Workspace & Project Permissions Guide

How roles, menu access and project permissions work together in Deep Space

Deep Space Horizon · October 2026

1. How access works — the two layers

Deep Space controls what each person can do with **two layers** that work together:

Layer	What it controls	Where it is managed
Workspace role	Which modules and pages appear in a person's menu — what they can *open* across the whole workspace.	**Admin** → **Security** (the Roles page)
Project permissions	What a person can *do inside each project* — viewing, contributing, managing the project, and accessing cost data.	**User Directory** → **Manage Project Access**, and each project's **Team** tab

A person typically needs both: a workspace role so the module shows in their menu, and project permissions on the projects they work on. For example, someone may see the *Budget Register* menu item through their role, but they will only work with the projects where they hold project permissions.

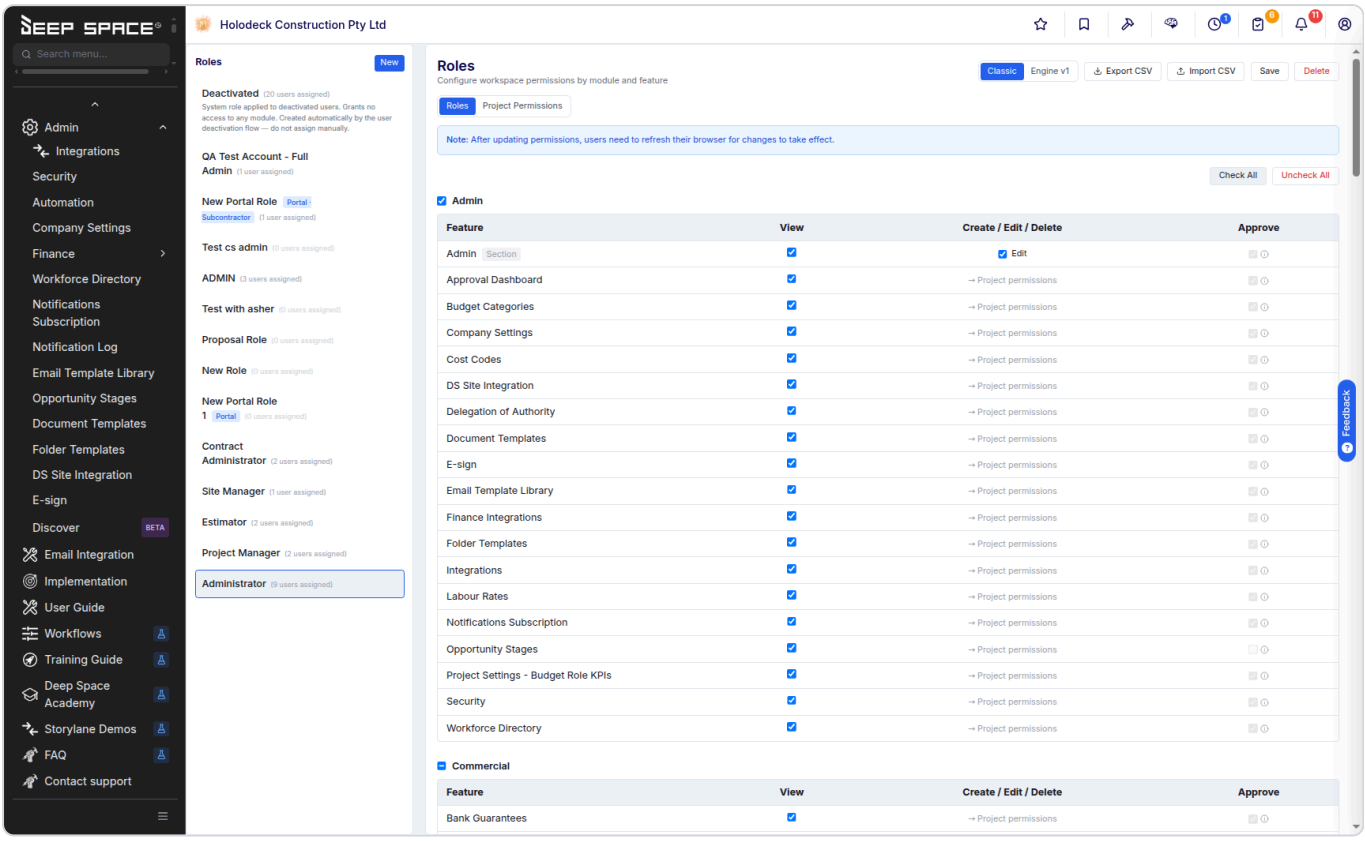
2. Workspace roles — the Security page

Open **Admin** → **Security**. Every workspace member is assigned one role, and the role defines their menu.

- **Roles list (left):** each role shows how many users are assigned — hover to see who. Renaming is instant via the pencil. Deleting a role with assigned users first asks you to switch those users to another role so nobody loses access.
- **View column:** the tick that matters for menus. A ticked *View* means the menu item is visible and the page can be opened by people with this role.
- **Create / Edit / Delete column:** these actions are governed by each member's *project permissions*, not by the role — the column links straight to the *Project Permissions* tab so you can see real access per person. The one exception is the *Admin* row's **Edit** tick, which allows editing workspace-level *Company Settings*.
- **Approve column:** approvals are configured in **Delegation of Authority** for supported entity types — the *(i)* beside each Approve cell is a reminder (see section 6).

- **Export / Import CSV:** download the full permission matrix, edit it in Excel and re-import — changes are previewed before anything is saved. Useful for bulk role setups.

> **Note:** after changing a role's permissions, affected users need to refresh their browser for the change to take effect.



The Security page (Classic view): role list on the left; per-module matrix with View ticks, the combined Create / Edit / Delete column pointing at Project Permissions, and the Approve column's Delegation of Authority reminder.

3. The four project permissions

Inside every project, access is controlled by four permissions held per person, per project:

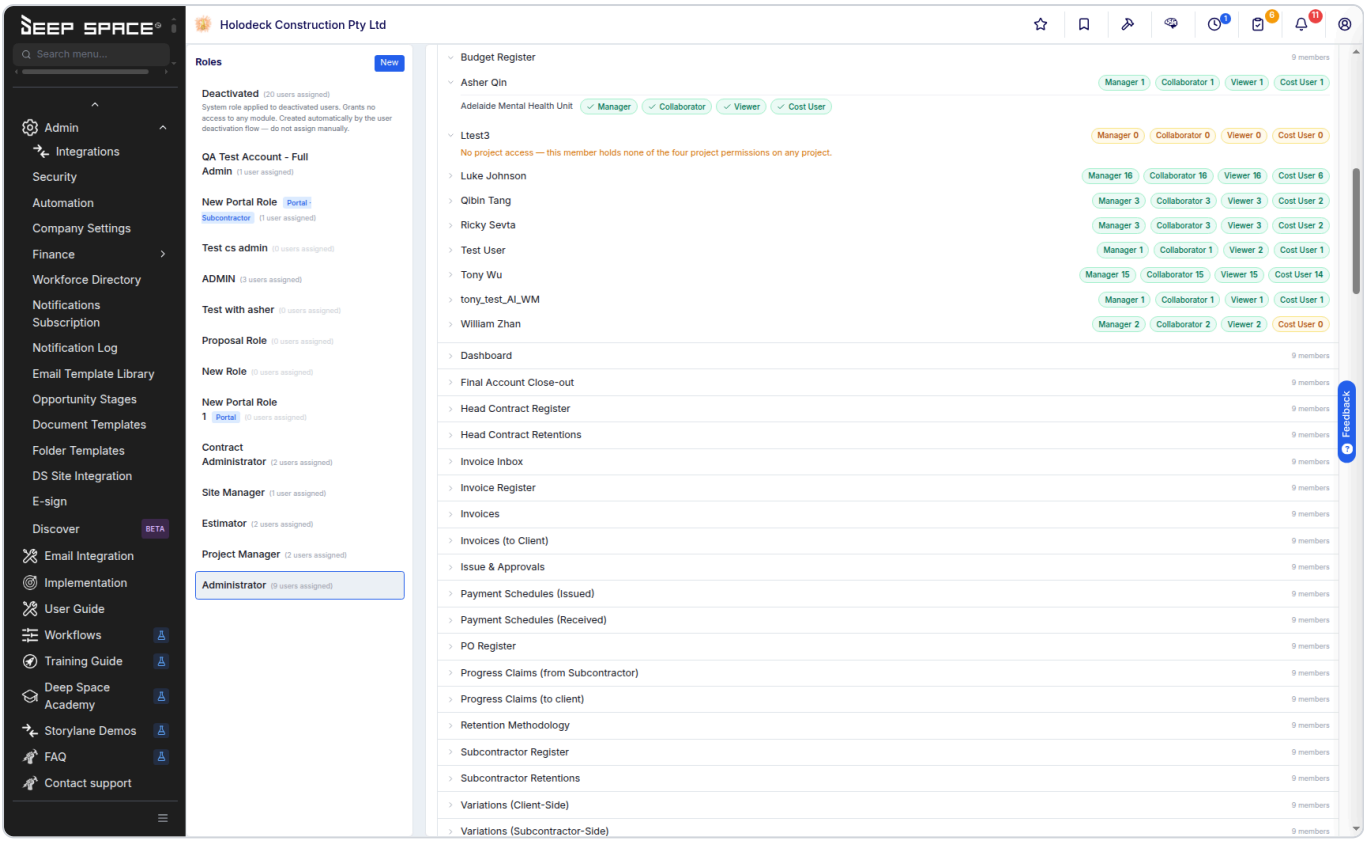
Permission	What it grants
Viewer	See the project — open its pages, registers and documents. The starting point for anyone added to a project.
Collaborator	Contribute to the project — create and edit project records in the modules their role shows.
Manager	Run the project — full control including managing the project team and settings. Manager always includes Viewer and Collaborator.
Cost User	Access the project's commercial data — budgets, subcontracts, claims and invoices. Kept separate so financial data can be limited to the right people.

The first three build on each other (view → collaborate → manage). *Cost User* is independent, so you can give someone full delivery control without exposing commercial data — or cost access without project management rights.

4. Seeing real access — the Project Permissions tab

On the Security page, switch to the **Project Permissions** tab to see the access a role's members actually hold:

- Select a role, then expand any menu item the role can see. Every assigned member is listed with a count of their **Manager · Collaborator · Viewer · Cost User** permissions across projects.
- **Zero counts are highlighted** — a member showing all zeros can open the menu through their role but holds no project access yet, so they will see no project data until they are added to a project.
- Expand a member to see exactly which projects they hold each permission on.

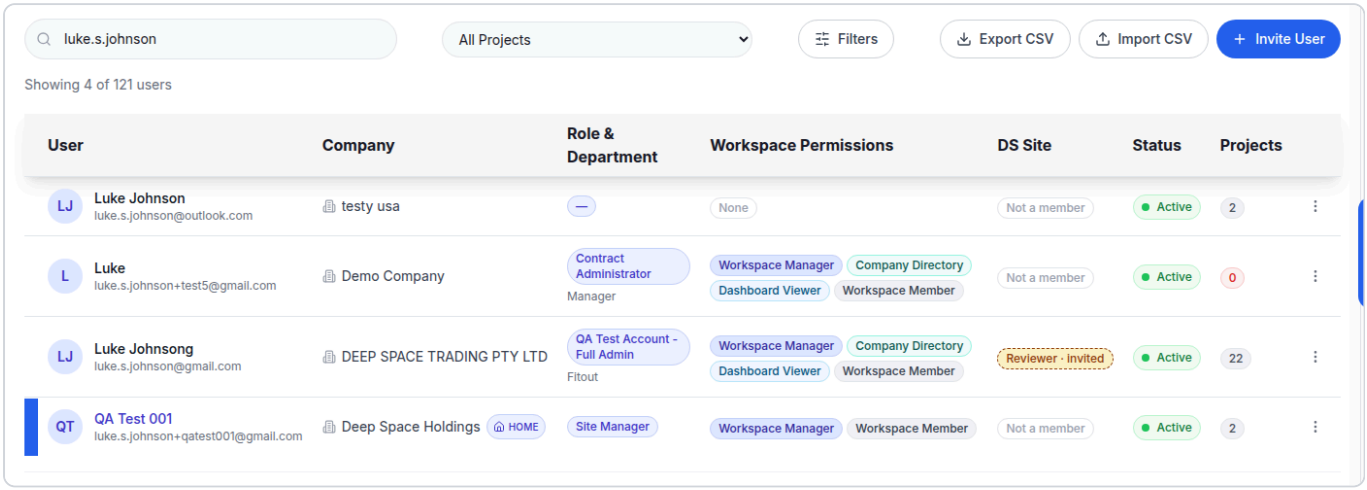


The Project Permissions tab: members of the selected role with per-permission counts. Amber zeros flag members with no project access; expanding a member shows their per-project permissions.

5. Granting and changing access

User Directory

Directory → User Directory is the home for people management: invite users, assign roles, and manage project access.

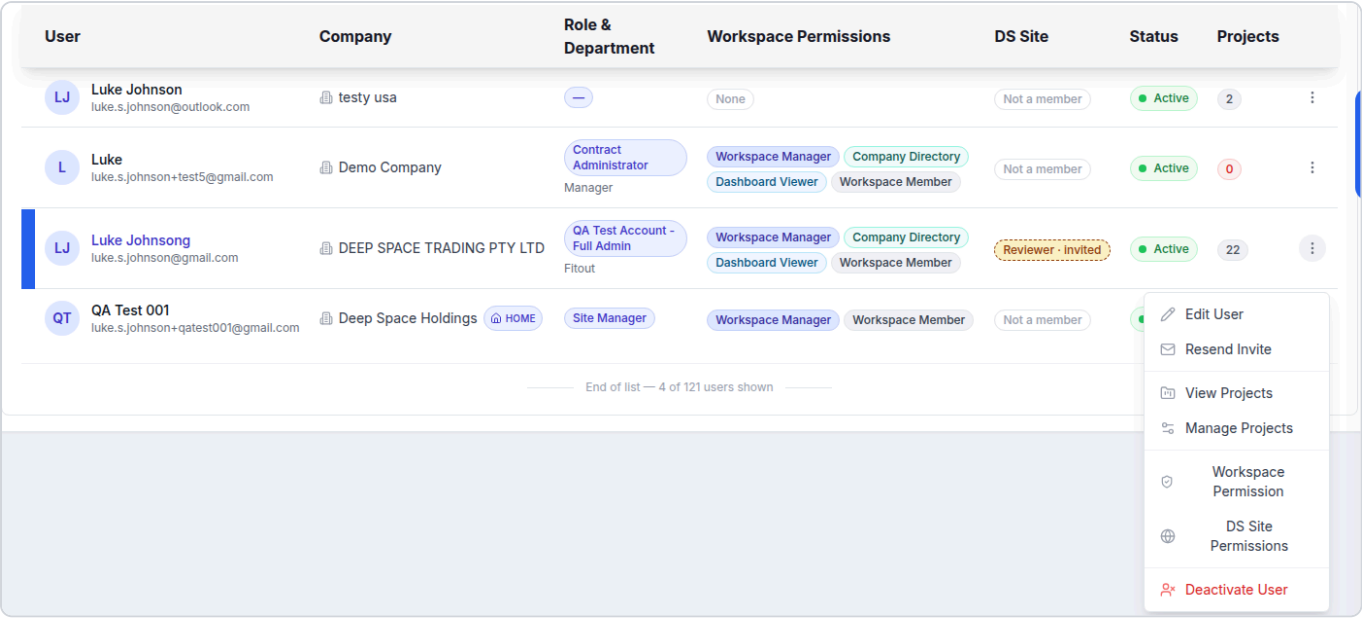


The User Directory: each member's company, role, workspace permissions, DS Site access, status and project count, with actions in the row menu.

Two columns show each person's access at a glance:

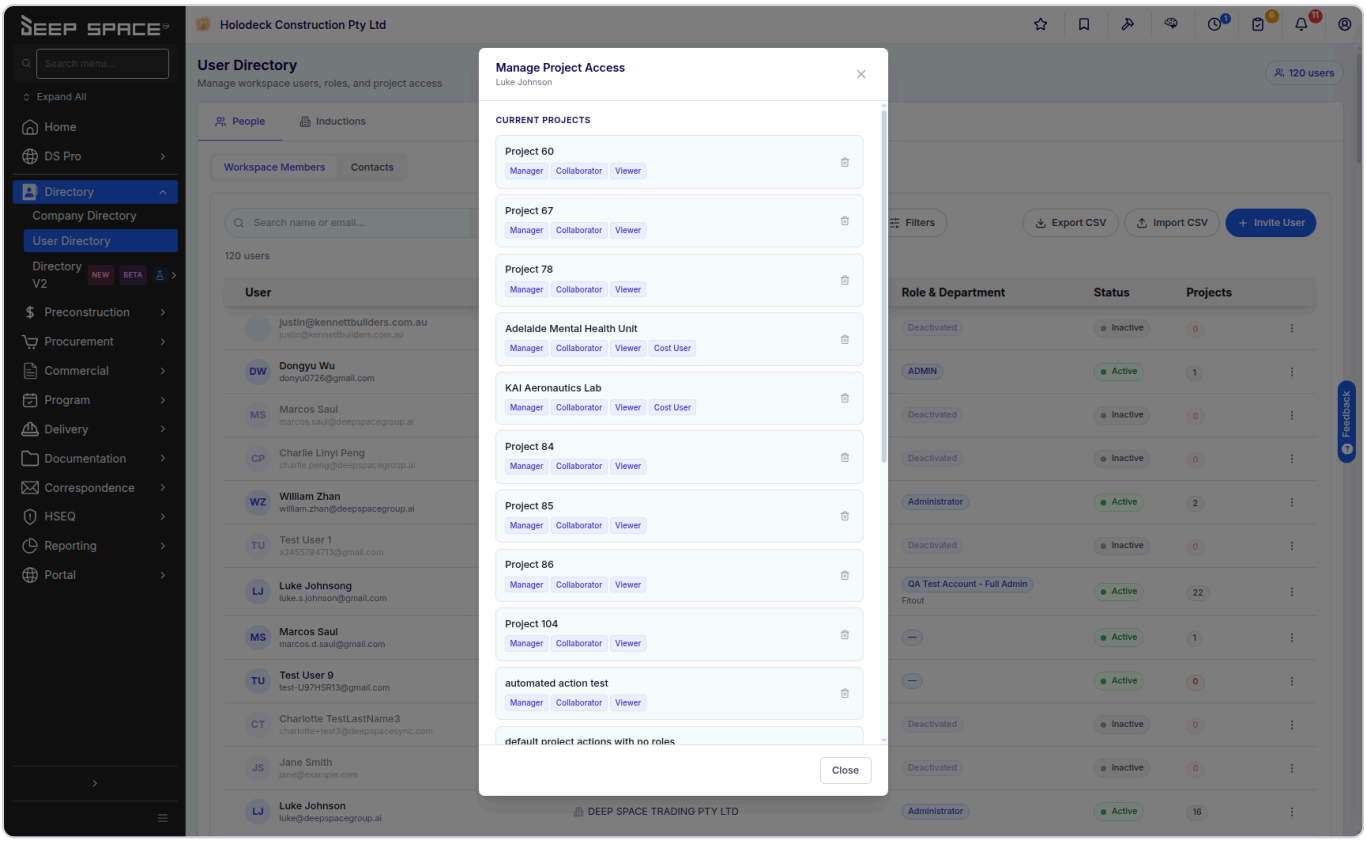
- **Workspace Permissions** — one pill for each workspace permission the person holds: *Workspace Manager*, *Company Directory* (View and Manage Company Directory), *Dashboard Viewer* and *Workspace Member*. A grey *None* pill means they hold none of them.
- **DS Site** — the person's role in the workspace's DS Site channel (for example *Reviewer* or *Administrator*). The pill notes when an invitation is still pending (*invited*, dashed outline) or the person has been *deactivated*, and shows *Not a member* when they aren't in the channel. This column appears only where the workspace is linked to a DS Site channel and you can manage it.

Click a pill to open the matching permissions window.



The row menu: Workspace Permission and DS Site Permissions sit alongside the project actions.

- **Invite User:** choose the person's role and the projects they should start with, in one step.
- **Row menu → Manage Project Access:** see every project the person is on, with their permissions shown per project; add them to more projects (new grants default to Viewer — increase from there) or remove access.
- **Row menu → Workspace Permission:** turn the four workspace permissions on or off. Only a **Workspace Manager** can change them. Anyone else can open the window to see the person's permissions, but it is read-only and shows *"Please ask a workspace manager to update these permissions."*
- **Row menu → DS Site Permissions:** add the person to the DS Site (mobile app) channel, change their role, resend or revoke an invitation, or remove them. Available to **Workspace Managers** and people with **View and Manage Company Directory**, where the workspace is linked to a DS Site channel.



Manage Project Access: the person's projects with their current permissions per project.

Project Settings → Team

Inside a project, the **Team** tab manages that project's team. Assigning someone a project role there also grants sensible project permissions for that role automatically. In the *Internal Team* section, each member's four permissions can be adjusted individually — only members who hold *Manager* on that project can change them, and a Manager always keeps Viewer and Collaborator.

6. Approvals — Delegation of Authority

Approval rights (who can approve, and up to what value) are not part of the role matrix. They are configured in **Delegation of Authority** under Admin, per entity type — for example progress claims, invoices and purchase orders — including multi-step approval workflows and a Highest Authority override. That is why every Approve cell on the Security page carries an *(i)* pointing there.

7. Portal roles — external parties

Portal roles give subcontractors, clients and consultants a focused portal experience instead of the full workspace menu. On the Security page, portal roles are marked with a purple *Portal* badge and are edited as a simple feature list per portal type. Ready-made presets cover the common cases:

- **Subbie Admin** — full subcontractor portal access, including commercials.
- **Subbie Worker** — documents, programme, action items and HSEQ; no commercials.
- **Client Representative** — full client portal access, and may manage their team members.

- **Superintendent** — full client portal access without team management.

8. Tips

- Permission changes apply after the affected user refreshes their browser.
- The *Deactivated* role is applied automatically when a user is deactivated — it grants no access and should not be assigned manually.
- Use **Export CSV** on the Security page for a complete, auditable snapshot of every role's permissions.
- When someone reports "I can't see the page": check their role's View tick first. When it's "I can see the page but no data": check their project permissions on the Project Permissions tab.