

UHF_Middleware

Documentation

3/25/2020
Version 1.0R7

This document describes the UHF_Middleware software supplied by GIGA-TMS Inc.

DEMONSTRATION SOFTWARE LICENSE

Please read this agreement carefully before you start to install this demonstration software. If you do not agree please stop the installation of the software.

Software developed by GIGA-TMS Inc is provided "AS IS" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of fitness for a purpose, or the warranty of non-infringement. Without limiting the foregoing GIGA-TMS Inc makes no warranty that:

- The software will meet your requirements.
- The software will be uninterrupted, timely, secure or error-free.
- The results that may be obtained from the use of the software will be effective, accurate or reliable.
- The quality of the software will meet your expectations.
- Any errors in the software obtained from GIGA-TMS Inc will be corrected.

The software and its documentation made available for test or demo purpose.

- could include technical or other errors, GIGA-TMS Inc may make changes to the software or documentation made available to shipped with the conjunction products.
- may be out of date, and GIGA-TMS Inc makes no responsibility to update such materials.

In no event shall GIGA-TMS Inc be liable to you or any third party for any special incidental, indirect or consequential damages of any kind, or any damages whatsoever, including, without limitation, those resulting from loss of use, data or profits, whether or not GIGA-TMS Inc has been advised of the possibility of damage, and on any theory of liability, arising out of or in connection with the use of the software.

The installation of the software is done at your own consideration and risk and with agreement that you will be solely responsibility for any damage to your system or loss of data that results from such activities.

UHF_Middleware User's Manual

UHF_Middleware User's Manual	3
Introduction	4
System Requirements	4
Preparation.....	4
Using UHF_Middleware	5
Configure DB parameters.....	5
Start the service	6
Log Data Table.....	7
Appendix A Sample SQL Schema.....	8
Appendix B Install a database.....	9
Install SQL Server 2019 Express	9
Install SQL Server Management Studio (SSMS)	12
Configure the Database	14
Appendix C Q & A.....	22
Update History.....	23

Introduction

UHF_Middleware helps you to save UHF tags' information which read by TS100 to Database (DB).

System Requirements

UHF_Middleware is a Windows-based program, following is the requirements:

- OS: Windows XP or later version.
- .NET Framework 4.0

Preparation

Before you start to use **UHF_Middleware**, you should set up TS100 with **TS100 Utility** as blow steps.

1. Open **TS100 Utility** (V1.1R2) program.
2. Plug in TS100 to your computer by USB.
3. Click [**Connect**] button to connect with TS100.
4. Select [**General**] tab and set up an Operating Mode.
5. Select [**Hardware**] tab / [**Wi-Fi Settings**] button to configure Wi-Fi settings in order to send tags' information to host via the internet.
6. Select [**Output**] tab:
 - 6.1. Set up [**Data Type**] to make TS100 sends different information to Middleware.
 - 6.1.1. Select "Decoded Data" in general case.
 - 6.1.2. Select "Raw Data" only when you need to retrieve "Remove Tag Event" and "EPC raw data".



- 6.2. Set [**TCP Server Address**] that is the IP and port used for Middleware to listen.

*Tip: When you click [**Start**] button in the **UHF_Middleware**, it shows which IPs & port are listening. (as below)*

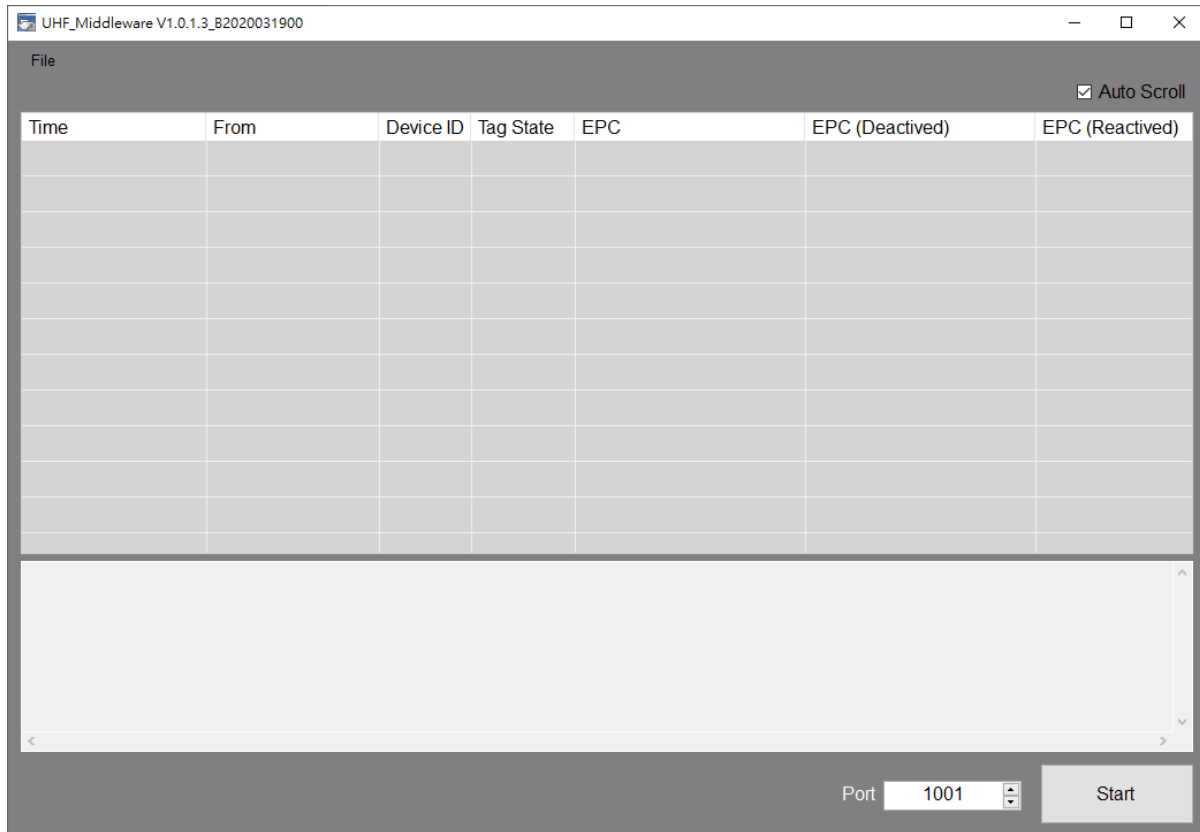


- 6.3. Select [**TCP Server (Wi-Fi)**] to enable TS100 sends data to TCP Server.
7. Click [**Update**] button to save the modifications.
 8. Close **TS100 Utility**.

Now, TS100 is ready to send tag's information to TCP Server via Wi-Fi.

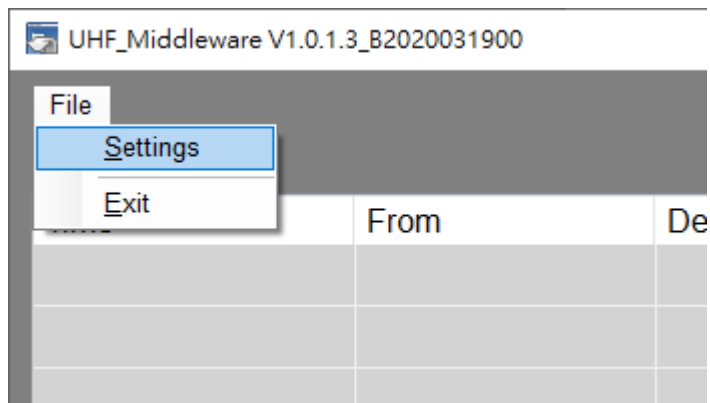
Using UHF_Middleware

Open **UHF_Middleware** (V1.0.1.3) program.



Configure DB parameters

1. Click **[File]** / **[Settings]** in the top left menu.



2. It shows a window as below.

- (1) Select **[Save records to Database]** in order to save data to DB.

- (2) Fill up the **[Target Database]** form.

Then Click **[Test Connection]** button to make sure the settings are correct.

- (3) Click **[↻]** button to update Table Name. And select the target table in the list to store tag data.

- (4) Mapping Table Fields with Log Data:

(4.1) Click empty fields under [**Log Data**] column. It shows a list in the field.

Table Field	Log Data
ID	
DateTime	
DeviceID	DeviceID
DeviceSerialNumber	
TagState	
EPC	

(4.2) Select a Log Data in the list to bind to the table field.

Note: Refer to Log Data Table for more information.

- (5) Select [**Save log to file**] will save logs to local files.
- (6) Select [**Keep alive when closing Middleware**] to make the middleware been running at the background after click [**X**] button.
- (7) Click [**Save**] button to save current settings to registry.
- (8) Click [**Close**] button to close the setting window.

Start the service

1. Click [**Start**] button to start the process of receiving tag data.
2. you could view the received tag data and log:
 - (1) Enable [**Auto Scroll**] to see the latest record in the below grid.
 - (2) The tag data received from TS100 shows in the grid.
 - (2.1) For the records that don't save to DB, the background color is white.
 - (2.2) For the records that have saved to DB, the background is highlight.
 - (2.3) For the records that have occur errors in processing, the background color is red.
 - (3) History log. If you select [**Save log to File**], the log will be saved in the same folder of UHF_Middleware.
 - (4) Click [**Stop**] button to end the process of receiving tag data.

Log Data Table

Name	Type	Description
DateTime	datetime	Time of data retrieved.
FromIPAddress	string	IP address and port of TS100.
DeviceID	string	device id of TS100.
DeviceSerialNumber	string	device serial number of TS100.
TagState	byte	Enable " <i>Remove Tag Event</i> " to retrieve tags removing state. 0: Present, 1: Disappeared
TID	string	TID of the tag.
EPC	string	EPC of the tag. (raw data) * Retrieve the data when <i>Data Type</i> is "Raw Data" or <i>Decoded Data</i> contains "EPC"
DeactivatedEPC	string	Deactivated EPC of the tag. * Retrieve the data when TS100 in " <i>Deactivated Mode</i> ".
ReactivatedEPC	string	Reactivated EPC of the tag. * Retrieve the data when TS100 in " <i>Reactivated Mode</i> ".
DecodedData	string	Decoded data of EPC. * Retrieve the data when <i>Data Type</i> is "Decoded Data".
TagSerialNumber	string	Serial number of UPC encoding. * Retrieve the data when 1. <i>Data Type</i> is "Decoded Data" 2. <i>Decoded Data</i> contains "EAN/UPC" or "EAN/UPC + EAS"
Ascii	string	EPC as ASCII. * Retrieve the data when 1. <i>Data Type</i> is "Decoded Data" 2. <i>Decoded Data</i> contains "ASCII (EPC)"

* The gray rows in the table means that data packets may not exist. It depends on the settings of TS100 and tags' data.

Appendix A Sample SQL Schema

Using below sample schema to create a table for testing.

```
CREATE TABLE [dbo].[TagsInfo](
    [ID] [bigint] IDENTITY(1,1) NOT NULL,
    [DateTime] [datetime] NULL,
    [DeviceID] [varchar](10) NULL,
    [DeviceSerialNumber][varchar](20) NULL,
    [TagState] [tinyint] NULL,
    [EPC] [varchar](50) NULL,
    [DeactivatedEPC] [varchar](50) NULL,
    [ReactivatedEPC] [varchar](50) NULL,
    [TID] [varchar](50) NULL,
    [DataSource] [varchar](21) NULL,
    [DecodedData] [varchar](256) NULL,
    [TagSerialNumber] [varchar](10) NULL,
    CONSTRAINT [PK_TagsInfo] PRIMARY KEY CLUSTERED
(
    [ID] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
    ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
```

In the UHF_Middleware, set data binding as below.

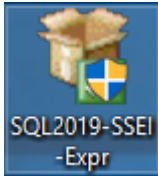
Appendix B Install a database

Following below steps to install a database for testing.

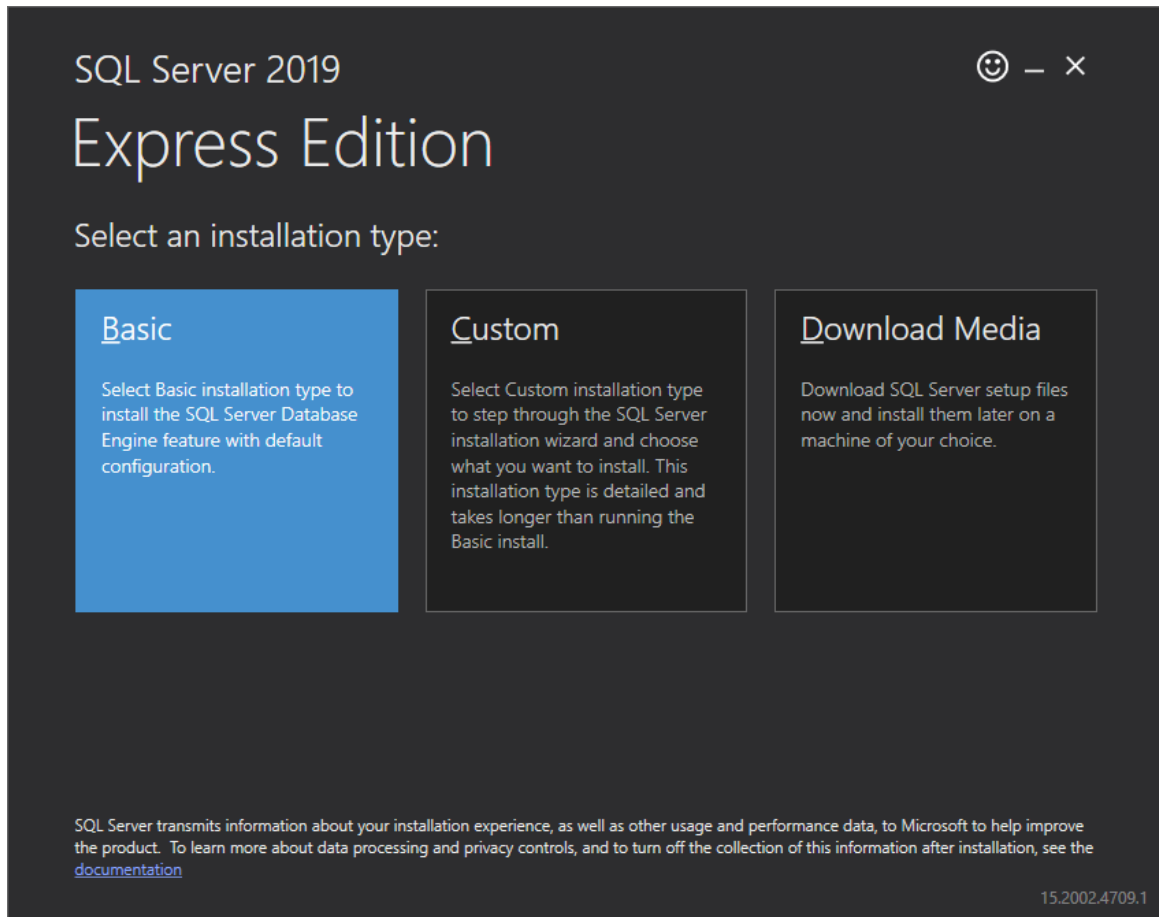
Install SQL Server 2019 Express

1. Download SQL Server 2019 Express.
<https://go.microsoft.com/fwlink/?linkid=866658>

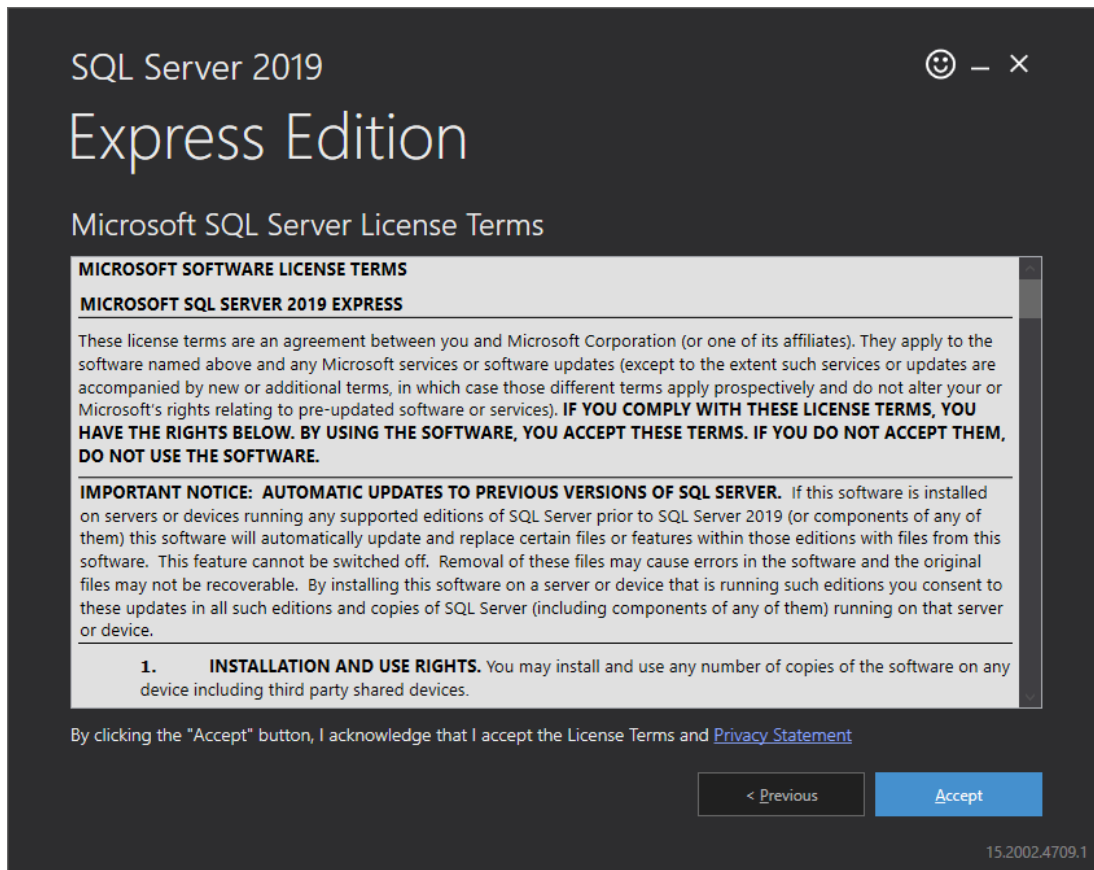
2. Execute the installer.



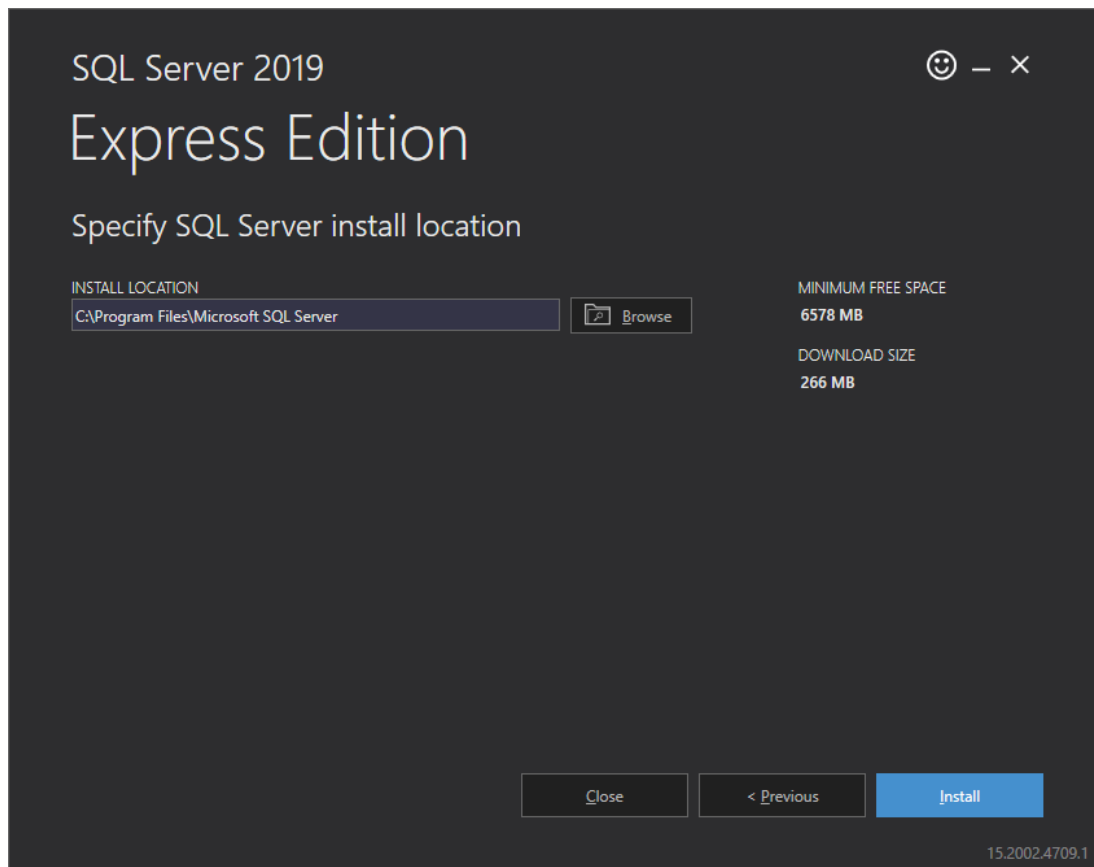
3. Select [Basic] option.



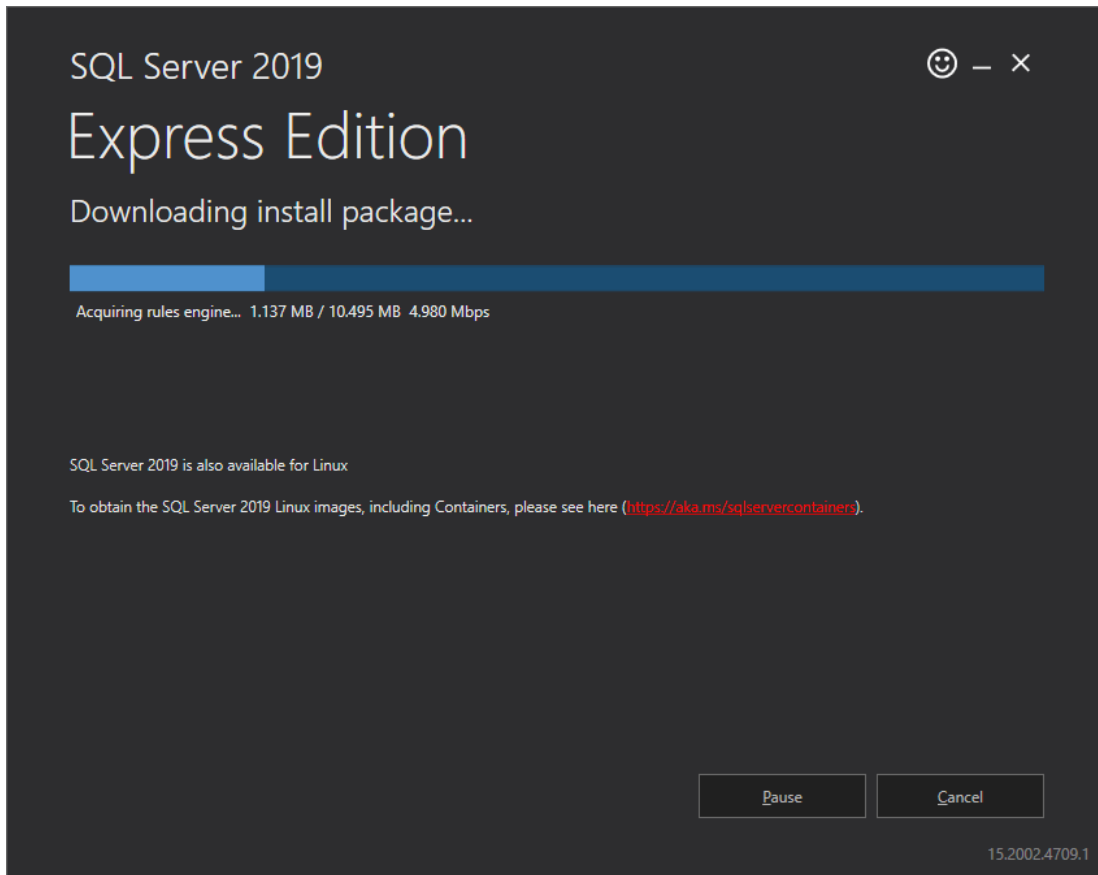
4. Click [Accept] button.



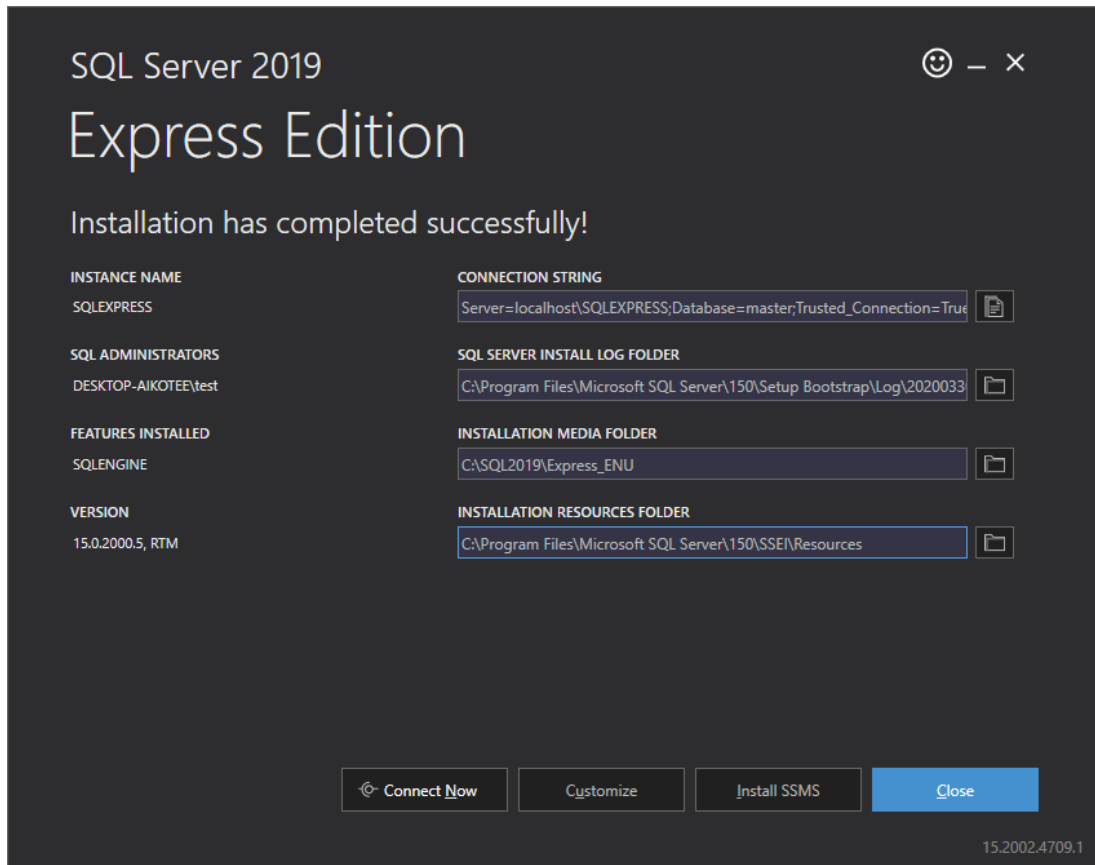
5. Click [Install] button.



6. Wait for installing.

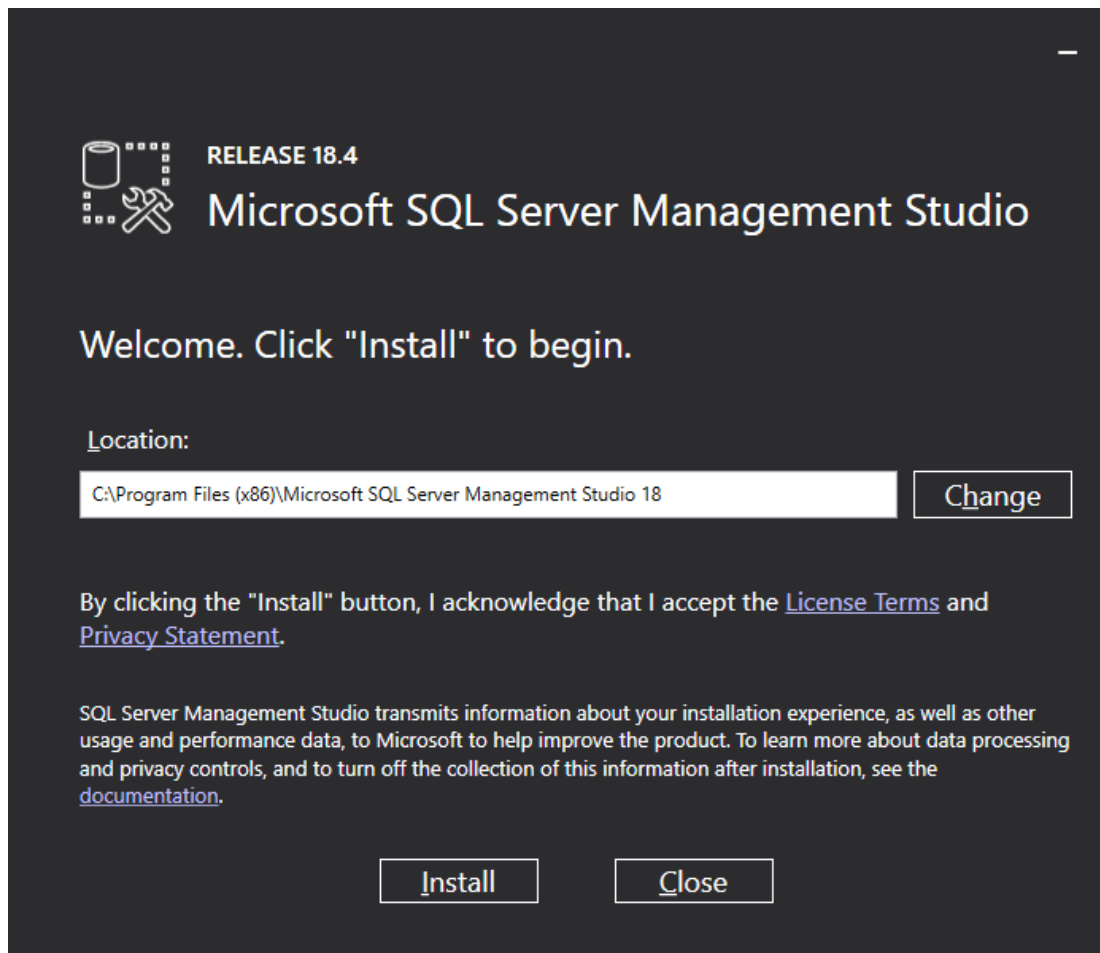


7. Click [**Close**] button.

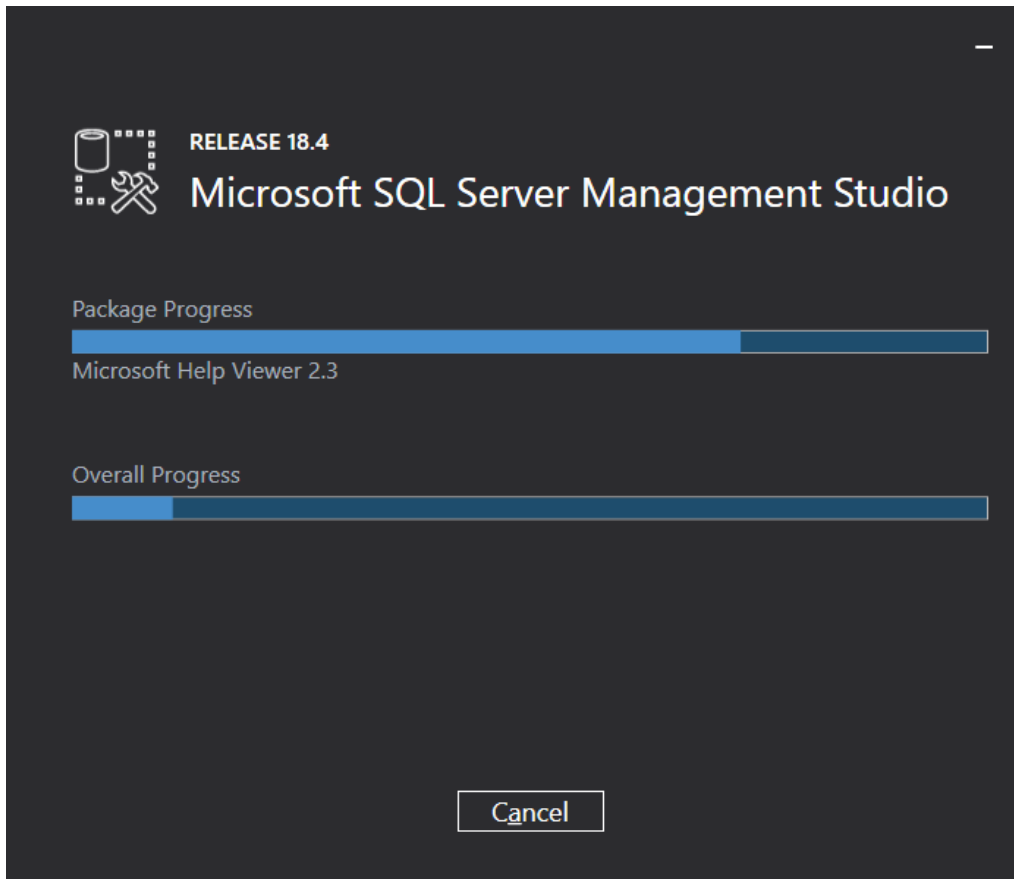


Install SQL Server Management Studio (SSMS)

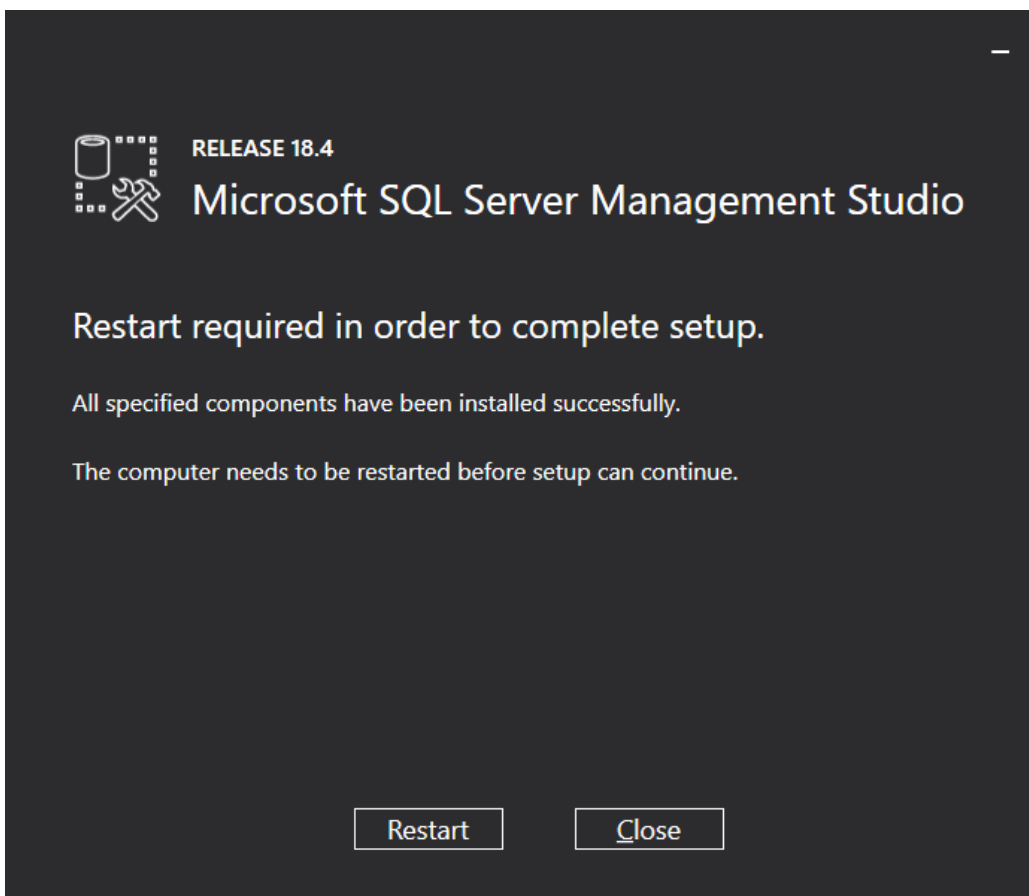
1. Download SQL Server Management Studio (SSMS)
<https://aka.ms/ssmsfullsetup>
2. Execute the installer. Click [**Install**] button.



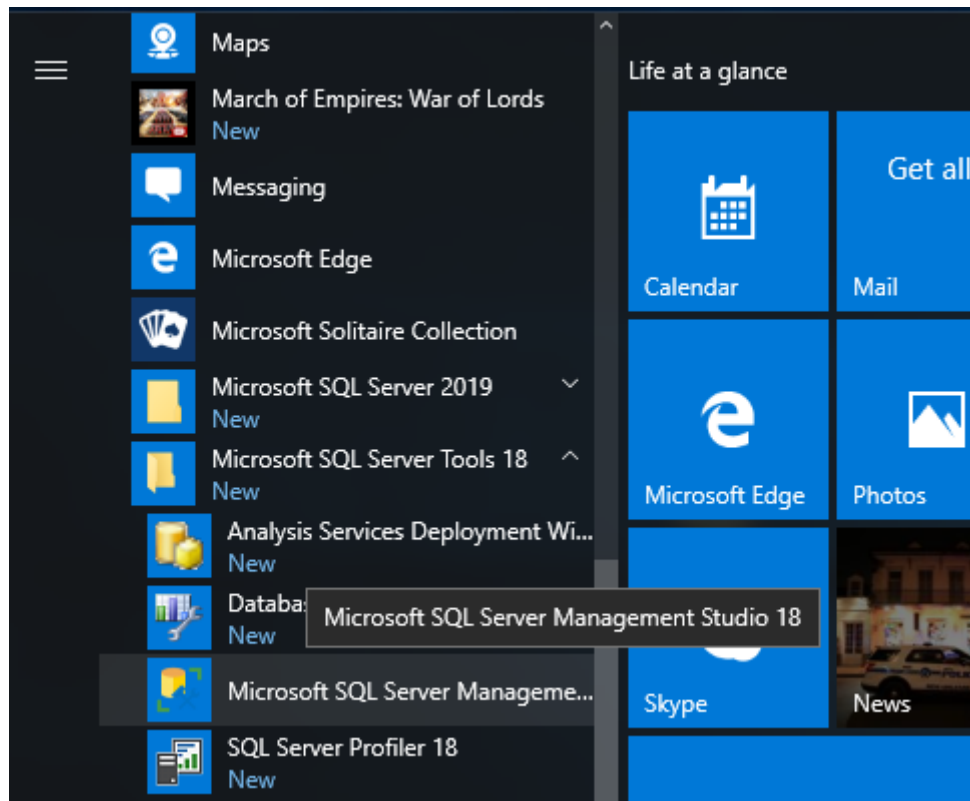
3. Wait for installing.



4. Click [**Restart**] button to restart your PC.



5. Execute SSMS.

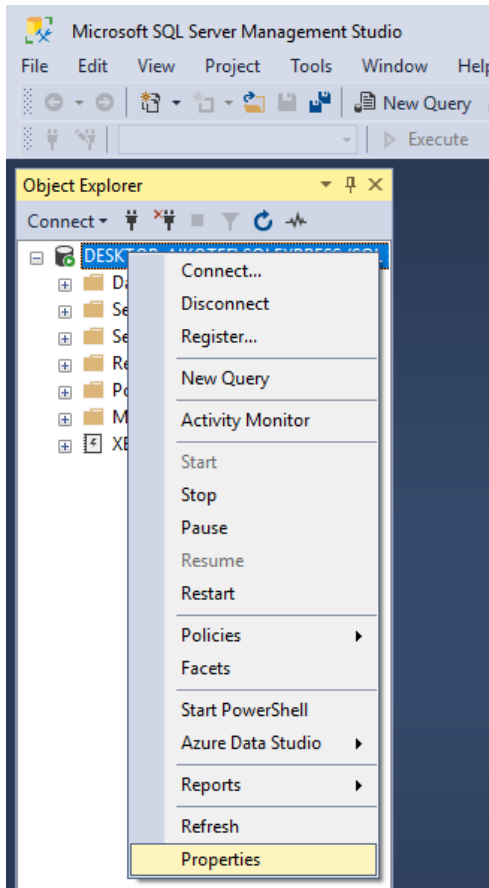


6. Click [**Connect**] button.

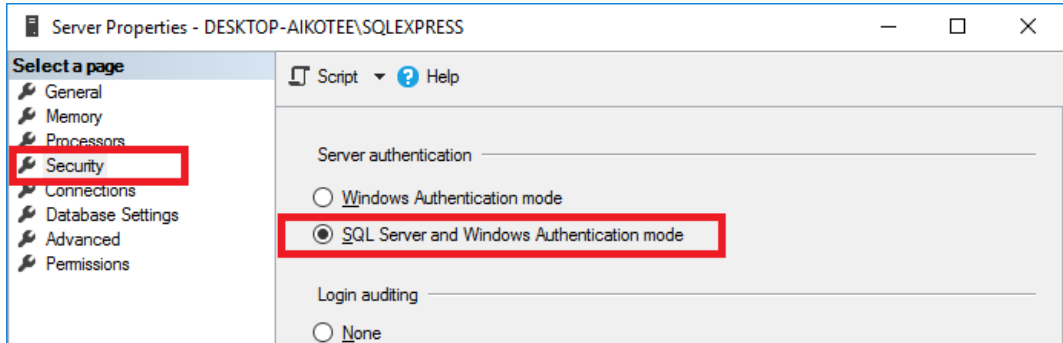
Configure the Database

1. Change authentication mode with SSMS.

1.1 Right click on [**Object Explorer**] / Database Node. Click [**Properties**] on pop-up menu.



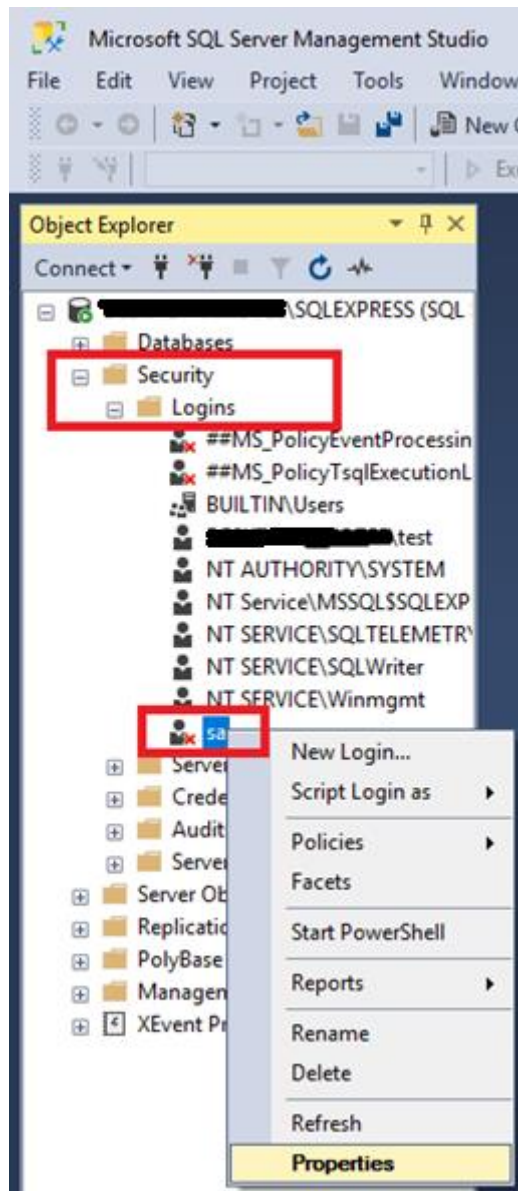
1.2. Select [Security] page and select [SQL Server and Windows Authentication mode]



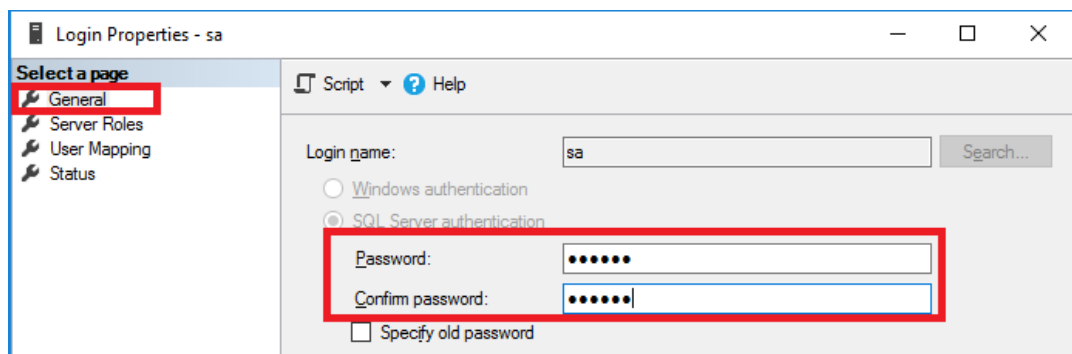
1.3. Click [OK] button.

2. Enable sa login

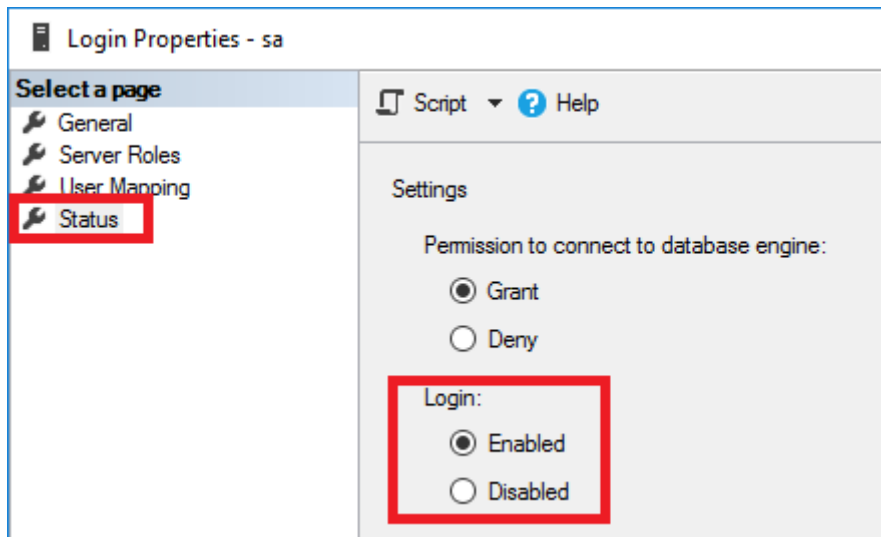
2.1. Expand [Object Explorer] / [Security] / [Logins], right click [sa], and click [Properties] on pop-up menu.



2.2. Set Password for the account sa in [General] page.



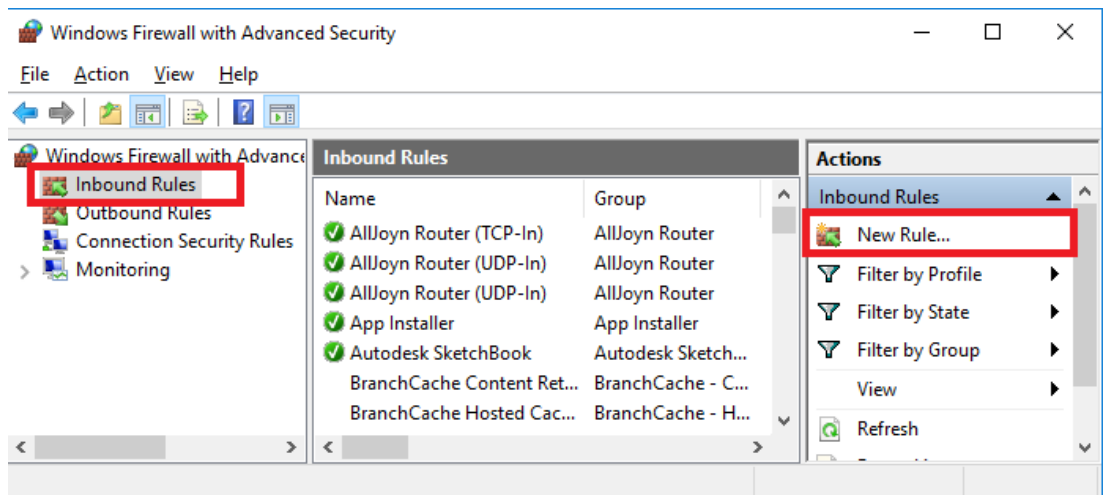
2.3. Set Login to [Enable] in [Status] page.



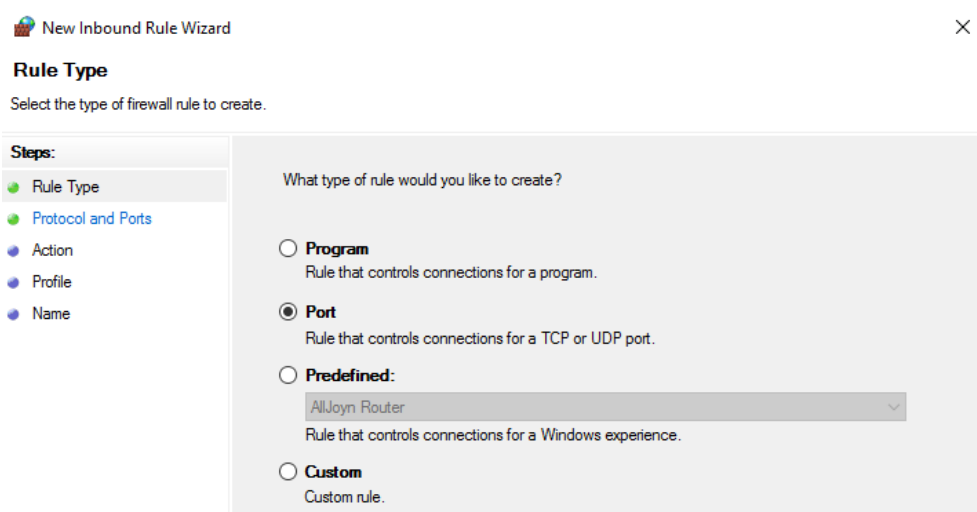
2.4. Click [OK] button.

3. Allow 1433 port through the firewall.

3.1. Execute [WF.msc]. Click [New Rule] in [Inbound Rules] page.



3.2. Select [Port] option. Then click [Next] button.



3.3. Select [Specific local ports] and enter **1433**. Then click [Next] button.

Steps:

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

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

3.4. Click **[Next]** button.

Steps:

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

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

3.5. Click **[Next]** button.

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.

3.6. Enter the rule name. Then click **[Finish]** button.

Steps:

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

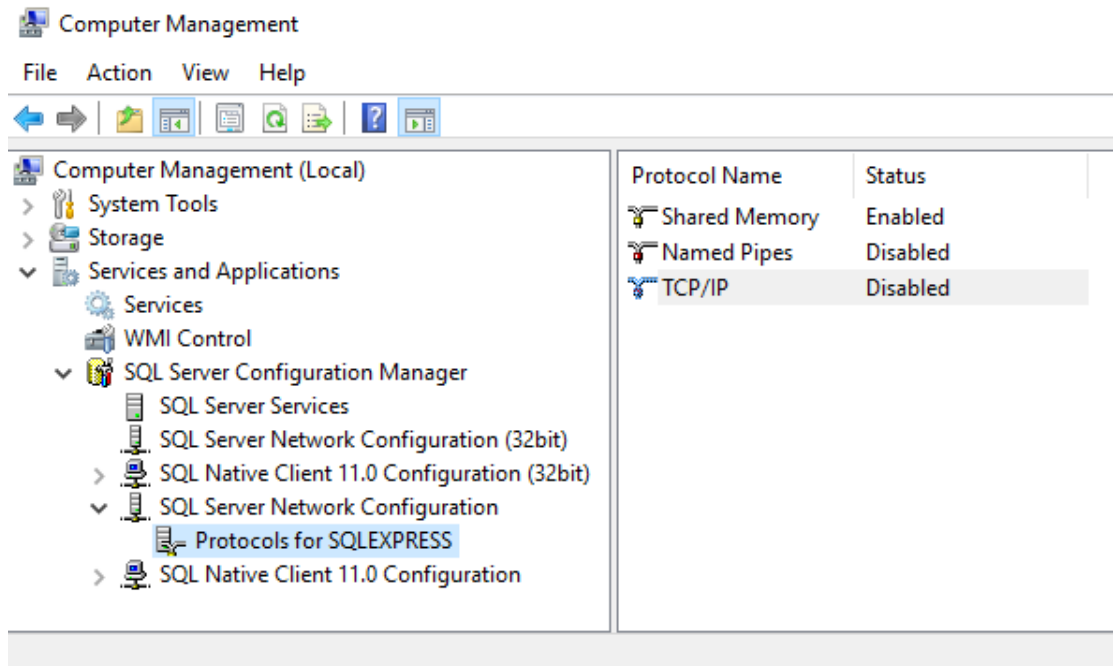
Name:

Description (optional):

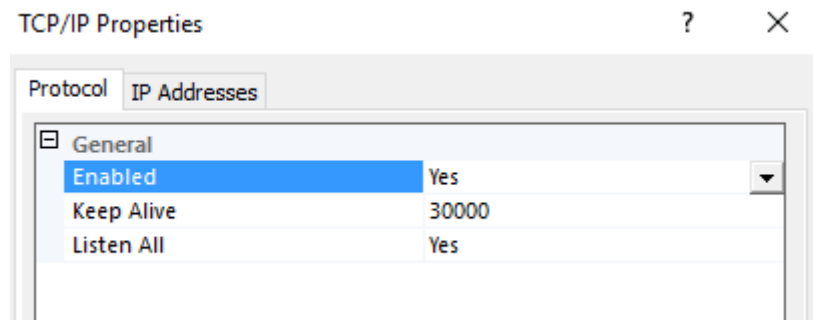
4. Enable SQL Server TCP/IP connection.

4.1. Open [Computer Management].

4.2. Select [Services and Applications] / [SQL Server Configuration Manager] / [SQL Server Network Configuration] / [Protocols for SQLEXPRESS]



4.3. Double click [TCP/IP] item. Set [Enabled] item to [Yes] in [Protocol] page.



4.4. In [IP Addresses] page:

4.4.1. Enter **1433** at [TCP Port]

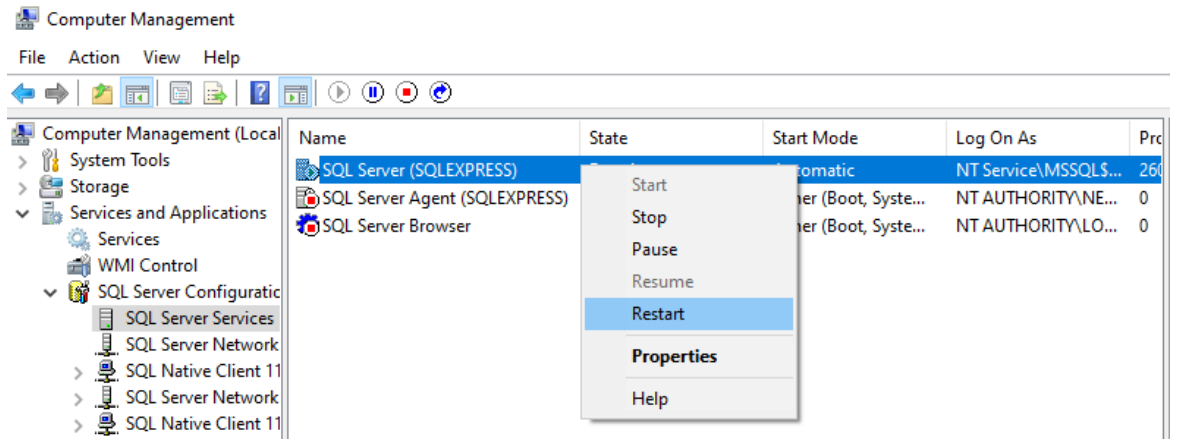
4.4.2. Set [Enabled] to [Yes]

4.4.3. Clear [TCP Dynamic Ports] value

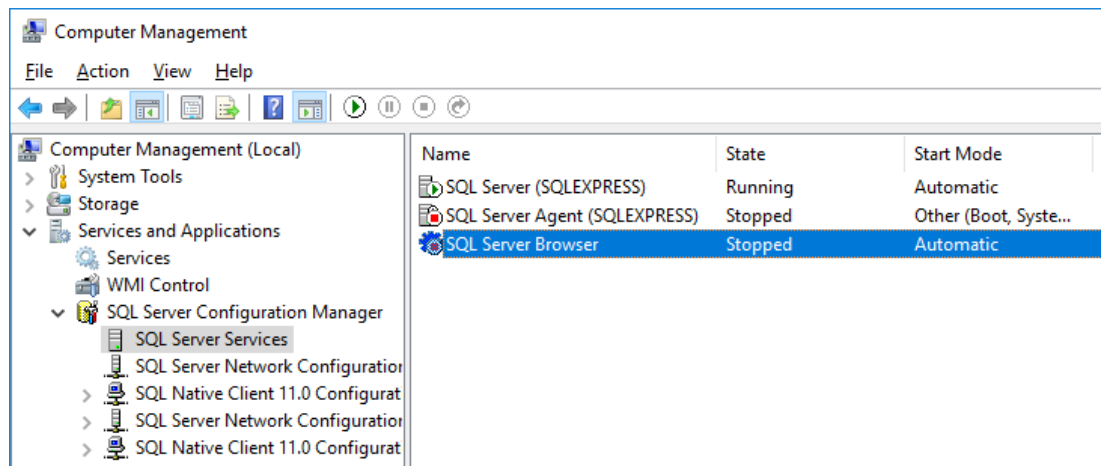
4.4. Then click [OK] button.

4.5. Select [SQL Server Services] item.

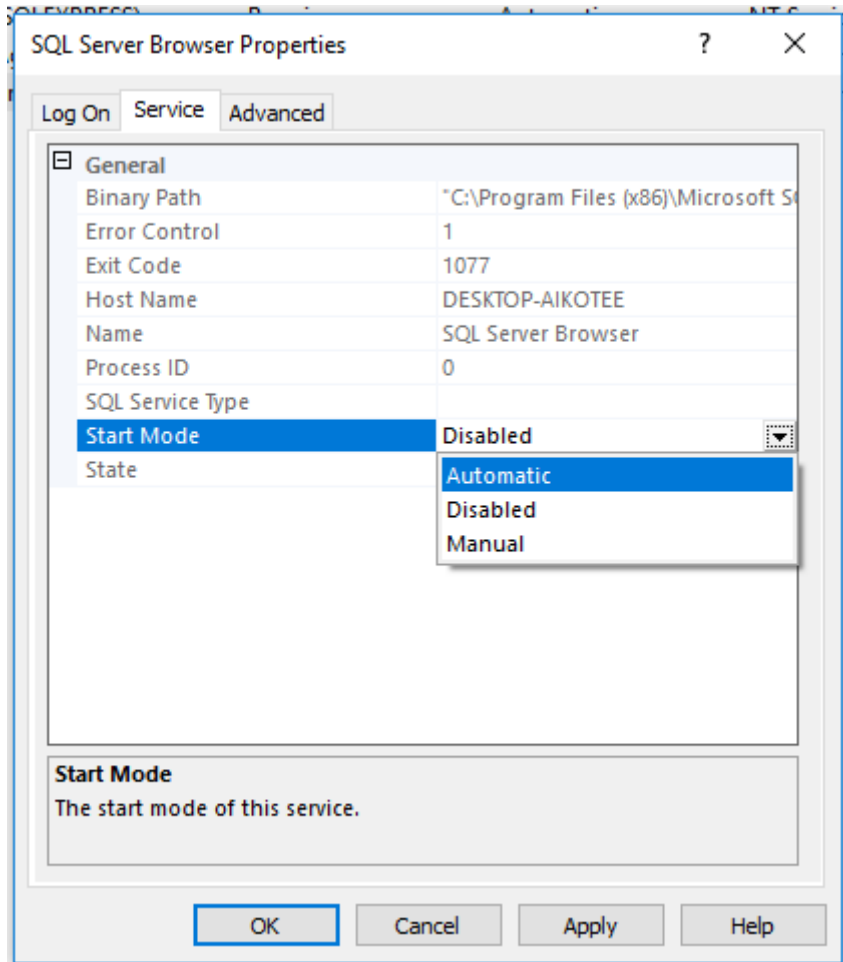
Right click [SQL Server (SQLEXPRESS)] and click [Restart] to apply new settings.



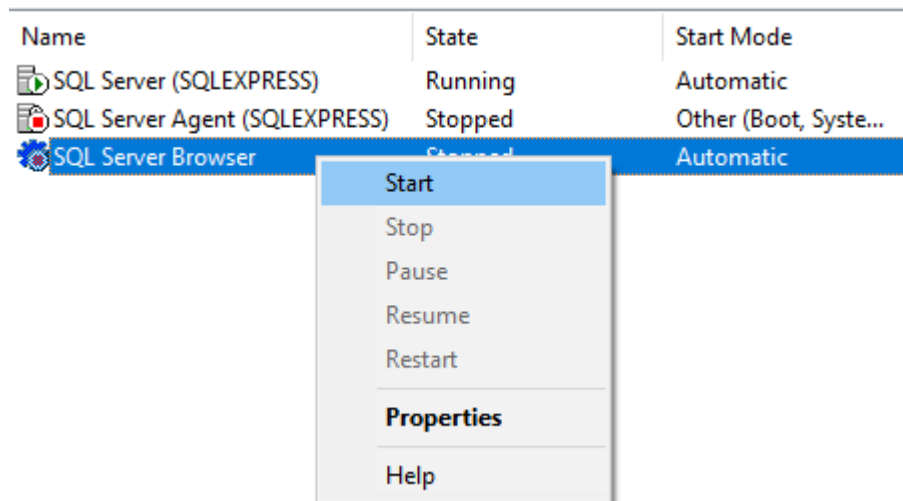
4.6. Double click [SQL Server Browser].



4.7. In [Service] page, change [Start Mode] to [Automatic]. Then click [OK] button.



4.8. Right click [SQL Server Browser] item and click [Start].



Appendix C Q & A

Q1. How to clear the tag data records and log message showing in the UI?

A1.

1. Right-click the list, in the drop-down menu, click to select **[Clear]**. (If there is any unsaved record, then they cannot be clear.)
2. Double-click the Log text box to clear log message.
3. The log message will also be automatically clear if the record count reach to 2000.

Q2. How to re-save the record to DB?

A2. Select one or more than one records, right-click the list view, in the drop-down menu, click **[Resend]**.

Time	From	Device ID	EPC	EPC (Deactivated)	EPC (Reactivated)	TID	Decoded Type	Decoded String	Saved
2019/05/24 17:30:47	192.168.100.58:23163	FF	AAAA1234560000000000...			E28011002000575A240601AA	TagData		V
2019/05/24 17:30:47	192.168.100.58:23163	FF	AAAA1234560000000000...			E28011002000575A240601AA	TagData		V
2019/05/24 17:30:47	192.168.100.58:47264	FF	00007D0000000000000000...			E280110020003B1393EB015B	TagData		V
2019/05/24 17:30:48	192.168.100.58:47264	FF	00007D0000000000000000...			E28011002000594E239601AA	TagData		V
2019/05/24 17:30:48	192.168.100.58:47264	FF	00007D0000000000000000...			E28011002000594E239601AA	TagData		V
2019/05/24 17:30:48	192.168.100.58:47264	FF				E20034120137FFB000C32762A141D01...	EAN_UPC	049886185099...	V
2019/05/24 17:30:48	192.168.100.58:47264	FF	00007D0000000000000000...			E280110020005101228801AA	TagData		V
2019/05/24 17:30:48	192.168.100.58:47264	FF	00007D0000000000000000...			E280110020005101228801AA	TagData		V
2019/05/24 17:30:48	192.168.100.58:47264	FF	00007D0000000000000000...			E280110020005B1A260501AA	TagData		V
2019/05/24 17:30:48	192.168.100.58:47264	FF	00007D0000000000000000...			E280110020005B1A260501AA	TagData		V
2019/05/24 17:30:49	192.168.100.58:47264	FF	00007D0000000000000000...			E28011002000568E23D101AA	TagData		V

Resend
Clear

Update History

25MAR2020 release

- Version 1.0R7
- Update Using UHF_Middleware.

04Dec2019 release

- Version 1.0R6
- Update Sample SQL Schema.

22Nov2019 release

- Version 1.0R5
- Update Sample SQL Schema.
- Update Log Data Table.

16AUG2019 release

- Version 1.0R4
- Update Sample SQL Schema.
- Update the content according to UHF_Middleware (V1.1R1).
- Add Log Data Table.

2JUL2019 release

- Version 1.0R3
- Update Sample SQL Schema

11JUN2019 release

- Version 1.0R2
- Add Sample SQL Schema

3JUN2019 release

- Version 1.0R1