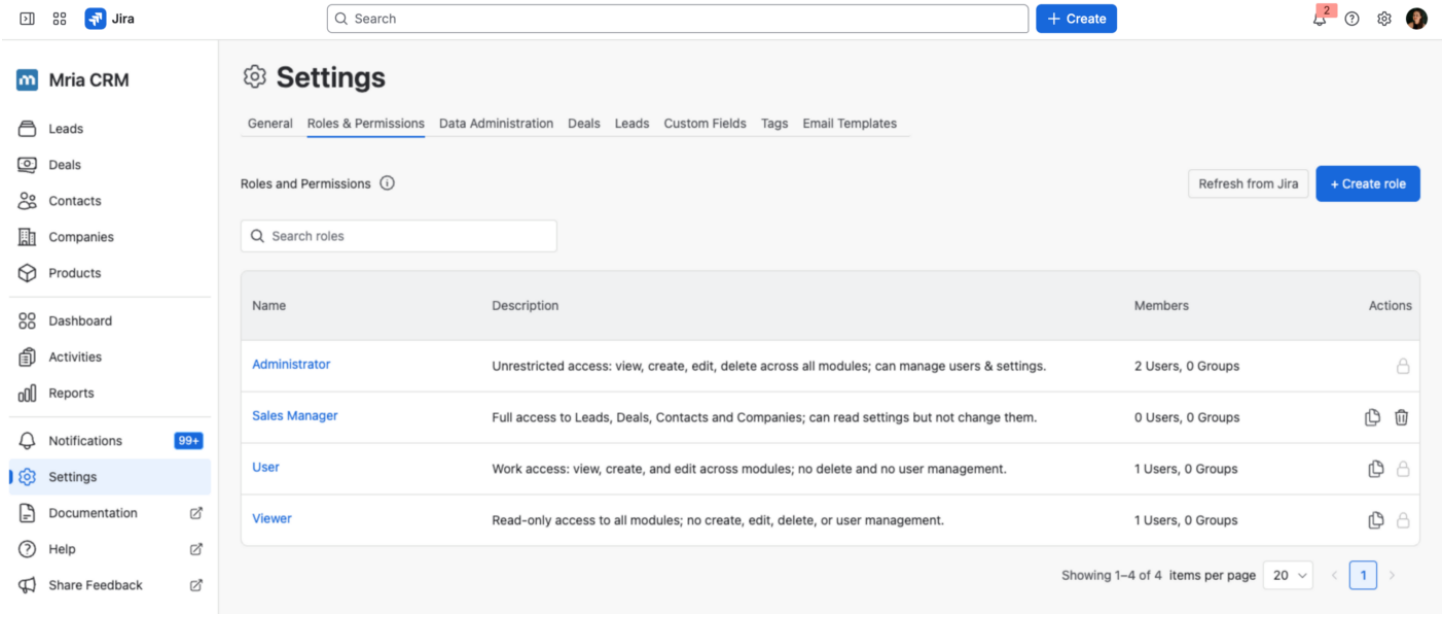
Roles & Permissions

Settings · https://mriacrm.com/docs/roles-and-permissions/

The Settings section allows you to configure access levels, user management, and other CRM preferences. One of the key areas here is **Roles & Permissions**.



1. Roles

Mria CRM ships with three built-in roles:

- **Administrator** – Unrestricted access: view, create, edit, delete across all modules. Can also manage users and settings.
- **User** – Work access: view, create, and edit across all modules, but no delete permissions on the five core entities and no user management. Emails and Email templates have their own Delete grants, which User does have.
- **Viewer** – Read-only access to all modules; cannot create, edit, delete, or manage users. Note that **Reports** is on for Viewer by default, and reports expose and export record data — see the warning under *What a role can be allowed to do*.

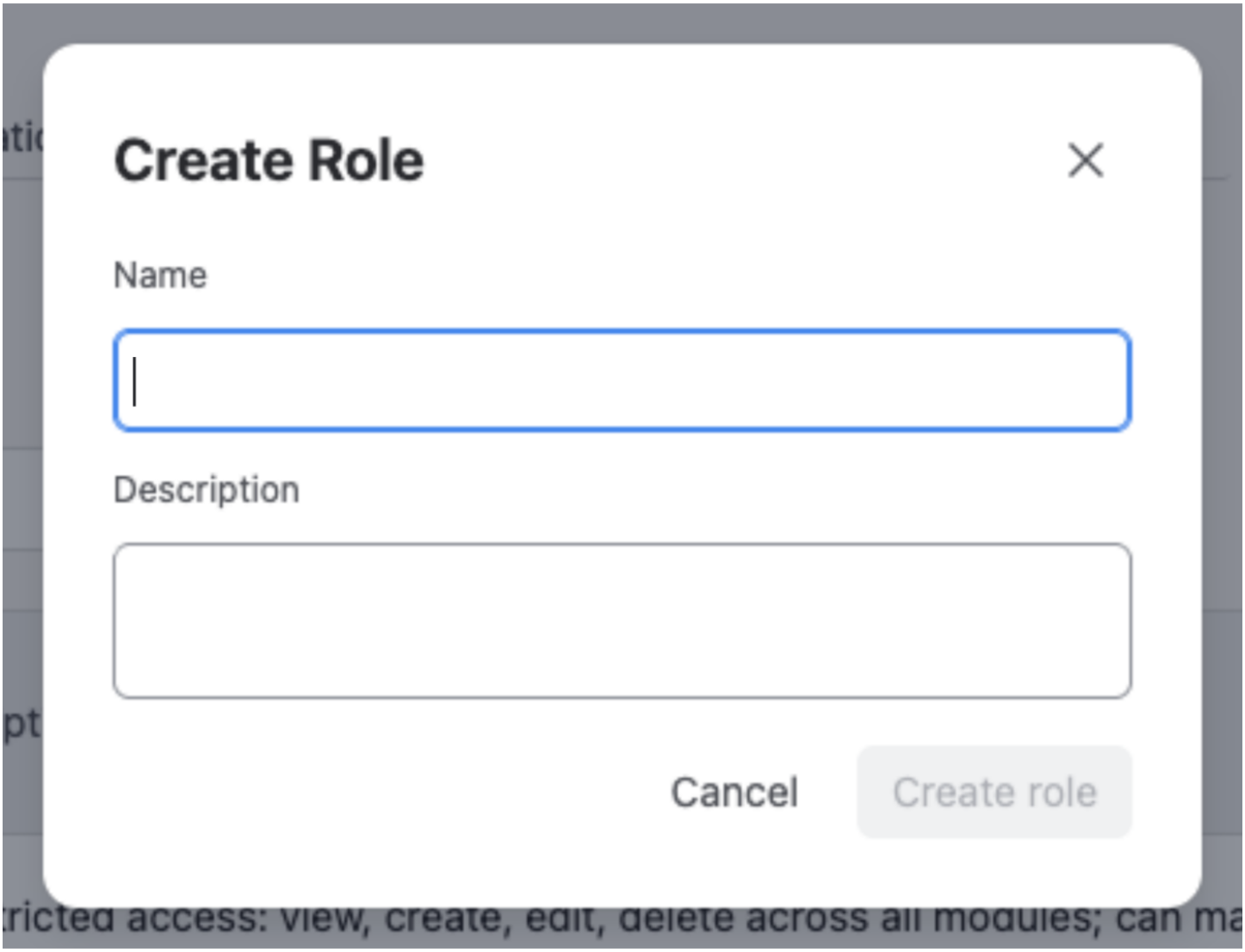
Each one is a starting point rather than a limit — you can add your own roles alongside them. The built-in three cannot be deleted, and a padlock in the **Actions** column marks them as such.

> **Important:** Jira administrators are automatically assigned the **Administrator** role in Mria CRM. This cannot be changed. However, Administrators can also assign the Administrator role to regular Jira users.

2. Creating your own role

Open **Settings → Roles & Permissions**. There are two ways to add a role, and the difference is only where its permissions start from:

Option	Starts from
+ Create role	A blank slate. Give the role a **Name** and a **Description**, then set its permissions.
Duplicate (the icon in the Actions column)	A copy of an existing role's permissions, which you then adjust. Usually faster — most new roles are 'User, but also allowed to…' or 'Viewer, plus…'.

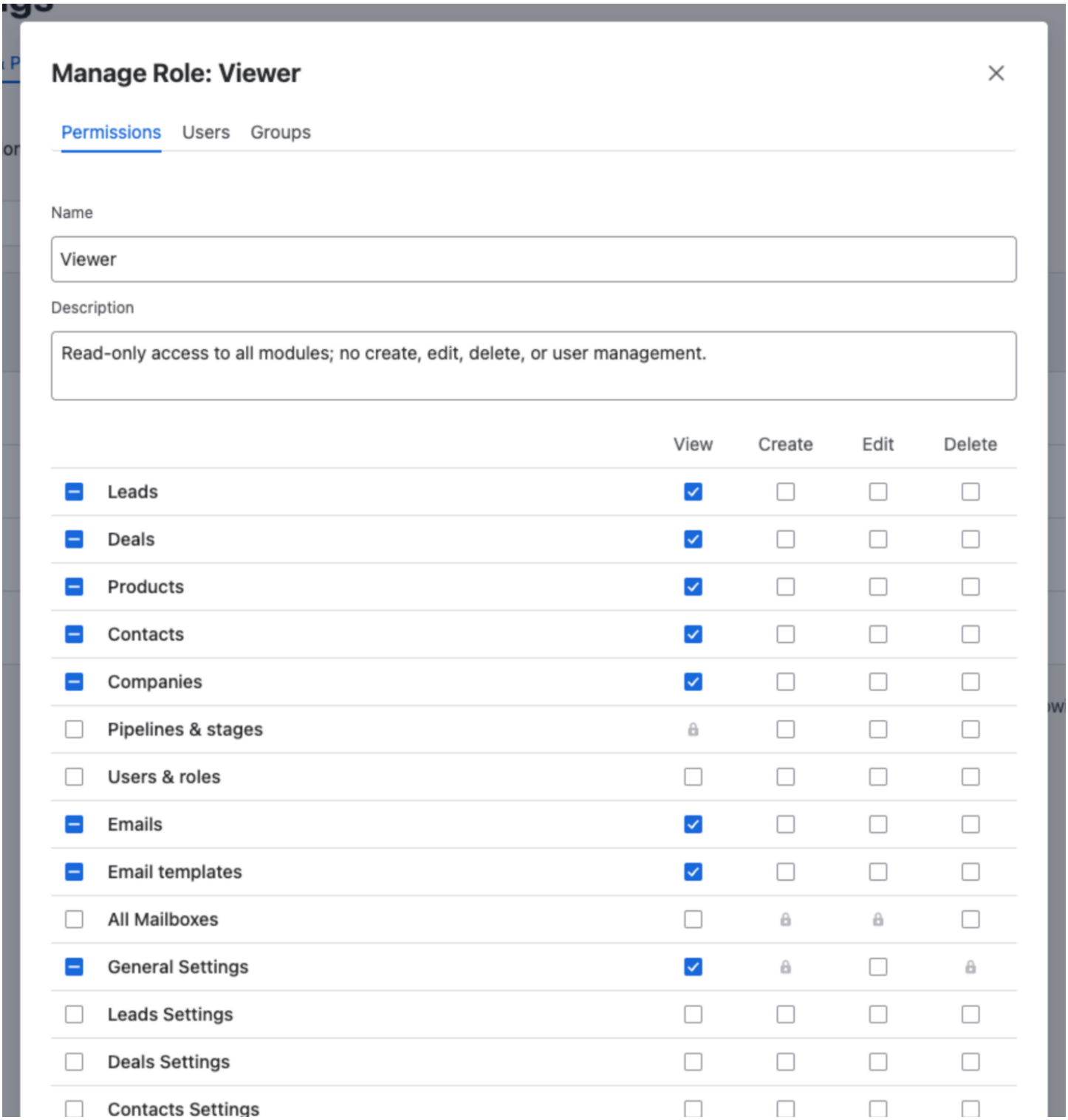


The description is worth writing properly. It is what everyone else sees in the roles list, and it is the only place the intent behind a role is recorded.

> Use the **Search roles** box above the list once you have more than a handful. The list is paginated.

3. What a role can be allowed to do

Clicking a role's name opens **Manage Role**, which has three tabs — **Permissions**, **Users** and **Groups**. The Permissions tab is a grid: one row per area of the CRM, and four columns.



Column	Means
View	See the records or the settings page at all. Without this the area is effectively hidden.
Create	Add new records or new entries.
Edit	Change what is already there.

Column	Means
Delete	Remove it.

The rows cover both the records people work with and the settings behind them:

Group	Rows
Records	Leads, Deals, Products, Contacts, Companies
Email	Emails, Email templates, All Mailboxes
Configuration	Pipelines & stages, Users & roles, General Settings, and the per-entity settings areas — Leads, Deals, Contacts, Companies and Products

- Each row has a **select-all** checkbox in front of it, which grants that module in full in one click rather than four.
- **Reports** is a single on/off toggle at the bottom rather than a row of four, because a report is either available to the role or it is not.
- Some combinations do not apply — you cannot *create* a mailbox from inside Mria CRM, for example. Those cells show a **padlock** and cannot be ticked.
- Changes are not live until you click **Save**.

Reports are not permission-shaped. The **Reports** grant is a single toggle, and turning it on shows Deal, Contact and Company names and email addresses through the reports — and allows exporting them to CSV — regardless of whether the role can see those records anywhere else in the CRM.
This matters most for **Viewer**, which has Reports **on** by default: a role you set up as read-only can still export a list of contact names and email addresses. If that is not what you want, turn the Reports toggle off for that role.

Giving a role **Users & roles** permissions lets the people in it change who can do what — including granting themselves more. Treat it the way you would treat handing out admin, and keep it to the roles that really need it.

Why an action is grayed out

The **Actions** column shows a padlock where an action does not apply, and says why when you hover it:

Role	What you get
Administrator	A padlock on both actions — *the Administrator role always holds every permission, so it cannot be duplicated or deleted*.
User and **Viewer**	Duplicate is available; Delete is padlocked, because a built-in role cannot be removed.
Your own roles	Both Duplicate and Delete are real buttons.

> Duplicating a built-in role is the usual way to start: it gives you an editable copy of a sensible permission set, and the original stays untouched.

4. Users and Groups

Membership is managed per role, on the **Users** and **Groups** tabs of the same **Manage Role** dialog.

- Each role can be managed by **adding or removing users and groups**.
- The **Administrator role cannot be deleted**.
- If a user belongs to multiple roles (e.g., Viewer + Administrator), the **higher role is applied** (Administrator).

5. Sync with Jira

The **Refresh from Jira** button pulls the latest data about users and groups directly from Jira, instead of waiting for the automatic hourly sync.