MSSQL Penetration Testing

Lab Setup

iGNITE Technologies

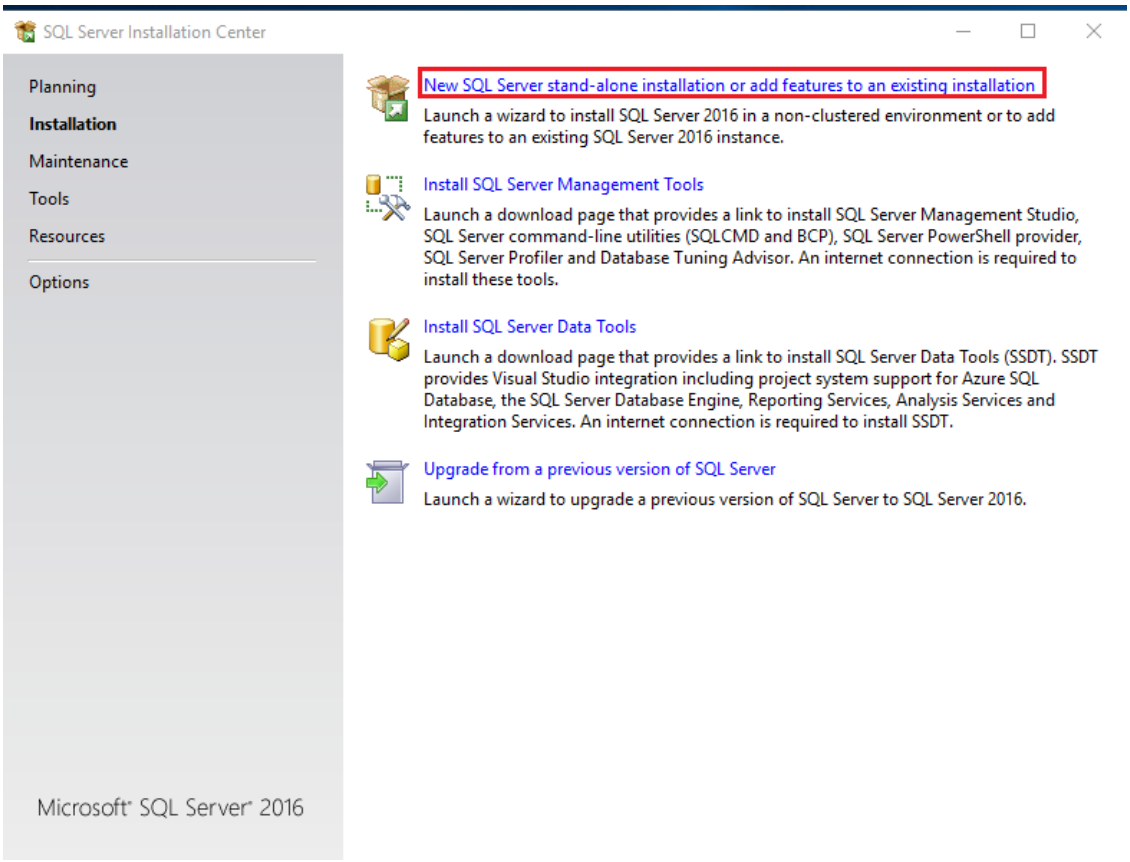
Contents

Requirement:

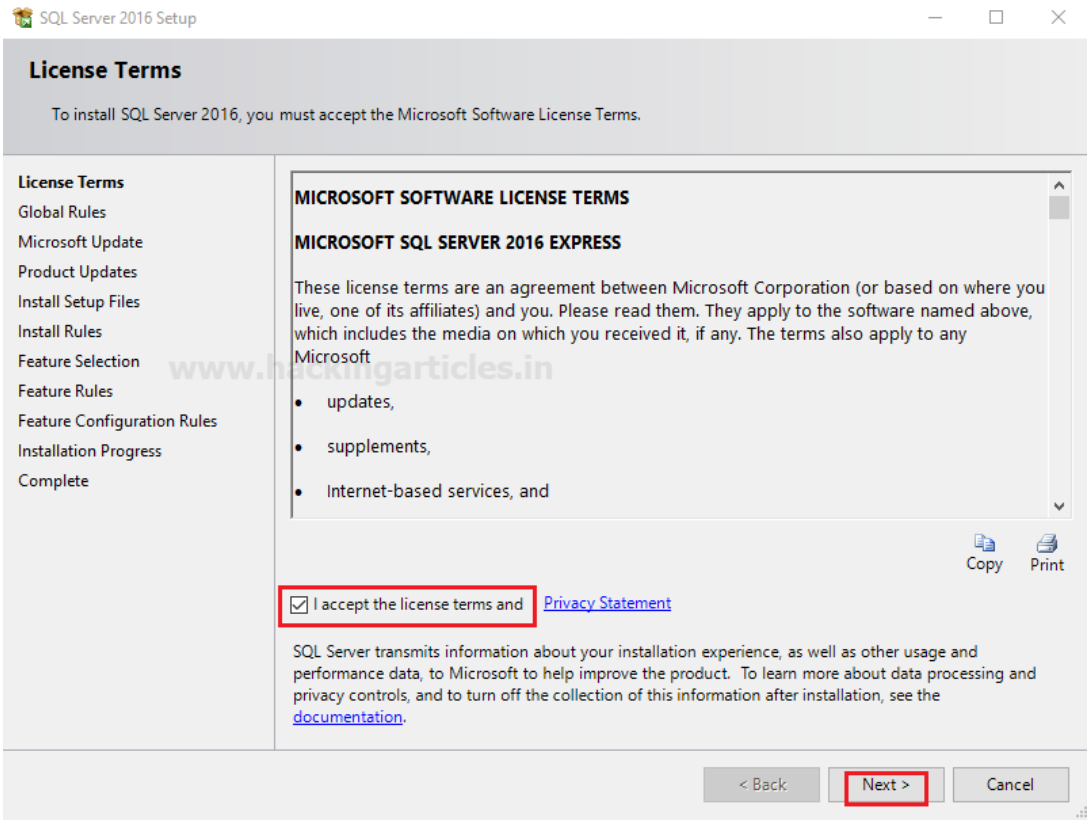
1. **Download setup file ENU\x64\SQLEXPR_x64_ENU.exe**
2. **Download setup file ENU\x86\SQLManagementStudio_x86_ENU.exe from**
3. **Download heidisql tool**

Configure SQL express setup

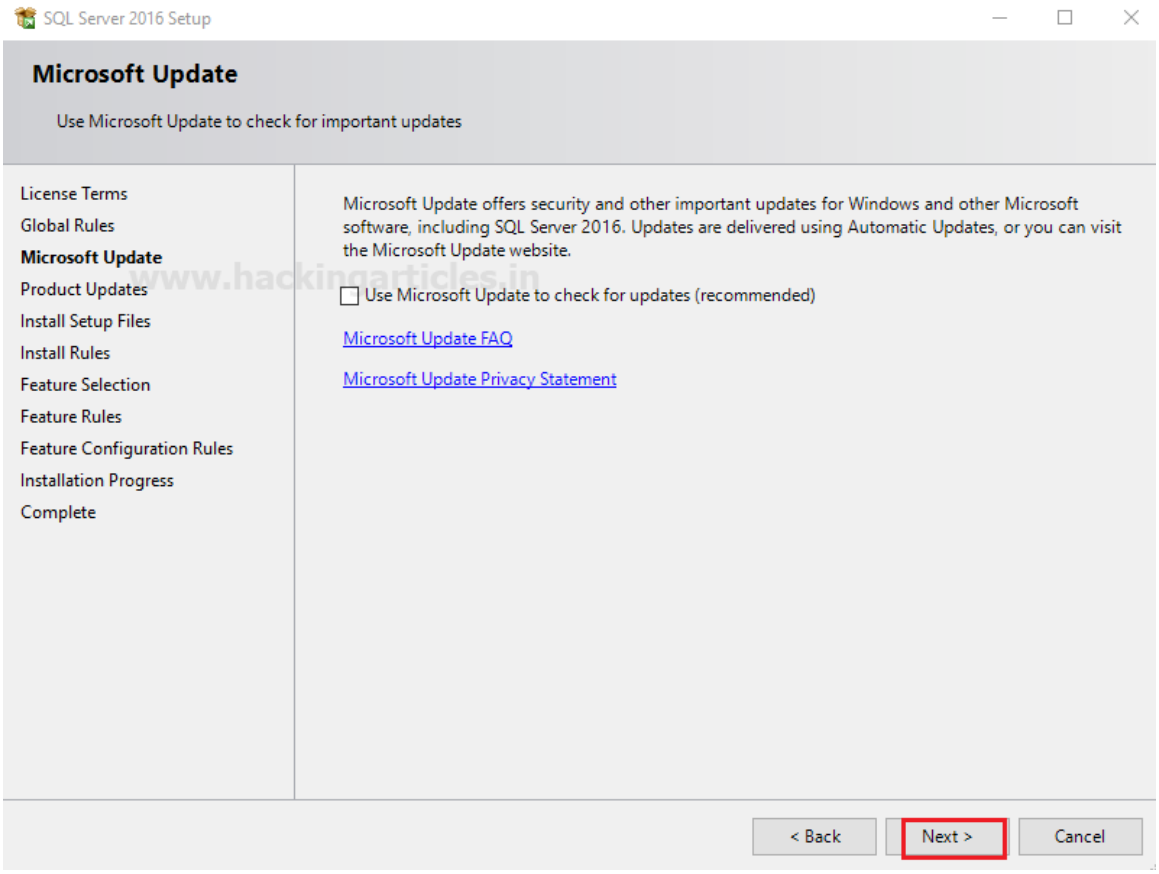
Open the **1st** download file for SQL server installation and run it as administrator. Click on installation then go with **New SQL Server standalone installation.**



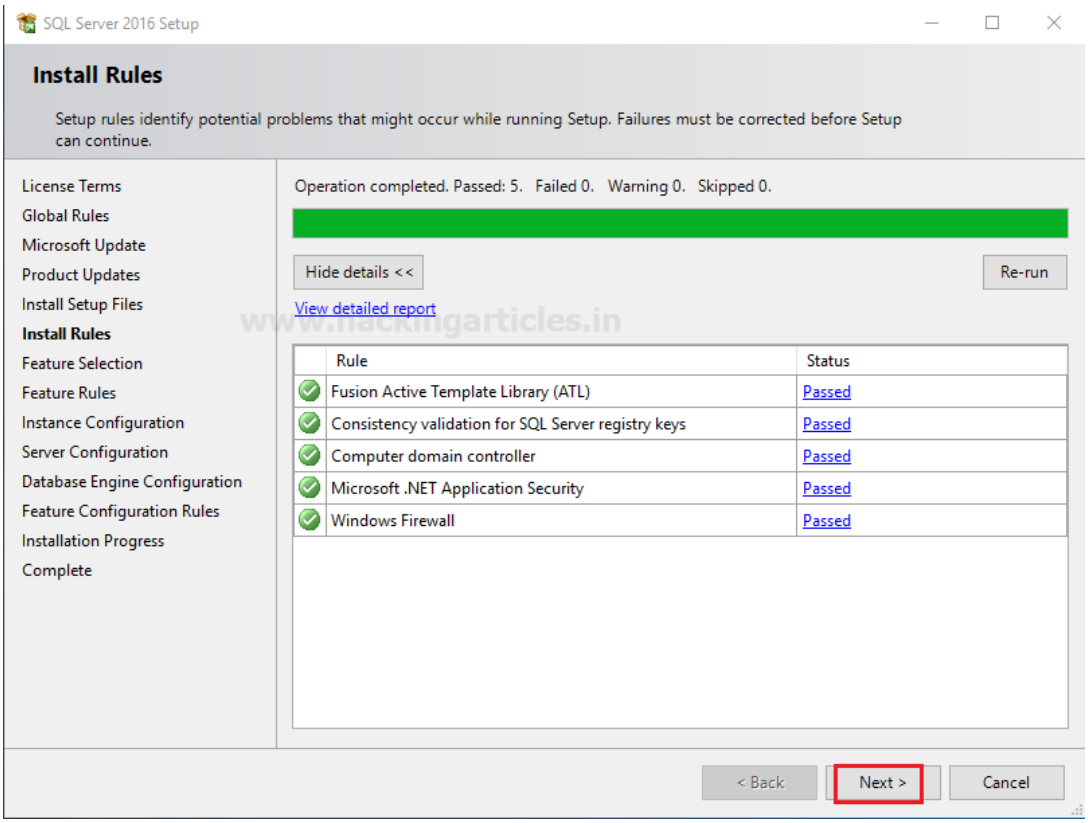
Here enables the checkbox for “I accept the license terms” and click on **next**.



Enable the checkbox for “use Microsoft update to check for update” to enhance the SQL server security and performance will install the update when you will click on **next**.



Now it will start installing SQL Server Rules files on your system, which takes some time. As soon as setup gets installed, you will get a new window screen with feature selection for your SQL server.

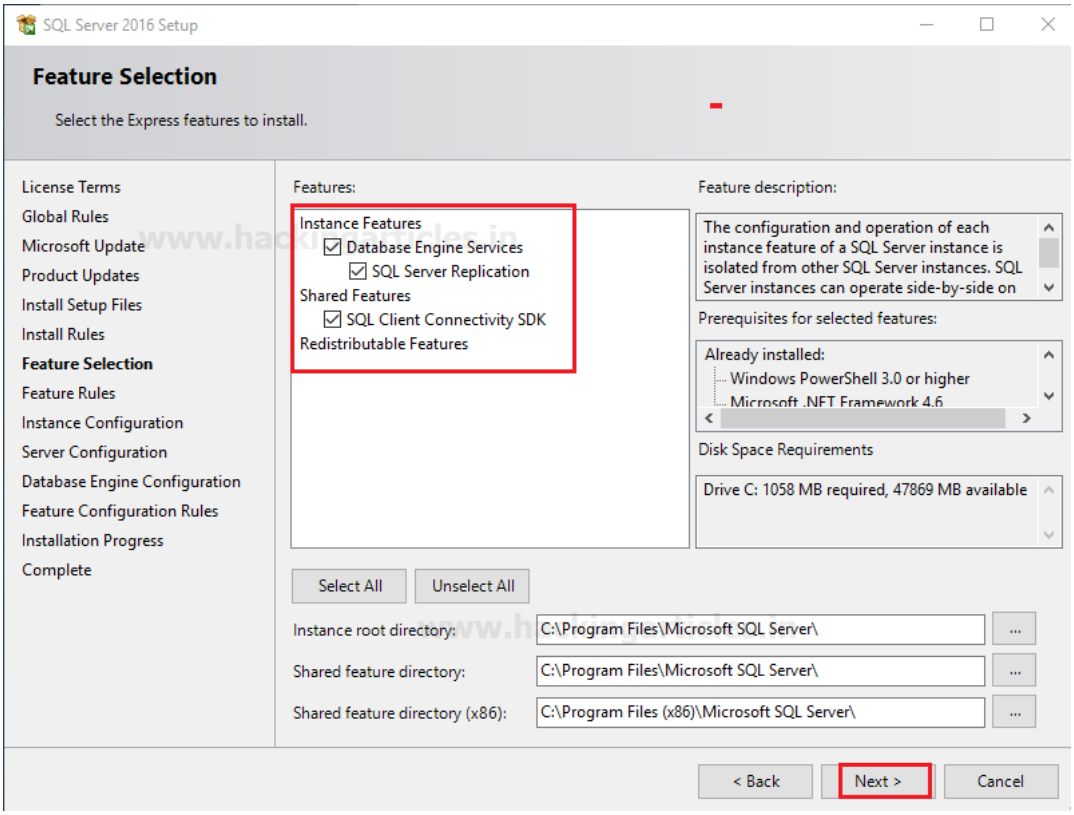


Feature Selection

Now select the features you want to install from the given image you can see I had **enabled a check box** for the following features.

- Database Engine service
- SQL Server Replication
- SQL Client Connective SDK

Click on next.



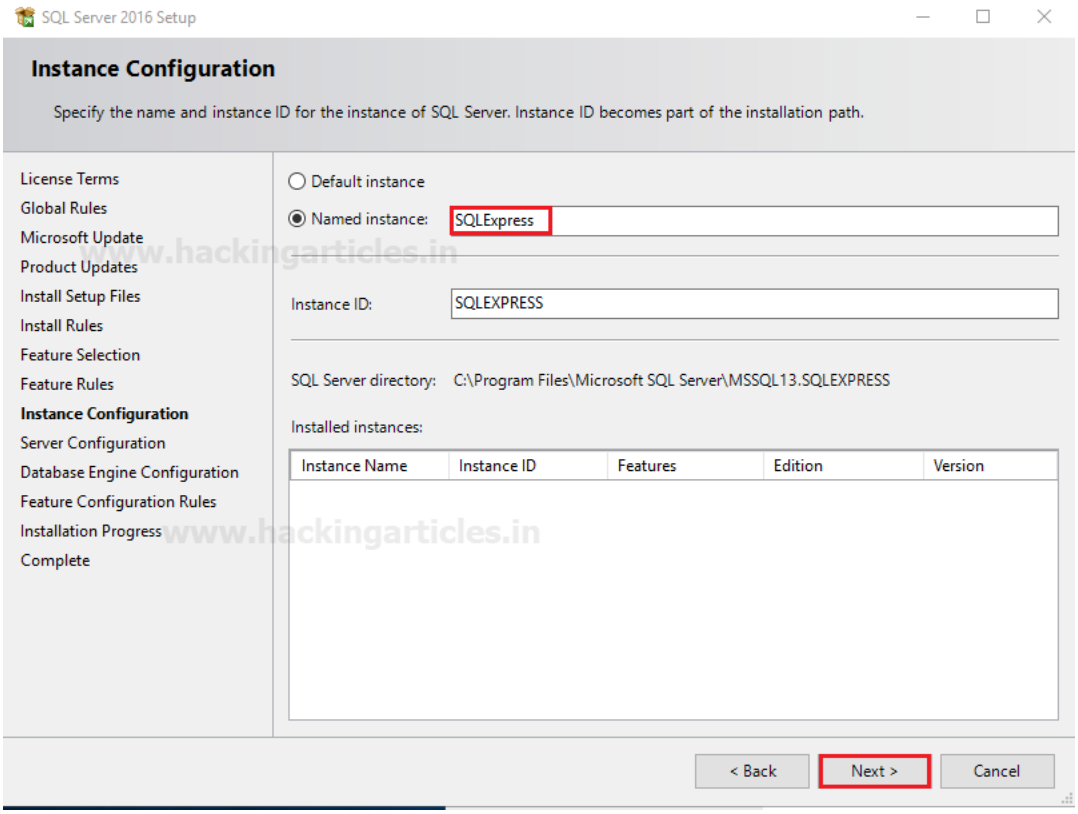
Instance Configuration

Specify the name and instance ID for this instance of SQL Server. The directory structure, registry structure, and service names all replicate the instance name and a specific instance ID. The Instance ID becomes part of the installation path.

- Enter SQLExpress in the text filed for **Name Instance**
- Enter SQLExpress in the text filed for **Instance ID**

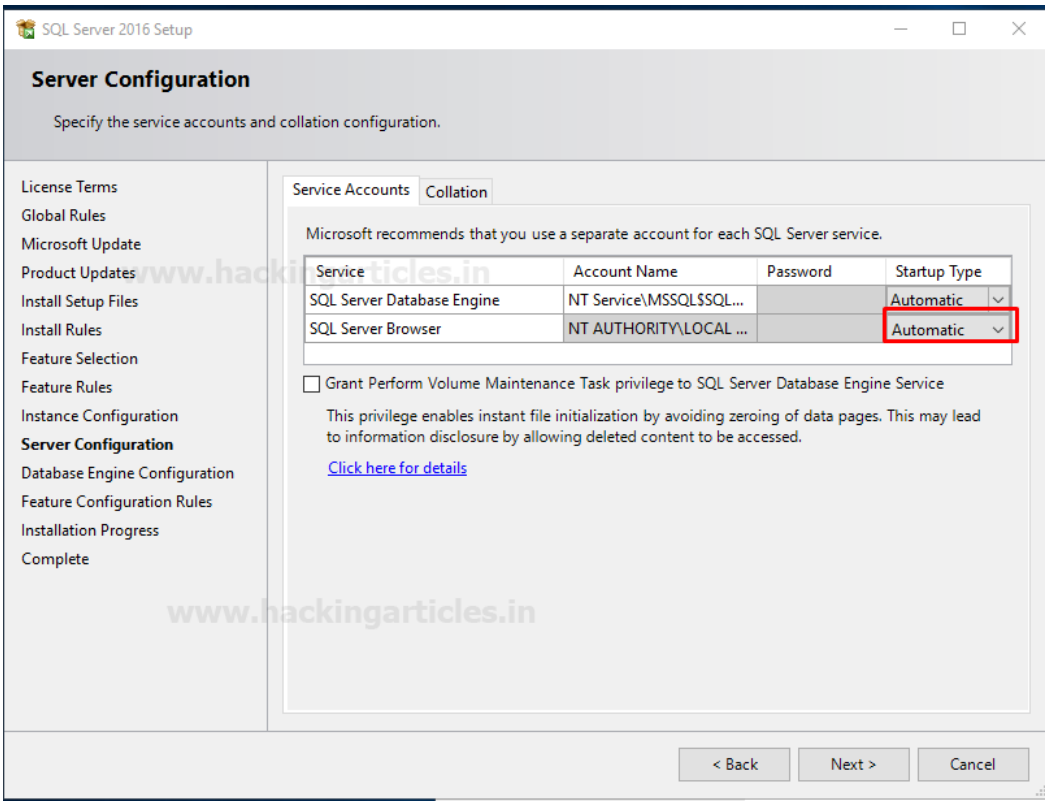
After that click on next.

You can also select a **Default Instance** also if an instance of SQL Server has not been installed previously. It does not require a user to give the name of the instance to create a connection.



On Server configuration, Specify the service accounts and collation configuration. Microsoft recommends that you use a separate account for each SQL Server service. Select the SQL Server Database Engine & SQL Server Browser Startup type Automatic. You can choose the AQL Server Browser startup type as per your requirements.

After that, click on next.



Database Engine Configuration

Specify Database Engine authentication for its security mode

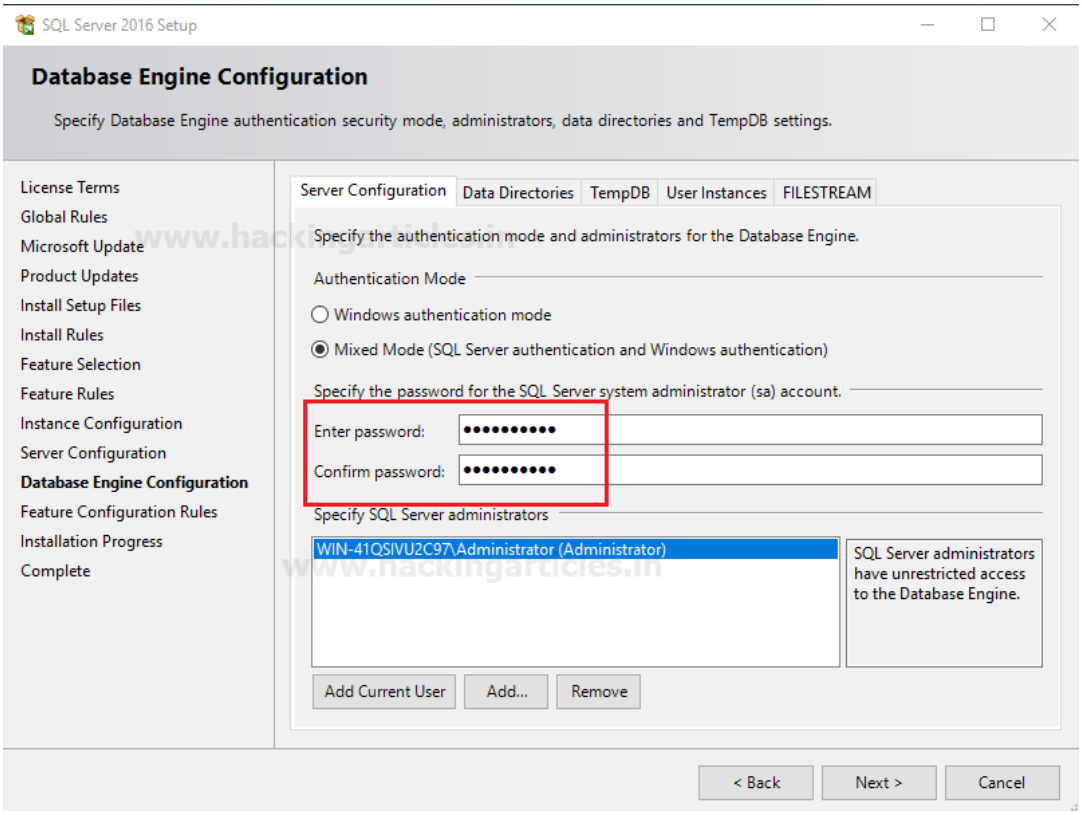
By default, **sa** is the administrator of MS SQL

Under the panel of authentication mode:

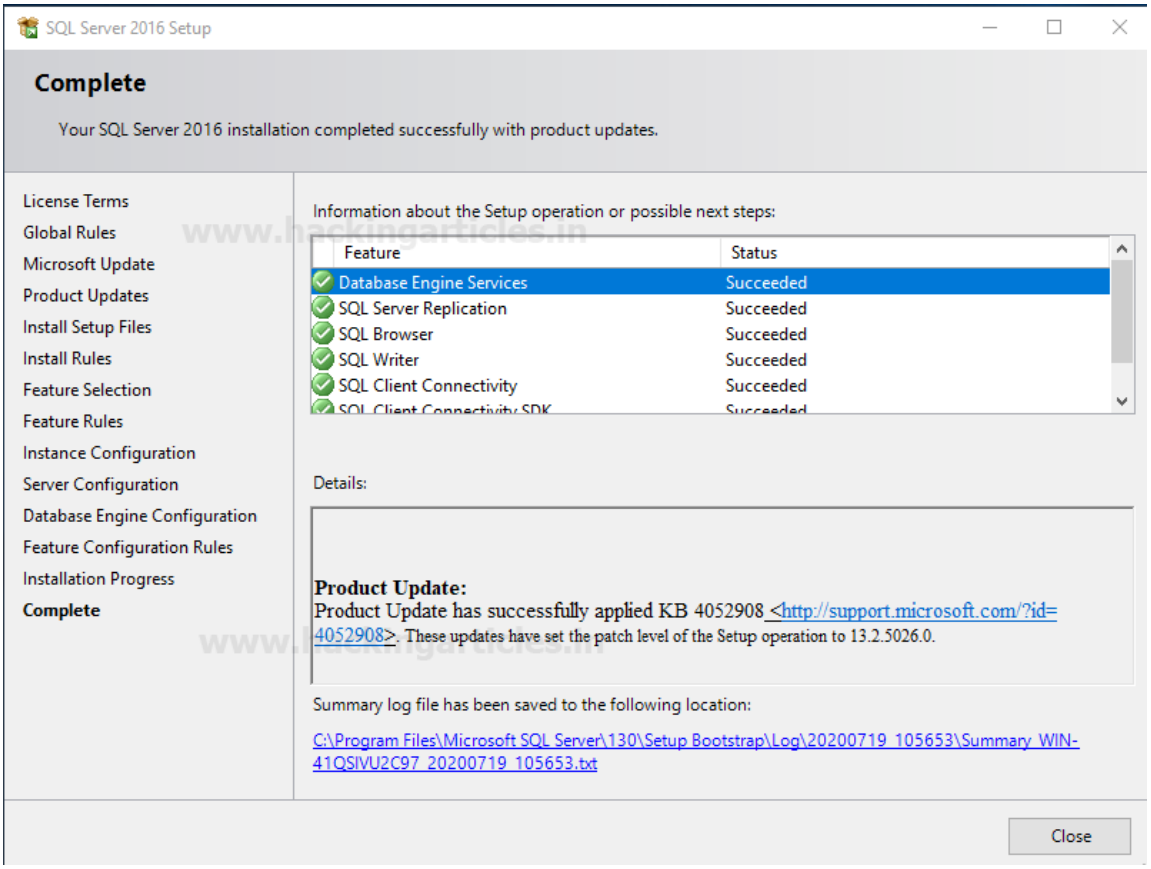
- Click on **mixed mode which** is a combination of both types of authentication SQL Server and Windows.
- Type your password and confirm the password for the administrator account.

From the given image you can observe that the selected user will be part of the administrator account of the SQL server who has unrestricted access to the database engine.

After then click on **next** and **next**.

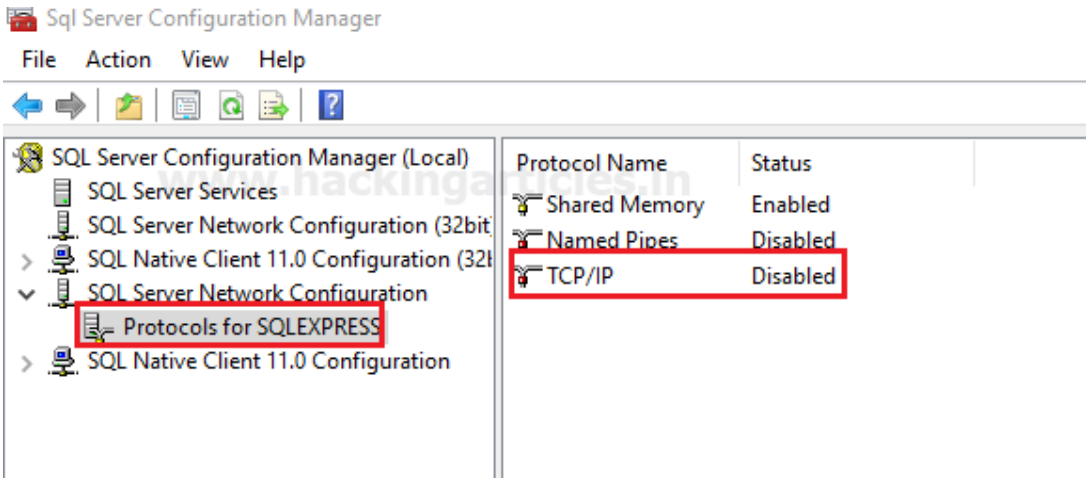


Your SQL server 2016 installation was completed successfully, here you can check the status for installed features.

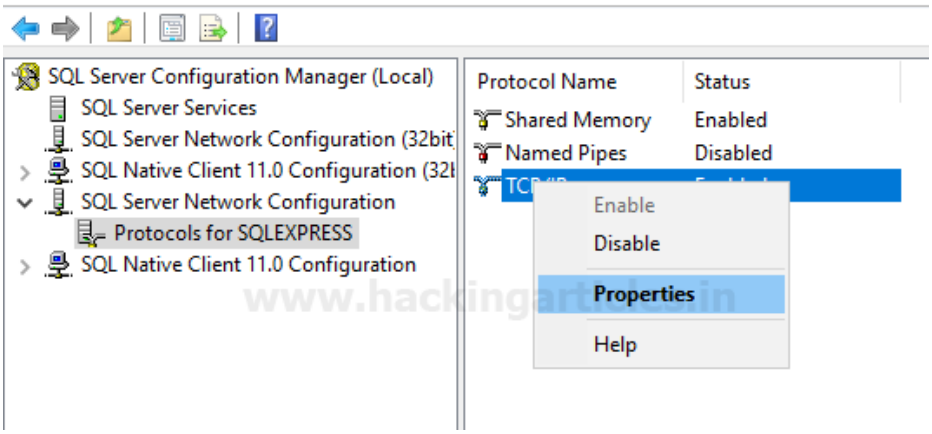


Now **open the SQL server configuration manager** where you will see the left and right panel.

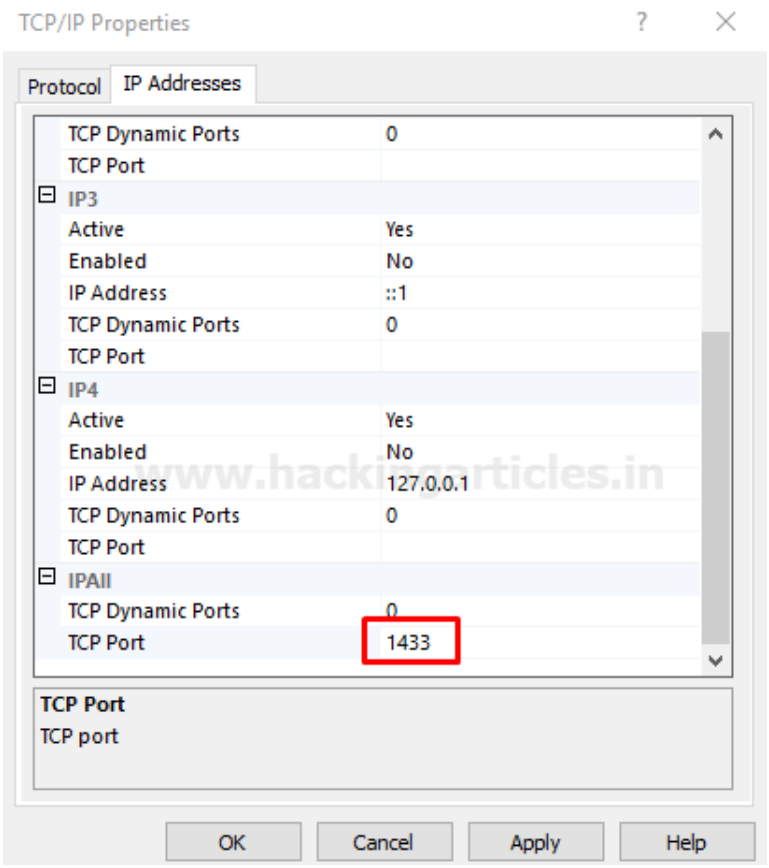
Click on the **protocol for SQL Express** in the left panel and then select protocol name "**TCP/IP**" in the right panel.



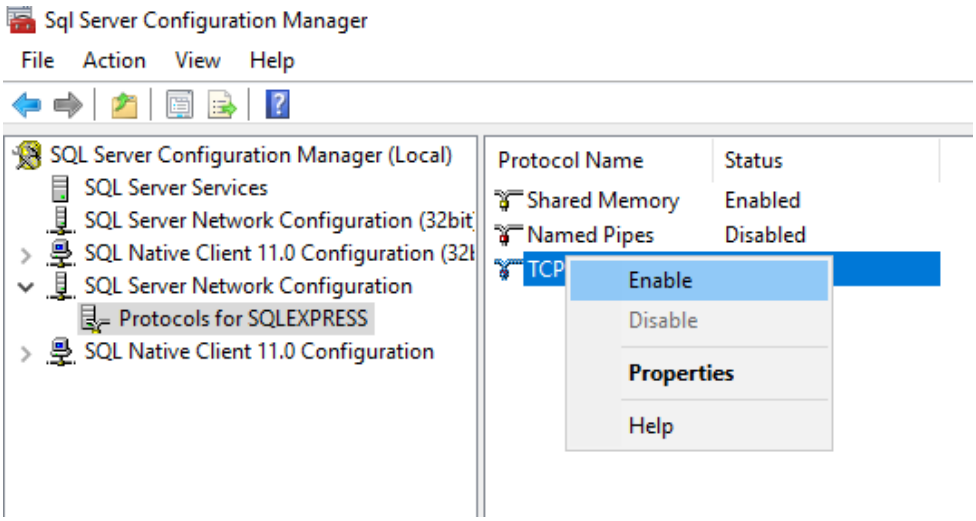
Go to **TCP/IP** protocol Properties



Under IP Addresses specify **TCP port 1433** tab, Click on Apply, and **Enable the TCP/IP.**

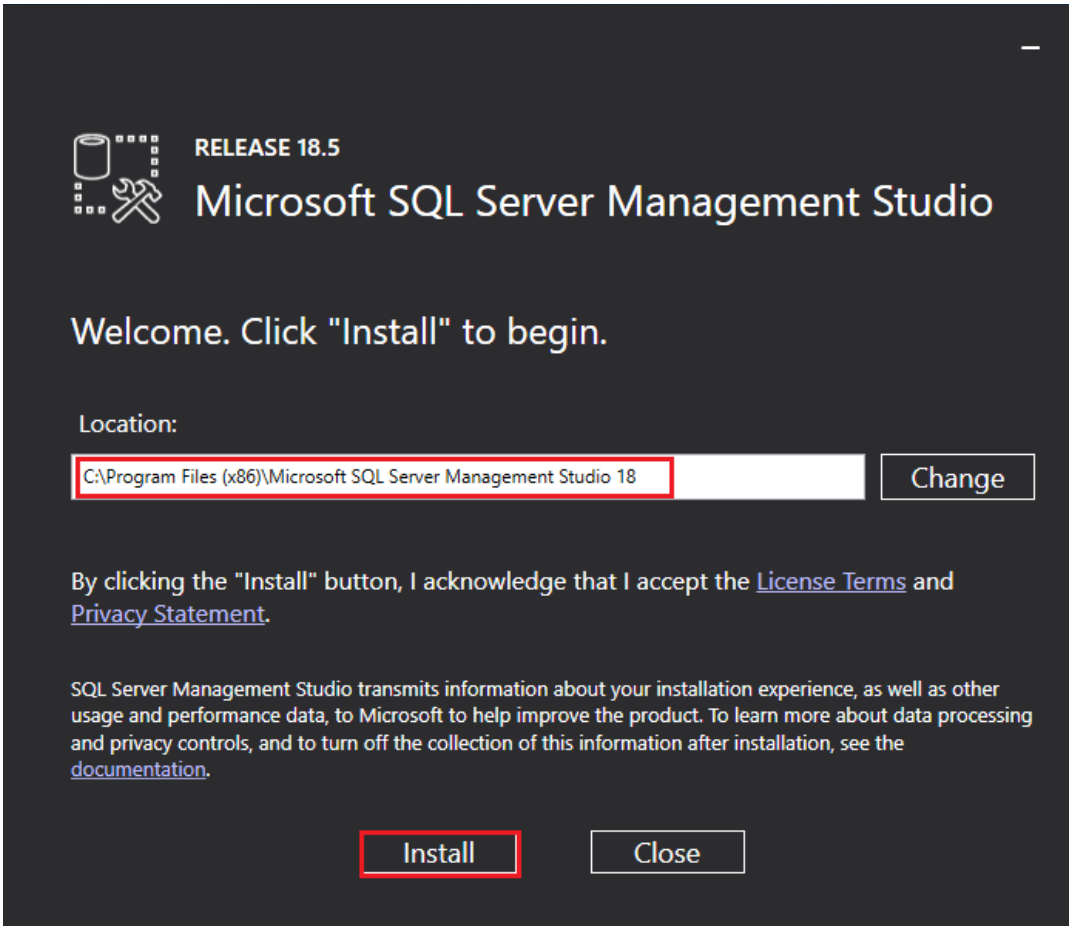


Now you can see, the TCP/IP is enabled as shown in the image.

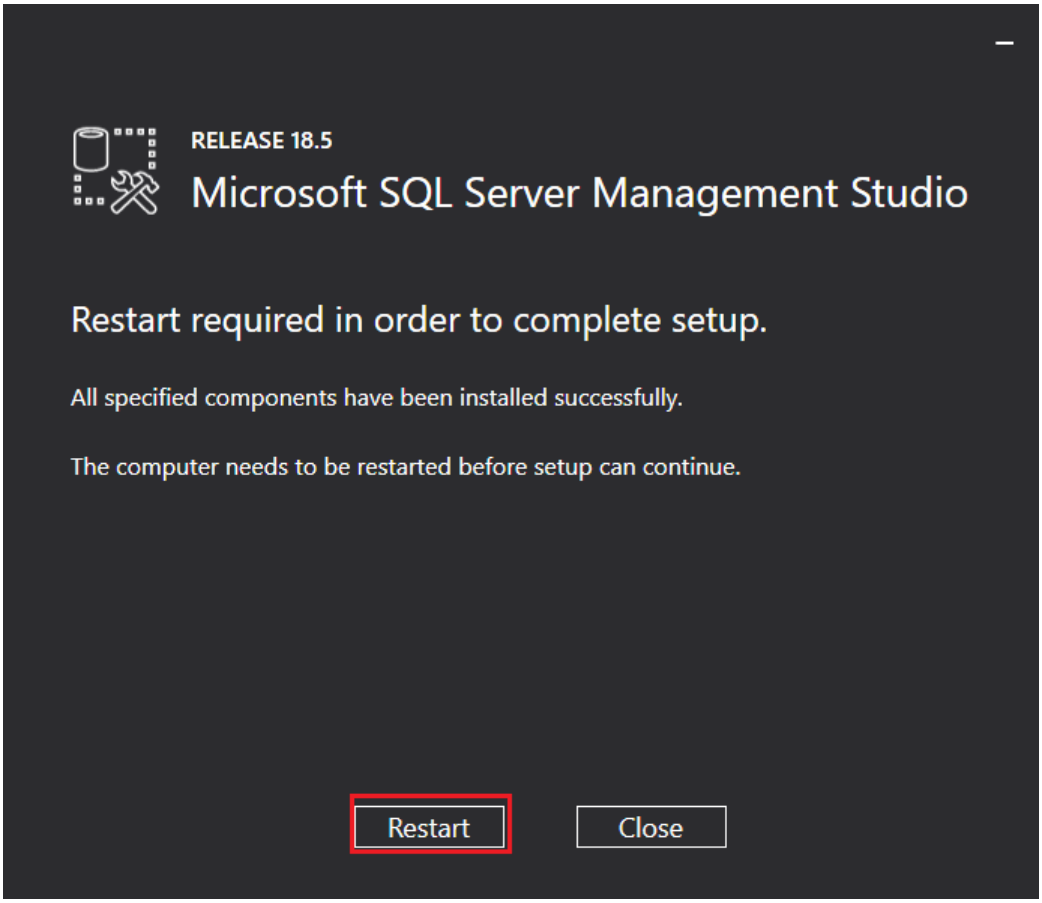


Configure SQL Management Studio setup

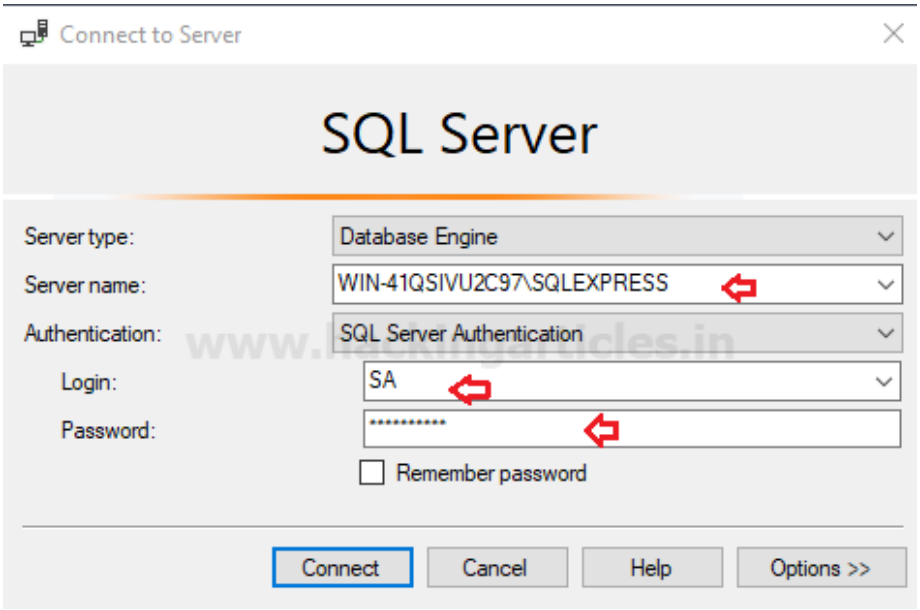
Now open 2nd downloaded application for SQL server management setup and click on Install.



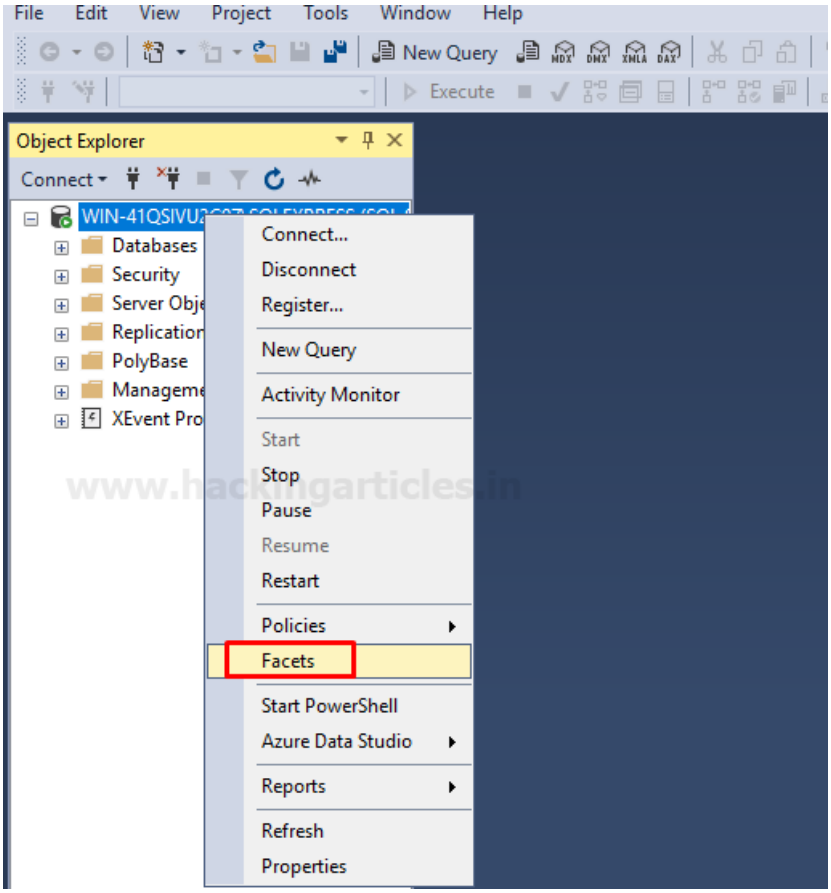
Now it will start installing SQL server Management Studia setup file on your system which takes some time once done will ask to restart.



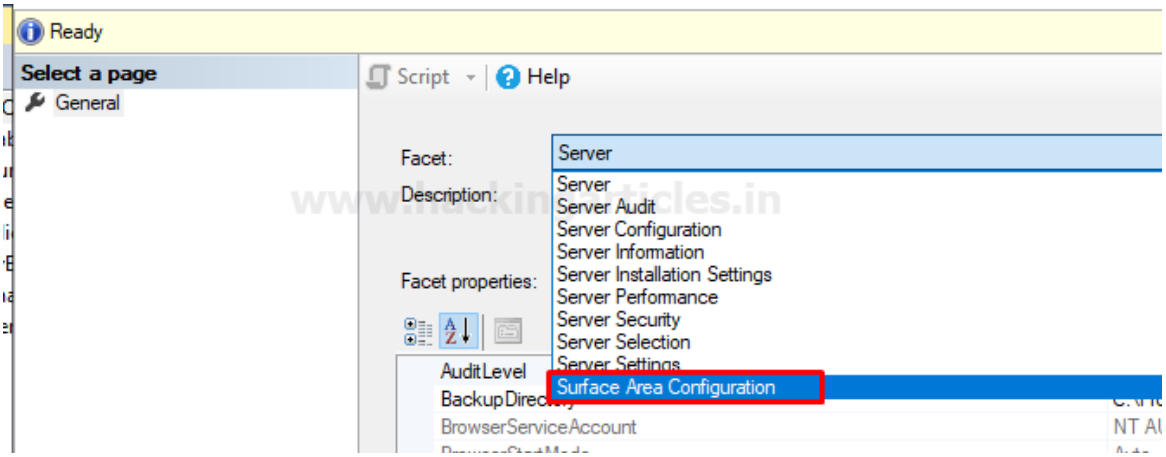
Now login into SQL Server using admin credential and click on connect.



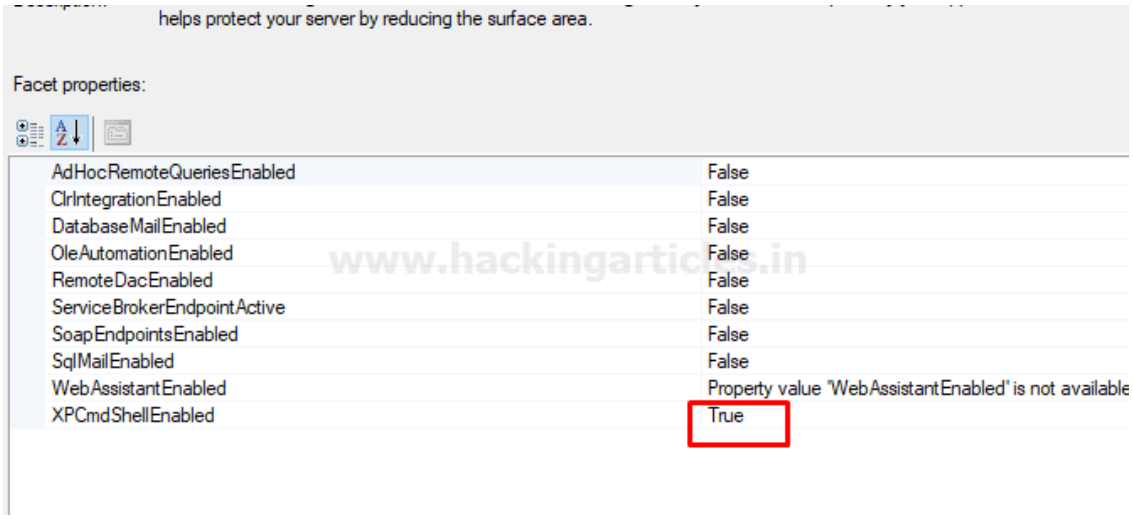
Once you are login into the SQL server then Right Click on SQLEXPRESS(SQL Server) and go to Facets



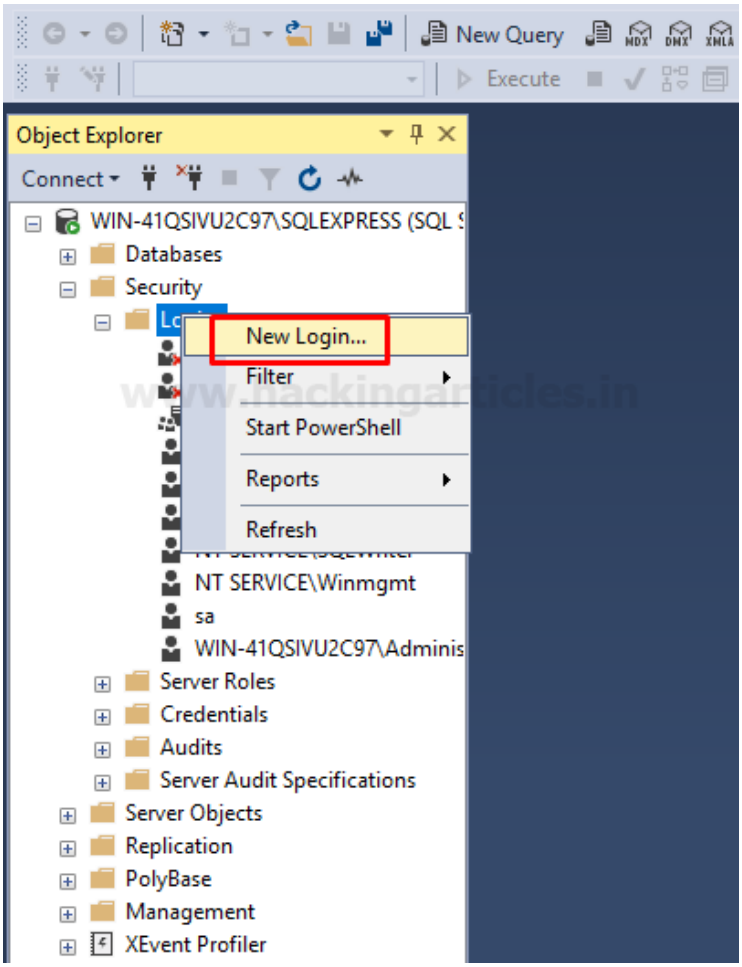
On the window, go to the **General tab** left side, then on the right side explore the **Facet** and select **Surface Area Configuration**.



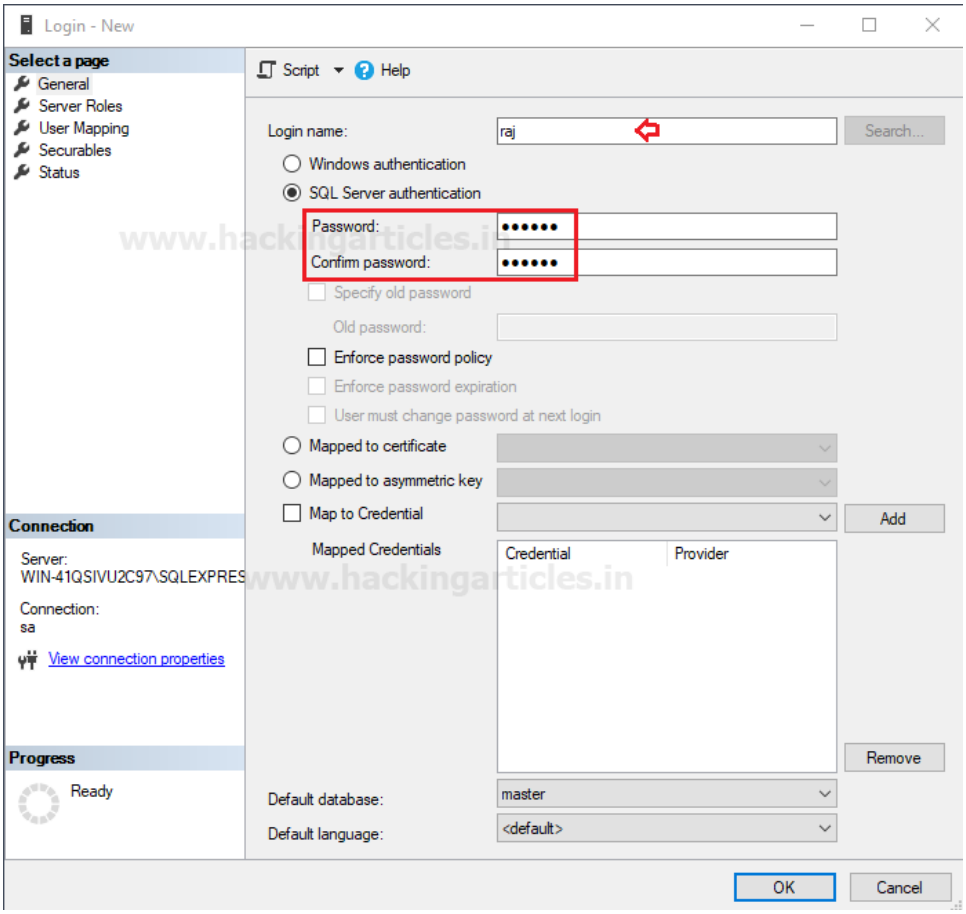
In the next window select **True** on **XPCmdShellEnabled** and apply.



Explore the security folder and create a new login account for other users.



Enter the user name as I had given “Raj” and set a password by choosing SQL server authentication for this user. From the given image, you can observe that **master** is the default database.



Connect to server from windows 10

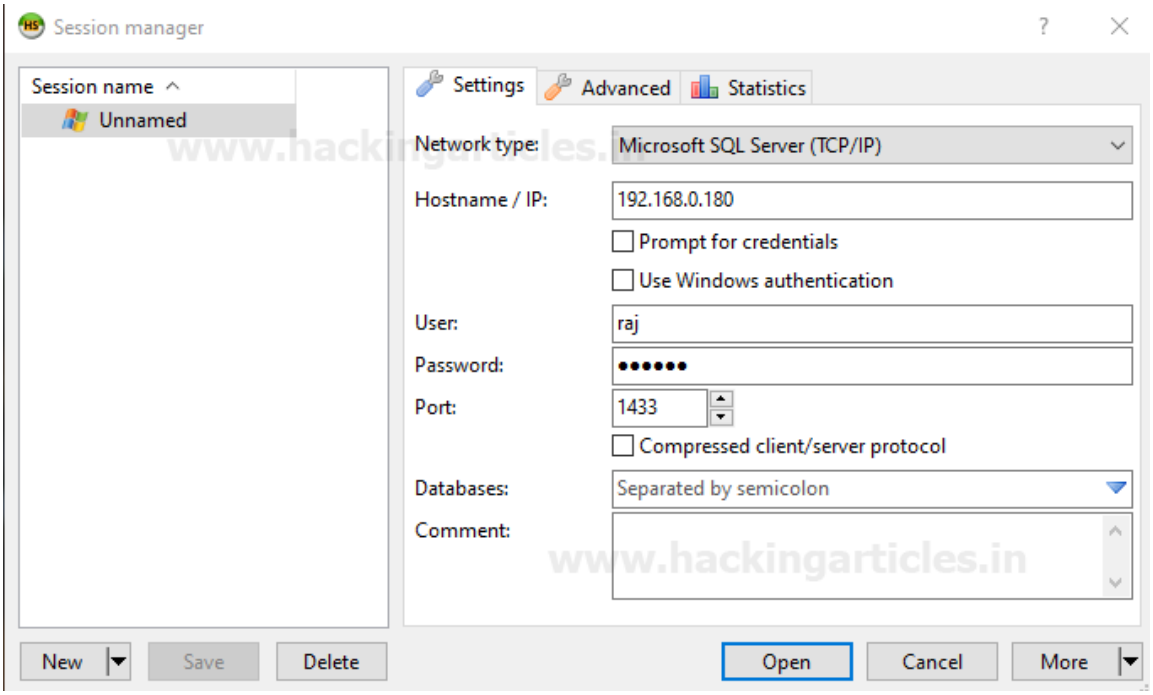
Run **heidisql** tool to connect with MS SQL Server through Raj user as given below:

Network type: TCP/IP

1	**Hostname /IP: 192.168.1.180**
2	**User: Raj**
3	**Password: 123456**
4	**Port: 1433**

HeidiSQL is a useful and reliable tool designed for web developers using the popular MySQL server, Microsoft SQL databases, and PostgreSQL. It enables you to browse and edit data, create and edit tables, views, procedures, triggers, and scheduled events.

Now click on **open**



Great!! We have successfully accessed the database system of the MSSQL server. You can modify or create a new table or new database and much more things.