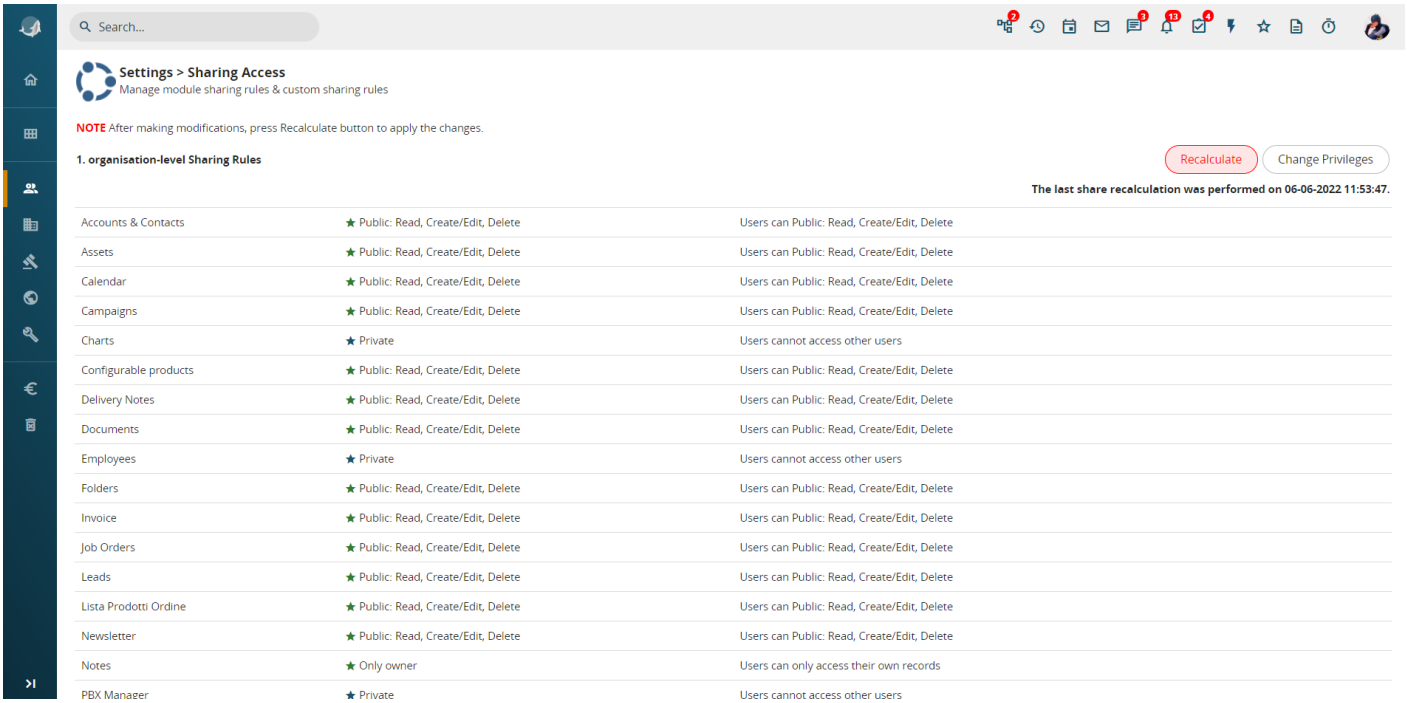
16.5 Sharing Access

vtenext allows you to set the access privileges of the Roles, defining whether the content of the CRM is generally accessible (public) or with limitations. There are various degrees of limitation. The rules are divided into two blocks: general global access rules and custom rules. The general rules of access are valid as standard for all Roles, but at the same time it is possible to attribute exceptional rules to certain Roles only, in order to cover the most diverse needs of the different company structures.

In general, what you will do through Sharing Access is to tell the system which users (based on their hierarchical role) will be able to see and/or modify the data contained in the CRM, module by module.

Warning! After any changes to the shared rules, **press the Recalculate button** to verify the configuration as a whole, avoid conflicts and make the changes operational.



The first thing to define is the Sharing Access rule for each of the modules. With what degree of freedom do you want the content of the modules to be accessible to users?

The most restrictive approach is private. When this sharing acess rule is applied to a module the visibility, creation, modification and deletion of records will follow the hierarchy that was defined inside the roles. In details the possible cases are shown below:

- users with the same roles will be able to see, modify and delete the records that were assigned to them, but they will not be able to make the same actions, mentioned

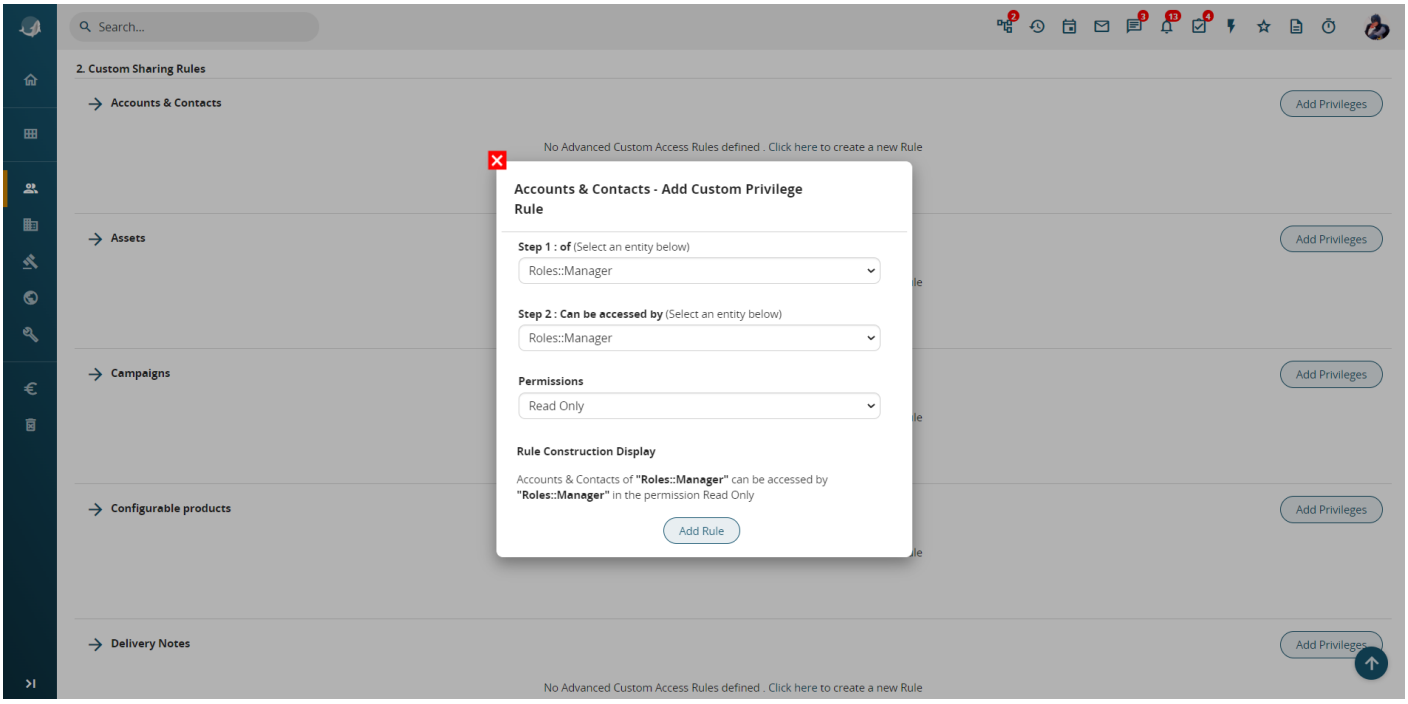
previously, to the users with the same roles;
- users that have subordinates in hierarchy will be able to see, modify and delete their own records and the records of their subordinates.

The Public approach has 3 levels of decreasing restrictions, therefore some privileges (visibility and/or creation and/or modification and/or deletion) will no longer be based on hierarchical roles, but will be open.

Public: read only	All users can access and view the module data. Only the assignee and users with a higher hierarchical role can publish, modify or delete data.
Public: read, create/edit	All users can view, create and edit the module data. Only the assignee and users with a higher hierarchical role can delete data.
Pubblic: read, create/edit, delete	All users can view, edit and delete data. With this setting the CRM is completely public.

Keep in mind that the behaviour of some modules implies the same induced behaviour of connected modules. For example, if the Accounts module is set to Private, Quotes, Tickets, Sales Orders, Purchase Orders and Invoices will also be in Private mode.
Messages and Notes allow you to set access privileges in a more systematic way. The sharing of the Calendar module differs in behaviour from the procedure of the other modules, and is analysed in detail in the relevant chapter. The sharing access settings cannot, therefore, be changed.

At the bottom of the Sharing Access panel, you can create exceptions to the permissions that you have defined so far, thus creating exceptions to the hierarchy of roles.



- Press Add privileges on the module for which you want to create an exception;

- Then select the entity owner role in Step 1;
- Select the role for which you want to extend visibility in Step 2;
- Then define the permission between Read Only or Read and Write;
- Enter the desired user tab and add the newly created rule in the "Owner-based sharing rules" menu item.

Revision #2
Created 2022-05-25 17:25:39 UTC by Alberto
Updated 2022-06-08 13:28:18 UTC