



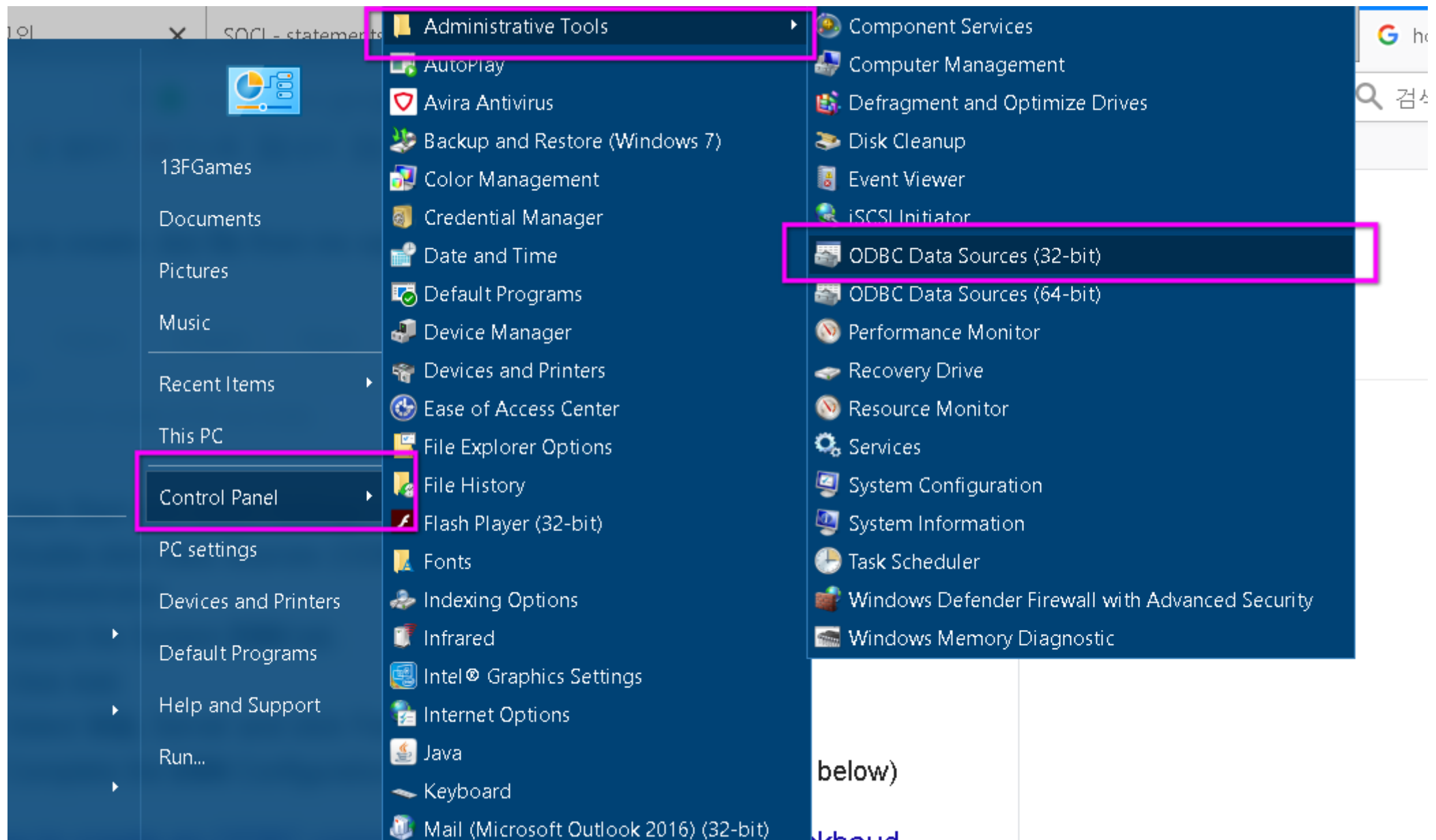
DIVISION OF
DIGITAL CONTENTS
DONGSEO UNIVERSITY

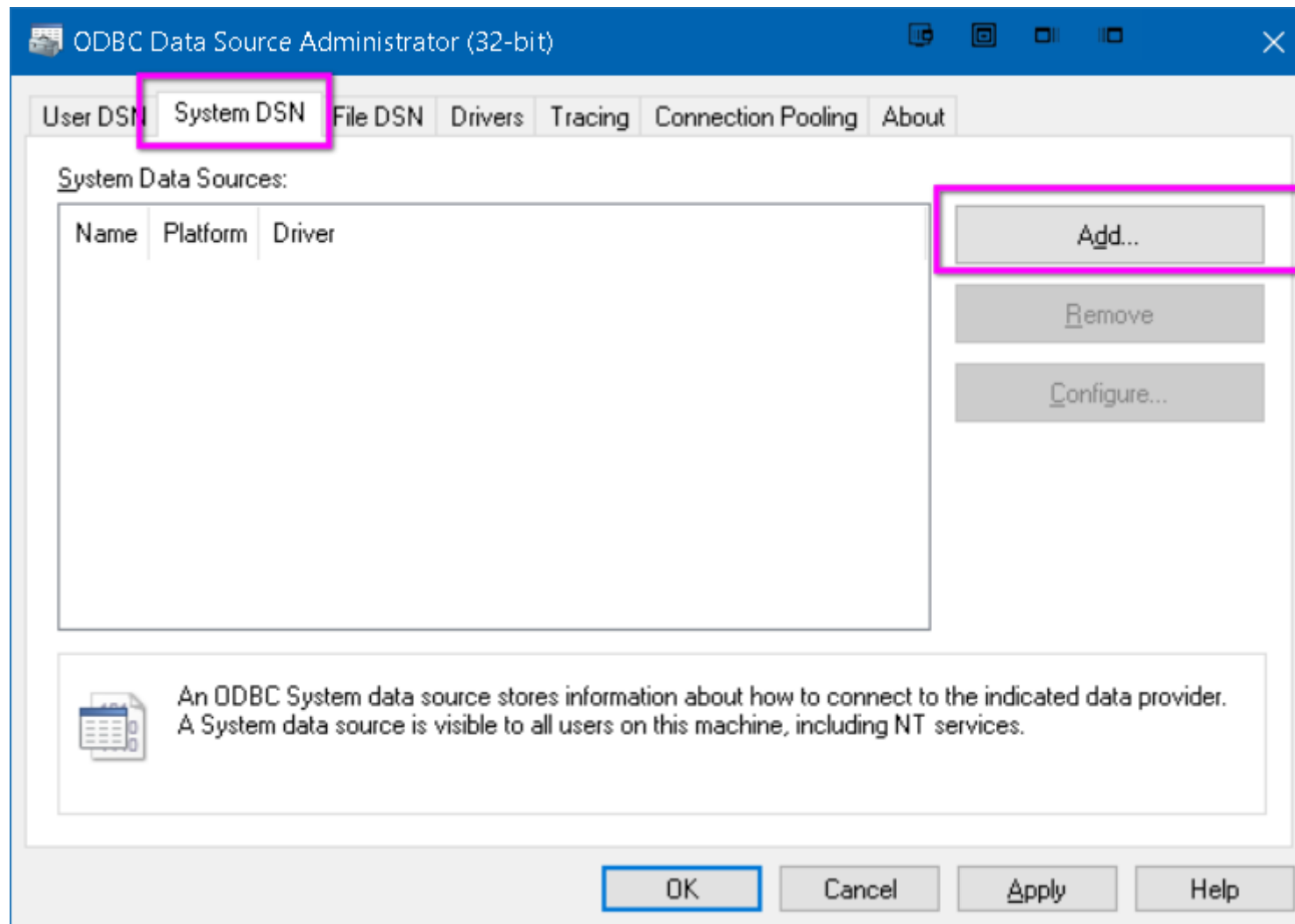
Database

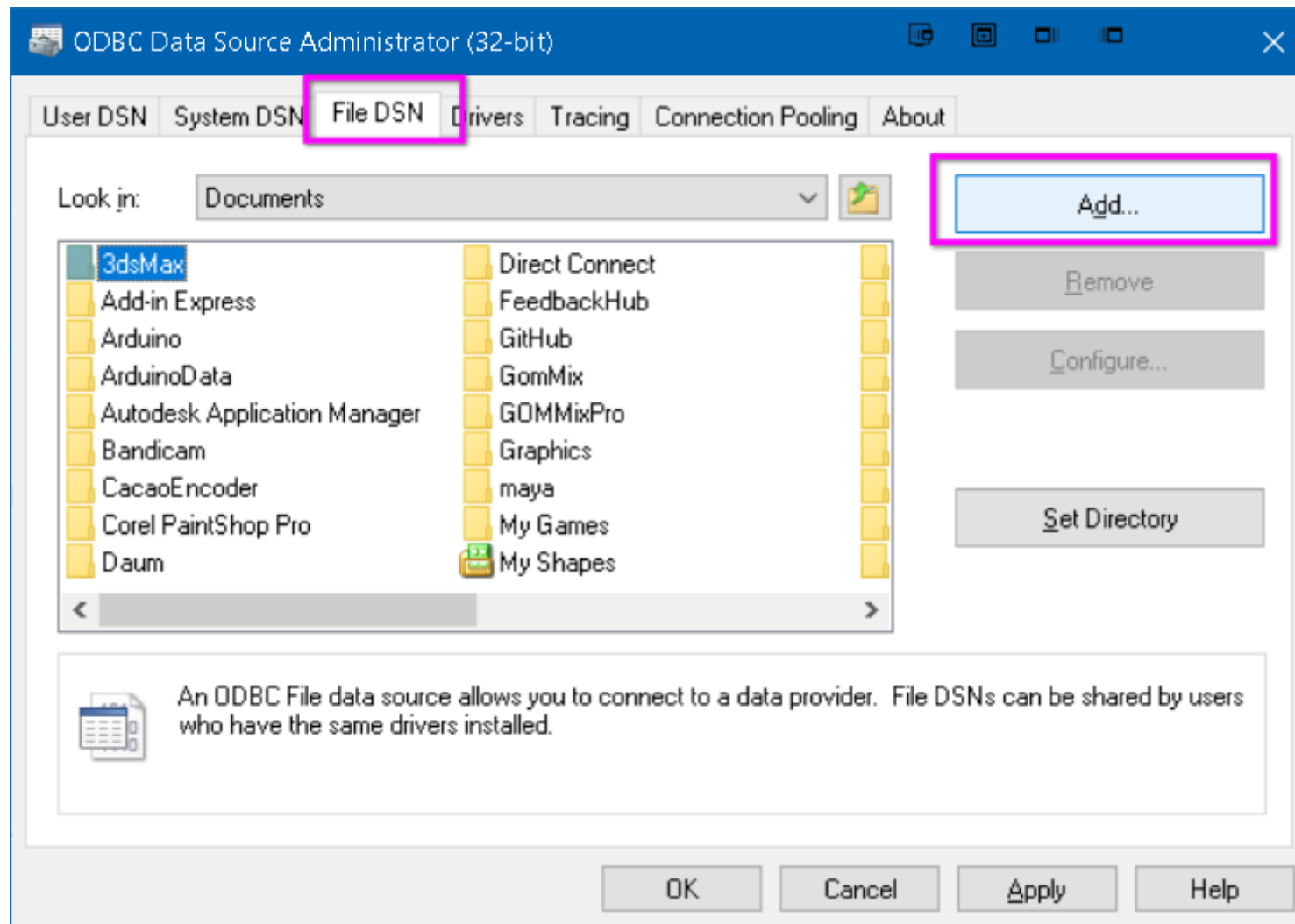
Create ODBC .dsn file

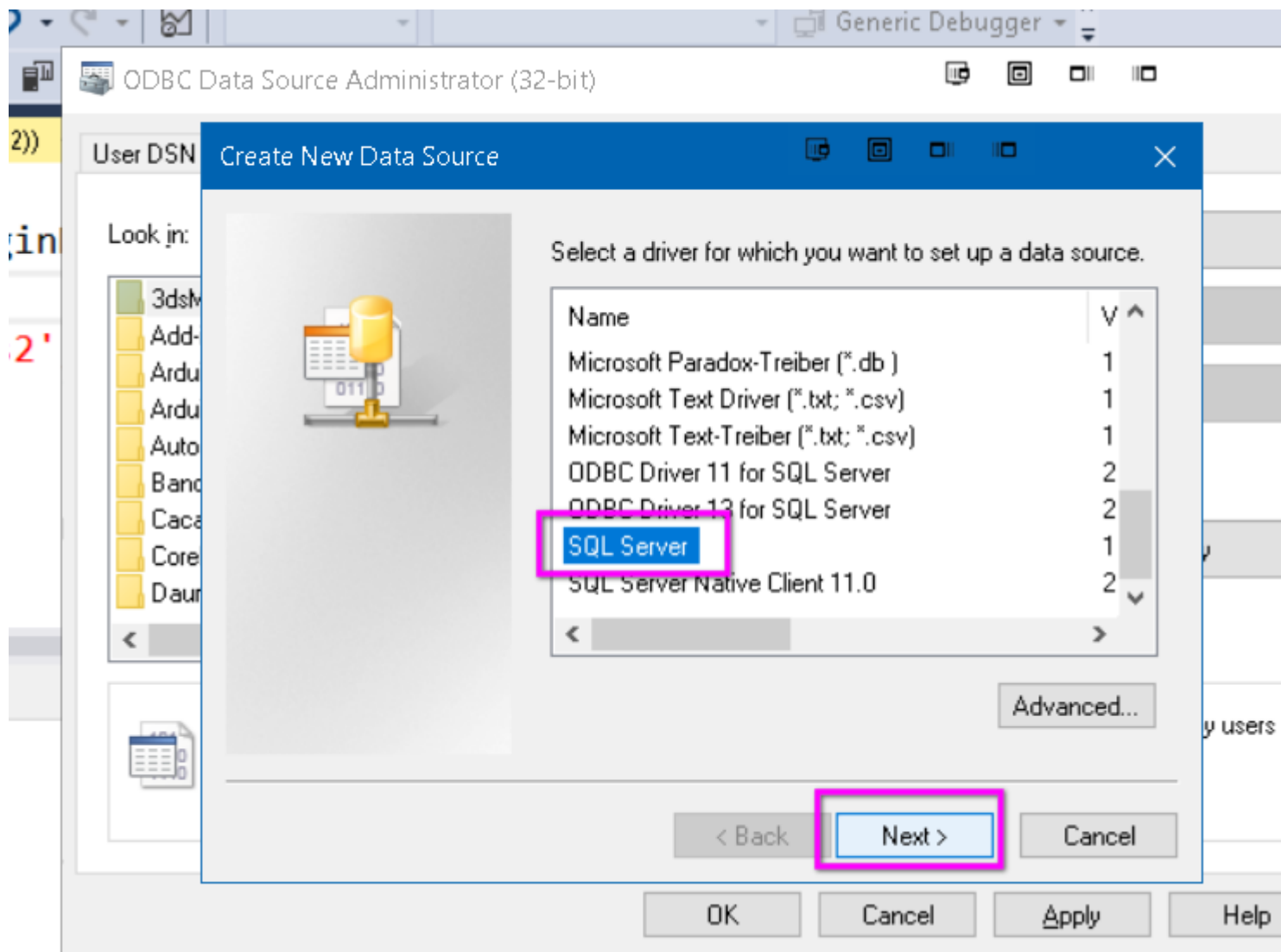
jintaeks@dongseo.ac.kr

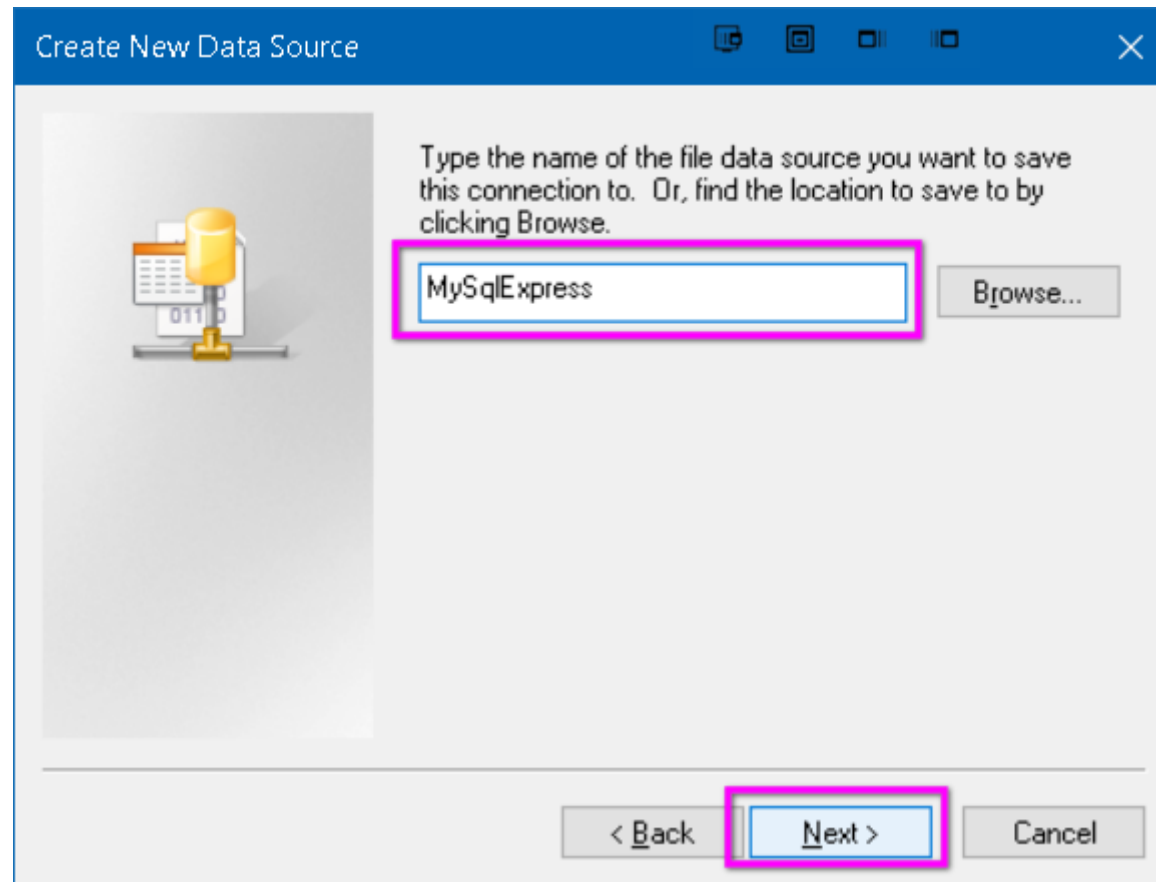
April 11, 2019

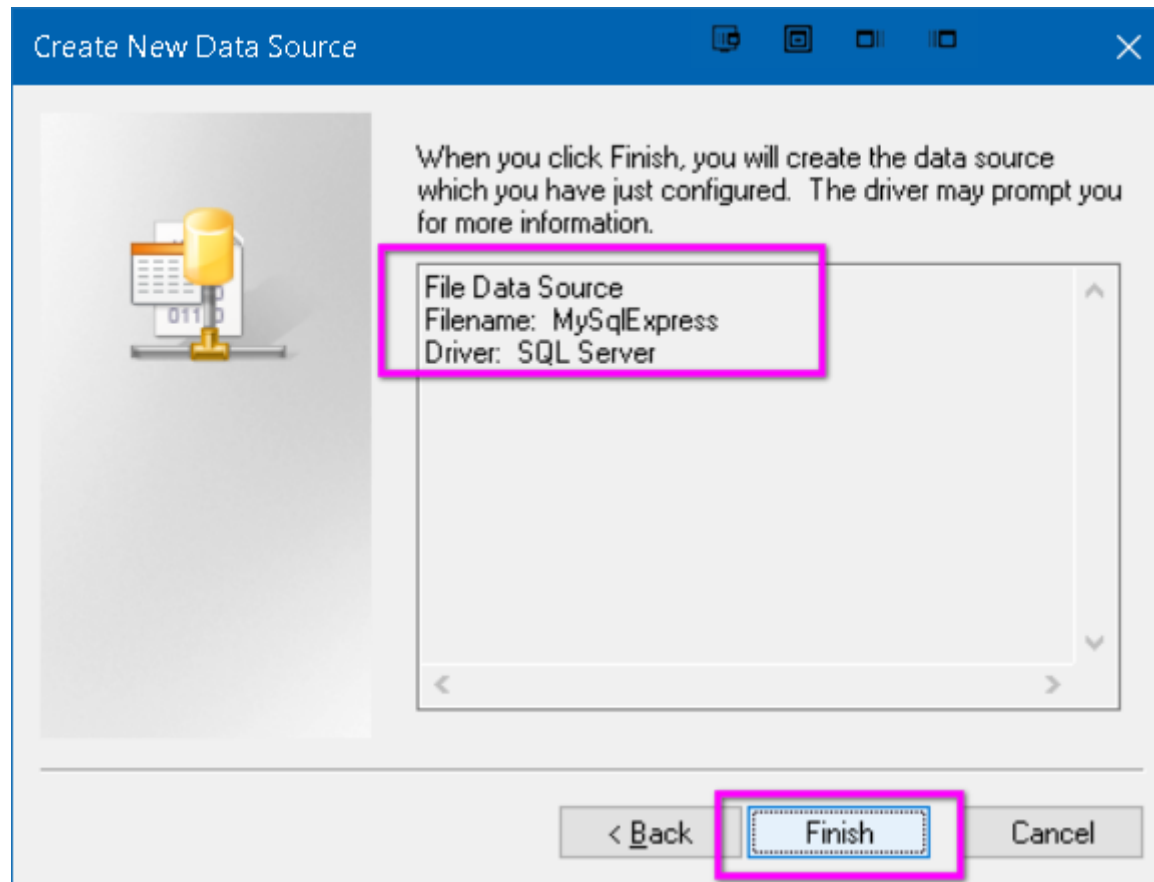


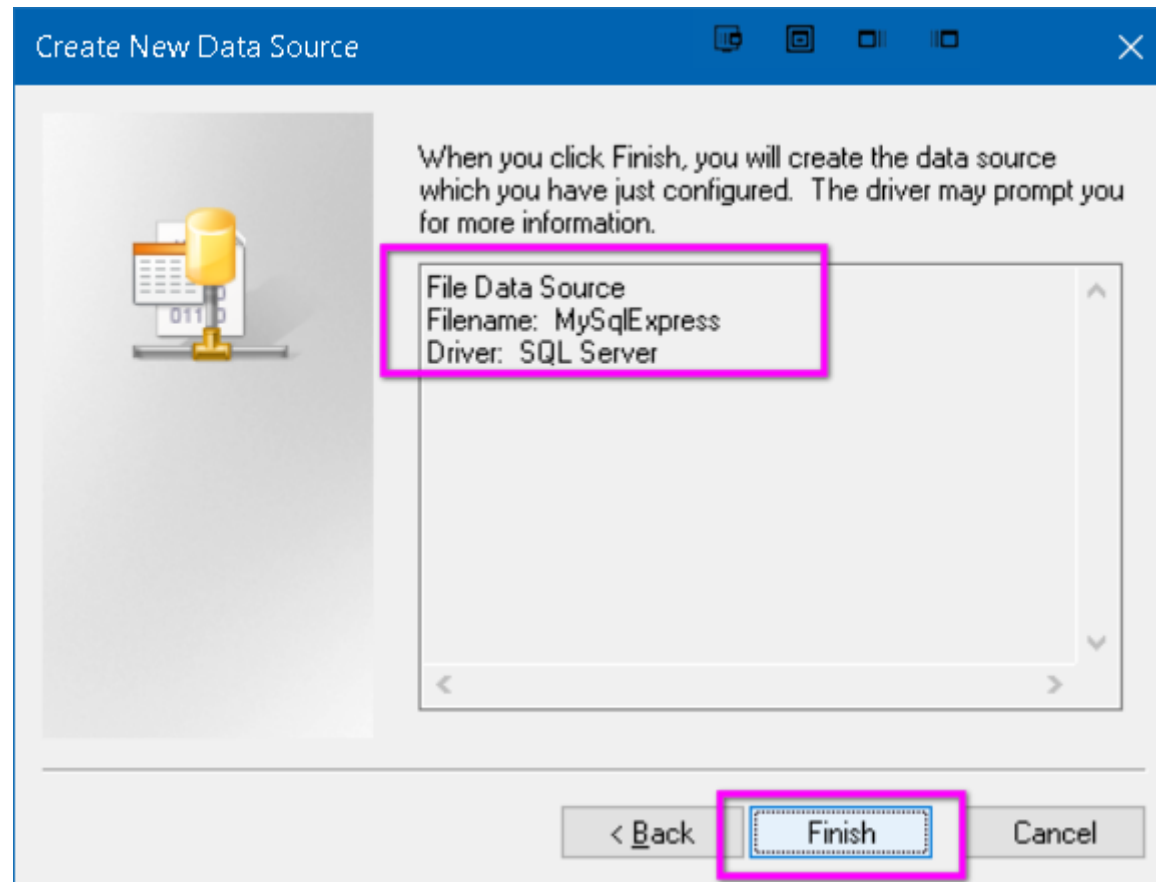












Create a New Data Source to SQL Server

This wizard will help you create an ODBC data source that you can use to connect to SQL Server.

What name do you want to use to refer to the data source?

Name:

How do you want to describe the data source?


Description:

Which SQL Server do you want to connect to?

Server:

Finish Next > Cancel Help

Create a New Data Source to SQL Server



How should SQL Server verify the authenticity of the login ID?

☐ With Windows NT authentication using the network login ID.

☒ With SQL Server authentication using a login ID and password entered by the user.

To change the network library used to communicate with SQL Server, click Client Configuration.

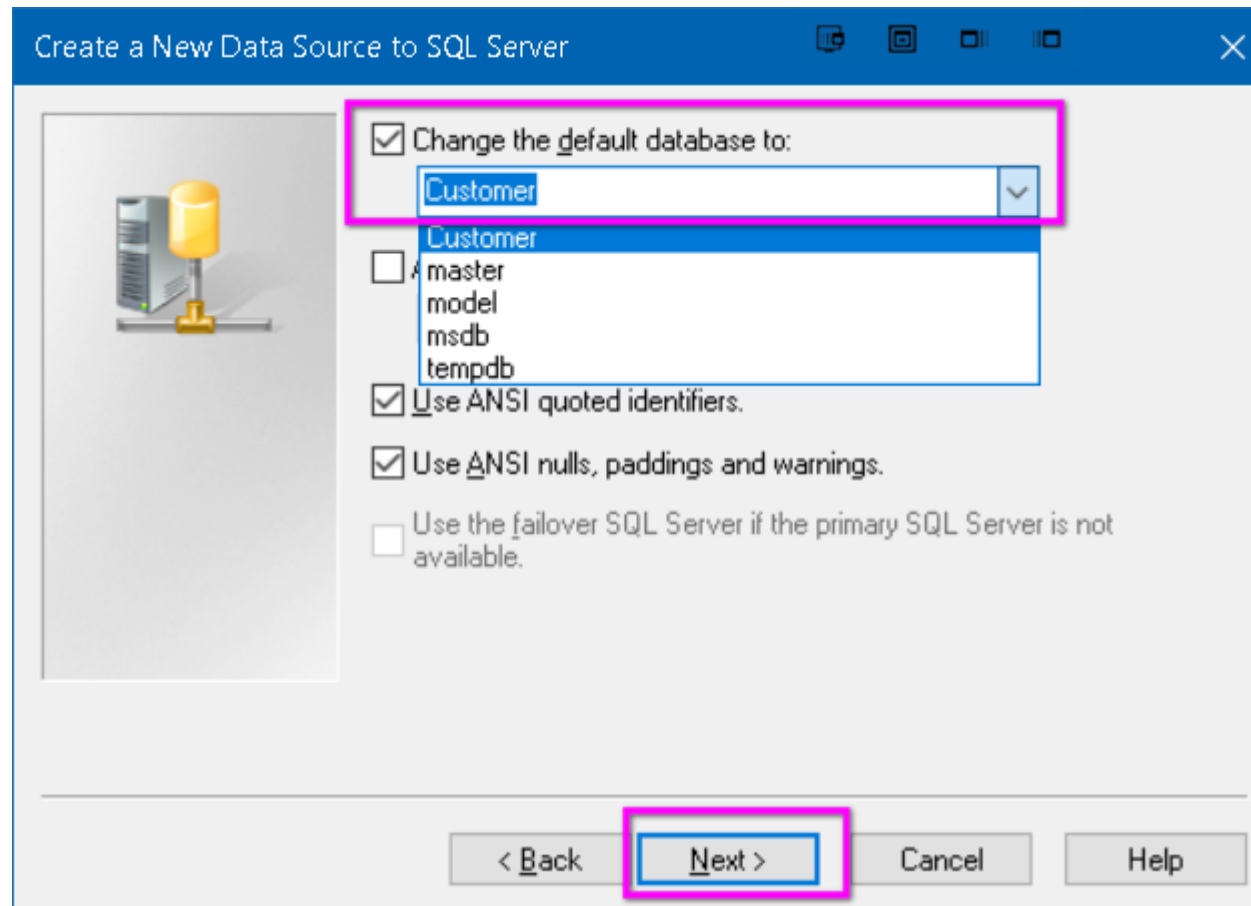
Client Configuration...

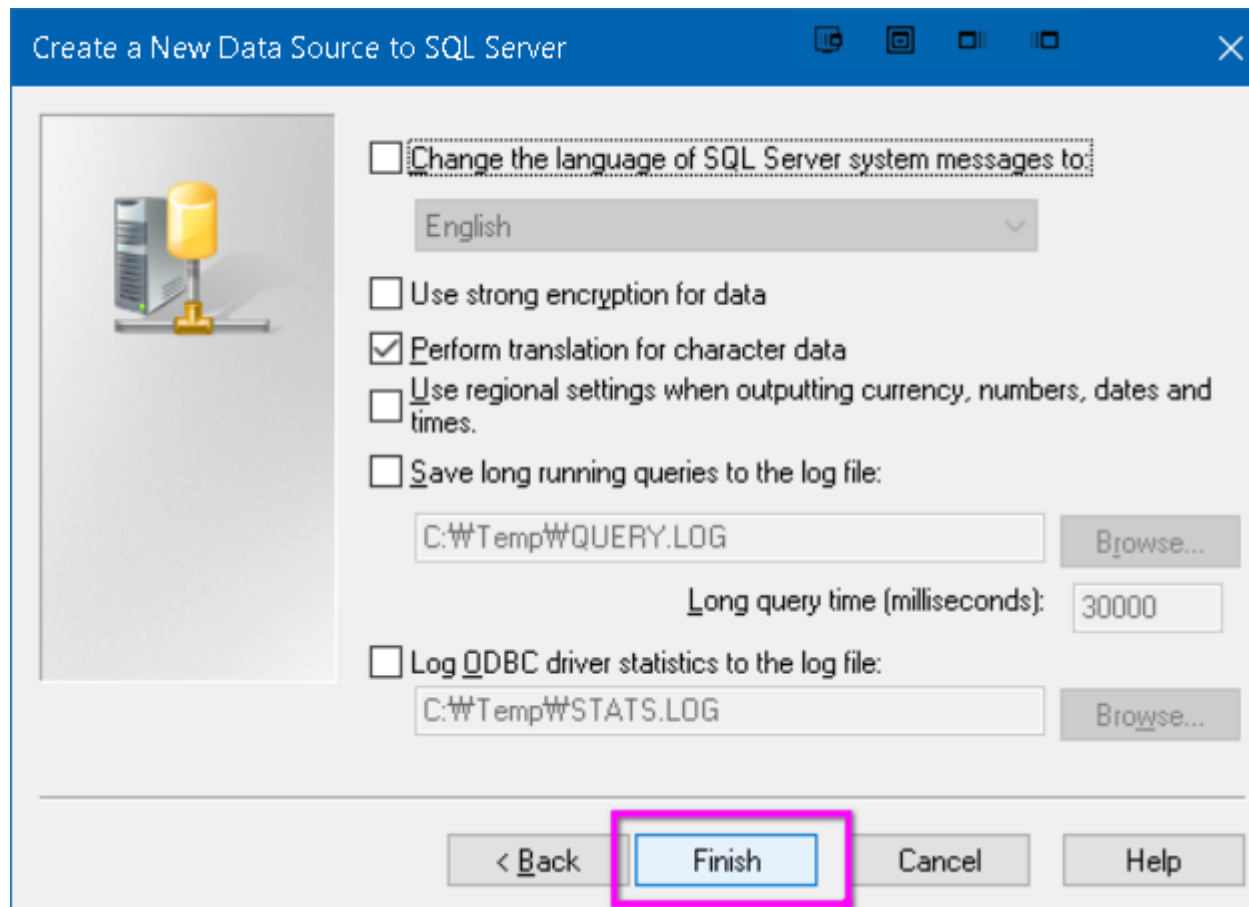
☒ Connect to SQL Server to obtain default settings for the additional configuration options.

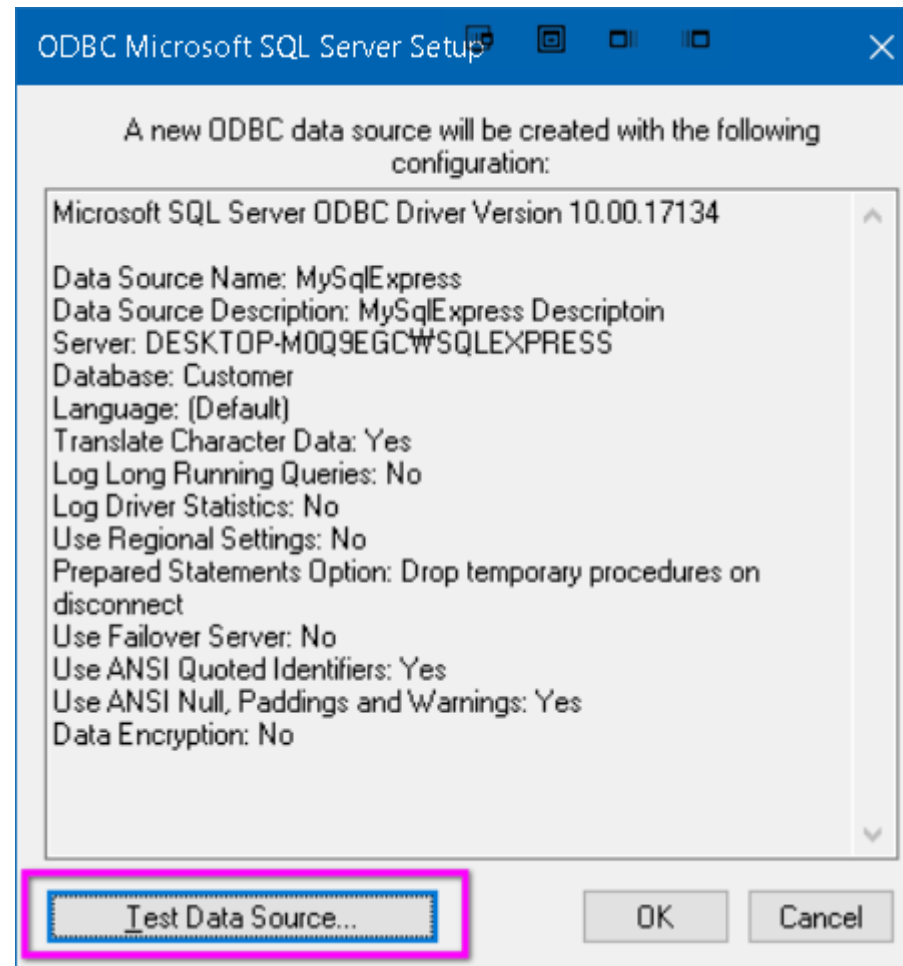
Login ID: sa

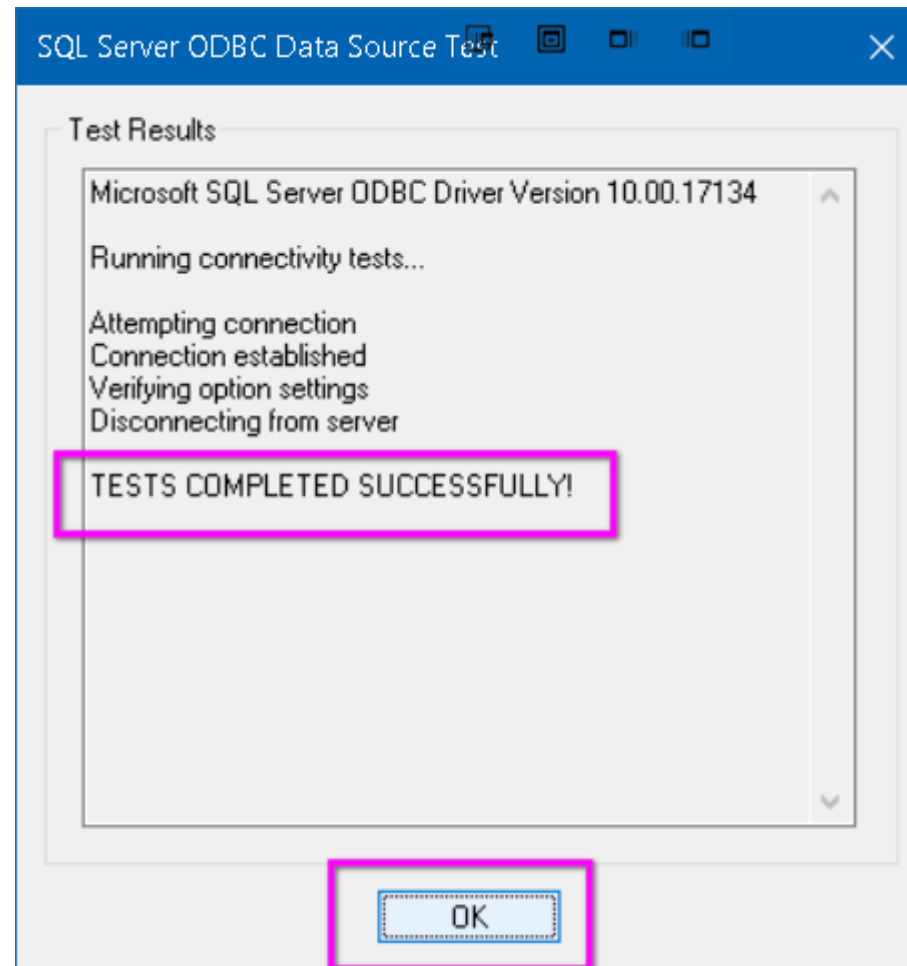
Password: ●●●●

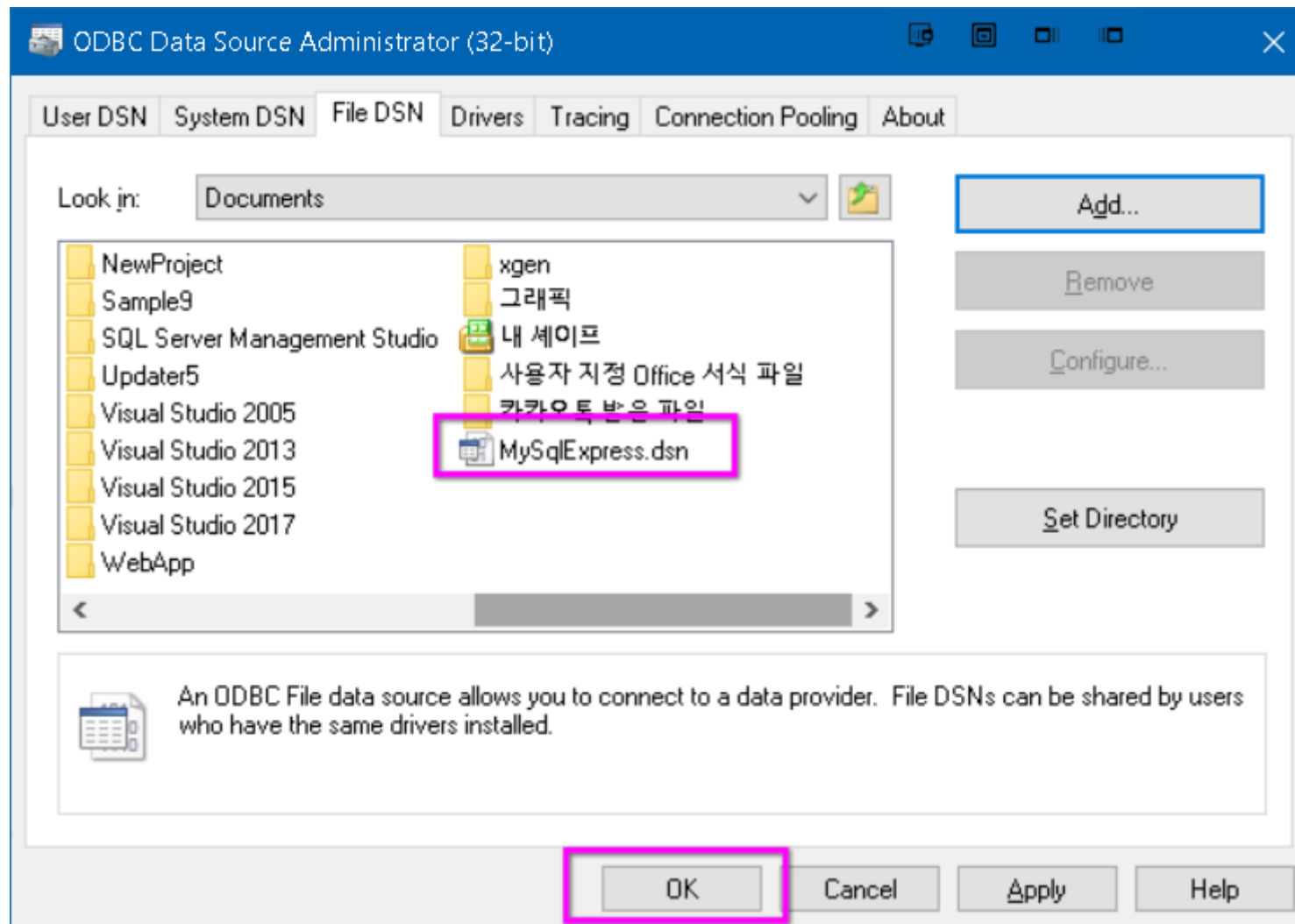
< Back Next > Cancel Help













- SQL Server Configuration Manager (Local)
 - SQL Server Services
 - SQL Server Network Configuration (32bit)
 - Protocols for SQLEXPRESS
 - SQL Native Client 11.0 Configuration (32b
 - Client Protocols
 - Aliases

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Enabled

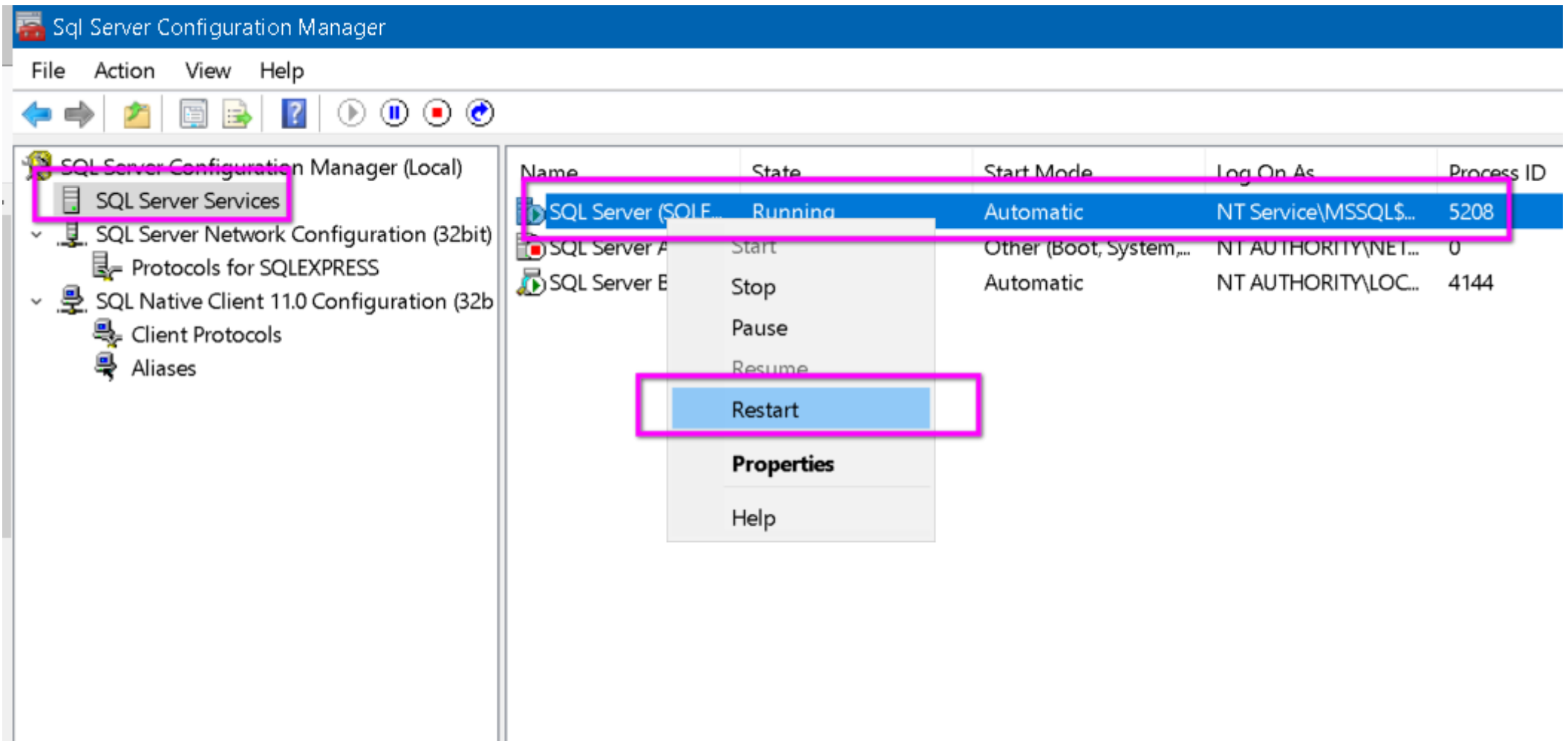
TCP/IP Properties

Protocol IP Addresses

Enabled	No
IP Address	169.254.201.226
TCP Dynamic Ports	0
TCP Port	
IP8	
Active	Yes
Enabled	No
IP Address	fe80::89f8:c689:93bd:fb7%32
TCP Dynamic Ports	0
TCP Port	
IP9	
Active	Yes
Enabled	No
IP Address	192.168.0.125
TCP Dynamic Ports	0
TCP Port	60009
IPAll	
TCP Dynamic Ports	0
TCP Port	

TCP Port
TCP port

OK Cancel Apply Help



Control Panel\All Control Panel Items\Windows Defender Firewall

< > > Control Panel > All Control Panel Items > Windows Defender Firewall

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off







Restore defaults

Advanced settings


Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

  Private networks	Not connected 
  Guest or public networks	Connected 

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	 iptime_jintaeks 2
Notification state:	Notify me when Windows Defender Firewall blocks a new app

See also

Security and Maintenance

Network and Sharing Center

0 items

Computer

Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall with Advanced Security

- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

Inbound Rules

Name	Group	Profile	Enabled	Action	Override
Avast Emergency Update		Public	Yes	Allow	No
Avast Emergency Update		Public	Yes	Allow	No
Avira.SoftwareUpdater.ToastNotificationsB...		Public	Yes	Block	No
Avira.SoftwareUpdater.ToastNotificationsB...		Private	Yes	Allow	No
Avira.SoftwareUpdater.ToastNotificationsB...		Domain	Yes	Allow	No
Avira.SoftwareUpdater.ToastNotificationsB...		Public	Yes	Block	No
Avira.SoftwareUpdater.ToastNotificationsB...		Private	Yes	Allow	No
Avira.SoftwareUpdater.ToastNotificationsB...		Domain	Yes	Allow	No
Avira.SoftwareUpdater.ToastNotificationsB...		Public	Yes	Block	No
Avira.SoftwareUpdater.ToastNotificationsB...		Domain	Yes	Allow	No
Avira.SoftwareUpdater.ToastNotificationsB...		Domain	Yes	Allow	No
Avira.SoftwareUpdater.ToastNotificationsB...		Public	Yes	Block	No
Avira.SoftwareUpdater.ToastNotificationsB...		Private	Yes	Allow	No
Avira.SoftwareUpdater.ToastNotificationsB...		Domain	Yes	Allow	No
Avira.SoftwareUpdater.ToastNotificationsB...		Public	Yes	Block	No
Avira.SoftwareUpdater.ToastNotificationsB...		Private	Yes	Allow	No
Avira.SoftwareUpdater.ToastNotificationsB...		Domain	Yes	Allow	No
Avira.SoftwareUpdater.ToastNotificationsB...		Domain	Yes	Allow	No
Avira.SoftwareUpdater.ToastNotificationsB...		Public	Yes	Block	No
Avira.SoftwareUpdater.ToastNotificationsB...		Private	Yes	Allow	No
Avira.SoftwareUpdater.ToastNotificationsB...		Domain	Yes	Allow	No
Avira.SoftwareUpdater.ToastNotificationsB...		Public	Yes	Block	No

Actions

- Inbound Rules
- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

New Rule...

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

- ☐ **Program**
Rule that controls connections for a program.
- ☒ **Port**
Rule that controls connections for a TCP or UDP port.

- ☐ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

- ☐ **Custom**
Custom rule.

< Back

Next >

Cancel

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports**
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

- ☒ TCP
☐ UDP

Does this rule apply to all local ports or specific local ports?

☐ All local ports

☒ Specific local ports:

60009

Example: 80, 443, 5000-5010

< Back

Next >

Cancel

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action**
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

☒ **Allow the connection**

This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

[Customize...](#)

☐ **Block the connection**

< Back

Next >

Cancel

New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile**
- Name

When does this rule apply?

- ☒ **Domain**
Applies when a computer is connected to its corporate domain.
- ☒ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.
- ☒ **Public**
Applies when a computer is connected to a public network location.

< Back **Next >** Cancel

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name**

Name:

Tcp Port for MySQLExpress

Description (optional):

Tcp Port for MySQLExpress Description

< Back Finish Cancel

MySqlExpress.dsn

[ODBC]

DRIVER=SQL Server

UID=sa

DATABASE=Customer

WSID=DESKTOP-M0Q9EGC

APP=Microsoft® Windows® Operating System

SERVER=DESKTOP-M0Q9EGC\SQLEXPRESS

Description=MySqlExpress Description

Address=192.168.0.125,60009

PWD=1234

MY **BRIGHT** FUTURE

DSU Dongseo University
동서대학교