



# Installing MSSQL

## Framework NET Genium



# Content

<b>1</b>	<b>SQL Server configuration options.....</b>	<b>3</b>
<b>2</b>	<b>Installing SQL Server 2016 .....</b>	<b>3</b>
2.1	Installation preparation .....	3
2.2	SQL Server 2016 installation via “Setup.exe” .....	3
<b>3</b>	<b>Install SQL Server Management Studio .....</b>	<b>10</b>
3.1	Installation preparation .....	10
3.2	Installing SQL Server Management Studio via “Setup.exe” .....	10
<b>4</b>	<b>Creating the “ConnectionString.txt” file .....</b>	<b>11</b>
4.1	Connection string for local access to the database.....	11
4.2	Connection string for accessing the database using a technology account from Active Directory .....	11
4.3	Connection string for accessing the database using a local SQL Server account .....	11
<b>5</b>	<b>Network penetration settings.....</b>	<b>12</b>
<b>6</b>	<b>Firewall settings .....</b>	<b>16</b>
<b>7</b>	<b>Setting permissions for access to the database .....</b>	<b>20</b>
7.1	Setting permissions for local access .....	20
7.1.1	Automatic permission setting via the “Setup.exe” NET Genium program.....	20
7.1.2	Manually set permissions through “Microsoft SQL Server Management Studio” .....	21
7.2	Setting permissions for access through the technology account from Active Directory .....	25
7.3	Setting permissions for access through the local SQL Server account .....	28

# 1 SQL Server configuration options

1 Depending on how NET Genium accesses the database, we distinguish three different types of database server configuration:

1. **Local access** – The database server is installed on the same computer as the application server.
2. **Access via technology account from Active Directory** – The database server is installed on a different computer than the application server, and NET Genium accesses the database under a technology account from Active Directory.
3. **Access via local SQL Server account** – The database server is installed on a different computer than the application server, and NET Genium accesses the database under the local SQL Server account.

## 2 Installing SQL Server 2016

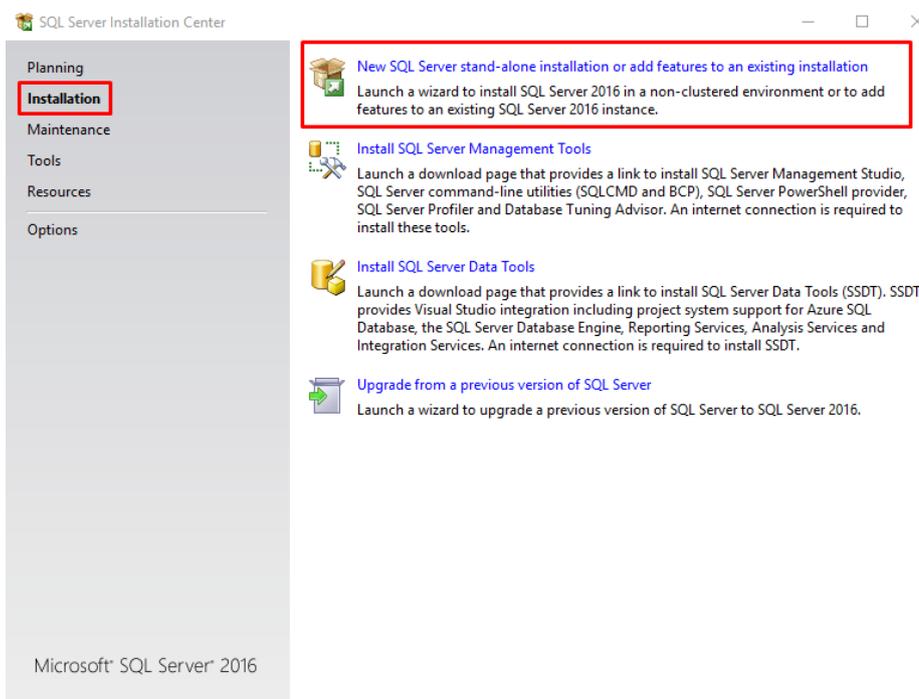
### 2.1 Installation preparation

↳ Mount the installation media in “iso” format, or open the “O:\Install\\_WIN\SQLServer2016Media” directory on the shared “\\office” server if the installation is located within the NetGenium internal computer network.

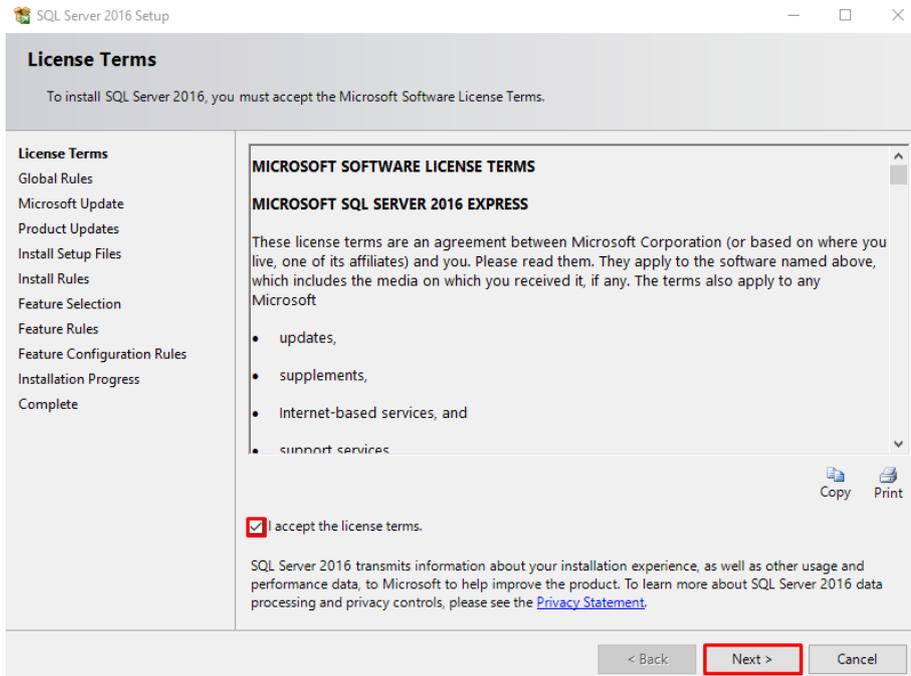
### 2.2 SQL Server 2016 installation via “Setup.exe”

↳ Run the “SETUP.exe” program.

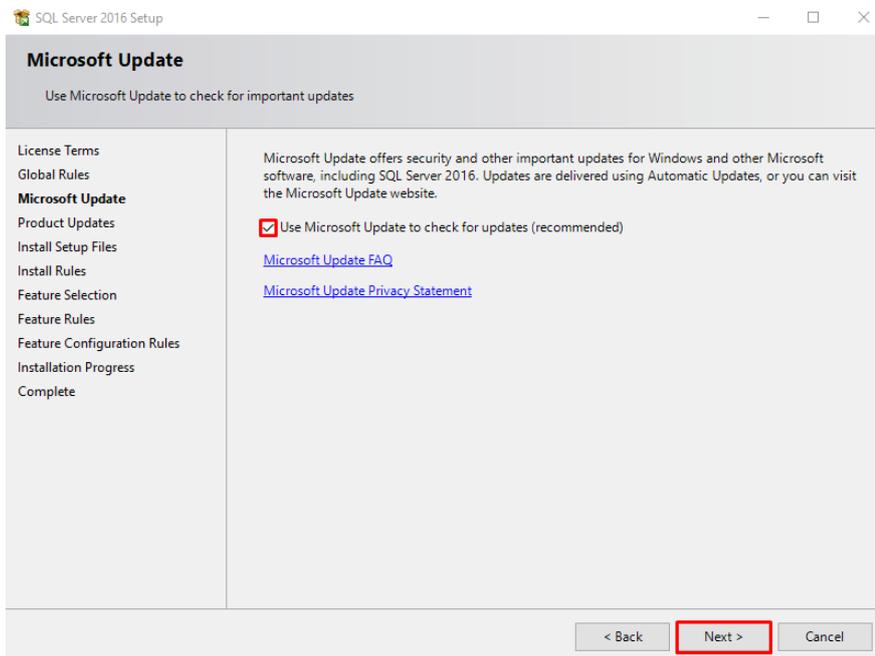
↳ In the “Installation” section, select the “New SQL Server stand-alone installation or add features to an existing installation” option.



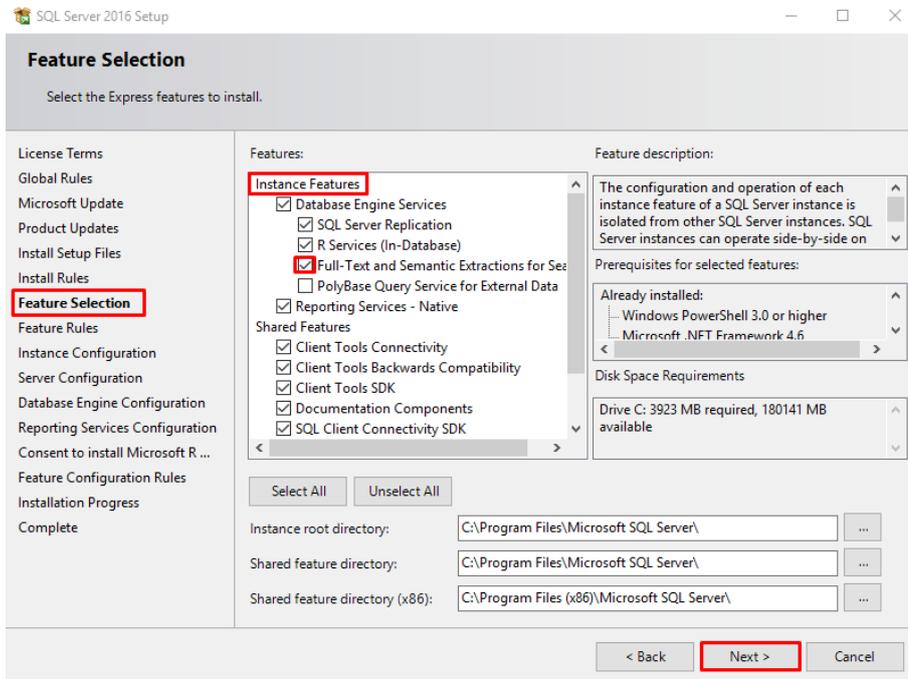
☞ Agree to the license terms and click “Next”.



☞ Check “Use Microsoft Update to check for updates (recommended)” and click “Next”.



- 1 If you require full-text indexing of the columns in the database, check the “Full-Text and Semantic Extractions for Search” option in the “Feature Selection” section and in the “Instance Features” category, and click the “Next” button.



The screenshot shows the 'Feature Selection' window in the SQL Server 2016 Setup wizard. The window title is 'SQL Server 2016 Setup'. The main heading is 'Feature Selection' with the instruction 'Select the Express features to install.' On the left, a navigation pane lists various setup steps, with 'Feature Selection' highlighted in red. The main area is divided into 'Features:' and 'Feature description:'. Under 'Features:', the 'Instance Features' category is selected and highlighted in red. Within this category, the following features are checked: 'Database Engine Services', 'SQL Server Replication', 'R Services (In-Database)', 'Full-Text and Semantic Extractions for Search' (highlighted in red), 'Reporting Services - Native', 'Client Tools Connectivity', 'Client Tools Backwards Compatibility', 'Client Tools SDK', 'Documentation Components', and 'SQL Client Connectivity SDK'. The 'Feature description:' pane shows details for the selected feature, including prerequisites like 'Windows PowerShell 3.0 or higher' and 'Microsoft .NET Framework 4.6', and disk space requirements for Drive C: (3923 MB required, 180141 MB available). At the bottom, there are fields for 'Instance root directory', 'Shared feature directory', and 'Shared feature directory (x86)', all set to 'C:\Program Files\Microsoft SQL Server\' or similar paths. The 'Next >' button is highlighted in red.

- ➔ In the “Server Configuration” section, on the “Service Accounts” tab, check the “Grant Perform Volume Maintenance Task Privilege to SQL Server Database Engine Service” option and click the “Next” button.

SQL Server 2016 Setup

### Server Configuration

Specify the service accounts and collation configuration.

- License Terms
- Global Rules
- Microsoft Update
- Product Updates
- Install Setup Files
- Install Rules
- Feature Selection
- Feature Rules
- Instance Configuration
- Server Configuration**
- Database Engine Configuration
- Reporting Services Configuration
- Consent to install Microsoft R ...
- Feature Configuration Rules
- Installation Progress
- Complete

Service Accounts
Collation

Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Database Engine	NT Service\MSSQL\$SQL...		Automatic <span style="float: right;">▼</span>
SQL Server Reporting Services	NT Service\ReportServer...		Automatic <span style="float: right;">▼</span>
SQL Server Launchpad	NT Service\MSSQLLaun...		Automatic
SQL Full-text Filter Daemon Launc...	NT Service\MSSQLFDLa...		Manual
SQL Server Browser	NT AUTHORITY\LOCAL ...		Disabled <span style="float: right;">▼</span>

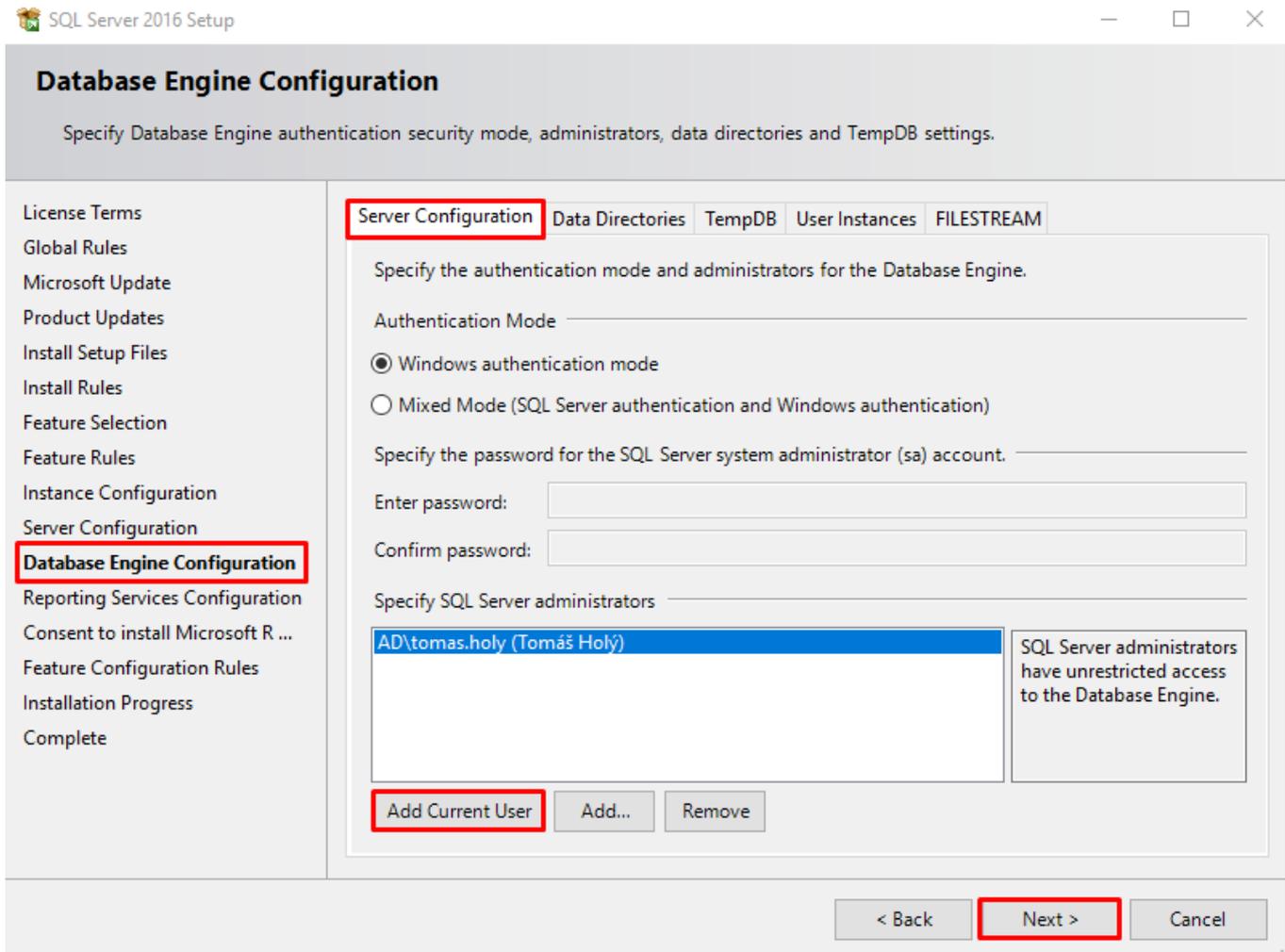
Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service

This privilege enables instant file initialization by avoiding zeroing of data pages. This may lead to information disclosure by allowing deleted content to be accessed.

[Click here for details](#)

< Back
Next >
Cancel

- ↳ In the “Database Engine Configuration” section on the “Server Configuration” tab, click the “Add Current User” button and then click the “Next” button.

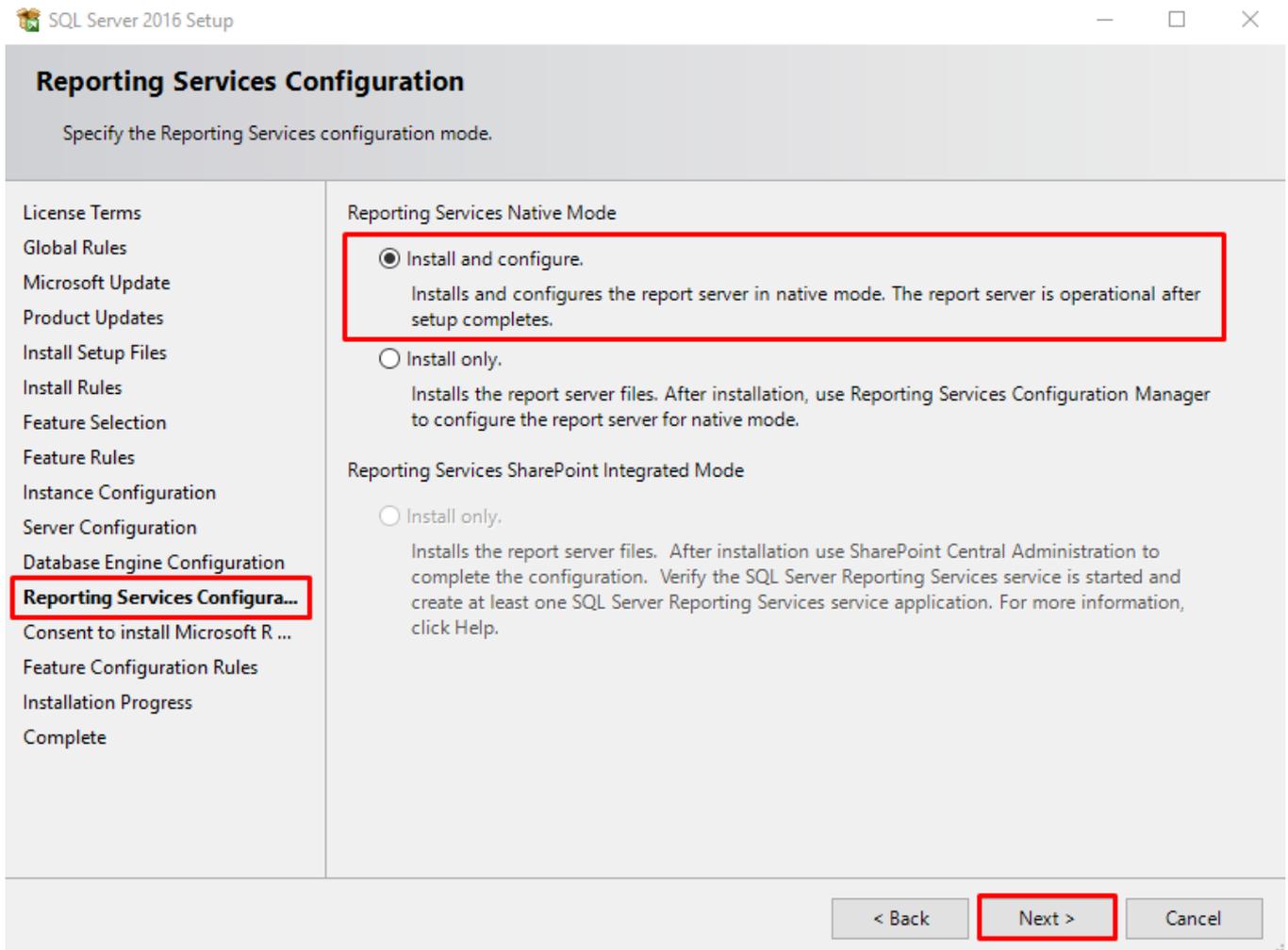


The screenshot shows the "Database Engine Configuration" window in the SQL Server 2016 Setup. The window title is "SQL Server 2016 Setup" and the subtitle is "Database Engine Configuration". The main instruction is "Specify Database Engine authentication security mode, administrators, data directories and TempDB settings." The left sidebar contains a list of configuration steps, with "Database Engine Configuration" highlighted in red. The main area has several tabs: "Server Configuration" (highlighted in red), "Data Directories", "TempDB", "User Instances", and "FILESTREAM". The "Server Configuration" tab contains the following options:

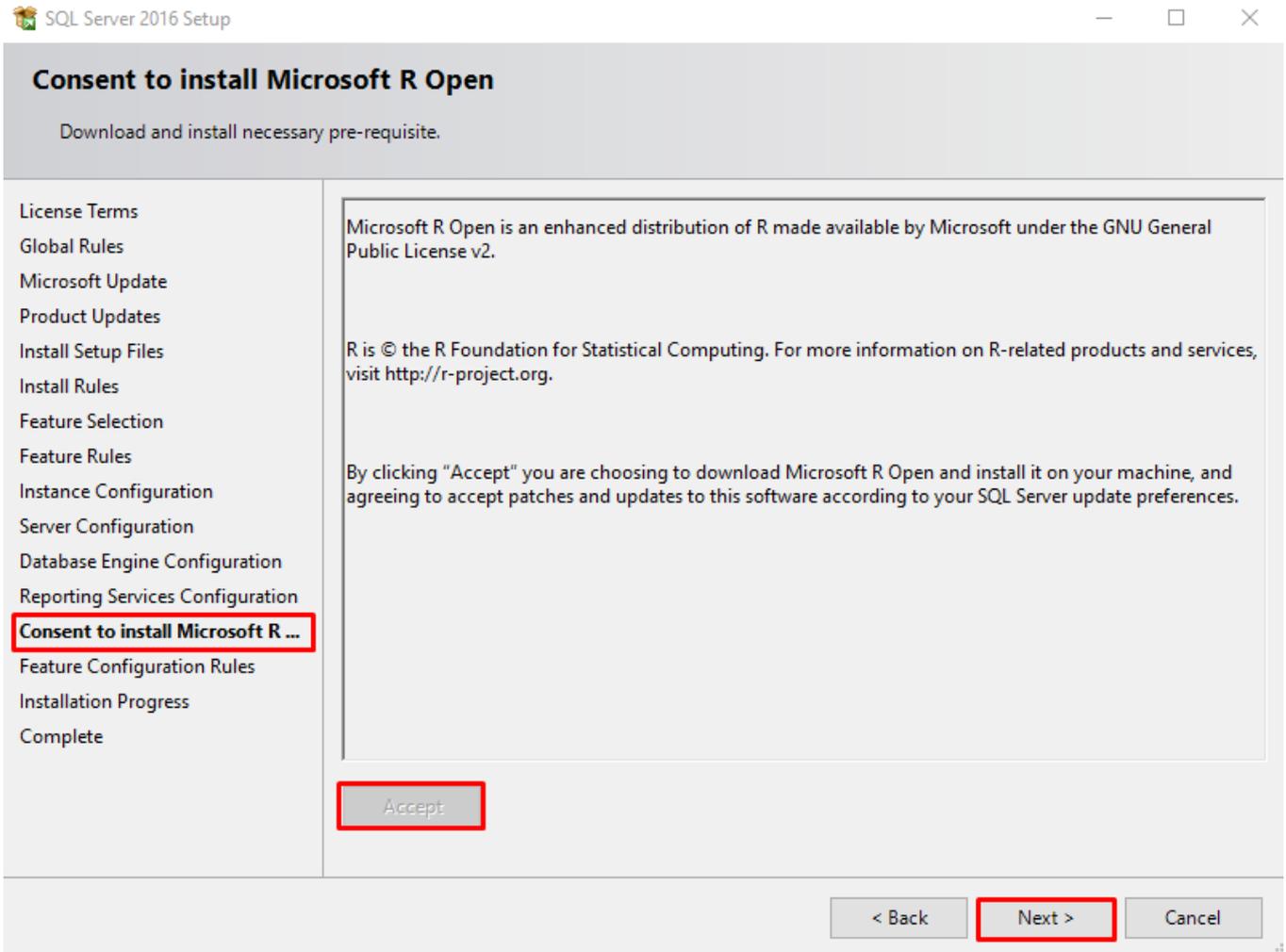
- Authentication Mode:  Windows authentication mode,  Mixed Mode (SQL Server authentication and Windows authentication)
- Specify the password for the SQL Server system administrator (sa) account. Enter password: [text box], Confirm password: [text box]
- Specify SQL Server administrators: [list box containing "AD\tomas.holy (Tomáš Holy)"]
- Buttons: "Add Current User" (highlighted in red), "Add...", "Remove"

At the bottom right, there are three buttons: "< Back", "Next >" (highlighted in red), and "Cancel". A warning box on the right side of the administrators list states: "SQL Server administrators have unrestricted access to the Database Engine."

↳ In the “Reporting Services Configuration” section, select the “Install and configure” option and click the “Next” button.



- ➔ In the “Consent to install Microsoft R Open” section, click the “Accept” button and click “Next” to complete the installation.



- ❗ You must restart your computer after the installation is complete.

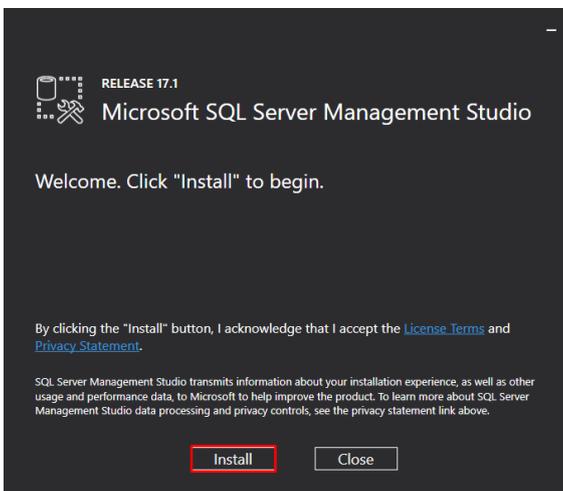
## 3 Install SQL Server Management Studio

### 3.1 Installation preparation

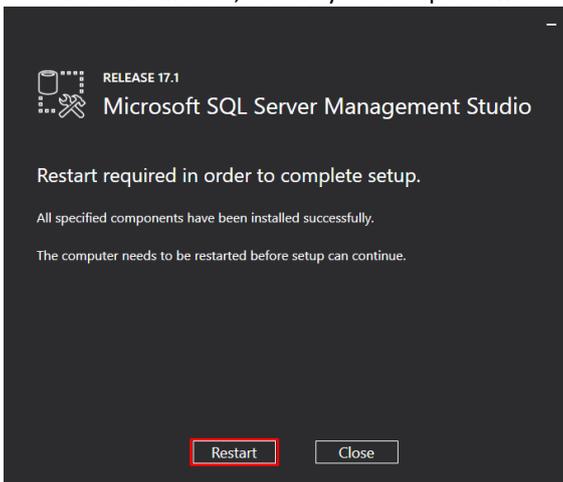
- ↳ Mount the installation media in “iso” format, or if the installation is located within the NetGenium internal computer network, open the “O:\Install\\_WIN” directory on the “\\office” shared server.

### 3.2 Installing SQL Server Management Studio via “Setup.exe”

- ↳ Start the program “SQLManagementStudio 17.1 SSMS-Setup-ENU.exe”.
- ↳ Click the “Install” button.



- ↳ After installation, restart your computer with the “Restart” button.



## 4 Creating the “ConnectionString.txt” file

- ❶ *“ConnectionString.txt” is a file in the “Config” directory that contains the database connection string definition.*
- ❶ *The procedure for creating the “ConnectionString.txt” file differs depending on the configuration type of the database server.*

👉 From the variants below, select the type of database server configuration you want to use and create and set up the “ConnectionString.txt” file accordingly.

1. **Local access** – The database server is installed on the same computer as the application server.
2. **Access via technology account from Active Directory** – The database server is installed on a different computer than the application server, and NET Genium accesses the database under a technology account from Active Directory.
3. **Access via local SQL Server account** – The database server is installed on a different computer than the application server, and NET Genium accesses the database under the local SQL Server account.

### 4.1 Connection string for local access to the database

- ❶ *When installing NET Genium via the “Setup.exe” program (see the “NET Genium installation” manual), after checking the “Create database” option, the “ConnectionString.txt” file is created in the NET Genium directory in the “Config” folder. This file contains the definition of the connection string to the database.*
- ❶ *For example, the contents of the “ConnectionString.txt” file contain the following connection string to the database: “server=(local)\SQLEXPRESS;Trusted\_Connection=true;database=netgenium”.*

### 4.2 Connection string for accessing the database using a technology account from Active Directory

👉 Create a “ConnectionString.txt” file in the “Config” directory of your NET Genium and paste the following information into this file:

- IP address or name of the database server
- Database name

👉 Save the data according to the following pattern:  
“server=123.456.789.123;Trusted\_Connection=true;database=netgenium”.

### 4.3 Connection string for accessing the database using a local SQL Server account

👉 Create a “ConnectionString.txt” file in the “Config” directory of your NET Genium and paste the following information into this file:

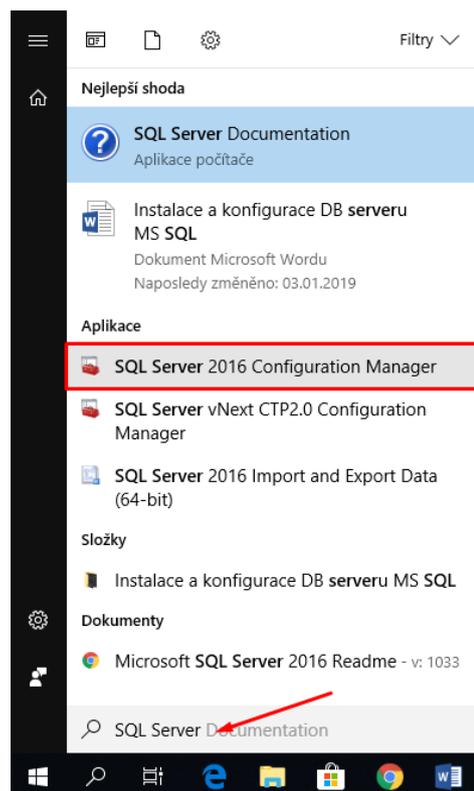
- IP address or name of the database server
- Database name
- The name of the local SQL Server account
- Password in this account

👉 Save the data according to the following pattern:  
“server=123.456.789.123;database=netgenium;User Id=svcnadmin;Password=1234”.

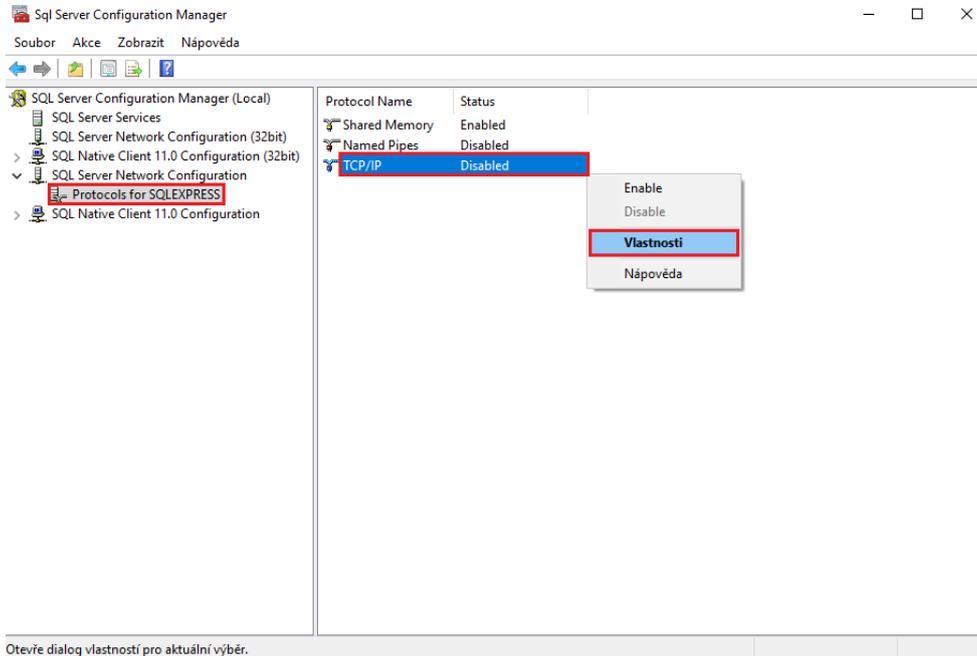
## 5 Network penetration settings

⚠ *Use this setting only if the database server is installed on a different computer than the application server and NET Genium accesses the database under the technology account from Active Directory or under the local SQL Server account.*

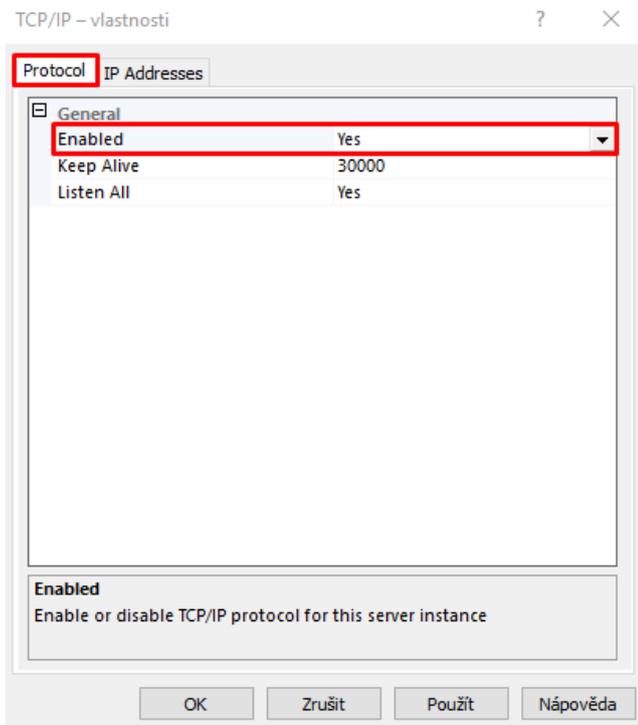
👉 From the “Start” menu, locate and run “SQL Server 2016 Configuration Manager”.



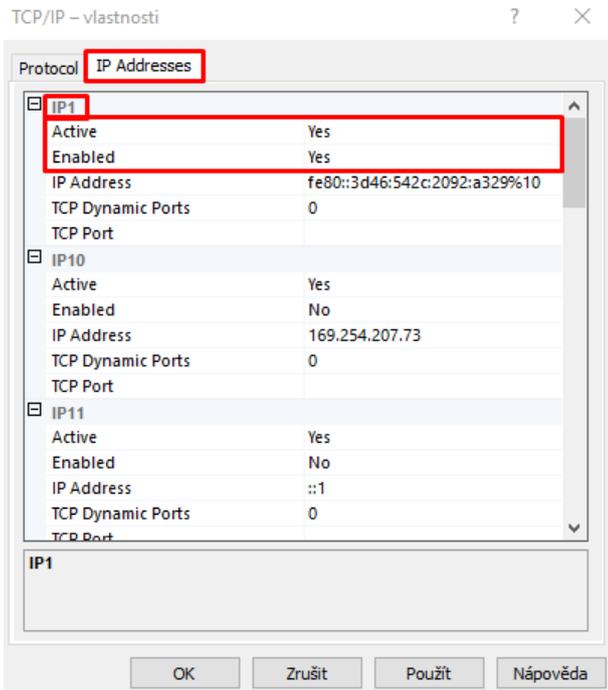
- Open the “SQL Server Network Configuration” node, select “Protocols for SQLEXPRESS”. Right-click on “TCP/IP” and select “Properties”.



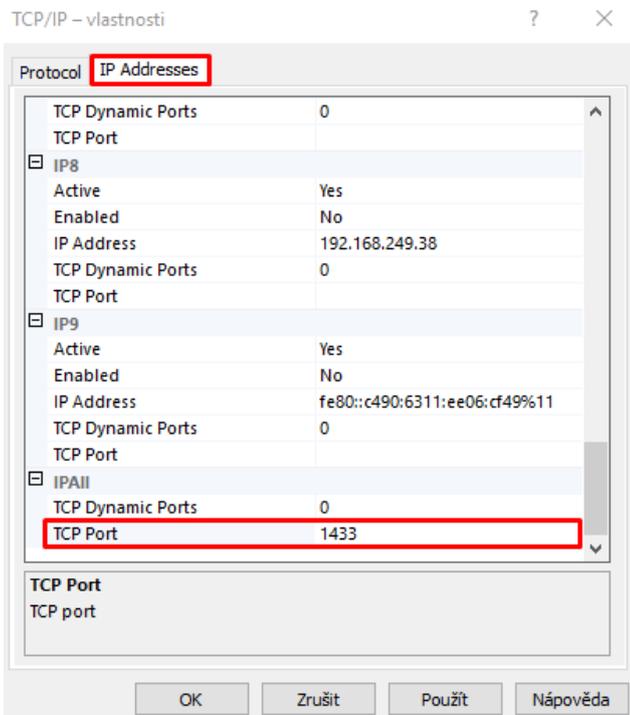
- On the “Protocol” tab, set “Enabled” to “Yes”.



On the “IP Addresses” tab, click on the “IP1” node and set “Active” and “Enabled” to “Yes”.

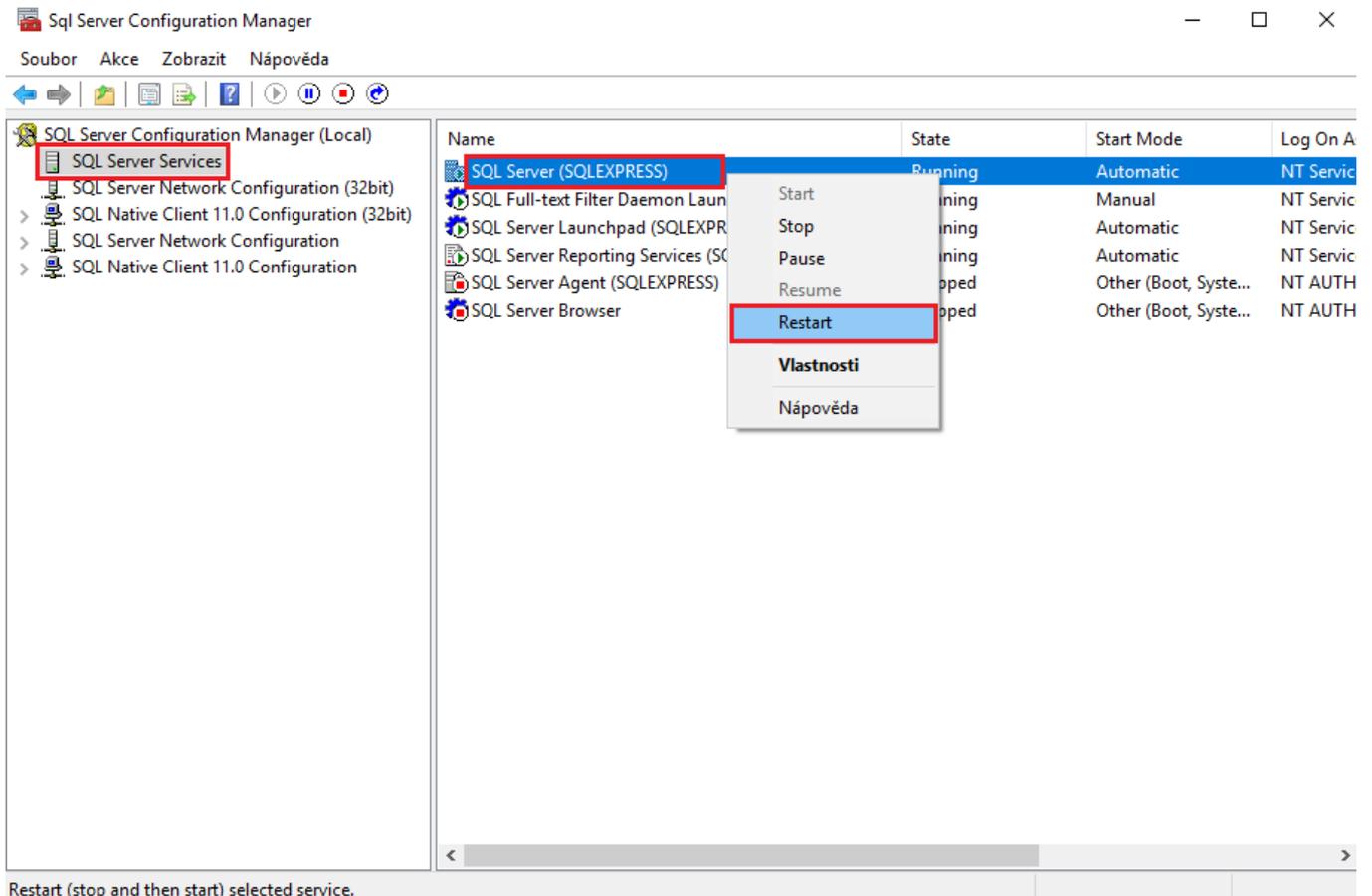


On the same tab, click on the “IPALL” node and set the “TCP Port” to “1433”.



1 In the last step, you need to restart SQL Server for the changes to take effect.

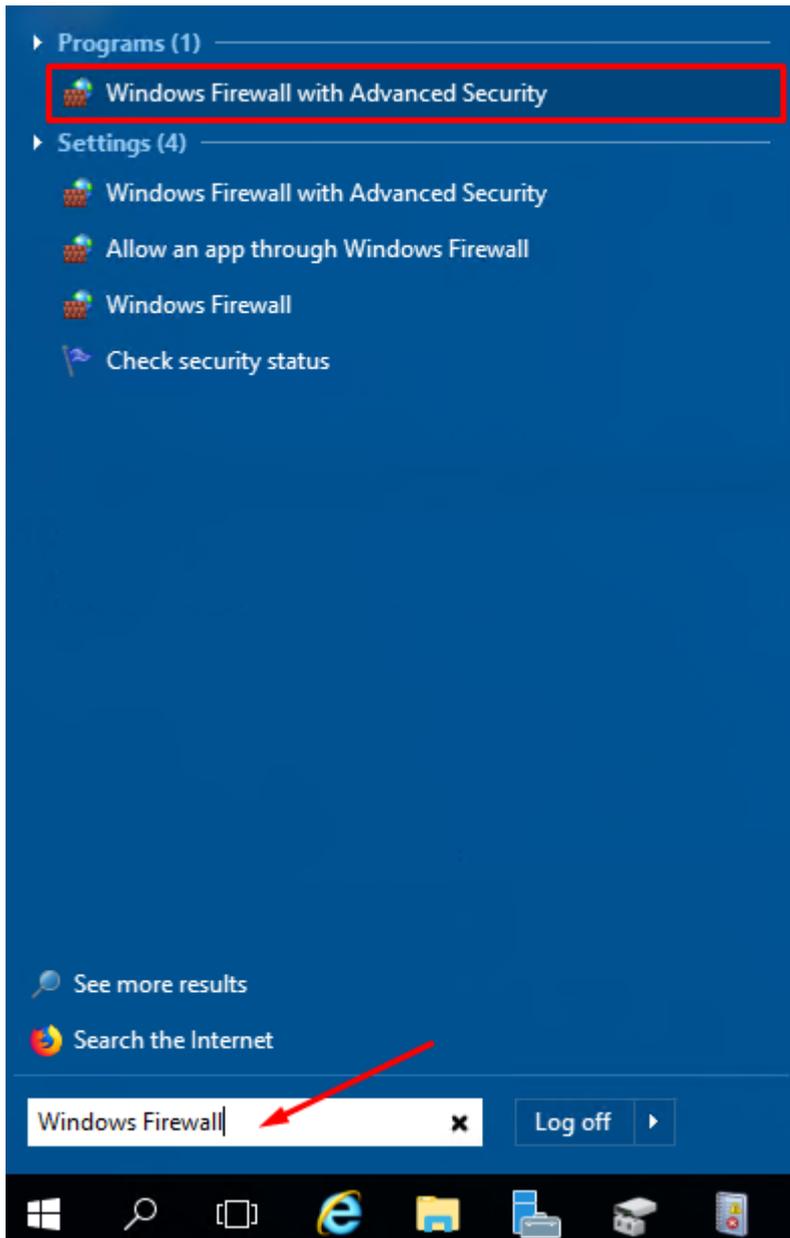
👉 Highlight “SQL Server Services”, right-click on “SQL Server (SQLEXPRESS)” and select “Restart”.



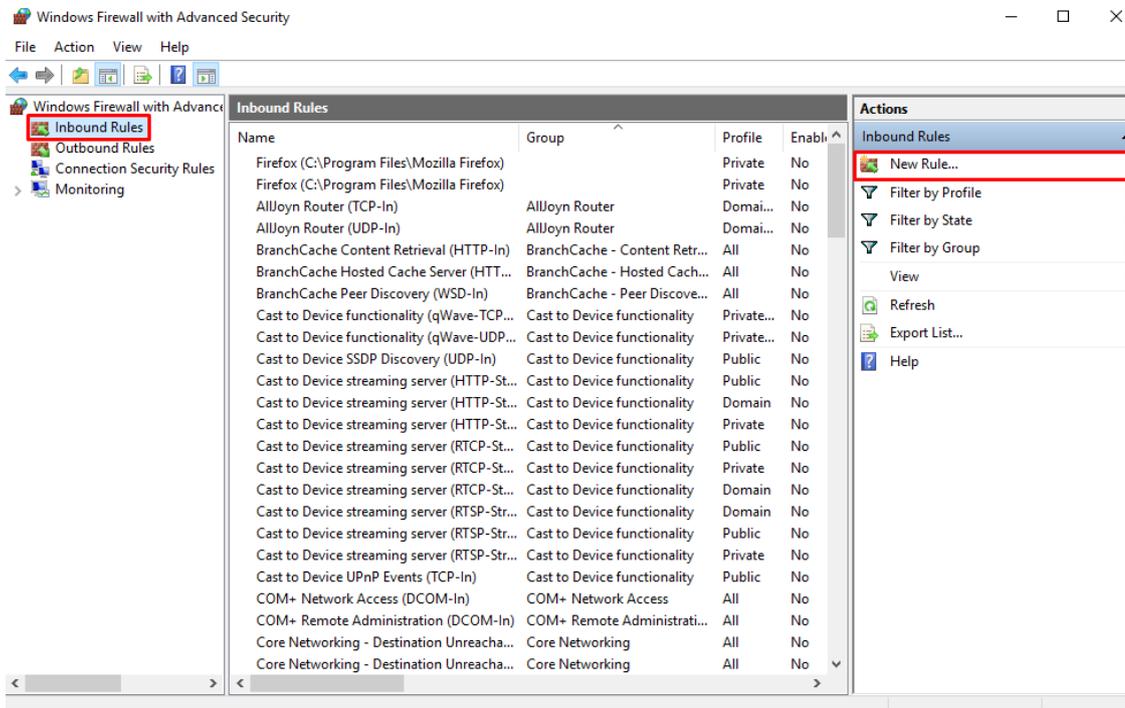
## 6 Firewall settings

⚠ *Use this setting only if the database server is installed on a different computer than the application server and NET Genium accesses the database under a technology account from Active Directory, or under local SQL Server account.*

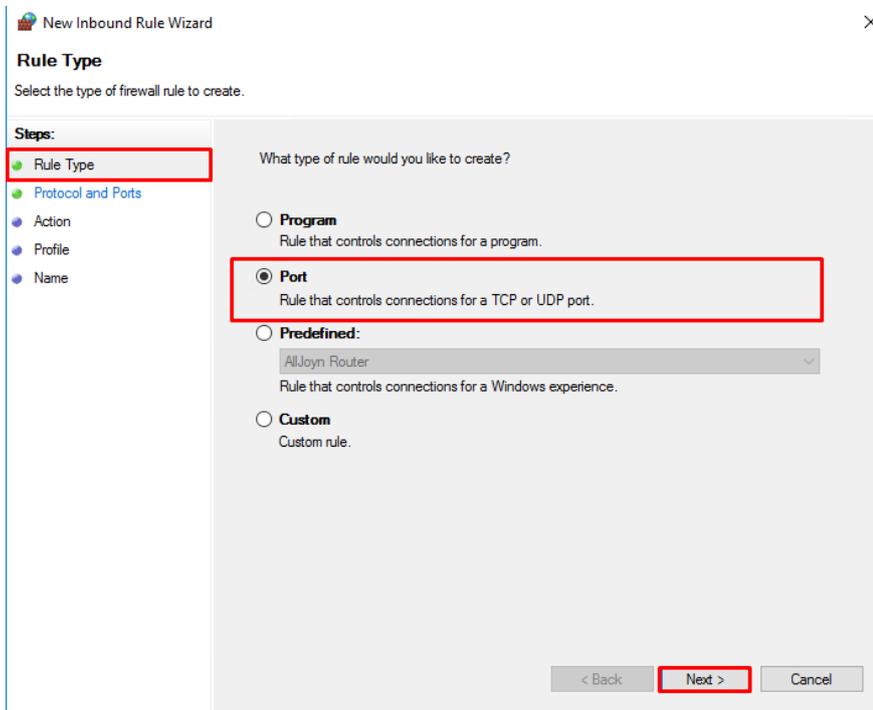
👉 From the “Start” menu, locate and launch “Windows Firewall with Advanced Security”.



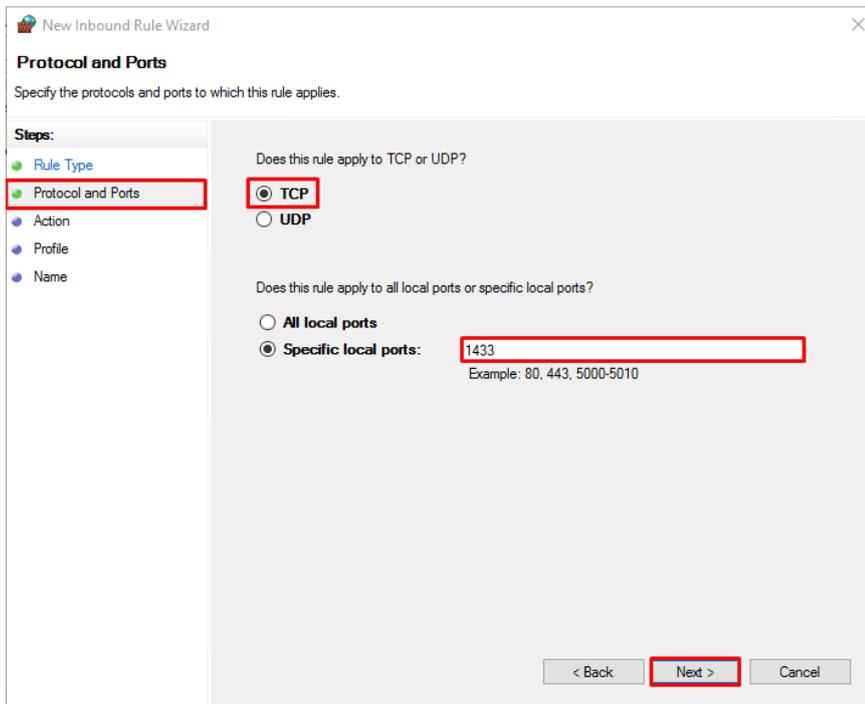
Click on “Inbound Rules” and select “New Rule...” in the “Actions” section.



In the “Rule Type” section, select the “Port” type and click the “Next” button.



➔ In the “Protocol and Ports” section, select “TCP” and enter the port number “1433”. Then click the “Next” button.

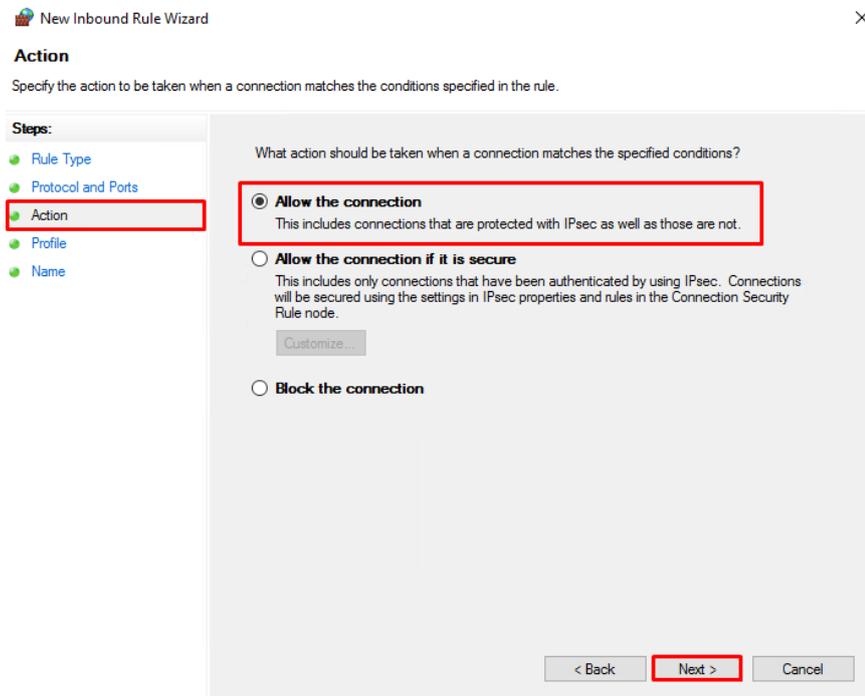


The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Protocol and Ports' step. The 'Steps' list on the left includes 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The 'Protocol and Ports' step is selected and highlighted with a red box. The main area contains the following options:

- 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:  (Example: 80, 443, 5000-5010)

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

➔ In the “Action” section, select the “Allow the connection” option and click the “Next” button.

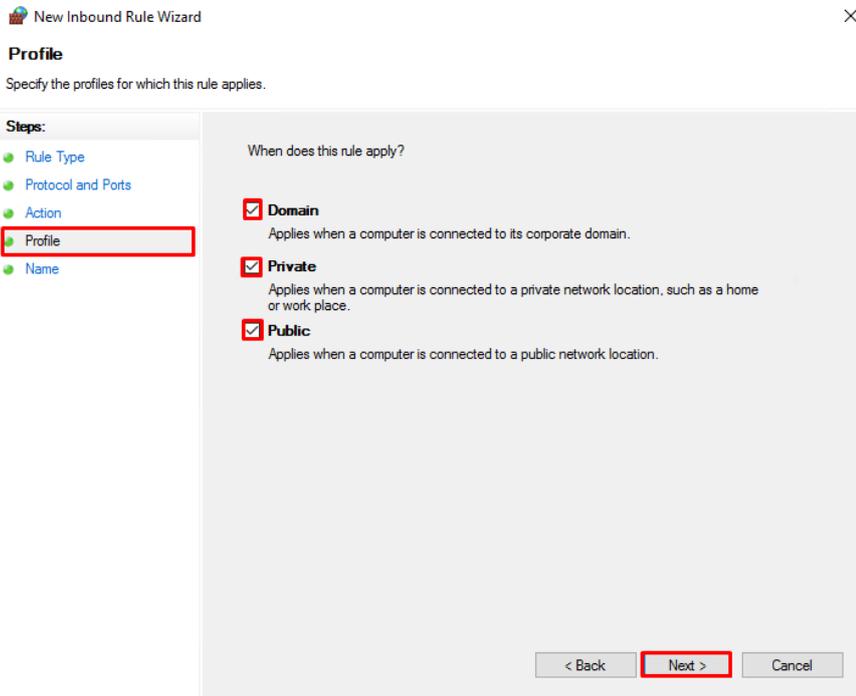


The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Action' step. The 'Steps' list on the left includes 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The 'Action' step is selected and highlighted with a red box. The main area contains the following options:

- 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.
  - Block the connection

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

👉 In the “Profile” section, check all three options: “Domain”, “Private”, “Public” and click “Next”.



New Inbound Rule Wizard

### Profile

Specify the profiles for which this rule applies.

**Steps:**

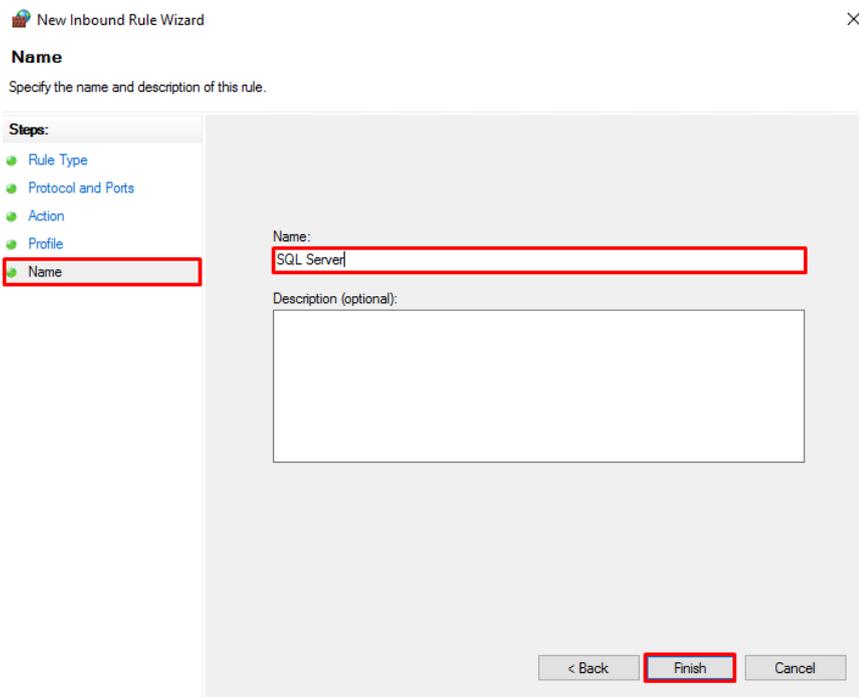
- Rule Type
- Protocol and Ports
- Action
- Profile**
- Name

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

👉 In the “Name” section, fill in the name of the “SQL Server” role and complete the setup with the “Finish” button.



New Inbound Rule Wizard

### Name

Specify the name and description of this rule.

**Steps:**

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

Name:

Description (optional):

< Back **Finish** Cancel

## 7 Setting permissions for access to the database

**i** The procedure for setting permissions differs depending on the type of database server configuration.

☞ From the variants below, select the type of database server configuration you want to use and set the permissions using Management Studio accordingly.

1. **Local access** – The database server is installed on the same computer as the application server.
2. **Access via technology account from Active Directory** – The database server is installed on a different computer than the application server, and NET Genium accesses the database under a technology account from Active Directory.
3. **Access via local SQL Server account** – The database server is installed on a different computer than the application server, and NET Genium accesses the database under the local SQL Server account.

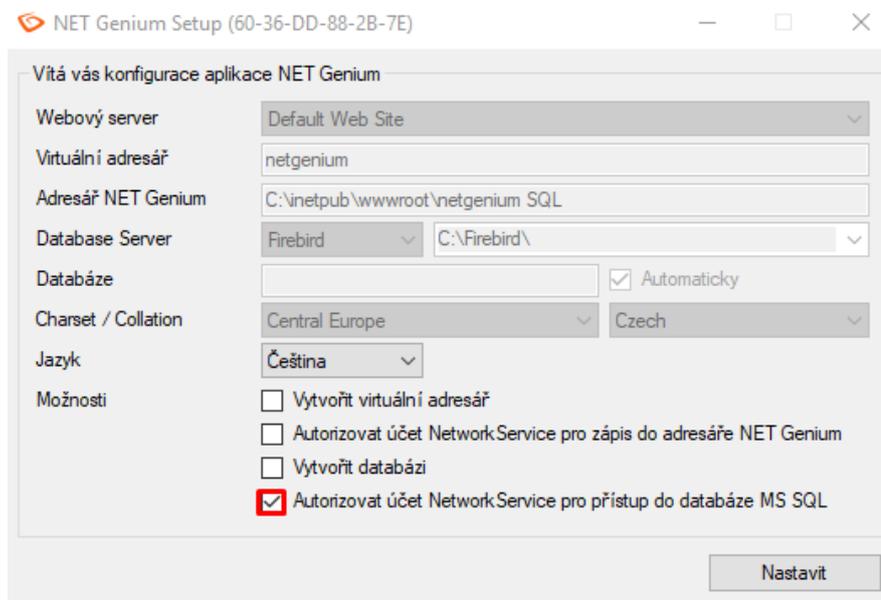
### 7.1 Setting permissions for local access

**i** There are 2 ways to set permissions for local access:

- Automatic authorization settings via the “Setup.exe” NET Genium program.
- Manually set permissions via “Microsoft SQL Server Management Studio”.

#### 7.1.1 Automatic permission setting via the “Setup.exe” NET Genium program

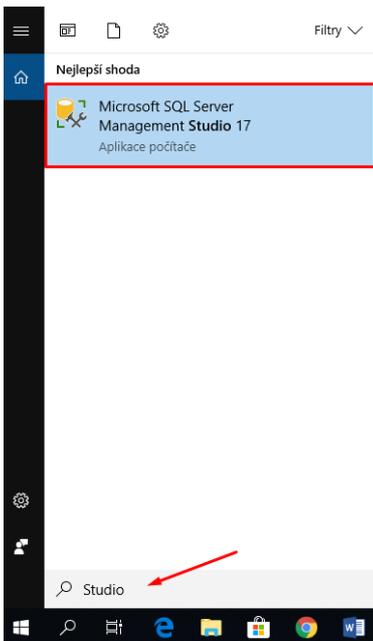
**i** When installing NET Genium via “Setup.exe” and checking the “Authorize Network Service account to access the MSSQL database” option, the program automatically sets the permissions to access the database (see the “NET Genium Installation” manual).



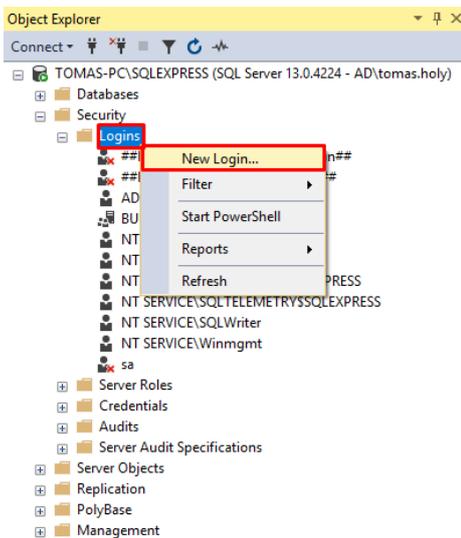
## 7.1.2 Manually set permissions through “Microsoft SQL Server Management Studio”

1 The settings for accessing the database to the predefined “NetworkService” account, which is selected in the application pool identity, are described below.

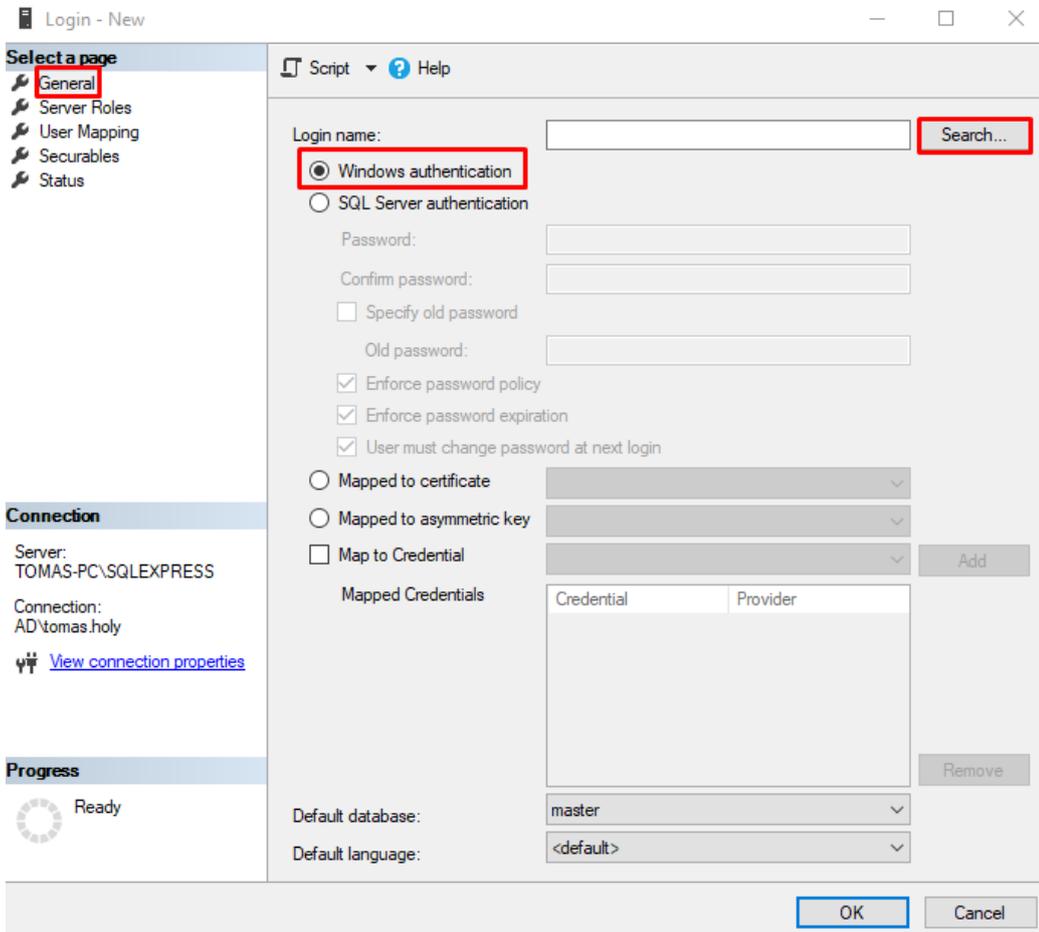
↳ From the “Start” menu, locate and run “Microsoft SQL Server Management Studio”.



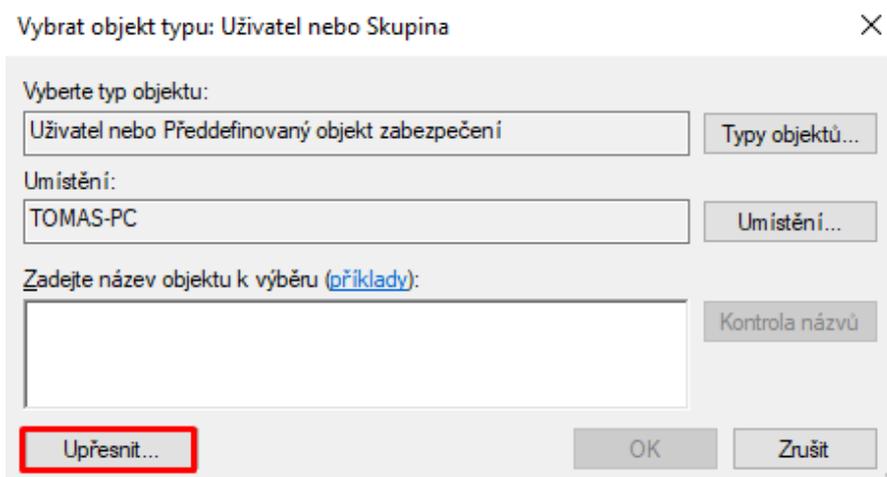
↳ Open the “Security” node, right-click on “Logins” and select “New Login...”.



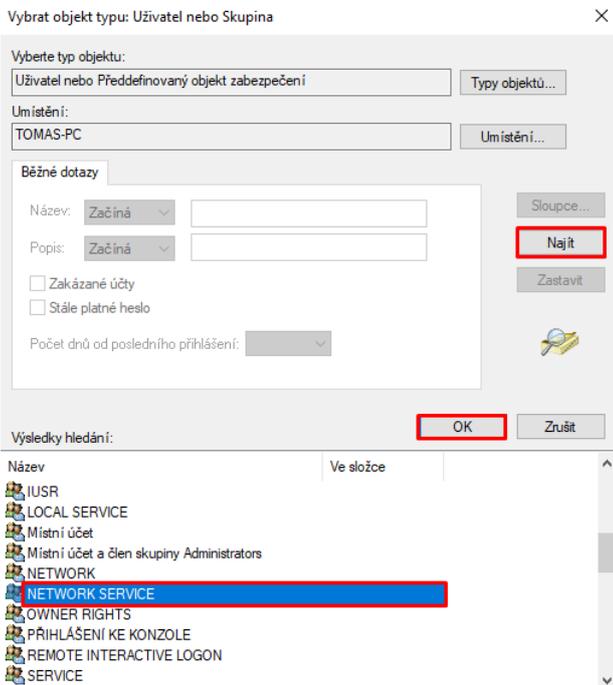
☞ On the “General” tab, check “Windows authentication” and click on the “Search...” button.



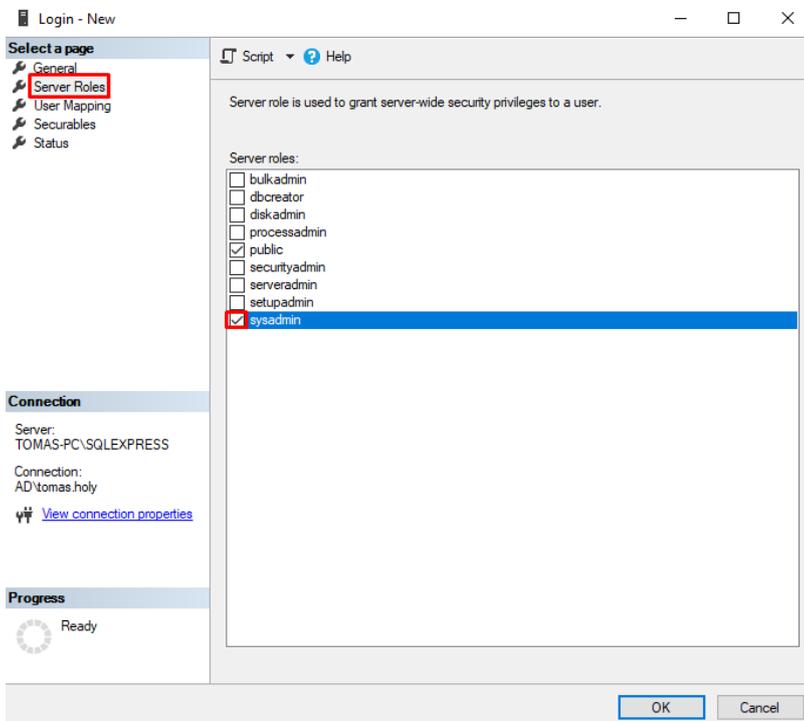
☞ In the newly opened dialog, click on the “Advanced” button.



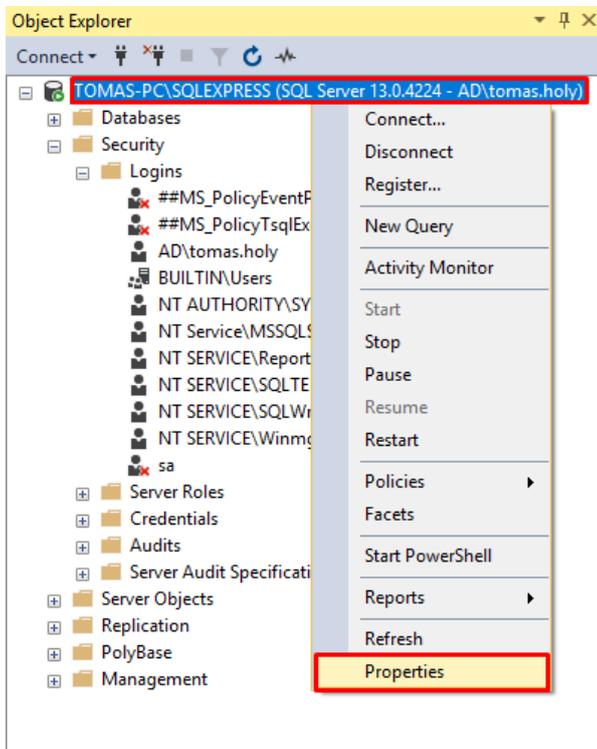
Click on the “Find” button, search for the “NETWORK SERVICE” account and confirm your choice with the “OK” button.



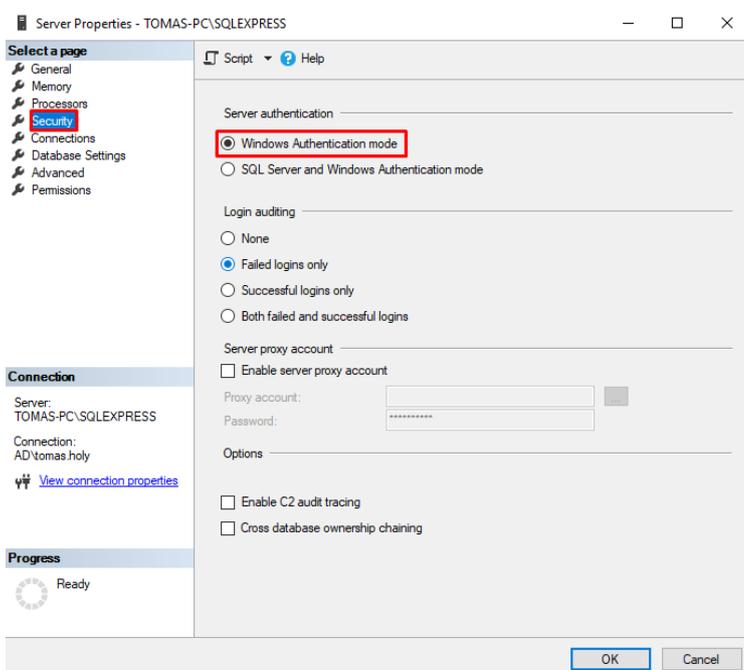
On the “Server Roles” tab, check the “sysadmin” option and confirm with the “OK” button.



➔ Right-click on the main node of your SQL Server and select the “Properties” option.



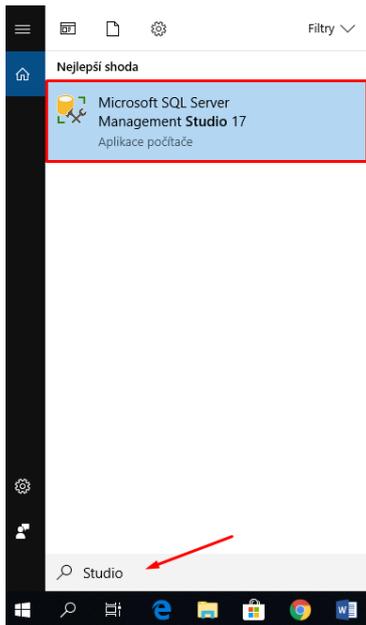
➔ On the “Security” tab, make sure that the default option “Windows Authentication mode” is checked.



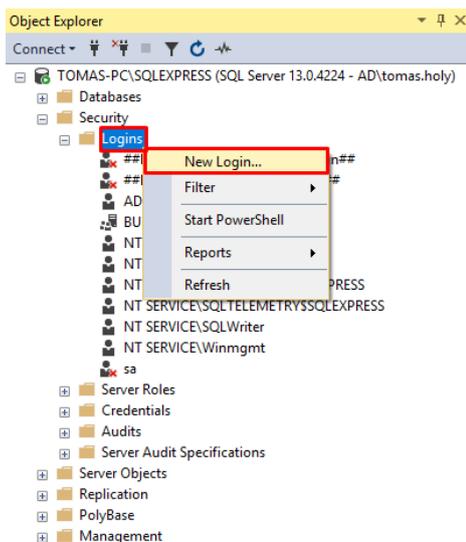
## 7.2 Setting permissions for access through the technology account from Active Directory

1 The following describes how to set permissions for accessing the database to a technology account that is selected in the application pool identity – for example, “AD\svcnadmin”.

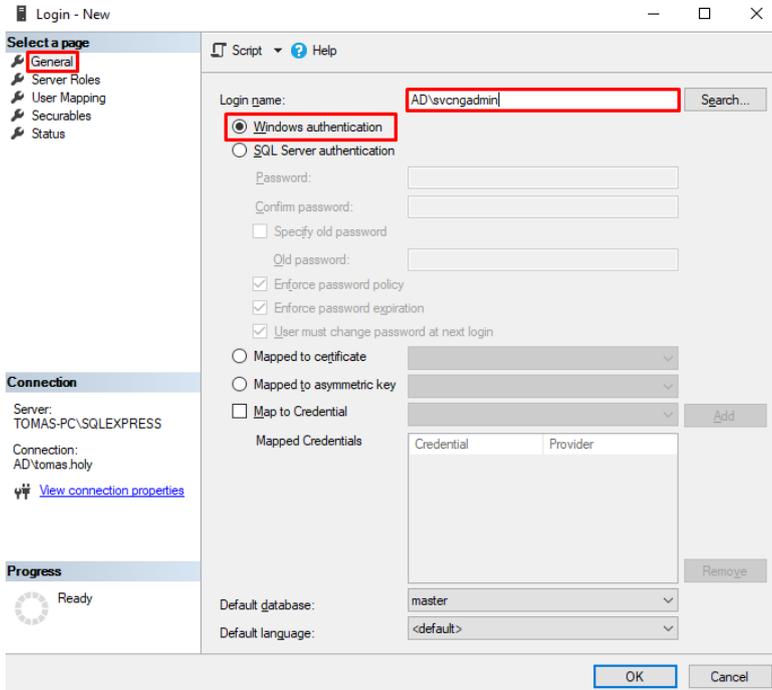
From the “Start” menu, locate and run “Microsoft SQL Server Management Studio”.



Open the “Security” node, right-click on “Logins” and select “New Login...”.

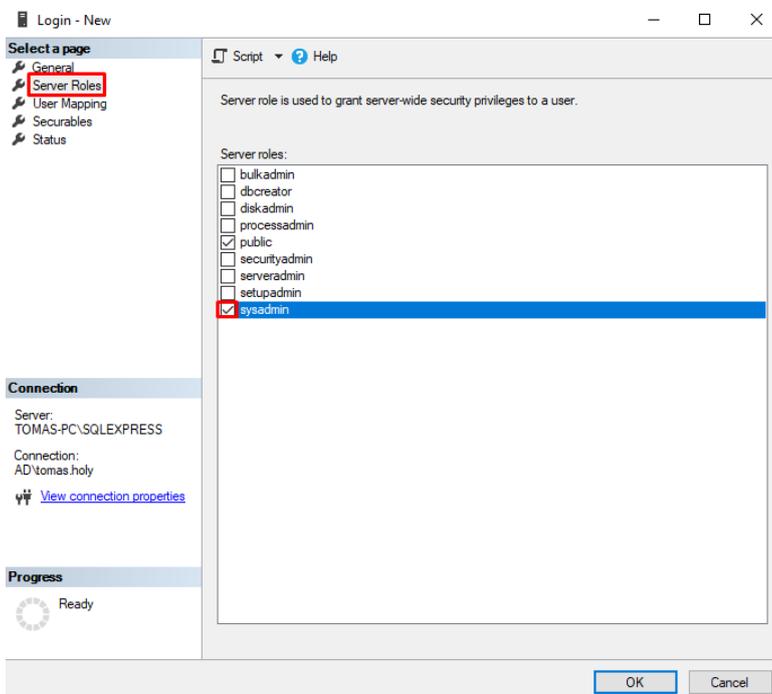


- ➔ On the “General” tab, check “Windows authentication” and enter the name of the technology account from Active Directory, including the domain name, for example “AD\svcnadmin” in the “Login name:” field.



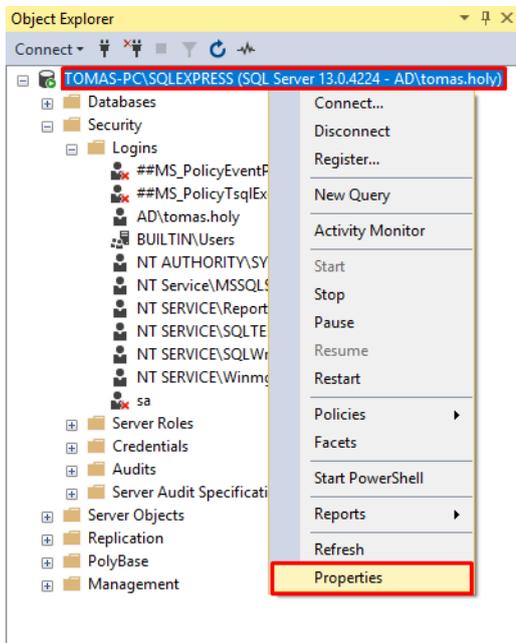
The screenshot shows the 'Login - New' dialog box with the 'General' tab selected. The 'Login name' field is populated with 'AD\svcnadmin'. The 'Windows authentication' radio button is selected, and the 'SQL Server authentication' radio button is unselected. The 'Default database' is set to 'master' and the 'Default language' is '<default>'. The 'OK' button is highlighted.

- ➔ On the “Server Roles” tab, check the “sysadmin” option and confirm with the “OK” button.

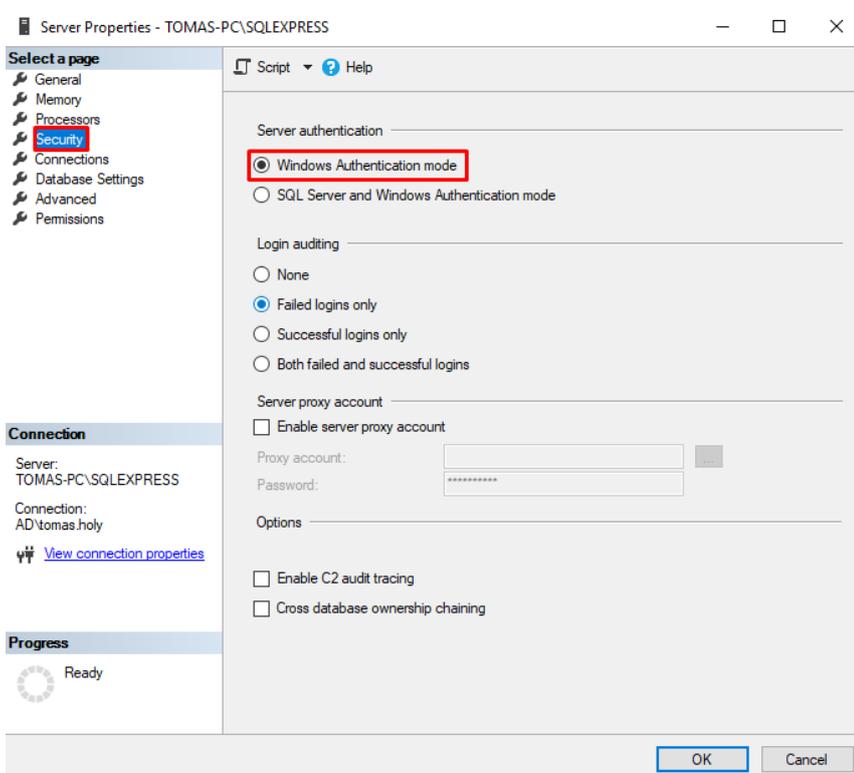


The screenshot shows the 'Login - New' dialog box with the 'Server Roles' tab selected. The 'sysadmin' server role is checked. The 'OK' button is highlighted.

➔ Right-click on the main node of your SQL Server and select the “Properties” option.



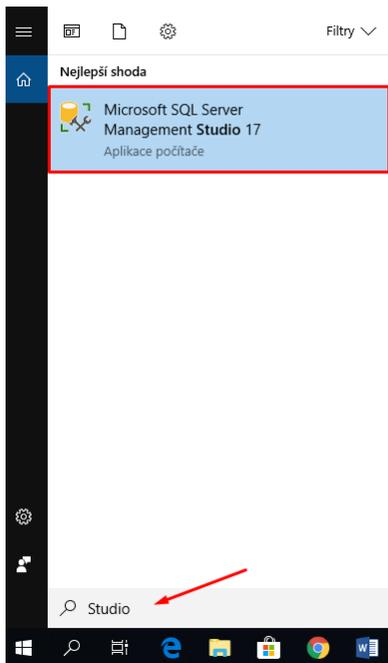
➔ On the “Security” tab, make sure that the default option “Windows Authentication mode” is checked.



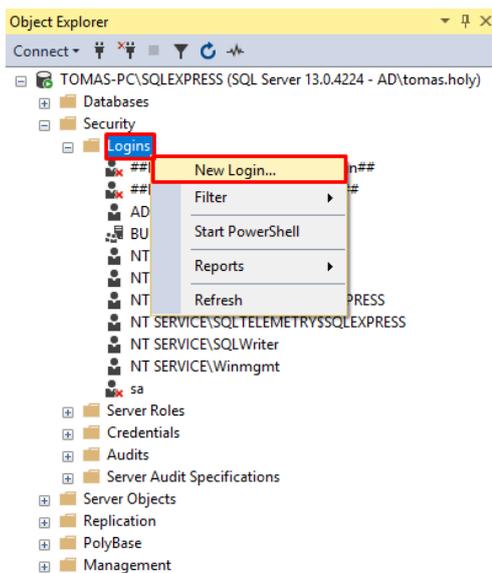
## 7.3 Setting permissions for access through the local SQL Server account

**i** The following describes how to set permissions to access the database on a local SQL Server account that is different from the technology account set in the application pool identity.

**h** From the “Start” menu, locate and run “Microsoft SQL Server Management Studio”.

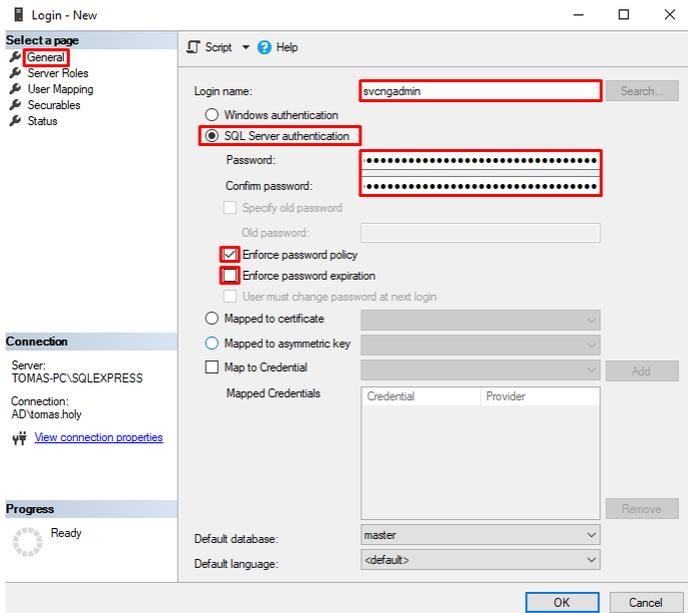


**h** Open the “Security” node, right-click on “Logins” and select “New Login...”.

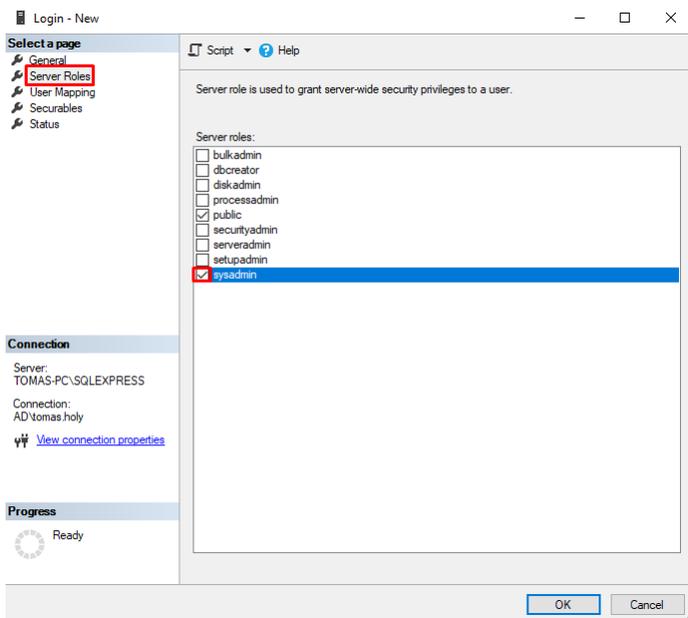


➔ On the “General” tab page, fill in:

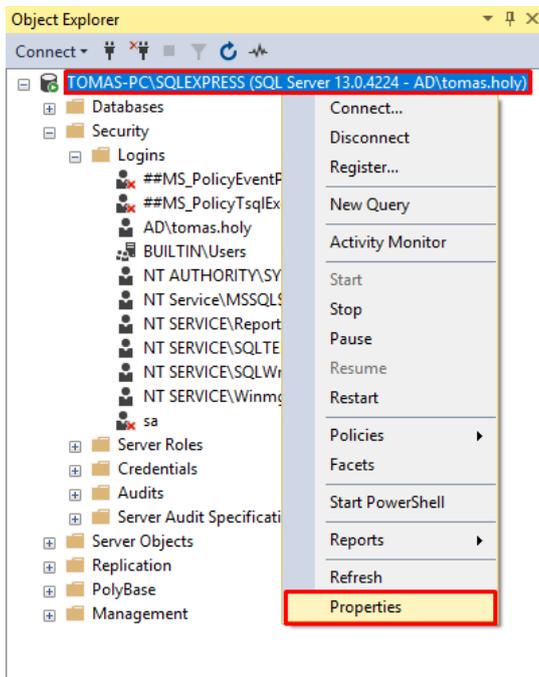
- Login name: for example “svngadmin”
- Check “SQL Server authentication”
- Password: choose a very strong password (this password will be specified in the “ConnectionString.txt” file)
- Check “Enforce password policy”
- Uncheck “Enforce password expiration”



➔ On the “Server Roles” tab, check the “sysadmin” option and confirm with the “OK” button.



➔ Right-click on the main node of your SQL Server and select the “Properties” option.



➔ On the “Security” tab, check the “SQL Server and Windows Authentication mode” option and confirm with the “OK” button.

