

# 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

❶ 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

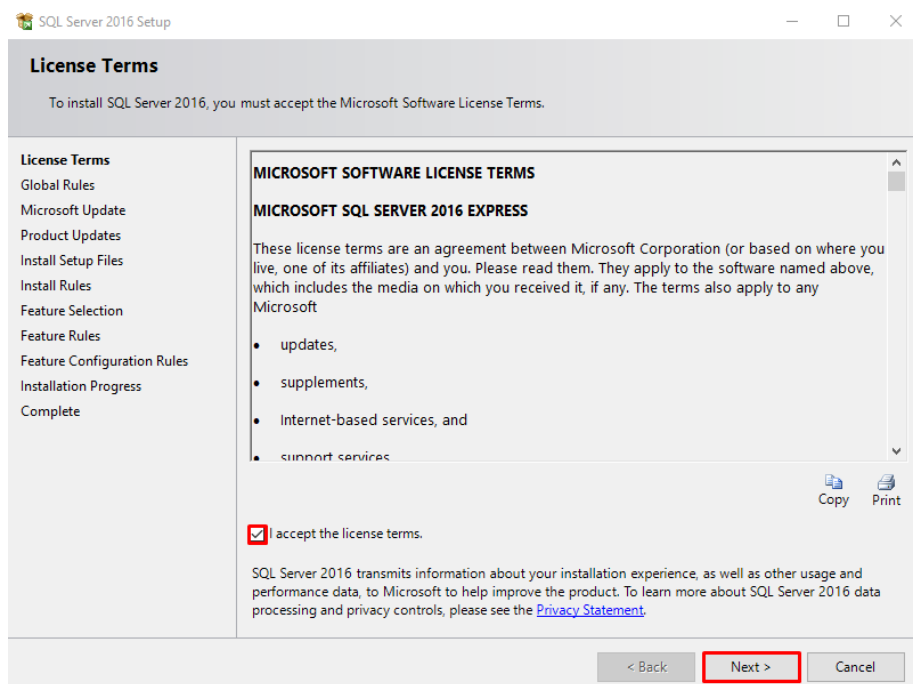
👉 Mount the installation media in “iso” format, or open the “O:\Install\\_WIN\SQLServer2016Media” directory on the shared “\\office” server if the installation is located within the NetGenium internal computer network.

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

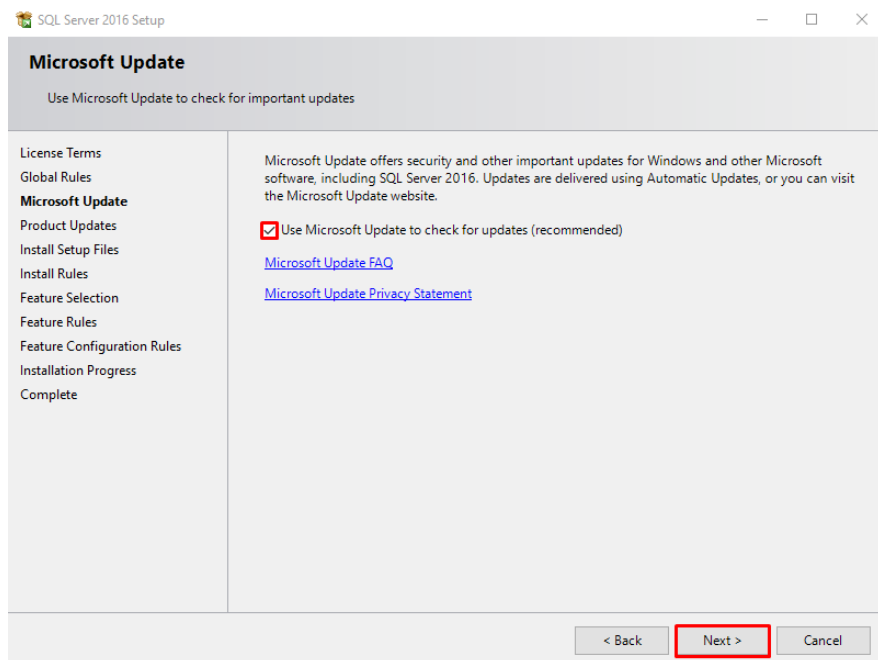
- 👉 Run the “SETUP.exe” program.
- 👉 In the “Installation” section, select the “New SQL Server stand-alone installation or add features to an existing installation” option.



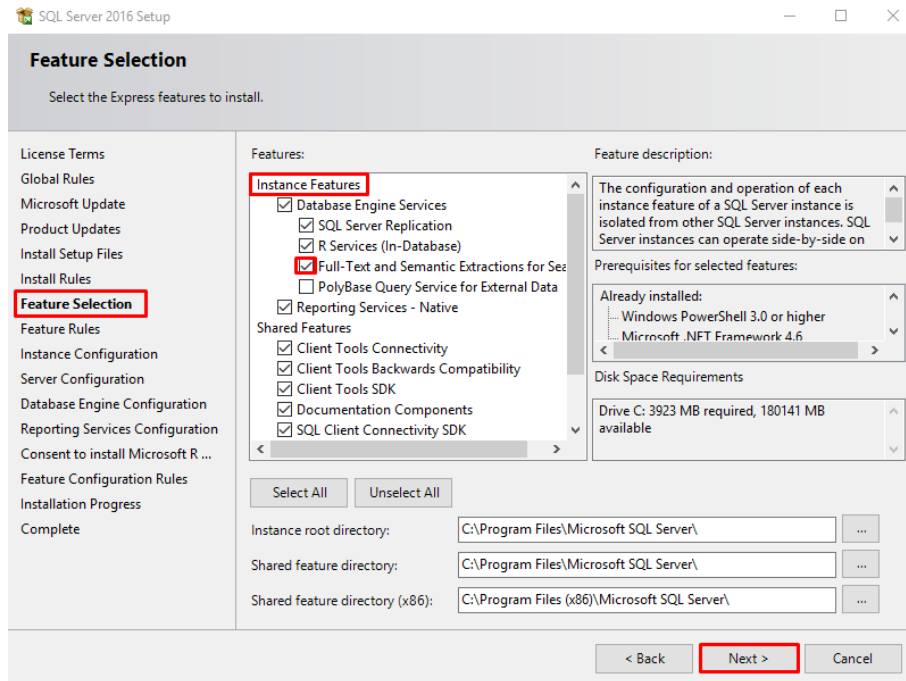
☛ Agree to the license terms and click “Next”.



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



- ❗ 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.



SQL Server 2016 Setup

### Feature Selection

Select the Express features to install.

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

Features:

**Instance Features**

- ☒ Database Engine Services
- ☒ SQL Server Replication
- ☒ R Services (In-Database)
- ☒ Full-Text and Semantic Extractions for Search
- ☐ PolyBase Query Service for External Data
- ☒ Reporting Services - Native

Shared Features

- ☒ Client Tools Connectivity
- ☒ Client Tools Backwards Compatibility
- ☒ Client Tools SDK
- ☒ Documentation Components
- ☒ SQL Client Connectivity SDK

Select All Unselect All

Instance root directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

Feature description:

The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL Server instances can operate side-by-side on

Prerequisites for selected features:

Already installed:

- Windows PowerShell 3.0 or higher
- Microsoft .NET Framework 4.6

Disk Space Requirements

Drive C: 3923 MB required, 180141 MB available

< Back **Next >** Cancel

- ➔ 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 ▾
SQL Server Reporting Services	NT Service\ReportServer...		Automatic ▾
SQL Server Launchpad	NT Service\MSSQLLaun...		Automatic
SQL Full-text Filter Daemon Launc...	NT Service\MSSQLFDLa...		Manual
SQL Server Browser	NT AUTHORITY\LOCAL ...		Disabled ▾

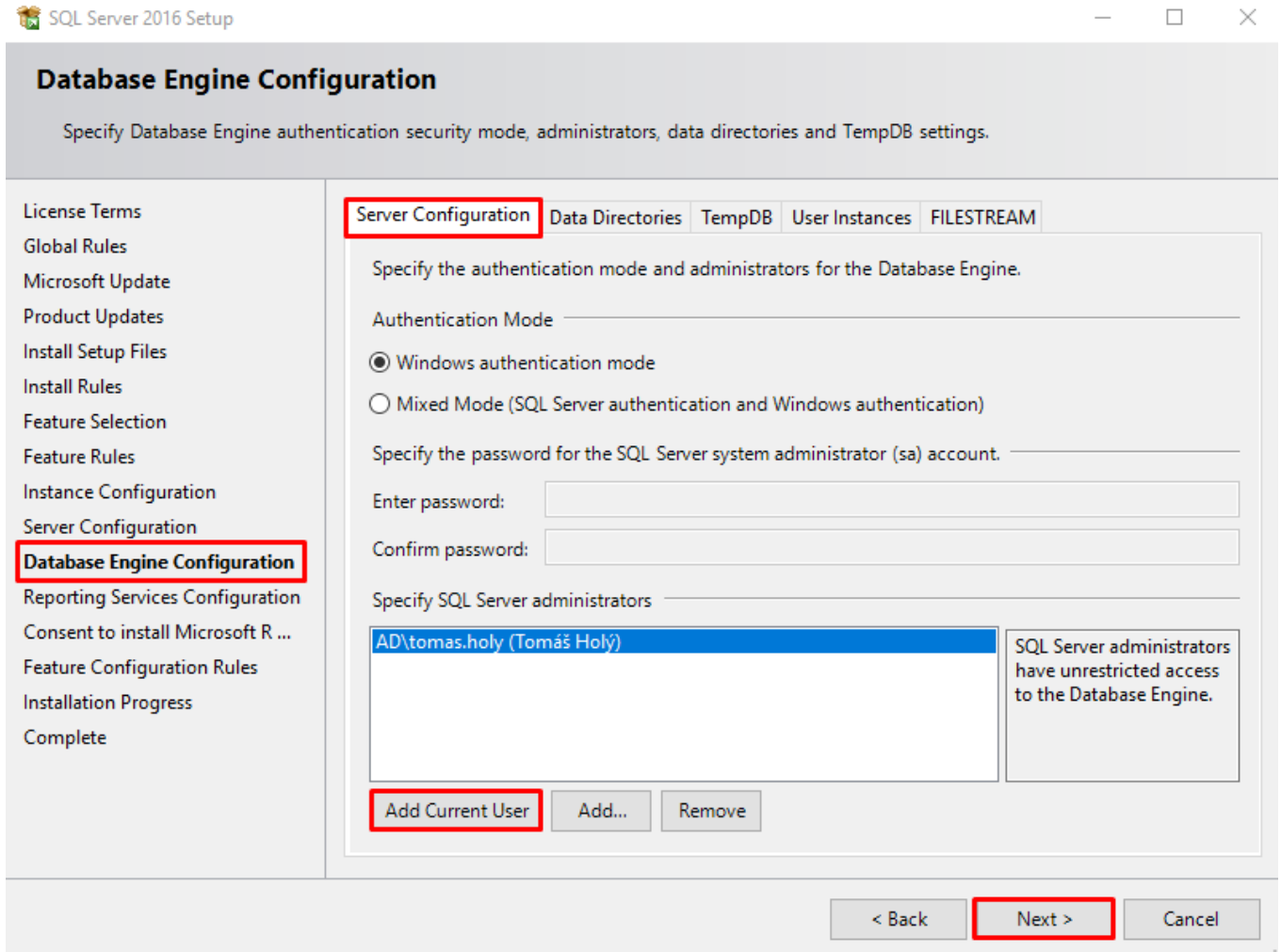
☒ Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service

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.



SQL Server 2016 Setup

### Database Engine Configuration

Specify Database Engine authentication security mode, administrators, data directories and TempDB settings.

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

**Server Configuration** Data Directories TempDB User Instances FILESTREAM

Specify the authentication mode and administrators for the Database Engine.

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:   
Confirm password:

Specify SQL Server administrators

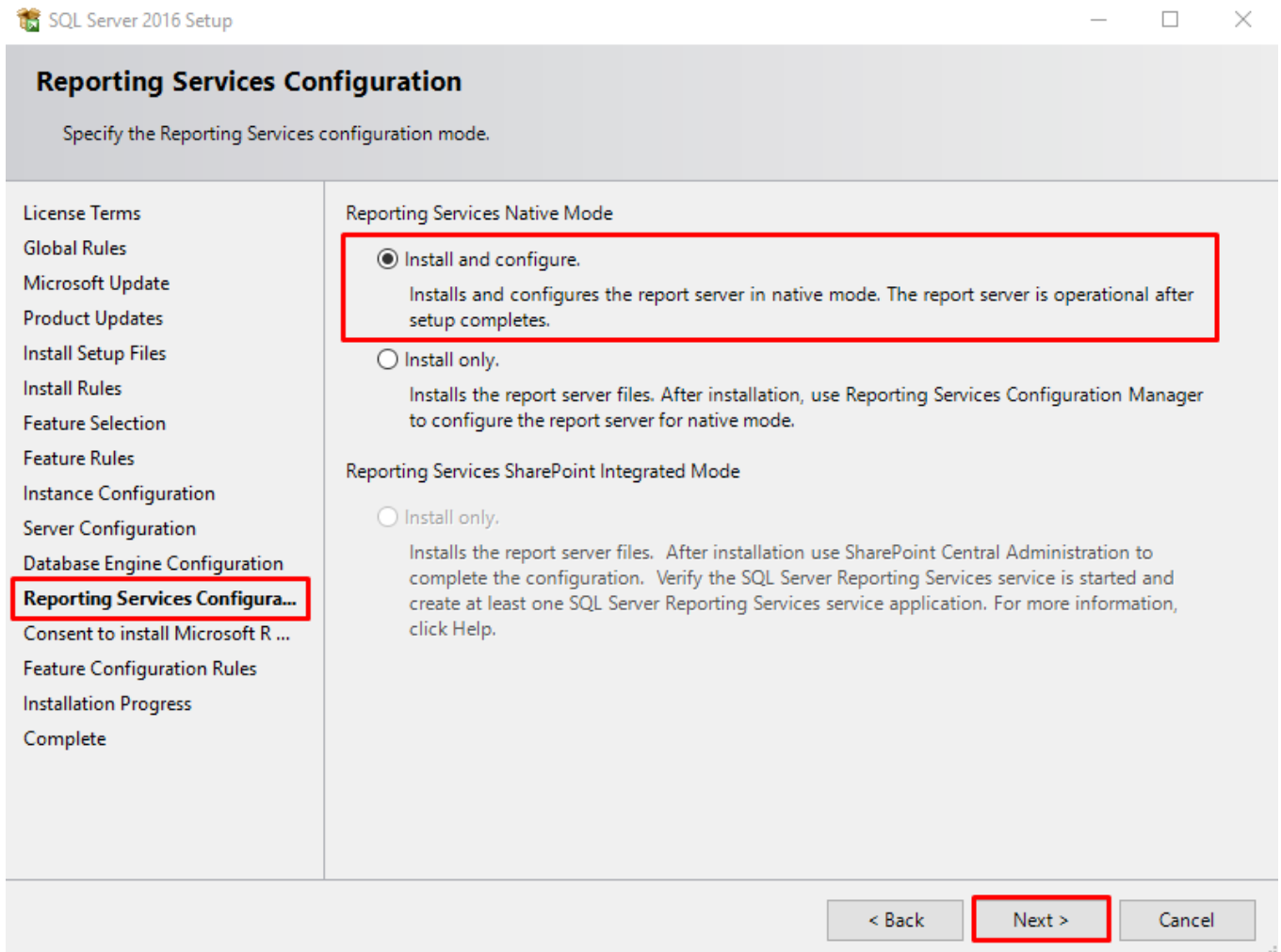
AD\tomas.holy (Tomáš Holý)	SQL Server administrators have unrestricted access to the Database Engine.

**Add Current User** Add... Remove

< Back **Next >** Cancel



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



The screenshot shows the "SQL Server 2016 Setup" window, specifically the "Reporting Services Configuration" section. The window title is "SQL Server 2016 Setup". The main heading is "Reporting Services Configuration" with the subtitle "Specify the Reporting Services configuration mode.".

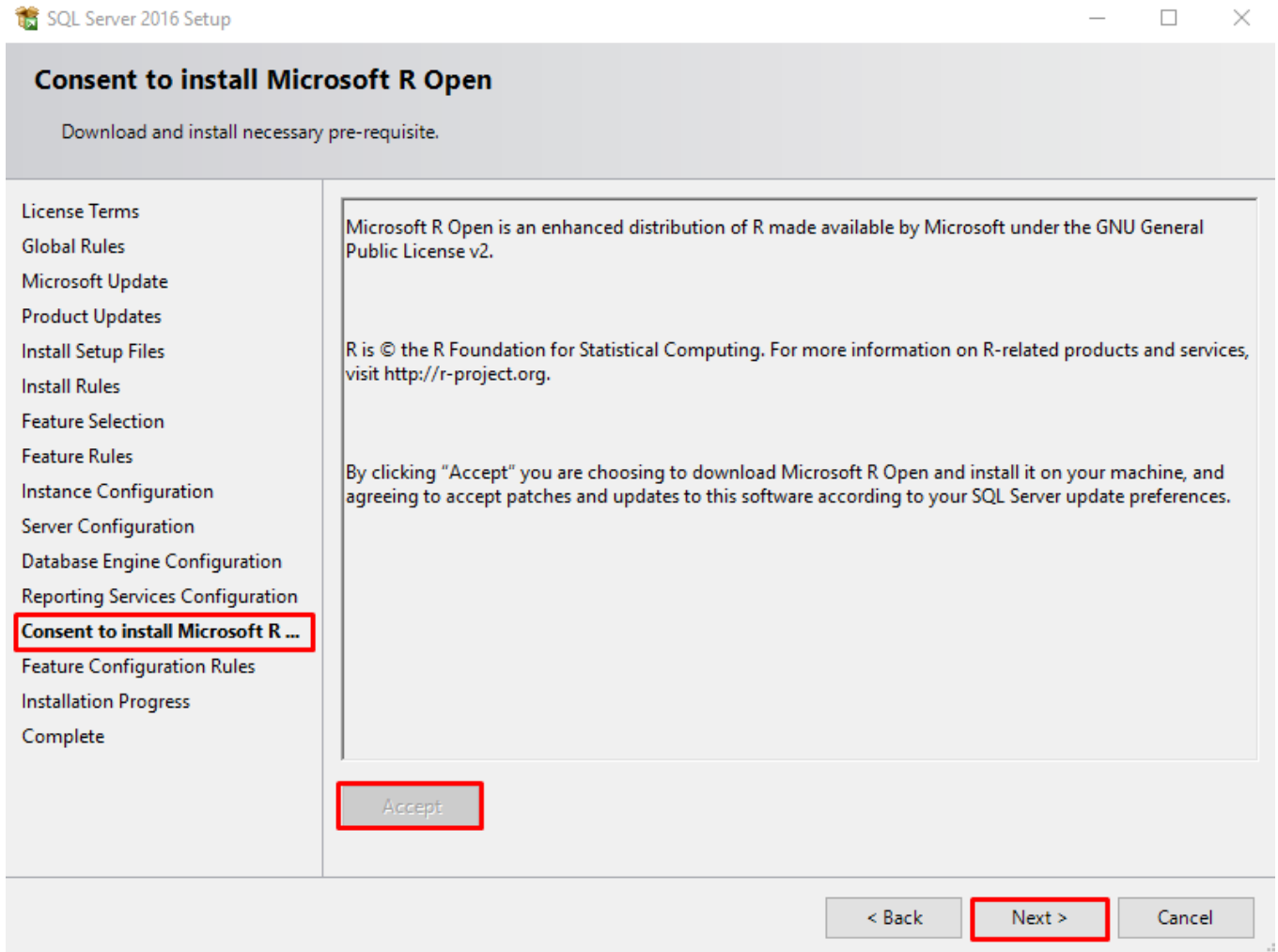
On the left, a list of setup steps is shown, with "Reporting Services Configura..." highlighted in a red box. The main area displays two configuration modes:

- Reporting Services Native Mode**
  - ☒ **Install and configure.**  
Installs and configures the report server in native mode. The report server is operational after setup completes.
  - ☐ **Install only.**  
Installs the report server files. After installation, use Reporting Services Configuration Manager to configure the report server for native mode.
- Reporting Services SharePoint Integrated Mode**
  - ☐ **Install only.**  
Installs the report server files. After installation use SharePoint Central Administration to complete the configuration. Verify the SQL Server Reporting Services service is started and create at least one SQL Server Reporting Services service application. For more information, click Help.

At the bottom right, there are three buttons: "< Back", "Next >" (highlighted with a red box), and "Cancel".



- 🔗 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.

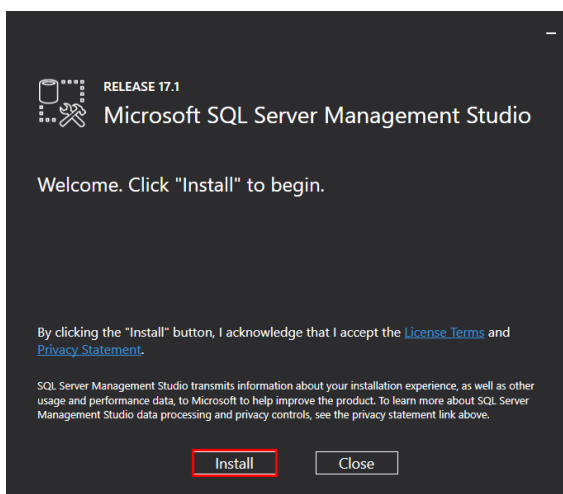
## 3 Install SQL Server Management Studio

### 3.1 Installation preparation

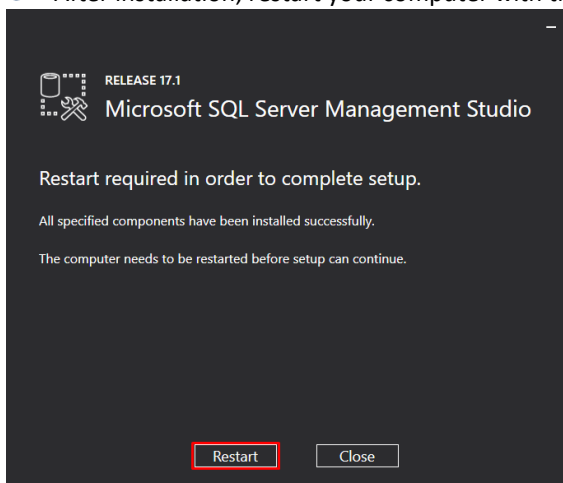
- ☛ Mount the installation media in “iso” format, or if the installation is located within the NetGenium internal computer network, open the “O:\Install\\_WIN” directory on the “\\office” shared server.

### 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:

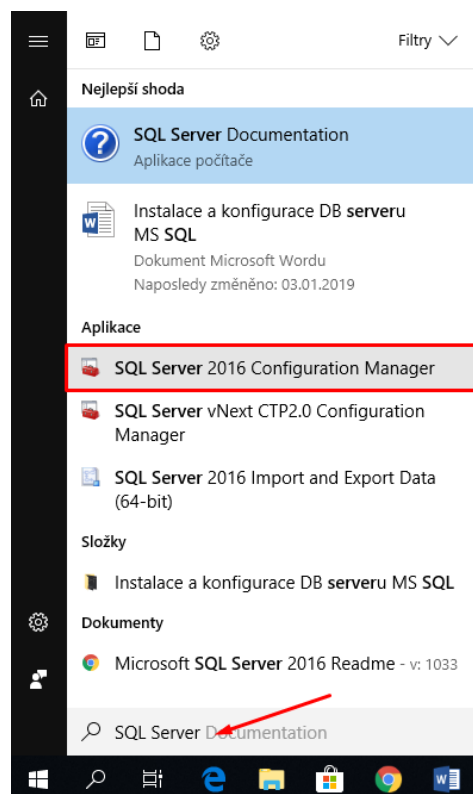
- IP address or name of the database server
- Database name
- The name of the local SQL Server account
- Password in this account

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

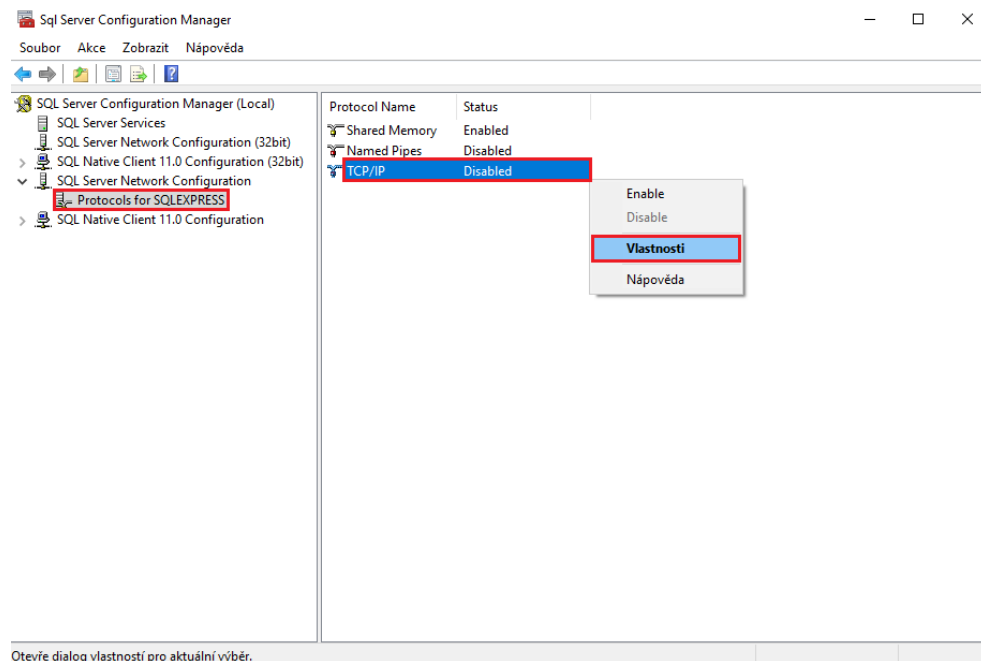
## 5 Network penetration settings

⚠ *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.*

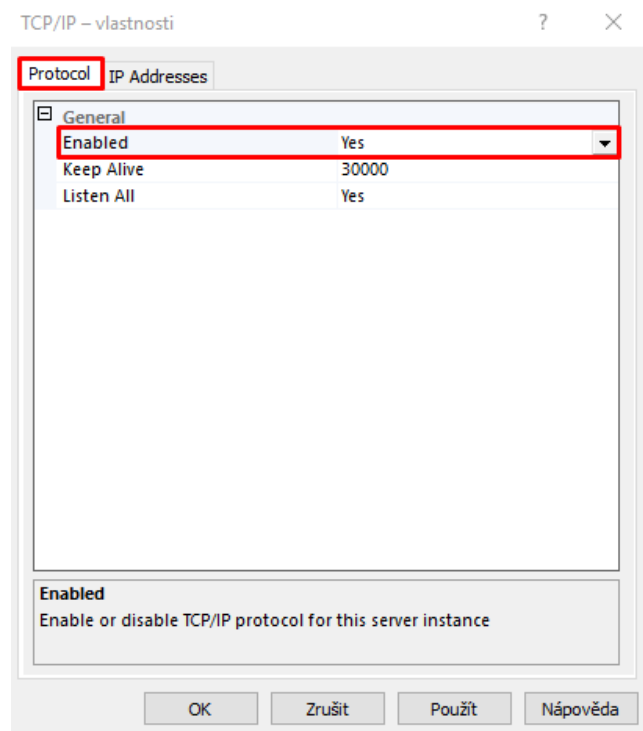
👉 From the “Start” menu, locate and run “SQL Server 2016 Configuration Manager”.



- 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”.

TCP/IP – vlastnosti

Protocol **IP Addresses**

<b>IP1</b>	
Active	Yes
Enabled	Yes
IP Address	fe80::3d46:542c:2092:a329%10
TCP Dynamic Ports	0
TCP Port	
<b>IP10</b>	
Active	Yes
Enabled	No
IP Address	169.254.207.73
TCP Dynamic Ports	0
TCP Port	
<b>IP11</b>	
Active	Yes
Enabled	No
IP Address	::1
TCP Dynamic Ports	0
TCP Port	

**IP1**

OK Zrušit Použít Nápověda

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

TCP/IP – vlastnosti

Protocol **IP Addresses**

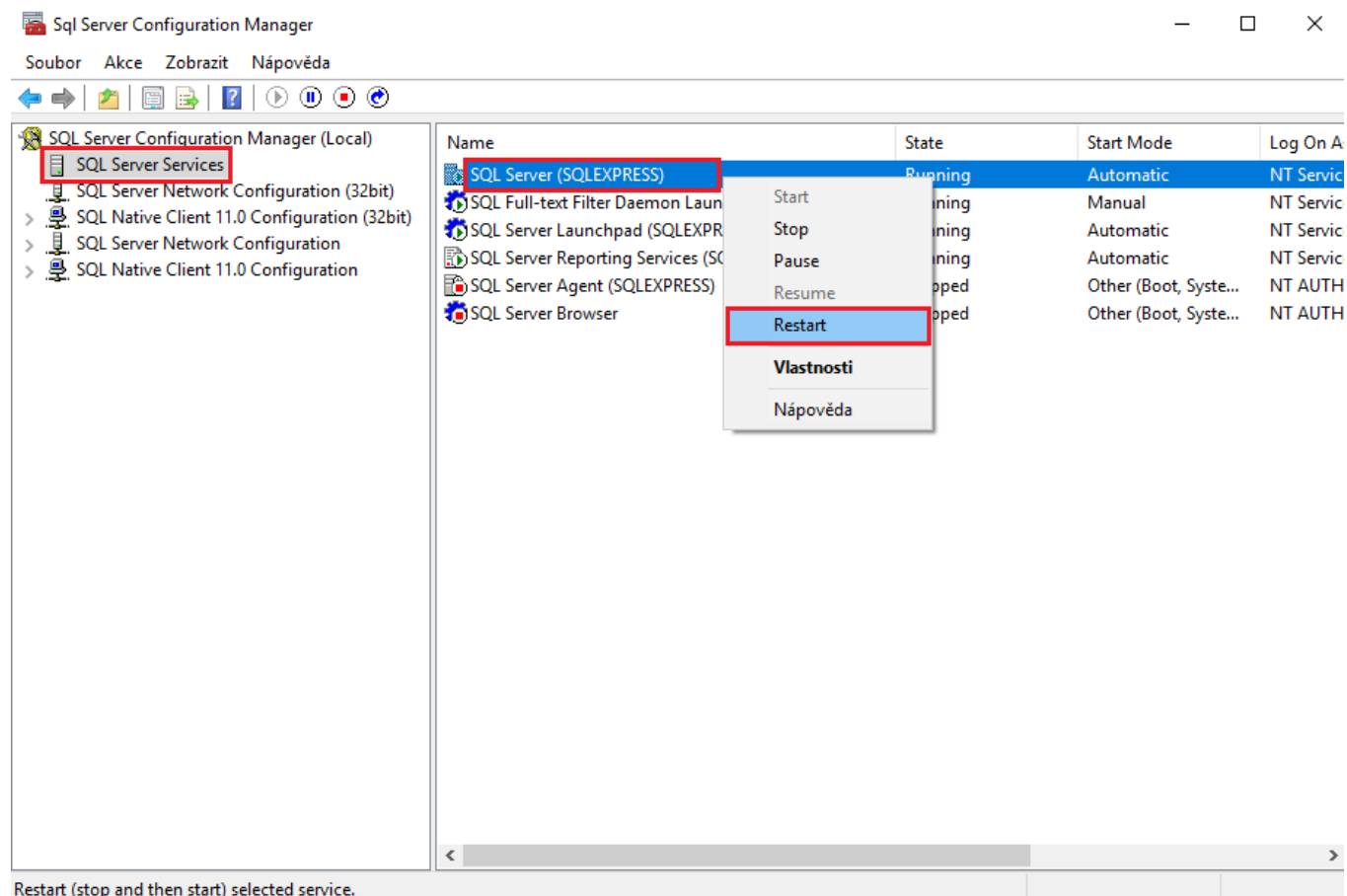
TCP Dynamic Ports	0
TCP Port	
<b>IP8</b>	
Active	Yes
Enabled	No
IP Address	192.168.249.38
TCP Dynamic Ports	0
TCP Port	
<b>IP9</b>	
Active	Yes
Enabled	No
IP Address	fe80::c490:6311:ee06:cf49%11
TCP Dynamic Ports	0
TCP Port	
<b>IPALL</b>	
TCP Dynamic Ports	0
TCP Port	1433

**TCP Port**  
TCP port

OK Zrušit Použít Nápověda

❗ 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”.

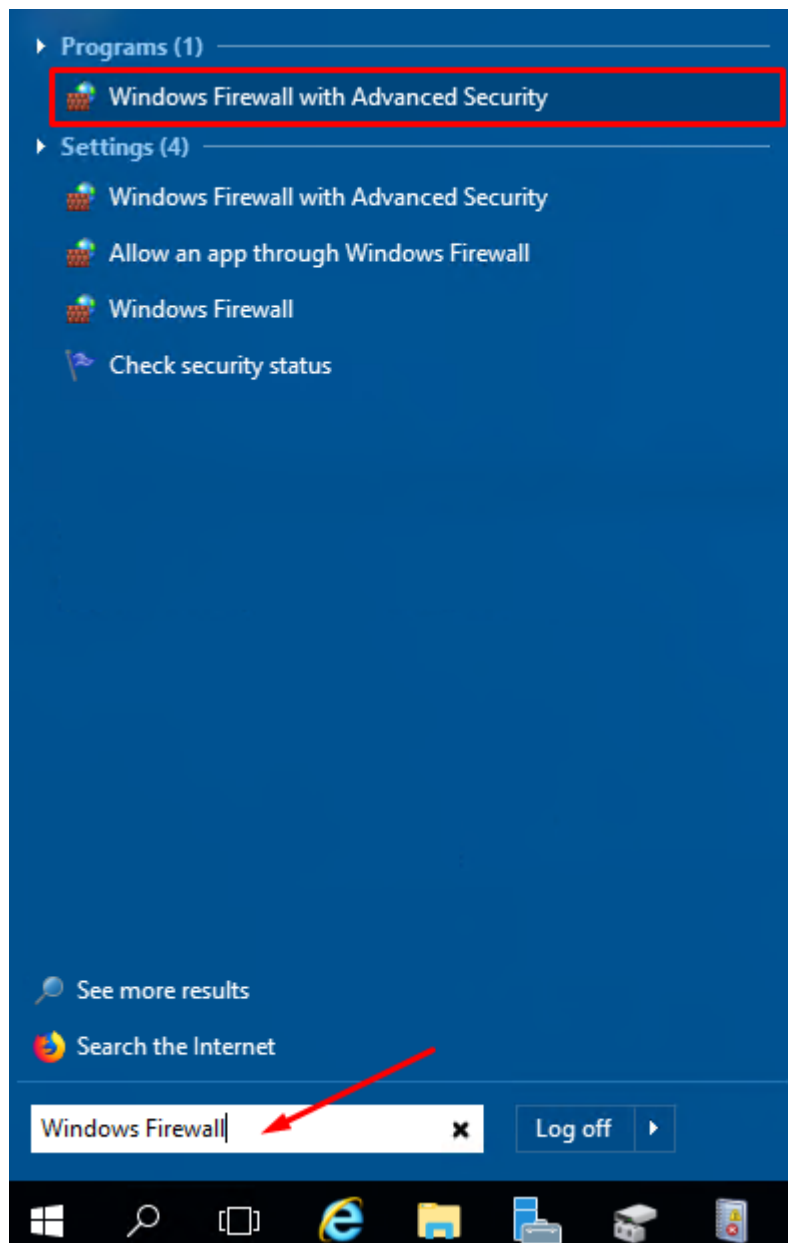




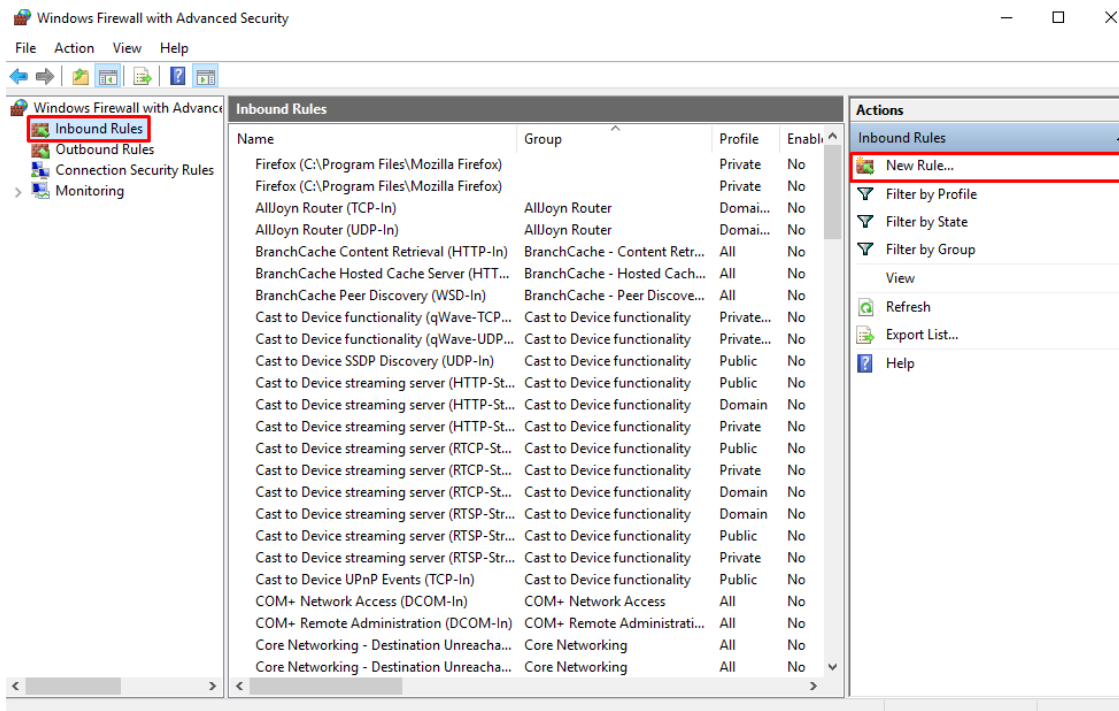
## 6 Firewall settings

⚠ 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.

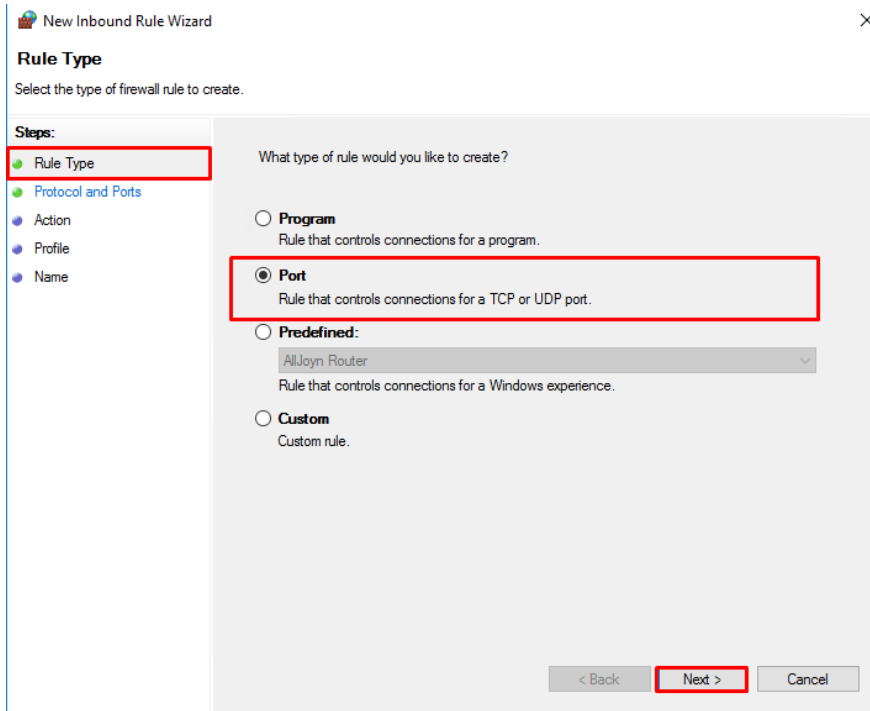
👉 From the “Start” menu, locate and launch “Windows Firewall with Advanced Security”.



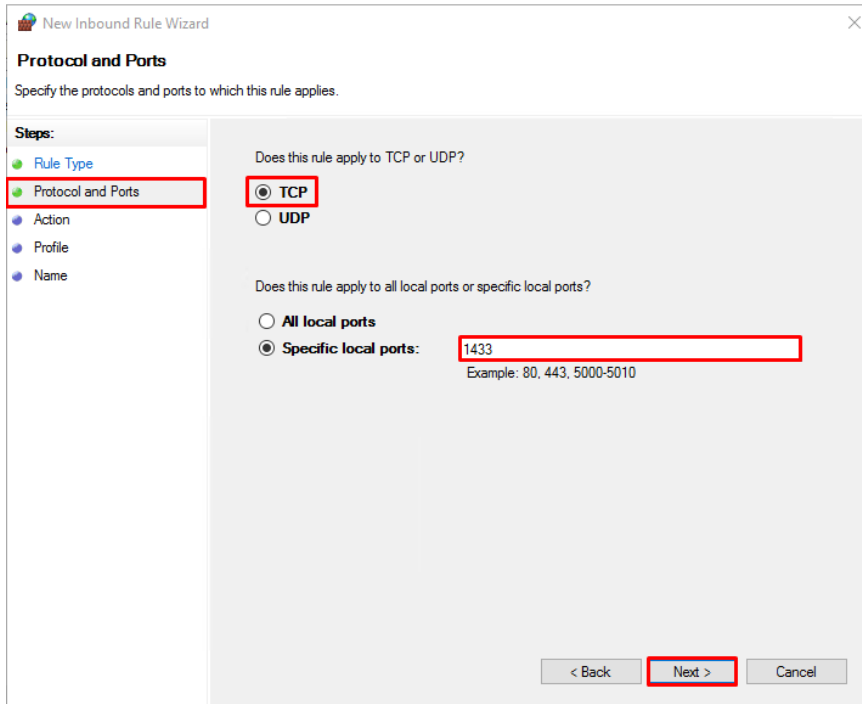
Click on “Inbound Rules” and select “New Rule...” in the “Actions” section.



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

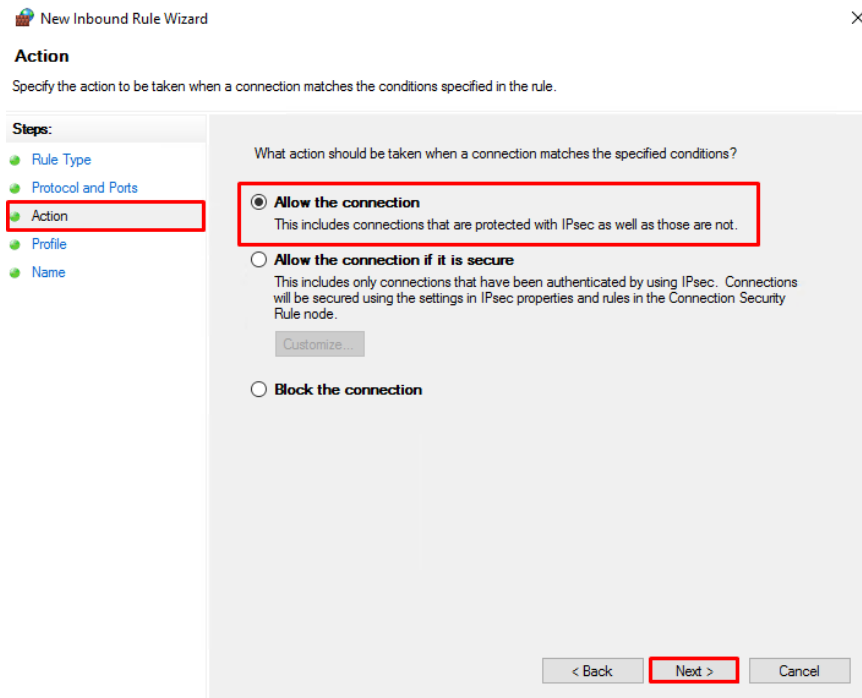


👉 In the “Protocol and Ports” section, select “TCP” and enter the port number “1433”. Then click the “Next” button.



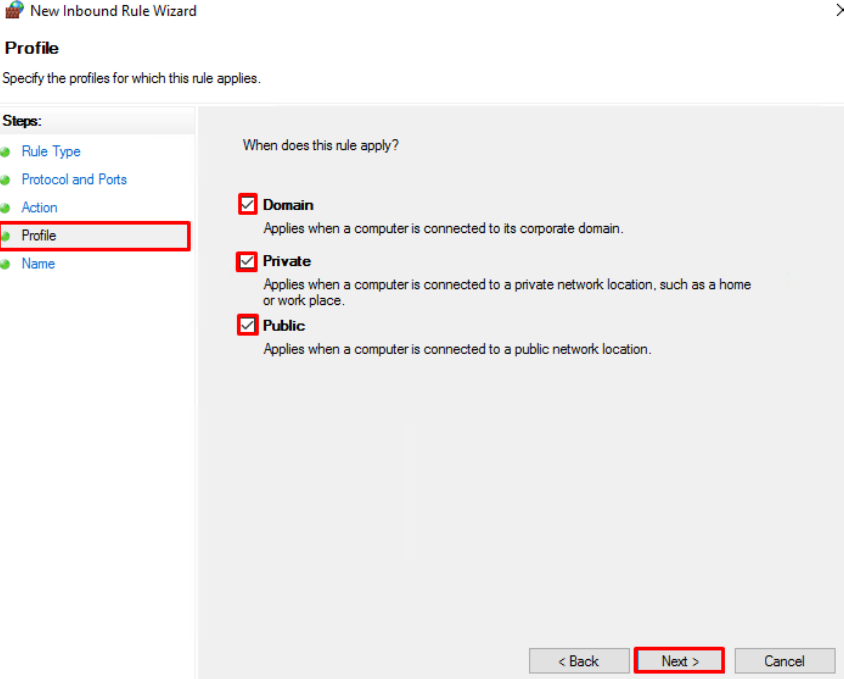
The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The 'Steps' list on the left includes 'Rule Type', 'Protocol and Ports' (highlighted with a red box), 'Action', 'Profile', and 'Name'. The main area contains two questions: 'Does this rule apply to TCP or UDP?' with 'TCP' selected (radio button and highlighted with a red box), and 'Does this rule apply to all local ports or specific local ports?' with 'Specific local ports:' selected (radio button) and the port number '1433' entered in the text box (highlighted with a red box). Below the text box is an example: 'Example: 80, 443, 5000-5010'. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.

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



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The 'Steps' list on the left includes 'Rule Type', 'Protocol and Ports', 'Action' (highlighted with a red box), 'Profile', and 'Name'. The main area contains the question 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 'Allow the connection' (selected and highlighted with a red box), 'Allow the connection if it is secure', and 'Block the connection'. Below 'Allow the connection' is a description: 'This includes connections that are protected with IPsec as well as those are not.' Below 'Allow the connection if it is secure' is a description: '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.' and a 'Customize...' button. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.

👉 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?

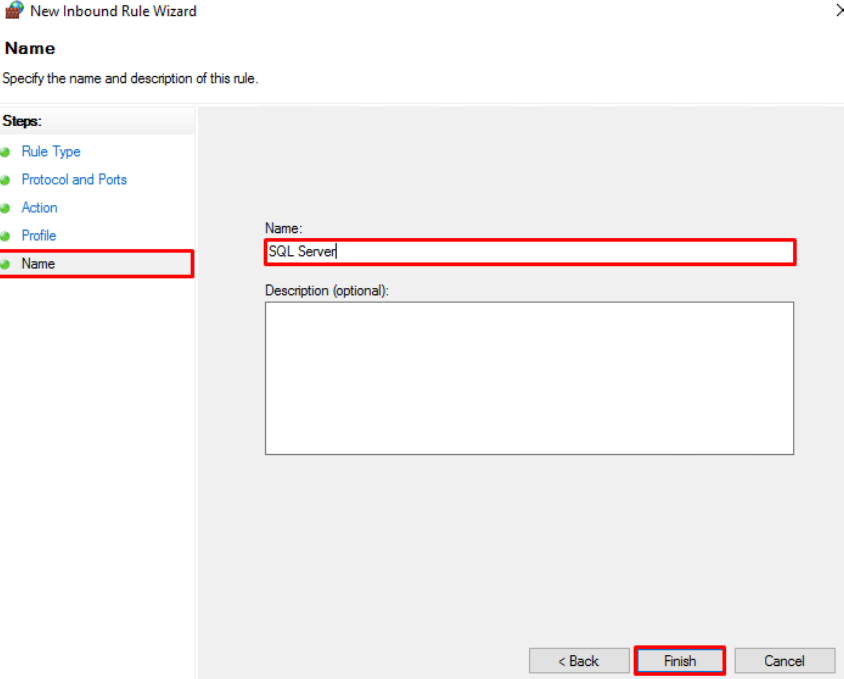
☒ **Domain**  
Applies when a computer is connected to its corporate domain.

☒ **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.

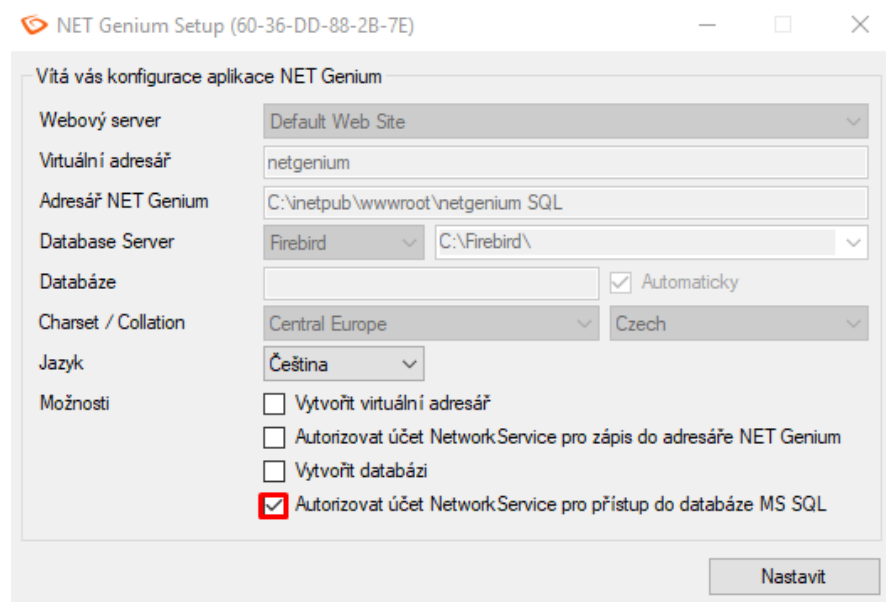
### 7.1 Setting permissions for local access

**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

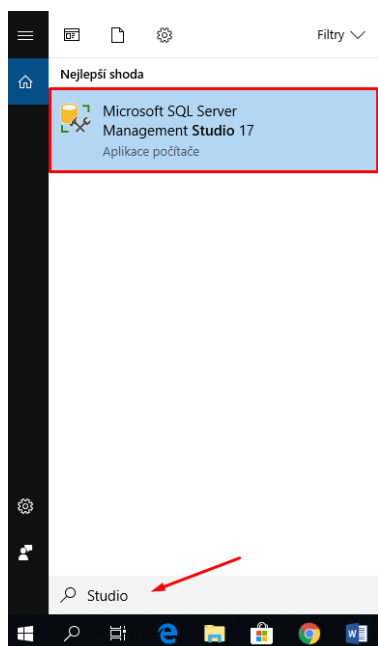
**i** When installing NET Genium via “Setup.exe” and checking the “Authorize Network Service account to access the MSSQL database” option, the program automatically sets the permissions to access the database (see the “NET Genium Installation” manual).



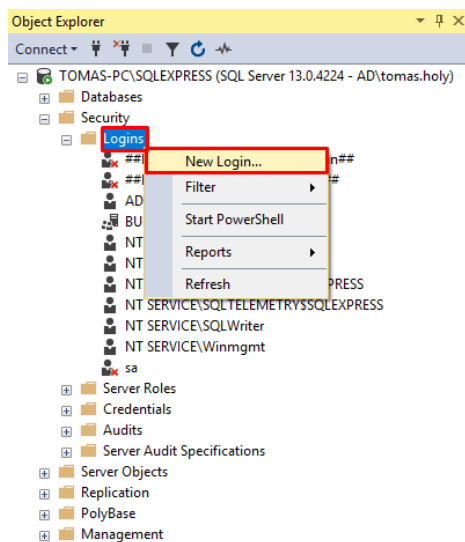
## 7.1.2 Manually set permissions through “Microsoft SQL Server Management Studio”

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

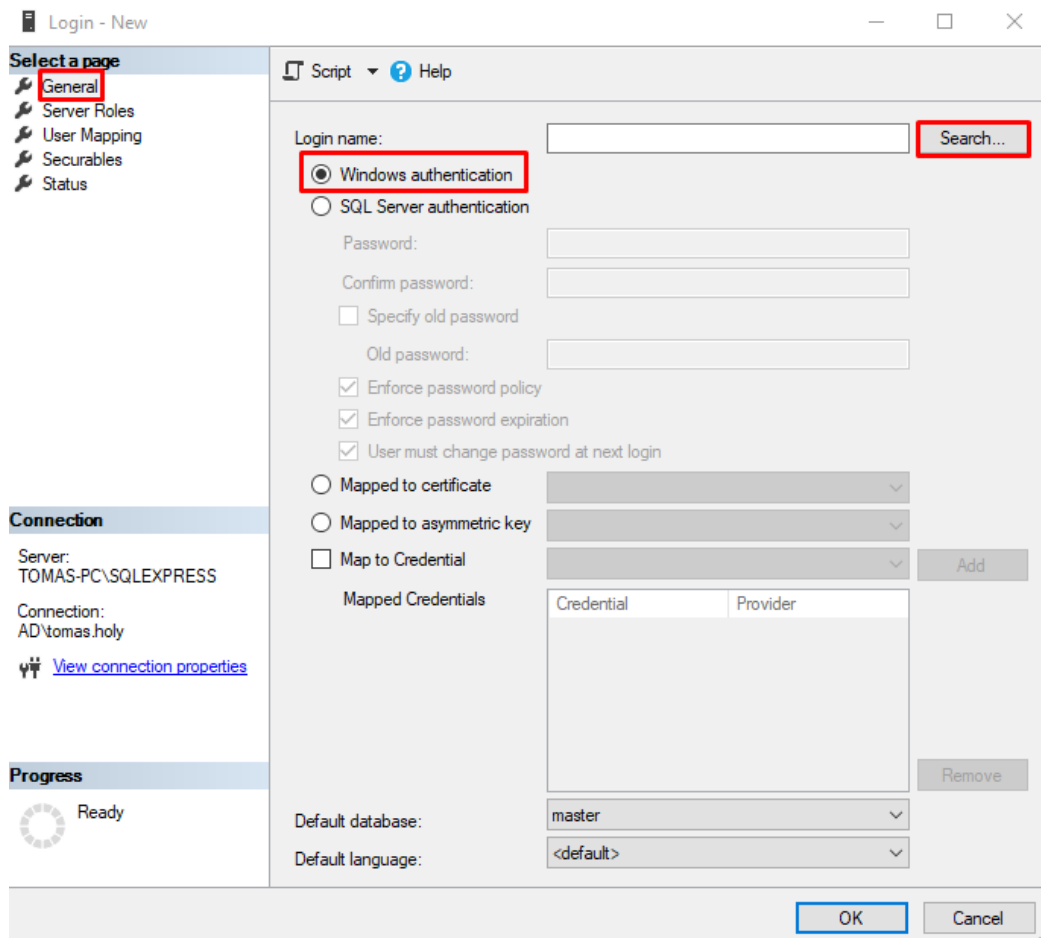
👉 From the “Start” menu, locate and run “Microsoft SQL Server Management Studio”.



👉 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.



Login - New

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Script ? Help

Login name:  Search...

☒ Windows authentication

☐ SQL Server authentication

Password:

Confirm password:

☐ Specify old password

Old password:

☒ Enforce password policy

☒ Enforce password expiration

☒ User must change password at next login

☐ Mapped to certificate

☐ Mapped to asymmetric key

☐ Map to Credential  Add

Mapped Credentials

Credential	Provider
------------	----------

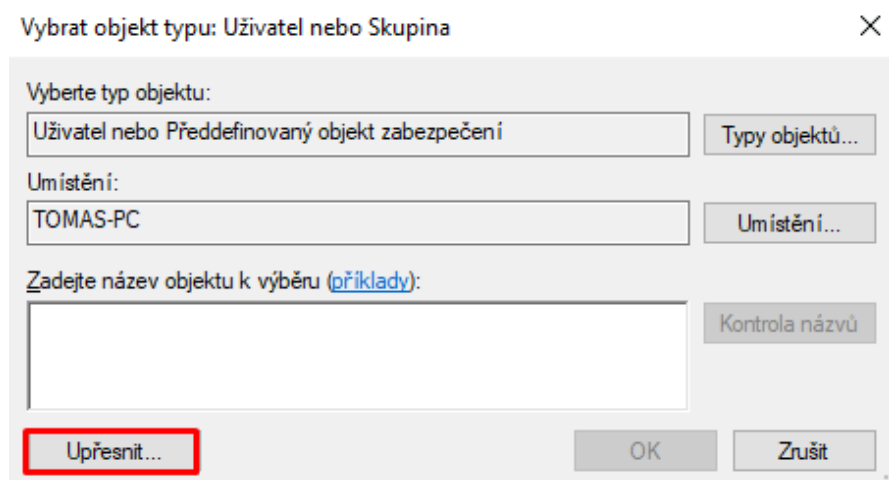
Remove

Default database: master

Default language: <default>

OK Cancel

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



Vybrat objekt typu: Uživatel nebo Skupina

Vyberte typ objektu:

Uživatel nebo Předdefinovaný objekt zabezpečení

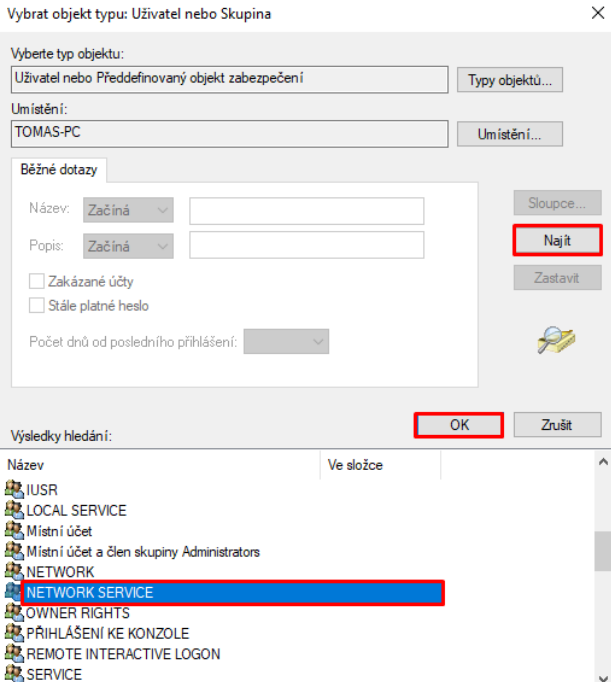
Umístění:

TOMAS-PC

Zadejte název objektu k výběru (příklady):



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



Vybrat objekt typu: Uživatel nebo Skupina

Výberte typ objektu:  
 Typy objektů...

Umístění:  
 Umístění...

Běžné dotazy

Název:

Popis:

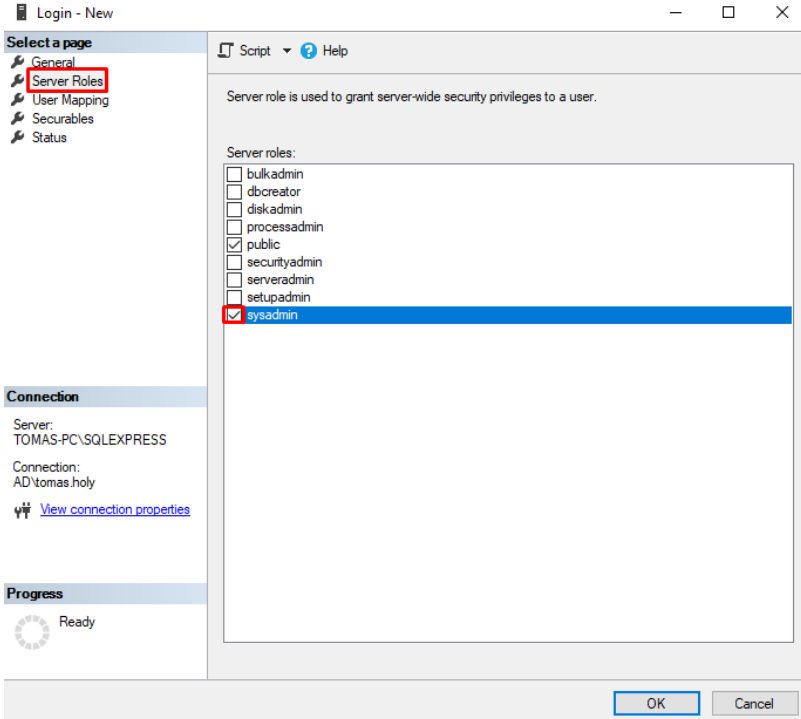
☐ Zakázané účty  
☐ Stále platné heslo

Počet dnů od posledního přihlášení:

Výsledky hledání:

Název	Ve složce
IUSR	
LOCAL SERVICE	
Místní účet	
Místní účet a člen skupiny Administrators	
NETWORK	
<b>NETWORK SERVICE</b>	
OWNER RIGHTS	
PŘIHLÁŠENÍ KE KONZOLE	
REMOTE INTERACTIVE LOGON	
SERVICE	

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



Login - New

Select a page

- General
- Server Roles**
- User Mapping
- Securables
- Status

Script Help

Server role is used to grant server-wide security privileges to a user.

Server roles:

- ☐ bulkadmin
- ☐ dbcreator
- ☐ diskadmin
- ☐ processadmin
- ☒ public
- ☐ securityadmin
- ☐ serveradmin
- ☐ setupadmin
- ☒ **sysadmin**

Connection

Server:  
TOMAS-PC\SQLEXPRESS

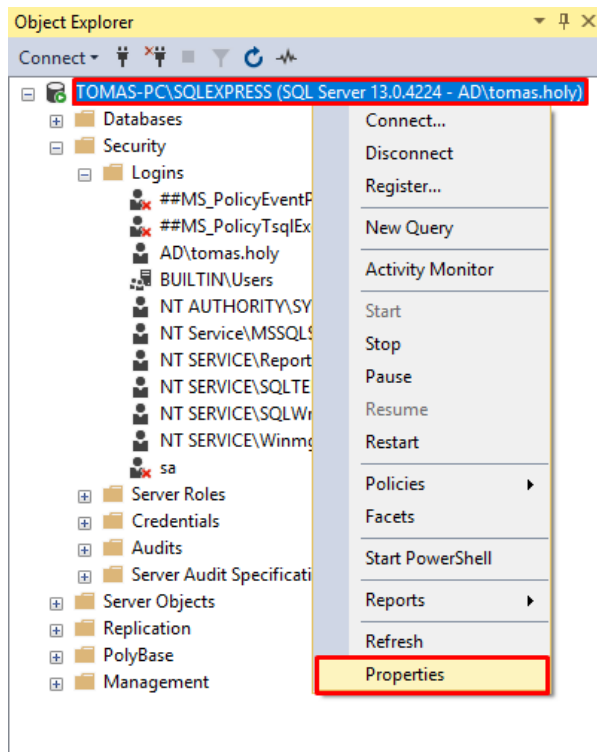
Connection:  
AD\tomas.holy

[View connection properties](#)

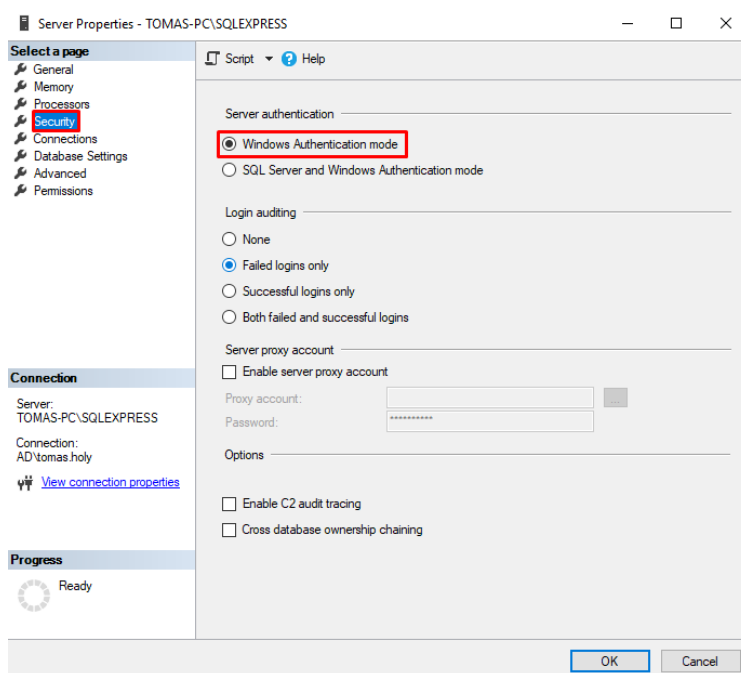
Progress

Ready

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



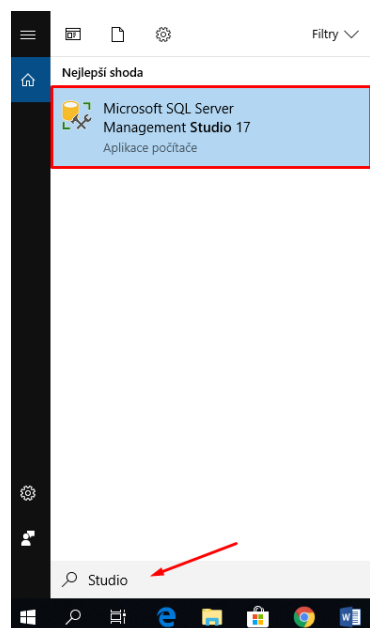
➔ On the “Security” tab, make sure that the default option “Windows Authentication mode” is checked.



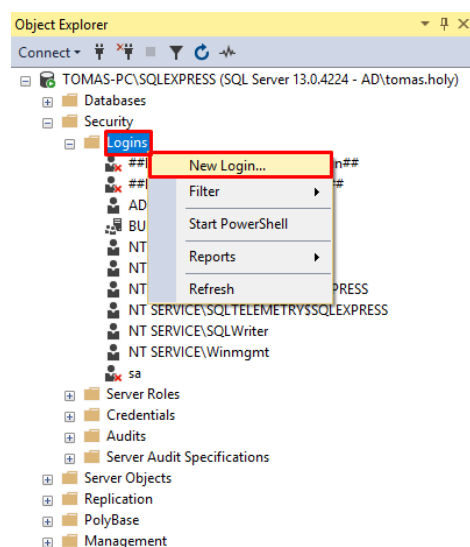
## 7.2 Setting permissions for access through the technology account from Active Directory

**i** 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\svcnsgadmin”.

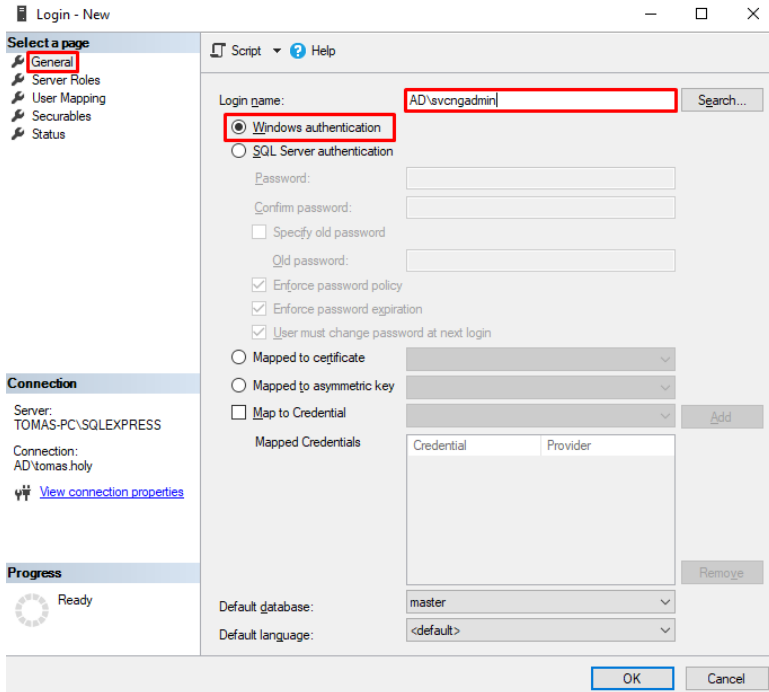
**+** From the “Start” menu, locate and run “Microsoft SQL Server Management Studio”.



**+** 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.



Login - New

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Connection

Server: TOMAS-PC\SQLEXPRESS

Connection: AD\tomas.holy

[View connection properties](#)

Progress

Ready

Script ? Help

Login name: AD\svcnadmin Search...

☒ Windows authentication

☐ SQL Server authentication

Password:

Confirm password:

☐ Specify old password

Old password:

☒ Enforce password policy

☒ Enforce password expiration

☒ User must change password at next login

☐ Mapped to certificate

☐ Mapped to asymmetric key

☐ Map to Credential

Map to Credential

Credential Provider

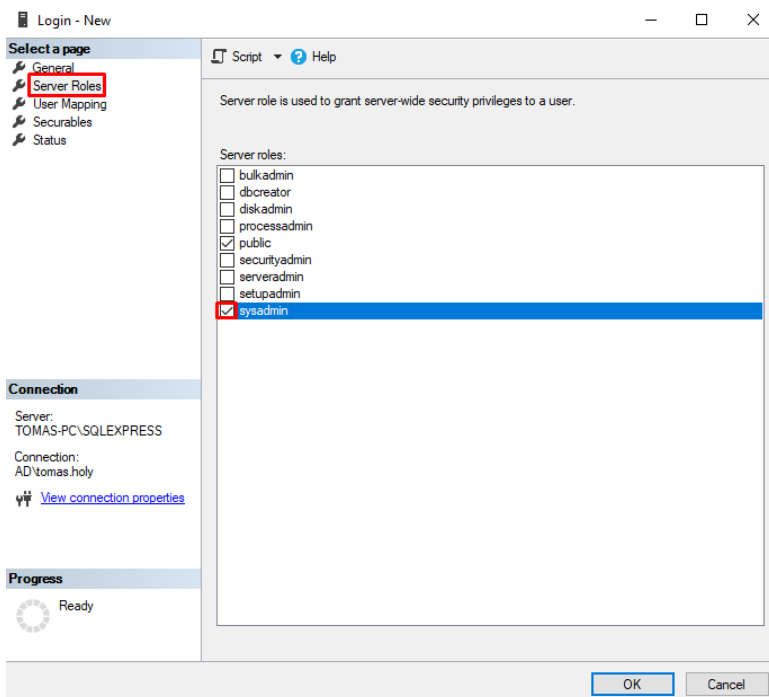
Remove

Default database: master

Default language: <default>

OK Cancel

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



Login - New

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Connection

Server: TOMAS-PC\SQLEXPRESS

Connection: AD\tomas.holy

[View connection properties](#)

Progress

Ready

Script ? Help

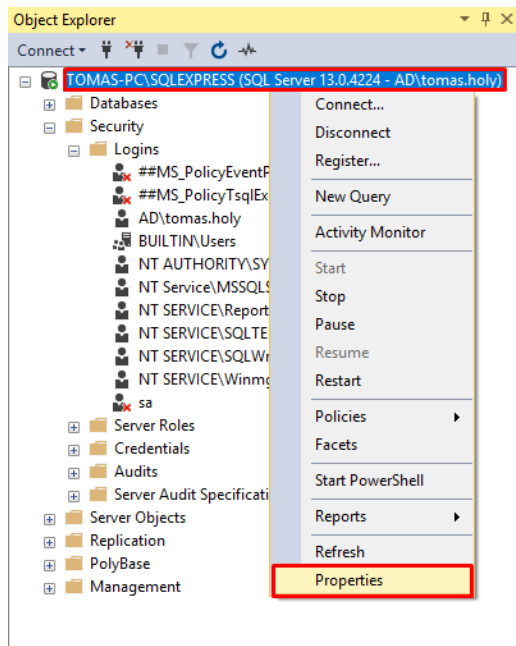
Server role is used to grant server-wide security privileges to a user.

Server roles:

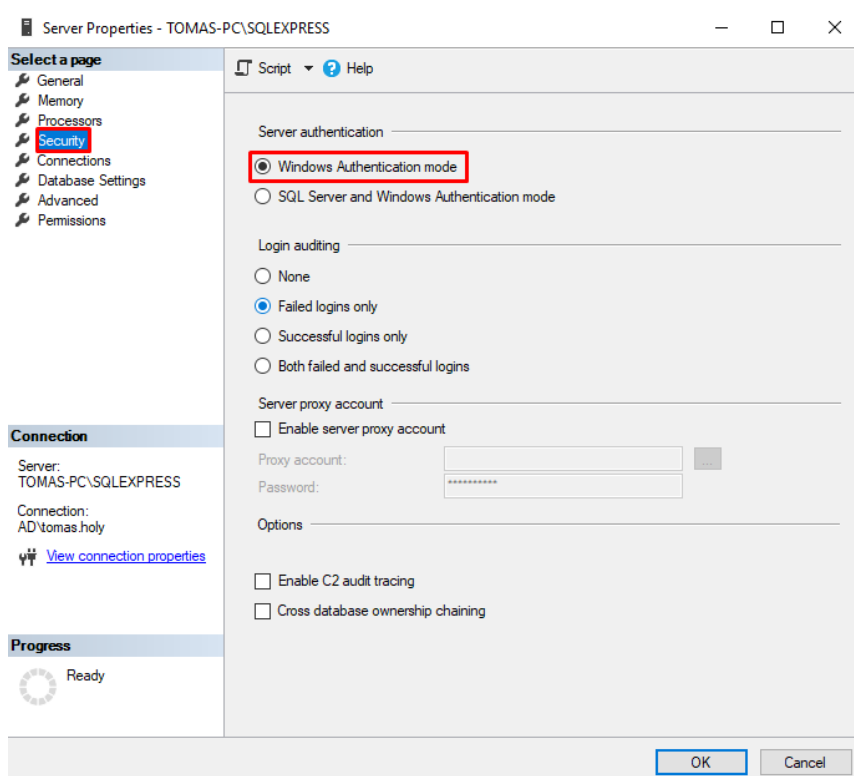
- ☐ bulkadmin
- ☐ dbcreator
- ☐ diskadmin
- ☐ processadmin
- ☒ public
- ☐ securityadmin
- ☐ serveradmin
- ☐ setupadmin
- ☒ sysadmin

OK Cancel

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



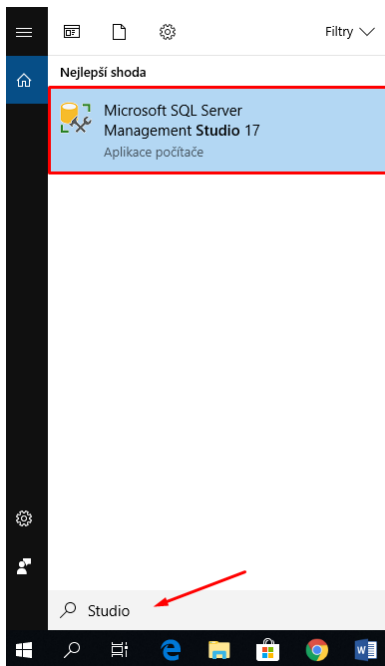
➡ On the “Security” tab, make sure that the default option “Windows Authentication mode” is checked.



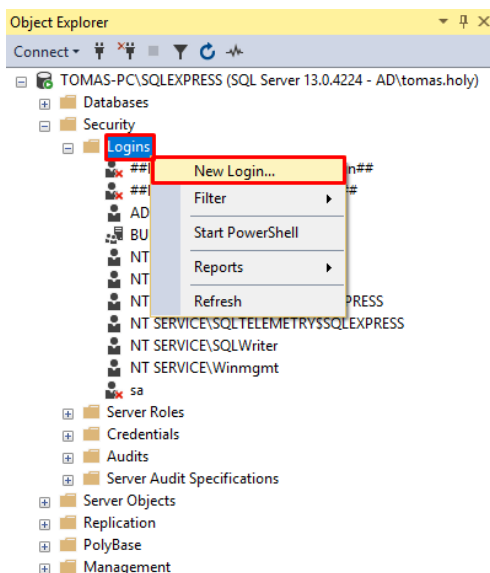
## 7.3 Setting permissions for access through the local SQL Server account

**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”.

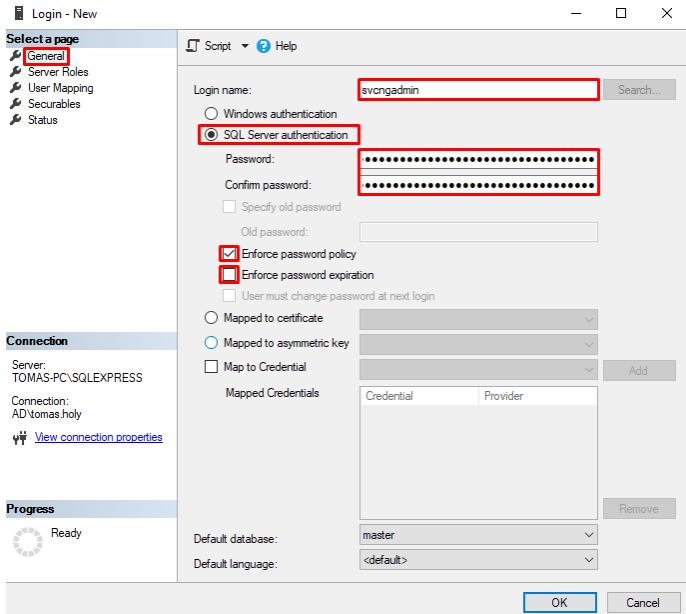


**h** Open the “Security” node, right-click on “Logins” and select “New Login...”.

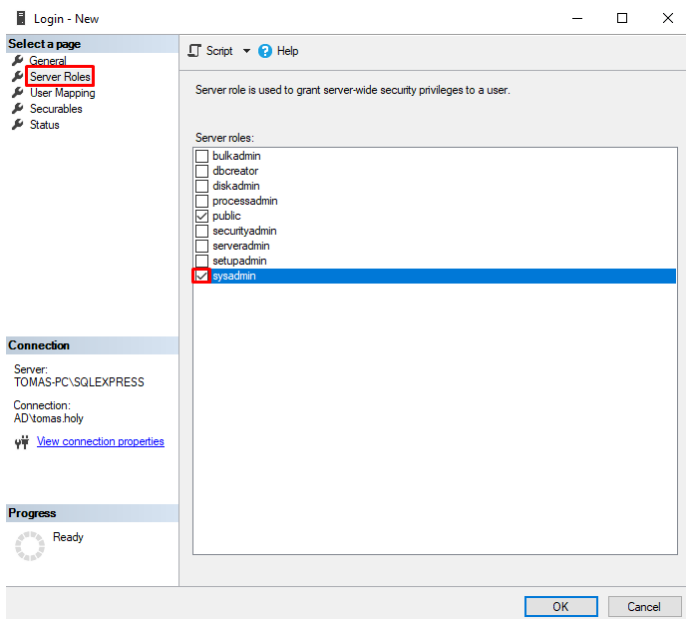


On the “General” tab page, fill in:

- Login name: for example “svcnadmin”
- 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”

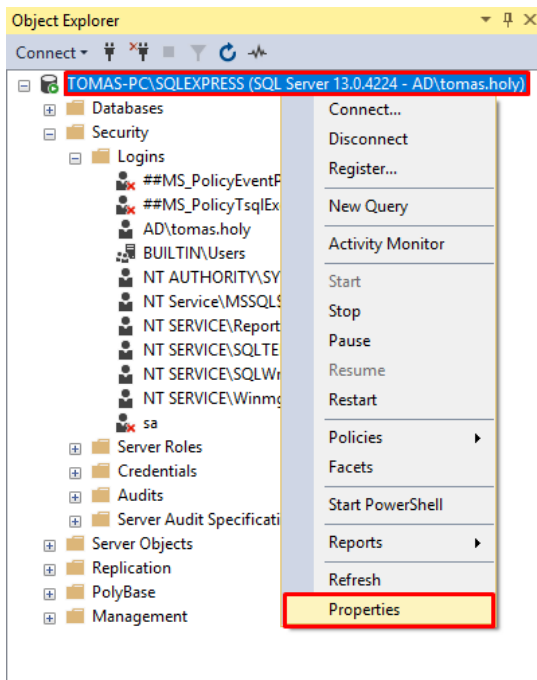


On the “Server Roles” tab, check the “sysadmin” option and confirm with the “OK” button.





➔ 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.

