December 12, 2008

Integrated Security for Shared ECMPS Client Tool Databases

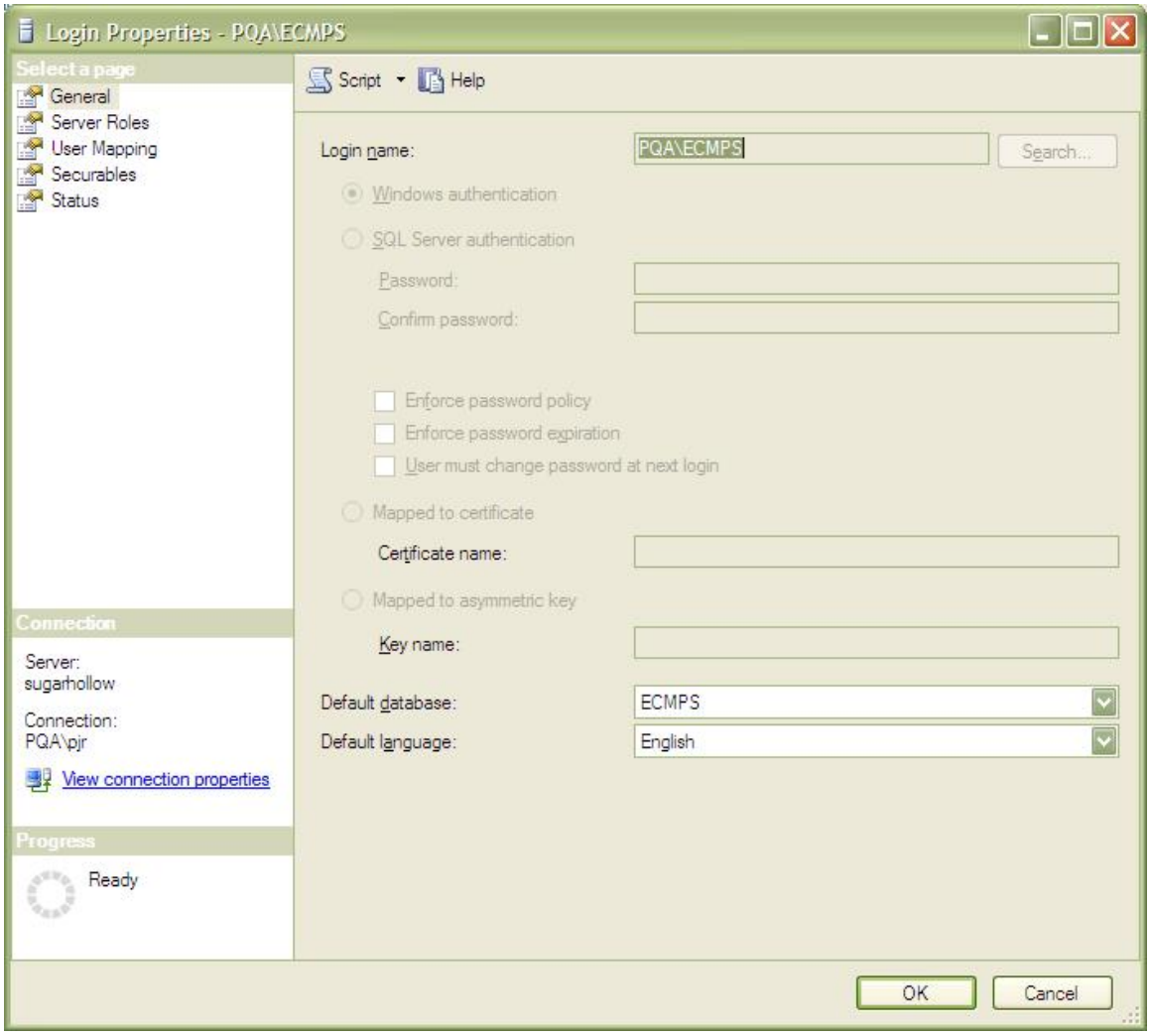
To implement integrated security for shared ECMPS Client Tool databases on a SQL Server, please perform the following steps:

1. Login

Add login to SQL Server.

Note: It is recommended that a domain/active directory group (or server local group) be created. The ECMPS users would be added in this step.

Figure 1
Add Login

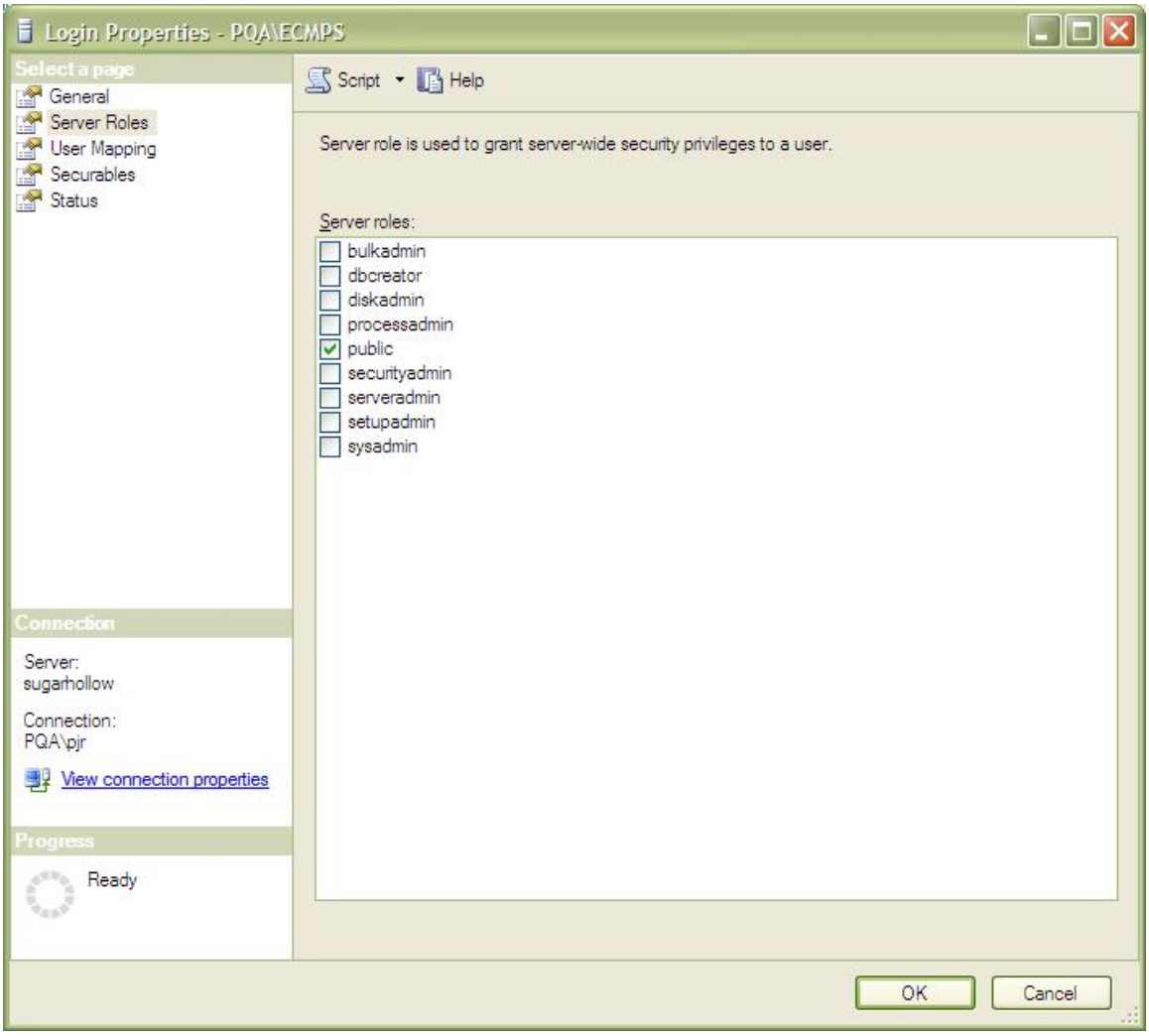


2. Server Role

Select the Server Role [public].

Note: The "sysadmin" server role is not required or recommended.

Figure 2
Server Role



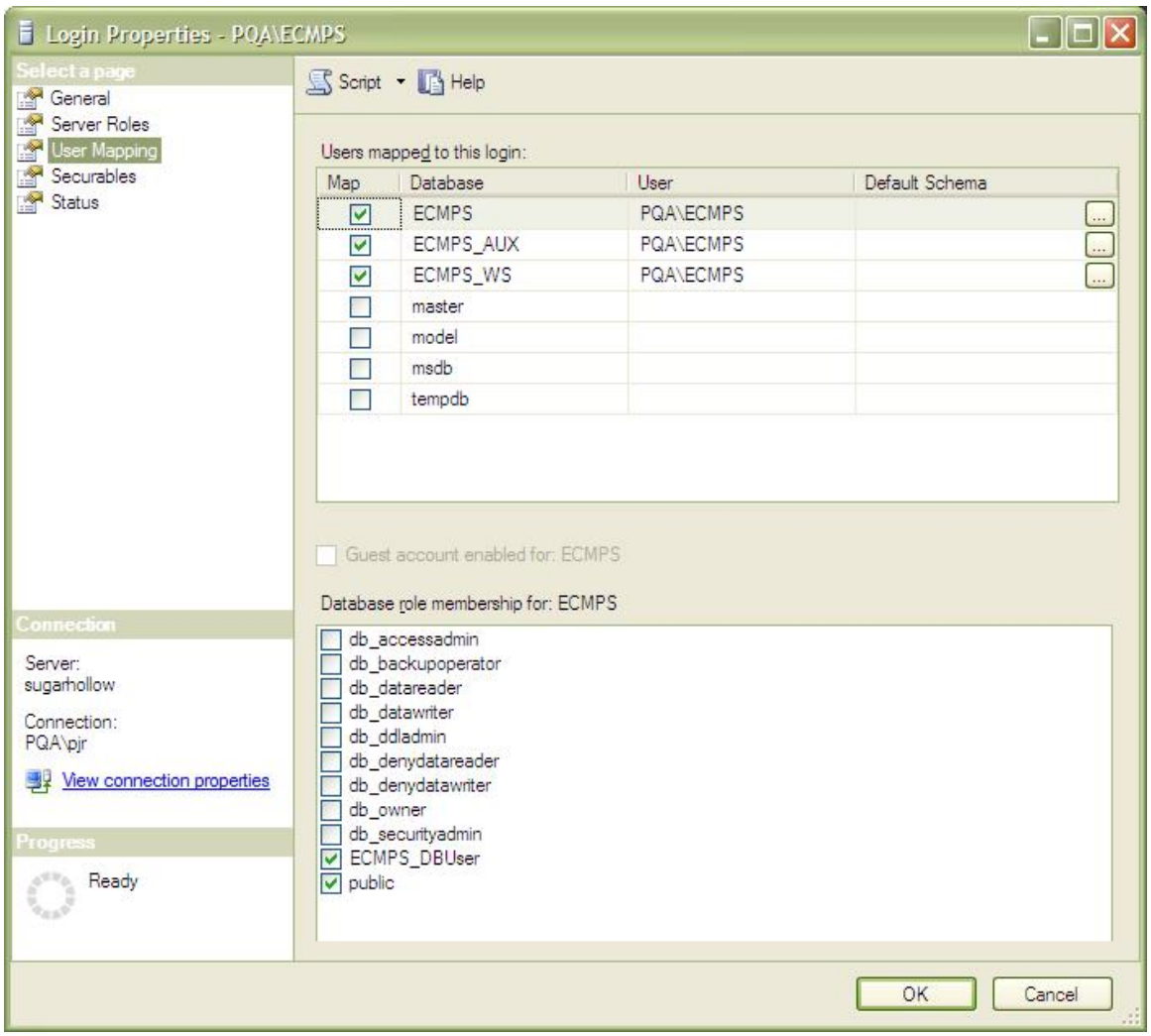
3. User Mapping

Select the following User Mapping settings:

Users: ECMPS, ECMPS_AUX and ECMPS_WS
Database role membership: ECMPS_DBUser and [public]

Note: In the 2008 Q4 release of ECMPS, a new database role called ECMPS_DBUser has been created for each of the three ECMPS databases. This role is made up of the system roles "db_datareader" and "db_datawriter." This new database role owns all schemas for the 2008 Q4 release. The ECMPS_DBUser has access to all data in the three ECMPS databases, but does not have access to any databases that are not mapped or permission to alter the database structures. &

Figure 3
Select User Mapping



4. Grants (Optional)

ECMPS has implemented locking of facilities using the built-in stored procedure sp_GetAppLock. For this to work optimally, the DBA should grant VIEW SERVER STATE to [login from step1]. ECMPS will not be adversely affected if this grant is not applied, but certain messages about locking resources may not be as detailed.