



## Exploring Remote Desktop Manager Permissions



---

**PERMISSIONS ARE A SET  
OF RIGHTS THAT CAN  
BE GRANTED TO ROLES  
INSTEAD OF USERS**

---

Recently, we took a look at [Roles](#) and RDM's [role-based security system](#), which allows you to set specific rights for one or multiple users. Today, I want to dig a little deeper by focusing on Permissions, which work hand-in-hand with Roles.

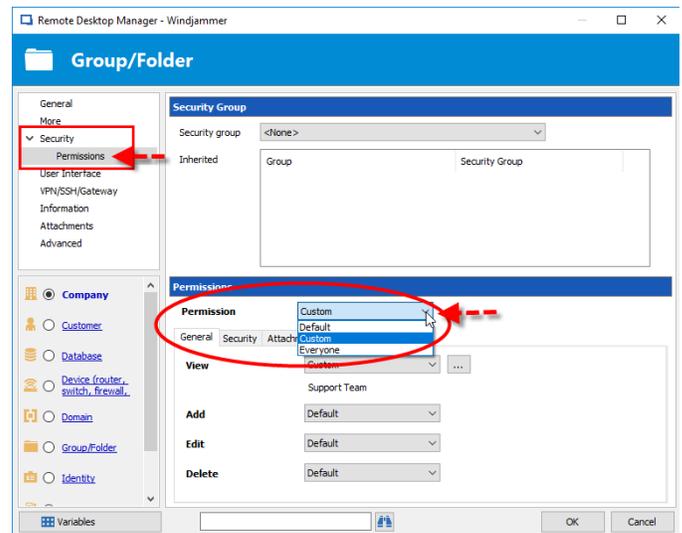
### **About Permissions**

[Permissions](#) are a set of rights that can be granted to roles instead of users. It allows for very accurate control of your security, giving you more flexibility and simplifying right management. For example, you can restrict access to entries, security settings, attachments, and so on. Plus, since you don't have to configure permissions for each user, you'll save time and reduce the risk of error.

# Setting Permissions

Once your users and roles have been created, **edit** the session or group/folder that you wish to add permissions to. Select the **Permissions** side menu, and then choose one of the following values:

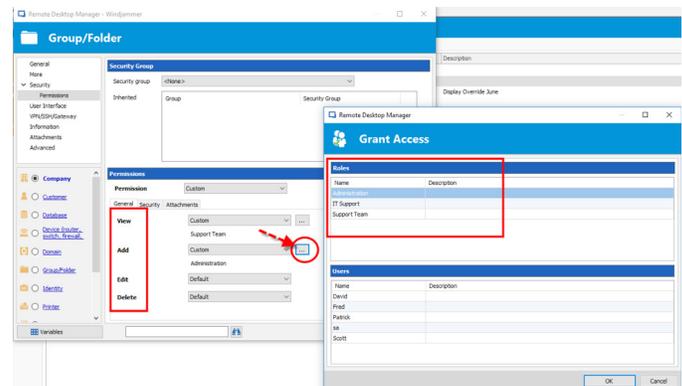
- **Default:** The permission will be inherited from the parent groups/folders.
- **Custom:** Lets you grant the permission to specific users or roles.
- **Everyone:** Everyone will be granted the permission.
- **Never:** Only administrators will be granted the permission.



Next, you can set granular-level permissions to users:

- **View:** Allows the user to view and use the entries for that security group.
- **Add:** Allows the user to add entries in groups/folders for that security group.
- **Edit:** Allows the user to edit the entries for that security group.
- **Delete:** Allows the user to delete the entries for that security group.

These rights are managed at the database level. If you want to grant permissions to all users who are part of the same role, set the **Permissions** to **Custom**, click on the **ellipsis (...)**, and grant access accordingly. Note that if a role is not included in a specific permission's list, access will automatically be denied.



Once your users, roles and permissions are set, when a new user is added, you can simply assign them the relevant role(s). You'll save time and effort, while also reducing the risk of error and making your overall security management model stronger and safer, all-in-all I would say that's a pretty good day of work!

As always, please let us know your thoughts by using the comment feature of the blog. You can also visit our forums to get help and submit feature requests, you can find them [here](#).