. Close the VBA editor and save the workbook (Ctrl+S; the platform keeps only the Start sheet visible in the saved file). Close Excel.
5. Re-open the file: the platform works as before; the VBA editor now asks for the password to show the code.
6. Keep the password in the organisation's password vault, with a deputy.
7. Check: Home > Export source code (Administrator) exports the queries and the contract; the VBA part reports that the project is locked, unless you unlock it for the session in the VBA editor first.

12. Backup and restore

- IT backs up the platform folder daily. The Log folder is the authoritative audit trail; the Archive folder holds the store (STORE_PAY.csv), the inbox (the stored source files) and the controls files.
- Restore = the workbook and ACP_Settings.ini of the same day together with the Archive folder of the same day (the ArchiveLog chain in the workbook must match the store), and the Log folder. After a restore, events written after the backup remain in the Log folder and show as INFO ("not in this workbook").
- If only the store file is damaged or lost, the inbox is enough to rebuild it: docs/guides/STORE_RUNBOOK.md.

13. Open items (Backlog)

Deferred decisions of the 3.0 register (A1, A3, A4, A6 - data owners; D36 - IT) are on sheet DecisionRegister, Backlog. Every open item of 3.2 with its owner and release target is in docs/BACKLOG.md; every decision with its status in docs/DECISION_INDEX.md. Record outcomes with Add changelog entry.

14. Files that do not enter the store (3.2.0)

Only companies in the company list (DimCompany), inside their reporting window, in their source mode and with a correctly named file reach the store (DECISIONS_P3 P3-86, P3-91, P3-92, P3-110). Every file of the active delivery that will not get in is listed in the rejected-lines log **STG_Rejected** (Show staging > STG_Files, right of the file list) with its rule and what to do; the analytics pages show "Not admitted to the store: n lines in m files", AN_Index explains it.

Rule	Meaning	Administrator path
NOT LISTED	the company is not in DimCompany; its lines are loaded for review (segment <i>Unassigned</i>) and block the close	add the company (DimCompany: CompanyID exactly as in the file name, name, type, ExpectedFromPeriod, SourceMode) and Refresh, or have the file removed
OUTSIDE WINDOW	the month is outside ExpectedFromPeriod..ExpectedToPeriod	correct the window, or remove the file
NEAR-MISS	the name breaks the pattern, or the company ID differs from a listed one only by leading zeros (COMP08302... while 8302 is listed)	have the file renamed; never add the zero-padded ID as a new company
MODE MISMATCH	a monthly file of a CUMULATIVE company, or an ALL file of a FOLDER company	correct SourceMode, or ask for the agreed delivery

Company IDs are text and are compared exactly as listed. An ID that really starts with a zero is allowed when it is listed that way (the CompanyID cells are text); Setup never proposes a zero-padded twin of a listed or discovered company. The *Unassigned* segment therefore holds only lines of companies outside the list (active month, not closable) or of a stored company whose type was later removed.

15. Changing the column map (3.2.0)

The store keeps only the dictionary fields that are in the model and is laid out by the dictionary, so the map is locked (check COLUMNMAP_LOCK, BLOCKING; Backfill, Close and Rebuild store refuse to run while it is not locked or has changed). To change it:

1. Sign in. Home > **Unlock column map** (column J), reason (SECURITY event, severity HIGH).
2. Edit tblColumnMap (sheet ColumnMap). Refresh; MAPPING_DQ must be OK and STG_DQ must show no DICTIONARY INCONSISTENT.
3. Home > **Lock column map**: who approved the change and when, then type LOCK.
4. If a model field was added or removed: Home > **Rebuild store** (typed REBUILD): every stored month is re-read from Archive\Inbox with the new layout; the old store moves to Archive\Superseded. Refresh; ARCHIVE_INTEGRITY must be OK. A change of ColumnID, notes or verification stamps does not affect the lock.

16. A second Administrator

Keep at least two active Administrators (the last one cannot be removed, and only another Administrator can reset a forgotten password).

1. The first Administrator signs in, Home > Users and roles > 1, enters the colleague's DOMAIN\logon, display name and the role Administrator.
2. The new Administrator opens the platform with macros enabled and signs in (Administrator sign-in): having no password yet, they set their own (at least 12 characters) and sign in with it from then on.
3. Check: Users and roles shows both as active Administrators; the ActivityLog holds the SECURITY events of the addition and of the first sign-in.
4. Each keeps the password in a password manager; a password reset (Users and roles > 3) is done by the other.

17. Location of the platform (3.2.0)

The platform runs only from a local or network (UNC) folder. Opened from a web address (SharePoint / OneDrive in the browser, AutoSave) or from a folder that OneDrive / SharePoint synchronises - the workbook or any of its Source, Archive, Log and Export folders - the red banner says so and every command that changes data is refused: two synchronised copies of the store, the logs or the lock file would diverge. Move the platform folder to the share agreed with IT (section 7) and open it from there.

Power Query privacy levels. The platform's queries combine the workbook (folders, parameters) with the files they read; the workbook therefore stores "ignore privacy levels" and the platform re-sets it at every open. If a machine policy enforces privacy levels for every file (Excel > Data > Get Data > Query Options > Privacy: *Always combine data according to your Privacy Level settings for each source*), Refresh stops with FIREWALL_BLOCKED: IT sets the option to *Combine data according to each file's Privacy Level settings* for the platform users. The two-minute check before go-live is item 1 of docs/guides/GO_LIVE_CHECKLIST.md; a redesign that survives the enforcement is planned for 3.3 (BL-65).

18. Password window and raw view (3.2.0)

- **Password window.** Sign-in uses the masked window frmPassword. If it is missing or damaged (for example re-imported without its .frx), sign-in is refused with a message and a SECURITY event; it never falls back to an unmasked box. Repair: in the VBA editor remove frmPassword, File > Import File > src\vba\frmPassword.frm (frmPassword.frx must be next to it), save.
- **Raw view (AN_RawView).** Analysts, Preparers and Reviewers list the lines of several companies and months (whitelisted, non-personal columns only), reconcile them to the recorded batch totals and export them as CSV; Preparers and Reviewers may open a line's source file (its inbox copy for a closed month) after giving a reason. Every use is one ActivityLog row; the lines are removed before the file is saved and are never exported as PDF. Viewers and Administrators do not see the sheet.