

Navynt Tenant Authority Guide

Assign business permissions and configure accountable approvals

Version 1.0 · 4 October 2026

This guide explains how workspace administrators assign business, security and recovery authority. It accompanies the tenant authority changes prepared for this release. Deployment and verification status are recorded separately.

Use the setup checklist before inviting users and whenever responsibilities change. Management is a broad company-wide role; use targeted layer permissions for department staff. Approval and payment require distinct people for incentives.

In this guide

- How access is decided
- Roles and special responsibilities
- Recommended department setup
- Buying permissions
- Approval practice
- Incentive approval and payment
- Security and emergency recovery
- Review and onboarding checklist
- Standards basis and limits

Design basis: OWASP authorization guidance and NIST AC-5/AC-6. This document is not a certification.

How access is decided

Access requires an active authenticated login in the correct tenant, an allowed action, access to the relevant record, the appropriate subscription/module entitlement, and a valid workflow state. Field permissions further limit accessible fields. A job title or a visible menu alone never authorizes a write.

Roles, organizational position, business permissions and record scope are separate. A layer's permissions apply to people on that layer. Tenant Admin and Management have fixed business permissions; Technical Owner has fixed technical permissions. Other internal users resolve their action rights through their hierarchy layer, with legacy fallbacks where no hierarchy exists.

Permission grants do not generally expand record scope. Explicit exceptions are documented: buying grants expose the supplier master; Procurement Approval exposes the procurement review queue; Mark Paid exposes claimed, paid and reconciled incentives for finance. Those grants do not give access to unrelated opportunities or accounts.

Roles and special responsibilities

Assignment	Suitable use	Boundary
Tenant Admin	Workspace setup, business configuration and people administration	Security operations require Security Owner once owners are designated
Management	Executives requiring company-wide business visibility and broad commercial authority	Do not assign merely because someone manages a department
Team Lead	People leading a reporting branch	Layer permissions and department-aware reporting scope apply
Standard User	Sales, Finance, Procurement or Operations contributors	Grant the precise actions required on their layer; keep unrelated actions off
Technical Owner	Assigned technical work	No automatic Products, buying or commercial approval authority
Partner user	A partner organization's portal	Only portal-safe records associated with that partner
Security Owner	Tenant security governance	A named principal independent of the business login role
Permission Manager	Field rules and layer permission configuration	Delegated capability, not a separate login role; only Security Owner may delegate it
Fixed Admin	Emergency recovery	Optional named recovery principal; does not acquire routine security or business authority

Recommended department setup

Management remains broad by design. Prefer Standard User with targeted layer grants for Finance or Procurement. A Security Owner can have an ordinary business role without receiving Management's company-wide commercial powers. Assigning separate responsibilities to separate people is a recommended tenant practice; the application does not automatically prohibit a person from holding multiple designations.

Create departments that represent actual business functions, then assign layers, managers and territories. For example, use Sales as the department and North/South as regions or reporting branches. Team Leads and their reports need the same department ID for department-scoped team access. Moving a person between layers may change their actions as well as their reporting scope; review both.

Use a Procurement contributor layer for purchase submission and vendor documents. Use separate Operations and Finance approval layers. A Finance payment recorder needs Mark Paid, not incentive approval or company-wide Management merely to record a payment. Invoice collection remains limited by linked account/deal scope or named collector access.

Buying permissions

In Organization Hierarchy, a Permission Manager can select Default role behavior, Allow or Deny for each buying permission. Explicit buying grants are available to hierarchy-backed Standard Users and Team Leads. Technical Owner retains its fixed technical map.

Permission	Allows	Does not imply
Vendors	Create and edit supplier records	Procurement approval or record deletion
Submit procurement	Create purchase requests and use the supplier master	Approving requests or changing supplier records
Approve procurement	Review the procurement queue and act on an eligible approval step	Self-approval, vendor editing, or an unrestricted departmental step
Vendor quotes and purchase orders	Prepare and progress vendor documents within their record scope	Procurement approval or editing an issued PO
Delete	With the relevant buying grant, delete an eligible inactive vendor, received/withdrawn quote or draft vendor PO	Deleting issued POs or bypassing record scope

Default business access is retained for Tenant Admin and Management. Editing Team Leads retain their existing buying defaults unless explicitly denied; their procurement approval default is retained only where the layer already grants administrative tools. Ordinary editing, technical work, or incentive approval does not grant buying rights to Standard Users or Technical Owners.

Buying features also require the appropriate plan entitlement. An explicit permission cannot unlock a feature excluded by the subscription.

Approval practice

Tenant Admin configures Approval Rules. Matching rules apply to internal and partner portal submissions; partner registration drafts receive their rule when submitted. Select an entity and threshold, then add steps using dropdowns for Role, Department, Named person, Tenant Admin or Management, or Configured delegate. Each actor still needs the underlying business approval permission and record access.

Role steps match the selected login role. A role can be restricted to a department. Department steps require a person in that department; named-person steps require that exact tenant login. Administrator status does not bypass these restrictions. Step labels describe the business purpose but do not confer authority.

New rules default to a different person at each approval step. Existing rules retain their distinct-person setting until reviewed. The same requester cannot approve or reject their own submission. Review every legacy rule, including existing in-progress approval states, before claiming department-specific or distinct-person enforcement for that workflow.

Set an optional escalation time and role. An escalation role has no authority until the SLA processor marks the step escalated. Department and named-person restrictions still apply after escalation. An escalation within a named-person step does not appoint a substitute person; choose an appropriate department/role step when substitution is required.

Example: a Procurement contributor submits a purchase request. Step one selects Operations; step two selects Finance; different-person enforcement is enabled. Operations and Finance approvers have Procurement Approval, belong to the selected departments and are different people. The requester cannot act on either step.

Incentive approval and payment

The sequence is request, approval, claim with uploaded evidence, payment recorded, then reconciliation. Mark Paid records a payment reference; Navynt does not transfer funds.

The requester and every person who approved the incentive are prohibited from recording its payment, including users with Tenant Admin or Management roles. A different login with Mark Paid must record it. New approval and payment records retain canonical login usernames; legacy approvals use their retained display-name history when no username exists. Missing attributable approval blocks payment and needs review, not a fabricated approver.

This control also applies to existing unpaid claims after release. Previously paid records are preserved. Keep at least two eligible people for approval/payment, and three where two distinct approval steps are required before payment. Reconciliation uses its existing Mark Paid gate; a separate reconciler is recommended but is not newly enforced by this release.

Security and emergency recovery

Designate at least one Security Owner and recommend a second active owner for continuity. While the owner list is empty, Tenant Admin has transitional security authority. Once configured, the final Security Owner cannot be removed; use an atomic transfer. Security Owner governs SSO, keys/webhooks, audit, sessions and other classified tenant security operations, subject to plan availability.

Security Owner or an authorized Fixed Admin can perform the relevant recovery operation; two simultaneous approvals are not required. Fixed Admin is optional, has a closed recovery allowlist and never inherits routine permission management. Keep MFA and recovery procedures reviewed for privileged users.

Tenant Security Owner is different from Navynt's platform operator. The separately deferred Cloudflare Access operator setup is not enabled by these tenant authority changes.

Review and onboarding checklist

1. Confirm who needs company-wide Management access; use targeted layers for other functions.
2. Assign active departments, layers and managers; check peer-branch isolation.
3. Select buying permissions explicitly and review supplier/approval-queue visibility.
4. Set departmental or named approvers and verify their underlying approval grant.
5. Confirm enough distinct people can complete approval and payment.
6. Designate Security Owners and document optional emergency recovery.
7. Test menus, direct links and API actions with Admin, Management, two Team Leads, a Standard User, Technical Owner and partner users.
8. Repeat checks after promotions, department transfers, role changes and departures. Review privileged assignments at least quarterly and after material changes; this cadence is a recommended tenant policy.
9. Record approval evidence and review audit events using authorized Security Owner access.

Standards basis and limits

The practice follows OWASP recommendations for least privilege, deny-by-default authorization, relationship/attribute-based decisions and checks on every request. NIST SP 800-53 AC-5 and AC-6 inform separation of duties and least privilege. These are design references; this guide is not a certification or a claim that all NIST controls have been implemented.

- https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html
- <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>

Customer onboarding is not a substitute for testing the application. Approval and buying controls in this release are covered by local security and workflow regression tests. Tenant assignments, real production configurations and the separately deferred platform operator gate require their own review.