# Permission control

How to use Avallone's permission control

---

### Permission control

Permission control is vital for data protection and, therefore, it is vital for our customers. With permission control, our customers can ensure that only the relevant users can access and handle data in Avallone.

Avallone is built for granular permission control where it is possible to limit access to features such as but not limited to: sharing, company overview, KYC Responder, and KYC Collector. The way Avallone is built, there are a high degree of possibilities for creating permission control in a way that is tailored for each individual customer.

Avallone has created some standard permission groups. These groups can be adjusted, and it is also possible to create new tailored permission groups.

### Standard permission groups in Avallone

From day 1, Avallone comes with some standard permission groups that all customers can use and benefit from. Below is a short description of the standard permission groups.

#### KYC Managers

The permission group "KYC Managers" gives users access to view, create, handle and share data. It also gives access to all the products (i.e. KYC Responder, KYC Collector, etc.) that the tenant has access to.

#### Security Management

The permission group "Security Management" gives access to permission controls and can create new permission groups or adjust existing security groups. Being in "Security Management" allows the user to add and remove users from the different permissions groups. Additionally, users in this permission group have access to API tokens and API users.

#### User Management

The permission group "User Management" gives the user access to invite new users to the platform and add them to relevant permission groups. Also, these users have access to tenant settings.

#### Product Management

This permission group is able to configure the product (e.g. update the company model) by adding custom fields, etc.

#### Default API Permission Group

The Default API permission group is used for the relevant user rights that are needed for API users.

### Examples of alternative permission control use cases

There are many ways that permission control can be used to limit access to data or functions in Avallone. The below list has a few examples for use cases and is not limited to just these cases:

- Create user access that restricts users to be only able to view information on the platform.
- Create users who are not allowed to share information.
- Create users who only can request information in the KYC Collector but will not be able to see and review the collected data.
- Users who do not have access to Officer and/or Legal entities in the Hub.
- Users who do not have access to specific features like signing, the Q&A, etc.
- Users without access to the KYC Collector or the KYC Responder; that is, they can only access the KYC Hub.

The above examples will require tailored permission groups. These permission groups can be designed with support from Avallone.

### How does a permission group work?

A permission group will give you a set of permissions that allows you access to view, handle and/or conduct tasks in the platform. Permission groups only add permissions; it is not possible to create a group where something is excluded/not allowed.

Therefore, if you want to exclude some users from having the ability to share information, then you would have two possibilities:

1. Create one permission group allowing view and handling of data and one permission group for sharing. Users there should be able to share must then have access to both groups and users there should not be able to share should only have access to the first group.
2. Create two permission groups with all the relevant permissions for the two types of users. Users should then be added to the relevant user group.

The method that will work best for you as a company is fully based on your needed granularity and how you operate in general within your team and organization.

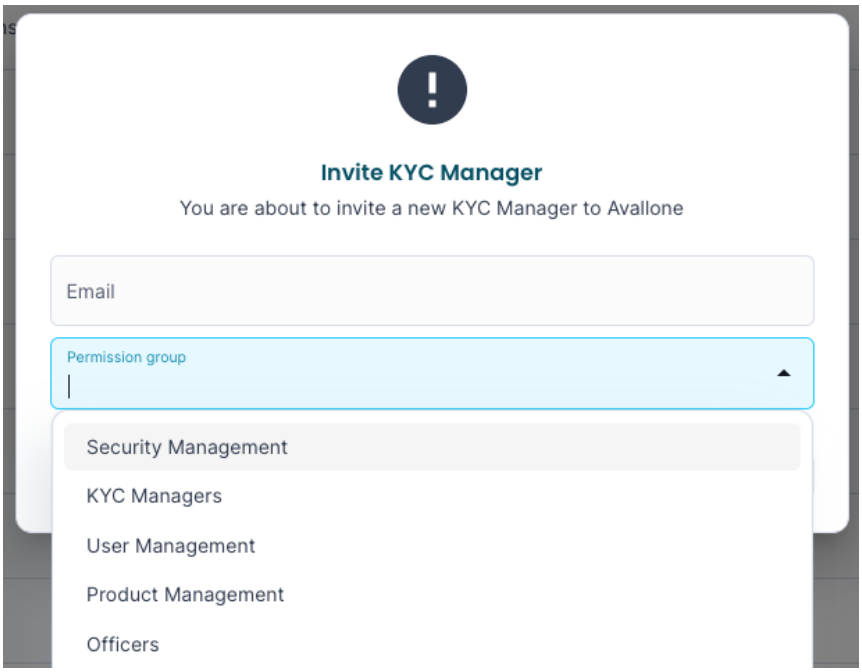
### Detailed insight

All features are built with the below permission levels. For some features, it does not make sense to have all of them, but in general, they will have them:

- ADD or CREATE: Allows the user to add or create data to the feature
- UPDATE: Allows the user to update/edit data in the feature
- VIEW: Allows the user to view data in the feature
- DELETE: Allows the user to delete data from the feature

### Creating a new user

When creating a new user, you will, as a part of the creation process, select the relevant permissions. You can add extra permission groups after the user is created.




### When does the permission group take effect?

When changes in permission groups have been made, the user needs to login again or switch the tenant to see the effect of the changes in permission groups.