

Access inventory: accounts, keys and permissions

Sample document. The business and people are fictional, and the names in square brackets are placeholders. It shows the format of a Teknetik access inventory.

This page lists every account, key and permission the workflow uses. Each one is in the firm's name and limited to what the workflow needs.

This page names keys but never contains them. Keys and passwords are never put in emails, documents, screenshots, chat messages or code.

What each one is for

ITEM	PURPOSE	LEAST-PRIVILEGE SCOPE	OWNER
Mailbox permission (read and send)	Reads new enquiries and sends approved replies	The one shared mailbox only: read messages and send from the shared address. Read-only access means it cannot move or delete mail. It cannot reach staff mailboxes.	The firm
Model supplier account	Holds billing, the spend limit and the keys	Owner: [named owner]. Teknetik is a member during the pilot only.	The firm
Model API key (live)	Used by the workflow for real enquiries	One key, used only on the firm's server. It sits in a separate area of the account (a workspace) with a monthly spend limit of [amount agreed at scoping].	The firm
Model API key (test)	Used for test runs only	A separate key with a lower spend limit of [amount agreed at scoping], never used for live enquiries	The firm
Job system API key	Creates a job record when an enquiry is approved	Create new jobs only. It cannot read invoices, edit or delete jobs, or see customer history. If the job system cannot limit a key this far, the gap is recorded here: [gap, if any, recorded at setup].	The firm
Server or hosting	Runs the workflow and holds the desk database	A named admin account for each person who needs it. No shared logins.	The firm
Desk logins	Lets approvers use the desk	One login for each approver, so the audit log shows who approved what	The firm

There are also two settings, which are not accounts:

- **The inbox rule** adds the "Desk" label to new messages in the shared inbox. It is named [rule name used at setup].
- **The mailbox app registration** is the name the workflow appears under in the email admin centre: [app name used at setup].

Who holds access, and when ours ends

ITEM	DURING THE PILOT	WHEN TEKNETIK'S ACCESS ENDS	ROTATE IT EVERY
Mailbox permission	Granted by the firm's email admin. Teknetik can reach its secret through the server.	Secret renewed at sign-off, and any Teknetik admin role removed	Sample: 12 months, and when anyone with access leaves
Model supplier account	The firm owns it. Teknetik is a member.	Membership removed at sign-off	Not applicable
Model API keys (live and test)	Created by Teknetik in the firm's account	Replaced at sign-off with new keys that only the firm has seen	Sample: 12 months, and when anyone with access leaves
Job system API key	Created by the firm and given to Teknetik for setup	Replaced at sign-off	Sample: 12 months, and when anyone with access leaves
Server or hosting	Teknetik has a named admin account	Removed at sign-off	Change passwords and keys when anyone with access leaves
Desk logins	Sam, the cover approver and the owner. Teknetik has an admin login.	Teknetik's login removed at sign-off	Remove leavers on their last day

Sign-off is recorded in 07-acceptance-review: [date agreed at acceptance].

If you take monthly care

Under care, we need a little access back for the health check and small changes. If you take care, the firm creates a separate care account with:

- a desk login that can view the report, the audit log and the manual queue
- an admin account on the server, for checks and small changes (this can reach the keys held on the server)
- no access to the mailbox, the model supplier's billing or the job system's admin settings

The firm can remove care access at any time. We ask for it to be removed on the day care ends.

How to rotate each one

To rotate is to replace a key or password with a new one, then switch off the old one. Do it on the schedule above, when someone with access leaves, and whenever a key may have been seen by someone who shouldn't have it.

Model API key

1. In the firm's Claude API console, create a new key, named as before with today's date added.
2. Put the new key into the server's settings, then restart the workflow.
3. Send a test enquiry from a test address to the shared inbox and check that a job card appears.
4. Delete the old key in the console.

Job system API key

1. Create a new key in the job system with "create jobs" permission only.

2. Put it into the server's settings and restart.
3. Approve a test enquiry with every job detail and check that the record appears. Then delete the test record.
4. Revoke the old key.

Mailbox permission

1. In the email admin centre, find [app name used at setup].
2. Renew its secret or certificate, or remove access and grant it again with the same limits.
3. Put the new secret into the server's settings and restart.
4. Send a test enquiry and check that it appears in the desk.

Server accounts and desk logins

1. Remove the account of anyone who no longer needs access.
2. Change any password or key they may have known.
3. Check that the list of accounts matches the table above.

Sign-off checklist

Completed at the acceptance review, and recorded in 07.

- ☐ Teknetik's membership of the model supplier account removed
- ☐ Live and test model keys replaced, and the old keys deleted
- ☐ Job system key replaced, and the old key revoked
- ☐ Mailbox permission secret renewed, and any Teknetik admin role in the email admin centre removed
- ☐ Teknetik's server account removed
- ☐ Teknetik's desk login removed
- ☐ Care account created, if care was taken