ProjectX

LIFECYCLE · DATASHEET

Day-one access. Day-zero offboarding.

Joiners, movers and leavers handled as governed requests: role profiles decide what a person gets, approvals happen in order, and every step is executed, recorded and evidenced — so offboarding is one approval and a revocation record, not a week of tickets.

Why teams choose it

01
Day-one access without the ticket queue
A role profile decides what a new joiner gets before they start. Approvals happen in order, execution is automatic, and their credentials are handed over exactly once.

02
Offboarding is one approval
A leaver request executes every revocation step in order and records each one. Access ends when the approval lands — not when someone works through a spreadsheet.

03
Every step can be evidenced
Each request carries its owner, effective date, approvals and execution history, so “who had access, from when, by whose approval” is a record, not an investigation.

04
A failed step never leaves a mess
Execution retries safely where it stopped, and every completed step names the rollback that undoes it — partial change never becomes permanent drift.

In numbers

2
approvals, manager then IT, before anything runs

1
read of a new joiner’s credential, then it is gone

500
people in one bulk cohort, each with their own approvals and record

What it does

Structured joiner, mover and leaver requests

Every change starts as a tracked request with an effective date, an owner and a full history — not an untracked instruction in an inbox.

A request is raised with the person, the role, the effective date and the owner, and it keeps its full history from that moment. Nothing about someone's access changes outside one, so "how did they get this?" always has an answer.

Role profiles and ordered approvals

Reusable entitlement bundles define what a role gets. Manager and IT approvals happen in order, and nothing executes until every required approval is in.

Define the bundle once — the access a support engineer gets, the access a finance lead gets — and every request reuses it. Manager and IT approve in a defined order, and execution waits until every required approval has landed.

Safe retries and explicit rollback

Every step of execution is recorded. A partial failure can be retried safely, and each completed step names the rollback that undoes it.

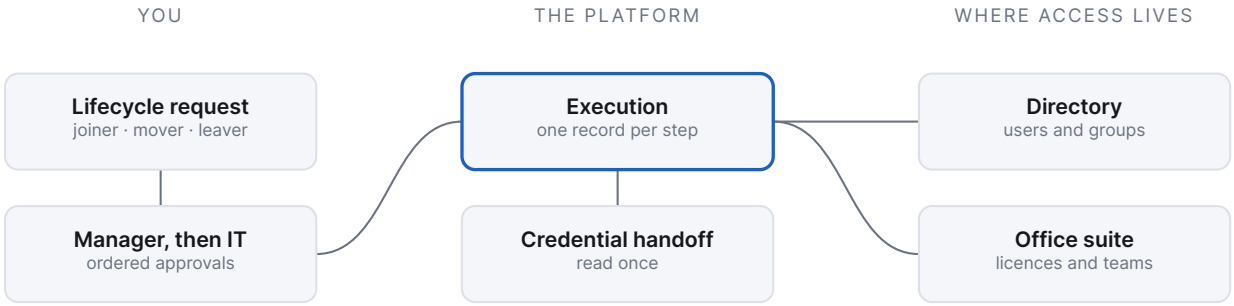
Execution records every step as it runs. A step that fails retries safely where it stopped, and each completed step names the rollback that undoes it — a partial change never becomes permanent drift nobody can explain.

Single-read credential handoff

New credentials are handed over once and expire — the platform keeps a fingerprint of the handoff, never the reusable secret.

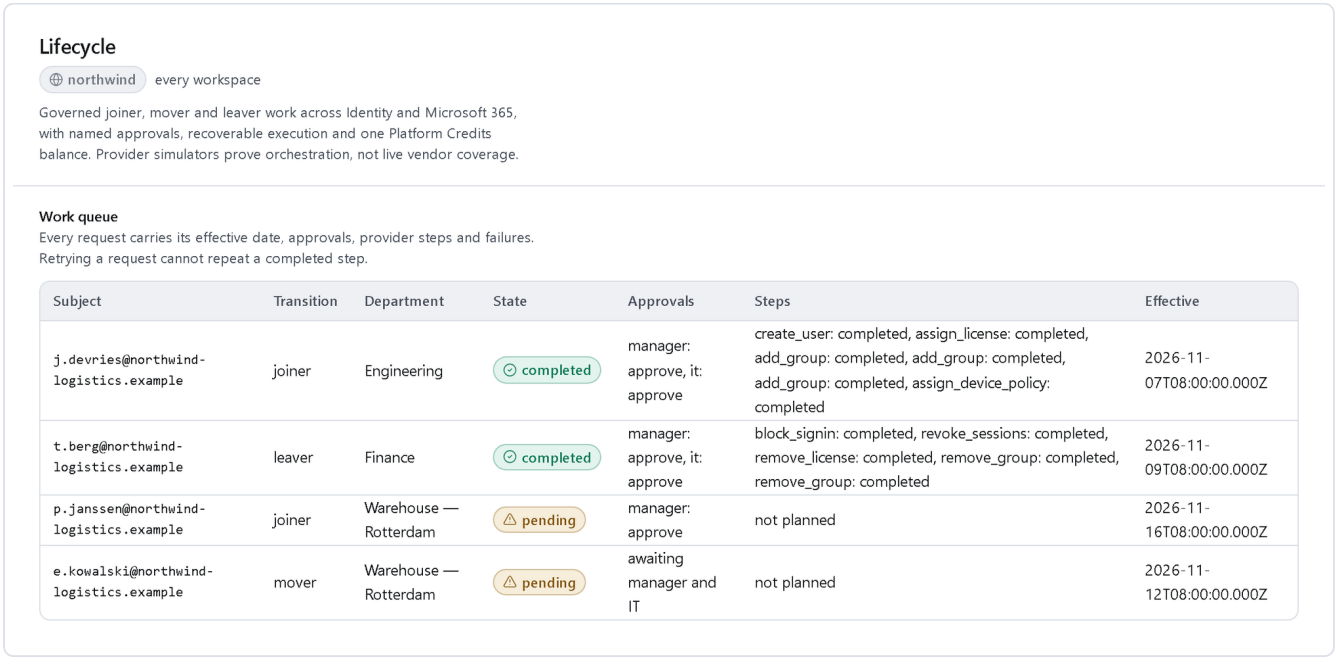
The new joiner's credentials are shown once, to the person they belong to, and then they expire. The platform keeps a fingerprint proving the handoff happened — never the reusable secret itself.

How it fits together



A request names the person, the effective date and the role profile. The manager and IT approve in order. Only then does the platform run each provider step, record it, and hand the first credential over once.

In the console



Every joiner, mover and leaver with its approvals and the steps it ran. Screens shown with demo data.



Role profiles: the access each kind of employee gets, defined once. Screens shown with demo data.

Key ideas

Role profile

A named bundle of licences, groups, teams, applications and device policy for one kind of employee. A request points at a profile instead of listing access by hand.

Joiner, mover, leaver

The three changes a person’s access goes through. Each is a request with an owner, an effective date and a history that cannot be edited.

Compensation

The explicit undo for a step that completed before a later one failed. It is run on purpose and recorded, never presented as a successful run.

In depth

Execution you can retry
Each provider step is recorded as it runs. Retrying a request skips the steps that already completed, so running it twice never creates a second account or assigns a licence twice.

HR as the source of truth
A full read from the HR system flags people who exist in the directory but not in HR as orphans for a person to decide on. Nobody is suspended automatically on a mismatch.

Licence insight
Lifecycle prices its own execution history against your licence rate card and names the reclaim candidates: suspended, deprovisioned, orphaned and 90 days idle.

For service providers
A client grants its service provider a time-boxed window, eight hours at most, that the client can see and revoke. No query ever crosses from one company into another.

How it works

01 **Model your roles** · Console
Role profiles bundle the access each kind of employee gets — defined once, reused for every request.

02 **Raise a request** · Console
A joiner, mover or leaver request carries an effective date and an owner from the moment it is raised.

03 **Approvals run in order** · Console
Manager and IT approve in a defined order; nothing executes until every required approval is in.

04 **Watch it execute** · Audit trail
Every step runs, retries safely if it fails, and leaves evidence — with new credentials handed over exactly once.

Who it is for

HR and IT together
A joiner starts Monday and needs everything ready — accounts, access, credentials.

The role profile decides the access, the approvals run in order, and the handover happens once, on the effective date.

Security teams
A leaver's access must end completely and provably, the day they leave.

One approval executes the revocation sequence and leaves an evidence record behind.

Growing companies
People change teams constantly, and access quietly piles up.

Mover requests adjust access as a tracked change with history, so entitlement follows the role, not the person's memory.

Works with

Console · API · Audit trail

Questions buyers ask

How does a new joiner get access?
You define role profiles once — the bundle of access each kind of employee gets. A joiner request names the profile and the effective date, the manager and IT approvals happen in order, and execution runs automatically. Credentials are handed over once, single-read.

What happens when someone leaves?
A leaver request executes the revocation steps in order and records each one. Every completed step names its rollback, and the finished request is the evidence the access is gone.

Can we prove this to an auditor?
Yes. Every request carries its owner, effective date, ordered approvals and full execution history — the record is the evidence.

How is it priced?
At published usage rates in Platform Credits — you pay for what you use, on the same invoice as the rest of the platform. The rates are on the pricing page.

Pricing

Current published rates, in your currency: https://adaydev.com/pricing/products/lifecycle