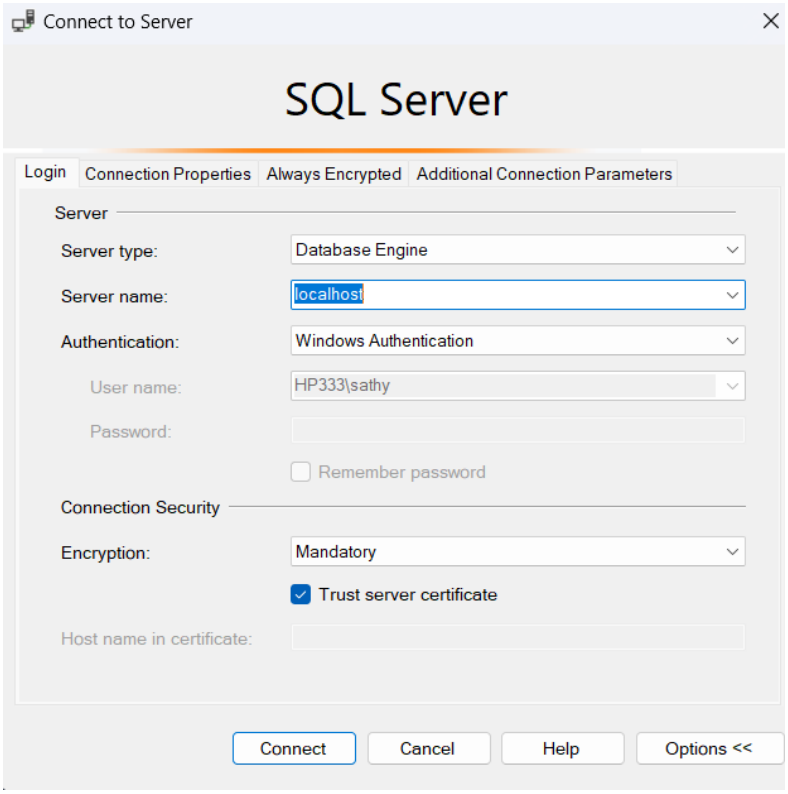
SQL SERVER USER MANAGEMENT AND ACCESS CONTROL

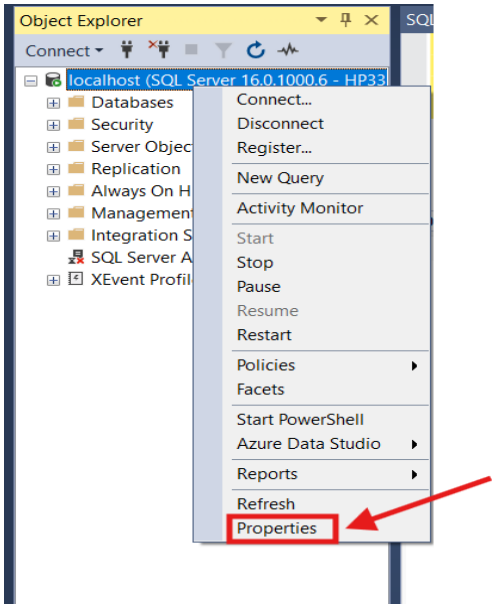
Step 1: Connect to your Microsoft SQL Server DB

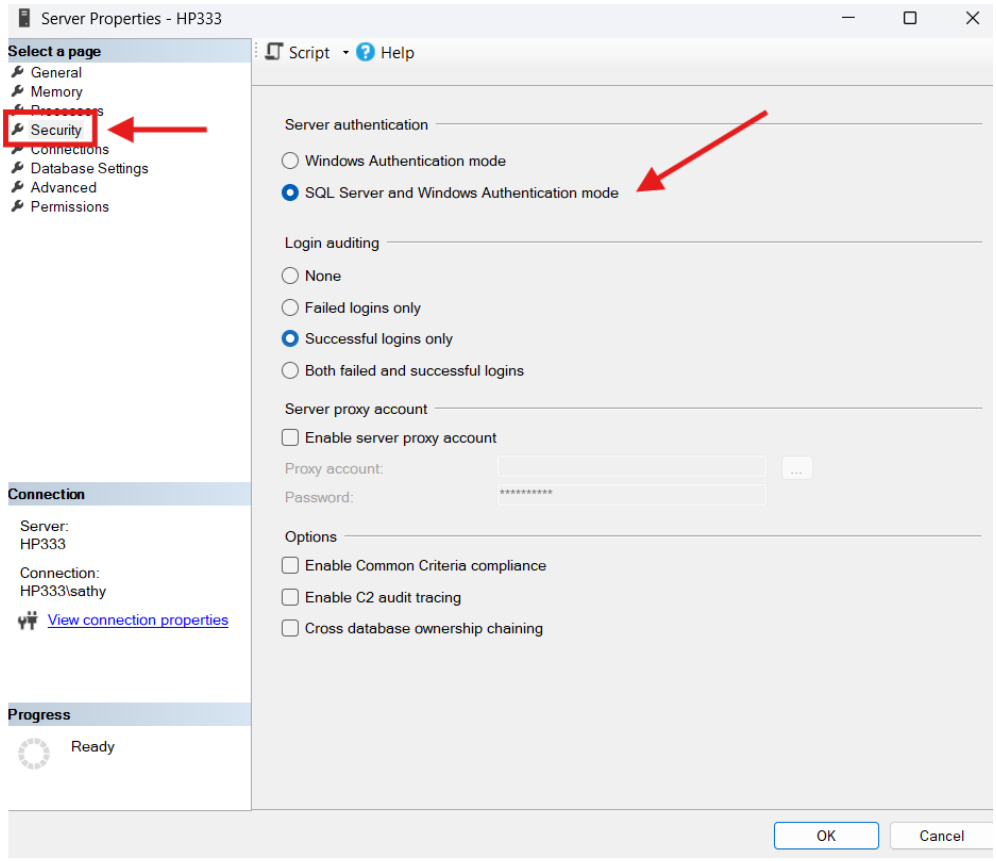


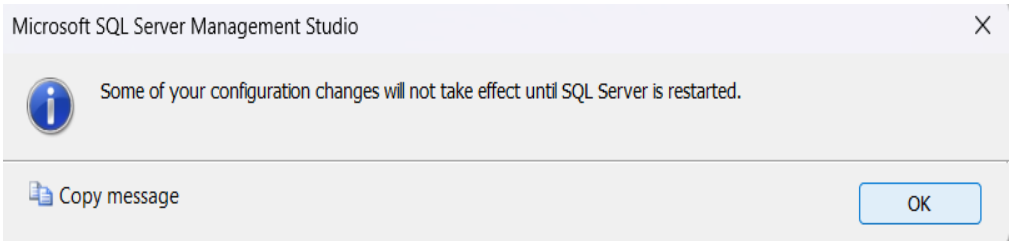
Step 2: Set up a sample database where the user you create will have access to resources and can perform operations within that specific database.

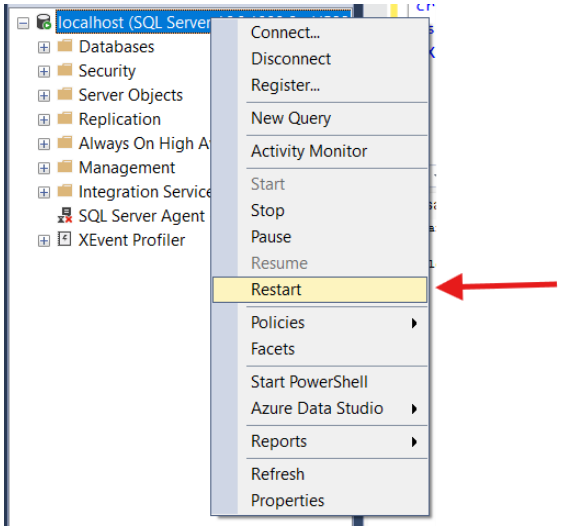
```
create database demo_db;
```

Step3: Perform the following configurations



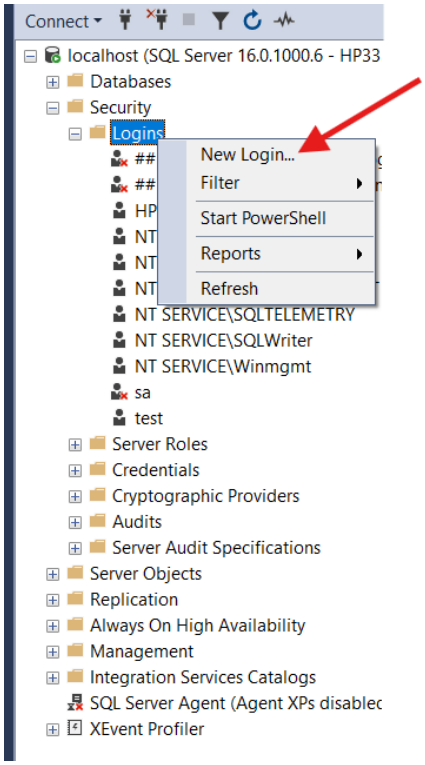

Server Properties - HP333
Select a page
General
Memory
Processors
Security
Connections
Database Settings
Advanced
Permissions
Script
Help
Server authentication
Windows Authentication mode
SQL Server and Windows Authentication mode
Login auditing
None
Failed logins only
Successful logins only
Both failed and successful logins
Server proxy account
Enable server proxy account
Proxy account:
Password:
Options
Enable Common Criteria compliance
Enable C2 audit tracing
Cross database ownership chaining
Connection
Server:
HP333
Connection:
HP333\sathy
View connection properties
Progress
Ready
OK
Cancel

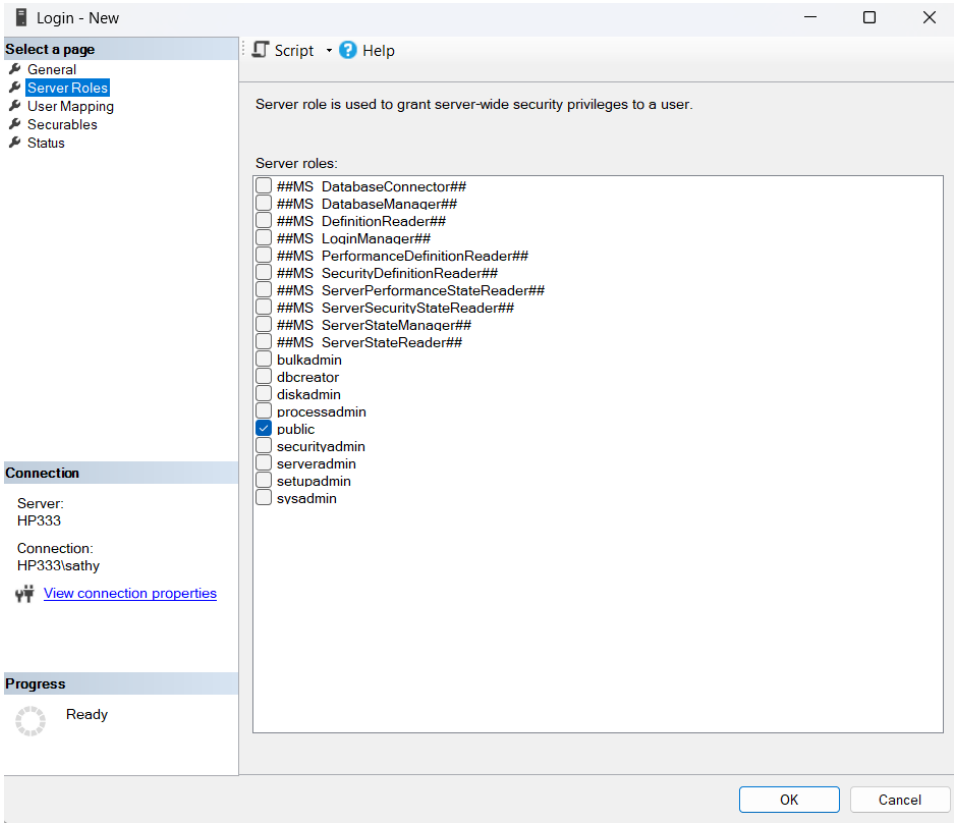

Microsoft SQL Server Management Studio
Some of your configuration changes will not take effect until SQL Server is restarted.
Copy message
OK

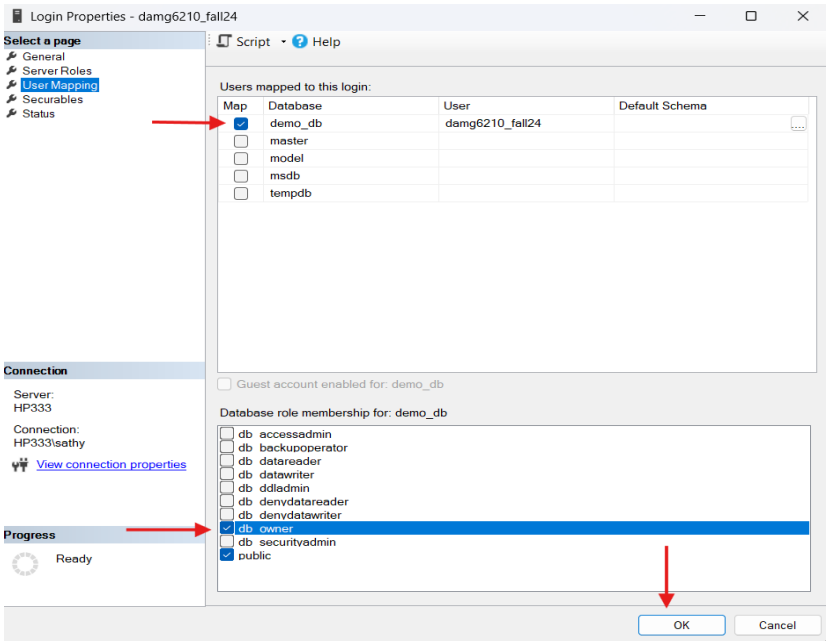

Databases
Security
Server Objects
Replication
Always On High A
Management
Integration Servic
SQL Server Agent
XEvent Profiler
Connect...
Disconnect
Register...
New Query
Activity Monitor
Start
Stop
Pause
Resume
Restart
Policies
Facets
Start PowerShell
Azure Data Studio
Reports
Refresh
Properties

Step 3: (Follow either of the below methods (1 --> UI, 2 --> SQL)

Method 1 (UI based)



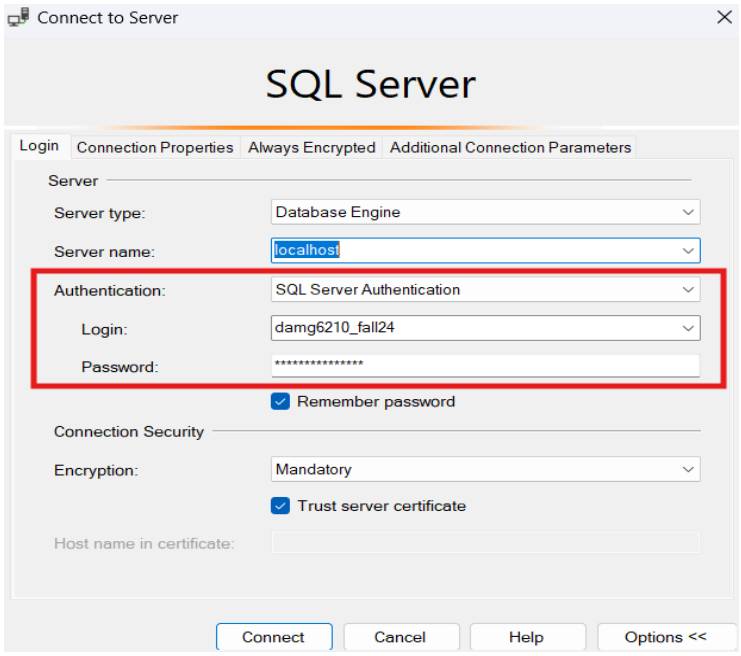




Method 2 (SQL based): Execute the following script (Replace the object names with your preferred choices)

```
create login damg6210_fall24 with password = 'Damg6210_Fall24';
create user damg6210_fall24 from login damg6210_fall24;
use demo_db;
EXEC sp_addrolemember 'db_owner', 'damg6210_fall24';
```

Step 4: Test your connection (Make sure you use Windows Authentication)



You're all set once you successfully establish the connection!