Your web application should be run with the smallest set of rights that allow the application to function correctly. For example, a web application should NOT have access anywhere outside of the web application space. If attackers happen to find a flaw in the web application, at least they will not gain access to sensitive information stored on the server (for example the SAM database, where user passwords are stored).

You should explicitly ensure that:

- IIS runs under a custom low-rights user account.
- The IIS application pool runs under a correctly configured user account. We recommend creating a custom user account with minimum rights. See Specify an Identity for an Application Pool (IIS 7).
- The SQL Server Services run under separate low-rights Windows or Local user accounts. See Configure Windows Service Accounts and Permissions.
- Unsafe SQL functions, like xp_cmdshell(), are not enabled.

Minimal Kentico requirements

Below you can find the minimal configurations for SQL and IIS user accounts required to work correctly with Kentico.

Minimal configuration for SQL user accounts

Instead of assigning users to the **db_owner** database-level role, we recommend setting permissions according to the operations that the user account must perform:

Operations	Required permissions
Actions related to **browsing on the live website**	Connect, Delete, Execute, Insert, Select, Update
Managing of **Forms**, **Page types**, **Custom tables** or **Module classes**	Alter schema, Connect, Create table, Create view, Delete, Execute, Insert, Select, Update
Working with the **Database objects** application	Connect, Create procedure, Delete, Execute, Insert, References, Select, Update
Creating a database	Alter, Connect, Delete, Execute, Insert, References, Select, Update

To limit the permissions for an SQL user, you have to first create a new SQL login in SQL Management Studio, map it to the database and then assign the permissions for this login. For information about creating logins in SQL Management Studio, see Create a Login.

Minimal configuration for IIS user accounts

- The account must have **Read**, **Write**, **Modify** permissions for the website directory.