zsoftly

WHITEPAPER · BUSINESS ACCESS

Business identity with Authentik Enterprise

A practical guide to access decisions, hosting, operations and a controlled pilot. Understand what is documented, what remains in preview and what your business still needs to own.

AUTHOR
Ditah Kumbong
ZSoftly Technologies Inc.

DATE
15 November 2026

VERSION
1.0

AUDIENCE
Business owners and IT leads

CONTENTS

Executive summary: decide who needs access	Page 2
Enterprise capabilities and maturity	Page 3
Office or cloud: architecture and responsibilities	Page 4
Joining, changing roles and leaving	Page 5
Provisioning directions and account ownership	Page 6
Coexistence and migration boundaries	Page 7
Operations, recovery and useful evidence	Page 8
Licensing example and cost worksheet	Page 9
Pilot acceptance and a scoped service	Page 10
Sources and publication notes	Page 11

Product facts checked on 15 November 2026. Our production experience is described on page 2. Examples, diagrams and acceptance criteria are planning aids. Preview features retain their documented limits.

START WITH THE WORK

Decide who needs access, then choose the system

A contractor joins for two weeks. They need a project application, permission to update assigned work and a clear end date. The owner needs to know who approved access and whether it ended. Those decisions belong to the business, even when a specialist operates the software.

Authentik connects sign-ins across applications supporting a common sign-in standard. Its open-source edition covers OpenID Connect, SAML, LDAP and RADIUS for sign-in, and provisions accounts over SCIM with a static token [7, 18]. Paid Enterprise adds the capabilities on page 3 [1]. Protocol support is where an integration starts. Each application still needs configuration, its own permissions and tests.

Three questions before a purchase

Question	Write down an answer
What work needs access?	Name the application, permitted action and business owner. Avoid starting with a list of products.
Who runs the service?	Assign updates, monitoring, recovery, incident response and application support.
What proves it works?	Define approval, denial, departure and recovery tests before changing daily work.

Make control observable

Hosting on your hardware or a chosen cloud gives you deployment choices. It does not settle administrator access, backup protection or handover. Ask for a written responsibility map and a demonstration of recovery. Keep business ownership of access decisions separate from technical administration.

For the contractor example, write a one-page access record: sponsor, application, role, start date, end date and removal owner. Use the same record when comparing an existing service with a proposed alternative. This exposes missing work before it becomes an urgent support problem.

> **A useful outcome:** one workflow with understood costs, tested access and a recovery owner. Do not make a complete platform migration the first acceptance criterion. Preview experiments belong outside essential daily work.

The ZSoftly team's production experience

We have run Authentik in production for two years on AWS EC2, Amazon EKS and on-premises. We have migrated it repeatedly and experienced no issues during those migrations.

NOVEMBER 2026 SNAPSHOT

Read feature status before planning around it

Documented means described by the vendor without a preview label. It is not an independent general-availability assessment. The table lists what Enterprise adds to the open-source edition [1–5].

Capability	Status / boundary
Privileged access requests (PAM)	Preview [1, 2]
Just-in-time approval and expiry	Preview, part of PAM [1, 2]
Agent accounts for automation	Documented, Authentik API scope [4]
Entra user and group provisioning	Documented, outbound from Authentik [5]
Google Workspace provisioning	Documented [1]
Chrome Enterprise Device Trust	Documented [1]
Fleet integration	Early preview [3]
Windows and Linux local login	Early preview [3]
Scheduled account offboarding	Preview [1, 2]
Enhanced audit records and CSV exports	Documented [1]
Client-certificate authentication (mTLS)	Documented [1]
Shared Signals security-event sharing	Documented [1]
Advanced device compliance	In development [3]
Object Lifecycle: app, group and role reviews	Preview [1]

> **Endpoint limit:** the vendor explicitly advises against production use of the early-preview endpoint feature set, including local login and Fleet integration [3]. Keep those experiments in test environments.

Translate features into requirements

Ask what decision each feature supports. A downloadable report needs a reader and a retention rule. An approval needs a named approver and a response process. Certificate-based authentication needs a plan for issuing, replacing and withdrawing certificates. Buying a feature does not assign those responsibilities.

Record the required version and configuration in the pilot plan. Recheck these statuses before procurement and release. A feature still in development should not be the basis of a delivery commitment.

CONCEPTUAL ARCHITECTURE

The location changes. The operating work remains.

The documented architecture includes server and worker components, PostgreSQL and uploaded files outside the database [15]. The drawing shows logical responsibilities. It does not specify capacity, network exposure or a tested deployment.

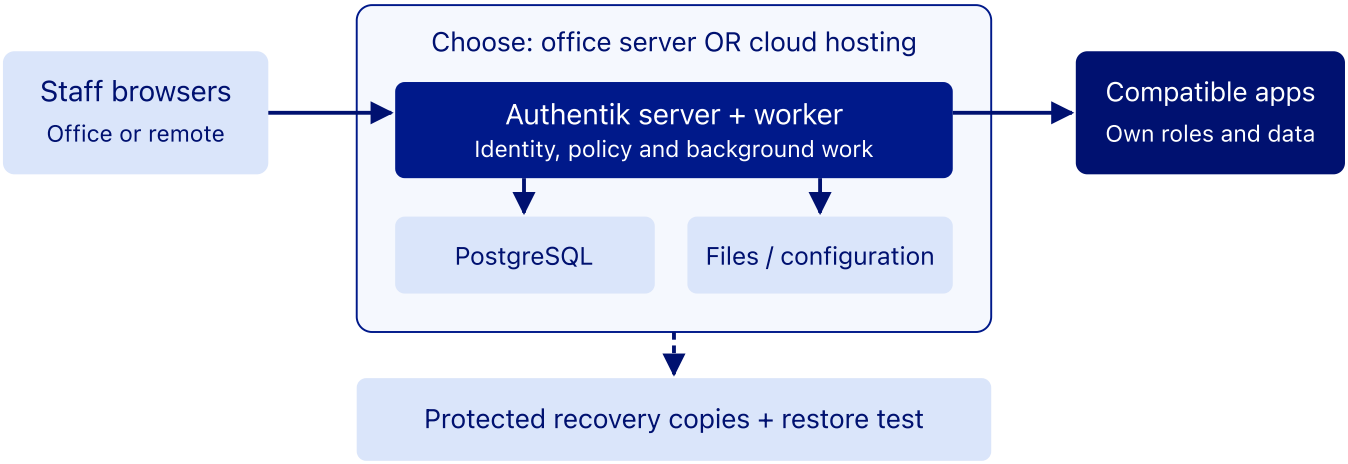


Figure 1. Conceptual choices and dependencies. Each application retains its own data and permissions.

Business owner	Assigned operator
Approves access, retention and support priorities	Configures integrations, monitoring and updates
Chooses location and recovery expectations	Maintains infrastructure and tests restoration
Accepts results and authorises expansion	Records evidence and escalates failures

ZSoftly manages Authentik on a server in your office or on ZSoftly Cloud Platform (ZCP) [14]. For an office server, budget power protection, physical access, hardware replacement and remote support. For cloud hosting, document provider access, connectivity and exit arrangements. Local hosting does not prove offline operation: connected apps, name resolution or other sign-in steps might still need external services.

Availability is a separate design decision

The vendor describes parallel server and worker instances, with database availability handled separately [16]. Decide what outage the business must tolerate before selecting this architecture. Adding application instances alone does not prove recovery from database or site loss.

Ask the delivery team to trace a failed sign-in through the browser, identity service and application. Name the first responder for each boundary. This makes support responsibilities clearer than a general promise to manage the server.

PEOPLE AND AUTOMATION

Test the end of access as carefully as the start

Use the contractor example as a test. PAM approval and expiring access remain preview capabilities [1, 2]. Rehearse them in a separate environment before you rely on them. The sequence below describes acceptance work, not a guaranteed automatic chain.

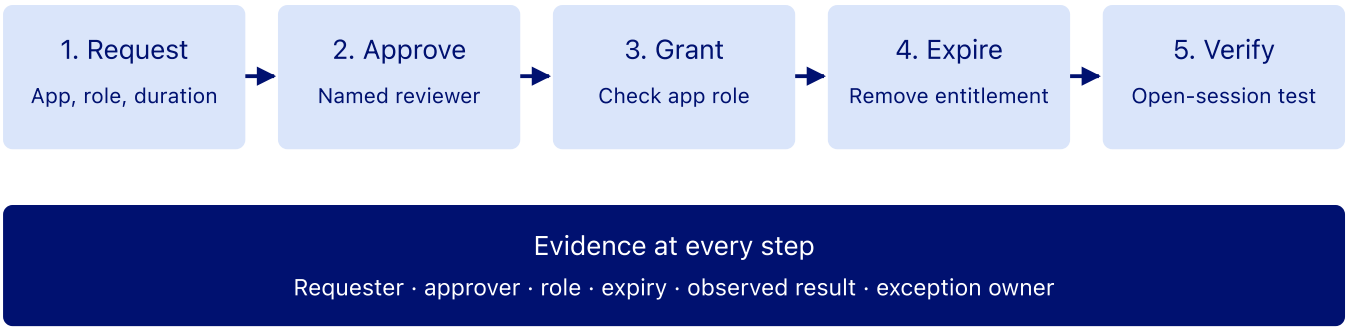


Figure 2. Proposed test sequence. Permission expiry and application-session termination require separate verification.

Separate sign-in from account provisioning

Provisioning creates or updates accounts and groups. Sign-in establishes identity. Record which system owns each field, how a change reaches the application and how failures are detected. A successful first login does not prove a later role change reached every application.

For departures, list local accounts, active sessions, application tokens, group membership and delegated automation. Check a fresh login and an already-open session. Assign a manual removal route when an application lacks the required integration. Do not close the departure task on the strength of one disabled account.

When an approval is delayed, use a named escalation route. Do not let an urgent request quietly become an unreviewed permanent permission.

Machine identities need owners too

Authentik agent accounts call its API for a parent user. Their permissions still govern access. They are distinct from the endpoint Agent, and do not grant an AI assistant general access to business software. Deleting a parent user leaves the agent as a parentless service account [4].

Keep an automation register with purpose, accountable owner, granted permissions, expiry and revocation procedure. Test removal against the actual request the automation performs. Review this register when people change roles, not only when a token expires.

> **Acceptance question:** after the contractor leaves, which attempted actions fail, and where is the evidence? A documented exception needs an owner and a deadline.

MAKE THE DIRECTION EXPLICIT

Choose which directory owns each account

SCIM is a standard way to create and update users and groups across systems. Authentik separates incoming sources from outgoing providers. Its SCIM provider provisions compatible applications alongside their sign-in connection [17, 18]. Draw each direction before enabling synchronisation.

Direction	Documented path
Entra ID → Authentik	Entra provisioning to an Authentik SCIM source [17]
Authentik → Entra ID	Native Enterprise Entra provider [5]
Authentik → compatible SCIM apps	SCIM provider. Static token authentication is open source. OAuth token authentication requires Enterprise [7, 18].
Authentik → Google Workspace	Native Enterprise Google Workspace provider [19]
Google Workspace → Authentik	Authentik documents Google sign-in sources, OAuth and SAML [23]. Google's provisioning app list does not include Authentik [20], so no inbound SCIM route is confirmed.

The native Entra and Google outbound providers are separate from generic SCIM connections [5, 19]. The two Entra directions are separate designs. If you use both, choose one owner for each attribute and decide how to treat changes made in the other system. Keep passwords, application permissions and sign-in sessions in their own verification scope.

Test the account lifecycle

In an isolated pilot, create a user, change their name, change a group and remove access. Check the destination after every operation. Record delay, failed changes and retry behaviour. Include existing-account matching and duplicate identities before connecting a live directory.

For example, test a surname change: it should update the intended account without creating a duplicate or losing application history. Agree the matching rule with the application owner.

Keep cloud permissions in their own scope

Google Workspace provisioning concerns directory identities. Google Cloud IAM determines who is allowed to act on cloud resources [21]. Review resource roles and policies separately. A successful directory sync does not prove that a person has the correct permissions in a cloud project.

> **Before enabling a connection:** agree the source of truth, attributes, access-removal behaviour, failure owner and reversal procedure. Sign-in success and account synchronisation are separate acceptance tests.

CHOOSE BY REQUIREMENT

Replace identity services where requirements match

Authentik can replace a SaaS identity provider for compatible-app single sign-on, multi-factor authentication and account provisioning after the required workflows pass acceptance tests [1, 7, 18]. Evaluate the identity functions you buy from JumpCloud or Entra against those requirements. JumpCloud also includes device management [22], which needs its own plan.

The Entra provider synchronises users and groups from Authentik to Entra ID. Sign-in federation is configured separately [5]. Microsoft 365 still uses Entra ID for its identity model [9]. Connecting another sign-in service does not remove the tenant or establish which licences your organisation still needs.

Existing responsibility	Boundary to preserve
Device and app management	Intune includes enrolment, configuration and updates [10]. Identity checks alone do not deliver that work.
Identity governance	Microsoft Entra ID Governance covers access reviews and lifecycle processes [11]. Compare workflows and evidence individually.
Identity threat detection	Entra ID Protection detects identity risks [12]. Sharing security events is different from producing risk detections.
Application data and work	A new sign-in does not migrate mail, documents, meetings or business records. Plan those separately.

A coexistence worksheet

For each application, record the current identity source, account owner, authentication method, role mapping and departure process. Add one proposed change and a reversal procedure. Keep the existing working route until the new route passes its agreed tests.

Use a separate test population. Check account matching before synchronising records. An email address change, duplicate identity or conflicting group name should have a reviewed handling rule. Filtering a user out of the Entra sync does not disable the Entra account, so test removal directly [5].

Apply the same tests to other candidates, including Keycloak, which documents single sign-on and identity brokering [13]. Compare operating skills and support, alongside functionality.

> **Decision rule:** preserve a required control until its replacement is demonstrated. Mark missing evidence as unresolved. A similar feature name is not proof of equivalent behaviour. Record which services will be replaced, retained or integrated, with a named owner for each decision.

A PROPOSED OPERATING AGREEMENT

Recover the service, then prove access is correct

Authentik's backup guidance makes PostgreSQL essential to recovery. Uploaded files, filesystem certificates, custom templates and blueprints need attention when used [6]. Build the backup inventory around the actual deployment, including protected configuration and external storage where applicable.

A completed backup job is not a demonstrated recovery. Use this checklist as your acceptance standard. Set the frequency and recovery targets with the business. Record actual elapsed time and any manual steps during the exercise.

- ☐ **Restore in isolation.** Recover a recent copy into a separate environment. Prevent accidental messages, provisioning writes or connections to production applications.
- ☐ **Check the records.** Verify users, groups, policy configuration and required files. Compare selected records with the expected state.
- ☐ **Exercise access.** Test an approved user, a denied user and an administrator recovery path. Test recovery when a user loses the phone or security key used for sign-in verification.
- ☐ **Inspect application behaviour.** Confirm roles and sessions after recovery. Identify changes made since the backup that need reconciliation.
- ☐ **Record the result.** Save the backup date, test date, duration, failed checks and corrective owner. Repeat a failed acceptance check after fixing it.

Runbooks should answer practical questions

Who responds when sign-in fails? Who approves an emergency access method? Where is recovery material kept, and who retrieves it if the identity service is unavailable? Rehearse these questions before an incident. Avoid a recovery procedure that depends entirely on the failed sign-in service.

Operating record	What a reviewer should find
Change and update log	Reason, approval, test result, reversal plan and observed result
Access review	Scope, reviewer, exceptions, removals and completion date
Incident and recovery record	Impact, actions, recovered state and follow-up owner

Agree how long to retain these records and who reads them. Protect exports because they contain identity information. Logs and reports support a review, but do not by themselves establish compliance or prove every required control operated.

ILLUSTRATIVE CALCULATION, NOT A QUOTE

Price the licence and the operating work separately

The open-source edition has no software subscription charge. Enterprise is a paid licence. Enterprise Plus includes everything in Enterprise and adds options such as invoice billing, dedicated support with agreed response times, volume discounts and FIPS-compliant deployment [1, 7]. Hosting and implementation are separate purchasing decisions.

Worked annual licence example

Assume 25 workforce accounts and 200 registered customer accounts, using published monthly rates with annual billing checked on 15 November 2026 [7]. Amounts below use the source's dollar symbol. Confirm currency, taxes and current terms in a written quote.

Assumption	Calculation	Annual amount
25 workforce accounts	25 × $5 × 12	$1,500
200 customer accounts	200 × $0.02 × 12	$48
Software only	**Illustrative subtotal**	**$1,548**

Workforce includes employees and business partners. Customer pricing covers registered consumer accounts, not monthly active users or every external user. Agent and service accounts are included. The published Enterprise Plus starting point is $20,000 annually [7].

Ticket-based vendor support requires an Enterprise subscription above US$1,000 per year. Plus support commitments depend on the agreement [8]. Confirm your quote shows the subscription meets this threshold. Vendor tickets do not provide day-to-day operation of your service.

Complete the business cost worksheet

One-time work	Recurring work
Discovery and application assessment	Software licensing and hosting or hardware upkeep
Integration, account reconciliation and testing	Updates, monitoring and application changes
Training, documentation and handover	Backup storage, restore exercises and support

Assign an owner and an estimate to each line. Compare options over the same period, with the same support hours and recovery expectations. Include staff time during transition and the cost of retaining any existing services.

> **Commercial question:** what changes when users, applications or support needs grow? Ask for the charging rule and exclusions. This example establishes arithmetic, not a savings claim or a ZSoftly service price.

A BOUNDED EVALUATION

Expand only after the agreed tests pass

Start with one compatible application and a small group whose normal work is understood. Keep a working alternative during the pilot. Name the sponsor, application owner and operator. Decide in advance which result would stop expansion.

Acceptance gate	Evidence to retain
Identity and permissions	Approved actions succeed. An unauthorised user and a wrong-role user are denied.
Role changes and departure	Updated roles take effect. New and existing sessions follow the agreed removal requirements.
Recovery	A lost sign-in device and administrator lockout have demonstrated recovery paths.
Restore and handover	Required records restore, exports are usable and another authorised operator follows the runbook.
Customer separation	If customer login is included, one customer's users cannot reach another customer's records.
Operational readiness	Named support owner, monitoring route, update process and accepted outstanding issues.

Keep evidence small and useful

Use a test record with the requirement, steps, expected result, observed result and reviewer. Remove personal information and secrets from shared review material. A screenshot of successful sign-in is one observation, not the whole acceptance pack.

If a gate fails, describe the consequence and the owner of the correction. Retest it before accepting the affected scope. If the requirement depends on an early-preview endpoint feature, keep that work in the test environment rather than treating it as a production exception.

What to scope with ZSoftly

ZSoftly's identity service covers assessment, Authentik implementation, integration and managed operations, on a server in your office or on ZSoftly Cloud Platform (ZCP) [14]. An engagement should specify applications, hosting, access rules, recovery tests, support hours, deliverables and exclusions. Define the service around your requirements and the results of your pilot.

> **Bring three things:** your application list, the actions each job role needs and your hosting preference. Start at zsoftly.ca/contact. The first deliverable is a reviewed scope and pilot plan, with named owners after launch.

At the final review, choose expand, revise or retain the current arrangement. Keep the decision and evidence together so the next application starts from a known result.

OFFICIAL DOCUMENTATION

Sources

Checked 15 November 2026. Feature status, prices and support terms change. Recheck before procurement or implementation. Numbered references support vendor facts. Planning worksheets and acceptance gates are proposed guidance.

1. Authentik, Enterprise features. docs.goauthentik.io/enterprise/enterprise-features/
2. Authentik, Release 2026.8. Read with current feature maturity labels in [1]. docs.goauthentik.io/releases/2026.8/
3. Authentik, Endpoint Devices, early preview. docs.goauthentik.io/endpoint-devices/
4. Authentik, Agent accounts, permissions and parent deletion. docs.goauthentik.io/users-sources/user/account-types/agent-accounts/
5. Authentik, Microsoft Entra ID provider. docs.goauthentik.io/add-secure-apps/providers/entra/
6. Authentik, Backup and restore. docs.goauthentik.io/sys-mgmt/ops/backup-restore/
7. Authentik, Pricing and account categories. goauthentik.io/pricing/
8. Authentik, Enterprise support. docs.goauthentik.io/enterprise/enterprise-support/
9. Microsoft, Determine your cloud identity model. learn.microsoft.com/en-us/microsoft-365/enterprise/deploy-identity-solution-identity-model
10. Microsoft, What is Intune? learn.microsoft.com/en-us/intune/fundamentals/what-is-intune
11. Microsoft, Entra ID Governance overview. learn.microsoft.com/en-us/entra/id-governance/identity-governance-overview
12. Microsoft, Entra ID Protection overview. learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection
13. Keycloak, project capabilities. www.keycloak.org/
14. ZSoftly, Identity management services. zsoftly.ca/professional-services/identity/
15. Authentik, Architecture. docs.goauthentik.io/core/architecture/
16. Authentik, High availability. docs.goauthentik.io/install-config/high-availability/
17. Authentik, Entra ID SCIM provisioning. docs.goauthentik.io/users-sources/sources/social-logins/entra-id/scim/
18. Authentik, SCIM provider and authentication modes. docs.goauthentik.io/add-secure-apps/providers/scim/
19. Authentik, Google Workspace provider. docs.goauthentik.io/add-secure-apps/providers/gws/
20. Google Workspace, automated provisioning catalogue. support.google.com/a/topic/10018788?hl=en
21. Google Cloud, IAM overview. docs.cloud.google.com/iam/docs/overview
22. JumpCloud, platform and device-management scope. jumpcloud.com/platform
23. Authentik, Google sign-in sources. docs.goauthentik.io/users-sources/sources/social-logins/google/

> **Version 1.0.** Our production experience is first-hand. The contractor scenario is illustrative, and diagrams are conceptual. Product documentation and our experience inform planning. Acceptance still depends on tests in your environment.