Managing Security and permissions

Step-by-Step Guide Using SSMS 2022 GUI

1. Create Logins

- Open SSMS and connect to your SQL Server instance.
- Expand Security > Logins.
- Right-click Logins and select New Login.
- Enter the login name, set authentication type (Windows or SQL Server), and set a password.
- Click OK.

2. Create Database Users

- Expand your database under Databases.
- Expand Security > Users.
- Right-click Users and select New User.
- Enter the user name and select the login from the drop-down.
- Click OK.

3. Create a Database Role

- Expand your database > Security > Roles > Database Roles.
- Right-click Database Roles and select New Database Role.
- Enter the role name and select the owner.
- Click OK.

4. Assign Users to the Role

- Expand Database Roles, right-click the role you created, and select Properties.
- Go to the Members page.
- Click Add and select the user to add.
- Click OK.

5. Grant Permissions

- Expand Database Roles, right-click the role, and select Properties.

- Go to the Securables page.
- Click Search, select All objects of the types..., and choose the objects (e.g., tables, views).
- Click OK.
- Select the permissions (e.g., SELECT, INSERT, UPDATE, DELETE) and click OK.

6. Deny Access for Others

- For users who should not have access, do not create a database user or role membership.
- If a user already exists, right-click the user, select Properties, and under Securables, explicitly deny permissions.

7. Audit and Review

- Regularly review users and roles under Security > Users and Roles.