

PC-SAMPLE-ACC-01 / EN / V1.1

Secure access design and rollout

ILLUSTRATIVE SAMPLE • FICTIONAL SCENARIO

PREPARED FOR
PREPARED

Orivane Industrial Group
2026-08-07

Access design and business needs

This report presents an original fictional scenario. Orivane, its people, suppliers, systems, records and results are invented; established technology names identify the example stack only. No client material was used. Example hostnames use the reserved .example domain.

Orivane Industrial Group has 2,400 staff, 180 external partners and 36 internal applications. Sofia Caron owns the Nacre Access rollout under ACC-2608. The design gives each user access to approved applications instead of the wider internal network. Teams must be able to work reliably from all locations, partners must stay within their approved services, and operations must have a recovery procedure if identity or access services fail.

Access is approved for a specific application and task. The gateway checks who the user is, whether their device meets the policy and whether their session is valid. The application then checks its own permissions. Passing the gateway does not give the user permission to perform every action.

CONSTRAINT	DESIGN RESPONSE
Legacy protocols	Publish a bounded connector path for approved services; retain a narrow network path only where application mediation cannot work.
Partner devices	Separate partner resources and sessions; do not infer staff-equivalent access from a valid external identity.
Administration	Use a distinct privileged identity and device requirement; ordinary collaboration sessions carry no administrative rights.
Availability	Deploy connectors across independent failure domains and test the policy decision service as a separate dependency.

Success means the required work can be done through a documented, observable path while unrelated resources remain inaccessible. It does not mean every application must use the same connector or every failure should result in an unrestricted fallback.

Services and agreed access rules

The 7 August register ACC-036 identifies all 36 applications. Orivane ID supplies workforce identity; the Nacre Access policy service evaluates application access. The six connectors acc-mtl-01/02, acc-iad-01/02 and acc-dub-01/02 serve Montréal, Ashburn and Dublin. Each pair occupies separate failure domains.

RESOURCE	ACCESS RULES
LedgerFlow / Tessa Lin	orders.orivane.example; HTTPS 443; group LF-OrderOps; managed staff devices. Eight-hour session, 15-minute idle timeout, revocation target five minutes.
Partspan / Samir Okafor	partners.orivane.example; HTTPS 443; group PS-Suppliers. Neralis Automation partner sponsorship expires 30 September; no internal DNS discovery.
ToolVault / Amira Chen	git.orivane.example; HTTPS 443 and scoped SSH 22. Engineering repositories only; release actions use a separate workload identity.
MillWatch / Marc Bellamy	millwatch.orivane.example; TCP 8443 through acc-mtl-02. Exception EX-019 allows 20 plant operators until 30 September.
Privileged access	Amira Chen uses a.chen-admin from managed device ORV-LT-0421. Fresh authentication within 15 minutes; target nacre-admin; session maximum 30 minutes.

Policy baseline and support

Policy access-2.3 fixes device-signal freshness at five minutes and rejects missing signals for internal data. Lucien Armand of Neralis Automation may view his supplier orders in Partspan from an unmanaged browser after strong authentication; exports and other suppliers' records remain denied. Sofia Caron approves membership; Maya Dufresne reviews exceptions. The Orivane desk queues ACC-DENY incidents for Julien Voss.

Resource inventory and policy ownership

RESOURCE CLASS	COUNT	POLICY OWNER
Business web applications	20	Business owner defines roles and approves partner access.
Engineering services	8	Engineering owner defines repository and build-system actions.
Administrative consoles	5	Security and system owner approve privileged operations jointly.
Legacy services	3	Service owner documents protocol limits and the compensating boundary.

The inventory totals 36 applications. ACC-036 records hostname, classification, protocol, population, owner, connector, dependencies and recovery procedure for every entry. These fields form the migration contract. An application with unknown ownership stays outside the production rollout.

Policy change is an application change

Access policy is versioned with a review record. The requester describes the business action, affected population and expiry; the resource owner approves the entitlement; platform security checks the boundary. A broad group name such as “all employees” is not evidence that every member needs the resource.

Partner sponsorship is time-bound. The sponsoring owner reviews both group membership and application roles when a contract ends. Removing a gateway entitlement does not remove application-local tokens; those credentials belong in the same offboarding checklist.

Access decisions and revocation

Identity, entitlement and required device context determine access to a named resource. The application then checks the requested action against its own permissions. Each refusal returns a useful reason; neither gate may silently broaden access when an input is missing.

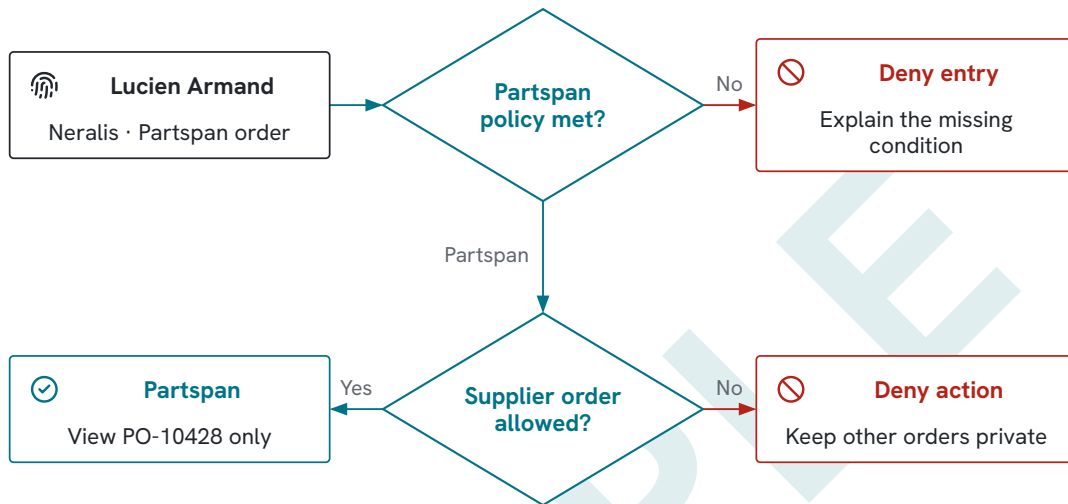


Figure 1 Two checks: application access, then permission to act.

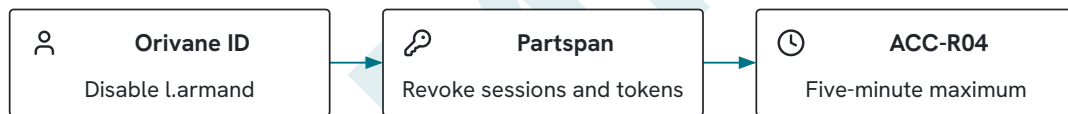


Figure 2 Revocation must reach downstream sessions and credentials.

Required acceptance evidence

- ✓ A permitted business task succeeds while unrelated resources remain denied.
- ✓ A disabled user cannot start new access; existing sessions are timed and reconciled.
- ✓ Connector or identity failure does not reopen the previous broad access path.

Decision flow and policy matrix

A request is bound to a verified identity, a resource and an intended action. The decision service evaluates current entitlement and required context. The gateway forwards traffic only to the approved application. The application then evaluates its own role and object permissions. Correlation identifiers join these events without copying session credentials into logs.

PERSONA	REQUIRED CONTEXT	PERMITTED ACCESS
Mila Renaud / staff	Approved group, strong authentication and managed device for internal data.	Named business applications and their own application role.
Lucien Armand / Neralis	Active sponsor, expiring entitlement, approved authentication and resource-specific device rule.	Partner workspace only; no discovery of internal services.
Amira Chen / admin	Separate privileged identity, approved device, fresh authentication and change context.	Named management plane; no implicit data-reader role.
ledgerflow-release	Workload-bound credential, explicit audience and least-privilege action.	One service interface; no interactive workforce access.
Elias Moreno / recovery	Independent approved identity, narrow target and recorded authorization.	Recovery actions for the affected dependency only.

Unknown is not compliant

A missing, stale or contradictory device signal does not satisfy a managed-device rule. The policy specifies which resources may operate with limited context and for how long. Sensitive administration fails closed when required evidence is unavailable. A business exception uses a narrower resource path with an expiry; it does not mark an unknown device healthy.

Session, revocation and dependency failures

Removing access requires action in several systems. Disabling a user account can stop new sign-ins while existing application sessions or service tokens still work. ACC-R04 measures revocation at Nacre Access and the application: five minutes for LedgerFlow and Partspan, 60 seconds for nacre-admin. MillWatch cannot revoke active sessions; EX-019 requires connector termination within ten minutes.

FAILURE OR EVENT	REQUIRED BEHAVIOR
User disabled	Deny new decisions; terminate sessions where supported; expire or revoke downstream credentials. Measure the remaining exposure window per application.
Device becomes noncompliant	Reevaluate resource access at the supported enforcement boundary; prove what happens to already-open connections.
Connector lost	Route only through a healthy authorized connector; preserve destination limits and record the failed path.
Policy service unavailable	Deny sensitive new access. Cached low-risk PolicyShelf decisions expire after 60 seconds; privileged decisions are never cached.
Identity provider outage	Use the independent recovery route for restoration work; do not publish unrestricted network access.

Recovery access

Recovery credentials are stored and exercised outside the normal sign-in dependency. Their use generates a notification through an independent channel, has a named authorizer and ends with credential renewal and review. The runbook includes failure of DNS, time synchronization and certificate renewal, because an available connector alone does not make an application reachable.

Rollout groups and transition period

Migrate by application dependency and user role, not by switching the whole workforce on a single date. A pilot must include a partner, an administrator, an unmanaged-device denial and an offboarding exercise. A pilot consisting only of platform engineers would miss the operating conditions the design is intended to handle.

ROLLOUT GROUP	ENTRY AND EXIT CRITERIA
10 Aug / Montréal	120 staff and 20 Neralis partners; PolicyShelf, ShiftBoard, FieldNotes and Partspan. Sofia Caron accepts A1-A7 before expansion.
17 Aug / Regional services	1,680 staff and 160 partners; the other 16 web applications. Julien Voss confirms support readiness; task success must exceed 99% in the five-day observation.
24 Aug / Nacre engineering	580 staff; eight engineering services and five consoles. Amira Chen proves privileged separation and long-running sessions.
31 Aug / Plant integration	20 staff; MillWatch, BatchTrace Bridge and ForgeLink. Marc Bellamy owns EX-019-021; final route retirement is due 30 September.

The old path must close

Coexistence has an expiry and a per-application owner. Leaving the old broad path available indefinitely would allow users to avoid the new policy. Before closure, capture usage and identify unmodeled dependencies. After closure, test that the old hostname, address and protocol path no longer admit traffic. Rollback restores only the previous approved boundary and is time-limited.

Acceptance test catalogue

TEST	EXERCISE	EVIDENCE REQUIRED
A1	Mila Renaud creates LedgerFlow order LF-260810-17.	Gateway decision and application action correlate; unrelated resources remain denied.
A2	Lucien Armand attempts nacre-admin discovery from Partspan.	Named partner service works; internal names and destinations provide no broader access.
A3	Approved user uses an unknown device.	Sensitive resource refuses access with a useful reason; support can diagnose without overriding policy.
A4	Disable l.armand during a live Partspan session.	New access stops; existing sessions and tokens are measured against the application-specific revocation objective.
A5	Stop acc-mtl-01, then isolate the Nacre Access policy service.	Observed behavior matches the failure matrix; no unrestricted alternate route appears.
A6	Exercise privileged and service identities.	Workforce token cannot become a privileged or workload credential; actions remain narrowly scoped.
A7	Restore the identity dependency.	Independent recovery access works, is logged, and is closed and reviewed afterward.

Retain the policy version, resource, persona, device state, timestamp and expected versus observed decision for each test. Logs contain decision reasons and correlation identifiers, not raw authentication tokens or unnecessary personal data. A failed business task is investigated at both the gateway and application layers.

Operating model and design limits

The service desk owns enrollment assistance and first-line interpretation of denial reasons. Resource owners approve entitlements; security owns policy exceptions; the platform team owns connectors and decision-service health. Changes that cross these responsibilities need joint review rather than an informal emergency group assignment.

The operational dashboard should distinguish unavailable applications, failed authentication, denied authorization and unhealthy connectors. A high denial rate may be a correct control response or a broken rollout. Interpret it against affected resources and completed business tasks before weakening a rule.

Decisions still required before implementation

- Sofia Caron must attach ACC-R04 timing results by 10 August; the approved targets are five minutes for business apps and 60 seconds for privileged access.
- Samir Okafor must approve the Partspan view-only partner role; unmanaged devices cannot export records or reach LedgerFlow.
- Nadia Bellerose accepts suspension of new administrative work during an Orivane ID outage; Elias Moreno may authorize the independent recovery route.
- Marc Bellamy closes EX-019-021 on 30 September after MillWatch, BatchTrace Bridge and ForgeLink pass connector-termination tests.

Reference and residual risk

[NIST SP 800-207](#) informs the separation of resource authorization from network location. This design does not make a compromised approved device harmless, repair application authorization defects, or guarantee immediate session revocation. Those limits remain visible in acceptance and incident procedures. All populations and design choices here are fictional.