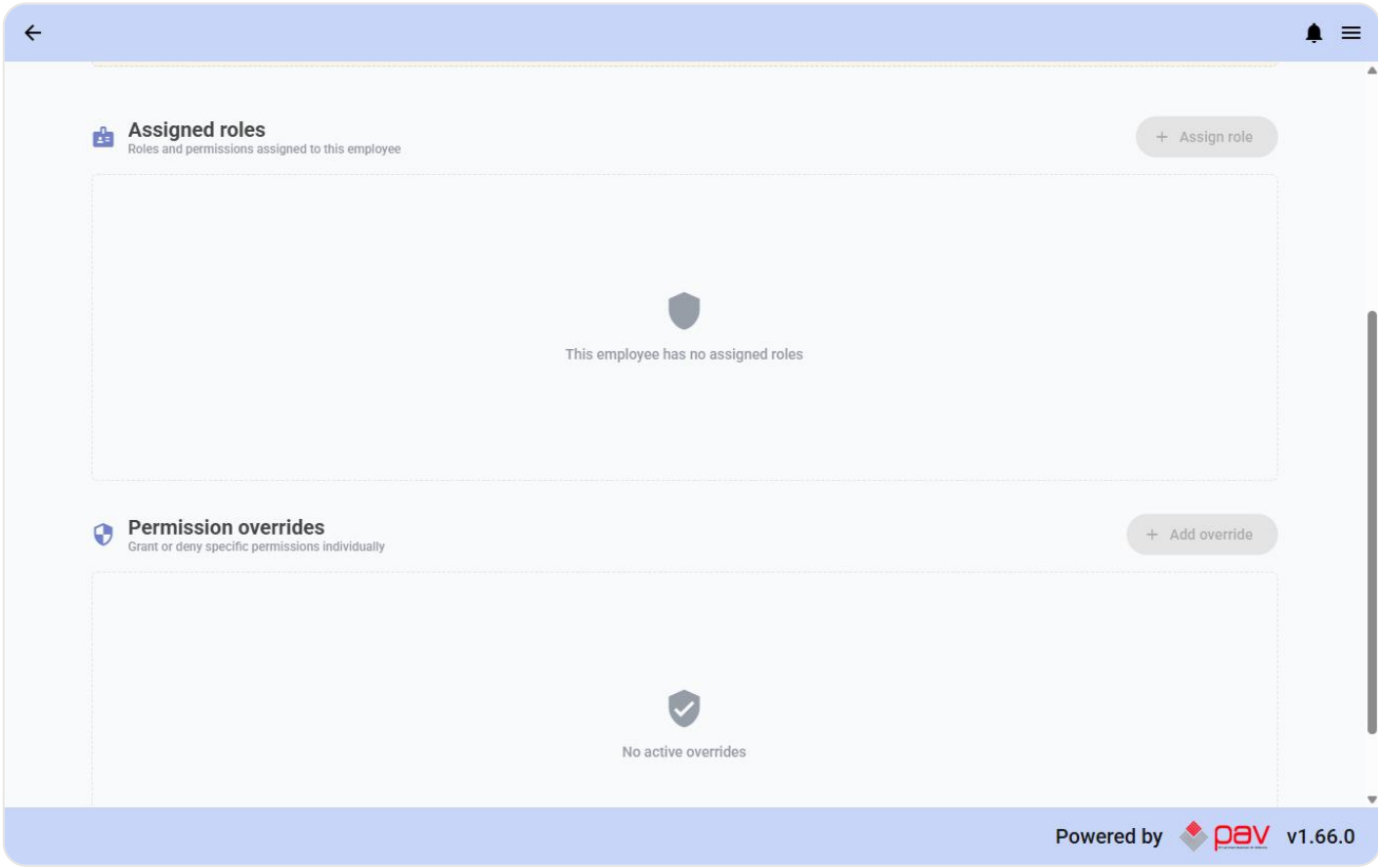
Permission overrides

> **You need:** `employees:read` and `employees:write` — held by `admin` and `employee_manager`.

An override grants or denies one specific permission to one specific employee, on top of whatever their roles say. Use it when a person matches an existing role in every respect but one. It lives under **Permission overrides** on the employee's screen.



The two effects

Effect	What it does	Typical use
GRANT	Adds one permission the employee's roles don't include	A shift operator who also needs to cancel orders, without giving them the whole manager role
DENY	Removes one permission the employee's roles do include	A store manager who should not be able to pause delivery

The one rule that decides conflicts

A deny always wins. It beats every grant, from every role the employee holds, and from an explicit grant override too. There is no ordering to reason about and no priority to configure.

This is deliberate: it means a deny is a reliable way to remove an ability, without auditing which roles might be putting it back.

> `super_admin` is the one special case — it bypasses all checks, including denies. `admin` does **not**; individual denies apply to it normally.

Creating one

1. In the **Roles** module, open **Role assignments**, find the employee and open their screen.
2. Under **Permission overrides**, click **Add override**.
3. Under **Permission**, search for and choose the permission.
4. Under **Effect**, choose **GRANT** or **DENY**.
5. Optionally set a date under **Expiry**.
6. Save. The record keeps who created it, for auditing.

Use the expiry date

Most overrides are temporary in intent — cover for an absence, a seasonal push, a trial of wider access. Very few are temporary in practice, because nobody remembers to remove them.

Setting an expiry date when you create the override turns that problem into a non-problem. If the access turns out to be permanent, the right fix is a role change, not an override that never ends.

When not to use an override

When two roles already cover it. If the person needs a whole area, assign the role for that area — see Common role combinations. Overrides are for single permissions, not for assembling an area out of parts.

When several people need the same thing. Three identical overrides are a sign the role is wrong. Request a role change instead — see Requesting a new or changed role.

To restrict data. Overrides control actions, not visibility. To limit what someone can see, set their scope — see Setting an employee's scope.

Reviewing them

Overrides are the part of the access model most likely to drift, because each one is invisible from the role catalogue. Review the overrides list periodically and remove the ones whose reason has passed.

Creado 2026-09-17 16:28:33 UTC por Fran Sanchis

Actualizado 2026-11-22 13:08:45 UTC por JLV