Problems, Causes and Solution

- **Problem**: When the computer reboots this error message "RISG-Database has stopped working" appears.
- **Problem**: The Odyssey Software takes 30 to 60 seconds to open
- **Problem**: Registry Access Denied

Problem: When the computer reboots this error message "RISG-Database has stopped working" appears.
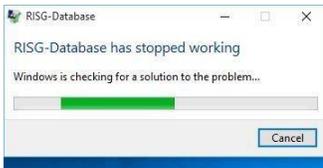
Cause: This message is cause by the **Database.exe** in the receptors folder not having administrator rights to run (execute) and failing to start.

Solution: Manually Start Database.exe, From the Windows Desktop, right click on the **RISG Menu icon** and select run as administrator from the pull-down menu and that should start **Database.exe** and finish the software installation.
OR
Go to Program Files\Receptors or Program Files (x86)\Receptors folder find and right click on **Database.exe** and then run as administrator that will start **Database.exe** and finish the software installation.

Problem: The Odyssey Software takes 30 to 60 seconds to open

Cause: The SQL Browser and the SQL Configuration TCP/IP settings are not enabled

Solution: Enable the SQL Browser and the SQL Configuration TCP/IP settings. To enable "Named Pipes and TCP/IP" connections in the configuration manager follow the above steps for **Configuring SQL Server 2019 Configuration Manager for TCP/IP access,** to enable or verify "SQL Browser" see below,

Scroll down to SQL Server Browser and right-click on it, in the pull down menu click on "Properties" set "Startup type" to Automatic and start the service once the SQL Server Browser is running click OK and exit.
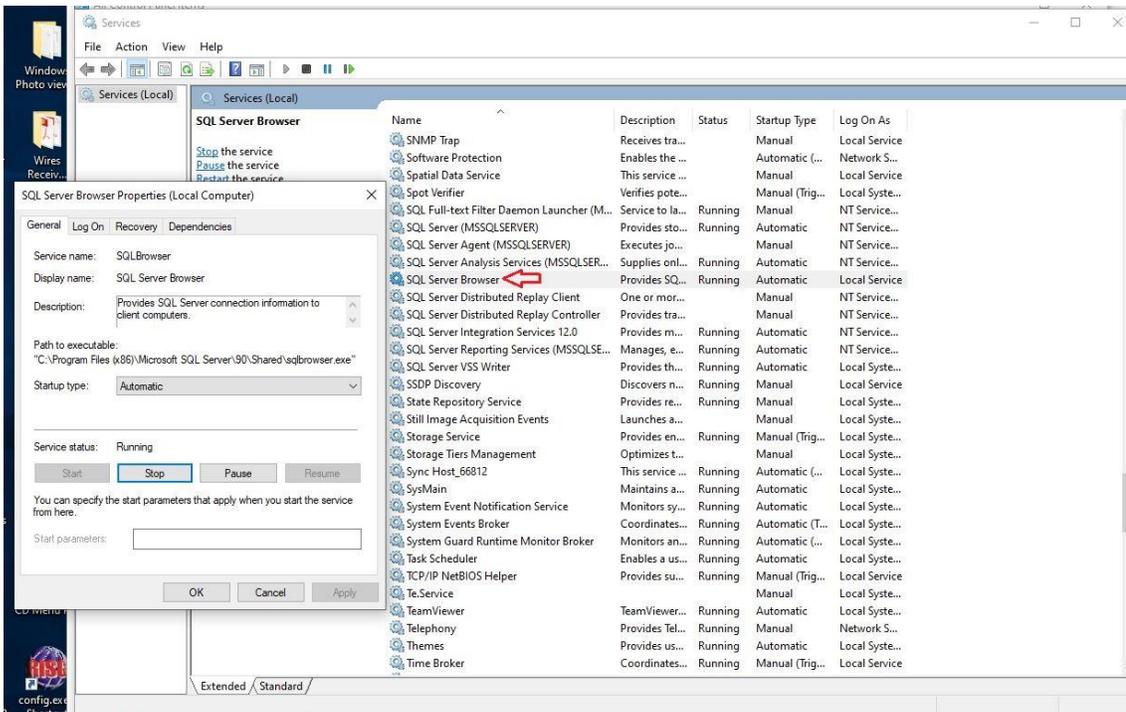
next under Administrator Tools click on SQL Server Configuration Manager to open

or go to Start\Menu\ Microsoft SQL Server 2014 and open SQL Server 2014 Configuration Manager

Click on the > sign for SQL Server Network Configuration click on Protocols for MSSQLSERVER
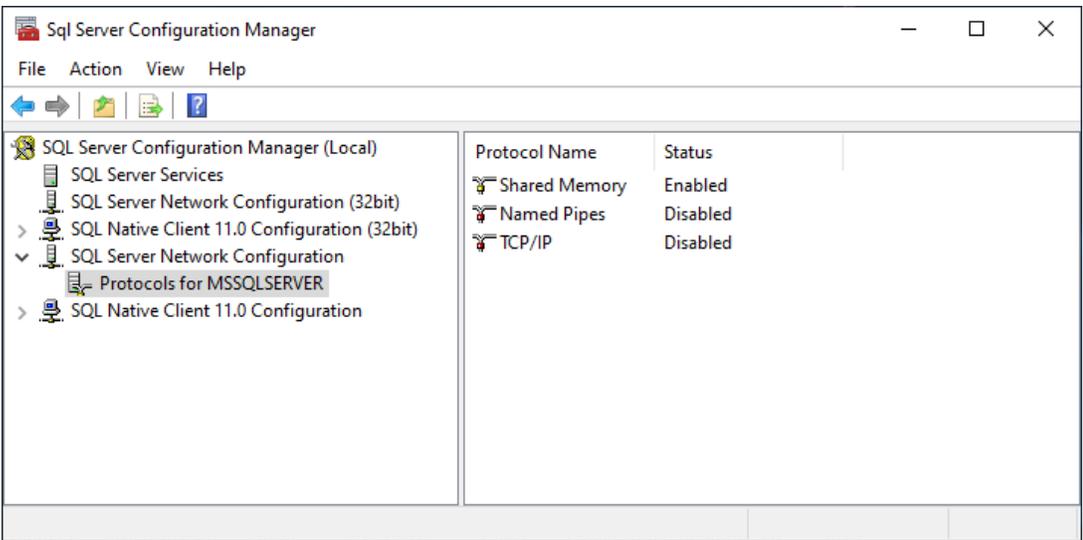
In the right side of the page right click on Named Pipes click on Enable, do the same for TCP/IP.
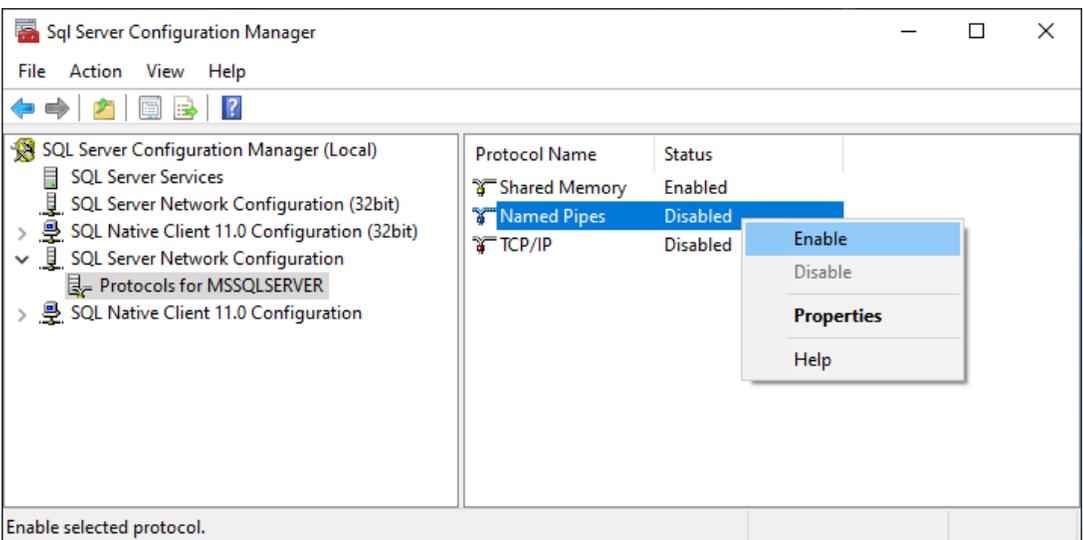
After TCP/IP and Named Pipes are enabled, Open SQL Native Client 11.0 Configuration (32bit) / Client protocol and SQL Native Client 11.0 Configuration / Client protocol Verify TCP/IP and Named Pipes are enabled
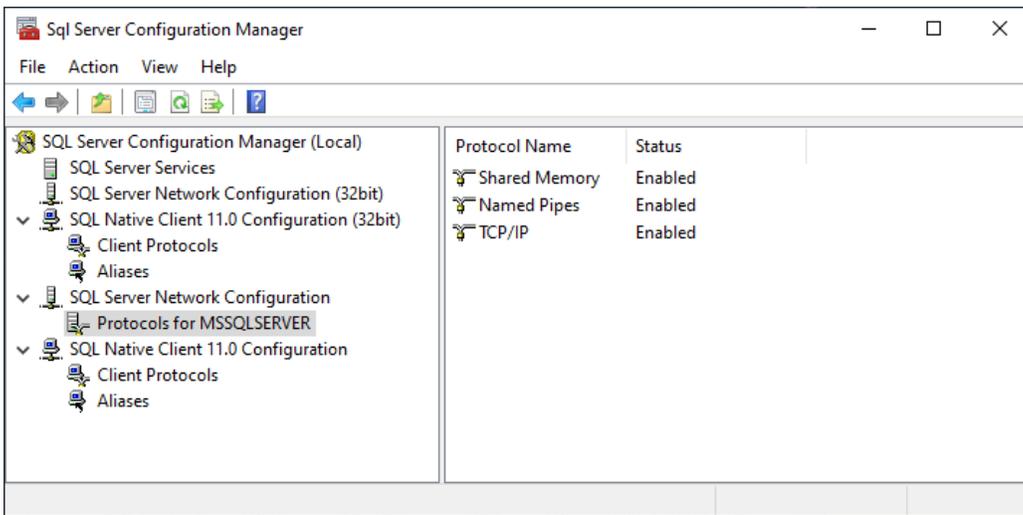
Verifying TCP/IP and Named Pipes are enabled
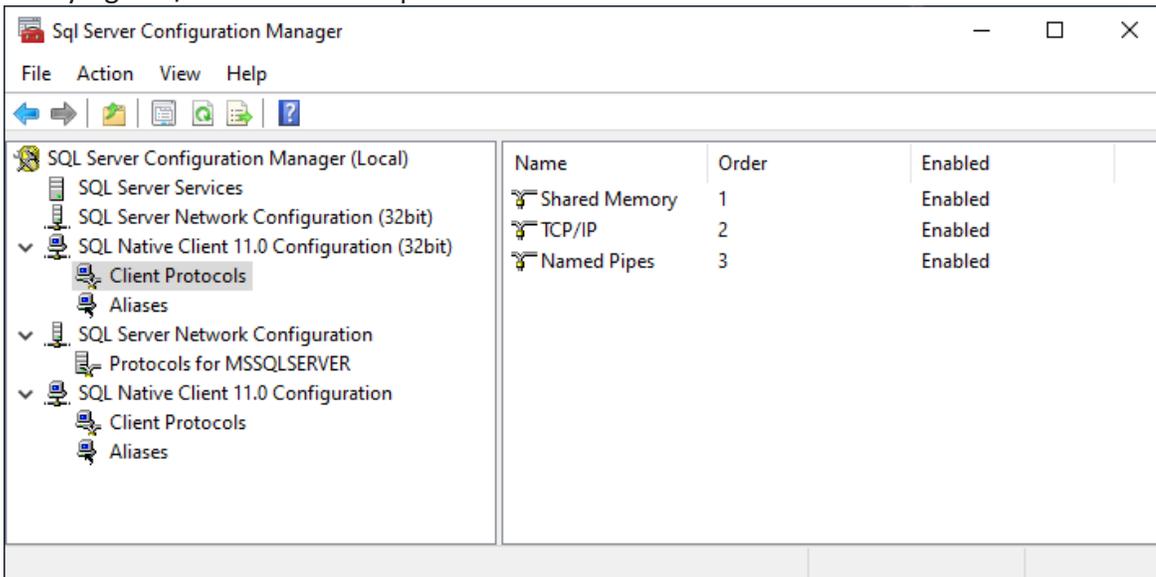
When finish close out the box and restart the computer so the new settings take effect. After the Server has rebooted, start services 2 and 3 verify they are running and then go to the workstation and install the software.

Problem: Registry Access Denied

Cause: Permissions for ris_group or individual users needs to be check the

Solution: Permissions for ris_group or individual users needs to be check, added and verified in the following places in the Windows Software, 1 place in SQL Management Studio,
Registry 4 places
   a. HKEY_LOCAL_MACHINE\SOFTWARE\ReceptorsInc
   b. HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ReceptorsInc

    c. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RidbioService

    d. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RiGP4Service

Windows file 2 places

    e. The hosts file @ C:\Windows\System32\drivers\etc

    f. The services file @ C:\Windows\System32\drivers\etc

Receptors Folder 1 place

    g. The Receptors folder @ C:\Program Files\Receptors (for 32-bit systems)

    h. The Receptors folder @ C:\Program Files (x86) \Receptors (for 64-bit systems)

First Registry settings (4 places),

Type **regedit** in the open box.
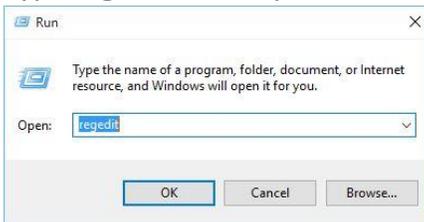
Go to

    a. **HKEY_LOCAL_MACHINE\SOFTWARE\ReceptorsInc** and right click on **ReceptorsInc** and click on **Permissions.**
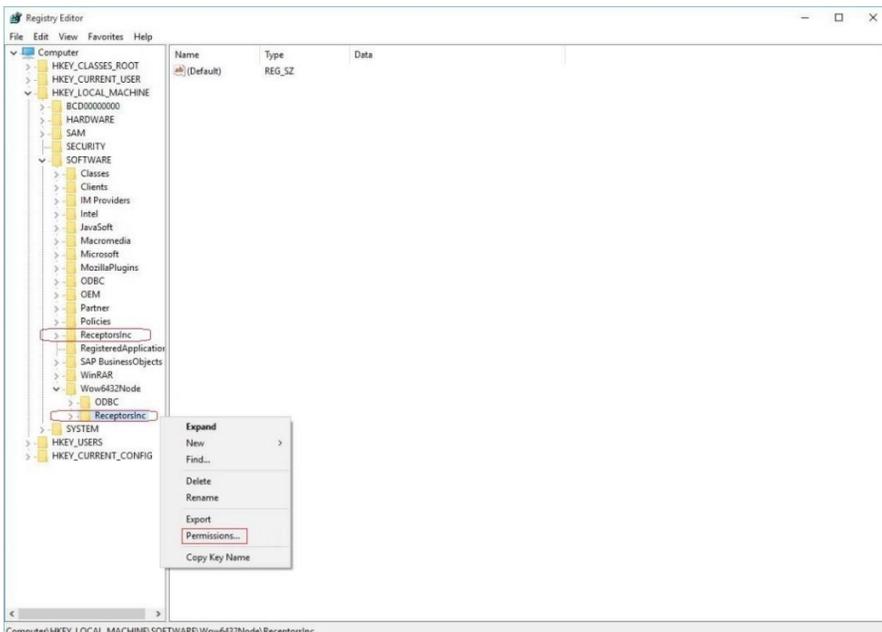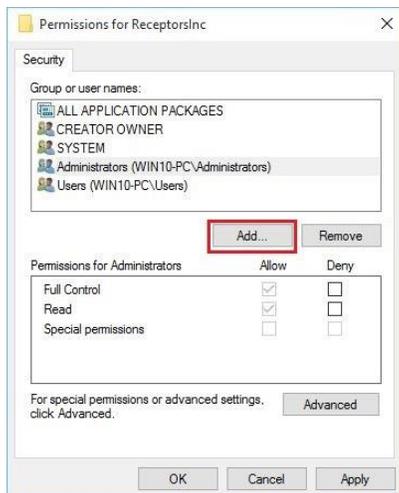
Click on **Add**   Click on **Advanced**
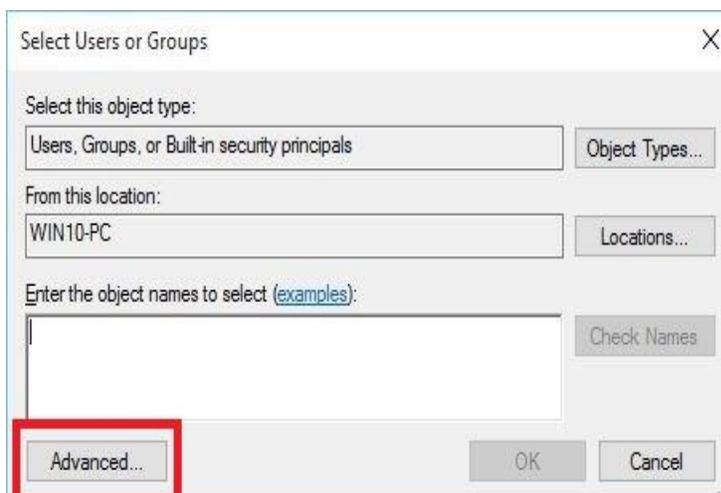
Click on Find Now and select ris_group
from the list click **OK**.   Allow Full Control and Read permissions click **OK,**
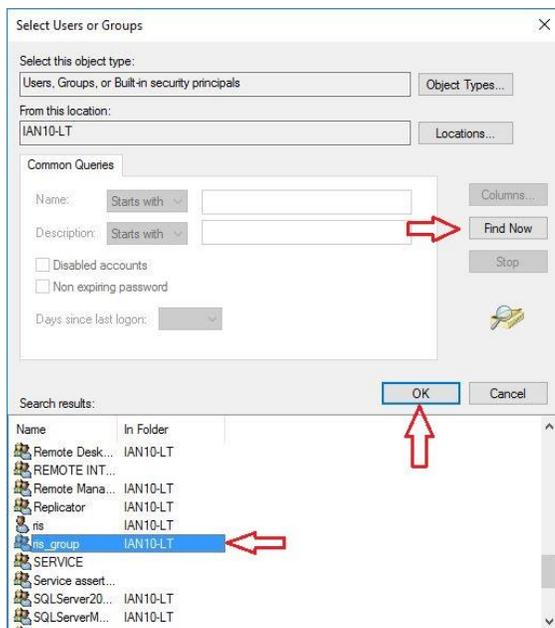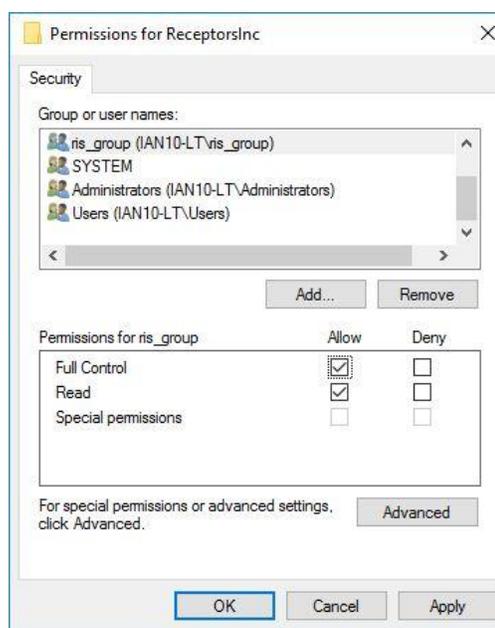
Repeat steps for,
  a. HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\
  b. ReceptorsIncHKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RidbioService
  c. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RiGP4Service

Windows file 2 places
  d. The hosts file @ C:\Windows\System32\drivers\etc
  e. The services file @ C:\Windows\System32\drivers\etc

Adding ris_group to etc\host and services file.
Go to **C:\Windows\System32\drivers\etc** right click on **hosts\properties\Security** and repeat steps from
above, Repeat for services file.
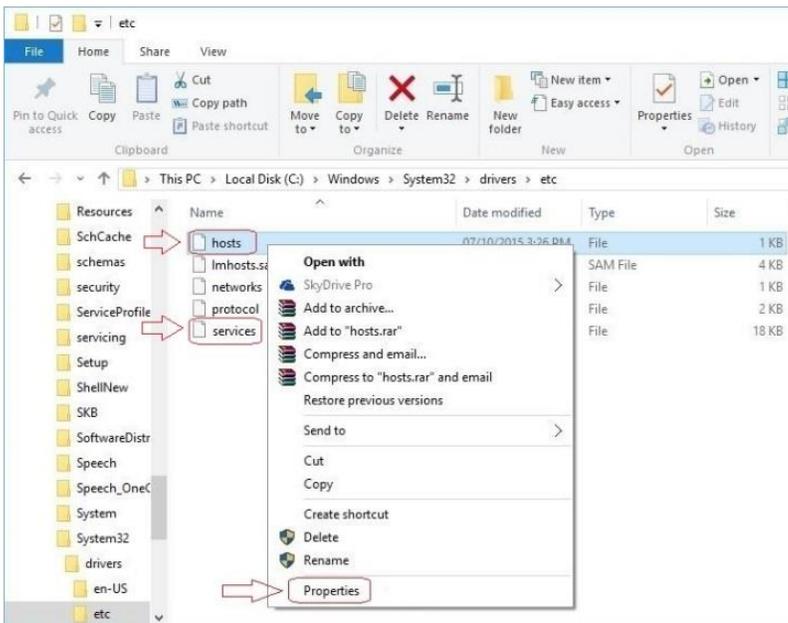
Adding ris_group to the receptors folder @
   a. C:\Program Files\Receptors (for 32-bit systems)
   b. C:\Program Files (x86) \Receptors (for 64-bit systems)

Right click on **Receptors** go to **Properties\Security** click on add and repeat the steps from above.
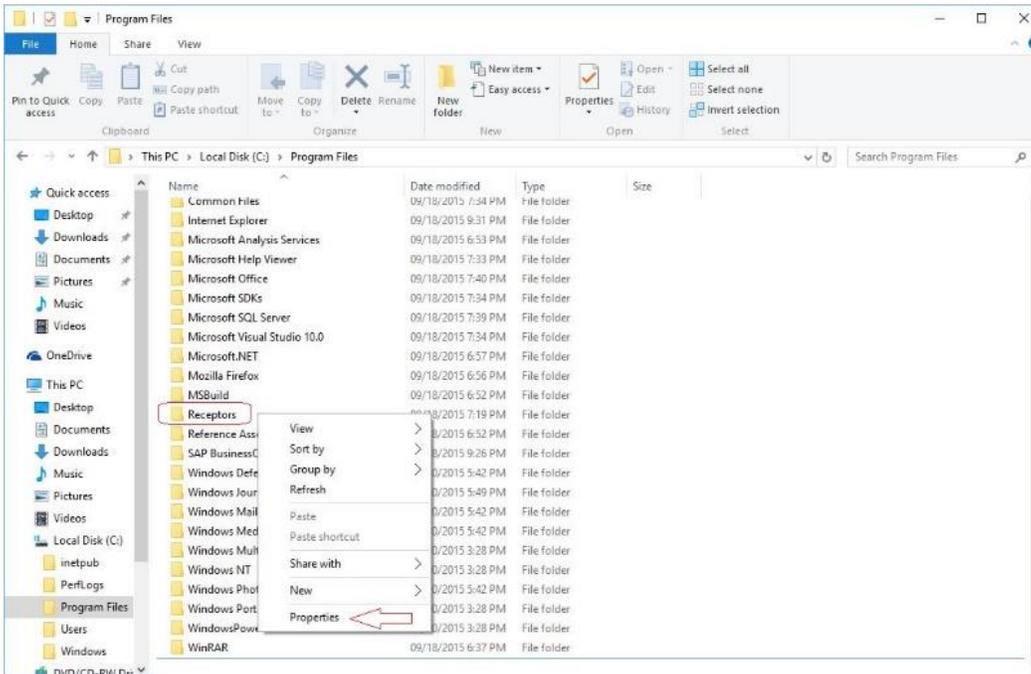
Verify the ris_group was added to **SQL Server** and mapped to the **ris database**

Checking SQL Management Studio for login accounts and permissions for local accounts. We are adding the **ris account** as a login in the example below.

On the Desktop click on "RISG Main Menu" Icon under Administrator Tools click on SQL Server Management Studio to open SQL.

Verify the server name and then click Connect
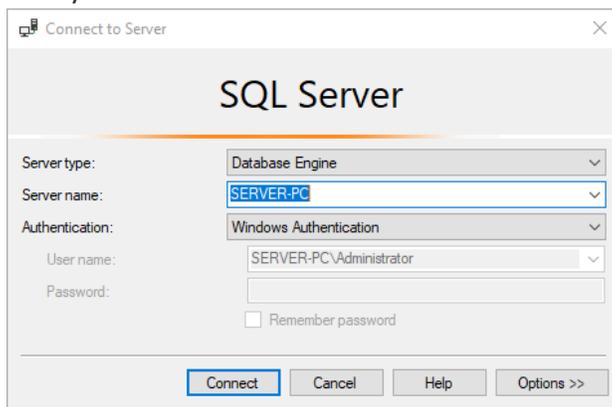
Once SQL Management Studio is open In the left-hand column open **Security** then right click on **Logins**. We are going to verify user mapping for ris_group, NT AUTHORITY\SYSTEM, any users and groups (local and domain) that need access to the ris database.

Verify,

1. ris_group
2. NT AUTHORITY\SYSTEM
3. All Users or Company groups

Right-Click on ris_group\Login Properties\User Mapping
Verify the ris_group mapping to the ris database,

Check the box next to ris, in the table below leave **pubic** checked and select,
db_datareader,
db_datawriter and
db_owner
Click OK,

Verify user mapping for **NT AUTHORITY\SYSTEM** this login is needed for running the services automatically (in the background).
Click OK when finish repeat for any users and groups (local and domain) that need access to the ris database.
for and exit from SQL Management Studio
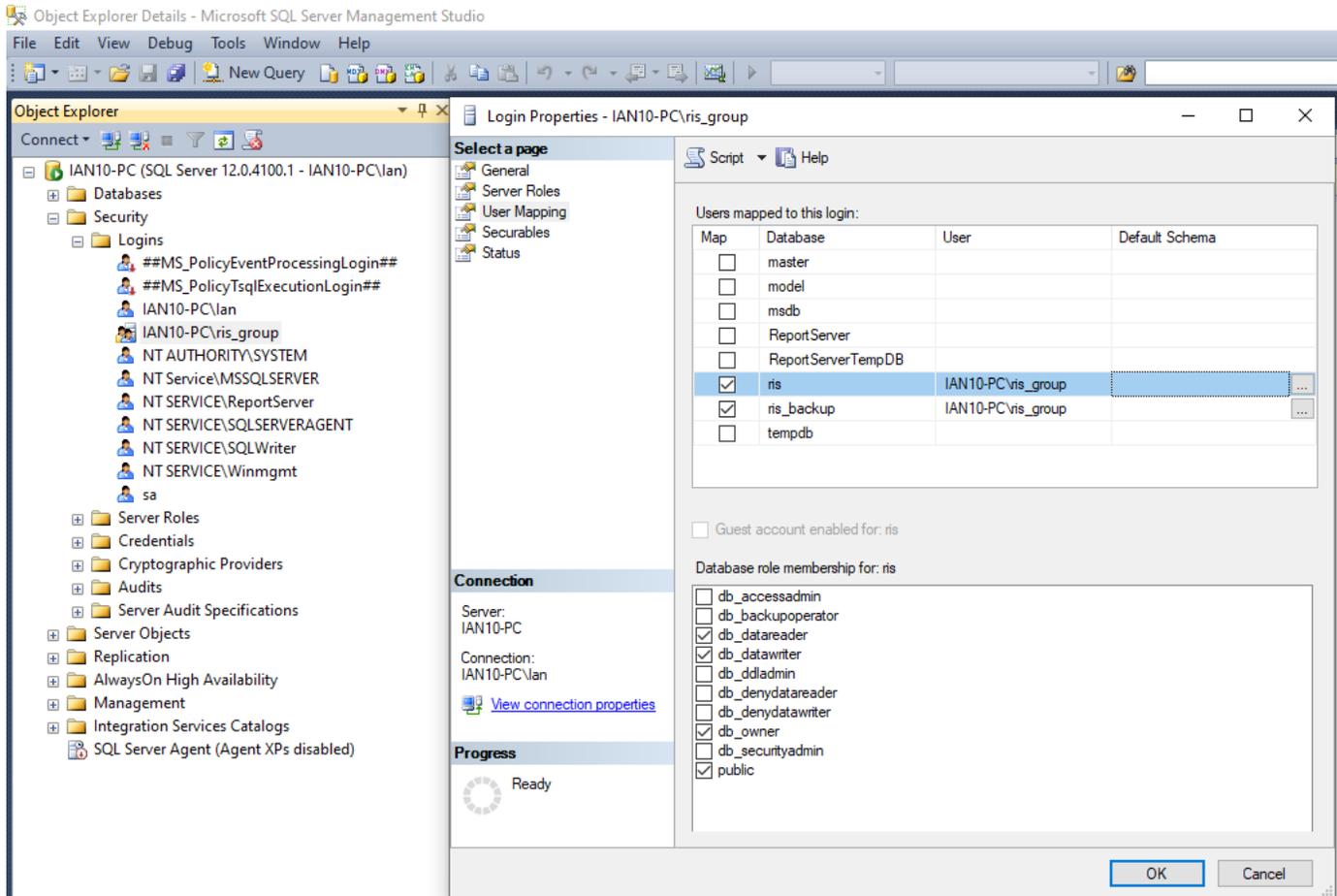
REBOOT the COMPUTER so the new settings will take effect.