Penetration Testing Lab Setup:MS-SQL

July 30, 2020   By Raj Chandel

Today you will learn how to install and configure MS SQL server in windows server 2019 operating system for penetration testing within the VM Ware. MSSQL is Microsoft SQL Server for database management in the network. By default, it runs on port 1433.

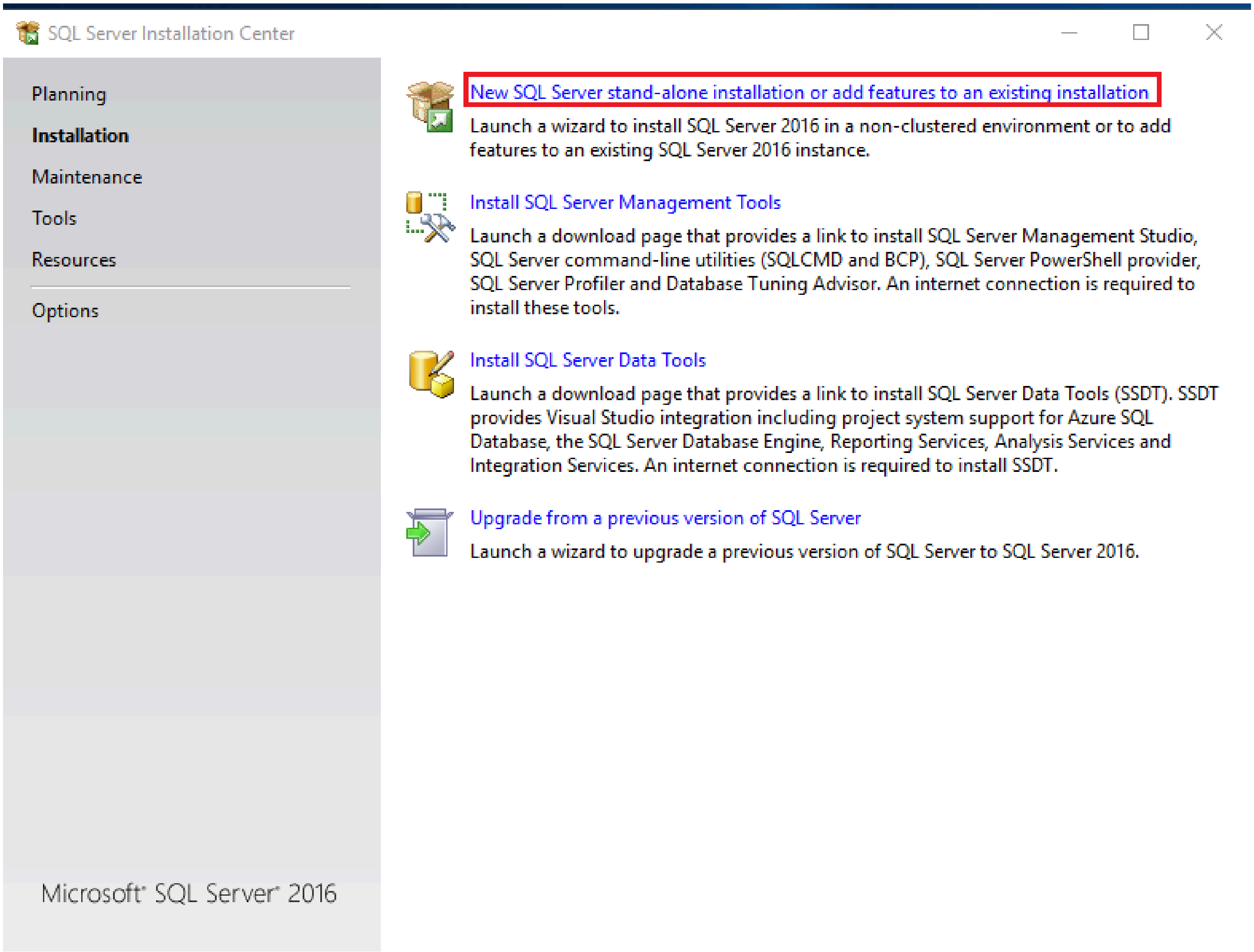
Table of Content

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 as administrator. Click on installation then go with **New SQL Server standalone installation.**



New SQL Server stand-alone installation or add features to an existing installation

Launch a wizard to install SQL Server 2016 in a non-clustered environment or to add features to an existing SQL Server 2016 instance.

Install SQL Server Management Tools

Launch a download page that provides a link to install SQL Server Management Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell provider, SQL Server Profiler and Database Tuning Advisor. An internet connection is required to install these tools.

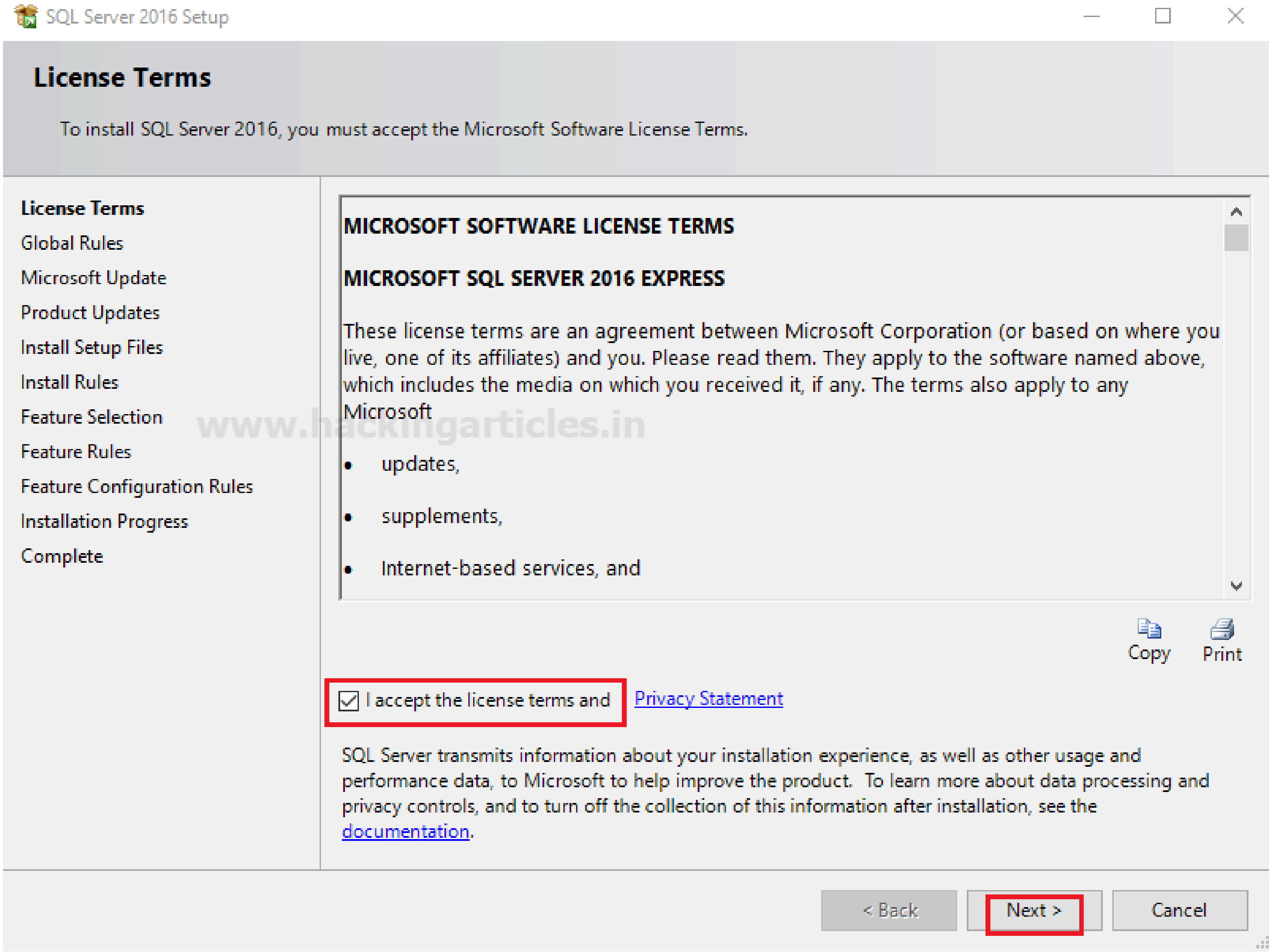
Install SQL Server Data Tools

Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.

Upgrade from a previous version of SQL Server

Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2016.

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



SQL Server 2016 Setup

License Terms

To install SQL Server 2016, you must accept the Microsoft Software License Terms.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT SQL SERVER 2016 EXPRESS

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

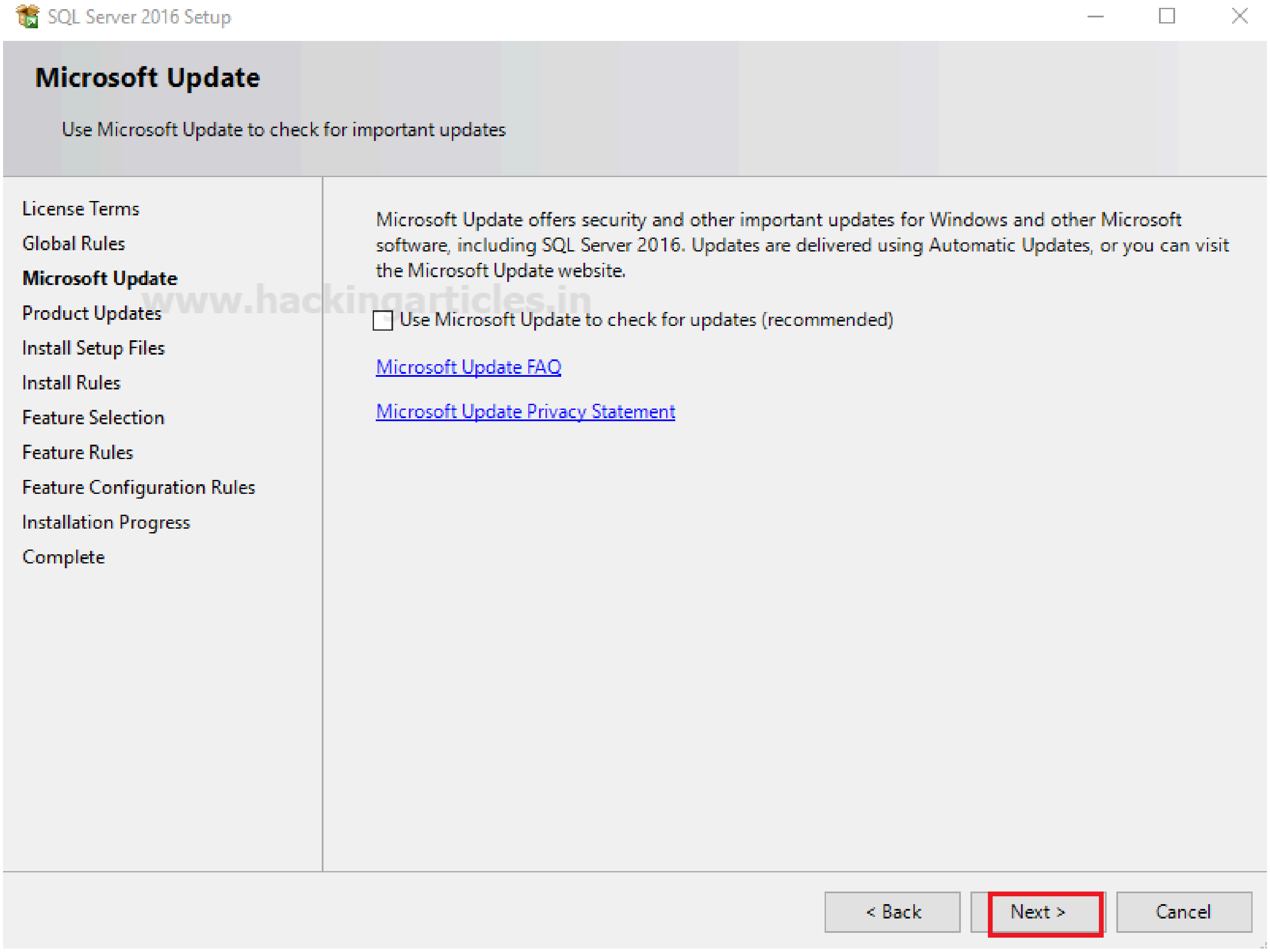
- updates,
- supplements,
- Internet-based services, and

www.hackingarticles.in

☑ I accept the license terms and Privacy Statement

SQL Server transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the documentation.

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**.



SQL Server 2016 Setup

Microsoft Update

Use Microsoft Update to check for important updates

Microsoft Update offers security and other important updates for Windows and other Microsoft software, including SQL Server 2016. Updates are delivered using Automatic Updates, or you can visit the Microsoft Update website.

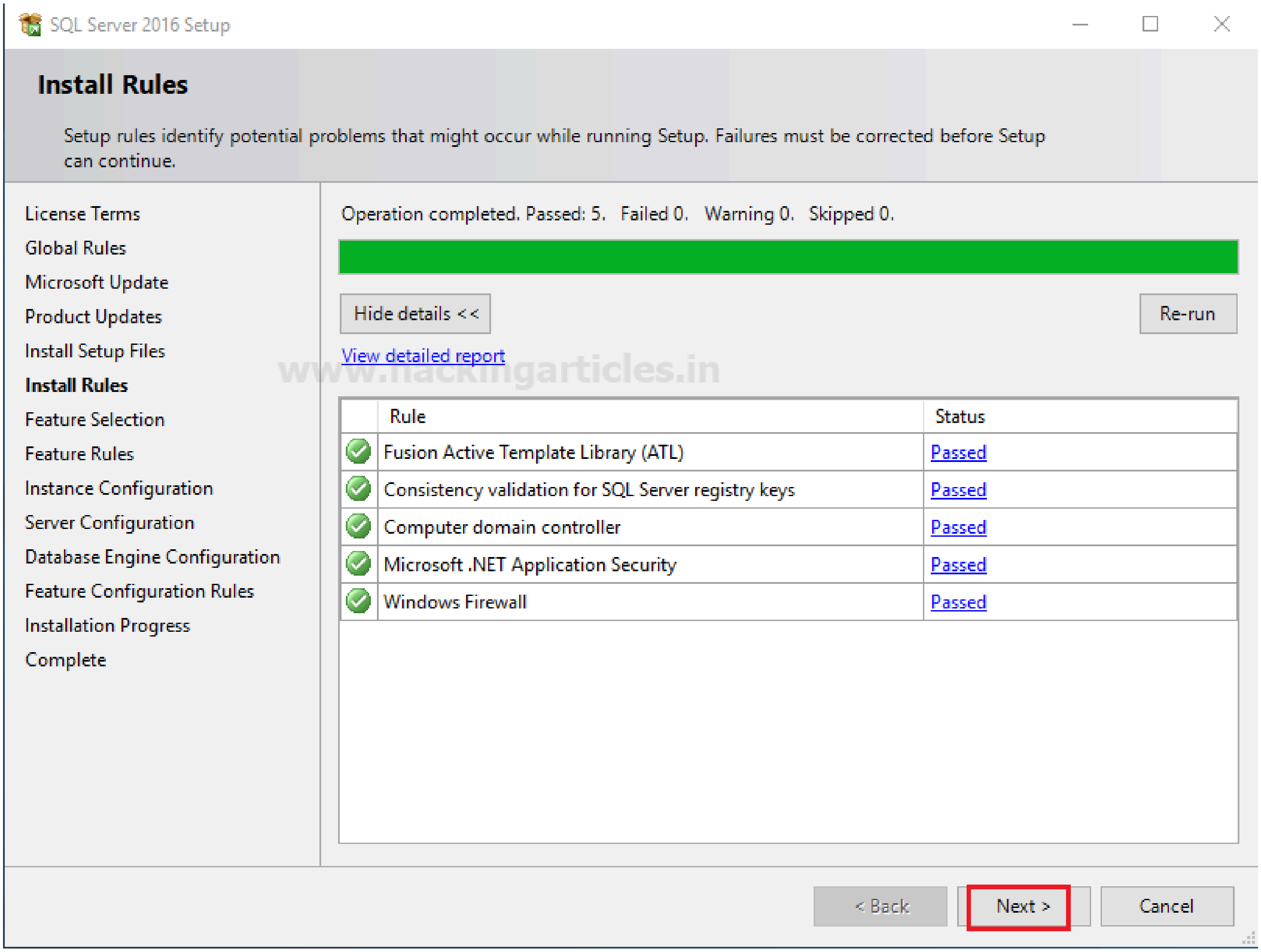
□ Use Microsoft Update to check for updates (recommended)

Microsoft Update FAQ

Microsoft Update Privacy Statement

www.hackingarticles.in

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



www.hackingarticles.in

Operation completed. Passed: 5. Failed 0. Warning 0. Skipped 0.

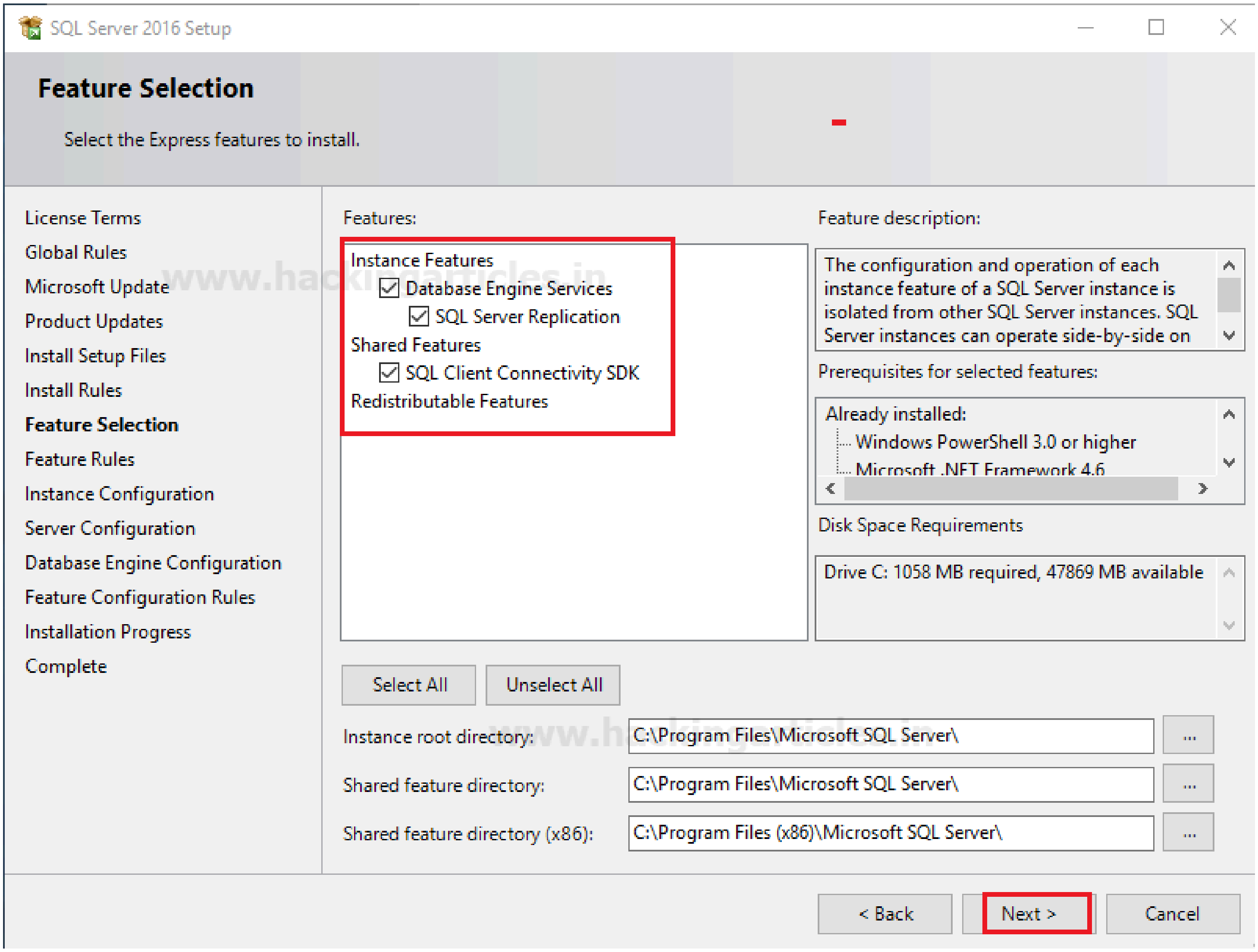
	Rule	Status
✓	Fusion Active Template Library (ATL)	Passed
✓	Consistency validation for SQL Server registry keys	Passed
✓	Computer domain controller	Passed
✓	Microsoft .NET Application Security	Passed
✓	Windows Firewall	Passed

Feature Selection

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

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

Click on next.



Feature Selection

Select the Express features to install.

Features:

Instance Features
- ☑ Database Engine Services
  - ☑ SQL Server Replication

Shared Features
- ☑ SQL Client Connectivity SDK

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

Prerequisites for selected features:

Already installed:
- Windows PowerShell 3.0 or higher
- Microsoft .NET Framework 4.6

Disk Space Requirements

Drive C: 1058 MB required, 47869 MB available

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\

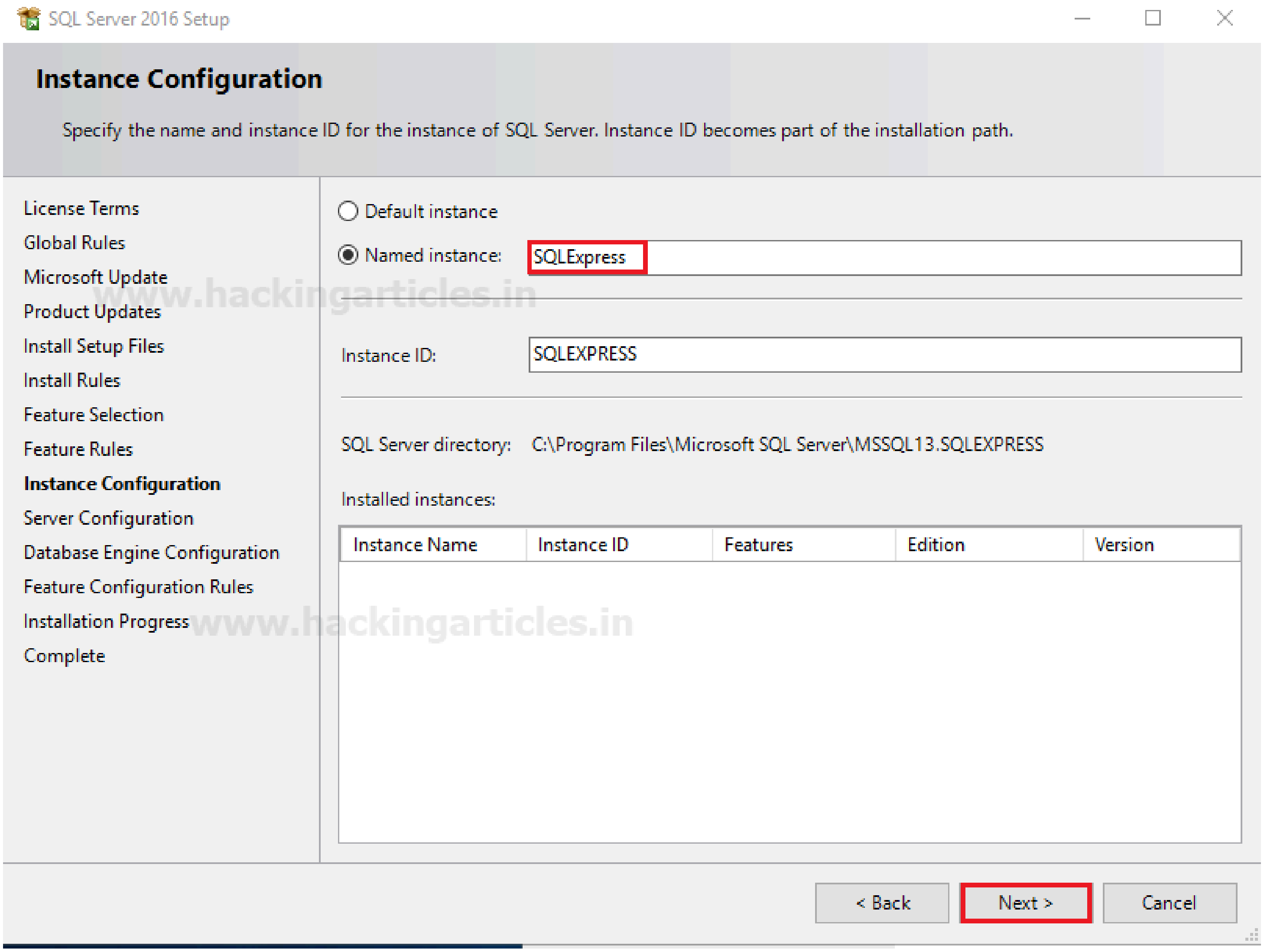
Instance Configuration

Specify the name and instance ID for instance of SQL server. The directory structure, registry structure, and service names all replicate the instance name and a specific instance ID. 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 then click on next

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



www.hackingarticles.in
www.hackingarticles.in

Instance Configuration

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

○ Default instance

● Named instance: SQLExpress

Instance ID: SQLEXPRESS

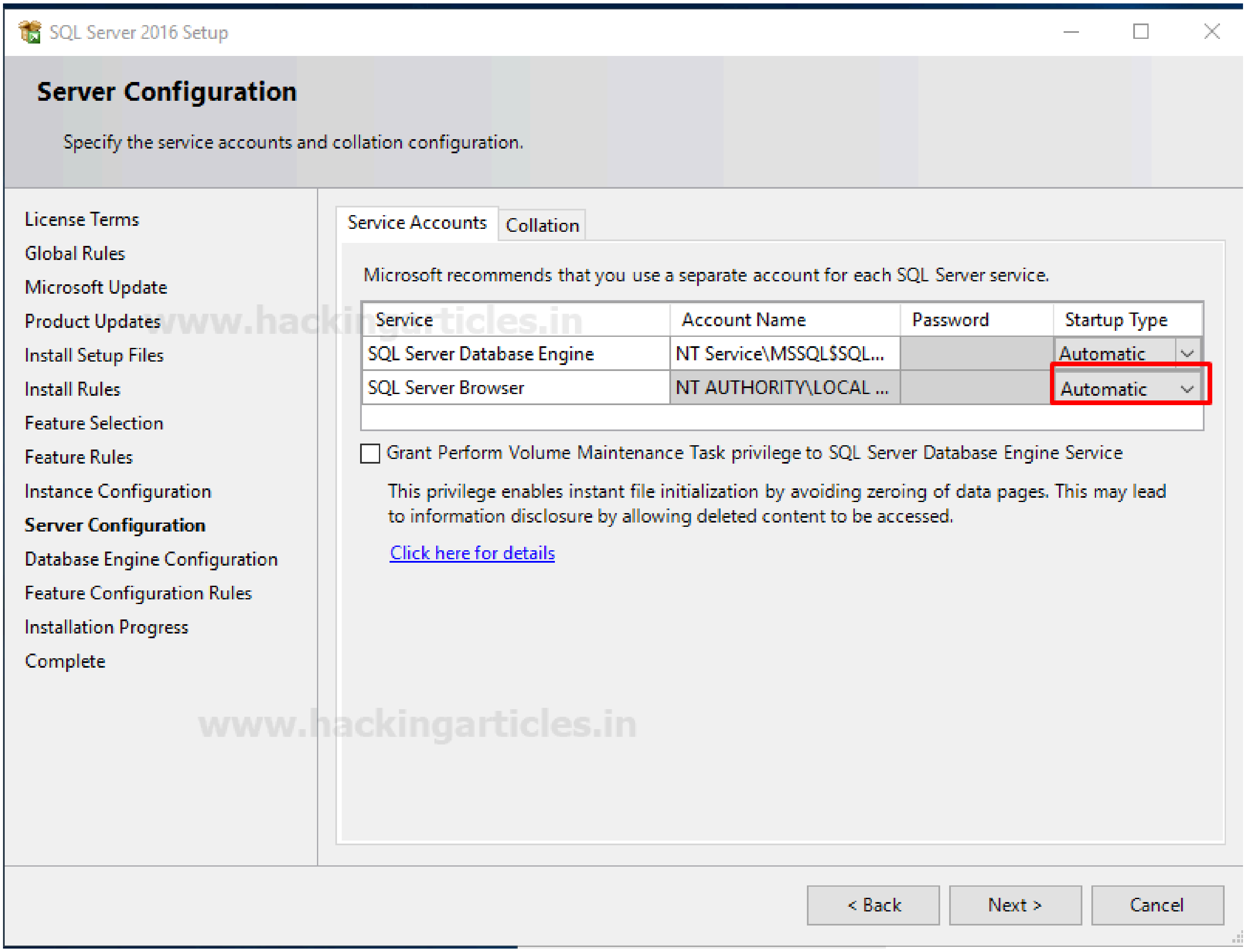
SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL13.SQLEXPRESS

Installed instances:

Instance Name	Instance ID	Features	Edition	Version

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 AQL Server Browser startup Type as per your requirement.

After then click on **next**



SQL Server 2016 Setup

Server Configuration

Specify the service accounts and collation configuration.

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 Browser	NT AUTHORITY\LOCAL ...		Automatic

☐ 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

www.hackingarticles.in

Database Engine Configuration

Specify Database Engine authentication for its security mode

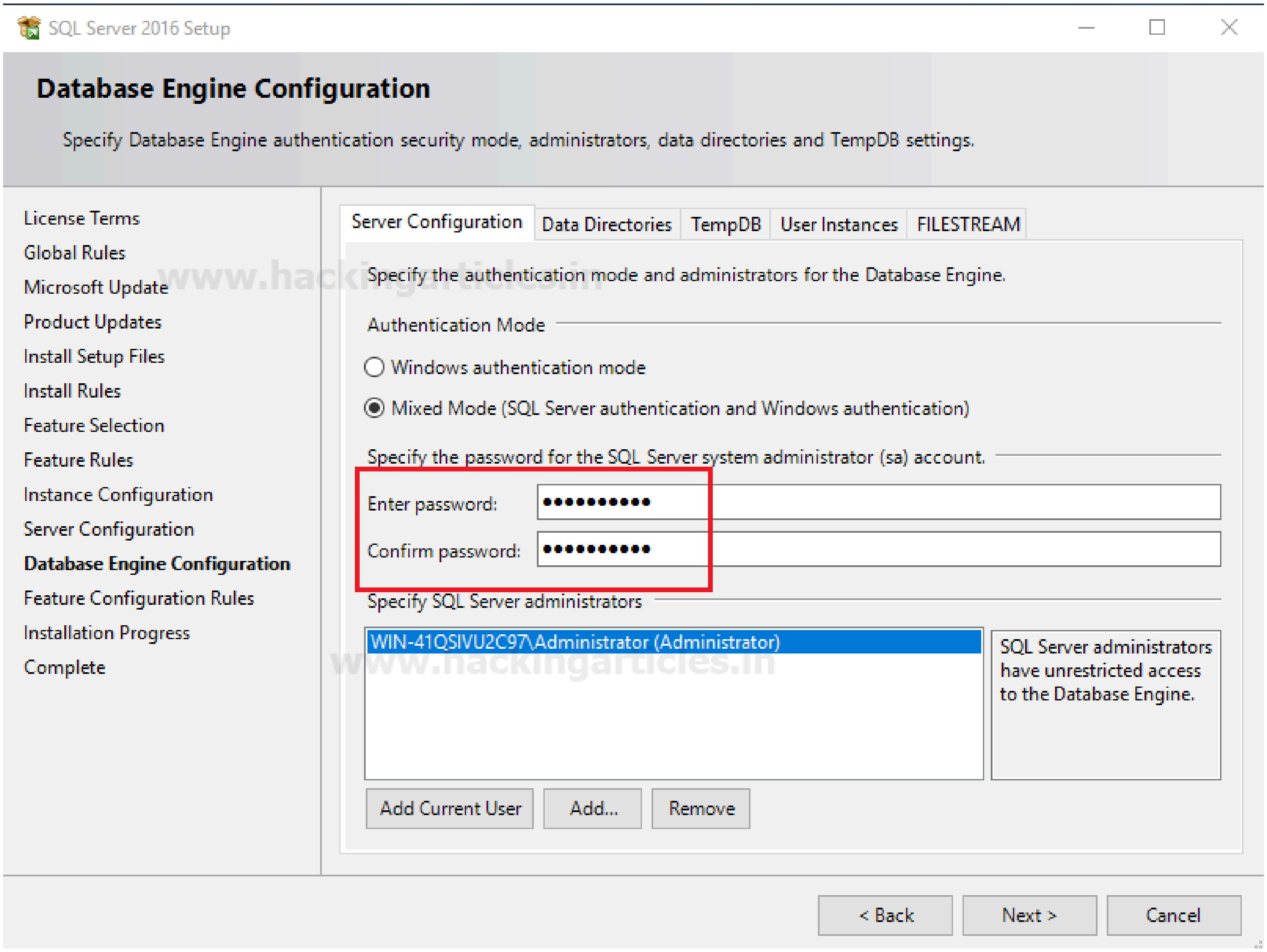
By default, **sa** is the administrator of MS SQL

Under the panel of authentication mode:

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

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

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



SQL Server 2016 Setup

Database Engine Configuration

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

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: ●●●●●●●●●●●

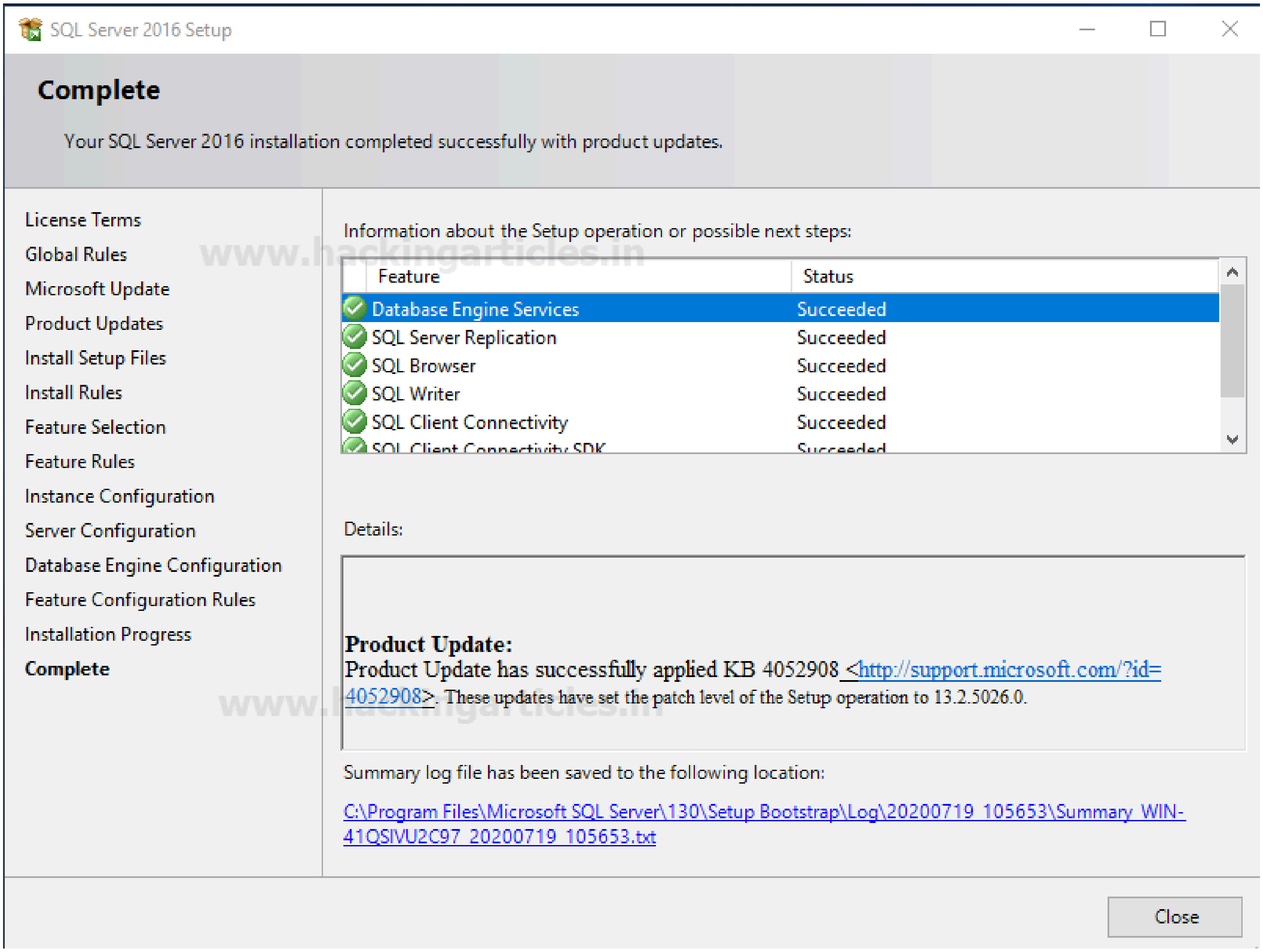
Specify SQL Server administrators

WIN-41QSIVU2C97\Administrator (Administrator)

SQL Server administrators have unrestricted access to the Database Engine.

www.hackingarticles.in

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



www.hackingarticles.in

Complete

Your SQL Server 2016 installation completed successfully with product updates.

Information about the Setup operation or possible next steps:

Feature	Status
Database Engine Services	Succeeded
SQL Server Replication	Succeeded
SQL Browser	Succeeded
SQL Writer	Succeeded
SQL Client Connectivity	Succeeded
SQL Client Connectivity SDK	Succeeded

Details:

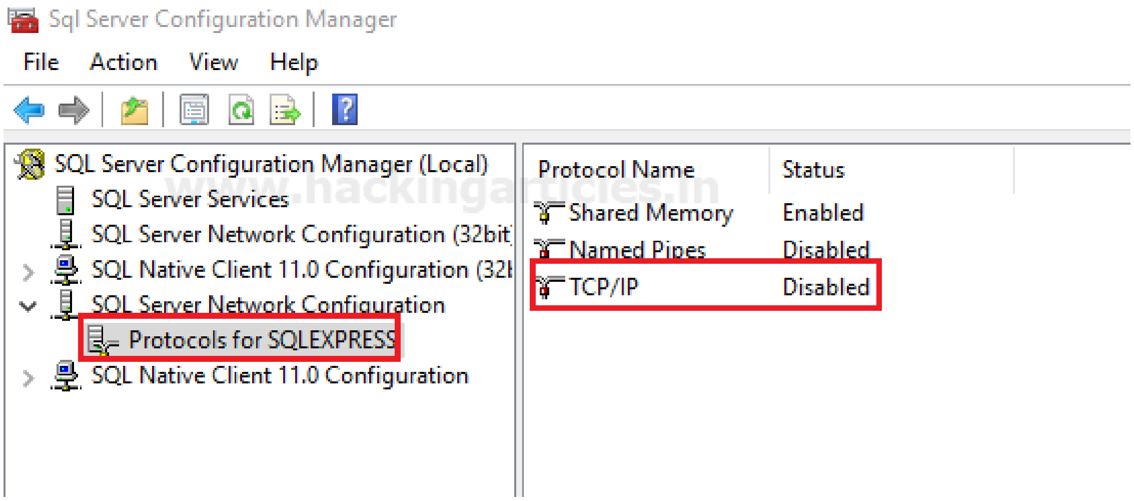
Product Update:
Product Update has successfully applied KB 4052908 <http://support.microsoft.com/?id=4052908>. These updates have set the patch level of the Setup operation to 13.2.5026.0.

Summary log file has been saved to the following location:

C:\Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20200719_105653\Summary_WIN-41QSIVU2C97_20200719_105653.txt

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

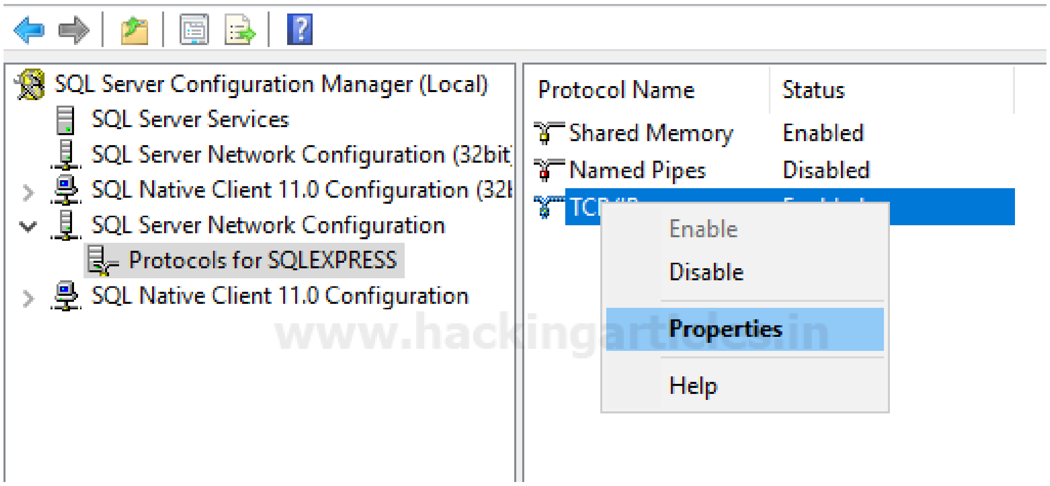
Click on the **protocol for SQL Express** in the left panel and then after select protocol name “**TCP/IP**” in the right panel.


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 11.0 Configuration (32l
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 11.0 Configuration

www.hackingarticles.in

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

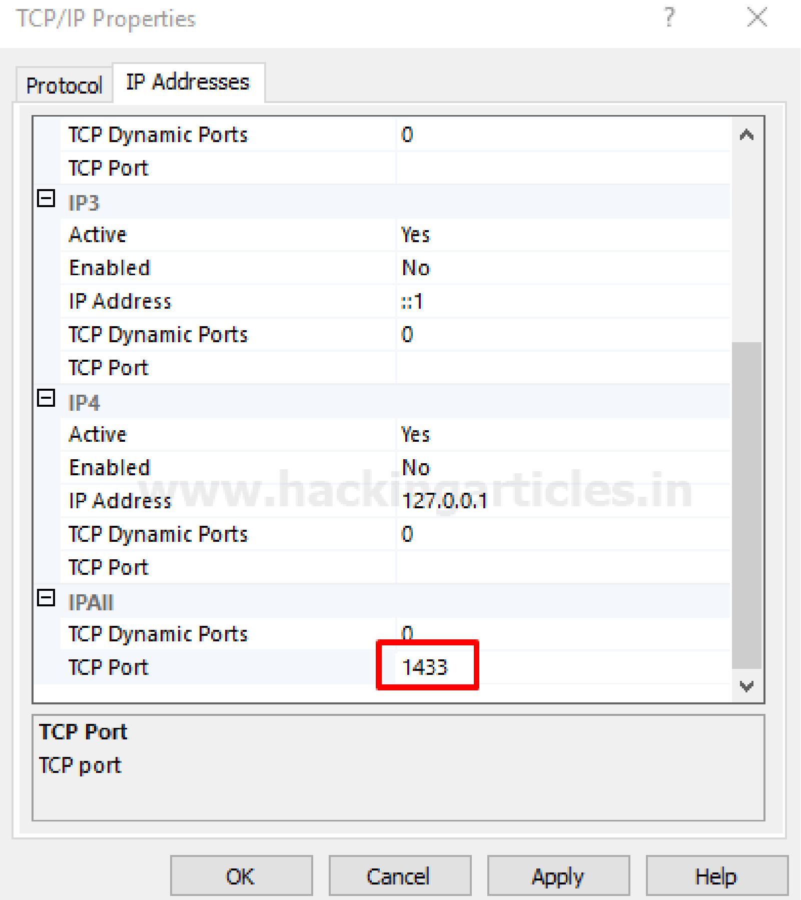
Go to **TCP/IP** protocol Properties


SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 11.0 Configuration (32
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 11.0 Configuration
Enable
Disable
Properties
Help

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

www.hackingarticles.in

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

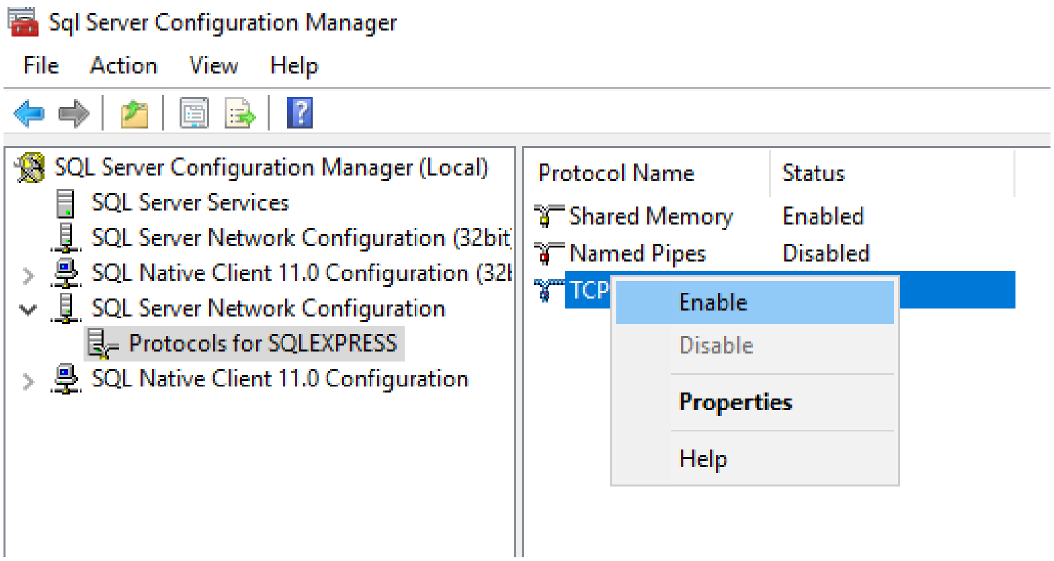


TCP Dynamic Ports	0
TCP Port	
⊟ IP3	
Active	Yes
Enabled	No
IP Address	::1
TCP Dynamic Ports	0
TCP Port	
⊟ IP4	
Active	Yes
Enabled	No
IP Address	127.0.0.1
TCP Dynamic Ports	0
TCP Port	
⊟ IPAll	
TCP Dynamic Ports	0
TCP Port	1433

TCP Port
TCP port

www.hackingarticles.in

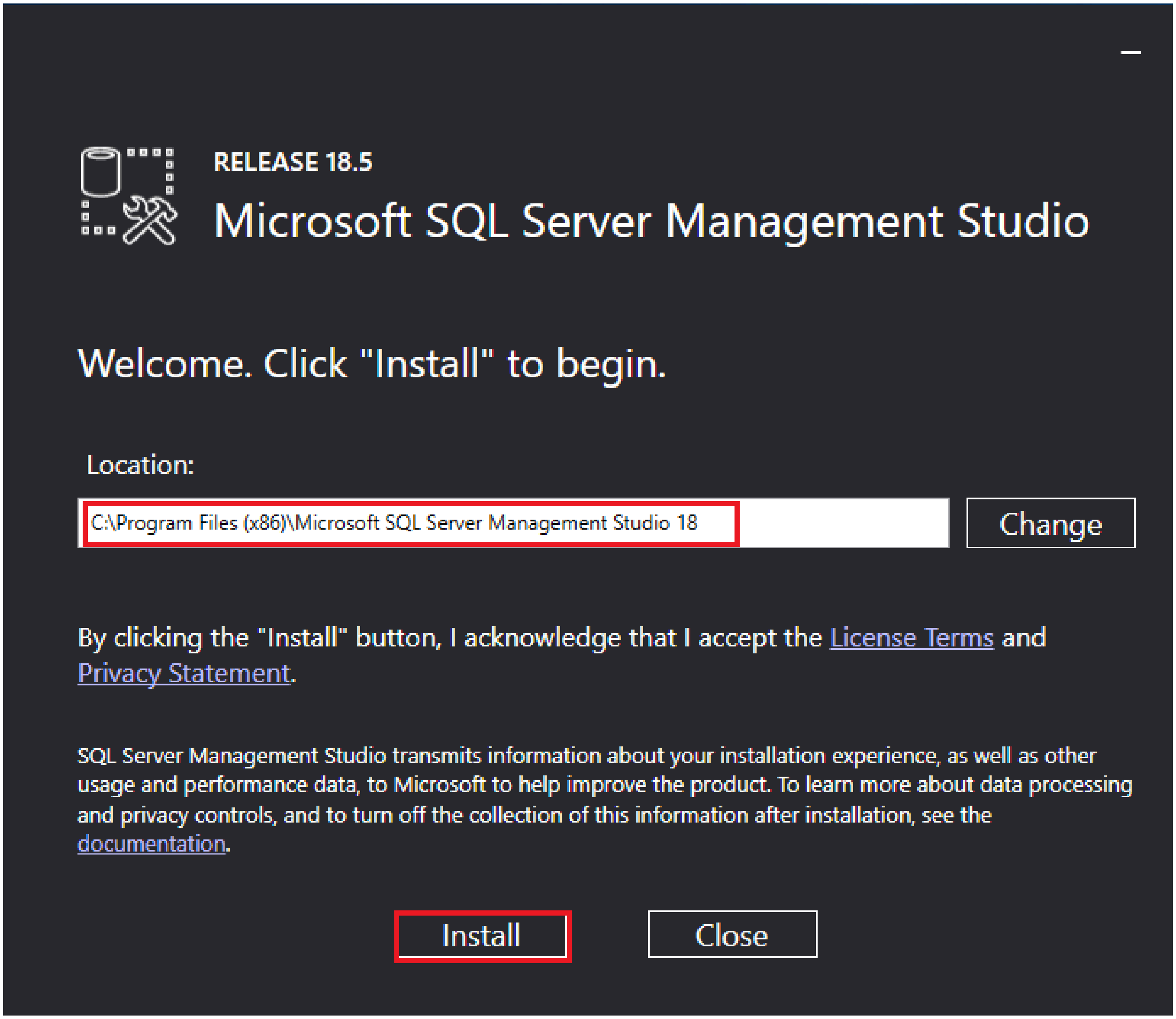
Now you can see, the TCP/IP is enabled as shown in the image.


Sql Server Configuration Manager
File Action View Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 11.0 Configuration (32l
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 11.0 Configuration
Enable
Disable
Properties
Help

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP	

Configure SQL Management Studio setup

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



Welcome. Click "Install" to begin.

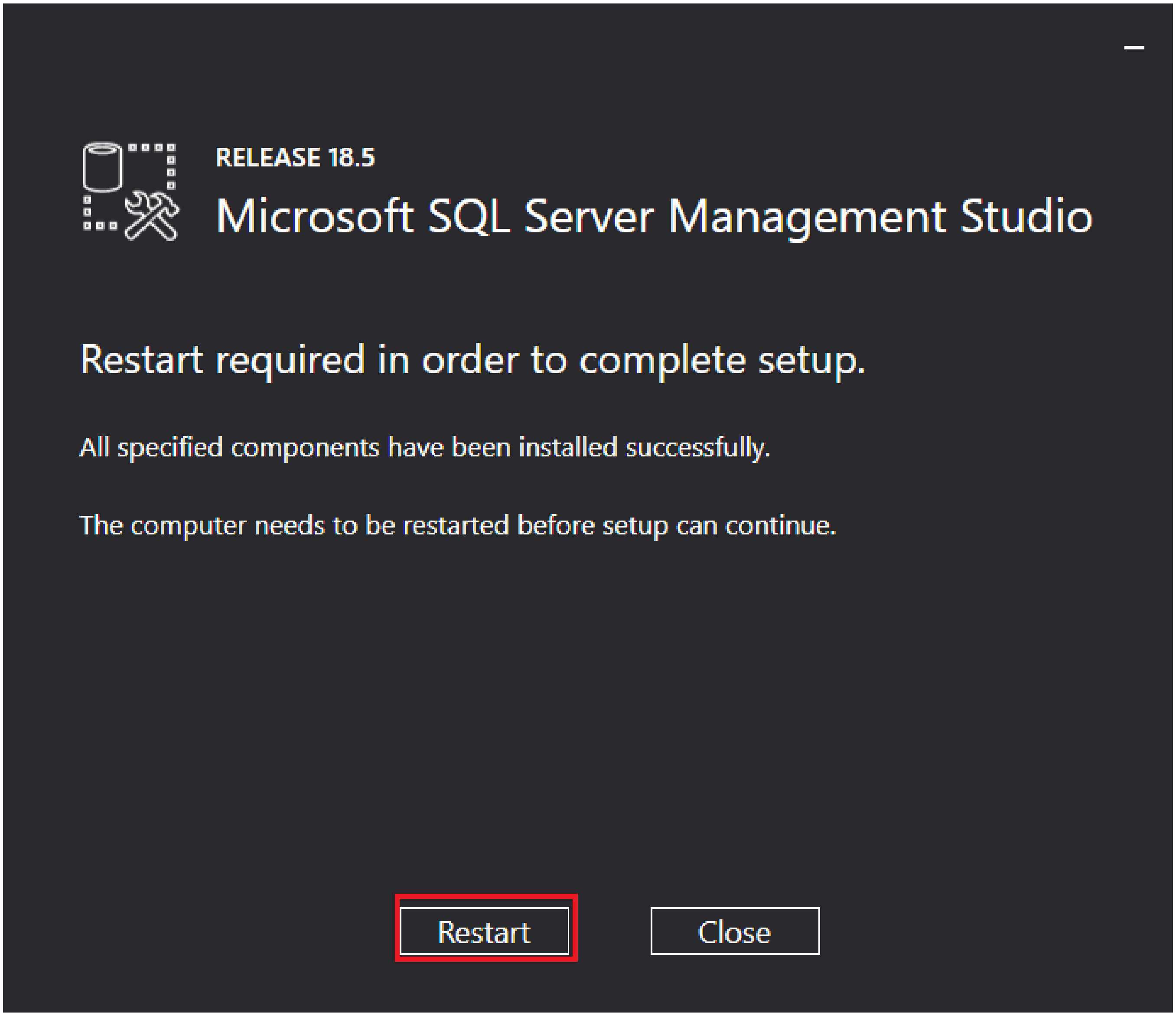
Location:

C:\Program Files (x86)\Microsoft SQL Server Management Studio 18

By clicking the "Install" button, I acknowledge that I accept the License Terms and Privacy Statement.

SQL Server Management Studio transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the documentation.

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



RELEASE 18.5

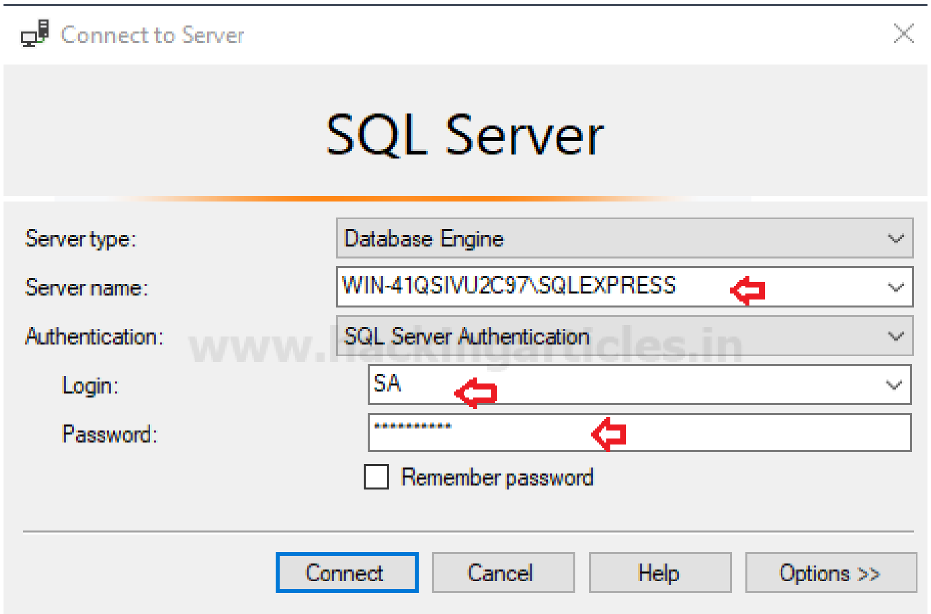
Microsoft SQL Server Management Studio

Restart required in order to complete setup.

All specified components have been installed successfully.

The computer needs to be restarted before setup can continue.

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



Connect to Server

SQL Server

Server type: Database Engine

Server name: WIN-41QSIVU2C97\SQLEXPRESS

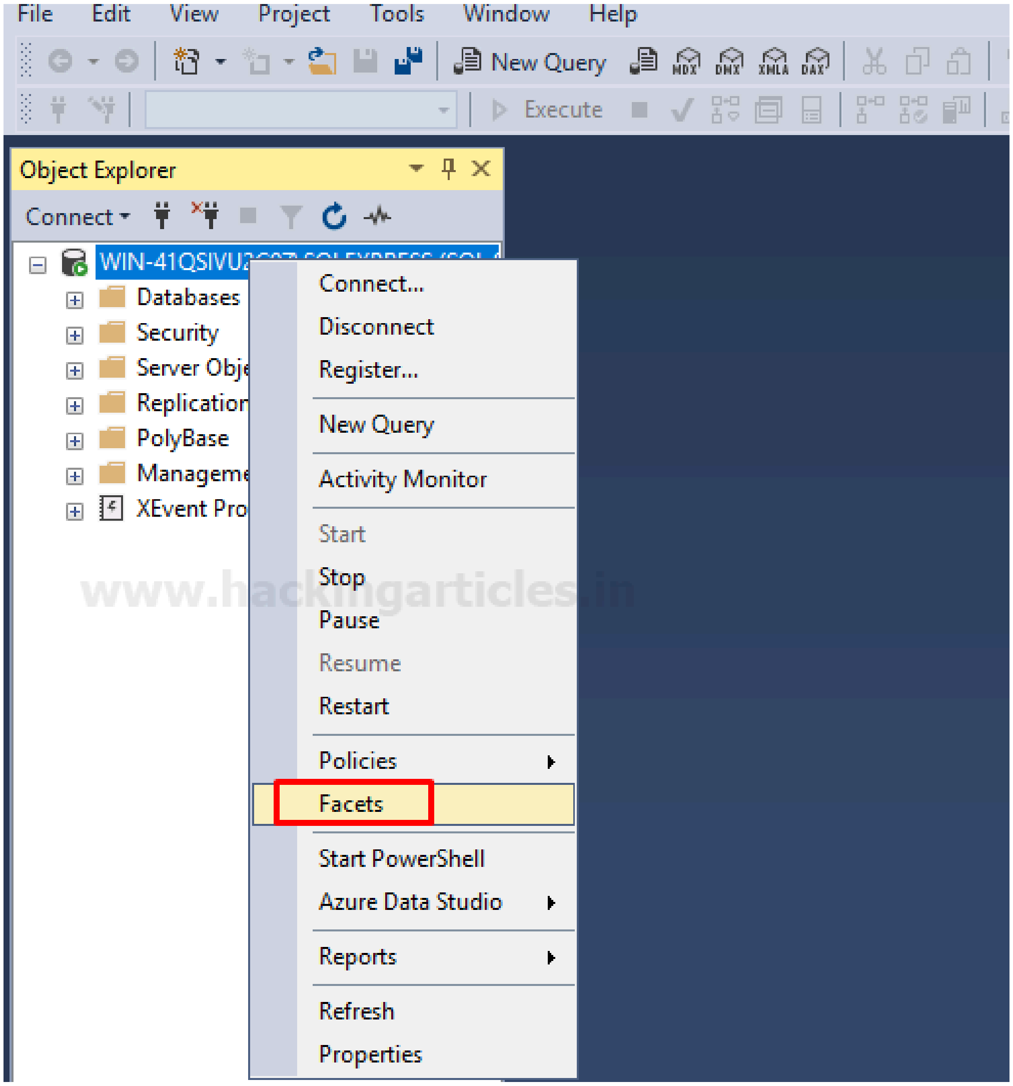
Authentication: SQL Server Authentication

Login: SA

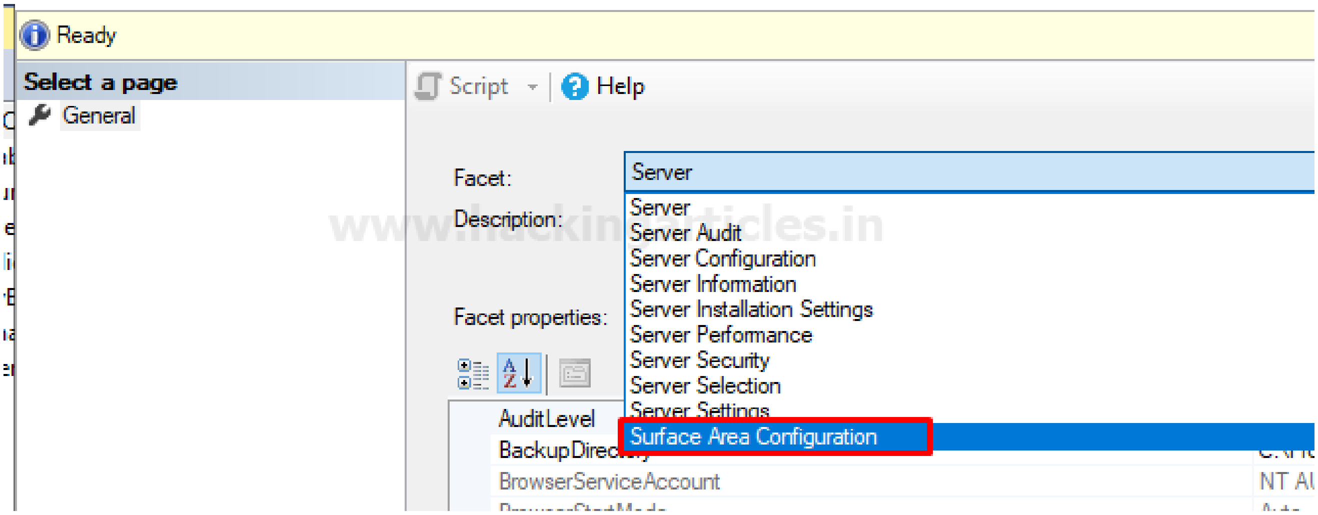
Password: ***********

☐ Remember password

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



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



Facet: Server

Description:

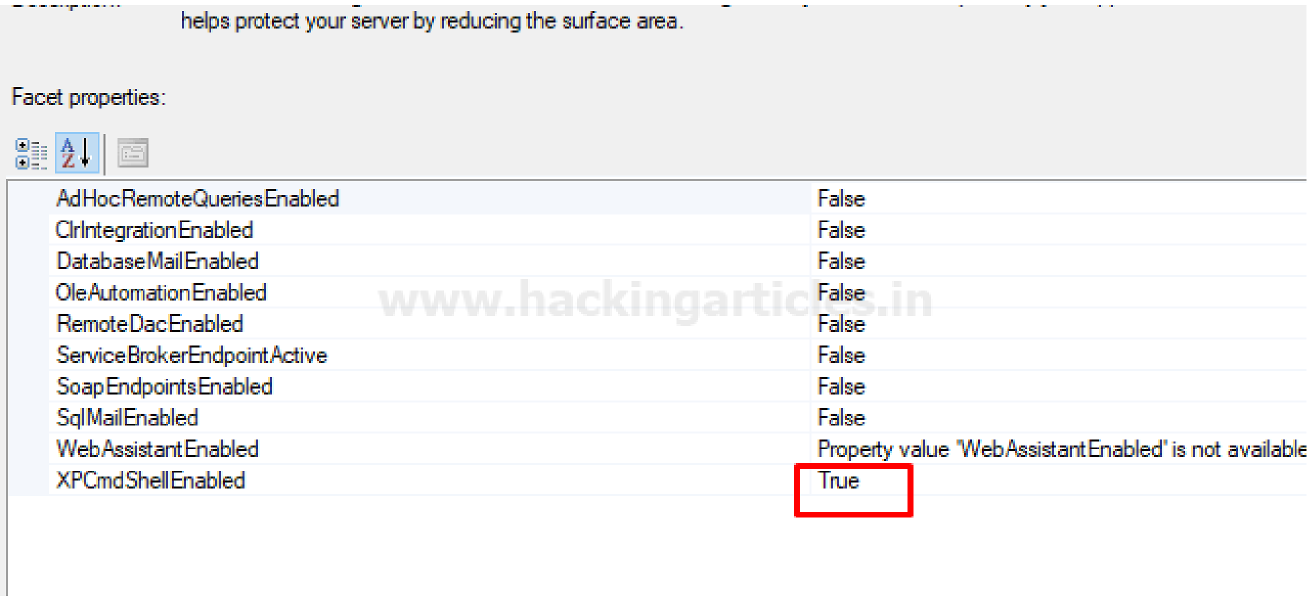
Facet properties:

Server
Server Audit
Server Configuration
Server Information
Server Installation Settings
Server Performance
Server Security
Server Selection
Server Settings
Surface Area Configuration

AuditLevel	
BackupDirec	C:\Pro
BrowserServiceAccount	NT AU

www.hackingarticles.in

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



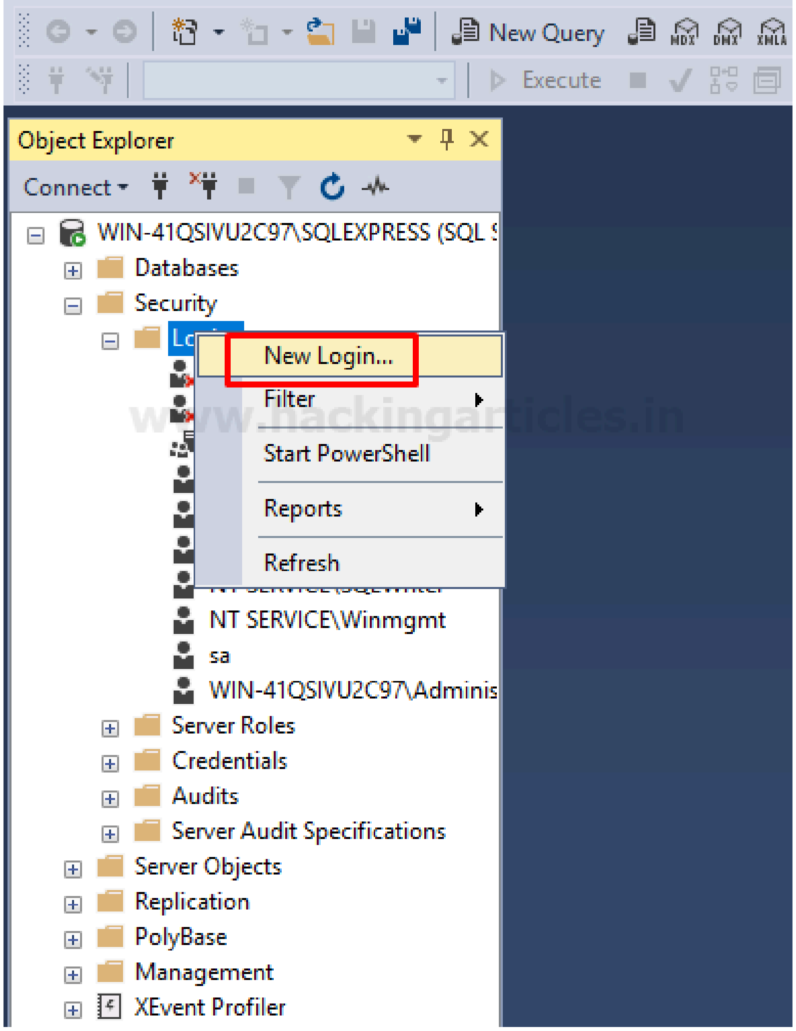
helps protect your server by reducing the surface area.

Facet properties:

AdHocRemoteQueriesEnabled	False
ClrIntegrationEnabled	False
DatabaseMailEnabled	False
OleAutomationEnabled	False
RemoteDacEnabled	False
ServiceBrokerEndpointActive	False
SoapEndpointsEnabled	False
SqlMailEnabled	False
WebAssistantEnabled	Property value 'WebAssistantEnabled' is not available
XPCmdShellEnabled	True

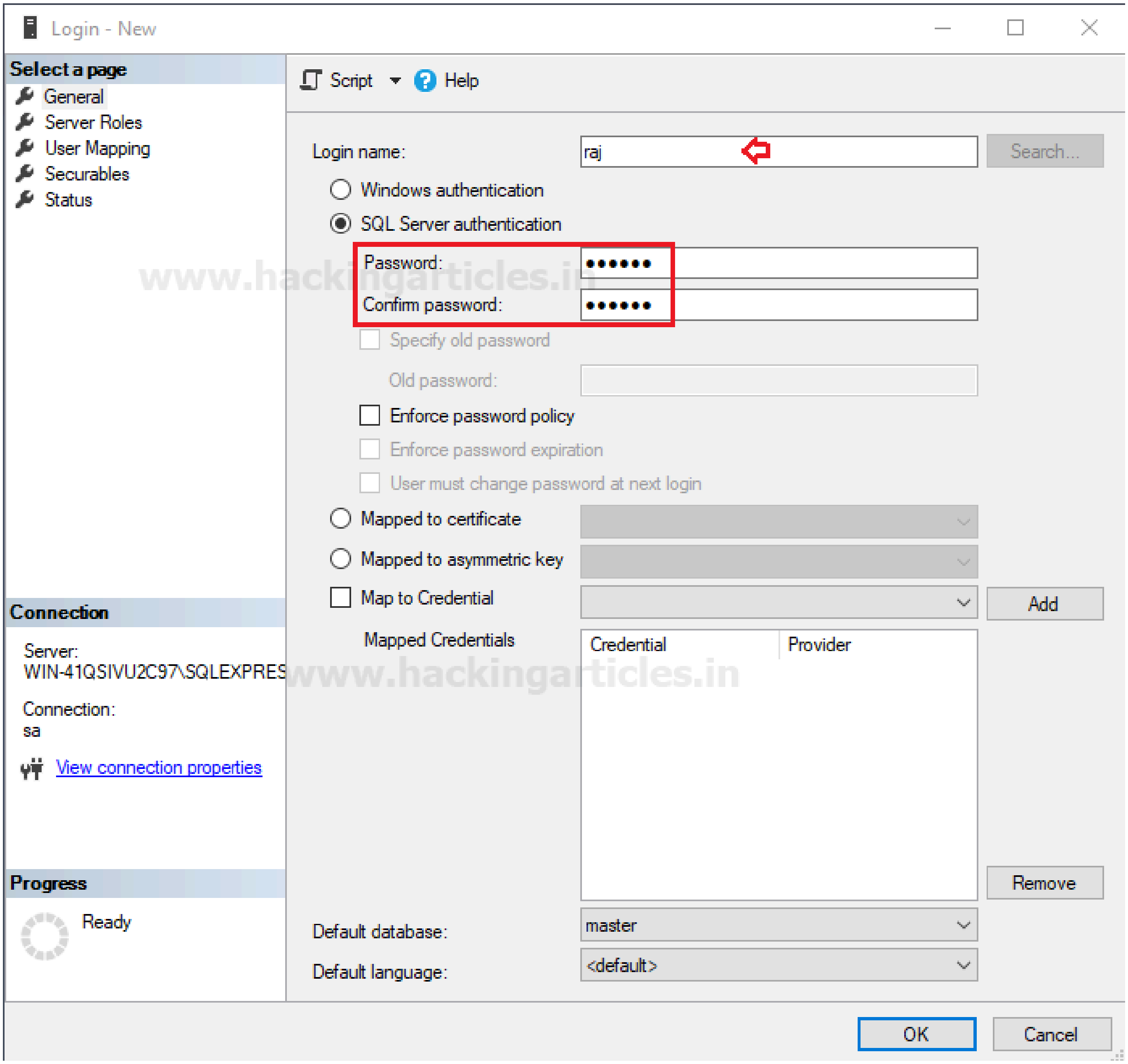
www.hackingarticles.in

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



www.hackingarticles.in

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.



Login name: raj

○ 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

Mapped Credentials

Credential	Provider

Default database: master

Default language: <default>

Connection

Server:
WIN-41QSIVU2C97\SQLEXPRES

Connection:
sa

View connection properties

Progress

Ready

www.hackingarticles.in

Connect to server from windows 10

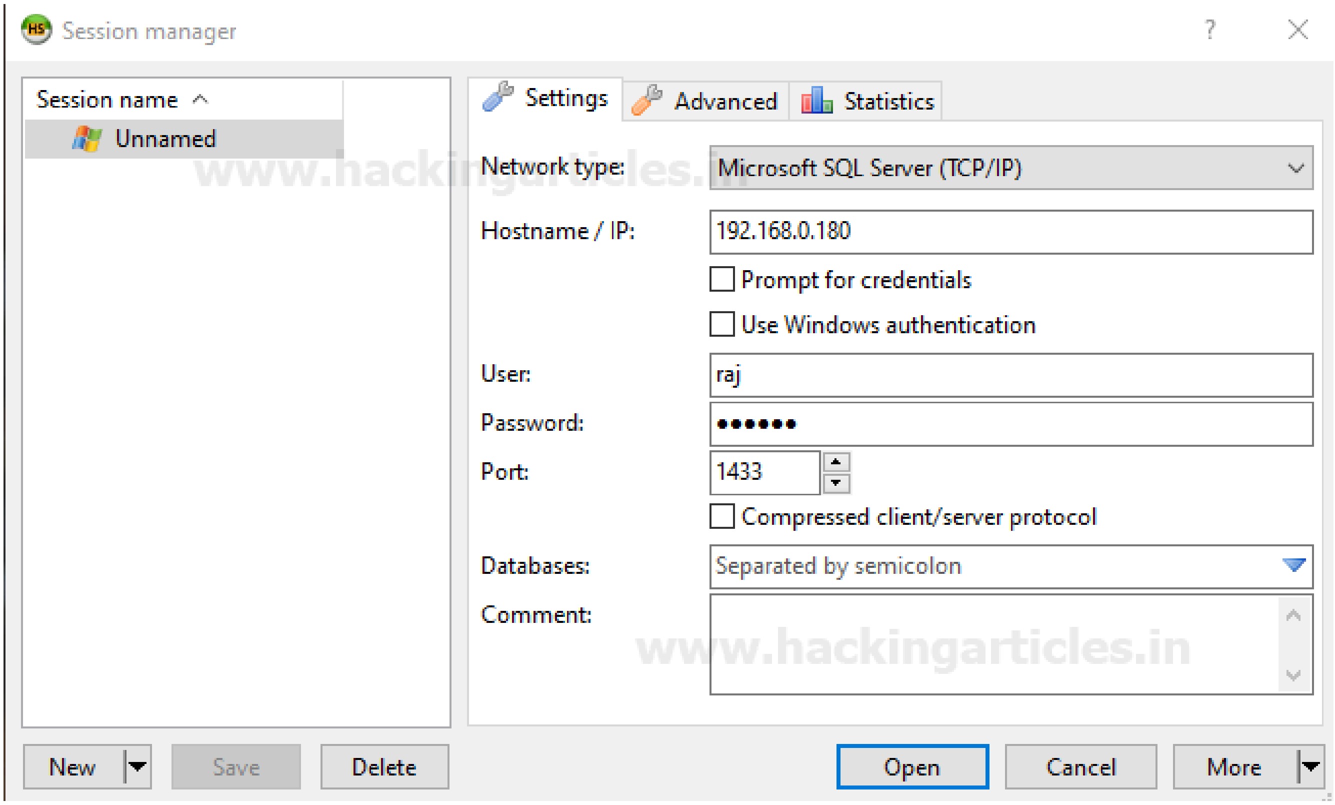
Run **heidisql** tool to connect with MS SQL Server through Raj user as given below:

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**



Network type: Microsoft SQL Server (TCP/IP)

Hostname / IP: 192.168.0.180

□ Prompt for credentials

□ Use Windows authentication

User: raj

Password: ••••••

Port: 1433

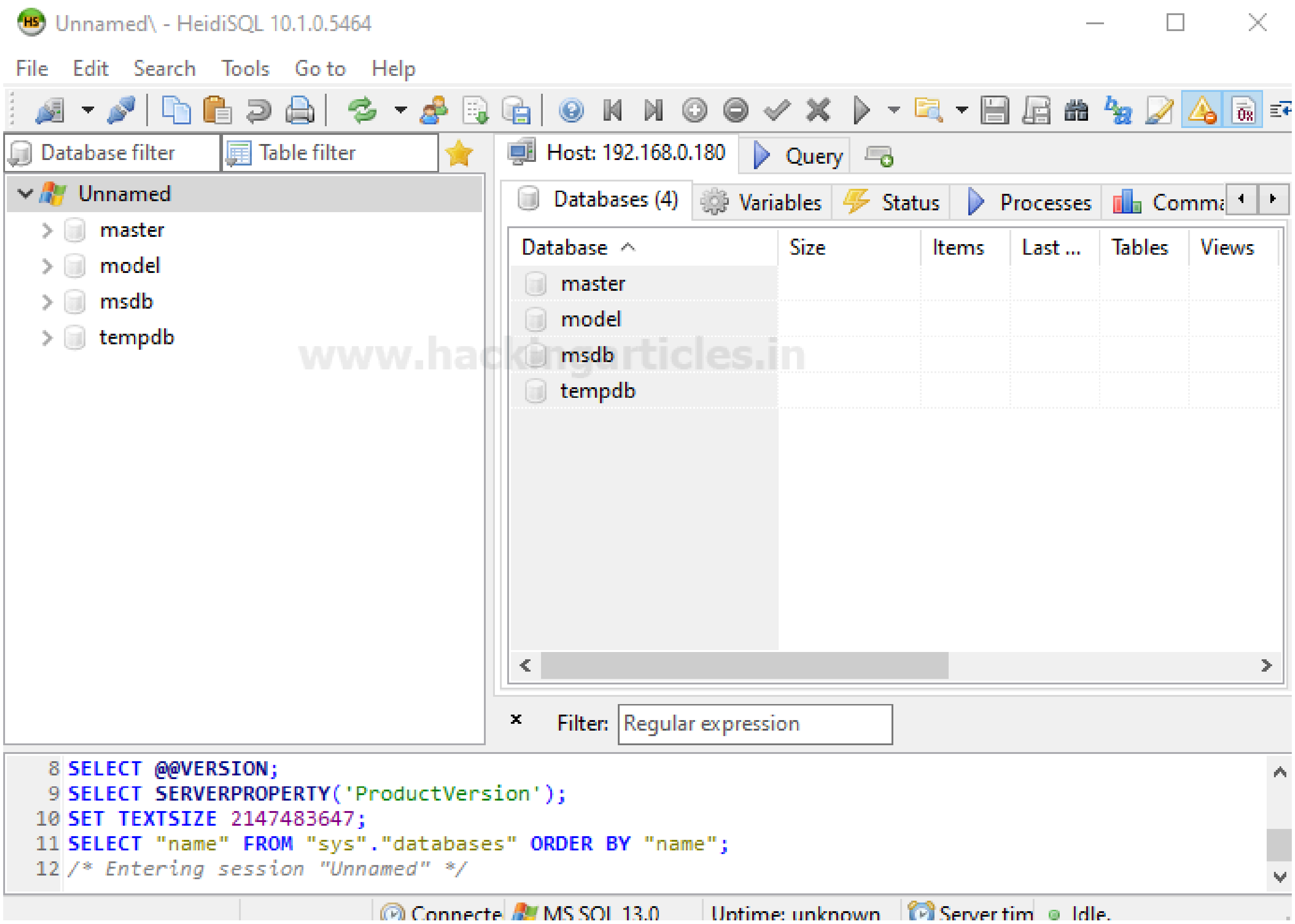
□ Compressed client/server protocol

Databases: Separated by semicolon

Comment:

www.hackingarticles.in

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.



Database	Size	Items	Last ...	Tables	Views
master					
model					
msdb					
tempdb					

```
SELECT @@VERSION;
SELECT SERVERPROPERTY('ProductVersion');
SET TEXTSIZE 2147483647;
SELECT "name" FROM "sys"."databases" ORDER BY "name";
/* Entering session "Unnamed" */
```

www.hackingarticles.in