Cortex Integrity SQL Server 2019 Installation Guide

Cortex Limited
Kings Park House,
22 Kings Park Road,
Southampton,
SO15 2AT

T +44 23 8254 8990
E **info@cortex-ia.com**

Status: Release
Release Date: 11/03/2022
Author: Cortex Product Development
Document Version: 1.0.5
Software Version: 15.0.X

Contents

Preface

About this Manual

Cortex Evolution is comprised of two engines: Cortex Integrity and Cortex Innovation. This document is intended for Cortex Integrity only. Please see **https://v2022.docs.cortex-ia.com/docs/** for Cortex Innovation.

This document provides detailed information regarding the installation of SQL Server 2019 for Cortex Integrity solutions.

This manual is organised into the following main sections:

- **Pre-requisites** – This section details necessary system configuration and third-party components for this software installation.

- **Attended Installation** – This section provides information on the installation of SQL Server via the user interface.

Audience

The intended audience is anyone required to install a SQL Server 2019 instance for use with Cortex Integrity solutions.

Related Material

Other documents related to this installation guide are as follows:

- Cortex Integrity - Installation Guide
- Cortex Integrity - Database Installation Guide

For further information, please also consult the following document:

- **Install SQL Server 2019 from the Installation Wizard (Setup)**

Abbreviations used in this Document

SQL   - Structured Query Language
TLS   - Transport Layer Security

Revisions to this Document

The following revisions have been made to this document:

Date	Author	Revision	Notes
18/02/2021	D. Smith	1.0.0	Final.
14/07/2021	D. Smith	1.0.1	Removed requirement for mixed mode authentication on dual site environments.
08/10/2021	S. Rudawski	1.0.2	Corrected Figure 16 - Analysis Services Configuration screenshot and incorrect paths to Reporter Server installation folder.
09/12/2021	J. Briers J. Black	1.0.3	Added steps to add 'DisableLoopBackCheck' registry entry. Added cumulative updates section.
20/01/2022	D. Smith	1.0.4	Added Steps to configure SQL Server to use TLS
08/03/2022	D. Smith	1.0.5	Modified title to reflect the document relates to Integrity systems, added a disclaimer that the document is for Integrity only and made modifications following release testing

1   Pre-requisites

1.1 System requirements

Component	Supported versions
Operating System	Windows Server 2019 (x64) Standard
	Windows Server 2019 (x64) Datacentre
SQL Server	2019 (x64) Product Version 15.0.x

1.2 Required service user account (within Database server setup)

The service user account that will run the SQL Server services should have been created and configured as per the Database server setup in the "Cortex Installation Guide". For deployment of the Cortex system it is required that all the SQL Server services use the same account except for the SQL Server Browser Service which runs as Local System. An example username is shown below:

- SQL Server Service   (Example: Cortex_SqlAdmin)
- SQL Server Agent Service   (Example: Cortex_SqlAdmin)
- SQL Server Analysis Services Service   (Example: Cortex_SqlAdmin)
- SQL Server Integration Services Service   (Example: Cortex_SqlAdmin)
- SQL Server Reporting Services Service   (Example: Cortex_SqlAdmin)

  ⚑ SQL Server 2019 cannot be installed using the built in Administrator account. A different user must be used.

1.3 Additional pre-requisites

  ⚑ The install must be executed from the machine that the software will be installed on.
  ⚑ The user that executes the install must have local admin rights on the machine and must be a domain user if the machine is on a domain.
  ⚑ The SQL Server install media must be available and visible to the local machine.

2   Attended Installation

2.1 Installation of SQL Server

1. Run the SQL Server installer. When the installer loads you will be presented with the SQL Server Installation Center as shown in Figure 1 - SQL Server Installation Center.
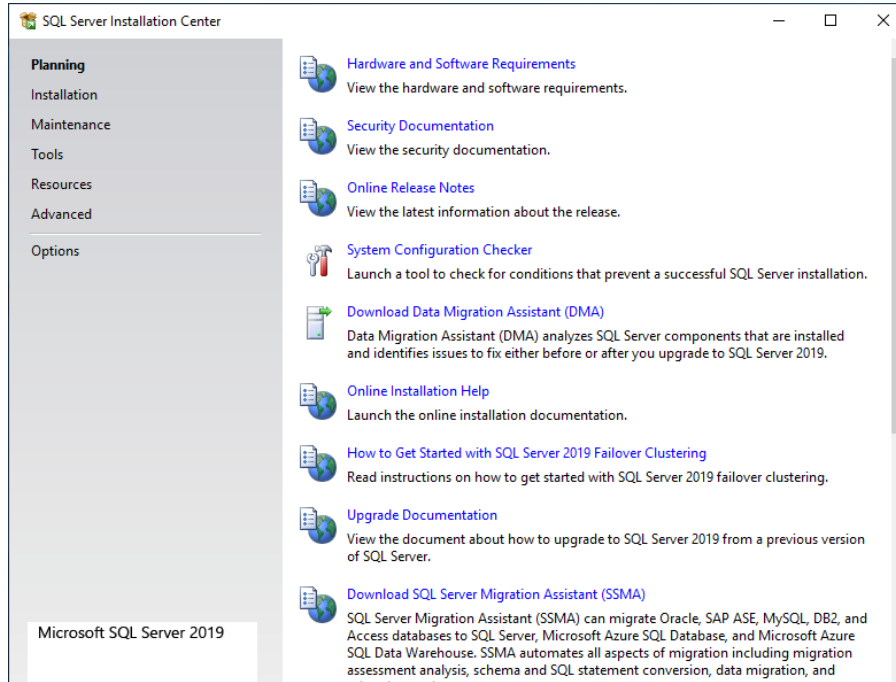

Figure 1 - SQL Server Installation Center

2. Click Installation from the list of options on the left of the screen.
3. Click New SQL Server stand-alone installation or add features to an existing installation as shown in Figure 2 - SQL Server Installation Center - Installation Menu.
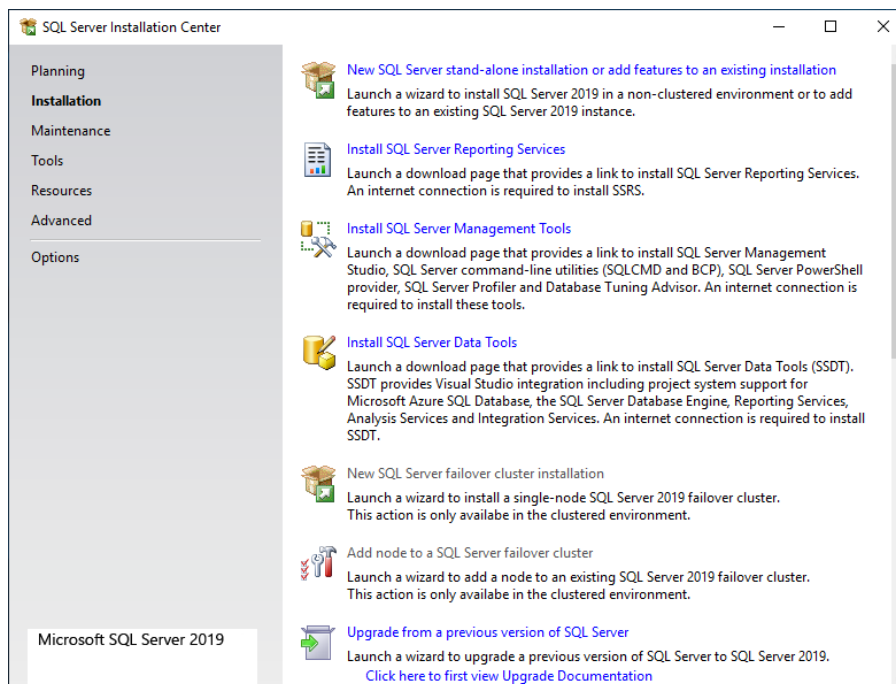

Figure 2 - SQL Server Installation Center - Installation Menu

4. The installer will show a Product Key screen. The product key may be pre-populated for you, if so, click Next. If the product key is empty as shown in Figure 3 - Product Key you will need to enter a Product Key. Click Next to continue.
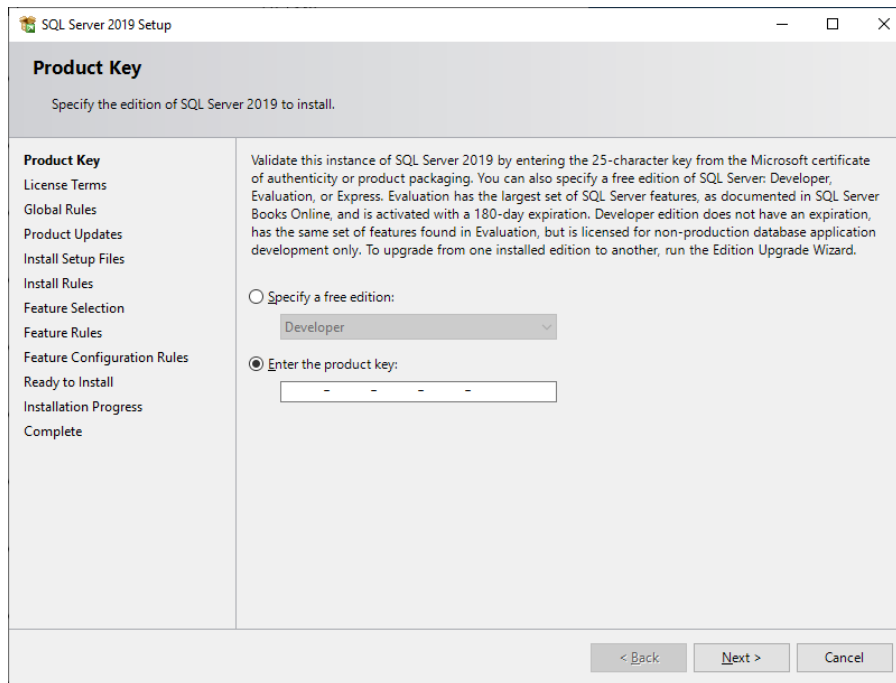

Figure 3 - Product Key

5. The installer will then show a License Terms screen as shown in Figure 4 - License Terms. Click to agree to the terms and conditions and click Next to continue.
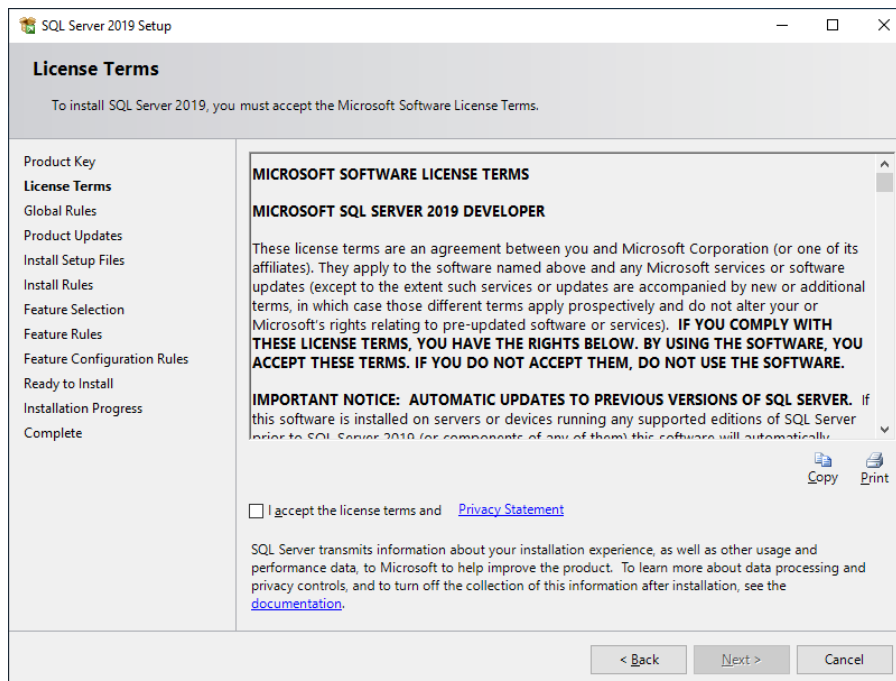

Figure 4 - License Terms

6. The installer will then check for any potential issues when installing the setup support files as shown in Figure 5 - Global Rules. Any issues highlighted should be addressed appropriately. This screen will only show if any problems arise. Once issues are resolved click Re-run and then click Next.
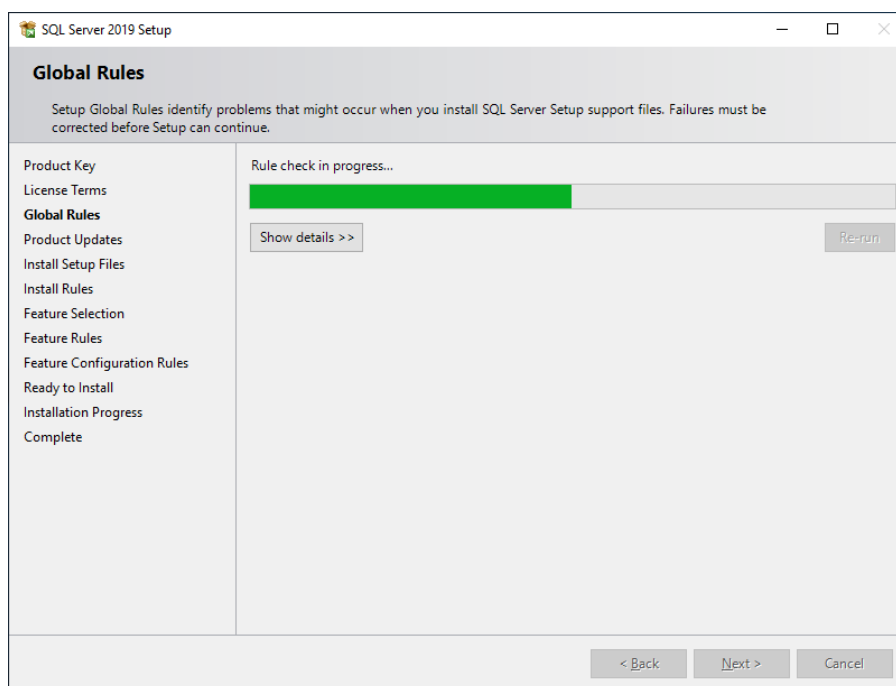

Figure 5 - Global Rules

7. The next step is installing setup files as shown in Figure 6 - Install Setup Files. Once complete, click Next.

    ◈ This screen is usually only displayed if there are any warnings or failures.
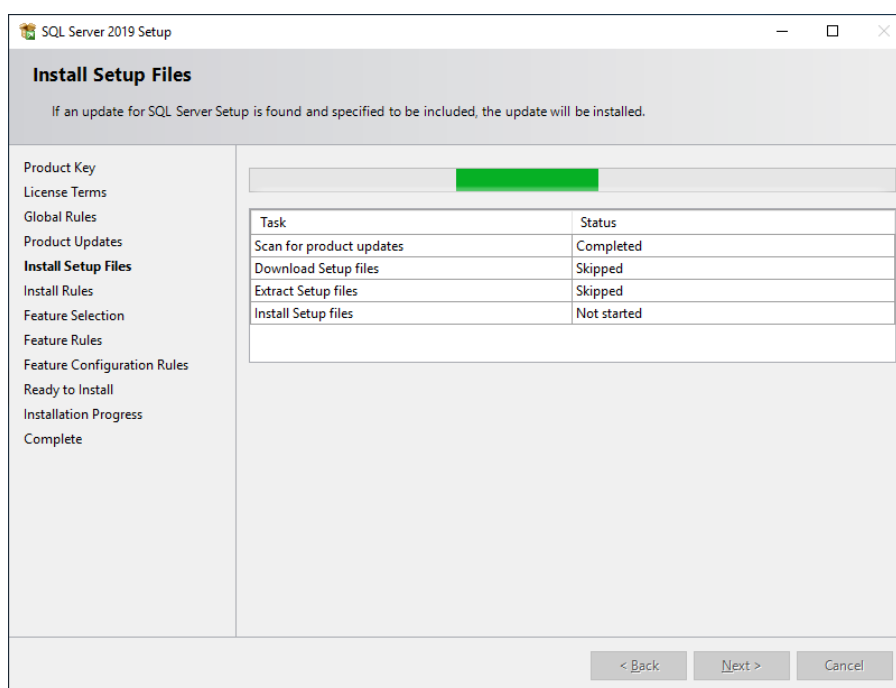

Figure 6 - Install Setup Files

8. Some install rules will then be verified as shown in Figure 7 - Install Rules. Click Next.

◇ This screen is usually only displayed if there are any warnings or failures.
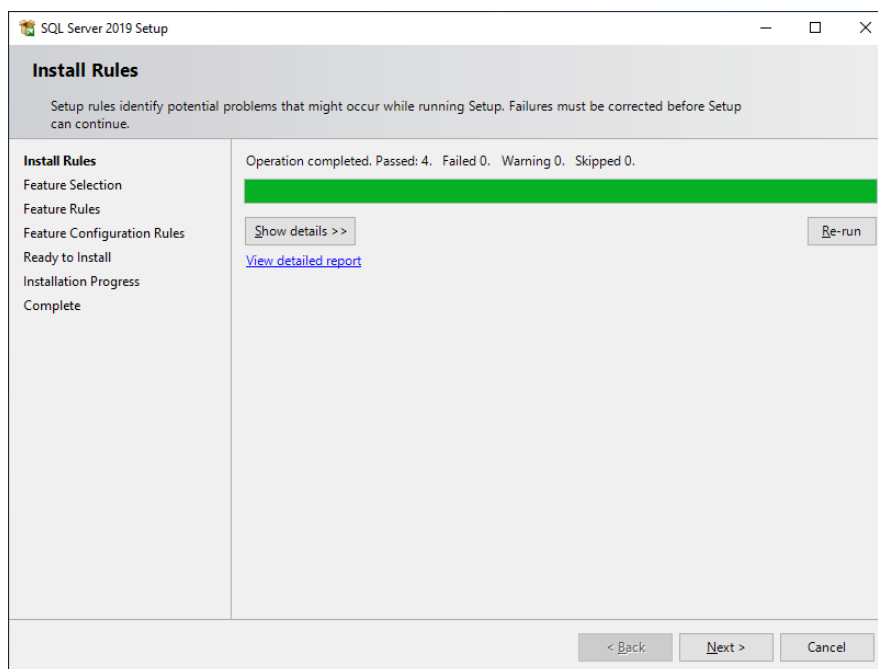
Figure 7 - Install Rules

9. If you currently have SQL Server components installed, you will then be presented with the Installation Type screen as shown in Figure 8 - Installation Type. For a new installation of SQL Server 2019 select the **Perform a new installation of SQL Server 2019** option. Click Next.

If you do not have any SQL Server components installed, you will not see this screen and can go straight to step 10.
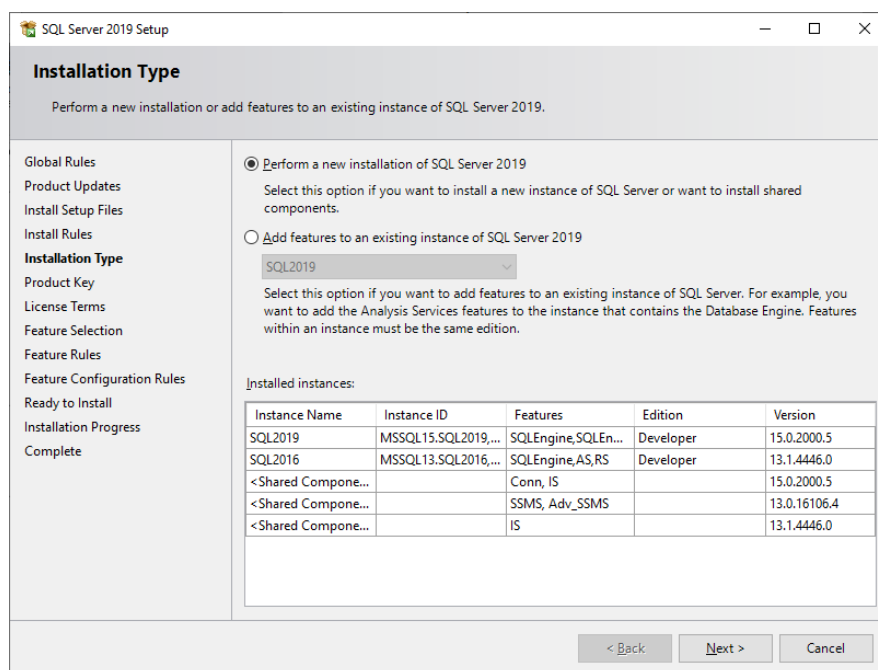
Figure 8 - Installation Type

10. On the Feature Selection screen, as shown in Figure 9 - Feature Selection you will need to select options based on whether you are installing a standard Cortex system or including Cortex LiveView and its associated components. Table 1 - Feature Selection Matrix shows which options should be selected based on the solution being deployed. Any components not specified in Table 1 should not be installed.

⌖ Depending upon the solution specification you may need to deploy some components on a separate server (which implies additional license costs). If you are unsure of what to install or where, speak to a member of the Cortex Support team.

Component	Cortex Standard	Cortex with LiveView
Database Engine Services	Yes	Yes
SQL Server Replication	Yes (if replicated)	Yes (if replicated)
Analysis Services	No	Yes
Client Tools Connectivity	Yes	Yes
Integration Services	No	Yes

Table 1 - Feature Selection Matrix

Once the options required have been selected, click Next.
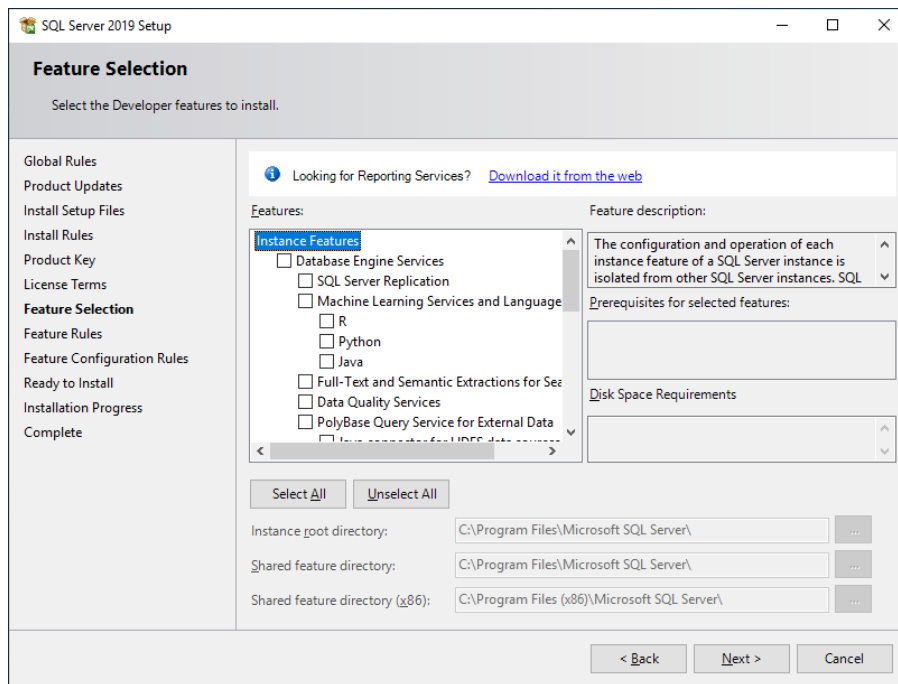
Figure 9 - Feature Selection

11. Some feature rules will then be verified as shown in Figure 10 - Feature Rules. Click Next.

◈ This screen is usually only displayed if there are any warnings or failures.
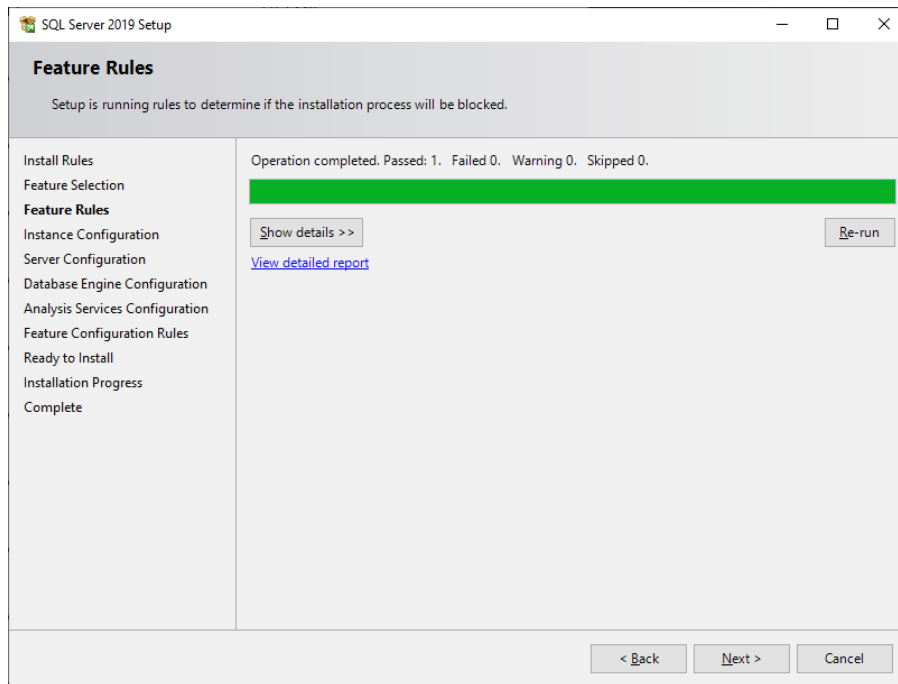
Figure 10 - Feature Rules

12. The Instance Configuration screen, as shown in Figure 11 - Instance Configuration allows you to install either the default instance or a named instance. You can install either, albeit that you can only have one default instance on any given machine.

    Typically, you should install the default instance unless told otherwise. You do not need to change any other default values, and once options have been selected, click Next.

Figure 11 - Instance Configuration

13. The Server Configuration screen as shown in Figure 12 - Server Configuration (Service Accounts) allows you to specify which account the SQL Server Services will run as. This would normally be a dedicated user account e.g. Domain\Cortex_SQL_Admin. You should also change the SQL Server Agent startup type from Manual to Automatic. Once you have configured service accounts and their associated passwords navigate to the Collation tab.
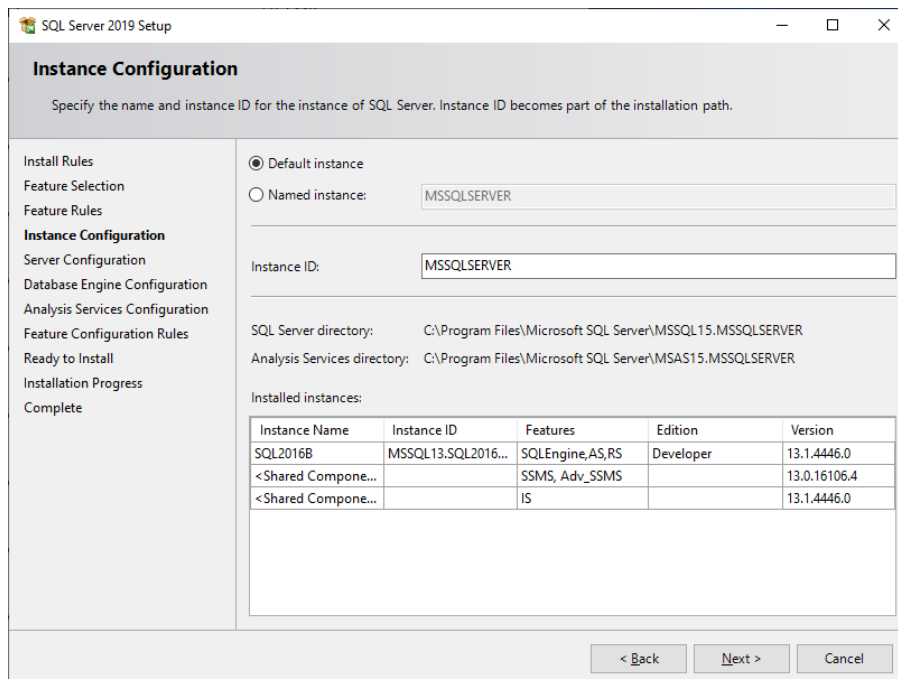
◇ If you have selected to install a named instance in step 12, the SQL Server Browser service should also be set to automatic start up, however the service account cannot be changed.
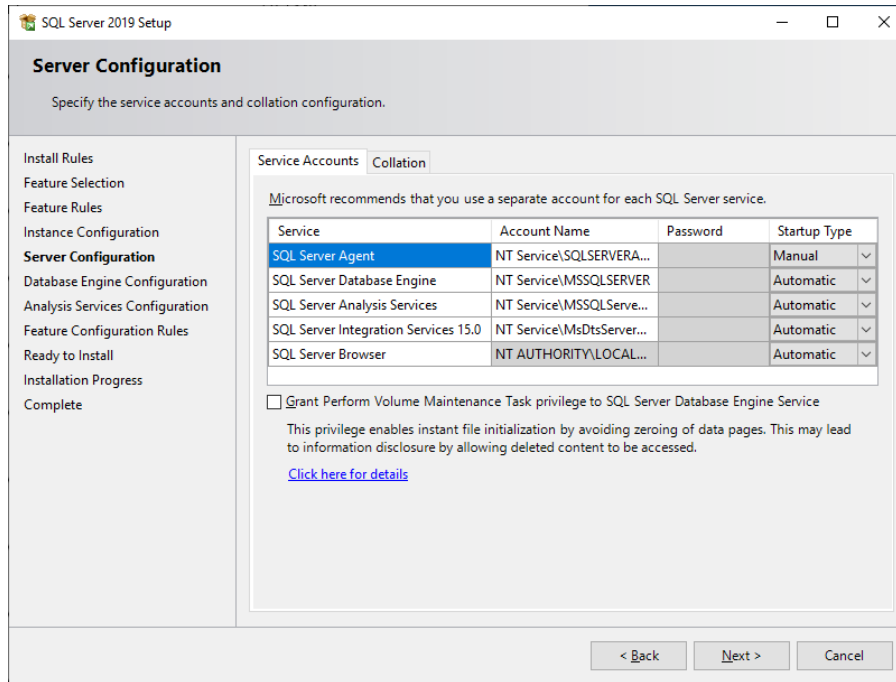

Figure 12 - Server Configuration (Service Accounts)

14. On the Collation tab as shown in Figure 13 - Server Configuration (Collation) you need to ensure that the collation for any items in the list is set to **Latin1_General_CI_AS**. If this is not the case, click the Customize… button and go to step 15. If the collation is set to **Latin1_General_CI_AS** click Next and go to step 16.
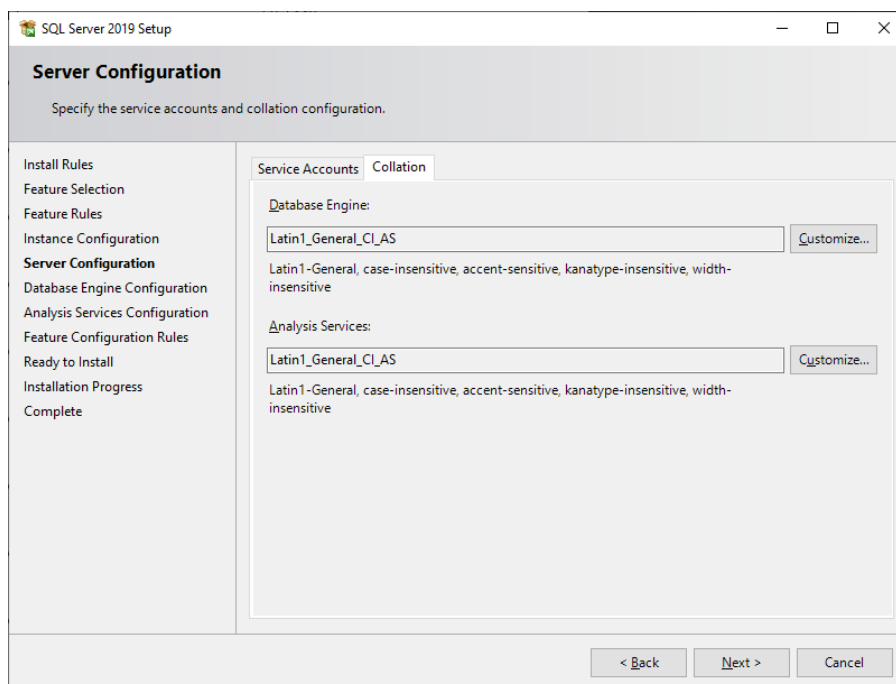
Figure 13 - Server Configuration (Collation)

15. On the customization screen ensure that the values are specified as shown in Figure 14 - Server Configuration (Collation Customization) and click OK.
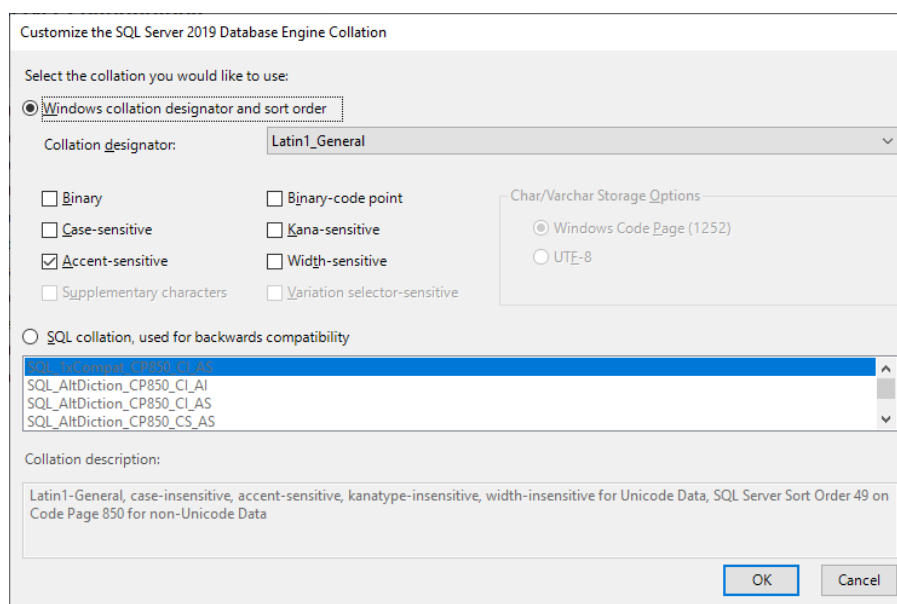
Figure 14 - Server Configuration (Collation Customization)

Back on the collation tab, ensure that the collation for any items in the list is now set to **Latin1_General_CI_AS** and click Next.

16. On the Database Engine Configuration screen as shown in Figure 15 - Database Engine Configuration you can specify whether to install in Windows authentication mode or Mixed mode. Mixed mode allows you to access the system using SQL Server authentication.

If you are installing in mixed mode, you will need to supply a password for the sa account.

You also need to specify SQL Server administrators for the system. You must specify at least one, and you have the option to select the current user and any other available Windows users and groups.

⚑ The MSSQLSERVER, Analysis Services, Integration Services and SQL Server Agent service user(s) should be configured as a system administrator.

Once authentication mode and administrators have been specified click Next.

◈ There is no need to change any configuration in the Data Directories, TempDB, MaxDOP, Memory or FILESTREAM tabs.
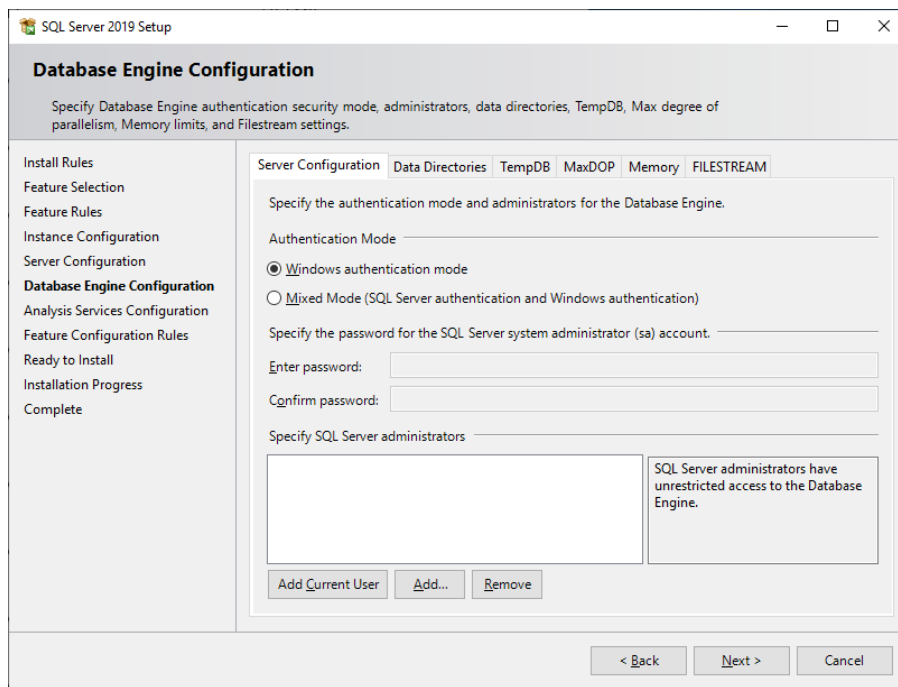
Figure 15 - Database Engine Configuration

17. If the Analysis Services feature was selected, you will be taken to the Analysis Services Configuration screen as shown in Figure 16 - Analysis Services Configuration. For the Server Mode specify Multidimensional and Data Mining Mode.

You also need to specify SQL Server administrators for Analysis Services. You must specify at least one, and you have the option to select the current user and any other available Windows users and groups.

⚑ The Analysis Services and MSSQLSERVER service user(s) should be configured as a system administrator.

Once server mode and administrators have been specified click Next.

◈ There is no need to change any configuration in the Data Directories tab.
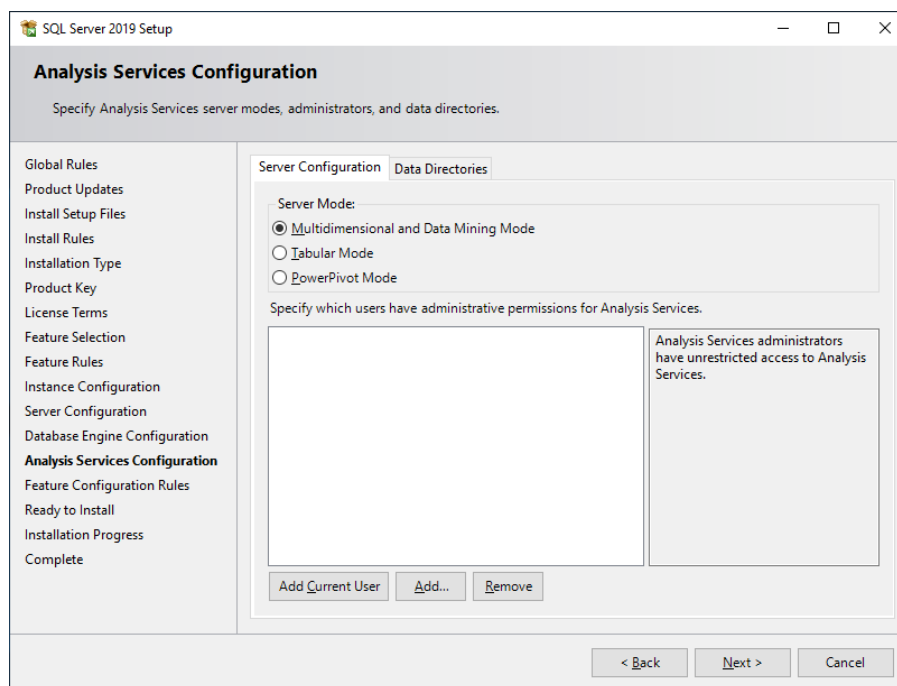
Figure 16 - Analysis Services Configuration

18. On the Feature Configuration Rules screen as shown in Figure 17 - Feature Configuration Rules click Next.

◈ This screen is usually only displayed if there are any warnings or failures.
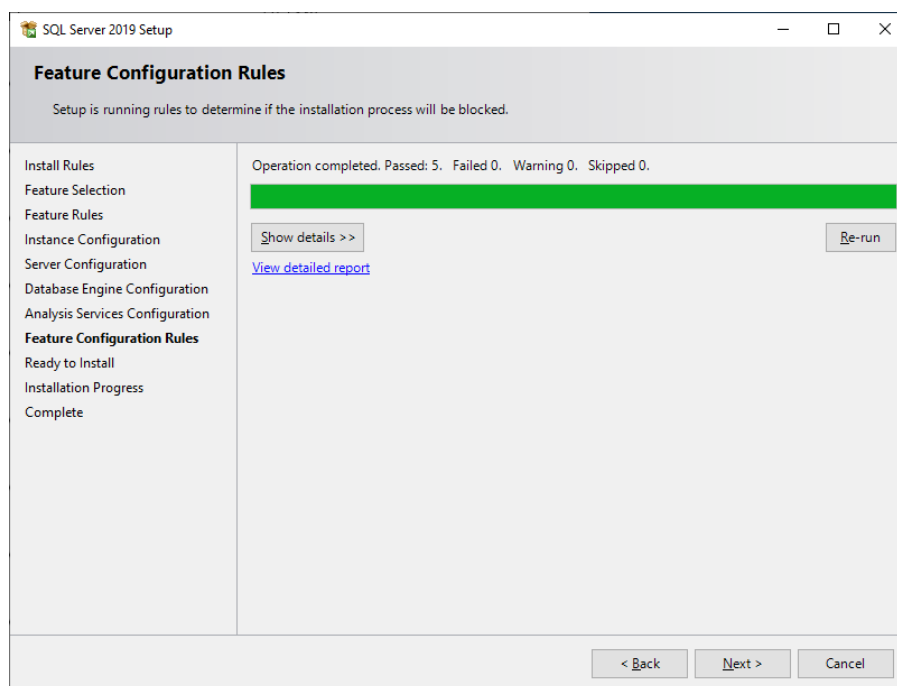
Figure 17 - Feature Configuration Rules

19. On the Ready to Install screen as shown in Figure 18 - Ready to Install, click Install.
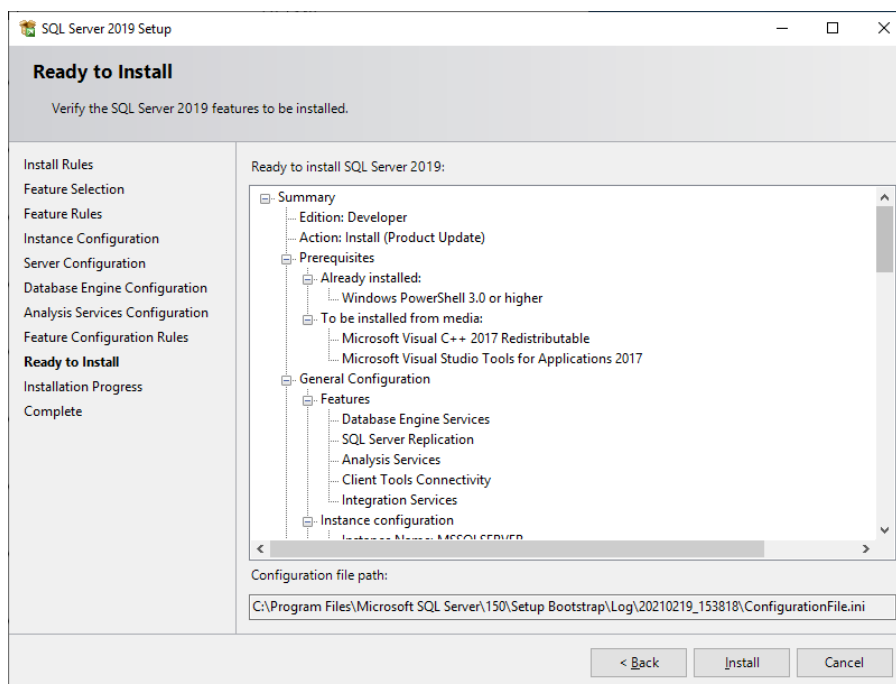
Figure 18 - Ready to Install

20. The Installation Progress screen as shown in Figure 19 - Installation Progress will then be displayed.
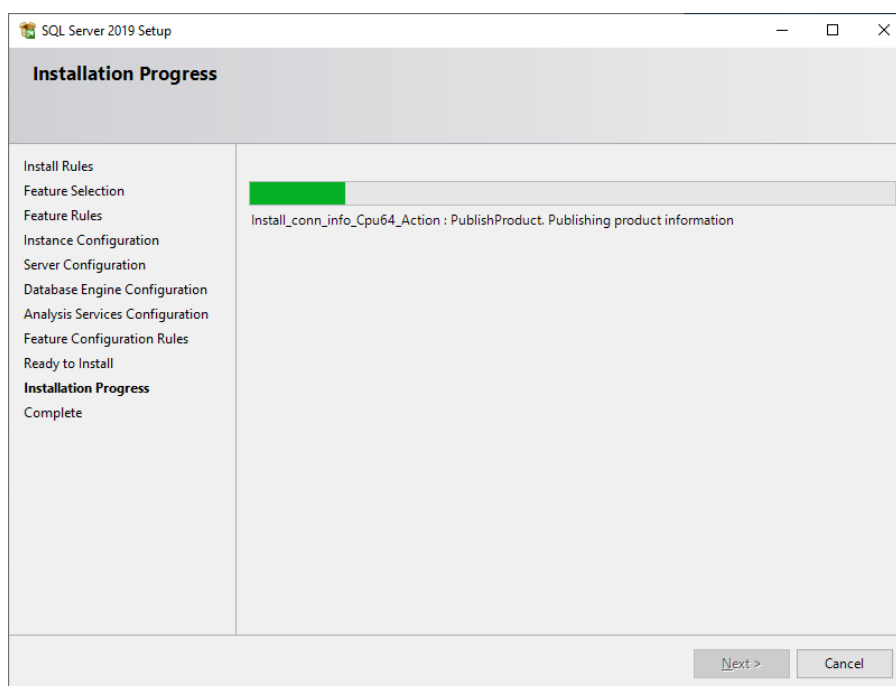
Figure 19 - Installation Progress

21. When the installation is finished, the Complete screen is shown as in Figure 20 - Complete. Click Close, and your SQL Server installation is complete.

Figure 20 - Complete

2.2 Installation of SQL Server Management Tools

1. Run the SQL Server installer. When the installer loads you will be presented with the SQL Server Installation Center as shown in Figure 21 - SQL Server Installation Center.

Figure 21 - SQL Server Installation Center

2. Click Installation from the list of options on the left of the screen.
3. Click Install SQL Server Management Tools as shown in Figure 22 - SQL Server Installation Center - Installation Menu.
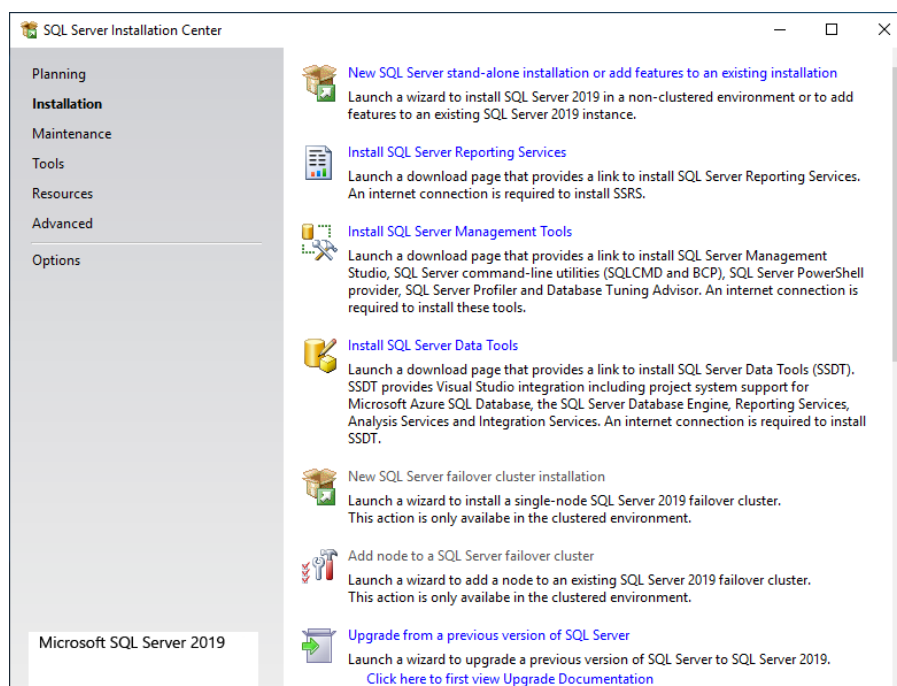
Figure 22 - SQL Server Installation Center - Installation Menu

4. You will be redirected to Microsoft's download website to download the file needed to install the SQL Server Management Tools as shown in Figure 23 – Microsoft SSMS Download Page.

Figure 23 – Microsoft SSMS Download Page

5. Locate and download the latest version of SSMS 18.x by clicking on the link and select Save As when prompted and save it to a known location. Wait for the download to complete.

The Microsoft SQL Server Management Tools must be version 18 to ensure the required tools are installed.

6. Open the location that the installer was saved to in step 5 and start the installation by double clicking on the SSMS-Setup-ENU.exe file.
7. When the Microsoft SQL Server Management Studio welcome screen is displayed as shown in Figure 24 - SQL Server Management Studio Welcome Screen, click Install.
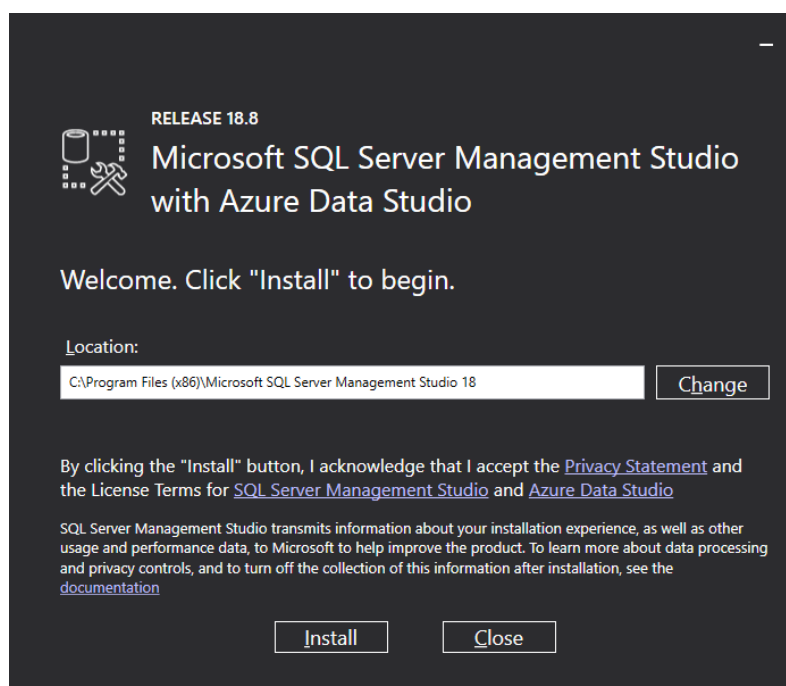
Figure 24 - SQL Server Management Studio Welcome Screen

You may be prompted with a Restart Required screen. Close any open applications and click Restart. If a restart is not required go to step 9.

8. Once the machine has restarted, open the location that the installer was saved to in step 5 and restart the installation by double clicking on the SSMS-Setup-ENU.exe file.

9. You will then see a progress screen as shown in Figure 25 - Loading Packages Progress while the installation packages are loaded.
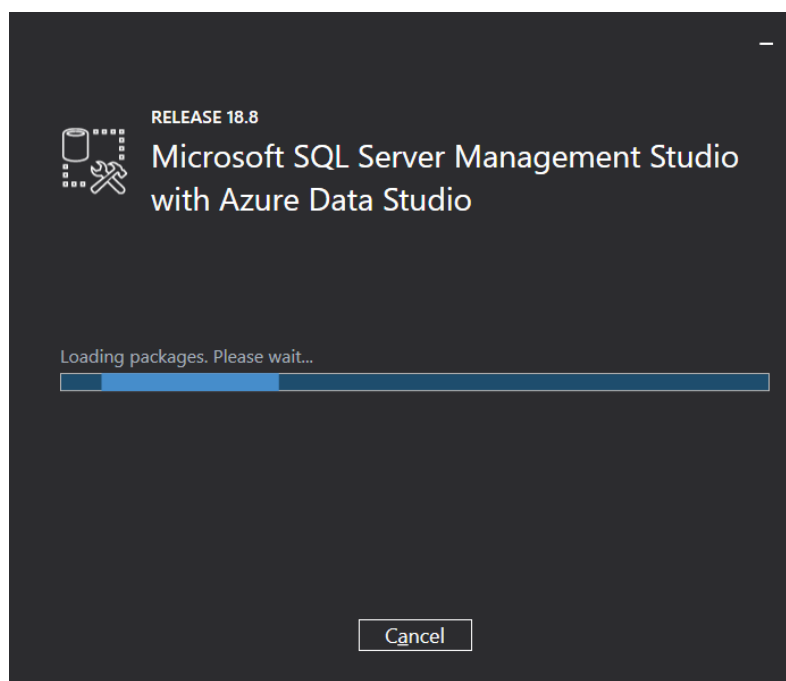
Figure 25 - Loading Packages Progress

10. A progress screen will then display the progress of the installation as shown in Figure 26 - Installation Progress.
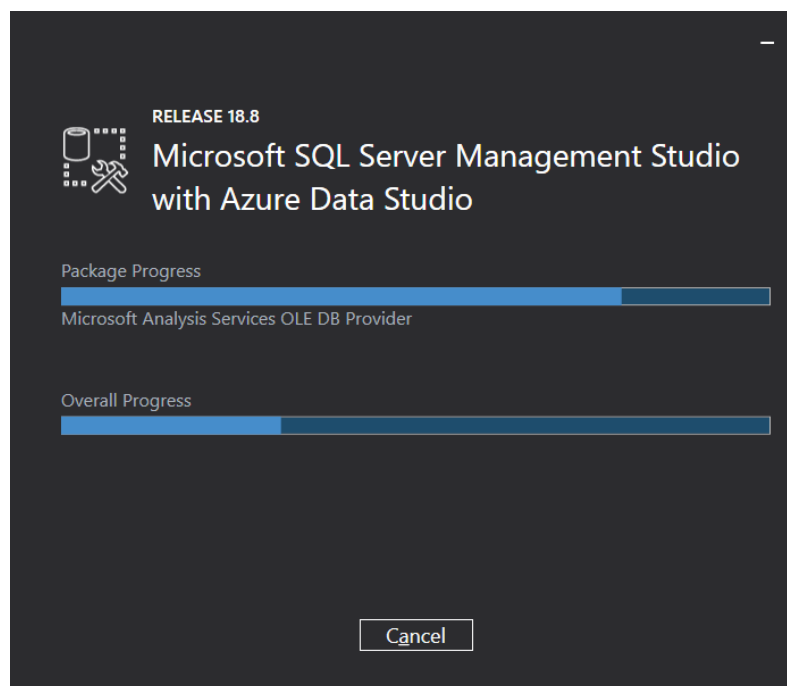
Figure 26 - Installation Progress

11. Once installation has completed a confirmation screen will be displayed and may request a machine restart as shown in Figure 27 - Installation Complete. Click Restart if prompted, else click Close.
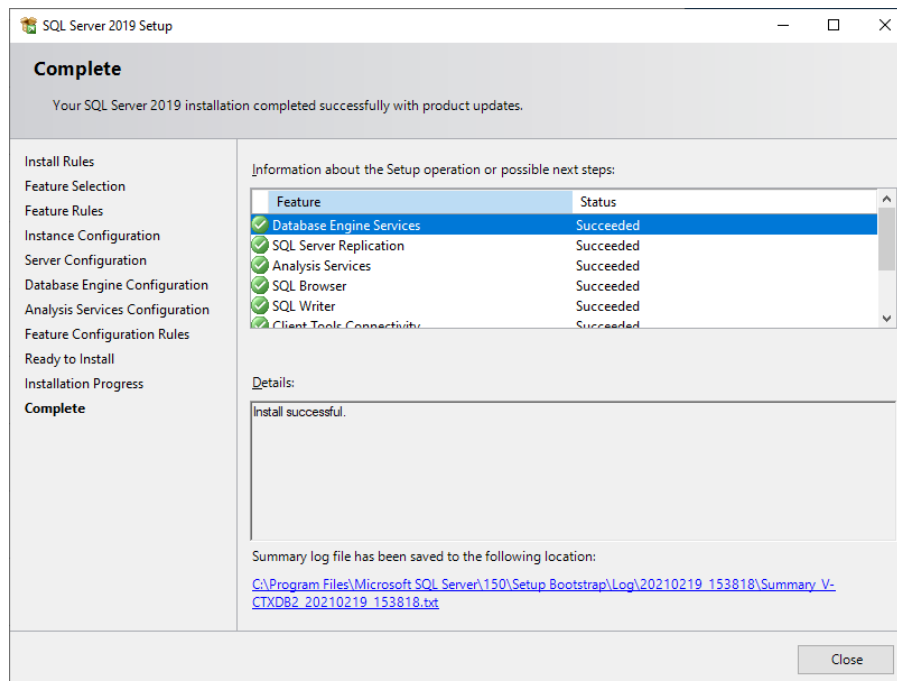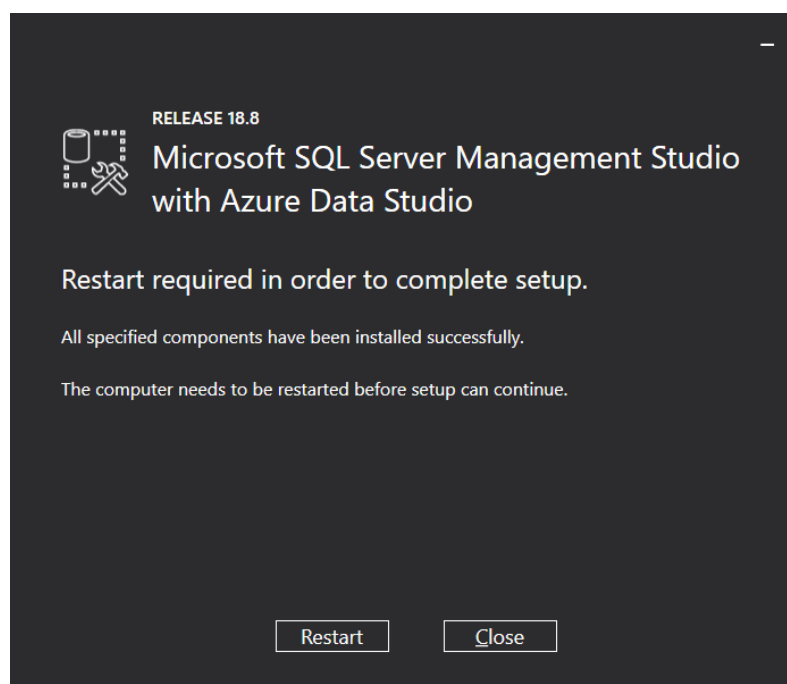

Figure 27 - Installation Complete

2.3 Installation of SQL Server Reporting Services

1. Run the SQL Server installer. When the installer loads you will be presented with the SQL Server Installation Center as shown in Figure 28 - SQL Server Installation Center.
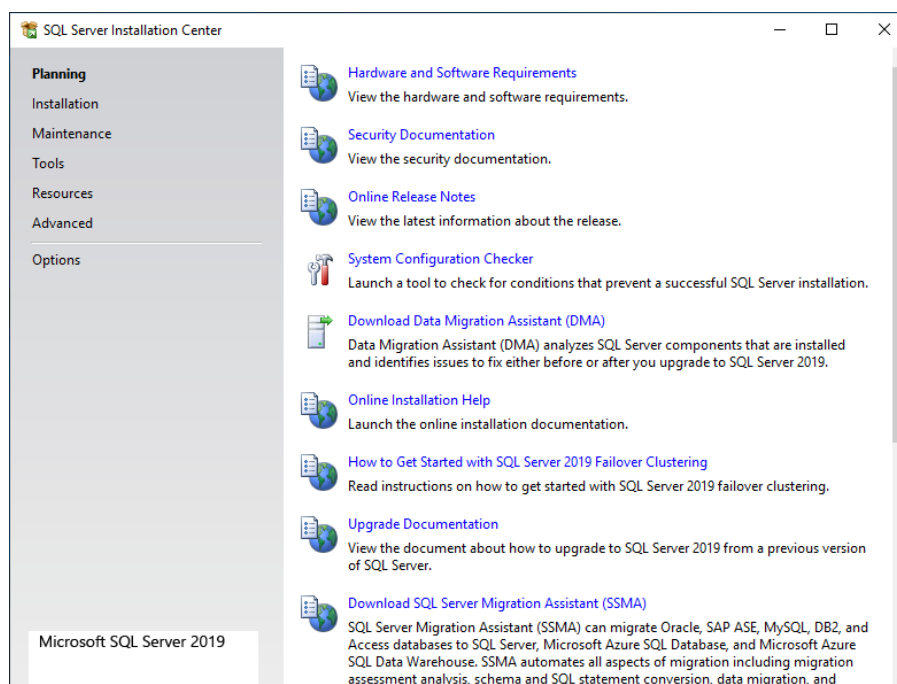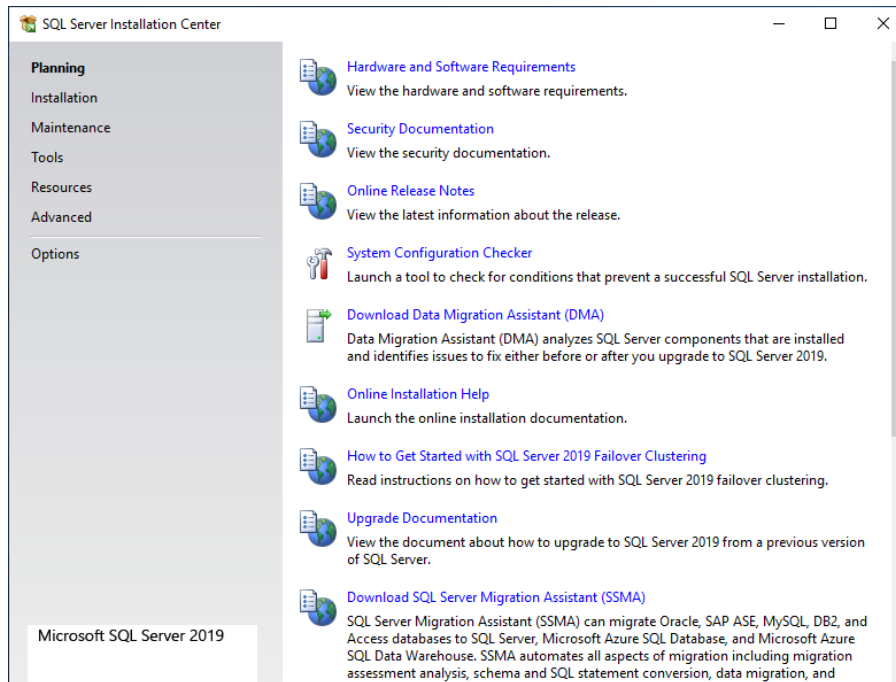

Figure 28 - SQL Server Installation Center

2. Click Installation from the list of options on the left of the screen.
3. Click Install SQL Server Reporting Services as shown in Figure 29 - SQL Server Installation Center - Installation Menu.
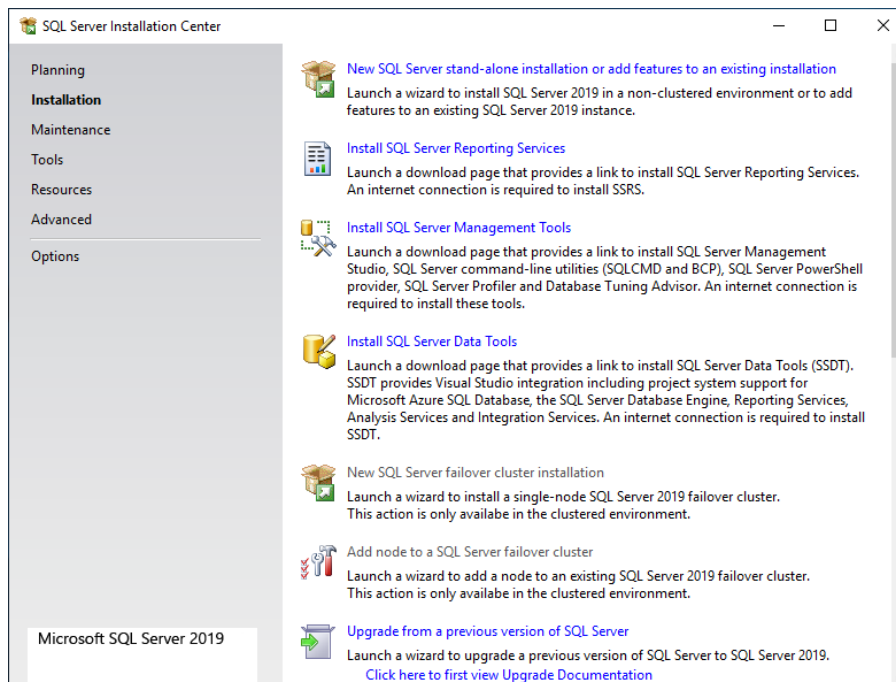
Figure 29 - SQL Server Installation Center - Installation Menu

4. You will be redirected to Microsoft's download website to download the file needed to install SQL Server Reporting Services as shown in Figure 30 - Microsoft SSRS Download Page.
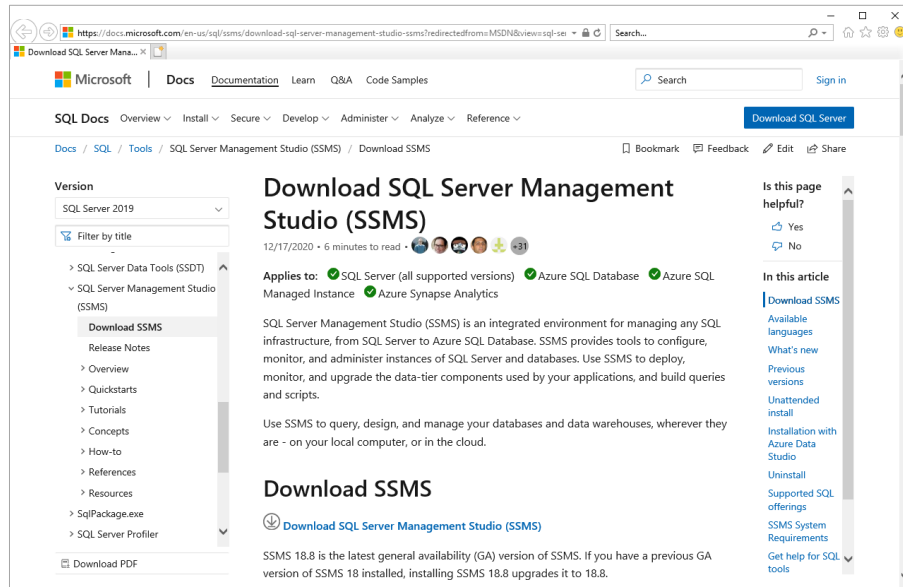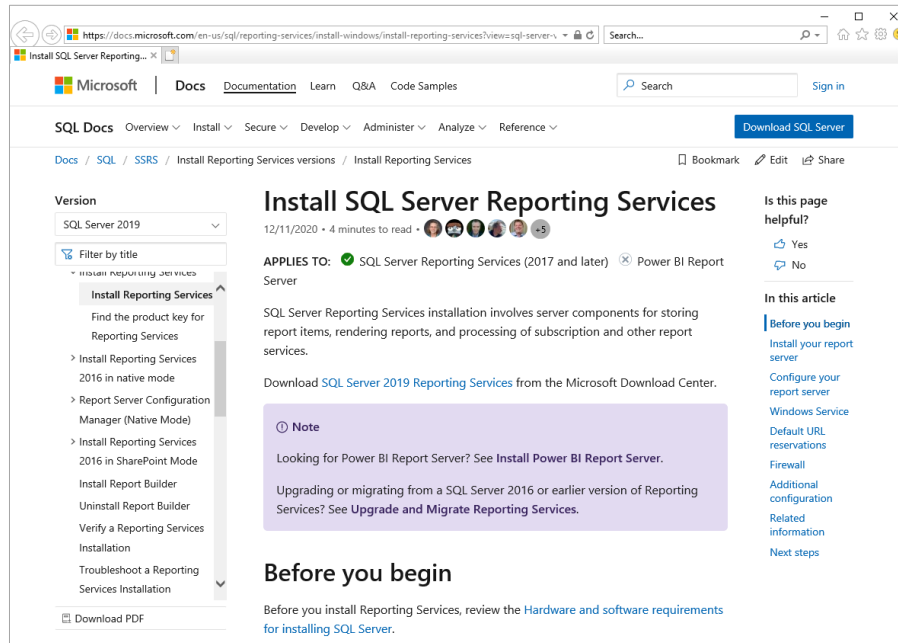

Figure 30 - Microsoft SSRS Download Page

5. Download SQL Server 2019 Reporting Services by clicking on the link. Select the English Language version and click Download. When prompted select Save as and save it to a known location. Wait for the download to complete.

6. Open the location that the installer was saved to in step 5 and start the installation by double clicking on the SQLServerReportingServices.exe file.

7. When the Microsoft SQL Server 2019 Reporting Services welcome screen is displayed as shown in Figure 31 - SQL Server 2019 Reporting Services Welcome Screen, click Install Reporting Services.

Figure 31 - SQL Server 2019 Reporting Services Welcome Screen

8. The installer will show a Product Key screen. Select Enter the product key and insert it in the text box as shown in Figure 32 - SQL Server 2019 Reporting Services Product Key. Click Next to continue.
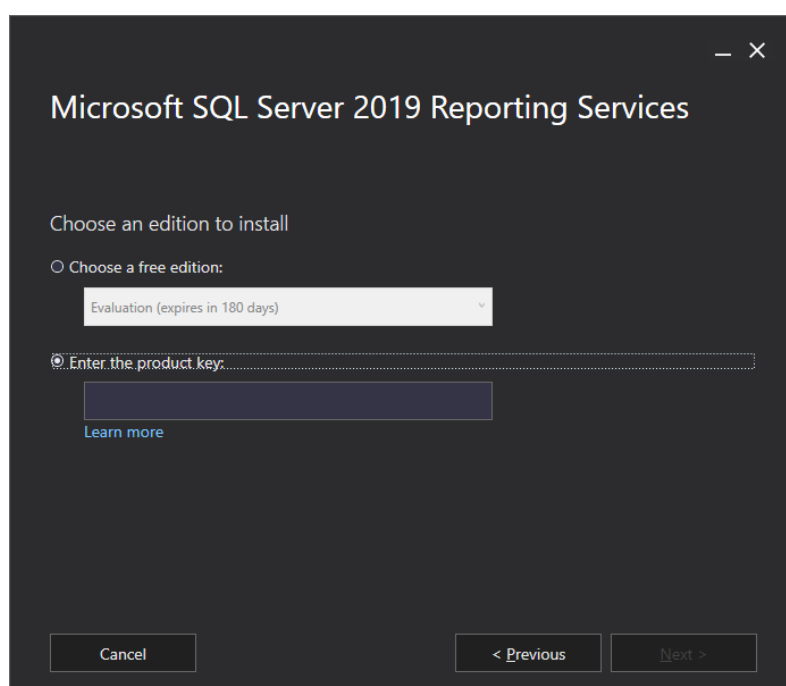
Figure 32 - SQL Server 2019 Reporting Services Product Key

9. The installer will then show a License Terms screen as shown in Figure 33 - SQL Server 2019 Reporting Services License Terms. Click to accept the license terms and click Next to continue.

Figure 33 - SQL Server 2019 Reporting Services License Terms

10. The installer will confirm that a Database Engine is required to store the report server database as shown in Figure 34 - SQL Server 2019 Reporting Services Database Engine. Ensure Install Reporting Services only is selected and click Next.

Figure 34 - SQL Server 2019 Reporting Services Database Engine

11. You will be prompted to specify an install location for Reporting Services as shown in Figure 35 - SQL Server 2019 Reporting Services Install Location. The default is sufficient unless you have a need to install it in a different location. If a different location is required, you should set it now by selecting browse and navigating to the correct location.

Figure 35 - SQL Server 2019 Reporting Services Install Location

12. You will then see a progress screen as shown in Figure 36 - SQL Server 2019 Reporting Services Loading Packages Progress while the installation packages are loaded.

Figure 36 - SQL Server 2019 Reporting Services Loading Packages Progress

13. A progress screen will then display the progress of the installation as shown in Figure 37 - SQL Server 2019 Reporting Services Installation Progress.
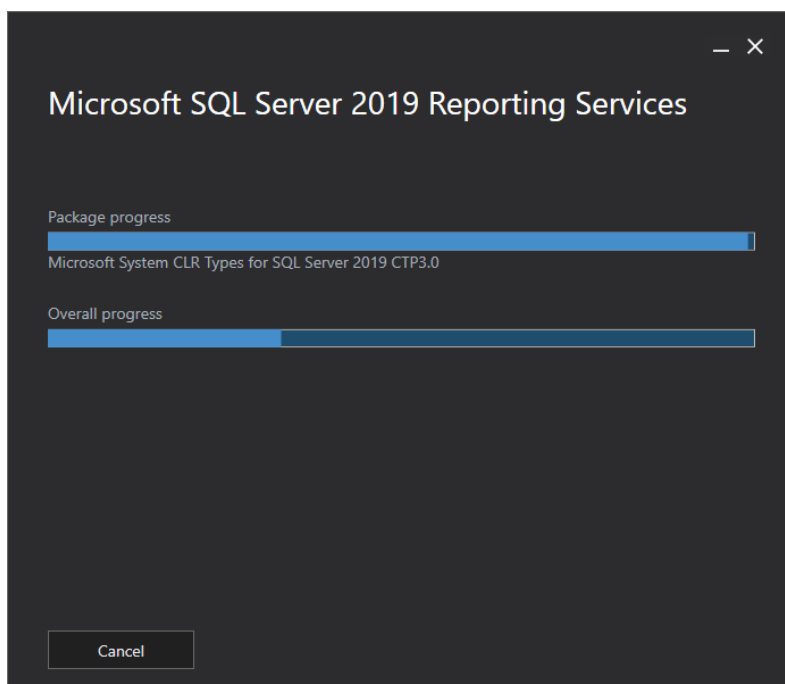
Figure 37 - SQL Server 2019 Reporting Services Installation Progress

14. Once installation has completed a confirmation screen will be displayed and will prompt you to configure the report server as shown in Figure 38 - SQL Server 2019 Reporting Services Installation Complete. Click Configure report server.

Figure 38 - SQL Server 2019 Reporting Services Installation Complete

2.4 Configuration of SQL Server Reporting Services

2.4.1   Initial Configuration

1.   The Report Server Configuration Manager should be opened automatically once the installation is completed however if it does not open, you will need to open it manually.

   a.   Click the **Start** button

   b.   Search for **RSConfigTool.**

   c.   Click the search result.

2.   Connect to the Server and Instance that SQL Server Reporting services has been installed on.

   ⚐ The Report Server Instance will always be SSRS for SQL Server 2019 Reporting Services installations.

3.   On the Server Node verify that the **Report Server Status** is set to started.

4.   On the **Service Account** page, check which account the service is running under. This will be required later.

   ⚐ If you require the service to run as a dedicated user, you can change it here and Apply your changes.

5.   On the Web Service URL Page:

   a.   Ensure that there is a Report Server URL Configured. If there is not, you will need to ensure that the settings are like below then click Apply.

   ⚐ If SQL Server Reporting Services is to be setup to use an SSL Certificate that uses Subject Alternative Names or has been configured with a Common Name other than the machine name you will need to ensure that it is configured initially to not use an SSL Certificate and follow the steps in 2.4.3 Configuration to use SSL to set this up manually.

Figure 39 - SQL Server 2019 Reporting Services Configuration Manager

6.   On the **Database Page**:

   a.   Create the Report Server Database by selecting Change Database.

      i.   Ensure the option is selected to Create a new report server database and click Next.

      ii.   Enter the Server and Instance name that the report server database is to reside on and specify Integrated Security for the Authentication Type. Test the connection. Once the connection has succeeded close the dialog by clicking ok and click Next.

      iii.   Specify the Name for the Report Server Database. This is usually left as ReportServer however if you have need to change it do so here. Click Next.

      iv.   For the credentials for report server to connect to the database specify Service Credentials and click Next.

      v.   Check the details specified on the Summary screen and click Next to proceed. If you need to change anything use the Previous button to go back to the necessary step.

      vi.   Wait for the Database configuration to be completed and click Finish.

   b.   Ensure that the **Current Report Server Database Credentials** are configured.

   📖 These have been set as part of the database configuration and therefore should not require modification.

7.   On the **Web Portal URL Page**:

   a.   Ensure that the **Virtual Directory** is set and that there is a URL Configured. If not, then you will need to **Set the Directory**. The Virtual Directory is typically set to the default of Reports, however if you have a need to change it then do so here. Click **Apply**

   📖 If SQL Server Reporting Services is to be setup to use an SSL Certificate that uses Subject Alternative Names or has been configured with a Common Name other than the machine name you will need to ensure that it is configured initially to not use an SSL Certificate and follow the steps in 2.4.3 Configuration to use SSL to set this up manually.
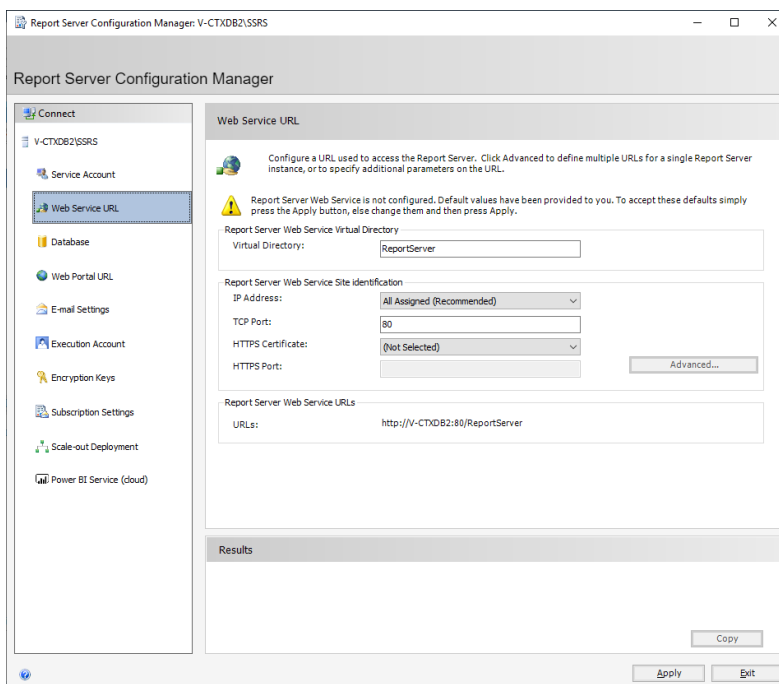
8.   Exit the **Reporting Services Configuration Manager**.

2.4.2 Configuration to enable Kerberos authentication

   📖 This is only required if Kerberos authentication has been configured as per section **1.3.2 User Authentication** in the **Cortex Installation Guide.**

1.   Open the **rsreportserver.config** file which by default can be found in **C:\Program Files\Microsoft SQL Server Reporting Services\SSRS\ ReportServer**.

   📖 The path for the rsreportserver.config file will be different if you have specified a different install location in 2.3 Installation of SQL Server Reporting Services step 11

2.   Locate the **<AuthenticationTypes>** section.

3.   Under <RSWindowsNTLM/>, add the following authentication types:

   a.   <RSWindowsNegotiate/>

   b.   <RSWindowsKerberos/>

4.   Save and close the file.

2.4.3 Configuration to use SSL

1. Open the **rsreportserver.config** file which can be found in **C:\Program Files\Microsoft SQL Server Reporting Services\SSRS\ReportServer**.

2. Locate the **<URLReservations>** section.

3. There should be 2 Applications listed, one with a <Name> of ReportServerWebService and one with a <Name> of ReportServerWebApp.

4. Make a note of the <URLString> associated with each of these applications as this will be needed later.

5. Amend the <URLString> associated with each of these applications to be the URL to use for Reporting Services. This should be in the format of https://FullyQualifiedMachineName:Port e.g.

   > https://machineName.domain.com:443, or
   > https://machineName.domain.com:4443

📖 If Reporting Services is being installed on a machine with another website, the port used by Reporting Services must be different than the one used by the other website.

6. Save and close the file.

7. Open a **Command Prompt** window in Administrator mode.

8. Execute the following commands substituting the URLs so that they match what was noted in step 4:

```
netsh http delete urlacl url=<Enter your URL here>/ReportServer
netsh http delete urlacl url=<Enter your URL here>/Reports
```

9. Execute the following commands substituting the URLs so that they match what was entered in step 5. Also, the user account must match the Service Account noted in step 4 of the Configuration:

```
netsh http add urlacl url=<Enter your URL here>/ReportServer
user="<Enter your user account here>"

netsh http add urlacl url=<Enter your URL here>/Reports user="<Enter
your user account here>"
```

10. Get the thumbprint of the SSL certificate to be used.

📖 A valid Certificate must be available to be able to perform the steps below.

To get a certificate's thumbprint:

    a. Open the Command Prompt.

    b. Execute the mmc command to start Microsoft Management Console.

    c. Select **File → Add/Remove Snap-in**.

    d. From the Available snap-ins select **Certificates** snap-in and click Add.

    e. In the Certificates snap-in dialog select **Computer account**.

    f. Click Next.

    g. In the Select Computer dialog select **Local computer**.

    h. Click Finish.

    i. Click OK.

    j. Expand the **Certificates** tree and locate the certificate which you want to use (its intended purpose should be client authentication).

    k. Right click on the certificate and select Open.

    l. In the **Certificate** window switch to the **Details** tab.

m. Select the **Thumbprint** field.

n. Copy the thumbprint of the certificate into a text editor.

o. Remove all spaces between the hexadecimal characters. One way to accomplish this is to use the text editor's find-and-replace feature and replace each space with an empty string. Keep this open for use in step 11.

p. At this point you may select **File → Save** in MMC and save the Microsoft Management Console file if you wish to access this Certificate easily at a later time.

11. Execute the following command substituting the port for the port specified in the URL, the certthumbprint for the thumbprint obtained in step 10 and the appid for a unique GUID that can be used to identify the application (any GUID generator, such as an online one, can be used to generate a unique appid):

```
netsh http add sslcert ipport=0.0.0.0:<port> certhash=<certthumbprint>
appid={<appid>}
```

12. Open the **Reporting Services Configuration Manager**

    a. Click the **Start** button

    b. Search for **RSConfigTool.**

    c. Click the search result.

13. Connect to the Server and Instance that SQL Server Reporting services has been installed on.

14. On the current server node, stop the Report Server Service.

15. Once it is stopped, Start it again.

16. Only perform these steps if a wildcarded certificate is being used to secure reporting services communications.

    a. Click the Windows Start button

    b. Search 'regedit.msc' and press enter

    c. Find the following registry path: "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa"

    d. Right click and click 'New'

    e. Click 'DWORD (32-bit) Value'

    f. Enter a name of 'DisableLoopBackCheck'

    g. Double click the newly created entry

    h. Type 1 in 'Value data:' textbox

    i. Click 'OK'

17. In Internet explorer navigate to both URLs and login if prompted.

    a. The <Enter Your URL Here>/Reports URL should load a friendly GUI for uploading and viewing SSRS Reports.

    b. The <Enter Your URL Here>/ReportServer URL should display a directory page.

2.5 Enable Named Pipes

Once SQL Server has been installed, we need to configure the instance so that it can be connected to via name rather than just IP Address.

1. Open the **SQL Server 2019 Configuration Manager**

a. Click the **Start** button

b. Search for **SQL ServerManager15.msc.**

c. Click the search result.

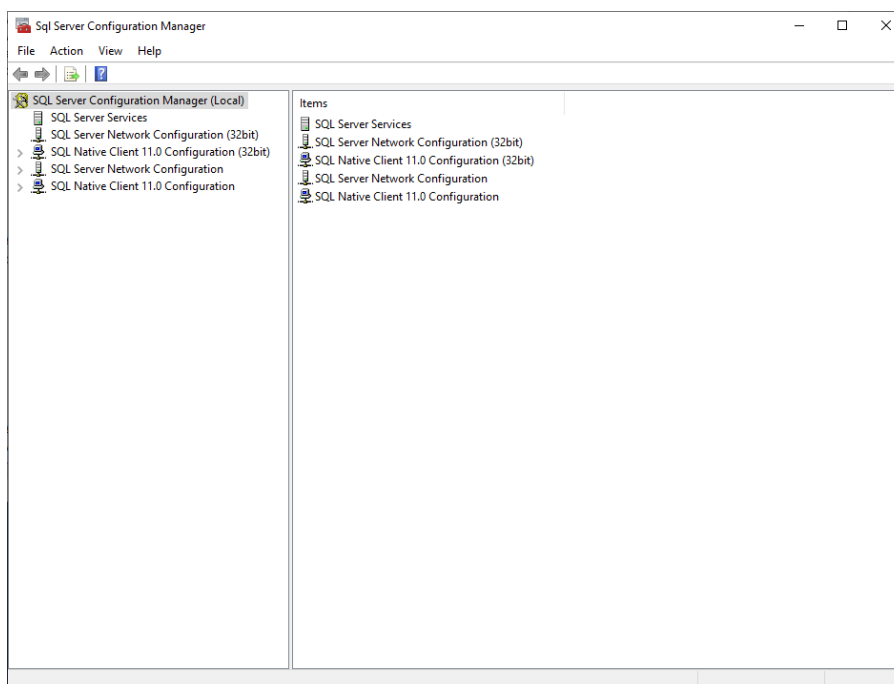The dialog should be like the one shown in Figure 40 - SQL Server Configuration Manager.

Figure 40 - SQL Server Configuration Manager

2. In the Left hand side of the Window, expand the "SQL Server Network Configuration" tree and select "Protocols for <instance name>" where instance name is the instance that you have installed in 2.1 step 12 as shown in Figure 41 - SQL Server Network Configuration.
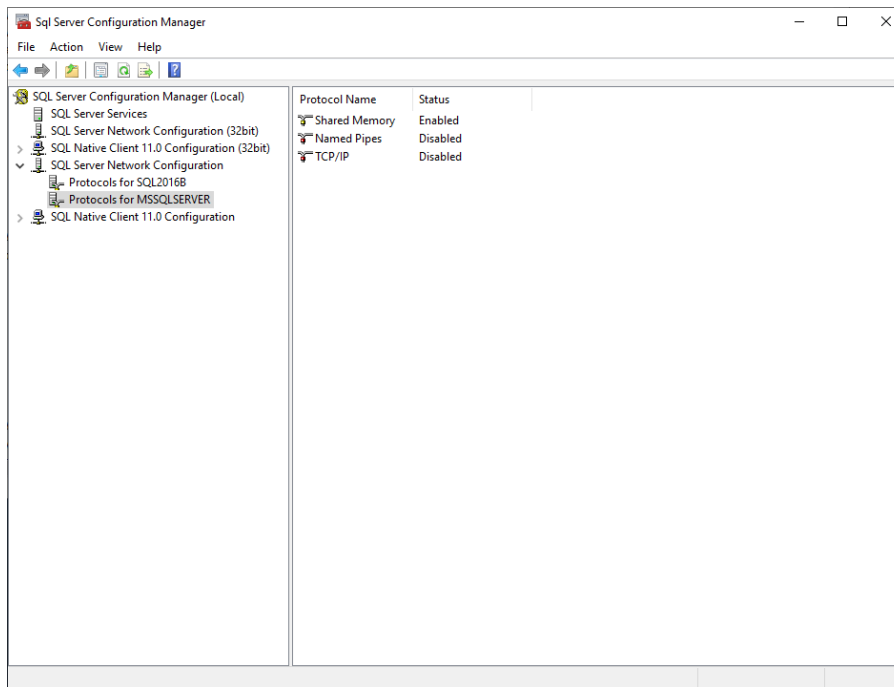
Figure 41 - SQL Server Network Configuration

3. In the right-hand side of the Window, locate the protocol "Named Pipes" and check whether it is enabled, if it is not right click on the protocol name and select enable.
4. You will be displayed a message as shown in Figure 42 - Confirmation Message that confirms that the SQL Server Service needs to be restarted for the changes to take effect.
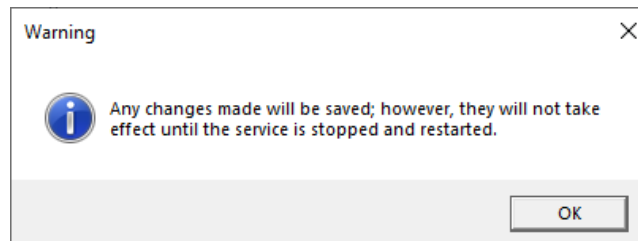
Figure 42 - Confirmation Message

5. Click OK
6. Now check the protocol "TCP\IP" and ensure that this is enabled, if not right click on the protocol name and select enable.
7. You will be displayed a message as shown in Figure 33 - Confirmation Message that confirms that the SQL Server Service needs to be restarted for the changes to take effect.
8. Click OK
9. Repeat steps 3 to 8 for the following options in the left-hand side of the screen:
   a. SQL Native Client 11.0 Configuration → Client Protocols
   b. SQL Native Client 11.0 Configuration (32bit) → Client Protocols
10. In the left-hand side of the window select "SQL Server Services".

1. In the right hand side of the window as shown in Figure 34 - SQL Server Services, locate the "SQL Server (<instance name>)" Service where instance name is the instance that you have installed in 2.1 step 12 as shown in Figure 43 - SQL Server Services.
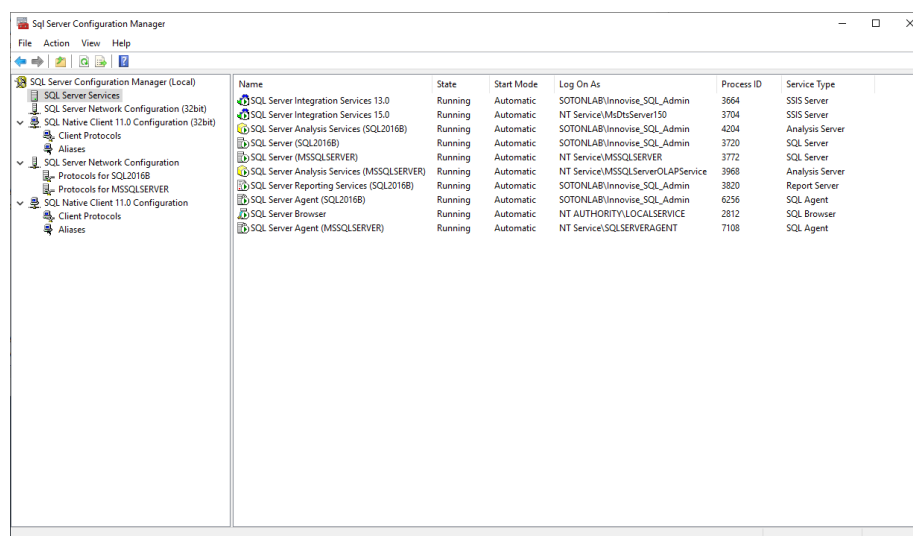

Figure 43 - SQL Server Services

2. Right click on the Name and select restart.
3. Once the necessary services have restarted and the restart dialogs have disappeared close the SQL Server Configuration Manager.

3   Cumulative Update Installation

Once the install of SQL Server 2019 is complete you should install the latest available cumulative update (CU). At the time of writing this document, the latest version available is CU 14. The latest CUs can be sourced from the **Microsoft Update Catalog**.

3.1 Cumulative Update Installation

1. Once you have sourced the CU installer, run it on the machine that is going to be updated.
2. When the installer runs, the first thing you will see is the SQL Server 2019 update screen as shown in Figure 44 – SQL Server 2019 update. Click Next.
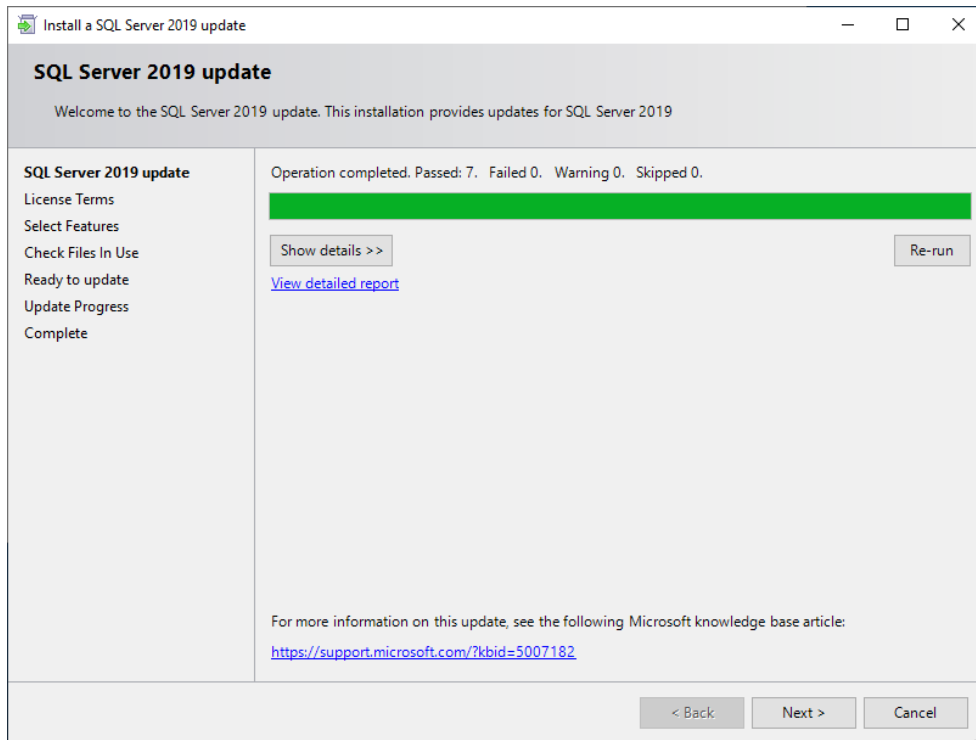
Figure 44 – SQL Server 2019 update

3. On the License Terms screen as shown in Figure 45 – Licence Terms, accept the terms of the licence and click Next.
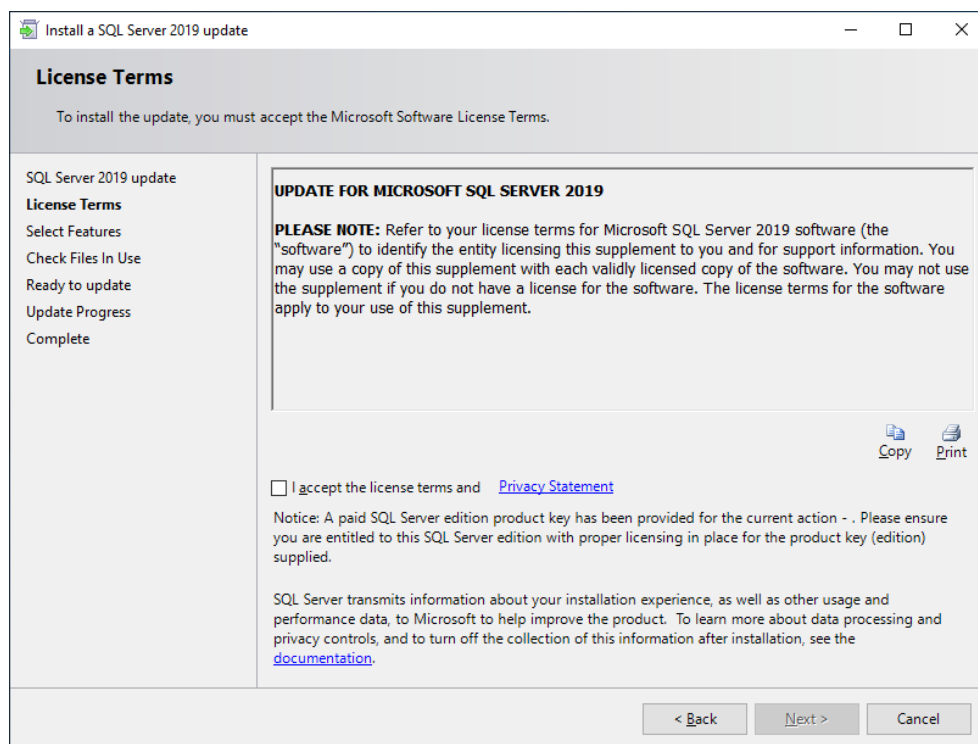
Figure 45 – Licence Terms

4. On the Select Features screen as shown in Figure 46 – Select Features, leave all defaults selected and click Next.
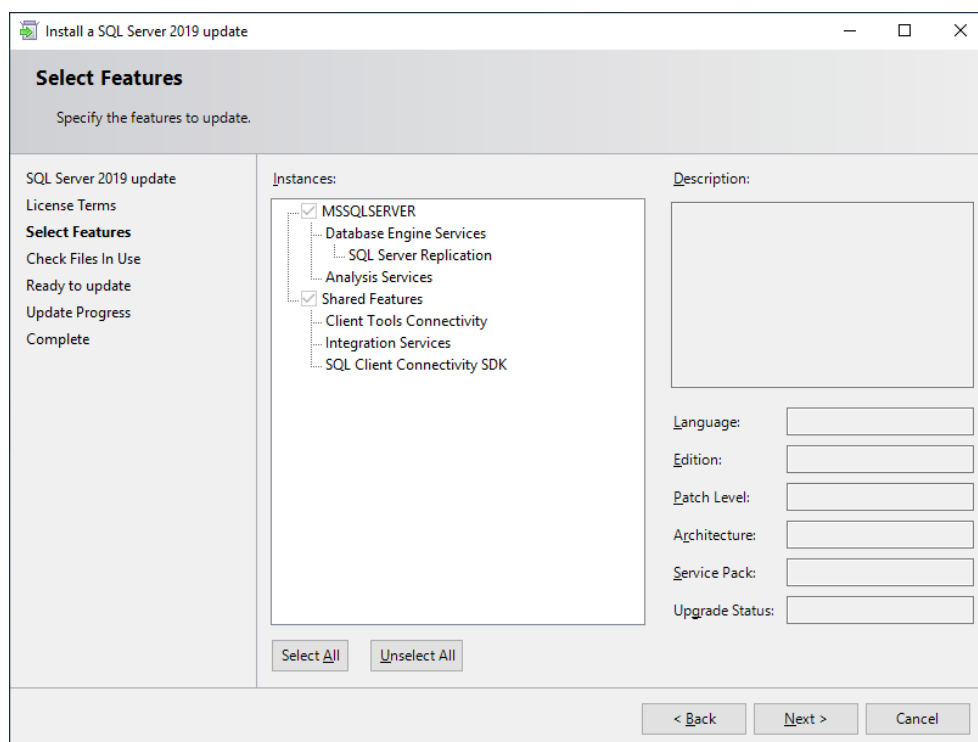
Figure 46 – Select Features

5. The installer then checks files in use as shown in Figure 47 - Check Files In Use. Close any applications highlighted and Click Refresh Check once done. Once there are no files in use warnings, click Next.
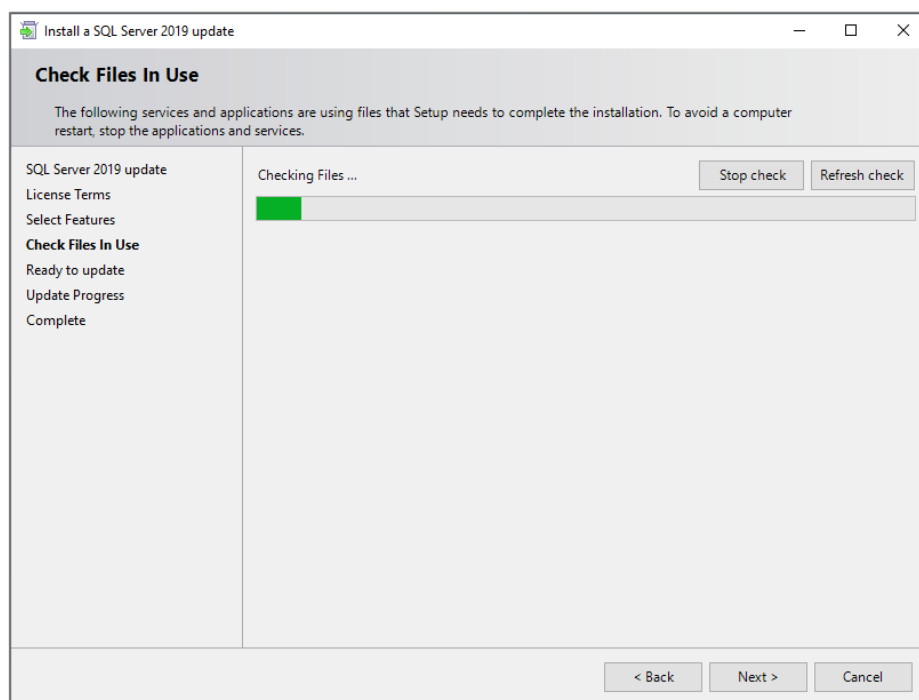
Figure 47 - Check Files In Use

6. On the Ready to update screen as shown in Figure 48 - Ready to update, click Update for the service pack to be applied.
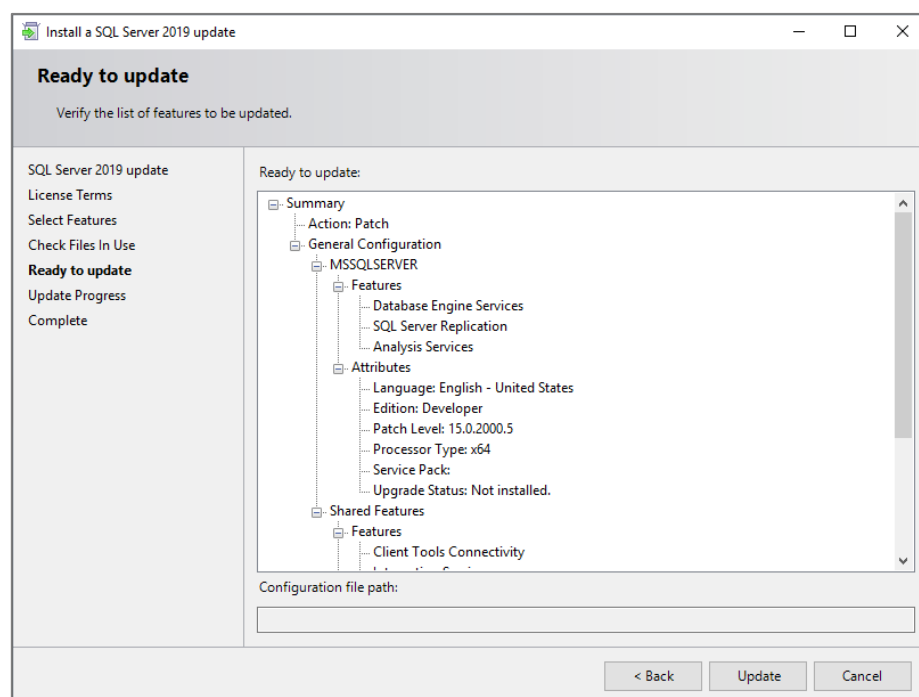
Figure 48 - Ready to update

7. The Update Progress screen as shown in Figure 49 - Update Progress then shows the update progress.

   ◈ No user interaction is required here.
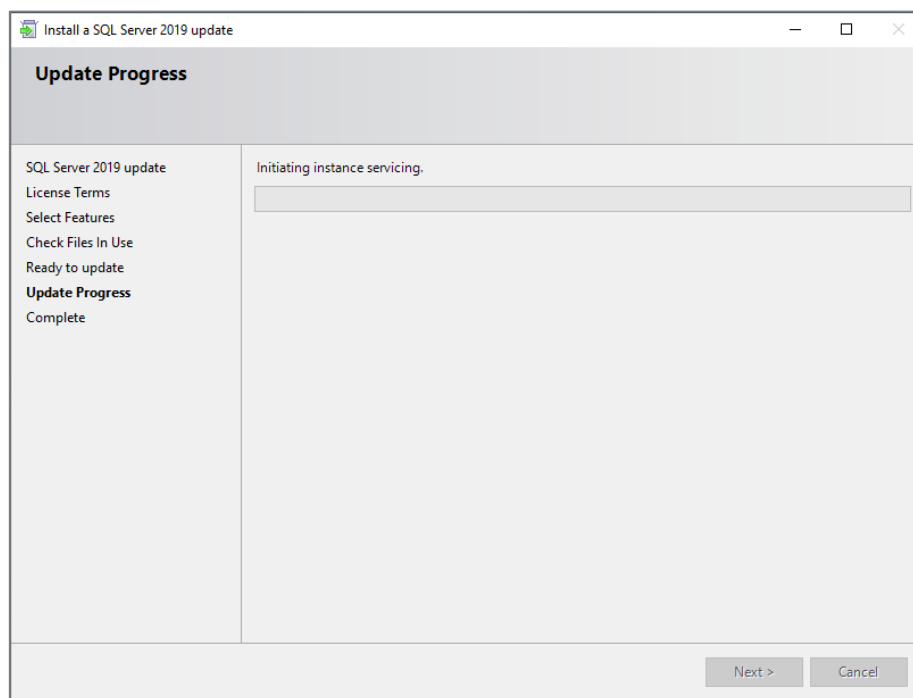
Figure 49 - Update Progress

8. Once the update is complete the Complete screen will be displayed as shown in Figure 50 - Update Complete. Click Close.
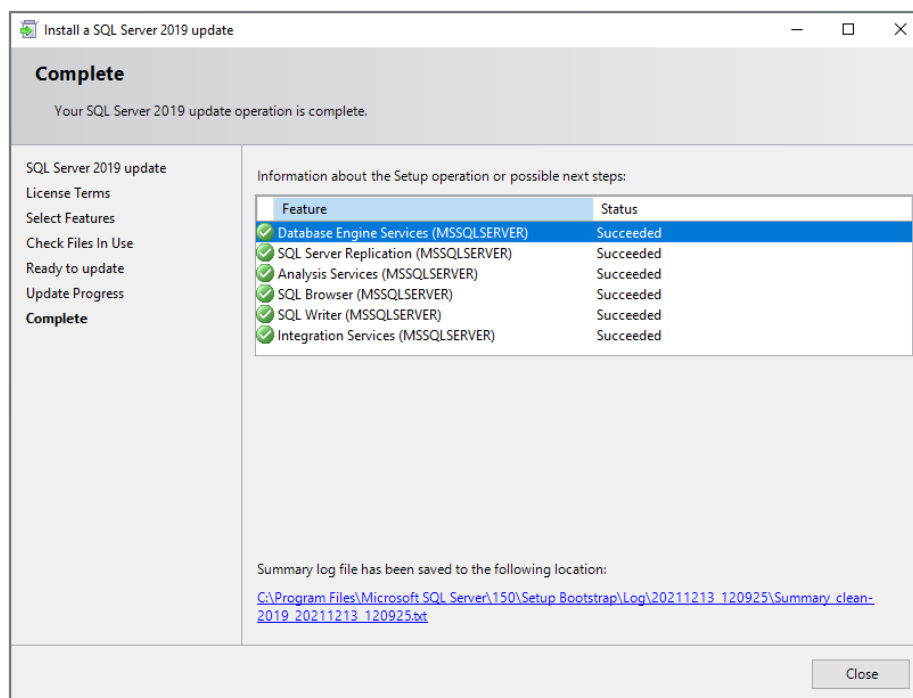
Figure 50 - Update Complete

4 Configure Security Policies

> 🏳 This section is only required if SQL Server Integration Services has been installed to install Cortex with LiveView.

4.1 Configure Local Security Policy

For the Cortex Databases installer to work successfully it is necessary to ensure that the following local security policies are granted to the SQL Server Service account configured in 1.2 Required service user account (within Database server setup). This can be achieved either by modifying the local security policy on the database server or by modifying the group policy that the server inherits its local policies from.

The following security polices need to be granted to the SQL Server Service account:

- Act as part of the operating system
- Adjust memory quotas for a process
- Bypass traverse checking
- Log on as batch job
- Log on as a service
- Replace a process-level token

For group policy modifications contact your network administrators and ask them to grant the policies above to the SQL Server Service account; alternatively, to do this on the Database Server using local security policy use the following steps:

9. Navigate to **Start** -> **Administrative Tools** -> **Local Security Policy**.

10. In the **Local Security Policy** dialog, expand the **Local Policies** node then select **User Rights Assignment**.

11. In the right-hand panel, double-click on the policy you are configuring from the list above.

12. In the **Properties** dialog, click on the **Add User or Group** button.

> ◈ For step 5 it is possible to use the Advanced… button to look up names rather than entering them manually. Various filters can be set to find the correct user or group more easily. Multiple users can be selected by holding down <CTRL> while clicking. OK adds the selected users or groups into the Enter the object names to select text box.

13. Type the name of the SQL Server Service account into the **Enter the object names to select** text box. Click the **Check Names** button to confirm that the user exists.

14. Click **OK** on the **Select Users** dialog, and then confirm the user is correct by clicking **OK** on the **Properties** dialog.

4.2 Modify DCOM Config

To be able to install the SQL Server Integration Services packages required by the Cortex Databases installer, it is necessary to explicitly grant the SQL Server Service account additional permissions in DCOM Config:

1. Navigate to **Start** -> **Administrative Tools** -> **Component Services**.

2. In the **Component Services** dialog, expand the **Component Services > Computers > My Computer > DCOM Config** nodes then right-click on **Microsoft SQL Server Integration Services 15.0** and select **Properties**.

3. In the **Properties** dialog, click on the **Security** tab.

4. In the **Launch and Activation Permissions** section, click the **Edit…** button.

5. In the **Permission** dialog, click the **Add…** button.

⬦ For step 6 it is possible to use the Advanced… button to look up names rather than entering them manually. Various filters can be set to find the correct user or group more easily. Multiple users can be selected by holding down <CTRL> while clicking. OK adds the selected users or groups into the Enter the object names to select text box.

6. Type the name of the SQL Server Service account into the **Enter the object names to select** text box. Click the **Check Names** button to confirm that the user exists then click **OK** on the **Select Users** dialog.

7. In the **Group or user names** section, ensure the user added in step 6 is selected.

8. In the **Permissions for [UserName]** section allow full access.

9. Click **OK** on the **Permission** dialog.

10. Repeat steps 4 – 9 for the following two sections:

    a. **Access Permissions**

    b. **Configuration Permissions**

11. Click **OK** on the **Microsoft SQL Server Integration Services 15.0 Properties** dialog.

5   Configure SQL Server to use TLS

It is recommended that SQL Server is configured to use TLS to ensure that all connections to the database are encrypted.

> ⚐ This cannot be done until after the Cortex Databases Installer has been run.

For full instructions on how to configure this see the following Microsoft website, however the instructions below can be followed:

https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2019

5.1 Obtain and Install a Valid Certificate

In order to configure SQL Server to use TLS, a certificate needs to be available however there are very strict requirements for the certificate to adhere to if it is not a domain wildcard certificate:

- The certificate must be signed by a valid Certificate Authority.
- The certificate must be issued for Server Authentication. This requires the Enhanced Key Usage property of the certificate to specify Server Authentication (1.3.6.1.5.5.7.3.1).
- The certificate must be created using the keyspec option of AT_KEYEXCHANGE.
- The SQL Server Service accounts must have the necessary permission to access the TLS certificate.
- The current system time must be after the valid from property and before the valid to property of the certificate.
- The certificate's common name must be the FQDN or hostname of the machine that SQL Server is installed on. If the hostname is used, the DNS suffix must be specified in the certificate.
- The certificate must be in either the local computer or current user certificate store.
- The certificate will need to be installed on both the SQL Server machine as well as any client machines (all application servers that communicate with the instance of SQL Server that will force encryption).
- If the SQL Server installation is part of a dual site installation the certificate will also need to be installed on the resilient SQL Server machine, e.g. DB1 will have the certificate for DB1 and DB2 installed and DB2 will also have both certificates installed.

5.2 Configure SQL Server to use the Certificate

Once the certificate has been installed you will need to configure SQL Server to use this certificate and force the encryption.

5.2.1 Domain Wild Card Certificate

If the certificate to be used is a domain wild card certificate, then the configuration to use the certificate is required to be done making a registry change:

1. Open a command prompt with elevated permissions.
2. Execute the following command to get a list of the certificates that are installed to the local computer:

```
certutil –store "my"
```

If the certificate is installed for the local user then execute the following command:

```
certutil –user –store "my"
```

3. Locate the certificate you wish to use and copy the Cert Hash value for this certificate.

4. If the value copied in the previous step contains spaces these need to be removed using a text editor.

5. Open the **Registry Editor**

   a. Click the **Start** button

   b. Search for **Regedit.exe**

   c. Click the search result

6. Locate the SQL Server instance hive which is typically in the following location where <InstanceName> should be replaced with your installed instance name or MSSQLSERVER if you have installed the default instance:

   ```
   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL
   Server\MSSQL15.<InstanceName>\MSSQLServer\SuperSocketNetLib
   ```

7. If there is a string value with the name **Certificate** skip to step 9.

8. If there is no string value with the name **Certificate** create one:

   a. Right click on the right hand panel of the registry editor.

   b. Select New → String Value.

   c. Enter the Name **Certificate**.

9. Right Click on the Certificate string value and select **Modify…**

10. In the Value data field enter the certificate hash copied in step 3 (or step 4 if spaces have had to be removed).

11. Open the SQL Server 2019 Configuration Manager

    a. Click the **Start** button.

    b. Search for **SQLServerManager15.msc**.

    c. Click the search result.

12. In the left hand side of the window, expand the **SQL Server Network Configuration** tree and right click the **Protocols for <instance name>** where instance name is the instance that you wish to configure to use TLS.

13. Select **Properties**.

14. In the Properties dialog that opens, on the Flags tab, set **Force Encryption** to be **Yes**.

15. Click **OK**.

16. A dialog will pop up confirming that changes will not take effect until the service is stopped and restarted.

17. Click **OK**.

18. In the left hand side of the window, right click the **SQL Native Client 11.0 Configuration (32 bit)** node and select **Properties**.

19. In the Properties Dialog set **Force Protocol Encryption** to **Yes**.

20. Click **OK**.

21. A dialog will pop up confirming that changes will not take effect until the service is stopped and restarted.

22. Click **OK**.

23. In the left hand side of the window, right click the **SQL Native Client 11.0 Configuration** node and select **Properties**.

24. In the Properties Dialog set **Force Protocol Encryption** to **Yes**.

25. Click **OK**

26. A dialog will pop up confirming that changes will not take effect until the service is stopped and restarted.

27. Click **OK**.

28. In the left hand side of the window select the **SQL Server Services** node, restart all SQL Server Services by right clicking on each service and selecting **restart**.

5.2.2   All Other Certificates

This is done using SQL Server Configuration Manager:

1. Open the **SQL Server 2019 Configuration Manager**

    a. Click the **Start** button.

    b. Search for **SQLServerManager15.msc**.

    c. Click the search result.

2. In the left hand side of the window, expand the **SQL Server Network Configuration** tree and select **Protocols for <instance name>** where instance name is the instance that you wish to configure to use TLS.

3. Select **Properties**.

4. In the Properties dialog that opens, on the Flags tab, Set Force Encryption to be **Yes**.

5. In the Certificate drop down select the certificate that has been installed for this purpose. If the certificate is not visible it does not meet the requirements for SQL Server to use and the certificate should be regenerated adhering to the requirements specified in **5.1 Obtain and Install a Valid Certificate**.

6. Click **OK**.

7. A dialog will pop up confirming that changes will not take effect until the service is stopped and restarted.

8. Click **OK**.

9. In the left hand side of the window, right click the **SQL Native Client 11.0 Configuration (32 bit)** node and select **Properties**.

10. In the Properties Dialog set **Force Protocol Encryption** to **Yes**.

11. Click **OK**.

12. A dialog will pop up confirming that changes will not take effect until the service is stopped and restarted.

13. Click **OK**.

14. In the left hand side of the window, right click the **SQL Native Client 11.0 Configuration** node and select **Properties**.

15. In the Properties Dialog set **Force Protocol Encryption** to **Yes**.

16. Click **OK.**

17. A dialog will pop up confirming that changes will not take effect until the service is stopped and restarted.

18. Click **OK**.

19. In the left hand side of the window select the **SQL Server Services** node, restart all SQL Server Services by right clicking on each service and selecting **restart**.