New SQL Server Custom Authentication Mode

Devolutions

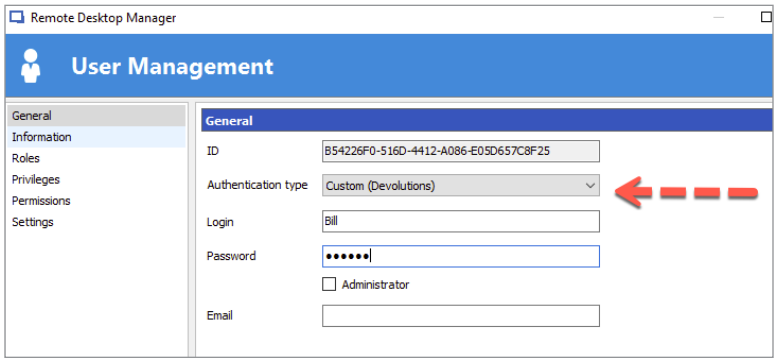
A NEW AUTHENTICATION MODE THAT USES A SINGLE ACCOUNT TO ACCESS THE DATABASE FOR USERS OF THIS TYPE

Custom (Devolutions) is a new authentication mode that uses a single account to access the database for users of this type. User accounts will be created for your staff to use Remote Desktop Manager (RDM), but to be entirely managed by RDM. SQL Logins are not created for these user accounts, therefore accessing the database directly (with tools such as Microsoft Excel or others) will no longer be possible.

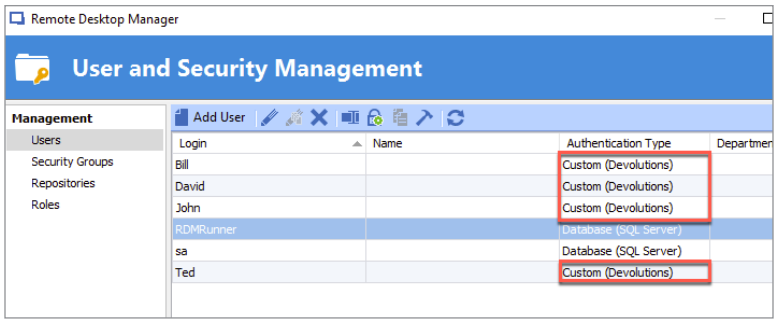
To ensure that the password of the account used for the database access is not revealed, the administrator will be required to distribute a Data source Definition file (.rdd) which contains the information beforehand.

Let's cover the entire process:

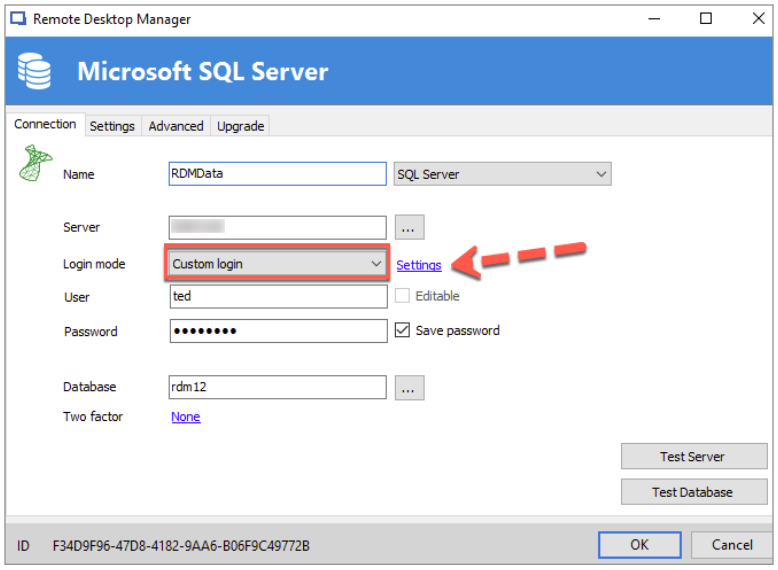
When creating a user, select Custom (Devolutions) as the Authentication type.



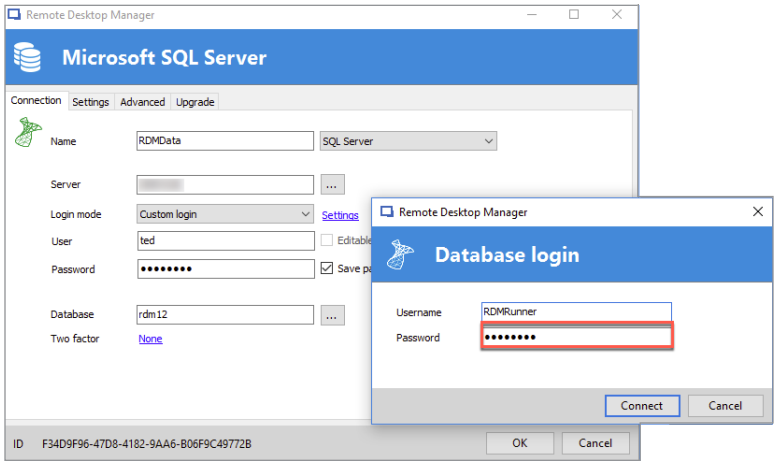
To ensure the highest level of security, most of your users should be using that model. There should be a limited number of user accounts of the Database (SQL Server) Authentication Type.



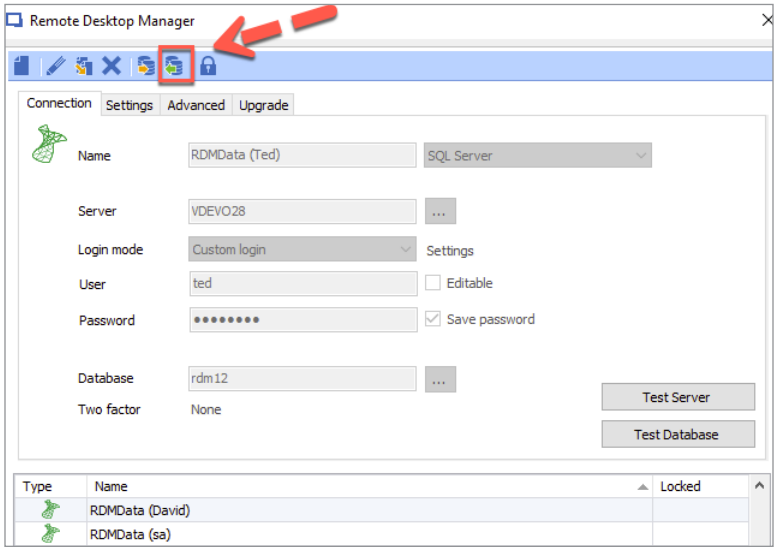
Next is the Data source definition. Using **File – Data sources.** You can see that **Custom login** is selected and that Ted's credentials have been entered. Please be aware that this is the screen appearing on the end user's screen. The credentials used to connect to the database are displayed in the **Settings** form.



In this screen, one can view the Username used to connect to the database. Note that the Password is not displayed and can not be revealed with any button or selection. Credentials can be overwritten by a user, but users of that category would not have access to that information.



As an administrator, there are two choices for providing the data source definition to their users, either by filling in everything but their own credentials, or filling in all the required information. The final decision will be dependent on the number of users. In either scenario, the button with the green arrow is needed to create the .rdd file.



For higher security, the account used to connect to the database should not be an account used to manage the entire SQL Server instance. Furthermore, using a distinct account to avoid confusing RDM's activity with other users is recommended if you do consult the SQL Server logs to monitor logins.