



DocurAI

INTELLIGENT DOCUMENT PROCESSING

Administrator Guide

Running a tenant on DocurAI Intranet

Illustrated with the Initech demo tenant — a fictional company used for screenshots and manuals so no real client data ever appears in product documentation.

DocurAI by BAARS Media
Administrator Edition

Contents

- 01** Introduction
- 02** Roles at a Glance
- 03** Managing Users
- 04** Managing Categories
- 05** Access Control: Roles vs. Groups
- 06** The Recycle Bin
- 07** Quick Reference Checklist

01

Introduction

This guide covers everything a tenant **Administrator** needs to run a DocurAI Intranet tenant day-to-day: adding staff, organizing documents into categories, deciding who can see what, and keeping the Recycle Bin under control.

Every screenshot and example in this guide comes from **Initech**, a fictional demo tenant seeded specifically for documentation and demos. Nothing here is a real customer's data — which also means nobody will mind if we have a little fun with the examples.

Who this guide is for

You should read this if your account has the **Administrator** role in a tenant. Administrators are the only users who can manage other users, categories, and tenant-wide settings — everything in this guide.

Looking for the Reader or Contributor guide instead? Those cover day-to-day document browsing and uploading, and are much shorter.

Meet the Initech staff

Five accounts are seeded in the demo tenant, each with a different role, so every screenshot in this guide reflects a real permission boundary rather than a hypothetical one.

Name	Username	Role
Bill Lumbergh	blumbergh	Administrator
Peter Gibbons	pgibbons	Contributor
Samir Nagheenanajar	snagheenanajar	Contributor
Michael Bolton	mbolton	Contributor
Milton Waddams	mwaddams	Reader

Milton's stapler privileges are not configurable from Settings.

02

Roles at a Glance

Every user in a tenant has exactly one baseline role. This role alone — with no further setup — decides what they can do. Section 5 covers an optional layer on top of this; everything below is always true, in every tenant, from the moment a user is created.

Role	View documents	Upload / manage own	Manage others' documents	Manage users & settings
Reader	Yes	No	No	No
Contributor	Yes	Yes	No	No
Administrator	Yes	Yes	Yes	Yes

In Initech: Milton Waddams (Reader) can open and read anything in the tenant, but cannot upload a file or edit a description. Peter, Samir, and Michael (Contributors) can upload documents and manage the ones they uploaded themselves — but not each other's. Bill Lumbergh (Administrator) can do all of the above for every document in the tenant, plus everything in Sections 3 and 4.

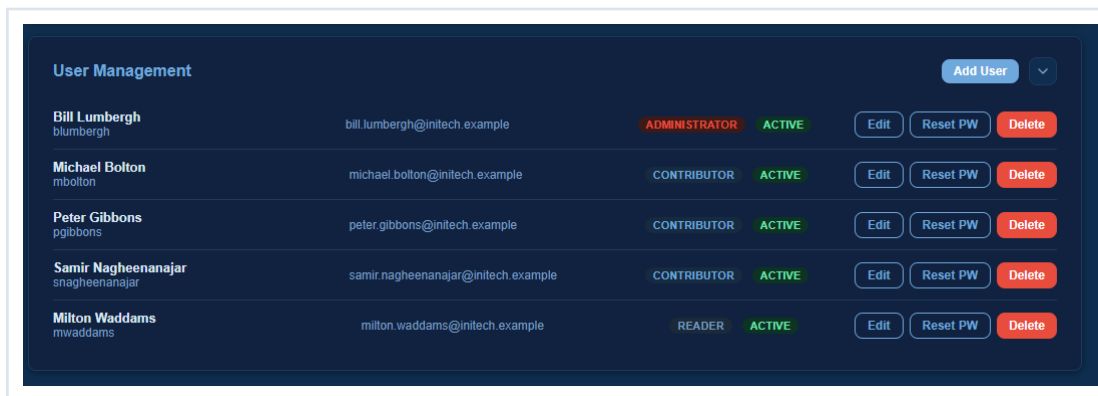
Changing a user's role

Settings → User Management → open a user → change the Role dropdown → Save. Takes effect on their next request — no need for the user to log out.

03

Managing Users

All user accounts for a tenant live under **Settings** → **User Management**, visible only to Administrators.



Settings — User Management, showing the five Initech accounts and their roles.

Adding a user

- Click **Add User** and fill in a username, display name, email, and a temporary password.
- Pick a role — Reader, Contributor, or Administrator (see Section 2). You can change this later.
- The user can sign in immediately with the password you set; there's no separate invite/activation step.

Editing, deactivating, and removing access

- Update display name, email, or role at any time from the user's row.
- **Deactivate** blocks sign-in without deleting the account or its document history — use this over deletion whenever someone leaves temporarily or their access just needs pausing.
- Resetting a password immediately invalidates the user's existing sessions.

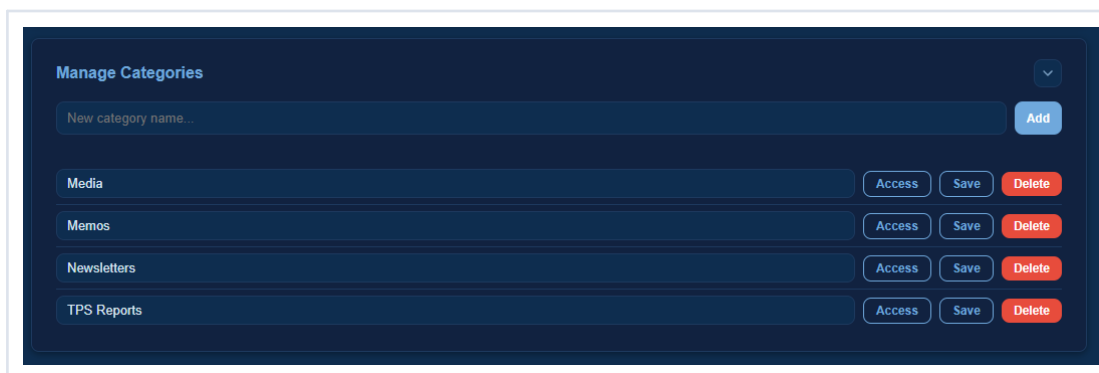
You can't lock yourself out

A tenant always needs at least one active Administrator. The system blocks demoting or deactivating the last one — so if Bill Lumbergh is the only Administrator on Initech, that protection stops Milton from ending up in charge by accident.

04

Managing Categories

Categories organize documents — every upload can be filed into one — and, if you turn on Access Control (Section 5), they're also the unit access is granted against. Every tenant starts with one built-in category, **Media**, used by the Media gallery; it can be renamed but not deleted.



Settings — Manage Categories, showing Initech's TPS Reports, Memos, Newsletters, and the built-in Media category.

Initech uses three categories to keep its (fictional) paperwork in order:

Category	Used for
TPS Reports	Status reports — and reminders about their cover sheets.
Memos	Company-wide notices from management.
Newsletters	The monthly employee newsletter.

Categories can be renamed at any time without breaking existing documents or permission grants — only the display name changes. Deleting a category un-files its documents (they become uncategorized rather than being deleted) and also removes any Access Control grants tied to that category, so old permissions never linger invisibly for a category that no longer exists.

05

Access Control: Roles vs. Groups

This is the section worth reading slowly. A tenant has **two** systems that both affect who can see and manage documents, and they interact in a way that's easy to misread.

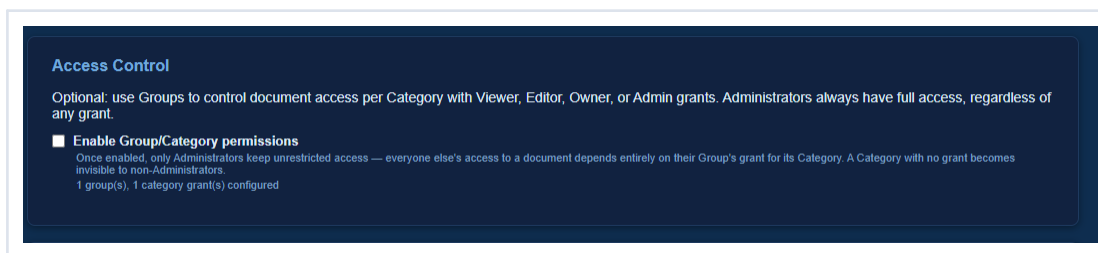
	Baseline roles (Section 2)	Groups & Category grants (this section)
Always on?	Yes, for every tenant	No — opt-in per tenant, off by default
Granularity	Whole tenant	Per Category
Who configures it	Administrator, per user	Administrator, via Groups + grants

Turning on Group/Category permissions is a cutover, not an addition

It's tempting to read Access Control as “extra rules on top of” the roles in Section 2. That's not what happens. The moment it's switched on, only Administrators keep their blanket access. Every Contributor and Reader loses the tenant-wide visibility their role used to give them, and their access to a document becomes governed entirely by whether one of their Groups has been granted a tier on that document's Category.

A Category with no grant is invisible

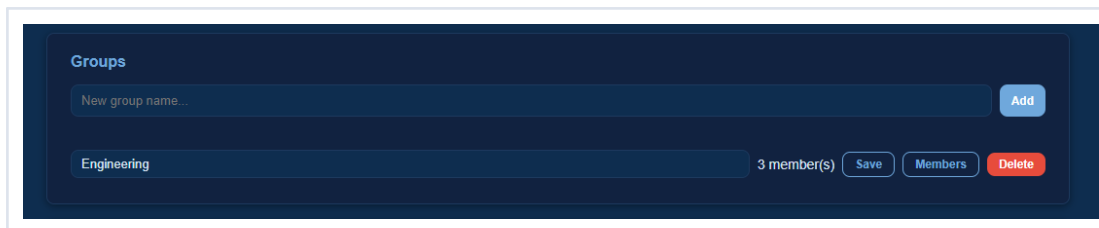
If you switch this on before setting up any Groups or grants, every non-Administrator loses access to every document, immediately — not just the ones in ungranted categories, all of them, since no category has a grant yet. The Settings page will warn you and ask you to confirm if you try to enable it with zero grants configured, precisely to prevent this.



Settings — Access Control card: the enable toggle and the live count of configured groups and grants.

Groups

A Group is just a named set of users — membership carries no access by itself. Access comes from granting a Group a tier on a Category (next section). Initech has one group, **Engineering**, containing Peter Gibbons, Samir Nagheenanajar, and Michael Bolton.



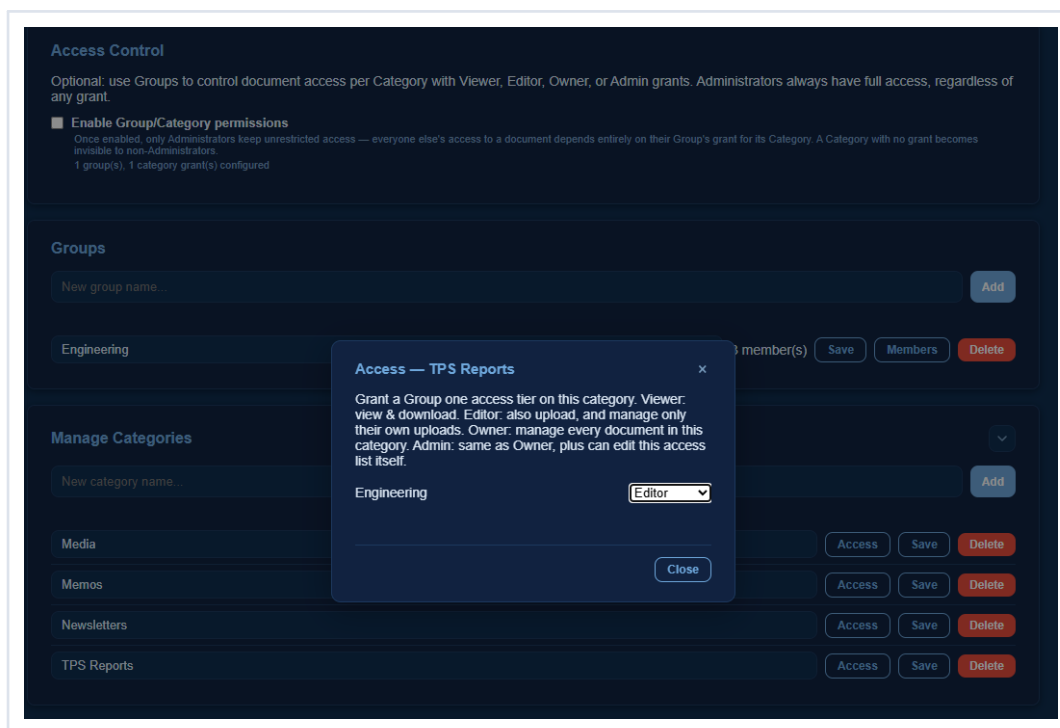
Settings — Groups card, showing the Engineering group and its three members.

Category permission tiers

Once a Group has a tier on a Category, every member of that Group gets that level of access to every document filed in it:

Tier	Can do
Viewer	See and download documents in the category.
Editor	Everything Viewer can, plus upload new documents and manage ones they uploaded themselves.
Owner	Everything Editor can, plus manage <i>any</i> document in the category, regardless of who uploaded it.
Admin	Everything Owner can, plus grant or revoke this category's own Group permissions — the one piece of governance that can be delegated below full Administrator.

Initech's Engineering group holds **Editor** on TPS Reports: Peter, Samir, and Michael can each file and manage their own TPS reports, but not rewrite each other's — nobody in the group holds Owner or Admin there.



Category permissions for TPS Reports — Engineering granted Editor tier.

What never changes, regardless of this setting

A few things stay governed purely by the baseline role from Section 2, whether or not Access Control is on — they're tenant-wide governance, not document access, so they're never delegated down to a Category-level grant:

- Managing users, categories, and this very toggle — Administrator only, always.
- Authoring company Announcements — governed by role, since announcements have no Category to hang a grant on.
- Emptying the Recycle Bin — Administrator only, always (see Section 6).

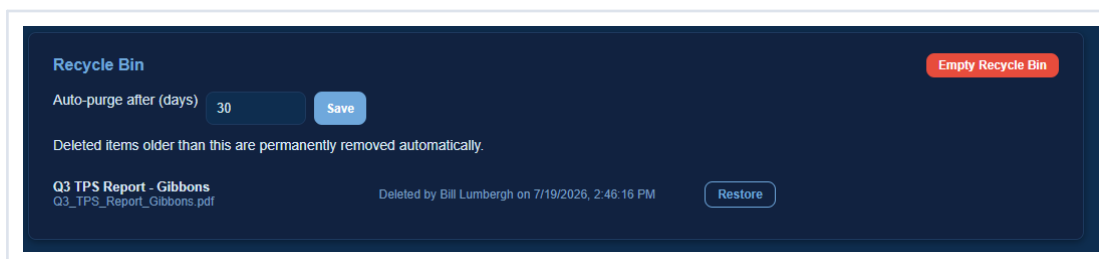
Turning it back off

Disabling the toggle is safe and fully reversible: no Group, membership, or grant is deleted — they simply stop being enforced and every user's access reverts to their baseline role from Section 2. Turning it back on later re-activates exactly what was configured before, which is also why the Settings page shows a live count of configured groups and grants even while the toggle is off.

06

The Recycle Bin

Deleting a document never removes it immediately — it moves to the Recycle Bin, where it stays until it's restored or the retention period configured here elapses.



Settings — Recycle Bin, mid-restore: Peter Gibbons' Q3 TPS Report was deleted (by Bill Lumbergh) and is one click away from coming back.

Action	Baseline roles only	With Access Control on
View the bin / restore any item	Administrator only	Administrator, or Owner/Admin tier on the category
Restore your own deleted upload	Not available to Contributors	Owner/Admin tier holders who also uploaded it
Empty the bin entirely	Administrator only	Administrator only — never delegated

Set **Auto-purge after (days)** to control how long deleted items are recoverable before they're permanently removed on a schedule — no manual cleanup required.

07

Quick Reference Checklist

Setting up a new tenant from scratch, in order:

- **Create categories** first — Settings → Manage Categories.
- **Add users** with the right baseline role — Reader, Contributor, or Administrator.
- Stop here if the baseline roles are enough. Most tenants never need Section 5.
- If you need per-category access: **create Groups**, add members, then **grant tiers** on the relevant categories — do this *before* switching Access Control on.
- **Enable Access Control** only once every group that needs access has a grant — the Settings page will warn you if you try to switch it on with nothing configured yet.
- Set a sensible **Recycle Bin retention period** for the tenant's needs.

One last thing

If you take nothing else from this guide: Access Control is a cutover for non-admins, not an add-on. Configure the grants first, flip the switch second — in that order, every time.

This concludes the Administrator Guide. The Contributor and Reader guides cover day-to-day use for everyone else — including, eventually, Milton.