# Roles in Remote Desktop Manager

Devolutions

WE ARE MOVING TOWARDS A ROLE BASED SECURITY SYSTEM

In the past, when discussing security in Remote Desktop Manager, we talked about Security Groups. But things have changed and we are moving towards a Role Based Security System, since this gives you more flexibility than ever and offers a more granular protection system.

Roles are available with an advanced data source (SQL Server, SQL Azure, MySQL/MariaDB and Devolutions Server), they allow you to easily grant permissions to roles instead of granting permissions to one user at a time. You could also assign multiple roles to a user, which would unify all permissions. For example, a user who is assigned both the "technical" and "administrative" roles would have more access rights than a user who is limited to one or the other.

# Creating a new role in RDM is fast and easy. Here's what to do:

- Go to **Administration – Roles – Add Role.**
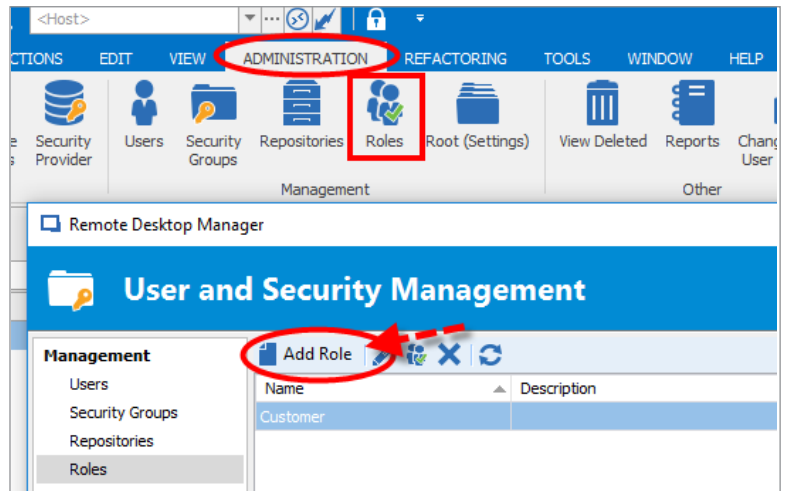
- Give your newly-created role a name.

- From the **Privileges** tab, select the privileges that will be assigned to the role.

- From the **Permissions** tab, you may leave everything to default, as rights can be granted to users.
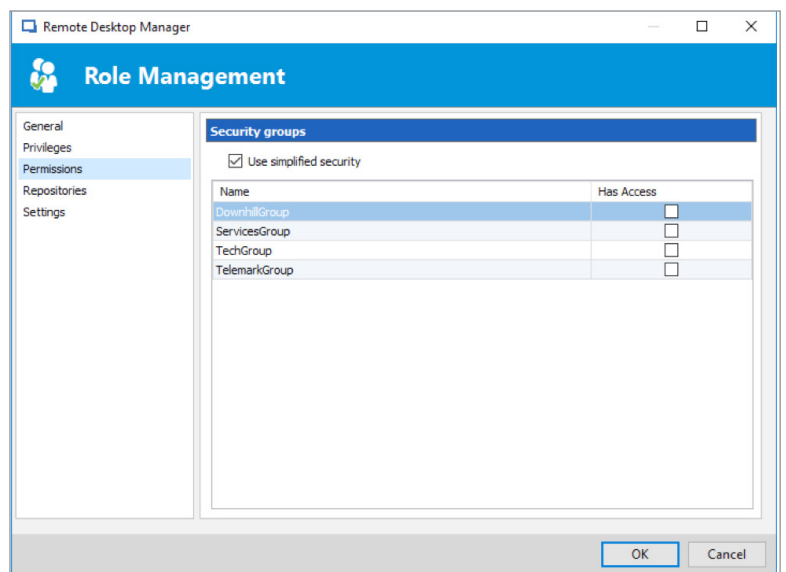

- Click **Assign Roles** to quickly assign the new role to one or multiple users.
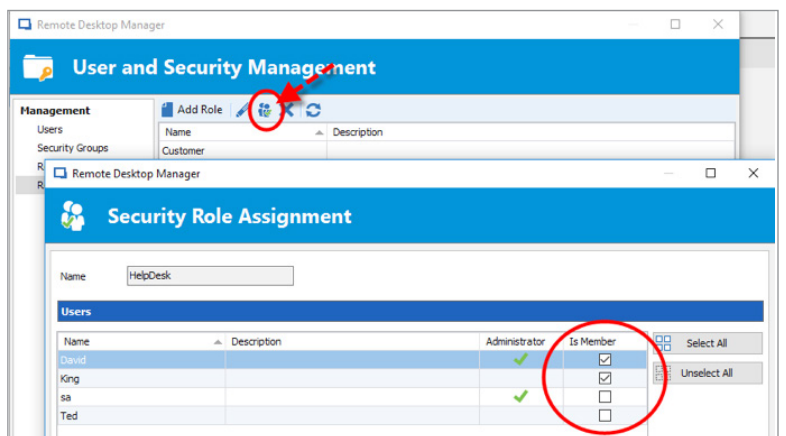
Also note that if you're using [Devolutions Server](#) as your data source, then the roles are actually links to Active Directory groups. By leveraging Active Directory integration, you can easily define access rights for all domain users in your organization.

Once the new role is created, it can be assigned discrete permissions to control user access. From the **Permissions** section of an entry properties, set the permission to Custom and assign it roles. Only users from these roles will be granted the permission.
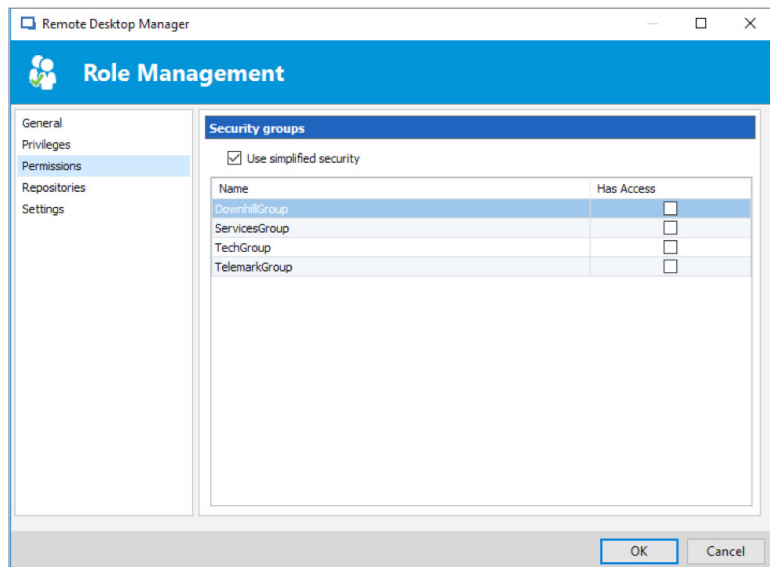
As always, please let us know your thoughts by using the comment feature of the blog. You can also visit our forums to get help and submit feature requests, you can find them [here](#).