

Configuration Manager on MS SQL Database

Managing large installations by using a central database



Configuration
Manager



Table of contents

1	Introduction	3
2	Configuration Manager setup for MS SQL as root DB	4
2.1	Configuring Parameter-based mode	5
2.2	Initial importing a local database	6
2.3	Sensitive database encryption passphrase	6
3	Appendix	7
3.1	Installation of MS SQL Server	7
3.2	Installation of SQL-Server Management Studio	15
3.3	Database preparation	17
3.4	Using built-in column encryption.	20
3.5	Using Cloud Database - Azure	20
4	References	26

1 Introduction

The Bosch Configuration Manager is a free and the central tool to scan, configure and manage Bosch devices. Over the years, it has seen a lot of enhancements, always keeping it up with newly introduced and evolving Bosch security products.

So far, Configuration Manager has been designed and used as a solitary client, holding its own local database. Though this could be centralized, working on this with multiple clients simultaneously had its challenges and restrictions.

Now, with version 7.70, we introduce the possibility to use a SQL database instead of the local database, at the same time enabling multiple simultaneous client access.

Since database installations and setups may vary extensively, only a certain number of setups could be tested and verified, so we need to consider this still an experimental feature. Feedback is welcomed to help us further improving this feature.

Configuration Manager 7.70 supports MS SQL Server 2019 and 2022, both as on-premises installation or in an Azure cloud.

In this tech note we assume a pre-installed SQL server that only needs to be configured for use with Configuration Manager.

If this is not the case, please refer to the appendix for installation hints and the references section for further documentation sources.

2 Configuration Manager setup for MS SQL as root DB

Navigate to Preferences → Page Access → Group Database.

From the combo-box dropdown list Database Mode, select MSSQL Database.

The Configuration Manager offers 2 configuration modes:

1. **Parameter-based** configuration allows selecting basic connection parameters using Configuration Manager UI.

Database Mode	▼
MSSQL Database	
Configuration type	▼
Parameters	
Server name	
██████████-DEV-HP\SQLEXPRESS	
Database name	
cm	
Authentication type	▼
SQL Server Authentication	
Login	
cm	
Password	
●●●●●●	
Connection encryption	▼
Encrypted with trust checking	
Sensitive data encryption passphrase	

2. **Connection String-based** mode allows for a possibility to define custom parameters that are not configurable via CM UI.

Database Mode	▼
MSSQL Database	
Configuration type	▼
Connection String	

Connection string

Sensitive data encryption passphrase

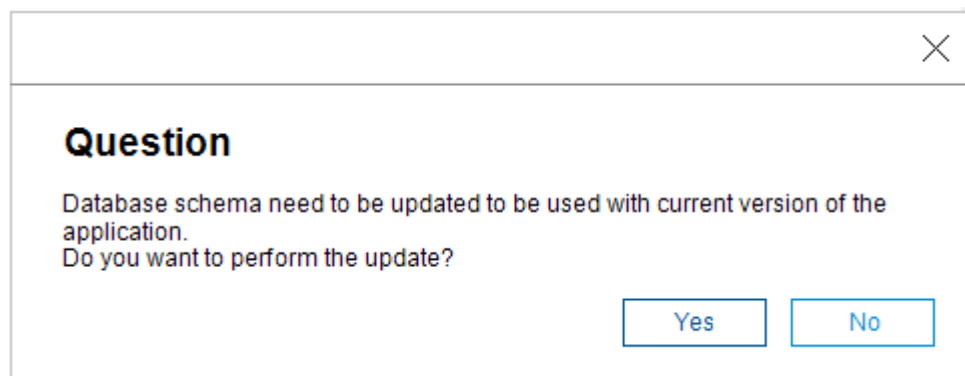
In this tech note we will focus on Parameter-based mode only.

2.1 Configuring Parameter-based mode

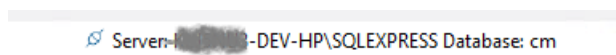
Possible parameters:

- **Server name**
Host name combined with instance id by "\"
- **Database name**
Database to be used. This can be an existing database, or a non-existing database in case a user with database creation rights is used.
- **Authentication type**
Can be chosen as Windows authentication, or SQL Server authentication.
In case of Windows authentication, no additional input is required.
In case of SQL Server authentication, a username and password are required (*see chapter 3.3.1*).
- **Connection encryption**
Defines if traffic between client and server is encrypted as well as if server certificate is being verified.
Recommended option is: Encrypted with trust check.
- **Sensitive database encryption passphrase**
A passphrase used to encrypt data in the database.
Recommended for small environments where column encryption is not enabled on the server.
For corporate environments, a method that uses built-in column encryption is recommended (*see chapter 3.4*).

After successful database connection, Configuration Manager will verify the version of the database and try to update the database schema.

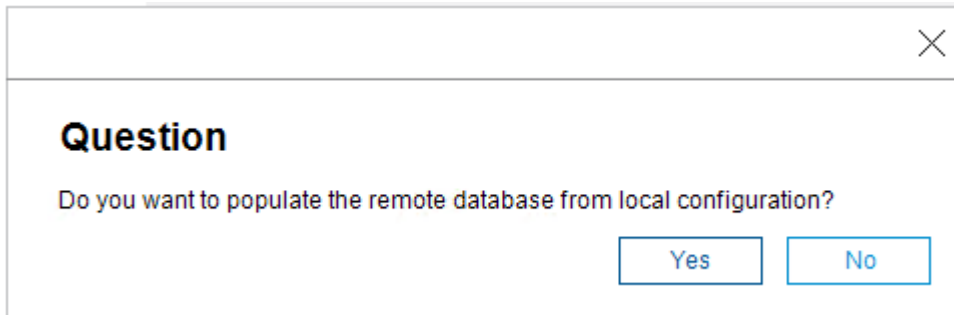


Successful connection is indicated by status message in the application's footer.



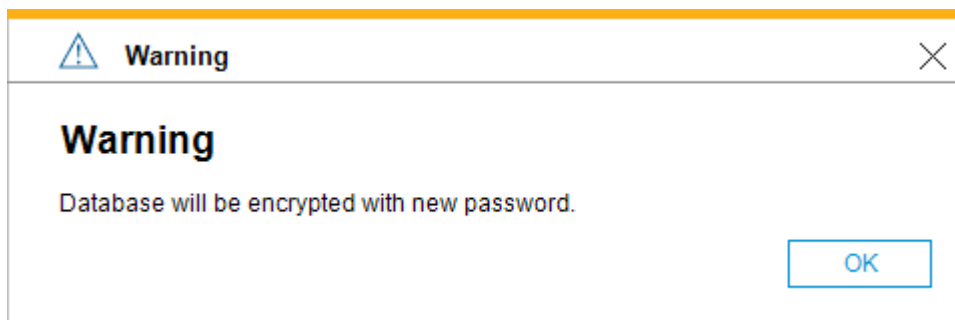
2.2 Initial importing a local database

In case it is the first time a user switched from file-based database to SQL database, Configuration Manager will offer the possibility to import the local database into the SQL server.



2.3 Sensitive database encryption passphrase

If provided, sensitive data, like access credentials for devices, will be encrypted with this passphrase. Changing of the sensitive data encryption passphrase on existing database will trigger re-encryption of all sensitive records.



Note:
For corporate environments, a method that uses built-in column encryption is recommended (*see chapter 3.4.*).

After enabling this option, all clients must use the same passphrase to access sensitive data. If the database uses built-in column encryption and a sensitive data encryption passphrase is provided, this will be used as additional encryption. Though it is not needed to use both encryptions, it is still possible.

3 Appendix

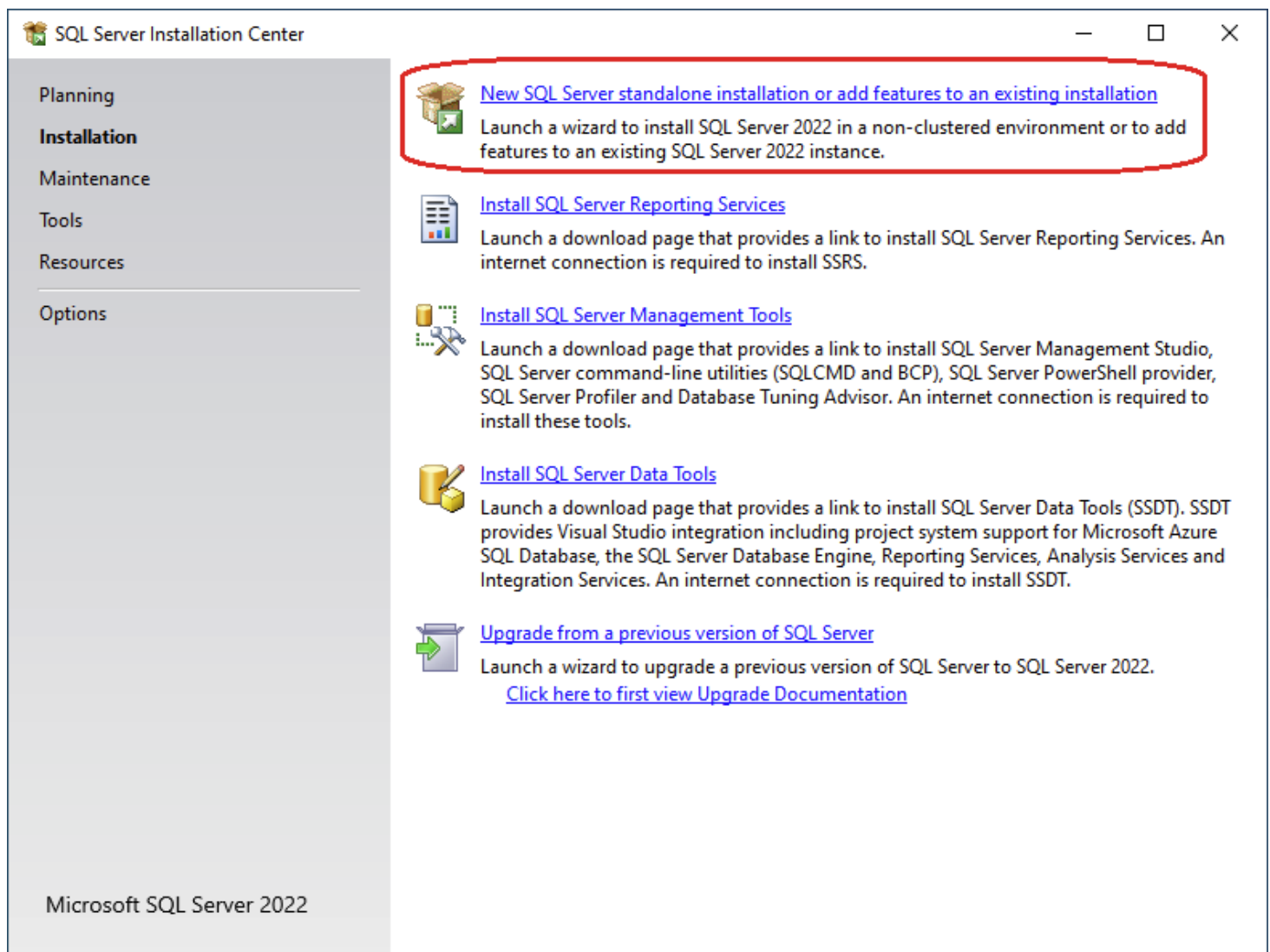
In this guideline we aim to provide hints for a SQL Server installation and setup that works with Configuration Manager. This is based on our own work processes and does not claim completeness nor correctness.

3.1 Installation of MS SQL Server

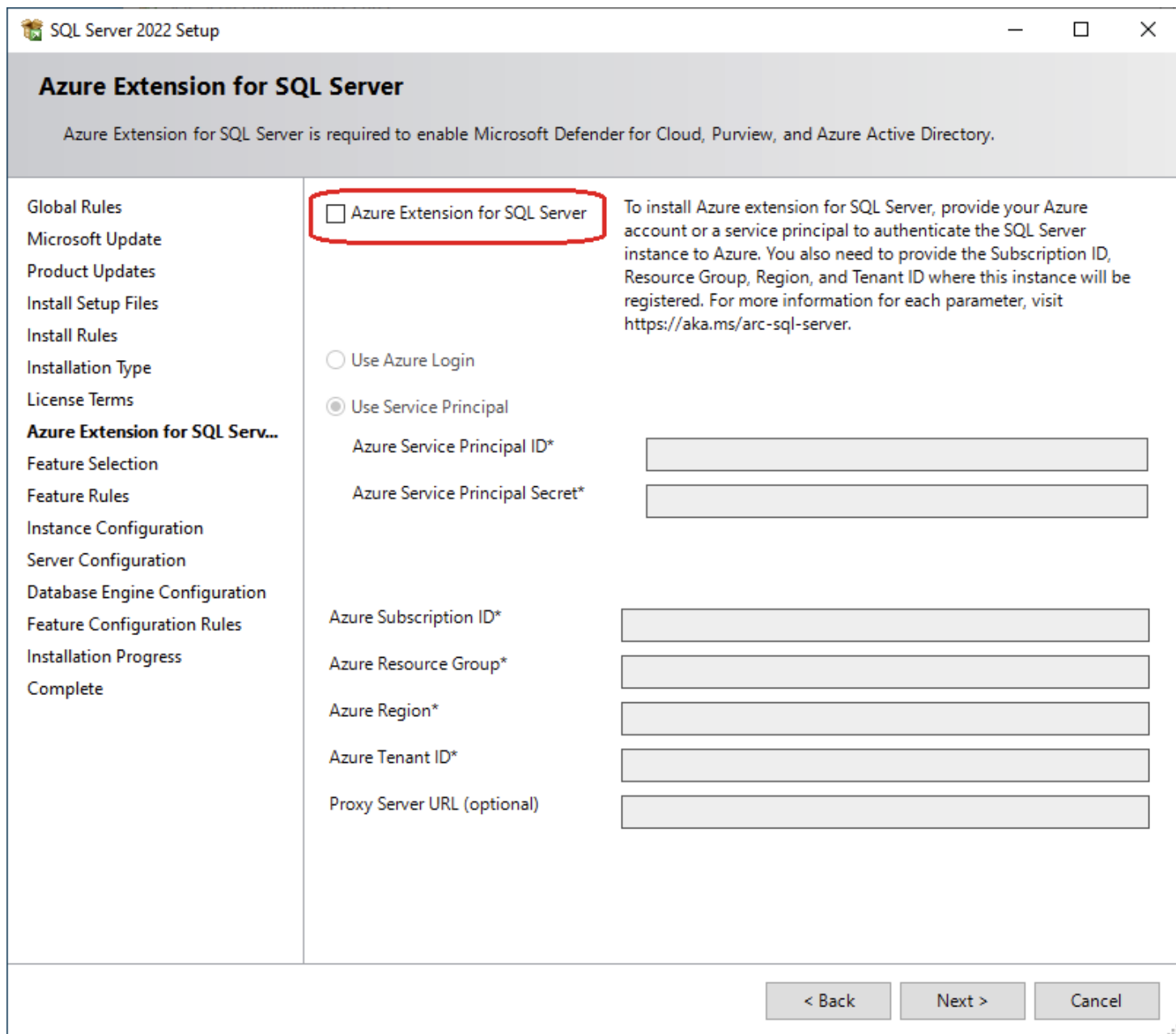
Download one of following versions of MS SQL server:

- SQL Server 2022 Express
<https://go.microsoft.com/fwlink/p/?linkid=2216019&clcid=0x409&culture=en-us&country=us>
- SQL Server 2019 Express
<https://www.microsoft.com/en-us/download/confirmation.aspx?id=101064>

To install SQL Server, select 'New SQL Server standalone installation'.



On the next screen, disable Azure Extension as shown below.



SQL Server 2022 Setup

Azure Extension for SQL Server

Azure Extension for SQL Server is required to enable Microsoft Defender for Cloud, Purview, and Azure Active Directory.

☐ Azure Extension for SQL Server

To install Azure extension for SQL Server, provide your Azure account or a service principal to authenticate the SQL Server instance to Azure. You also need to provide the Subscription ID, Resource Group, Region, and Tenant ID where this instance will be registered. For more information for each parameter, visit <https://aka.ms/arc-sql-server>.

☐ Use Azure Login

☒ Use Service Principal

Azure Service Principal ID*

Azure Service Principal Secret*

Azure Subscription ID*

Azure Resource Group*

Azure Region*

Azure Tenant ID*

Proxy Server URL (optional)

< Back Next > Cancel

Select all necessary components from group Database Engine Service.
Specify Instance root dictionary if needed.

SQL Server 2022 Setup

Feature Selection

Select the Express features to install.

License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Azure Extension for SQL Server
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Installation Progress
Complete

Looking for Reporting Services? [Download it from the web](#)

Features:

- Instance Features**
 - ☒ Database Engine Services
 - ☒ SQL Server Replication
- Shared Features
- Redistributable Features

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 the same computer.

Prerequisites for selected features:

Already installed:
... Windows PowerShell 3.0 or higher

To be installed from media:
... Microsoft Visual C++ 2017 Redistributable

Disk Space Requirements

Drive C: 994 MB required, 74762 MB available

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\

< Back Next > Cancel

Configure and note down the Instance Name and Instance ID. They will be needed for connection configuration. In this case:

- Instance Name: SQLExpress
- Instance ID: SQLExpress

SQL Server 2022 Setup

Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Installation Type
License Terms
Azure Extension for SQL Server
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Installation Progress
Complete

☐ Default instance

☒ Named instance: *

Instance ID:

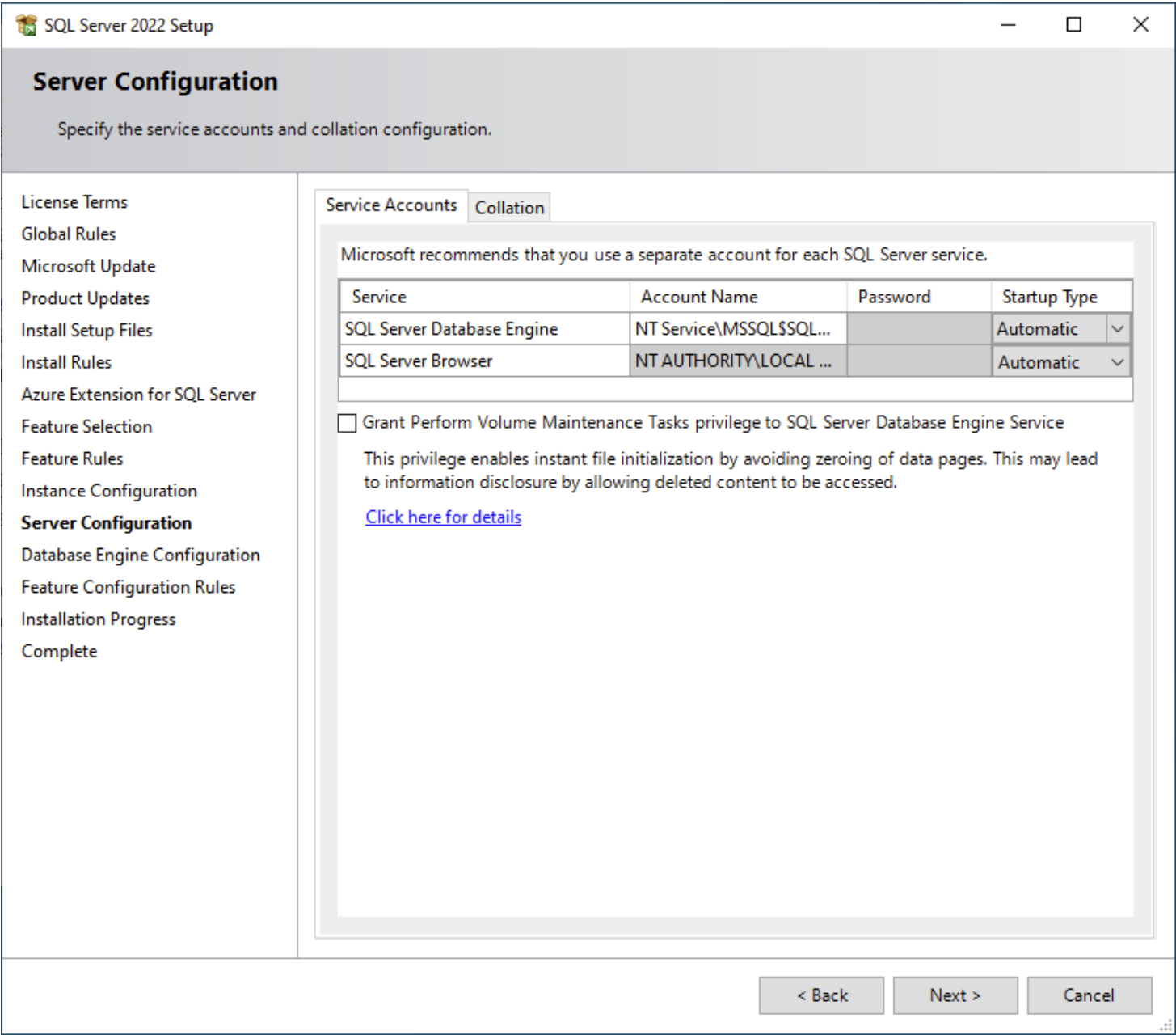
SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL16.SQLEXPRESS

Installed instances:

Instance Name	Instance ID	Features	Edition	Version
SQLEXPRESS	MSSQL16.SQLEXPRESS	SQLEngine, SQLEn...	Express	16.0.1000.6

< Back Next > Cancel

Make sure the server is started automatically by service account as shown on picture below.



For access configuration in Active Directory environment use Windows Authentication Mode; in other environments use Mixed Authentication Mode. Configure and note administrator password.

Such a configuration allows to login to the server using username Administrator and the configured password as well as access using Windows account defined as Server administrators.

SQL Server 2022 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators, data directories, TempDB, Max degree of parallelism, Memory limits, and Filestream settings.

- License Terms
- Global Rules
- Microsoft Update
- Product Updates
- Install Setup Files
- Install Rules
- Azure Extension for SQL Server
- Feature Selection
- Feature Rules
- Instance Configuration
- Server Configuration
- Database Engine Configuration**
- Feature Configuration Rules
- Installation Progress
- Complete

Server Configuration | Data Directories | TempDB | Memory | 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: [password field]

Confirm password: [password field]

Specify SQL Server administrators

SQL Server administrators have unrestricted access to the Database Engine.
VM-WIN10-SRV\...

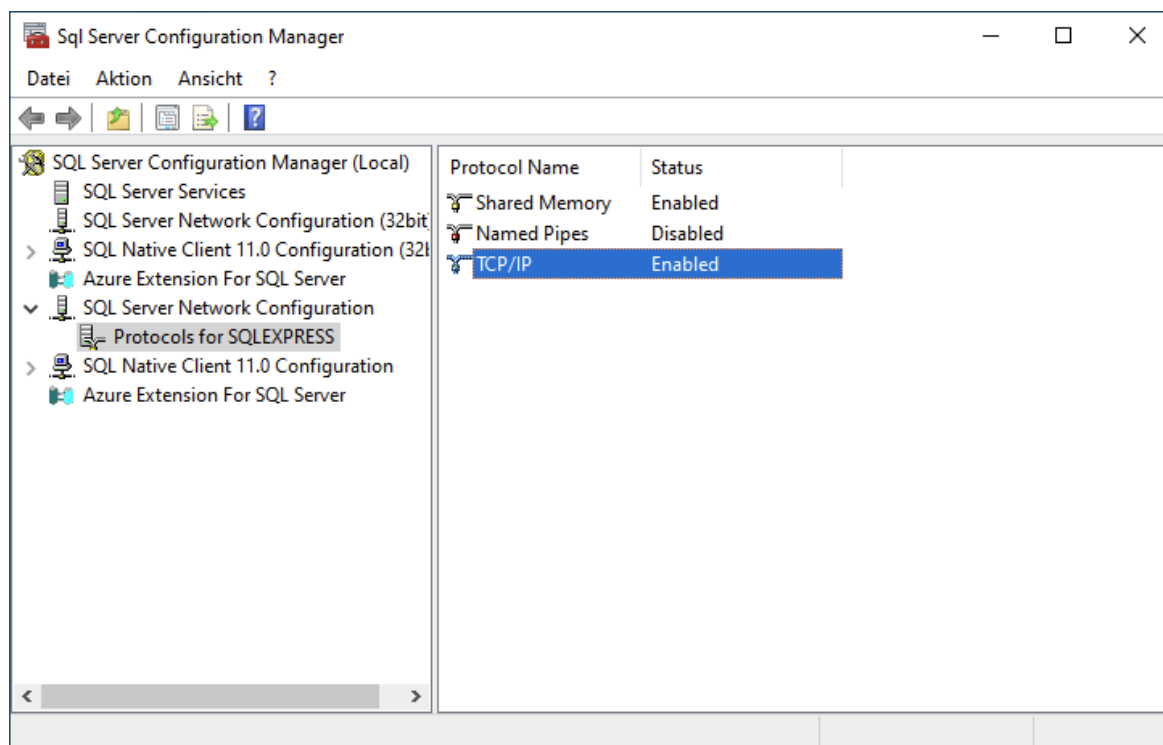
Add Current User | Add... | Remove

< Back | Next > | Cancel

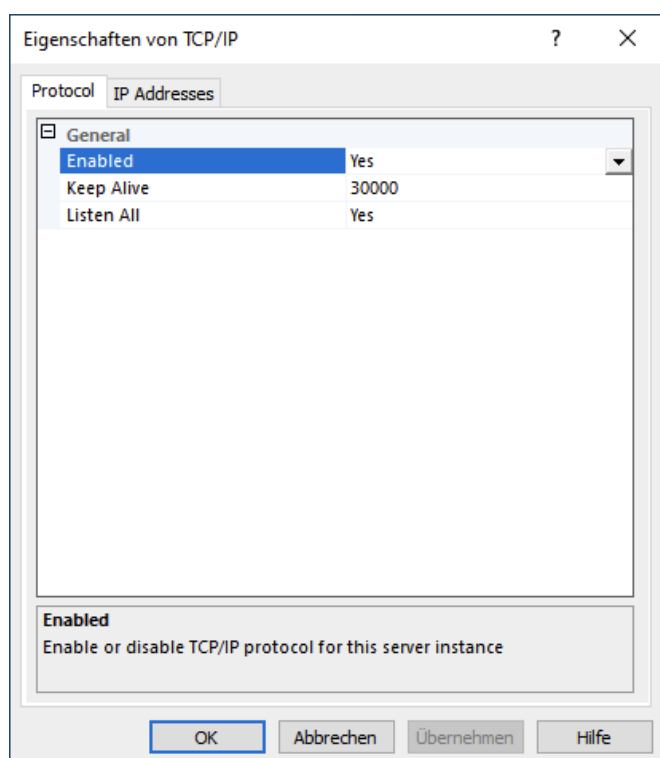
3.1.1 Enable Network access

On the Standard or Enterprise Edition of the SQL-Server the network access is enabled by default. For the Express edition, you need to activate it.

To do that, open the Sql Server Configuration Manager, go to 'Sql Server Network Configuration' → 'Protocols for SQLEXPRESS'

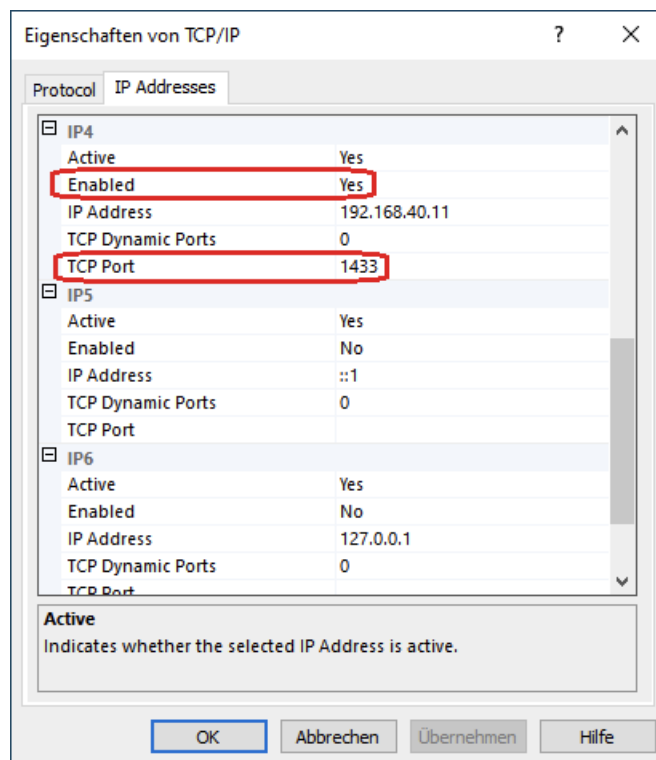
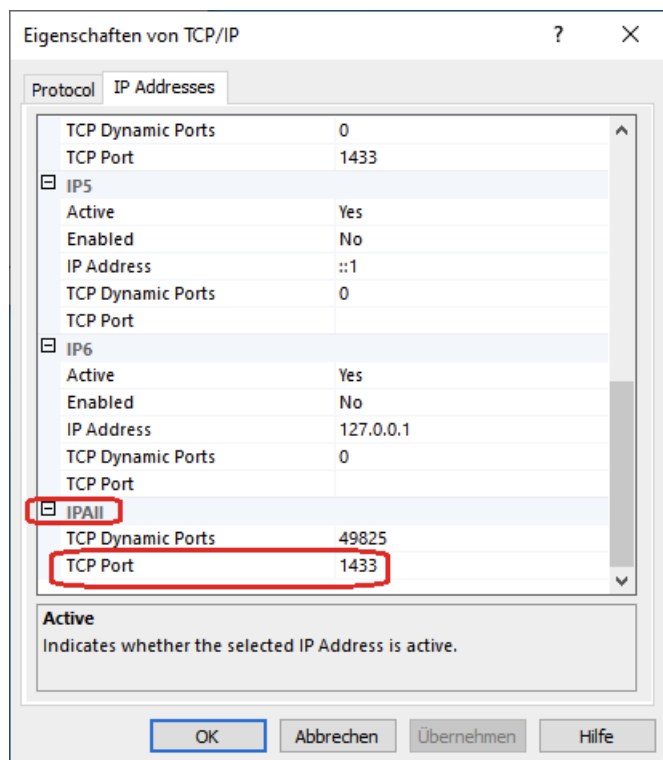


and double click 'TCP/IP' list item. Set 'Enabled' item to 'yes'



Next, go to tab "IP Addresses". Go to bottom of the list to item ""IPAll" and set port to 1433.

Afterwards set "Enabled" to "Yes" for each network interface that should listen for sql requests:



After saving, restart SQL Server.

3.1.2 Configure firewall

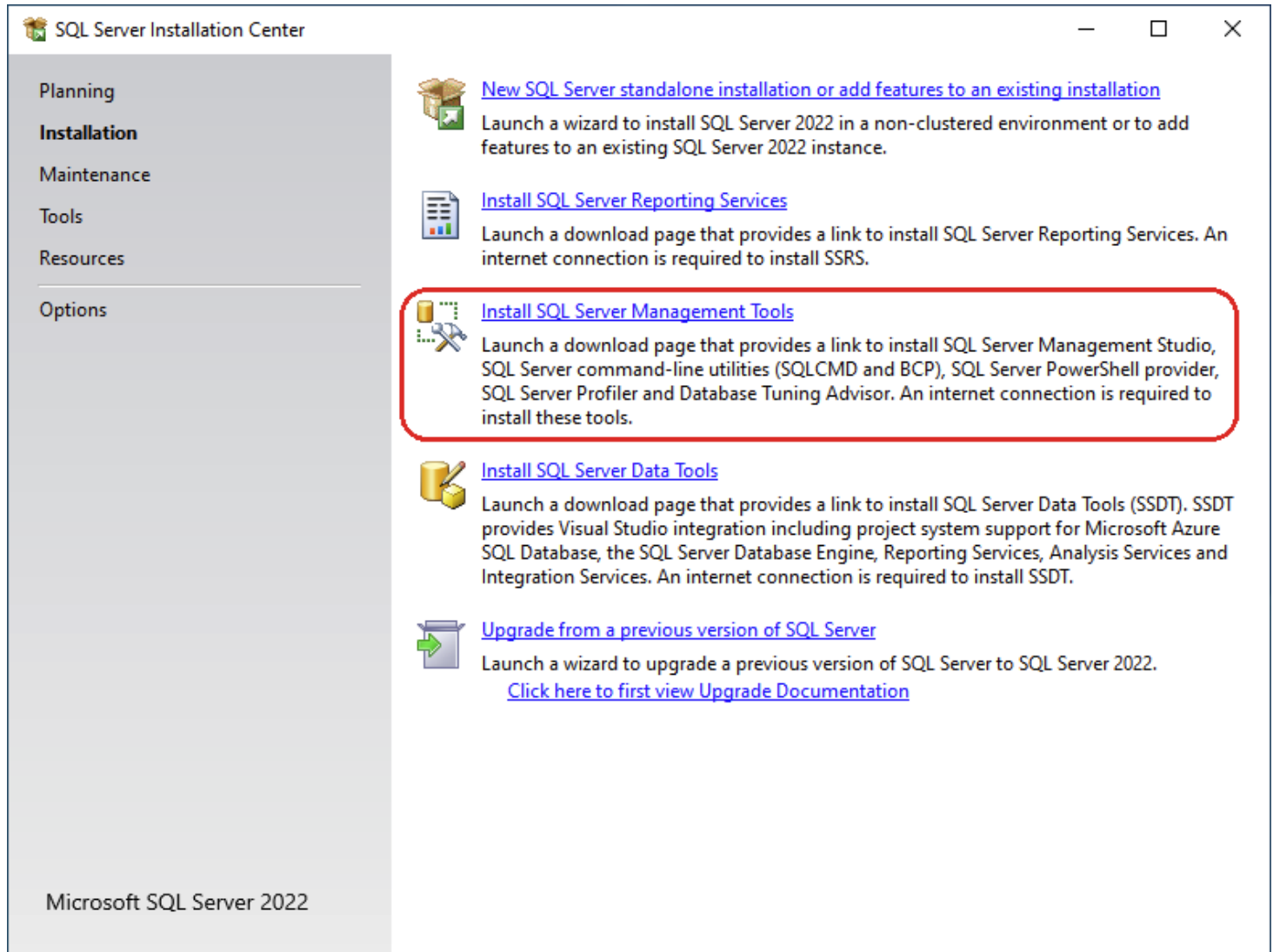
Run Windows PowerShell as Administrator and execute following commands:

New-NetFirewallRule -DisplayName "SQLServer default instance" -Direction Inbound -LocalPort 1433 -Protocol TCP -Action Allow

New-NetFirewallRule -DisplayName "SQLServer Browser service" -Direction Inbound -LocalPort 1434 -Protocol UDP -Action Allow

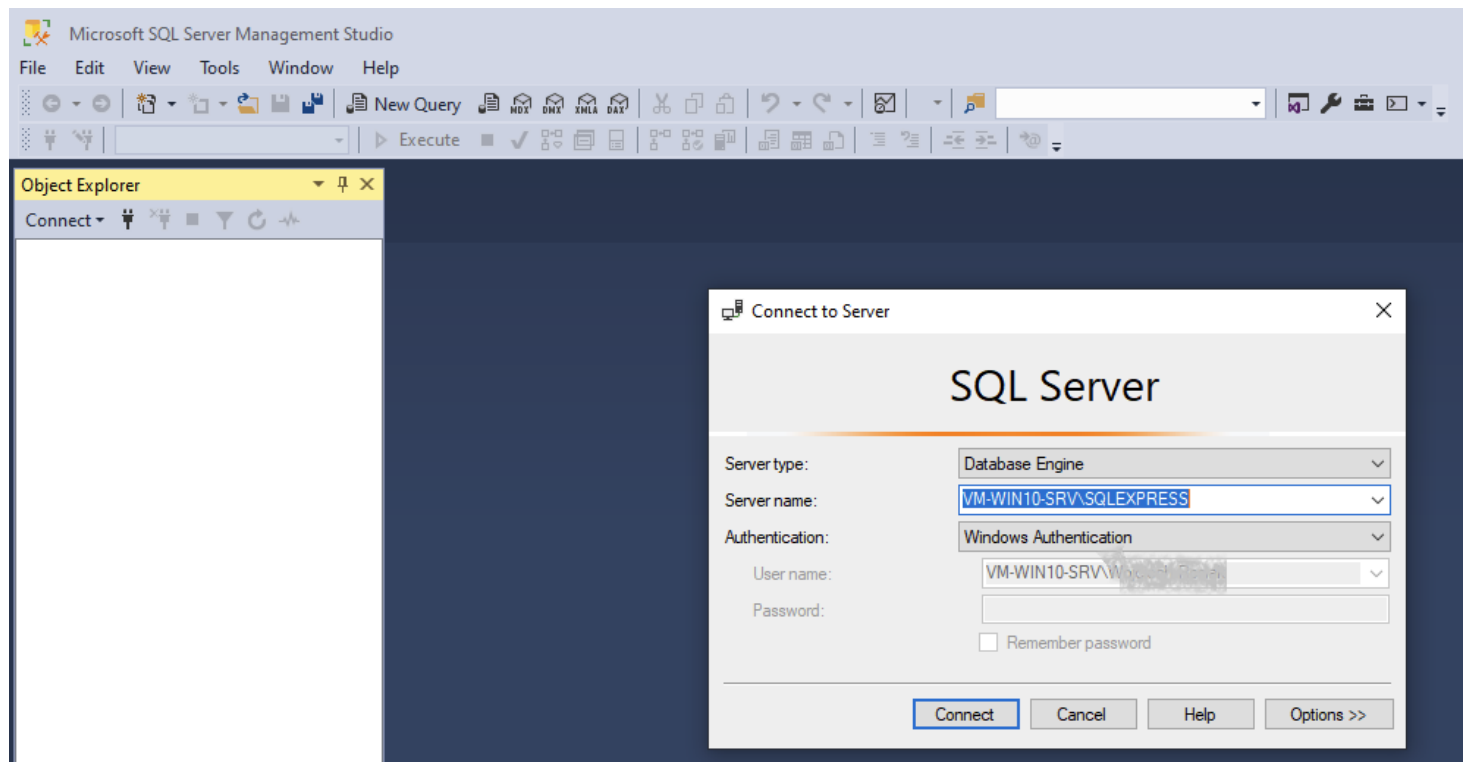
3.2 Installation of SQL-Server Management Studio

Start "SQL Server Installation Center" and select "Install SQL Server Management tools".



A web browser will be started with a page where you can download the "SQL Server Management Studio (SSMS)". Download it and start the setup. It is not necessary to install it on the SQL Server machine.

After installation, you can start the management studio, set the server name and connect.



3.3 Database preparation

The current implementation allows two possible database configurations.

The first one, using an account with table creation rights (i. e. Administrator), allowing the Configuration Manager to create database automatically, is **not recommended**.

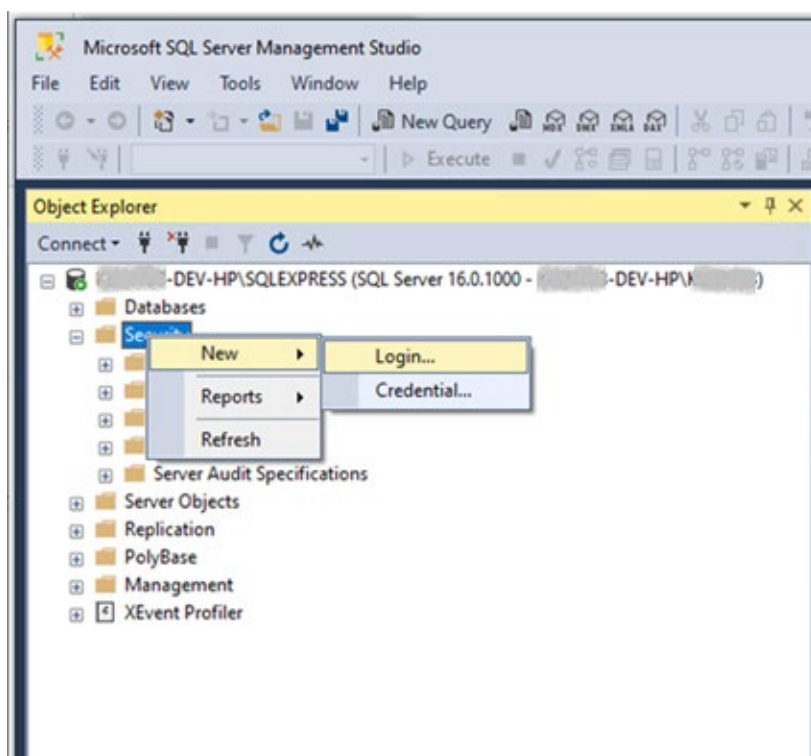
Better create user and database for Configuration Manager manually, using SQL Server Management Studio.

In both cases users can be Active Directory managed or database managed, in this how to we focus on creation of the user and table for the Configuration Manager.

Using the SQL Server Management Studio select correct instance, configure administrator access and connect.

3.3.1 User creation

Right click on directory Security, then select New→Login...



Set login name to desired value, for authentication type select SQL Server authentication, define password.

Login - New

Select a page

General

Server Roles

User Mapping

Securables

Status

Connection

Server: dev-hp\SQLEXPRESS

Connection: DEV-HPV

[View connection properties](#)

Progress

Ready

Script Help

Login name: cm

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

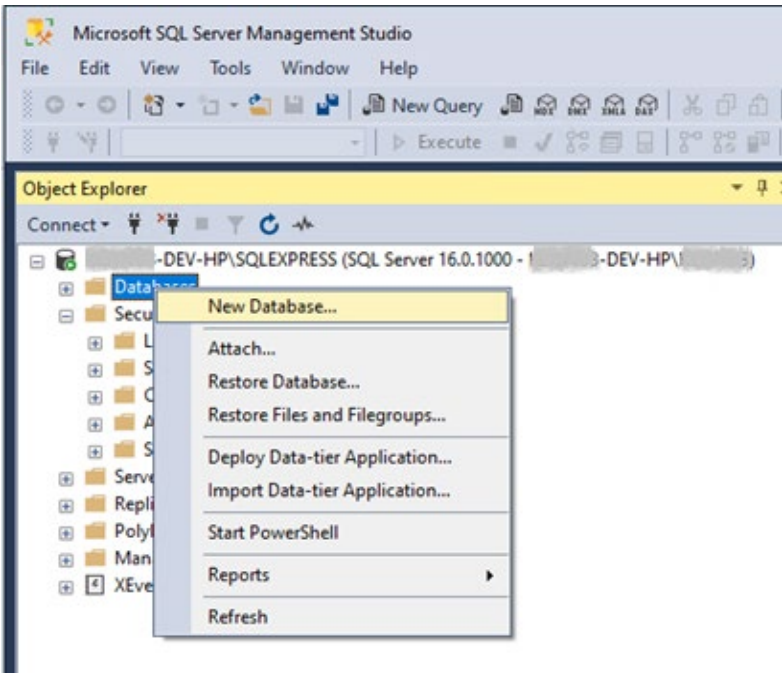
Cancel

Data subject to change without notice | June 23

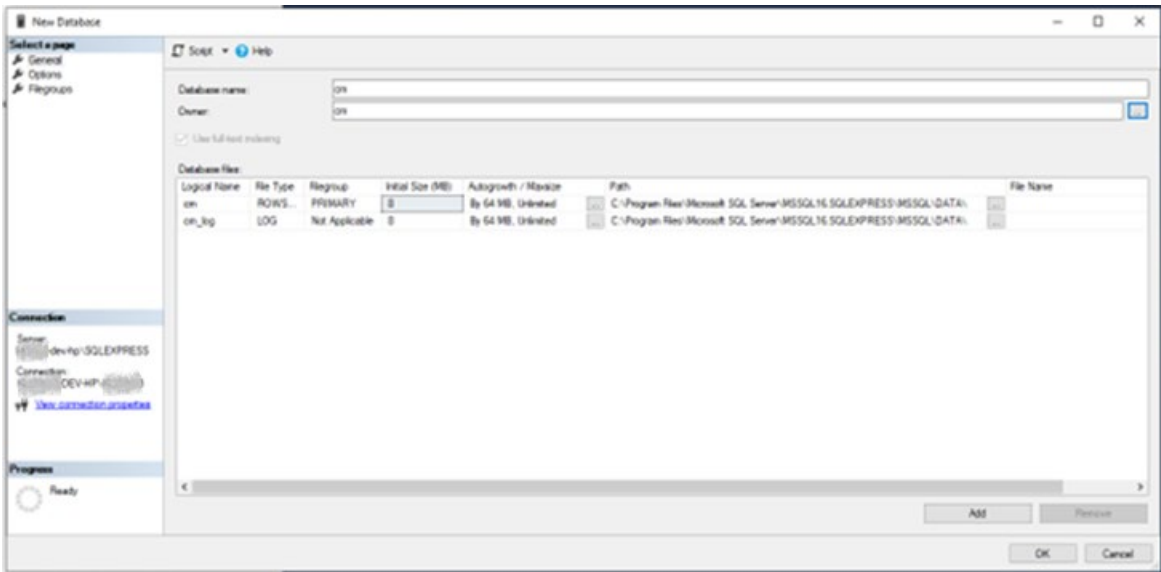
Security Systems / Video Systems

3.3.2 Database creation

Right click on directory Databases, then select New Database...



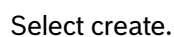
Define the desired database name (in this example cm) and select the owner (the user created before). The path to the database can be set as well.



MS SQL offers built-in columns encryption based on PKI.

Follow the tutorial to configure it correctly in the database: <https://sqlsolutionsgroup.com/sql-server-always-encrypted/>.

After logging into Azure portal, select SQL databases.



Create Server if needed:

Create SQL Database Server

Microsoft

Server details

Enter required settings for this server, including providing a name and location. This server will be created in the same subscription and resource group as your database.

Server name *

btvs-cm2

.database.windows.net

Location *

(US) East US

Authentication

Select your preferred authentication methods for accessing this server. Create a server admin login and password to access your server with SQL authentication, select only Azure AD authentication [Learn more](#) using an existing Azure AD user, group, or application as Azure AD admin [Learn more](#) , or select both SQL and Azure AD authentication.

Authentication method

☐ Use only Azure Active Directory (Azure AD) authentication

☐ Use both SQL and Azure AD authentication

☒ Use SQL authentication

Server admin login *

btvs-cm

Password *

●●●●●●●●

Confirm password *

●●●●●●●●

Configure database name and server used:

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ

[Create new](#)

Database details

Enter required settings for this database, including picking a logical server and configuring the compute and storage resources

Database name *

Server * ⓘ

[Create new](#)

Want to use SQL elastic pool? ⓘ ☐ Yes ☒ No

Workload environment ☒ Development ☐ Production

i Default settings provided for Development workloads. Configurations can be modified as needed.

Compute + storage * ⓘ

General Purpose - Serverless

Standard-series (Gen5), 1 vCore, 32 GB storage, zone redundant disabled

[Configure database](#)

Backup storage redundancy

Choose how your PITR and LTR backups are replicated. Geo restore or ability to recover from regional outage is only available when geo-redundant storage is selected.

Backup storage redundancy ⓘ ☐ Locally-redundant backup storage ☐ Zone-redundant backup storage ☒ Geo-redundant backup storage

Configure Database collation:

Basics Networking Security Additional settings Tags Review + create

Customize additional configuration parameters including collation & sample data.

Data source

Start with a blank database, restore from a backup or select sample data to populate your new database.

Use existing data * None Backup Sample

Database collation

Database collation defines the rules that sort and compare data, and cannot be changed after database creation. The default database collation is SQL_Latin1_General_CP1_CI_AS. [Learn more](#)

Collation * ⓘ SQL_Latin1_General_CP1_CI_AS
[Find a collation](#)

Maintenance window

Select a preferred maintenance window from the drop down. Please note, during a maintenance event, Azure SQL Database are fully available and accessible but some of the maintenance updates require a failover as Azure takes SQL DB instances offline for a short time to apply the maintenance updates. If the database is part of elastic pool, the maintenance configuration of elastic pool will be applied. [Learn more](#)

Maintenance window System default (5pm to 8am) ▾

Navigate to created server. Select Security → Networking.

Set Public network access to Selected networks.

In firewall rules add client's public IP.

btvs-cm | Networking SQL server

Search

Feedback

Public access Private access Connectivity

Public network access
Public Endpoints allow access to this resource through the internet using a public IP address. An application or resource that is granted access with the following Public network access

Public network access

☐ Disable

☒ Selected networks

Connections from the IP addresses configured in the Firewall rules section below will have access to this database. By default, connections from the Internet will be blocked.

Please save public network access value before adding new virtual networks.

Virtual networks
Allow virtual networks to connect to your resource using service endpoints. [Learn more](#)

+ Add a virtual network rule

Rule	Virtual network	Subnet	Address range	Endpoint status	Resource group	Subscription	State
No virtual network rules found.							

Firewall rules
Allow certain public internet IP addresses to access your resource. [Learn more](#)

+ Add your client IPv4 address (194.101.101.101) + Add a firewall rule

Rule name	Start IPv4 address	End IPv4 address
VCS Grey	194.101.101.101	194.101.101.101

Exceptions

☐ Allow Azure services and resources to access this server ⓘ

Navigate to created database:

cm (btvs-cm/cm)

SQL database

Search

CopyRestoreExportSet server firewallDeleteConnect with...Feedback

Overview

Activity log

Tags

Diagnose and solve problems

Getting started

Query editor (preview)

Settings

Compute + storage

Essentials

Resource group (move) : Broker-Azure

Status : Online

Location : West Europe

Subscription (move) : Subskrypcja programu Visual Studio Professional

Subscription ID : 83f7a668-0330-4c7b-9da6-01fef4a9e7c3

Tags (edit) : Click here to add tags

Server name : btvs-cm.database.windows.net

Connection strings : Show database connection strings

Pricing tier : General Purpose - Serverless: Gen5, 1 vCore

Auto-pause delay : 1 hour

Earliest restore point : No restore point available

Getting startedMonitoringPropertiesFeaturesNotifications (0)IntegrationsTutorials

Select Show database connection strings:

CopyRestoreExportSet server firewallDeleteConnect with...Feedback

Essentials

Resource group (move) : Broker-Azure

Status : Online

Location : West Europe

Subscription (move) : Subskrypcja programu Visual Studio Professional

Subscription ID : 83f7a668-0330-4c7b-9da6-01fef4a9e7c3

Tags (edit) : Click here to add tags

Server name : btvs-cm.database.window

Connection strings : Show database connection strings

Pricing tier : General Purpose - Serverless: Gen5, 1 vCore

Auto-pause delay : 1 hour

Earliest restore point : No restore point available

Copy ADO.NET (SQL authentication) connection string.

ADO.NETJDBCODBCPHPGo

ADO.NET (Active Directory passwordless authentication)

Microsoft.Data.SqlClient QuickstartEntity Framework Core Quickstart

Server=tcp:btvs-cm.database.windows.net,1433;Initial Catalog=cm;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;Authentication="Active Directory Default";

ADO.NET (SQL authentication)

Server=tcp:btvs-cm.database.windows.net,1433;Initial Catalog=cm;Persist Security Info=False;User ID=btvs-cm;Password={your_password};MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;

Set Connection string configuration mode in Configuration Manager, paste copied connection string, change password ({your_password}) used in connection string.

Database Mode

MSSQL Database

Configuration type

Connection String

Connection string

Info=False;User ID=btvs-cm;Password=;MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Conne

Sensitive data encryption passphrase

4 References

Limitations from database perspective are described by Microsoft. There are many of them depending on DB version, or OS version (e. g. CPU cores need licenses). More details can be found in MS documents:

1. <https://learn.microsoft.com/en-us/sql/sql-server/maximum-capacity-specifications-for-sql-server?view=sql-server-ver16>
2. <https://learn.microsoft.com/en-us/sql/sql-server/compute-capacity-limits-by-edition-of-sql-server?view=sql-server-ver16>

There are reference documents that may help users to set up an SQL database:

3. <https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/create-a-database-user?view=sql-server-ver16>
4. <https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/create-a-database-schema?view=sql-server-ver16>
5. <https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/create-a-login?view=sql-server-ver16>

Bosch Sicherheitssysteme GmbH

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

www.boschsecurity.com

© Bosch Sicherheitssysteme GmbH, 2023