**OPS-10 — SSO/SAML & SCIM (Enterprise Access)**

**Intent**  
Enable enterprise SSO and automated user lifecycle: **login**, **role mapping**, **de-provision** in minutes.

**Preconditions**

* Role model (Viewer/Operator/Reviewer/Approver/Admin).
* IdP choices (Okta/AzureAD/Google).

**Flow**

1. **SAML SSO**: configure metadata exchange; enforce signed assertions; bind to tenant.
2. **Attribute mapping**: IdP groups → product roles; deny on missing mapping.
3. **MFA enforcement**: require IdP MFA claim.
4. **SCIM 2.0**: provision/de-provision users & groups; map to roles; soft-delete then hard-delete via retention.
5. **Just-in-Time (JIT)**: first login creates user shell with least privilege if SCIM absent.
6. **Audit**: log SSO logins, SCIM changes, role grants.

**Edge cases**

* Orphaned admins → periodic report & auto-revoke.
* Role drift (IdP vs app) → app is read-only; IdP wins.

**Done when**

* SSO works for target IdPs; SCIM removes users ≤15 min; role mapping tested; audit entries visible.