SQL Server® Management Studio Server-Side Actions

NOTES:

- The eNICQ 6 application performs database transactions using the following isolation levels: RepeatableRead, ReadUncommitted, Snapshot, ReadCommitted. The SQL Server® database must allow usage of each of these isolation levels.

- To perform the following steps, you will need to have SQL Server® Management Studio (SSMS) installed and connected with the instance of SQL Server® where the eNICQ 6 Database resides. If you do not already have a copy you can download the installer for SQL Server® Management Studio Express from Microsoft's website, https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver15.

- The following instructions should be carried out in SQL Server® Management Studio by a database administrator or IT professional with equivalent skills and permissions. These instructions focus on using Windows Authentication to manage database access. Additional options and tips are available in our documentation on troubleshooting database connectivity in eNICQ 6.

1. Open SQL Server® Management Studio.
2. Locate the **Security** folder at the server level in the object explorer.

   Note that there is also a Security folder at the database level under the eNICQ6db database, *but that is not the correct Security folder to perform these actions*.
3. Expand the **Security** folder. Under the **Security** folder you will see the **Logins** folder.
4. Right-click on the **Logins** folder and choose **New Login…**

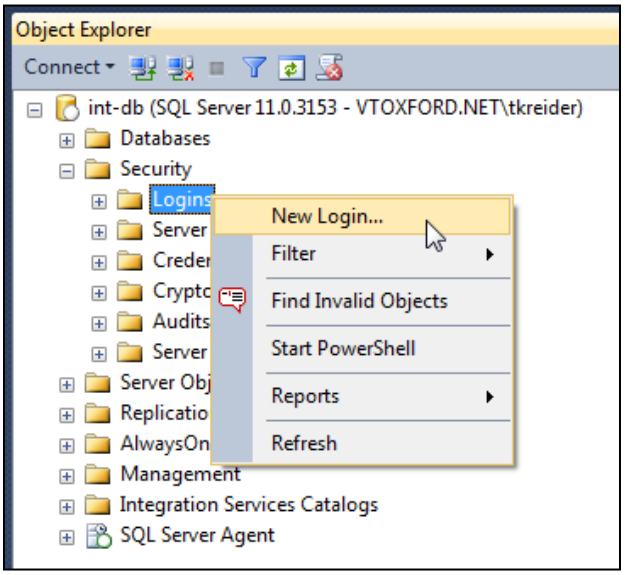

Figure 1 – Right click on the Logins folder located in the server Security folder, and select New Login

If the users have already been given permissions to another database on this server they will show in Logins already. Right click on them and select **Properties** and skip to step 19.

5. At the bottom of the **Login – New** dialogue, set the **Default database** to eNICQ6db unless you named it something other than the default name. In that case select the actual name of the database.

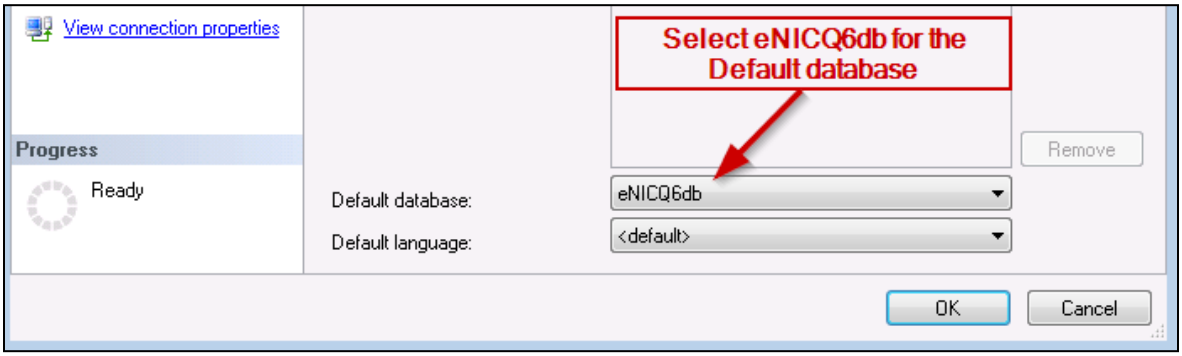

Figure 2 – Select eNICQ6db as the default database

6. Select the **Windows authentication** radio button.
7. Click the **Search** button

Figure 3 - – at the top of the same screen select Windows authentication, and click Search

8. Click **the Object Types** button on the **Select User or Group** dialog.

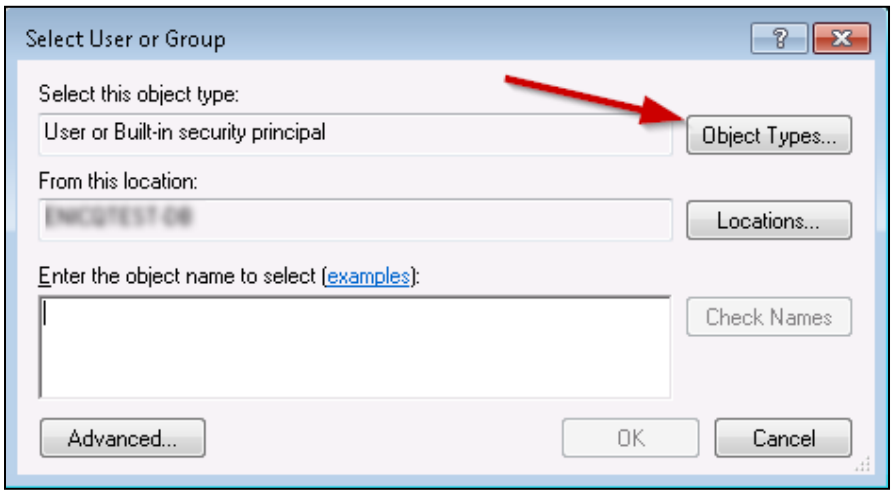

Figure 4 – click the Object Types button

9. Uncheck **Built-in security principals** and **Other objects**.

10. Check **Groups** and/or **Users**, whichever you are using. For multiple users, managing through group membership is recommended.

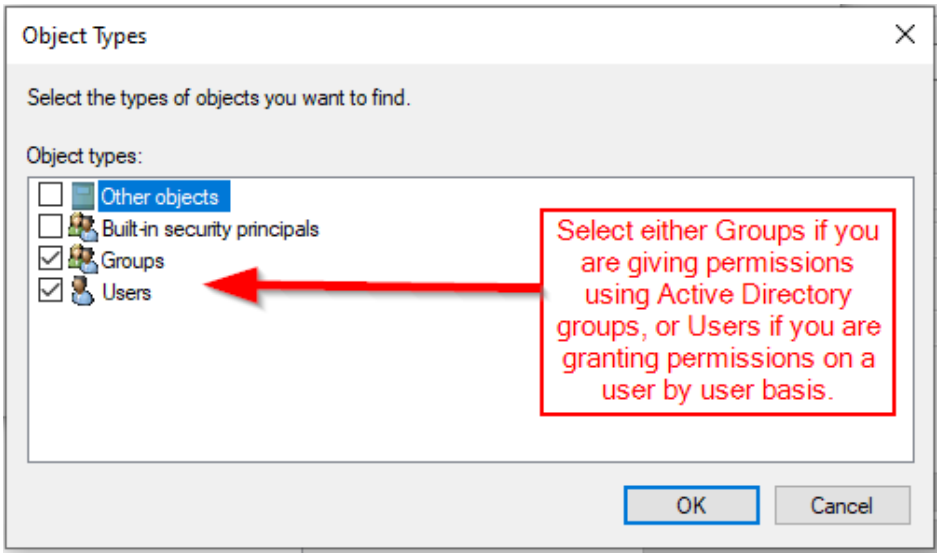

Figure 5 – unselect "Built-in security principals" and "Other objects" then select either Groups or Users

11. Click **OK** to continue.

12. On the **Select User, Service Account or Group** dialog Click **Locations…**

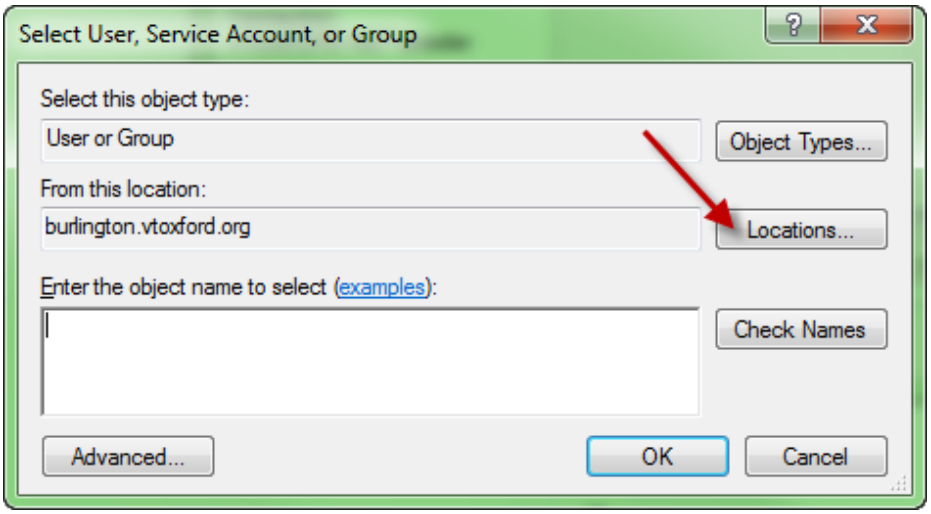

Figure 6 – Click "Locations…"

13. Select the location for the Windows account or group and click ok.

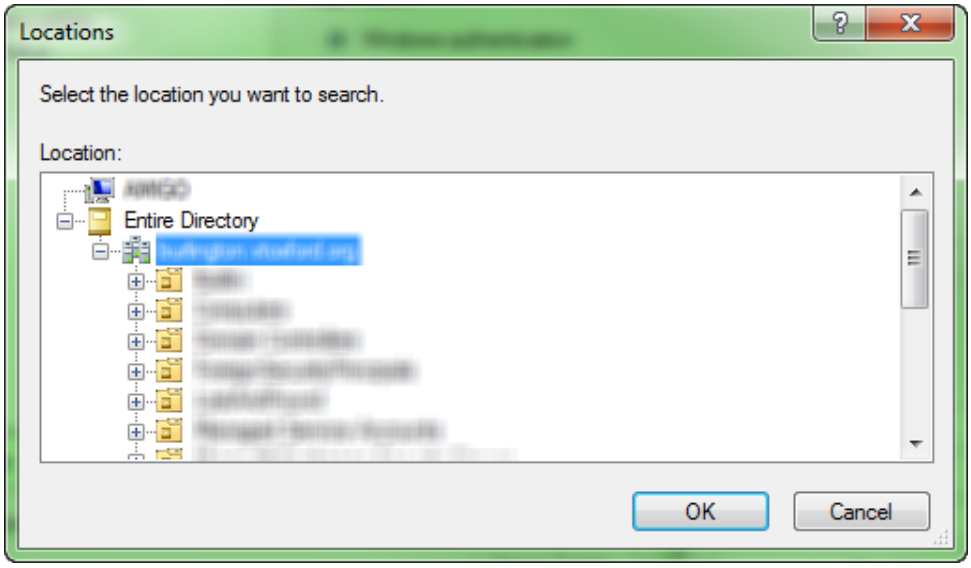

Figure 7 – After selecting the lcoations to find the user or group click OK

14. Enter the user or group in the space provided and click Check Names**.**

Figure 8 – Enter name of group or user and click Check Names. "enicquser" is only an example and will not be located on your network unless you create this user.

15. If you have been unable to identify the correct user or group, click **Advanced…** on the **Select User, Service Account or Group** dialog for more search options. Otherwise, continue to step 19.

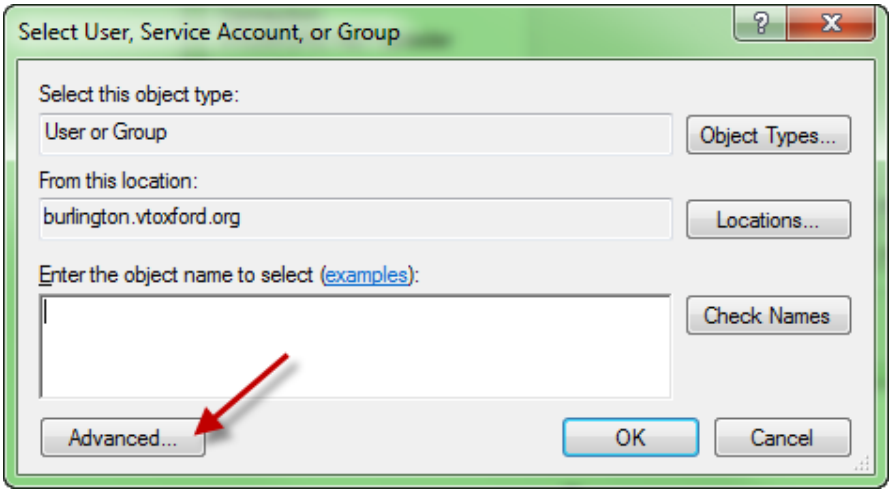

Figure 9 – Click the Advanced… button if the user or group is not found in previous step

16. Use the advanced features to find your user or group.

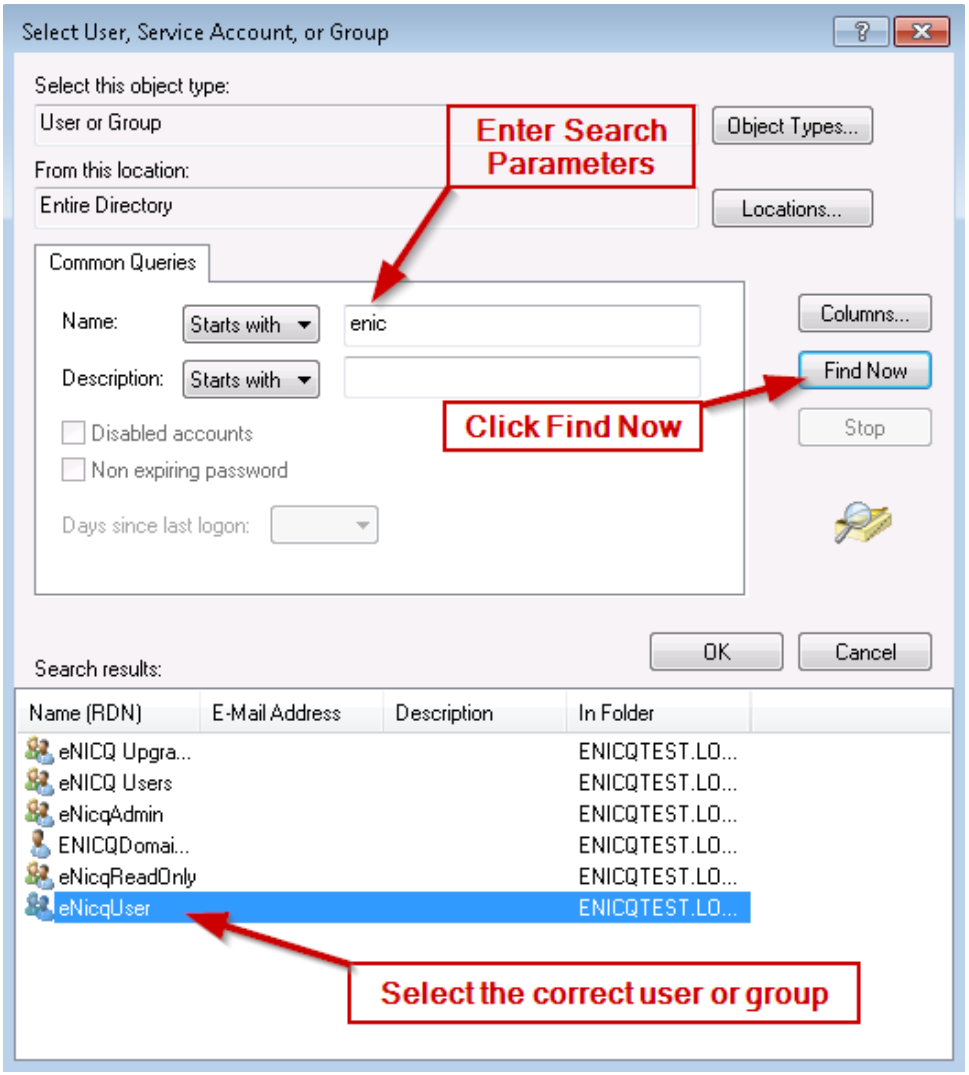

Figure 10 – Use the Common Queries fields to find the user or group, then select them at the bottom.

17. Please contact your System Administration team for assistance if you have difficulty with any of the following:
    - Locating the correct user or group.
    - Creating a user or group.
    - Adding or removing users to or from a group

18. On the **Login – New** screen, or the **Login Properties** screen if you are editing an existing user, click the **User Mapping** page.
19. Check the **eNICQ6db** database in the upper panel if you kept the default name. If changed the name to something other than the default look for that in the upper panel and select it.
20. Check the roles **EnicqDBUser** and **public** in the lower panel.

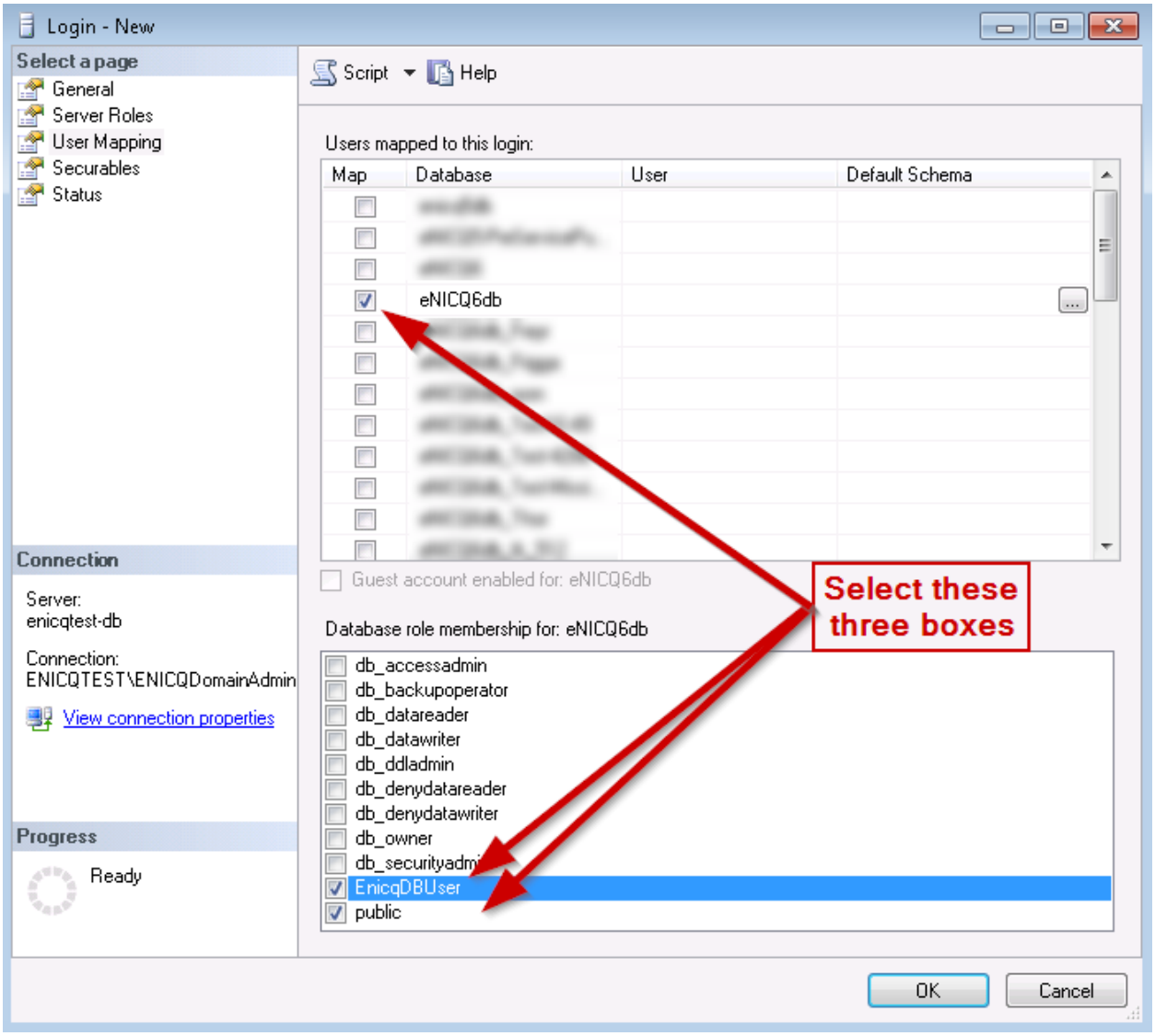

Figure 11 – Select User Mapping on the left. Make sure only the eNICQ 6 database is selected then select EnicqDBUser at the bottom (public should be selected by default already).

21. Click **OK** to complete Login creation.
22. Test the end-user's database authentication capability from the client machine by having the end user launch the application once it has been installed.

23. Set up SQL backups and secure your data according to your organization’s policies.