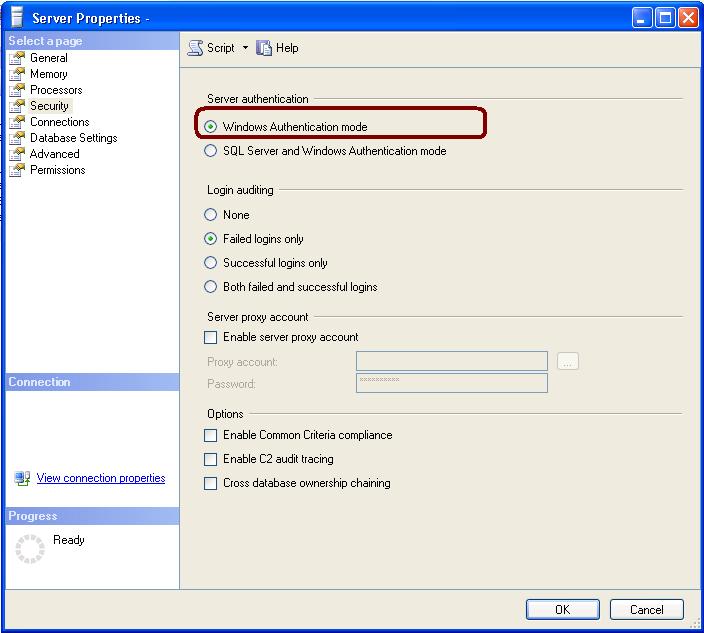
**Choosing authentication for SQL Server**

During the installation of SQL Server, an option for security is asked for, that is, the type of authentication you want SQL to apply; either Windows Authentication mode and mixed mode



If you chose Windows Authentication mode, then Windows Authentication will disables SQL Server Authentication by default

If you chose mixed mode (Windows Authentication and SQL Server Authentication) then you must provide and then confirm a strong password for the built-in SQL Server system administrator account named sa.

Because the sa account is well known and often targeted by malicious users, do not enable the sa account unless your application requires it and even then be very careful in giving it out. I create another account and give it sysadmin rights if need be. Ideally, you should not activate the sa account and if you do, rename the sa account.

[**Verifying connection via Windows Authentication**](javascript:void(0))

When a user connects through a Windows user account, SQL Server validates the account name and password using the Windows principal token in the operating system. As Windows authentication has built in security protocol, password policy enforcement, complexity for strong passwords, support for account lockout, and supports password expiration it’s recommended over SQL Authentication

[**Verifying connection via SQL Authentication**](javascript:void(0))

When using SQL Server Authentication, logins are created in SQL Server that is not based on Windows user accounts. Both the user name and the password are created by using SQL Server and stored in SQL Server.

**Some** [**Reasons to use SQL Server Authentication**](javascript:void(0))

* Support older applications
* Third parties applications that require SQL Server Authentication
* Supports mixed operating systems, where all users are not authenticated by a Windows domain
* Support Web-based applications where users create their own identities
* Allows software developers to distribute their applications by using a complex permission hierarchy