Identity & Access

IdP integration, SSO, SCIM provisioning, admin access paths, least-privilege model

- Chapter 9 — Identity & Access

Chapter 9 — Identity & Access

9.1 Current State and Scope

As of 2026-07-18 **no IdP integration exists**: Grafana and BookStack run on local admin accounts (both credentials exposed in the changelog — item 15 applies), the platform application is pre-deployment, and host access is the shared-key nonconformance of §2.5. This chapter defines the target identity architecture covering the IAM control family: IAM-01 (identity-aware proxy), IAM-02 (SSO federation), IAM-03 (phishing-resistant MFA), IAM-04 (tenant separation), IAM-05 (SCIM lifecycle), IAM-06 (access reviews). Human identity only — machine/agent credentials are Chapter 8; per-Compartment application RBAC internals (APP-05) are application-layer and specified in the platform application documentation, but their identity *source* is defined here.

9.2 Identity Provider

Single source of truth: SBS's corporate IdP. The Platform maintains **no local user store** — no local passwords on any surface (the two as-built local admins are migrated then reduced to break-glass, §9.6). Users exist on the Platform only as federated identities projected from the SBS directory.

Discovery dependency (blocking): SBS's incumbent IdP product (Entra ID, Okta, Google Workspace, or other) is unconfirmed — it is a named LH-SBS-DISC-002 IT-function question and a gate for this chapter's build items. The architecture below is written IdP-agnostic against capabilities every mainstream enterprise IdP provides: OIDC, SAML 2.0, SCIM 2.0, group claims, WebAuthn/FIDO2 MFA enforcement. Nelson Santos is execution owner for the IdP-side configuration (app registrations, group creation, SCIM token issuance).

Federation protocol: OIDC (Authorization Code + PKCE) everywhere it is supported — Grafana (native OIDC), the platform application (OIDC middleware), the identity-aware proxy (§9.3). SAML only where a component supports nothing better. Token hygiene: short-lived access tokens (≤1 h), refresh handled server-side, `email_verified` + group claims required in the ID token.

MFA (IAM-03): enforced **at the IdP**, not per-application — phishing-resistant methods only (WebAuthn/FIDO2 hardware or platform authenticators) for all Platform-mapped groups; TOTP acceptable *only* as a documented exception with expiry; SMS/voice prohibited. Conditional-access (where the IdP supports it): Platform app registrations require MFA on every authentication, no "remembered device" exceeding 12 h for admin roles.

9.3 Identity-Aware Proxy (IAM-01)

Enforcement point for surfaces that lack robust native OIDC or need pre-application gating. Implementation: **oauth2-proxy** deployed alongside nginx on the serving droplet, wired via `auth_request`:

Surface	Enforcement
`monitor.sbsdash.com`	Grafana native OIDC (preferred — it maps groups→roles internally, §9.5). oauth2-proxy not required
`wiki.sbsdash.com`	BookStack SAML/OIDC if licensed features suffice; else oauth2-proxy in front — **no unauthenticated byte** beyond the IdP redirect is served
`admin.sbsdash.com`	oauth2-proxy **in addition to** application auth — admin surface requires valid IdP session *before* the application sees the request, layered on the §5.7 edge IP allowlist
`sbsdash.com`, `clients.`	Application-native OIDC; anonymous access limited to the sign-in redirect itself (FE posture: the public fingerprint is a sign-in page, §5.5)

oauth2-proxy session cookies: `__Host-` prefix, `Secure`, `HttpOnly`, `SameSite=Lax`, secret from Vault (`secret/platform/`), session lifetime ≤ 8 h with IdP re-auth. The proxy passes identity to upstreams via signed headers; upstreams **reject unsigned/absent identity headers** so the proxy cannot be bypassed by direct container access (pairs with the `net-edge` design, §6.4).

9.4 SCIM Provisioning (IAM-05)

Lifecycle automation — the control that makes offboarding real:

- **Direction:** IdP → Platform. SBS directory group membership drives Platform access; the Platform never invites users directly.
- **Targets:** the platform application (SCIM 2.0 endpoint, Compartment-role mapping per §9.5) and Grafana (SCIM or team-sync per licensing; fallback is OIDC group-claim mapping at login — acceptable because login-time mapping plus short sessions bounds staleness to the session length).
- **Deprovisioning SLA:** IdP deactivation propagates to Platform deactivation **within 15 minutes** (SCIM push) and in the worst case at next token expiry (≤ 1 h). A user disabled in the SBS directory holds no live Platform session beyond that hour — this is the tested metric, not the config's existence.
- **SCIM tokens** live in Vault (`secret/platform/scim/`), rotate on the 90-day static schedule (§8.4), and their use is logged (MON-01).
- Joiner/mover/leaver flows are exercised end-to-end as a named gate: create test user → group add → verify access; group move → verify role change; deactivate → verify lockout inside SLA.

9.5 Least-Privilege Model and Group Mapping (IAM-04 / APP-05 boundary)

Access is **group-derived, never user-granted**. SBS directory groups map to Platform roles; the group list is the single audit surface for IAM-06:

Directory group (naming)	Grants
`dash-platform-admin`	Master Admin console; oauth2-proxy admission to `admin.sbsdash.com`. Named individuals only, target ≤ 4
`dash-c01-user` … `dash-c10-user`	That Compartment's surfaces and workflows — the human half of IAM-04 tenant separation, mirroring the network/data/secrets walls (§6.4, §7.4, §8.3)
`dash-c01-supervisor` …	Receives that Compartment's Medium/High/Critical routings from Supervisor Agents; resolution authority
`dash-monitor-view` / `dash-monitor-admin`	Grafana Viewer / Admin via group-claim mapping
`dash-wiki-edit` / `dash-wiki-view`	BookStack roles
`dash-exec-dashboard`	COO/CFO read-only reporting views

Rules: no wildcard "all-Compartments" user group exists — cross-Compartment humans (e.g., the COO) hold the exec-dashboard role, which reads *reporting outputs*, not Compartment interiors; platform-admin grants administration, and its members' actions are fully logged (MON-01) — admin ≠ unobserved. Group membership changes are IdP-audited events; the quarterly IAM-06 access review walks every `dash-*` group against current staffing (Alexandra Del Rey coordinates sign-off; Nelson Santos executes directory changes), and the review artifact is filed in the wiki with date and reviewer — access certification (MON-04) consumes the same artifact.

9.6 Admin Access Paths

Consolidated statement of every privileged path and its chain, replacing ad-hoc practice:

Path	Chain	Controls
Web admin	IdP (MFA) → oauth2-proxy → edge IP allowlist (§5.7) → `admin.sbsdash.com`	IAM-01/02/03; all actions app-logged
Host SSH	Operator (personal key) → bastion `monitor-servers` → target droplet	Per-person users post item 17; bastion sessions logged; admin allowlist IaC-managed (§3.5)
Vault admin	Bastion → named admin token under `policy-admin`	§8.2; every operation in Vault audit device
DO console / registrar / DNS	Provider MFA (phishing-resistant), SBS-owned accounts	§2.1, §4.1; console use in Prod is break-glass + logged (§2.2.3)
Break-glass	Sealed local credentials for Grafana/BookStack/app, stored in Vault + one printed copy in SBS-controlled physical custody	Used only on IdP outage; use triggers immediate rotation + incident note (MON-05); tested annually

The break-glass row is the honest residual of the "no local accounts" rule: total IdP outage must not equal total platform lockout, so exactly one dormant local admin per critical surface survives — vaulted, alarmed on use, rotated after.

9.7 Verification

Gates (LH-SBS-INST-001): unauthenticated request to every gated surface yields IdP redirect, zero application bytes (curl sweep); direct-to-container bypass attempt rejected (unsigned identity header); MFA challenge presented on fresh session for admin group (manual gate); SCIM lifecycle test — provision/move/deactivate with deactivation lockout ≤ 15 min (timed); group-mapping probe — `dash-c03-user` reaches c03 surfaces, denied on c08 (IAM-04 human-layer test mirroring §7.7); local password login disabled on Grafana/BookStack (negative login test); break-glass procedure executed in drill, rotation confirmed; IAM-06 review artifact exists with current date.