Getting Started

The InventoryCloud OP (On-Premise) is for the companies who want to host the application on their local server. This document explains how to set up the server. The installation guide is for the system administrator or technical person responsible for setting up the server.

[Set Up](#)

- [Prerequisites](#)
  - [IIS Settings Prerequisite](#)
  - [PowerShell Permission Configuration](#)
- [Installation Files](#)
- [Installation Steps](#)
-
-

Set Up

Prerequisites

Some settings need to be done before launching the InventoryCloud On-Premise (OP) installer. This will make the process go smoother. Be aware of and plan for one or more PC/server reboots during the installation process. **Note** that the Home/Standard edition of Windows 10 should not be used for this product (use Pro or Enterprise instead).

Note: Make sure to read all the prerequisites before InventoryCloud OP installation.

1. System Requirements - The system requirements for effectively running the InventoryCloud OP application are:
   - Operating System - Windows 8.1, Windows 10, Windows Server 2012 R2, and Windows Server 2016 (and onwards).
   - Memory – 8GB RAM.
   - Free disk space – Min 60GB HD space, 512 GB recommended.
   - Processor - Min i7 2.8 GHz, Min 1 LAN card (Typically static IP address).
2. Warning, many Anti-virus or H-IDS software may cause the setup to fail as they are not compatible with some component installers included in this setup. If you have issues during installation please try temporarily deactivating the Anti-Virus software before you retry the installation. Please make sure to do that and you have all such necessary administrative privileges before you contact Tech-Support.

   Warning, some Anti-Virus software have been found to severely degrade the performance of this software without proper configuration. See your antivirus products documentation for configuration recommendations.

   A well run web server should not have a commercial anti-virus (AV) package installed. The kind of Office macro viruses and mass-market trojans that AV packages are optimized for are a poor match to your Wasp web server.

   What you should do is:

   - Absolutely obsess over a single purpose. Installing your Wasp web server on a platform already hosting other services like active directory, database or file sharing just opens up additional avenues through which users can upload malicious content to your site.

- Keep your server patched up with the latest security updates, and configured according to best-practices. Look at things like Microsoft's security toolkit.
- Have a separate firewall. Doesn't help you much with regards to intrusions but it adds another layer of defense against misconfigured network services, and helps with simple DOS attacks. It also helps a lot with locking down remote management possibilities etc.
- Install a host intrusion detection system (H-IDS) on your server.

There is a lot of confusion about the terms, the words are often used in many different ways here. To be clear, what we mean by an H-IDS here is:

- a service on a computer
- which continuously check-sums all executable files on the computer
- and throws an alert whenever an executable file has been added or modified (without authorization).

Actually, a good H-IDS will do a bit more than this, such as monitoring file permissions, Registry access, etc, but the above gets the gist of it.

A host intrusion detection system takes some configuration, since it can give a lot of false errors if not set up properly. But once it's up and running, it will catch more intrusions than AV packages. Especially H-IDS should detect a one-of-a-kind hacker back door, which a commercial AV package probably will not detect.

H-IDS also lighter on the server load, but that's a secondary benefit -- the main benefit is a better detection rate.

Now, if the resources are limited; if the choice is between a commercial AV package and doing nothing, then some AV products are better than nothing.

So if you must install AV software you are responsible for making sure that the product is properly administered so that installing your new wasp server will go smoothly.

Please also make sure the platform is up to the additional load the AV software is putting on it.

3. Do not use a Domain Admin account to log into the PC to perform the InventoryCloud OP installation. If necessary, create a local user, add that user to the local Administrators group (not the Users group), then log on as this new local admin. This will ensure that the software is installed in a manner that does not depend on the domain user account. So, the **Set up** should be executed while logged in as a local user. Attempting to install some required Server components may fail if installed using a domain user account, even if that domain user is a member of the computers administrators group.

4. If you need to change the PC/server name to something else, perform the name change before starting the installation process. Consult your IT department for guidance if necessary. Rather than installing on a temporary server, then moving the database to the final server, perform the installation on the Cloud OP's destination server. This will avoid tedious and complicated reconfiguration steps.

5. If you have downloaded and extracted the On-Premise installer folder in the Downloads folder, move it somewhere else on the local drive. e.g. the Desktop, root of C: drive, etc. (This folder should be on a local drive (not a network location), and not in the Downloads folder.)

6. Wasp Cloud products require JavaScript to run properly. Additionally, full functionality can only be achieved if “Allow Popups” is also enabled.

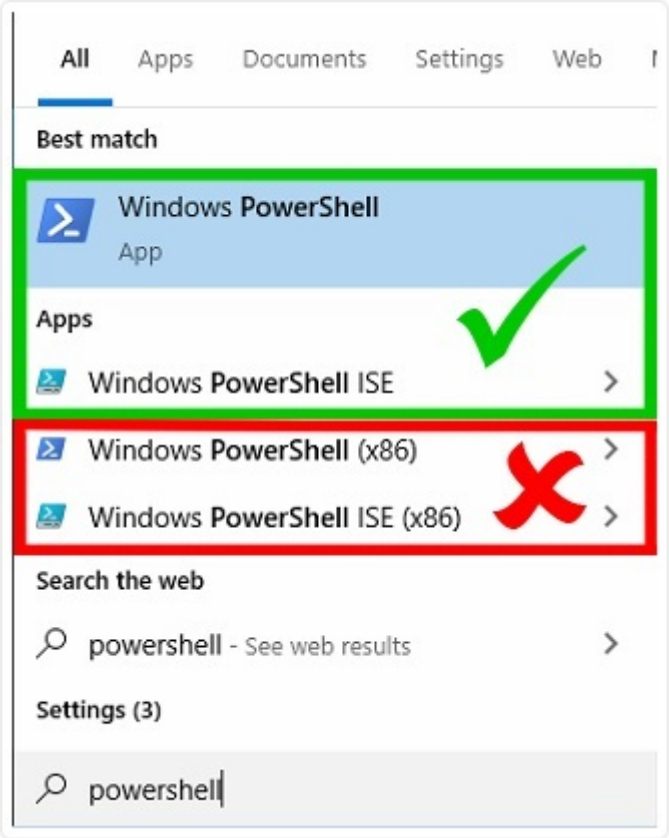
7. Some components used are installed with .bat files. Windows defender will also tend to block these portions of the installation. The installation will fail if you deny access.

8. Refer **IIS Settings Prerequisite** before configuring IIS.
   - **Warning**: WebDAV must NOT be installed in the IIS. WebDAV breaks our application. **DO NOT INSTALL WEB DAV**.

9. **PowerShell Permission Configuration:** The installation also requires the user to have execute permission on PowerShell scripts. Some Microsoft operating systems like Windows Server 2016 have these PowerShell script execution permission disabled by default. You must enable PowerShell script execution permission or setup will fail. To enable the privilege to execute Powershell scripts for the current user:
   a. In the Windows search box, type services.msc and run it.

b. In the list, search for Windows Remote Management (WS-Management). Right-click on it and then click on the Start button.

c. In the Windows search box, type powershell. Right-click either PowerShell or PowerShell ISE in the results shown (do not use either of the items with x86 in the name). Then Run As Administrator and click Yes in the User Account Control permission dialog.



d. Determine your current PowerShell script execution policy, and note it for future reference: Get-ExecutionPolicy

e. If your value (in above step **d**) is Unrestricted or RemoteSigned, skip to point **h** (no change is necessary).

f. Change the PowerShell script execution policy to Unrestricted (temporarily during install) and Set-ExecutionPolicy to Unrestricted -force

g. Click on the Yes button and press Enter.

h. After installation has completed, if you had to change the PowerShell script execution policy earlier in Step **5** set it back to the one from Step **4** (don't simply copy/paste the value below; use your own value), for example: Set-ExecutionPolicy Restricted.

Note: After successful installation, restore your initial Powershell settings.

10. While logged into the PC/server as a local administrator, right-click setup.exe, Run as Administrator. Refer the points below. If you receive an installation error, reboot the PC/server, then do this step again. If you get repeated errors, take screenshots and notes on the steps you took, and contact Wasp Tech Support.

    a. If a PowerShell window appears with a Security warning, asking if you want to run certain files with .ps1 extension, type R, Enter to allow that. You may need to do this multiple times before the automated process continues.

    b. The setup.exe installer is designed to recognize what components have already been installed, so it should be able to pick up where it left off, if the installation is interrupted or the PC is rebooted.

11. Set user-defined sa password in SQL Studio Management Studio (optional).

12. We strongly recommend a Firewall with one port open.

    - http (TCP) 8083 for InventoryCloud.

13. If the user want to use **mobile device** with On-Premise, they should

- Install IIS on the server.
- Make sure that each mobile device can access default site of the IIS in the mobile using the build in Mobile Web Browser (like Safari on Apple Chrome on Android.) This guarantees connectivity.
- If connectivity issues arise Computer name changes and/or IP Address changes may be required by customer IT. Such changes should ideally be made before running the Wasp On-Premise installer to ensure a smooth server installation.

14. Make sure that the character limit of your device/computer name should be 15 or less for successful On-premise installation.

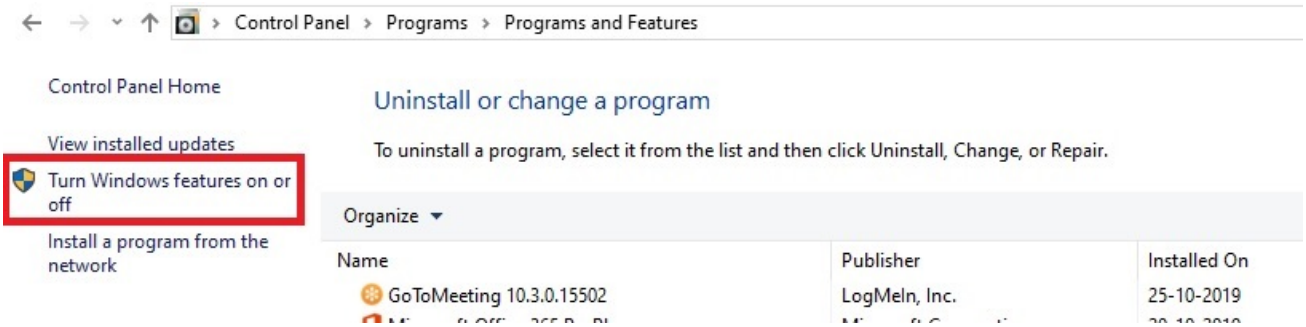
IIS Settings Prerequisite

Following settings should be configured in Internet Information Services (IIS) before installing the On-Premise version of InventoryCloud.

Warning: WebDAV must NOT be installed in the IIS. WebDAV breaks our application. **DO NOT INSTALL WEB DAV**.

1. In Windows Server 2012 R2, Windows Server 2016 and onwards - Open **Server Manager** > **Dashboard** > **Manage** > **Add roles and features**.

   In Windows 8.1 and Windows 10 - Open **Control Panel** > **Programs** > **Programs and Features** > **Turn Windows features on or off**.



- Expand the Internet Information Services feature.
- Verify that the IIS components listed below are turned on. If these components are not enabled, the installation will not proceed.

2. **For Windows Server 2016 and onwards** - Enable the following roles & features in Server Manager. You can enable most other features with no negative impact. **Exception: DO NOT enable WebDAV Publishing.**

   Note - Make sure the following are selected: .NET Framework 3.5 and 4.7 or 4.8, ASP.Net, Web Management tools, Server Side Includes WebSocket protocol. Also note that, in a single server scenario, our web products do not require file sharing.

Select server roles

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select one or more roles to install on the selected server.

Roles

- [ ] Fax Server
- [■] File and Storage Services (1 of 12 installed)
  - [ ] File and iSCSI Services
  - [✓] Storage Services (Installed)
- [ ] Host Guardian Service
- [ ] Hyper-V
- [ ] Network Policy and Access Services
- [ ] Print and Document Services
- [ ] Remote Access
- [ ] Remote Desktop Services
- [ ] Volume Activation Services
- [■] Web Server (IIS) (16 of 43 installed)
  - [■] Web Server (15 of 34 installed)
    - [■] Common HTTP Features (4 of 6 installed)
      - [✓] Default Document (Installed)
      - [✓] Directory Browsing (Installed)
      - [✓] HTTP Errors (Installed)
      - [✓] Static Content (Installed)
      - [ ] HTTP Redirection

Roles

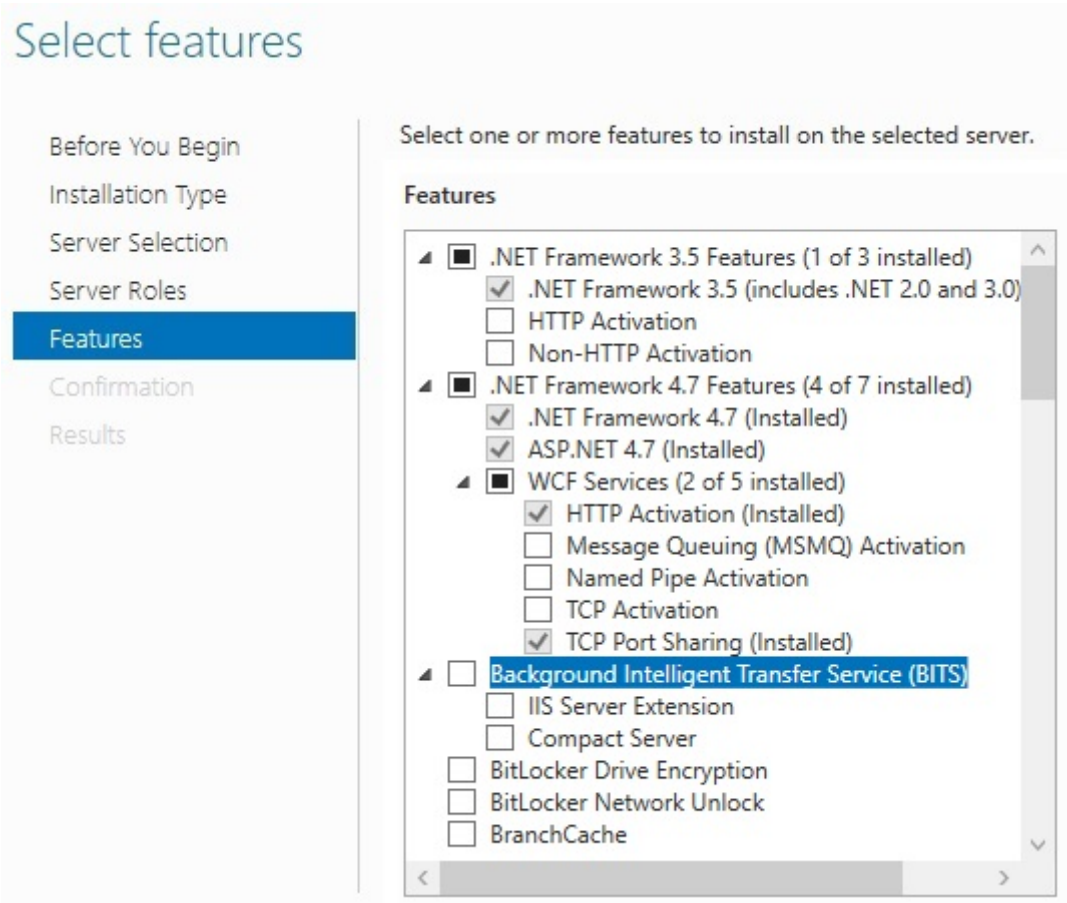
- [ ] HTTP Redirection
- [ ] WebDAV Publishing
- [■] Health and Diagnostics (1 of 6 installed)
  - [✓] HTTP Logging (Installed)
  - [ ] Custom Logging
  - [ ] Logging Tools
  - [ ] ODBC Logging
  - [ ] Request Monitor
  - [ ] Tracing
- [■] Performance (1 of 2 installed)
  - [✓] Static Content Compression (Installed)
  - [ ] Dynamic Content Compression
- [■] Security (1 of 9 installed)
  - [✓] Request Filtering (Installed)
  - [ ] Basic Authentication
  - [ ] Centralized SSL Certificate Support
  - [ ] Client Certificate Mapping Authenticati
  - [ ] Digest Authentication
  - [ ] IIS Client Certificate Mapping Authentic

Roles

- [ ] IIS Client Certificate Mapping Authentic
- [ ] IP and Domain Restrictions
- [ ] URL Authorization
- [ ] Windows Authentication
- [■] Application Development (8 of 11 installed)
  - [✓] .NET Extensibility 3.5 (Installed)
  - [✓] .NET Extensibility 4.7 (Installed)
  - [ ] Application Initialization
  - [✓] ASP (Installed)
  - [✓] ASP.NET 3.5 (Installed)
  - [✓] ASP.NET 4.7 (Installed)
  - [ ] CGI
  - [✓] ISAPI Extensions (Installed)
  - [✓] ISAPI Filters (Installed)
  - [ ] Server Side Includes
  - [✓] WebSocket Protocol (Installed)
- [ ] FTP Server
- [■] Management Tools (1 of 7 installed)
  - [✓] IIS Management Console (Installed)

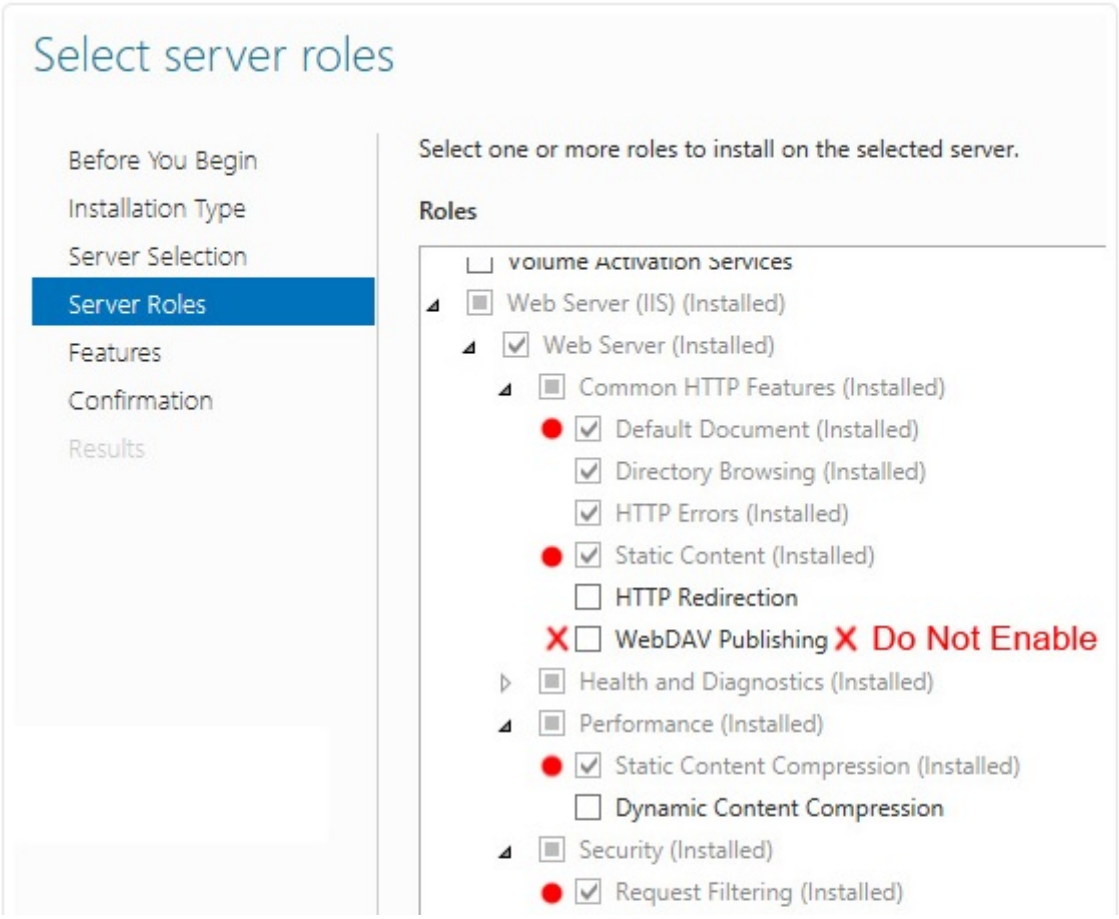
Roles

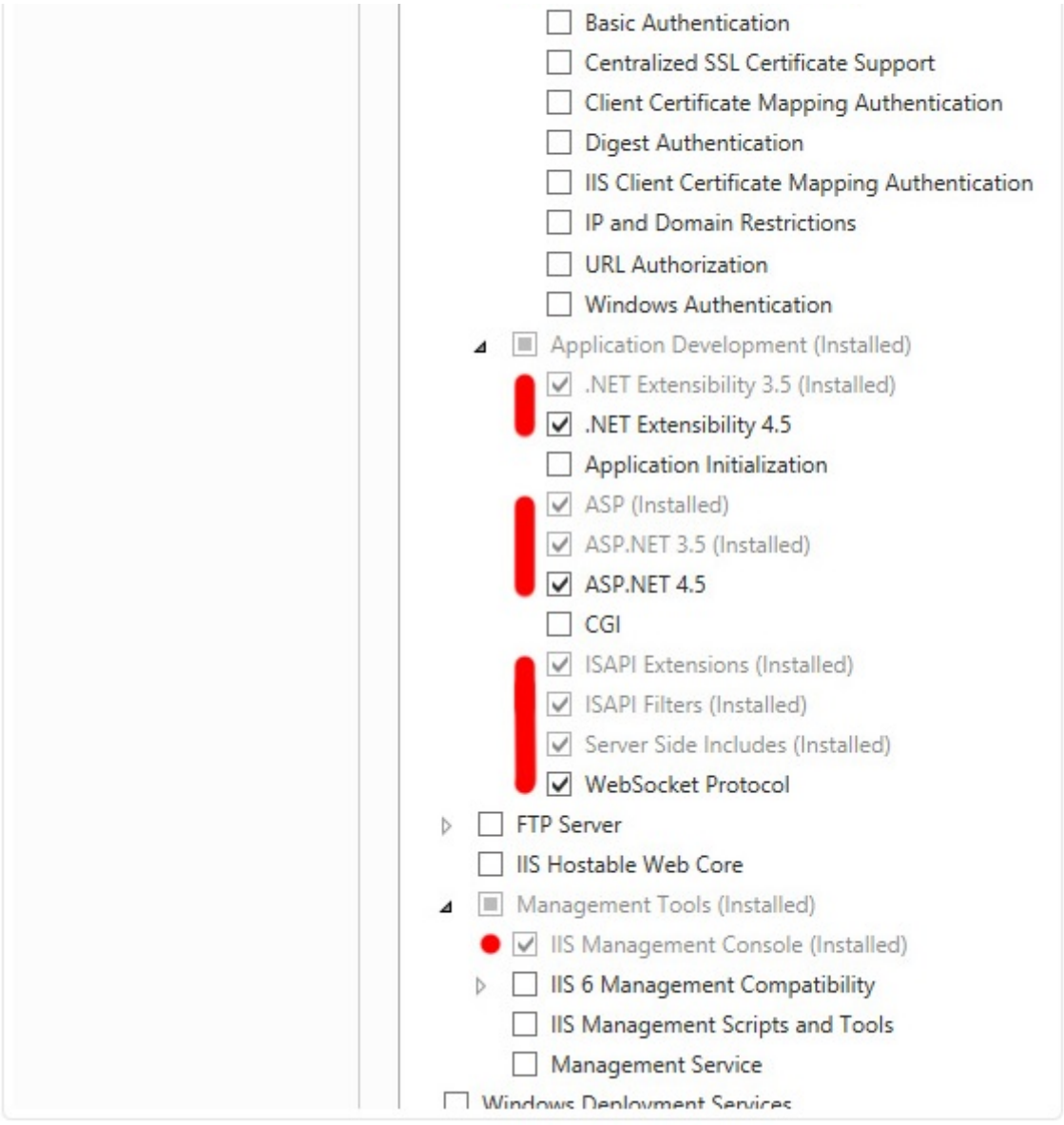
- [✓] .NET Extensibility 3.5 (Installed)
- [✓] .NET Extensibility 4.7 (Installed)
- [ ] Application Initialization
- [✓] ASP (Installed)
- [✓] ASP.NET 3.5 (Installed)
- [✓] ASP.NET 4.7 (Installed)
- [ ] CGI
- [✓] ISAPI Extensions (Installed)
- [✓] ISAPI Filters (Installed)
- [ ] Server Side Includes
- [✓] WebSocket Protocol (Installed)
- [ ] FTP Server
- [■] Management Tools (1 of 7 installed)
  - [✓] IIS Management Console (Installed)
  - [ ] IIS 6 Management Compatibility
  - [ ] IIS Management Scripts and Tools
  - [ ] Management Service
- [ ] Windows Deployment Services
- [ ] Windows Server Update Services

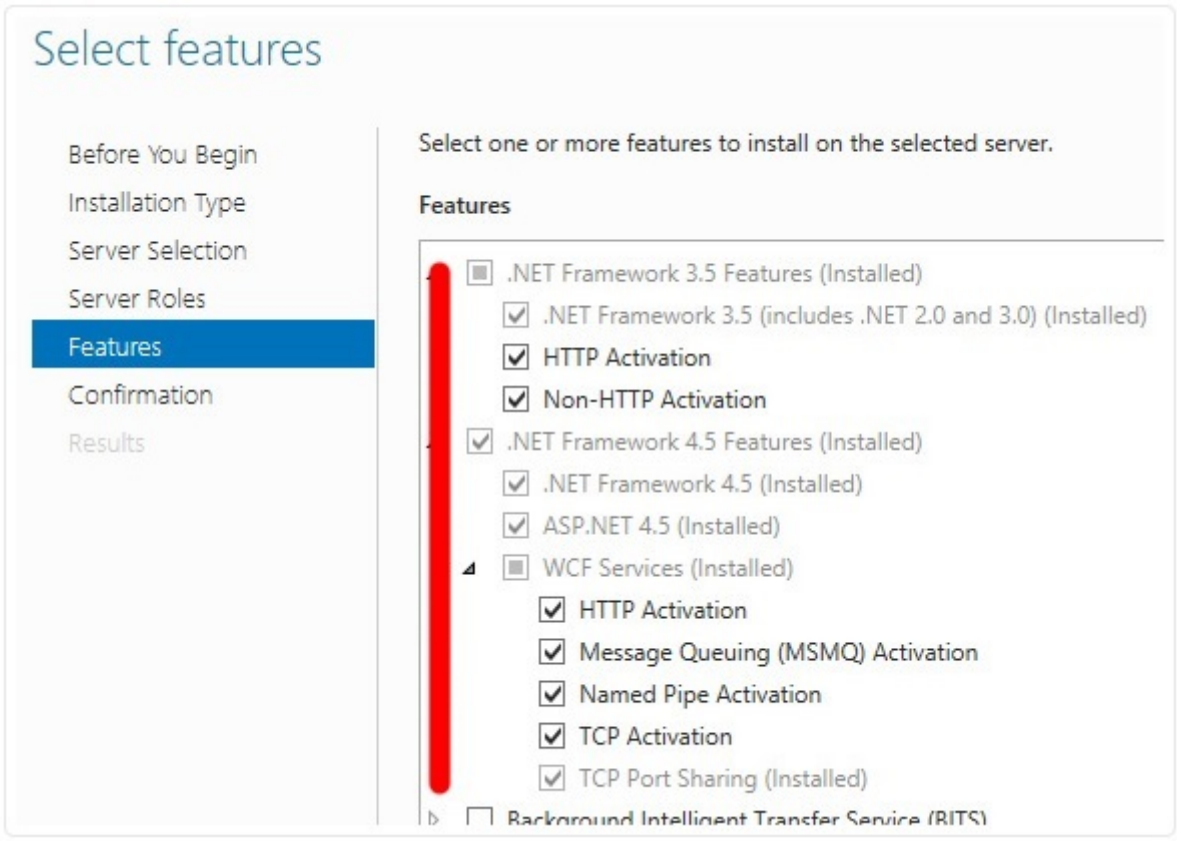


For Windows Server 2012 R2 - **E**nable the following roles & features in Server Manager. You can enable most other features with no negative impact. Exception: DO NOT enable WebDAV Publishing.

Note - Make sure the following are selected: .NET Framework 3.5 and 4.5-4.8 or whatever is there., Web Management tools, Server Side Includes WebSocket protocol



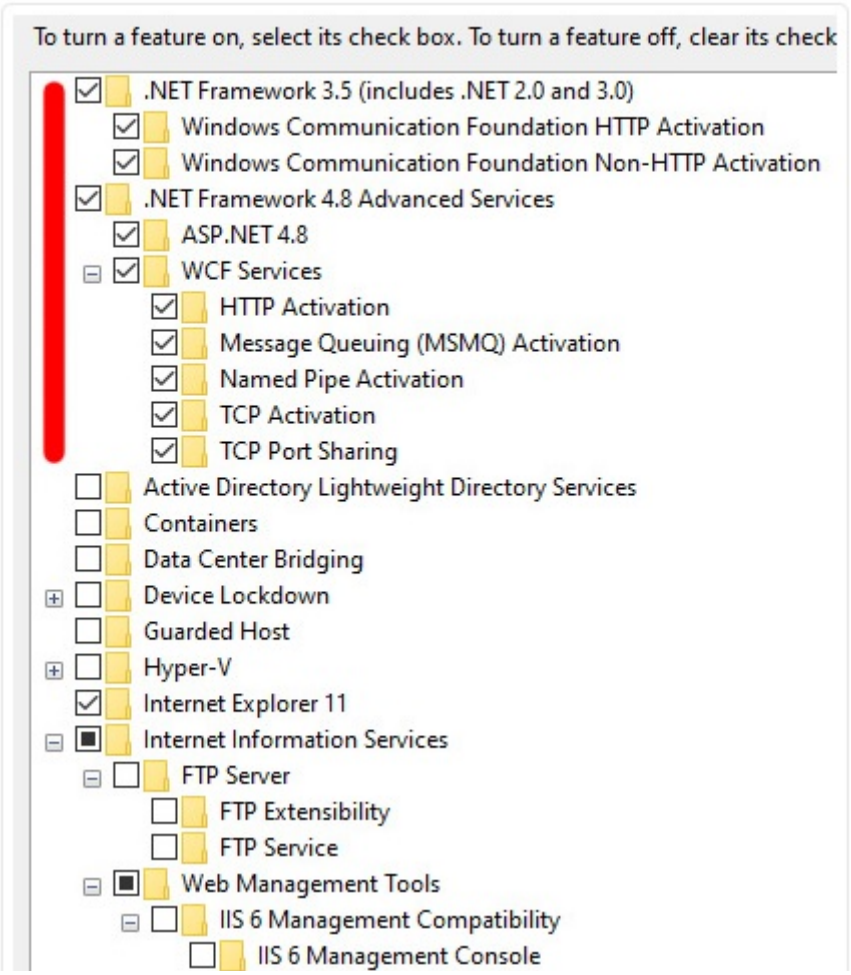

Basic Authentication
Centralized SSL Certificate Support
Client Certificate Mapping Authentication
Digest Authentication
IIS Client Certificate Mapping Authentication
IP and Domain Restrictions
URL Authorization
Windows Authentication
Application Development (Installed)
.NET Extensibility 3.5 (Installed)
.NET Extensibility 4.5
Application Initialization
ASP (Installed)
ASP.NET 3.5 (Installed)
ASP.NET 4.5
CGI
ISAPI Extensions (Installed)
ISAPI Filters (Installed)
Server Side Includes (Installed)
WebSocket Protocol
FTP Server
IIS Hostable Web Core
Management Tools (Installed)
IIS Management Console (Installed)
IIS 6 Management Compatibility
IIS Management Scripts and Tools
Management Service
Windows Deployment Services

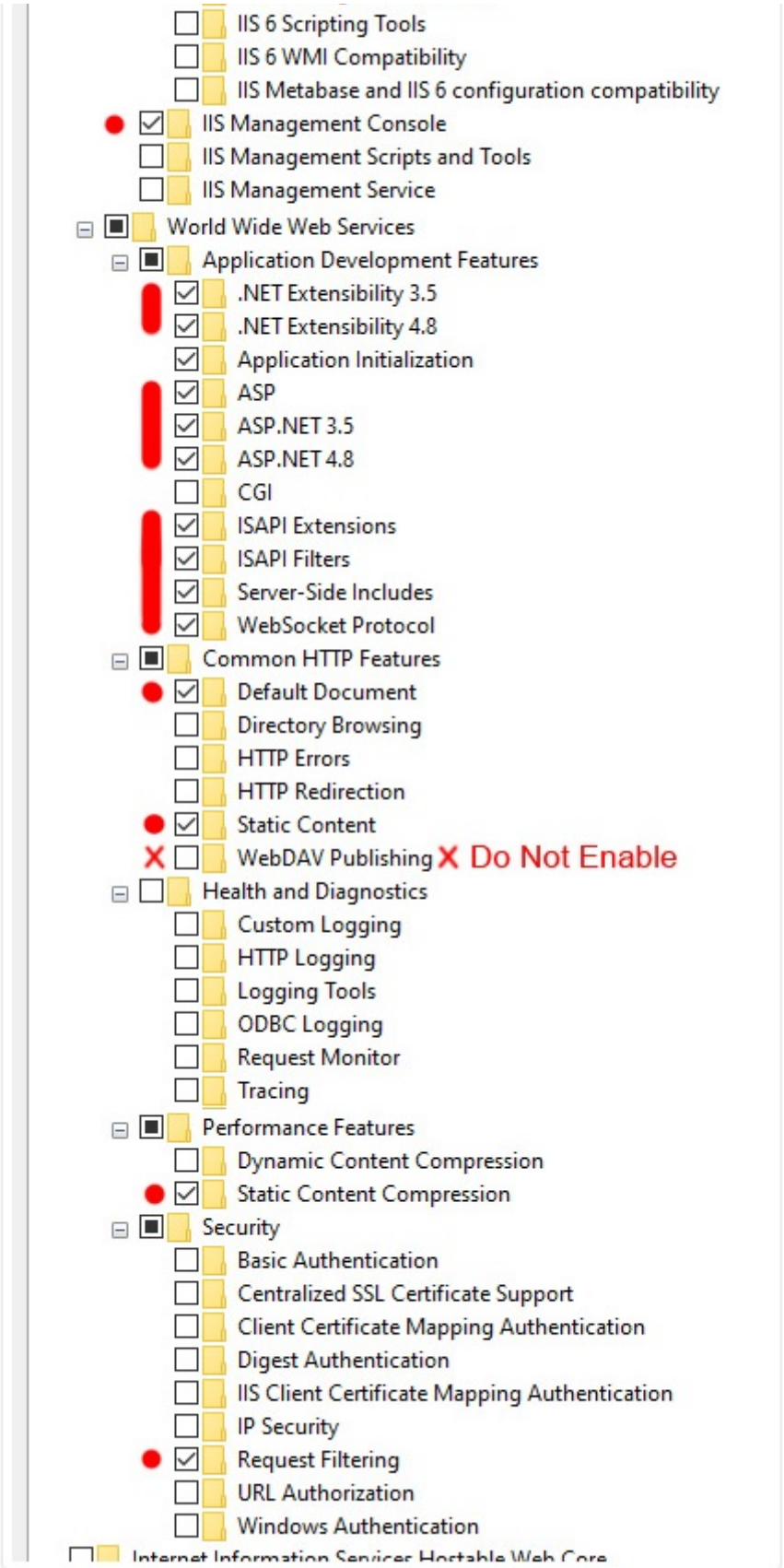


When the features are checked, click OK, and wait until the installation is complete. Go on to Step 3.

-

For Windows 10 - Enable the following features: Open the Programs and Features control panel, then click Windows Features at the left. You can enable most other features with no negative impact. **Exception**: DO NOT enable WebDAV Publishing.





When the features are checked, click OK, and wait until the installation is complete. Go on to Step 3.

3. Reboot the computer. If there are any Windows Updates that are available, perform them at this time. After the reboot, open Windows Features or Server Manager again and confirm all the above-specified features are still checked/enabled. If they're not, enable them again, then repeat this step.

4. Test to verify that you can access the default web page of IIS (on port 80) from ALL devices you wish to use to access your On-Premise software, especially Android and iOS devices. Verify that the URL used to access the site is the URL you wish to continue using to access your Wasp Cloud OnPremise product.

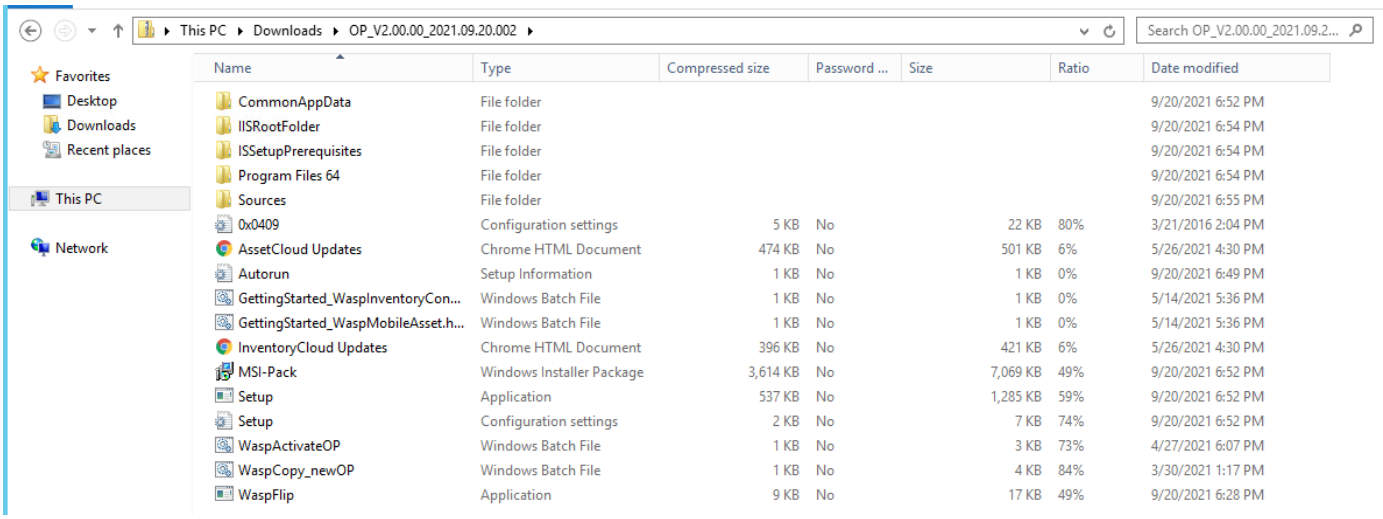
5. After successful testing, return to **Prerequisites** to continue with installation steps.

Installation Files

The installation package comes as a .zip file or you can install it from disk ISO. Unzip the file before you start installing.

Note – Do not Unzip the file on the desktop. It is safer to unzip to the system drive root. We do not support installing from a network drive at this time.

The .zip file contains the following files



Installation Steps

Follow the steps to install the InventoryCloud OP application:

1. Click on the **Setup** file.

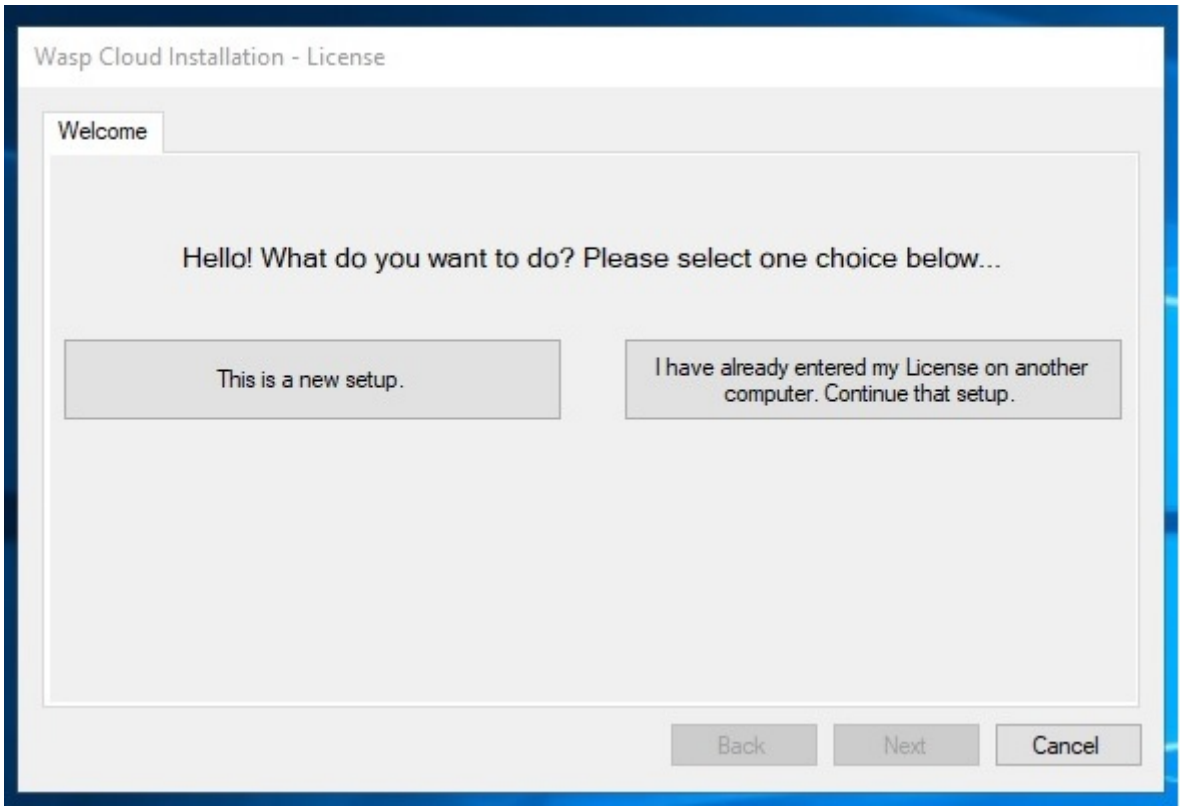
   Note: It is necessary to open the Setup file as an administrator (right-click - 'Run as administrator'). The user executing the Setup himself should also be a member of the machine administrators group.

2. The Wasp On-Premise Software - InstallShield Wizard will appear. Click on the **Install** button. The following requirement will get installed on your computer - vcredistX64.exe (a Microsoft Visual C++ 2010 x64 Redistributable Setup).

3. The Installation of Wasp On-premises Software requires a reboot. Click **Yes** to restart the computer.

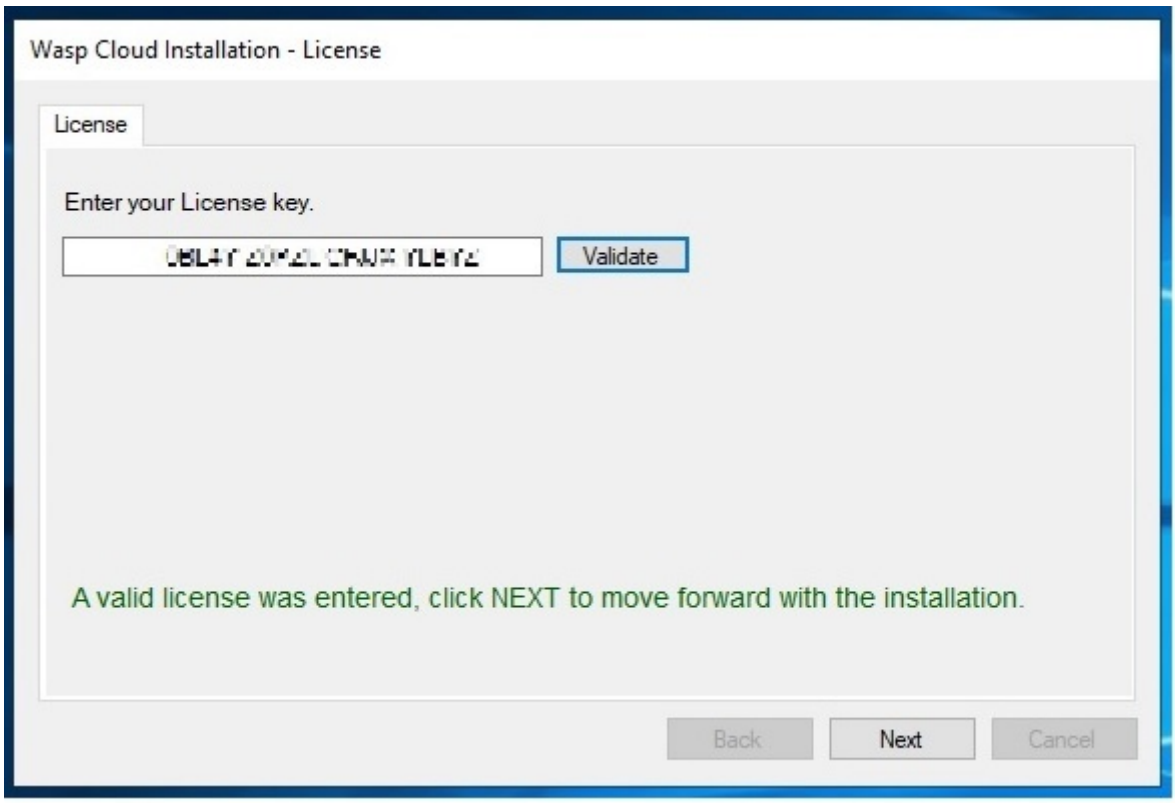
4. A welcome screen will appear where there will be two choices – "*This is a new setup*." and "*I have already entered my License on another computer. Continue that setup*.". Since the setup is new, choose "***This is a new setup***."

   If the setup is not new and the License is already entered, skip to **Step 21**.

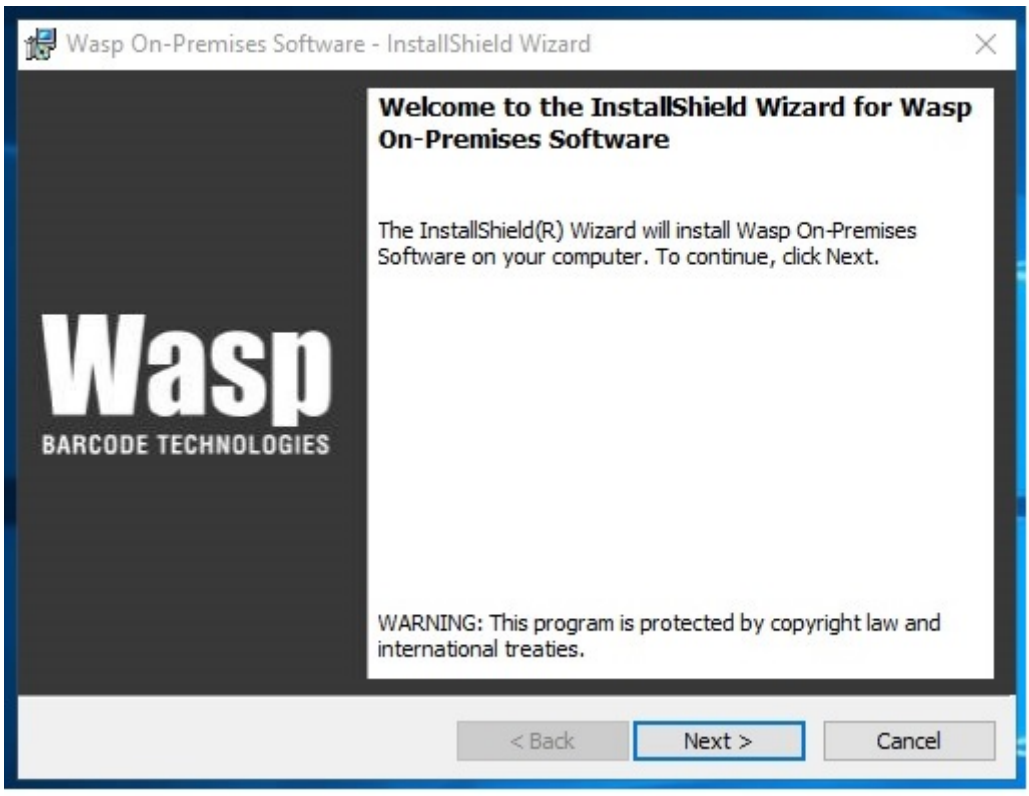


This is a new setup

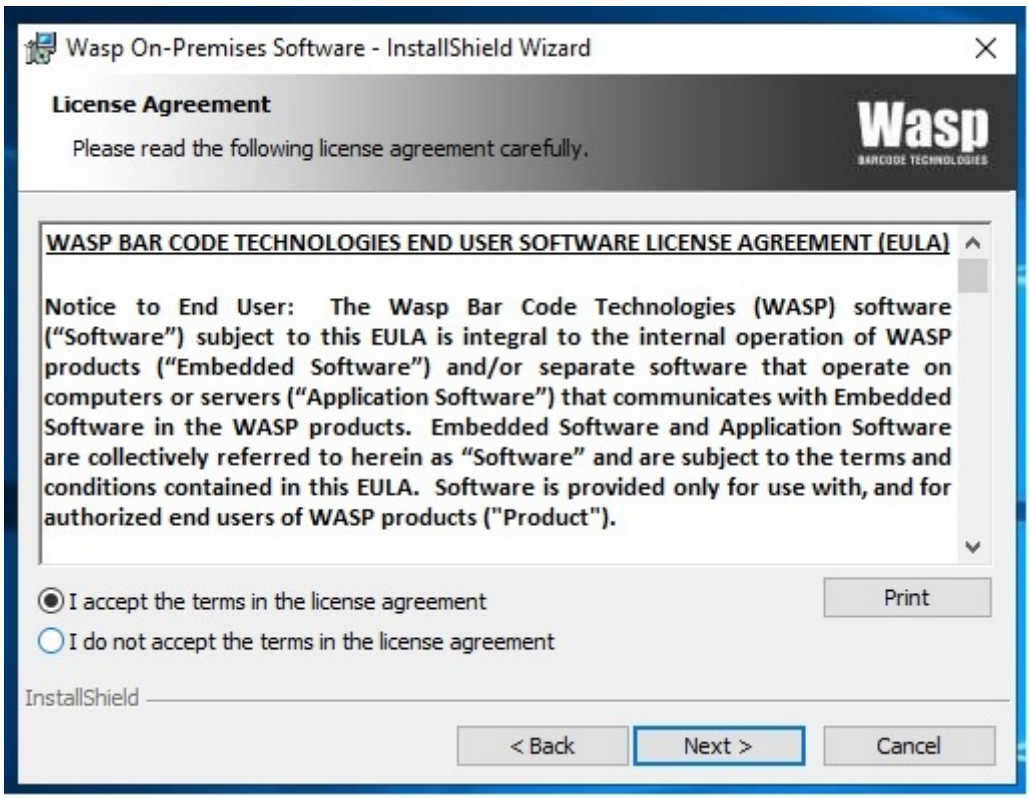
5. Enter your License key. Click **Validate**. A message will appear indicating that the "A valid license is entered and click Next to move forward with the installation. Click **Next**.



6. Wasp On-premise Software – Installshield Wizard will appear. It will install Wasp On-premise Software on your computer. Click **Next**.

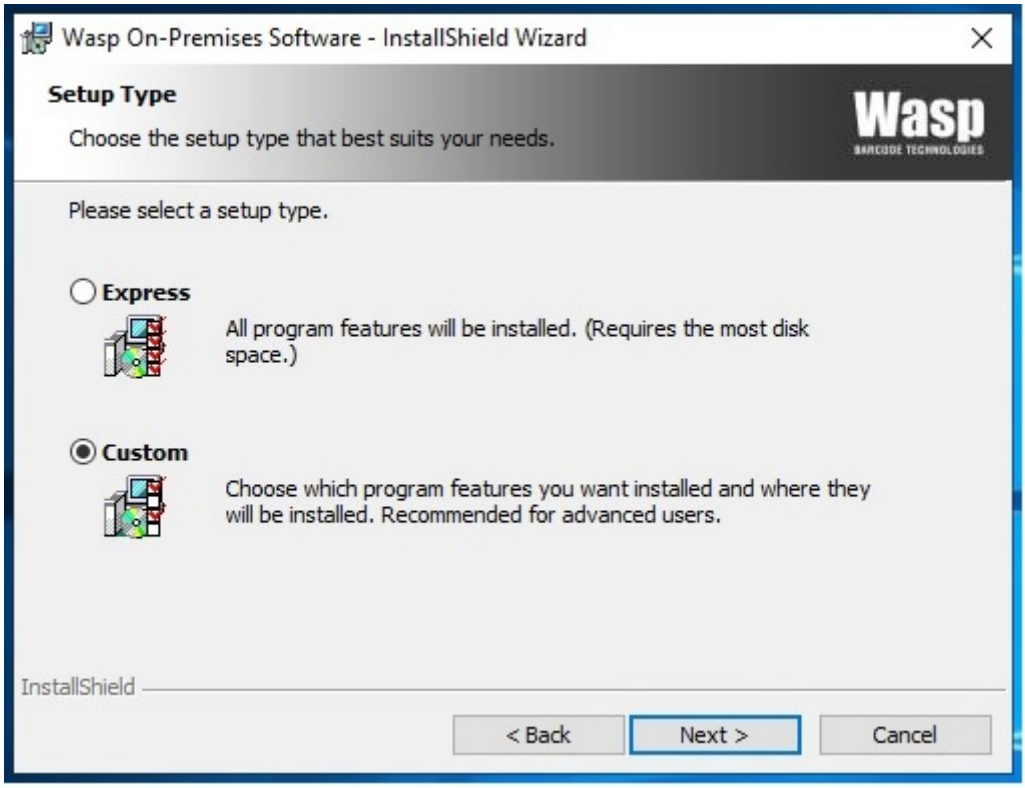


7. To proceed with the setup, you must accept the terms in the License Agreement. Please read the license agreement carefully and click on the radio button and then click **Next**.



8. Choose the setup that best suits your needs. The options are **Express** and **Custom**.

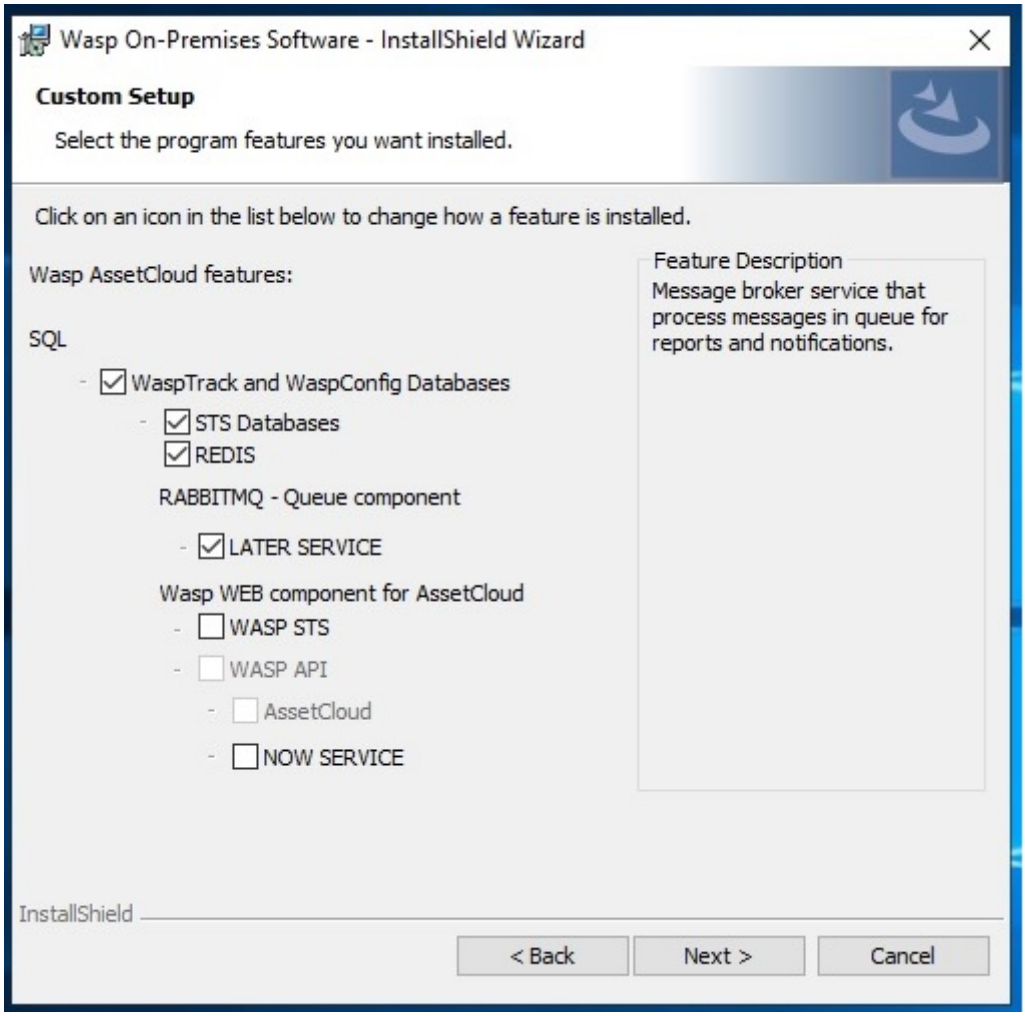
- **Express** – All program features will be installed. The 'Express' setup is recommended for all new or inexperienced users.
- **Custom** – You can choose the program features that you want to install and also you can choose the location where you want it installed. The Custom setup is **only** recommended for advanced users.



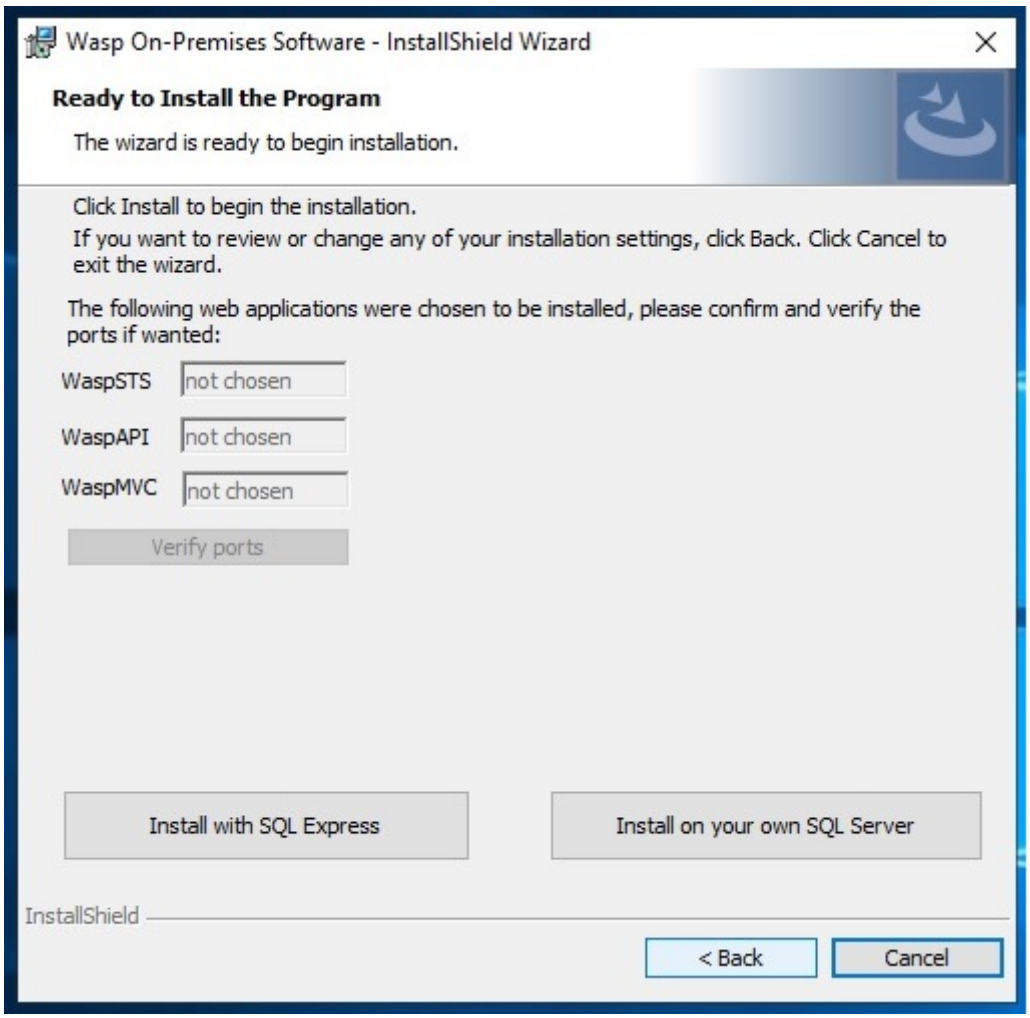
Installing Custom Setup:

9. Select **Custom** and click **Next**.

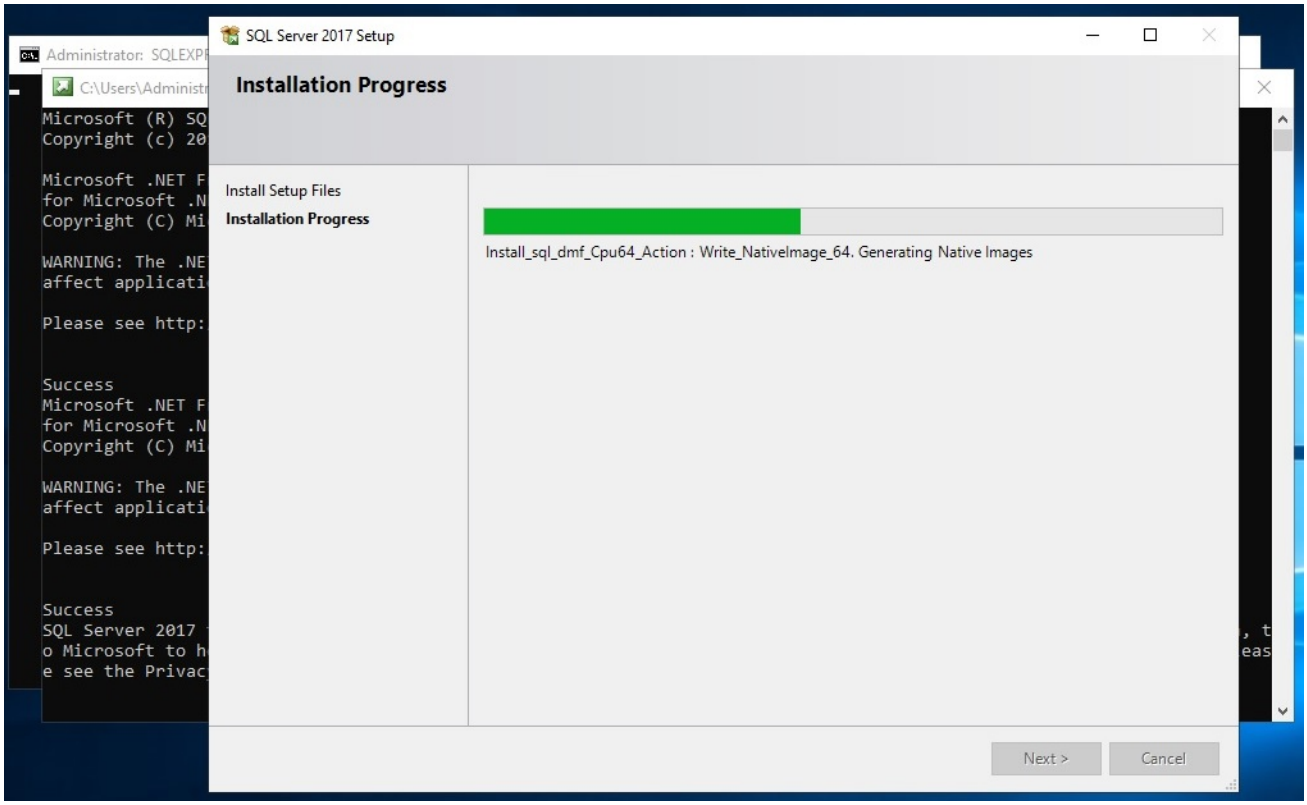
10. Select the program feature that you want to install. Consider that we are installing the first 4 features as shown in the image.



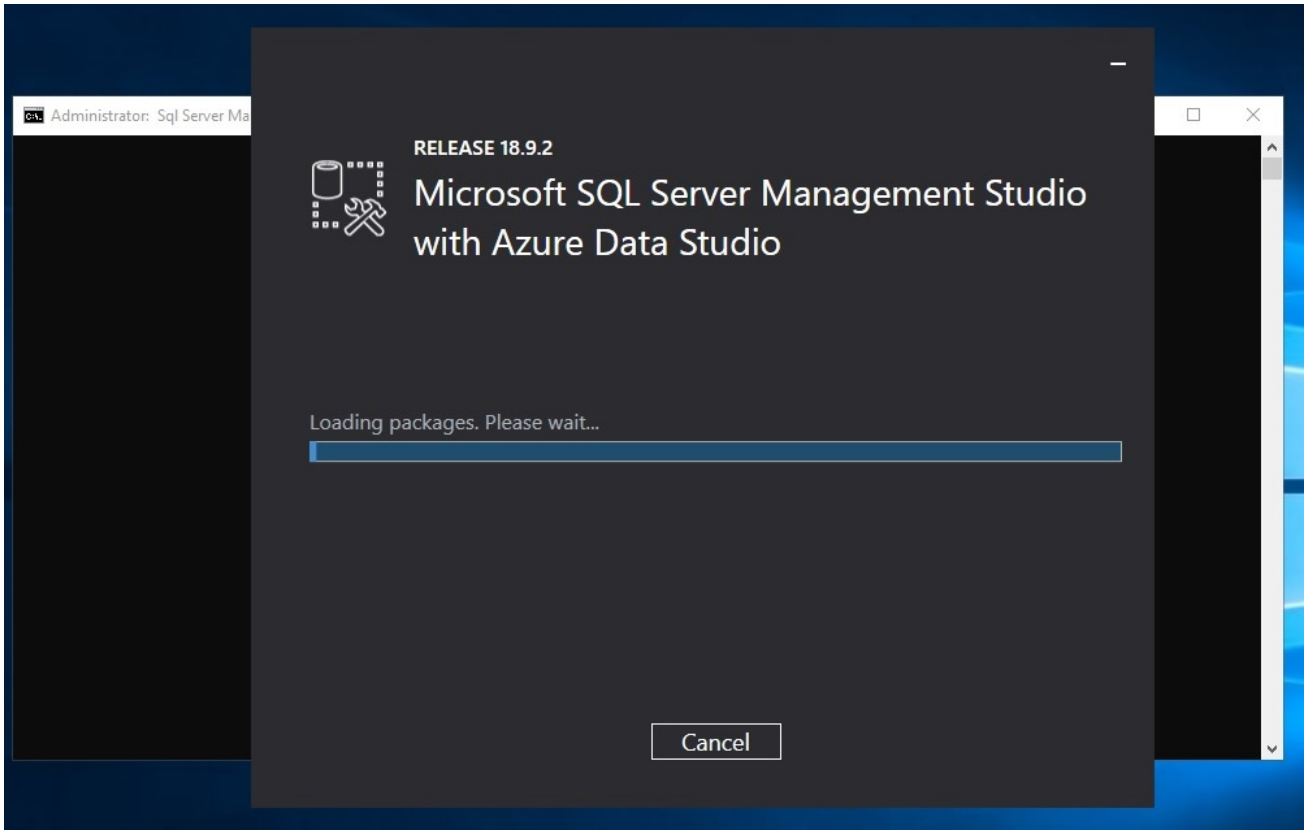
11. Select **Install with SQL Express.**



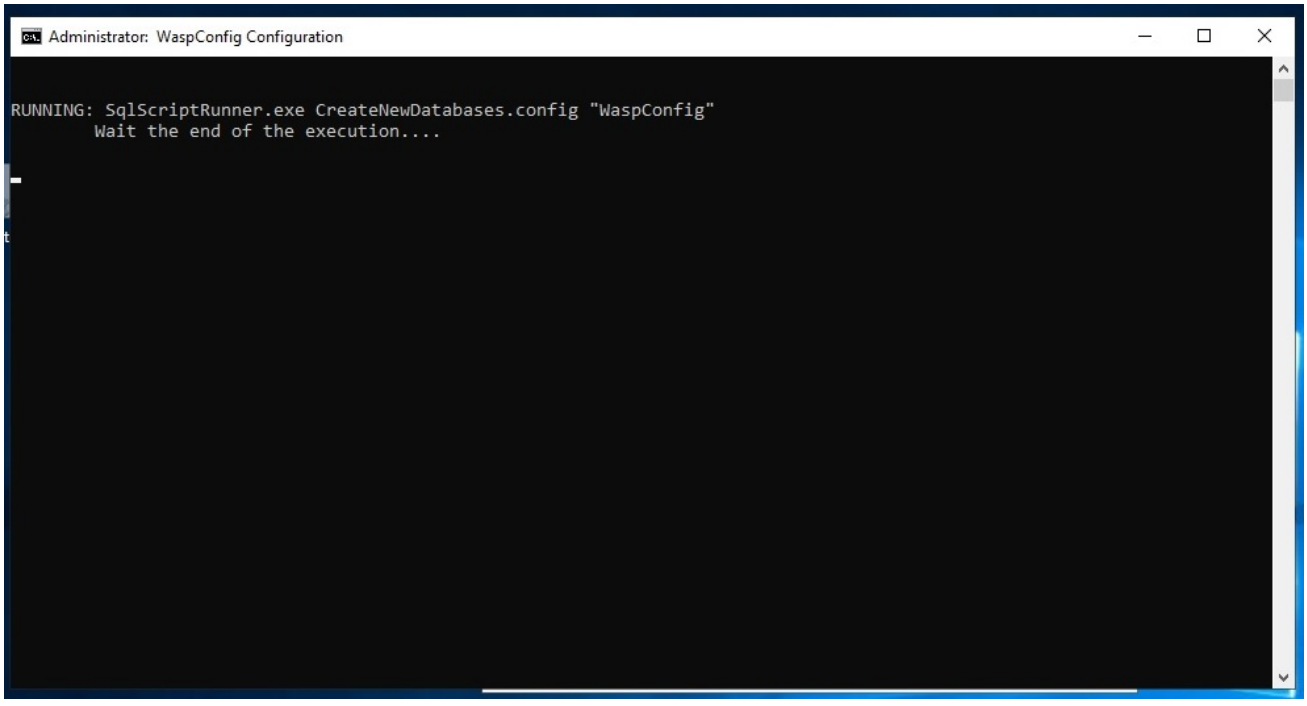
12. The Setup files and the Installation progress of the SQL Server 2017 will appear.



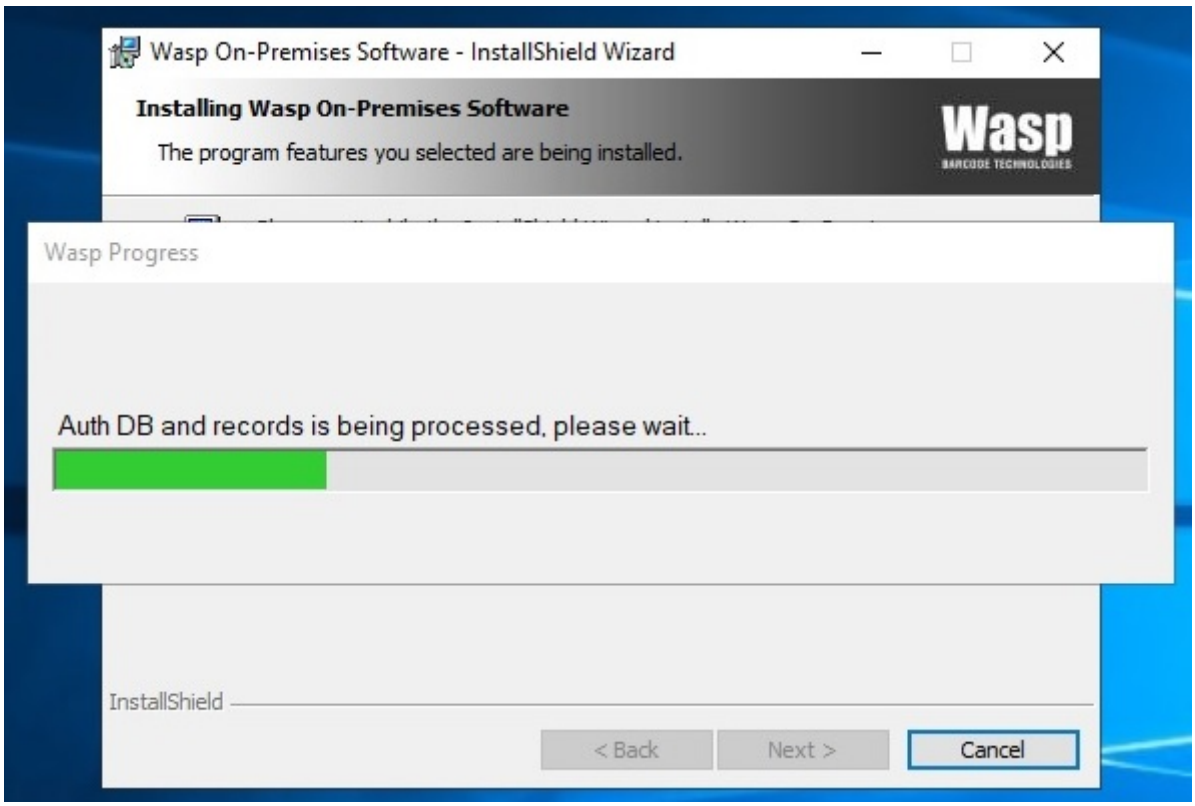
The SQL Server Management Studio with Azure Data Studio will install.



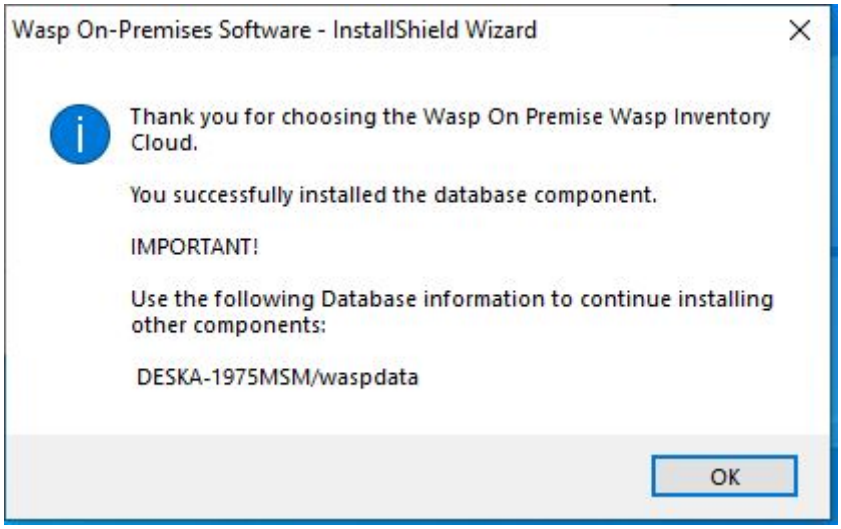
13. You will see the scripts running in the WaspConfig Configuration screen.



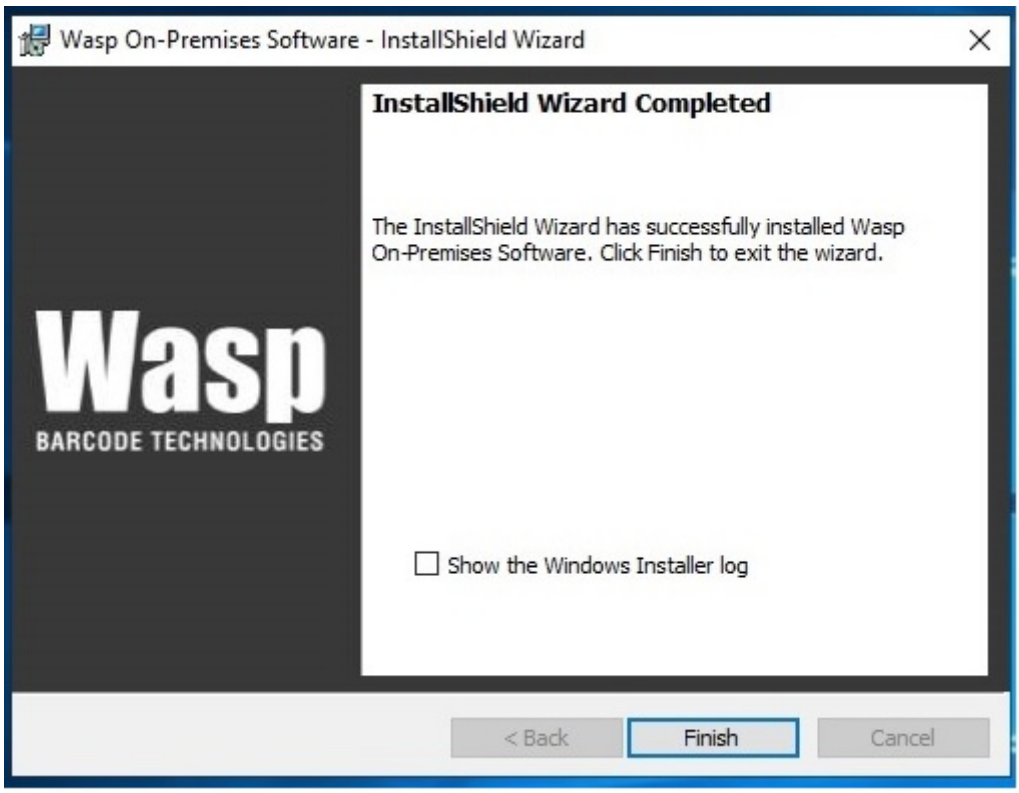
14. Also, you will see the Wasp Progress screen where AuthDB and records are being processed.



15. The installer will display the DatabaseName with instance info here. Refer to topic Steps to find the SQL database and instance.

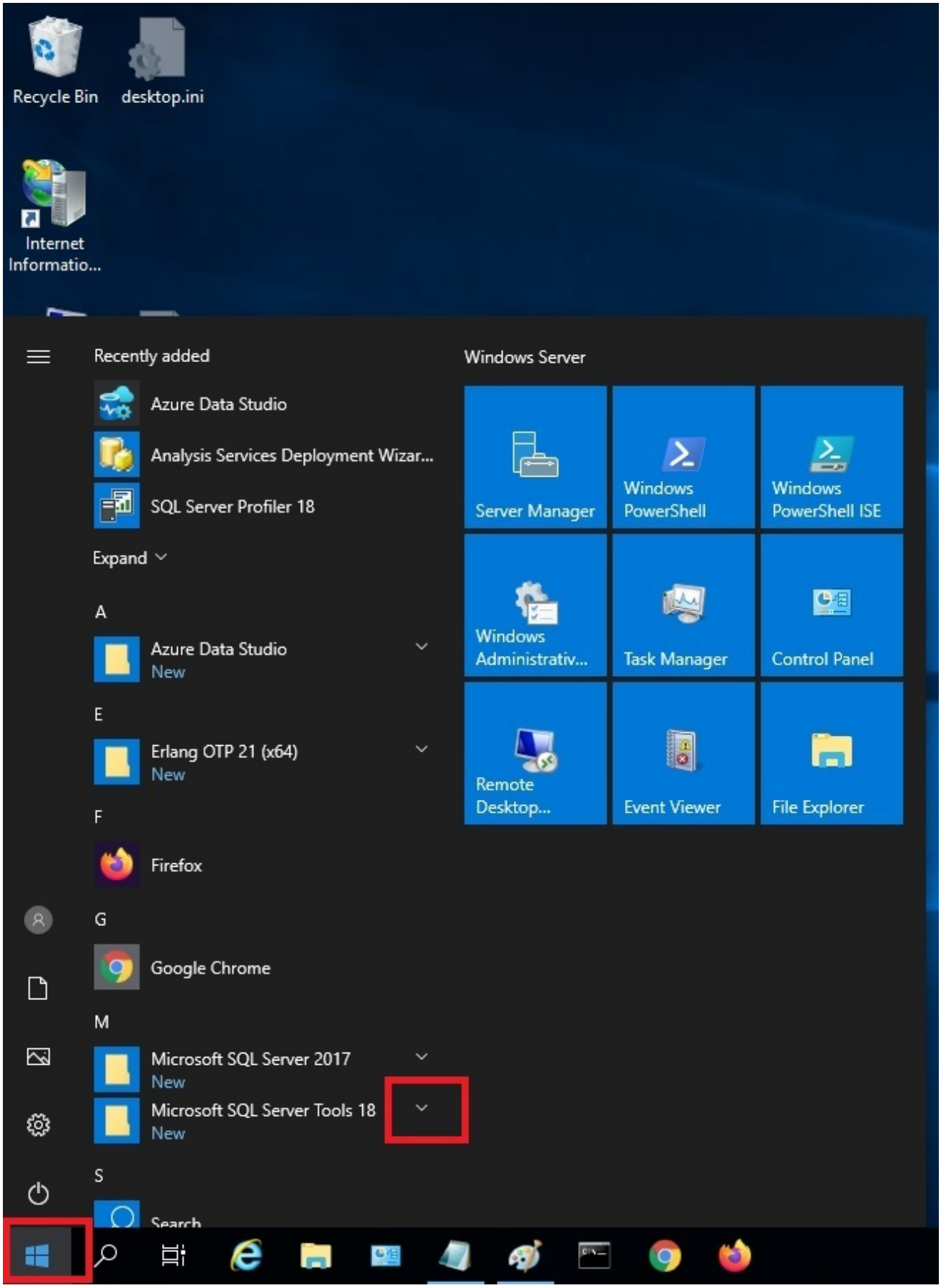


The Wasp On-Premise Software - InstallShield Wizard will appear again indicating that the Wasp On-premise software is installed.

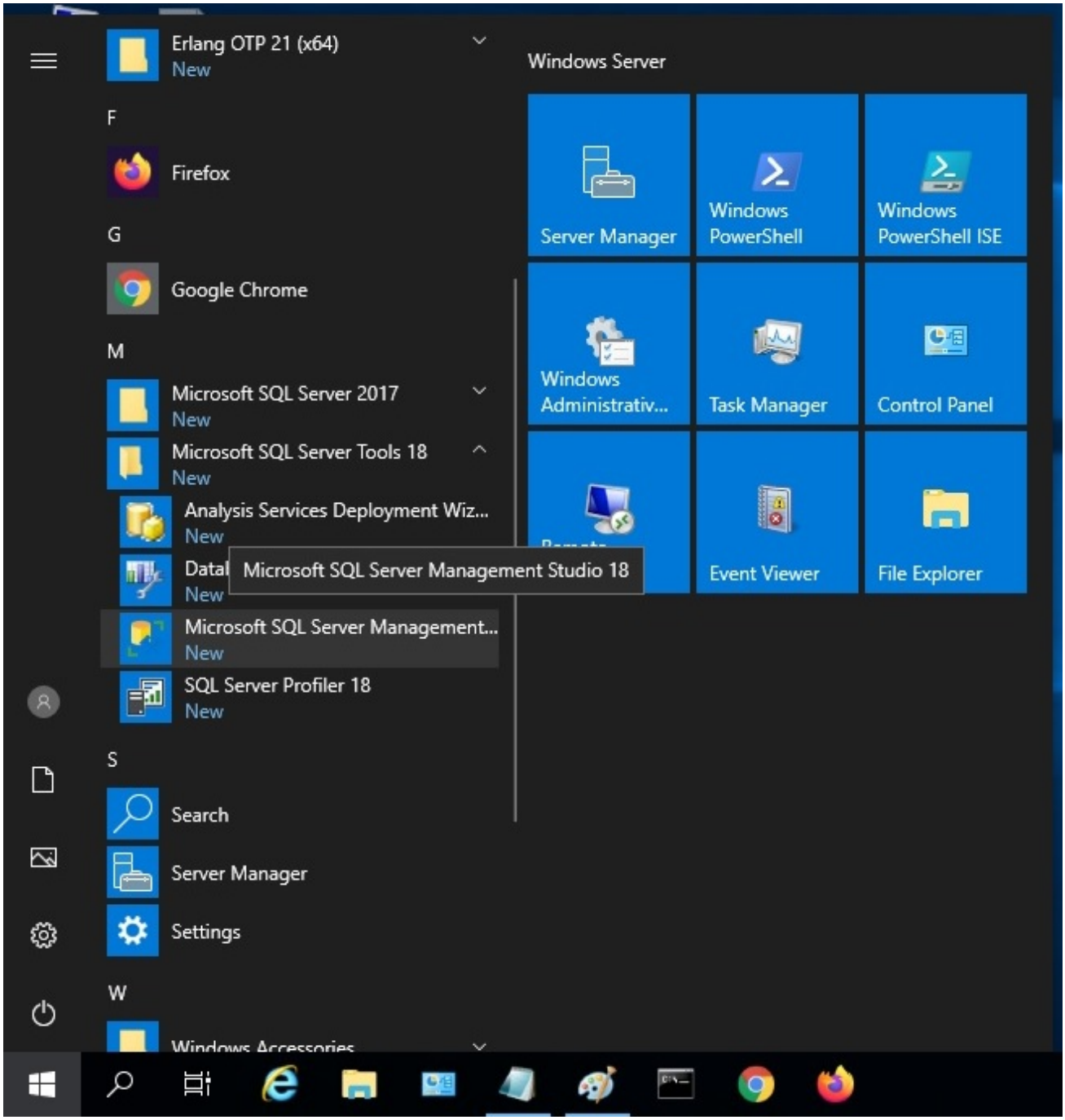


Steps to find the SQL database and instance

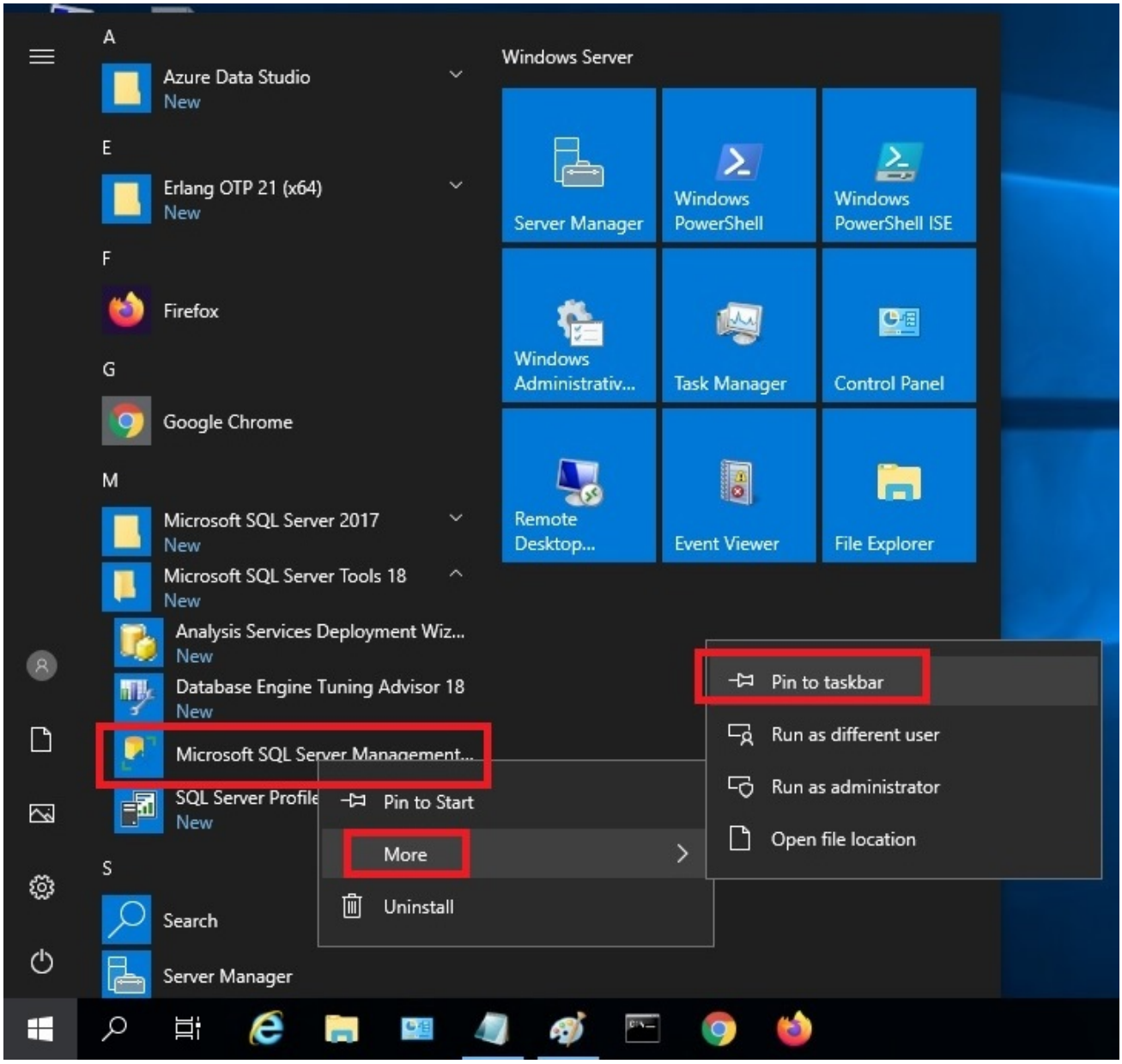
16. To find the SQL database and instance, select **Start** menu and Expand **Microsoft SQL Server Tools 18**.



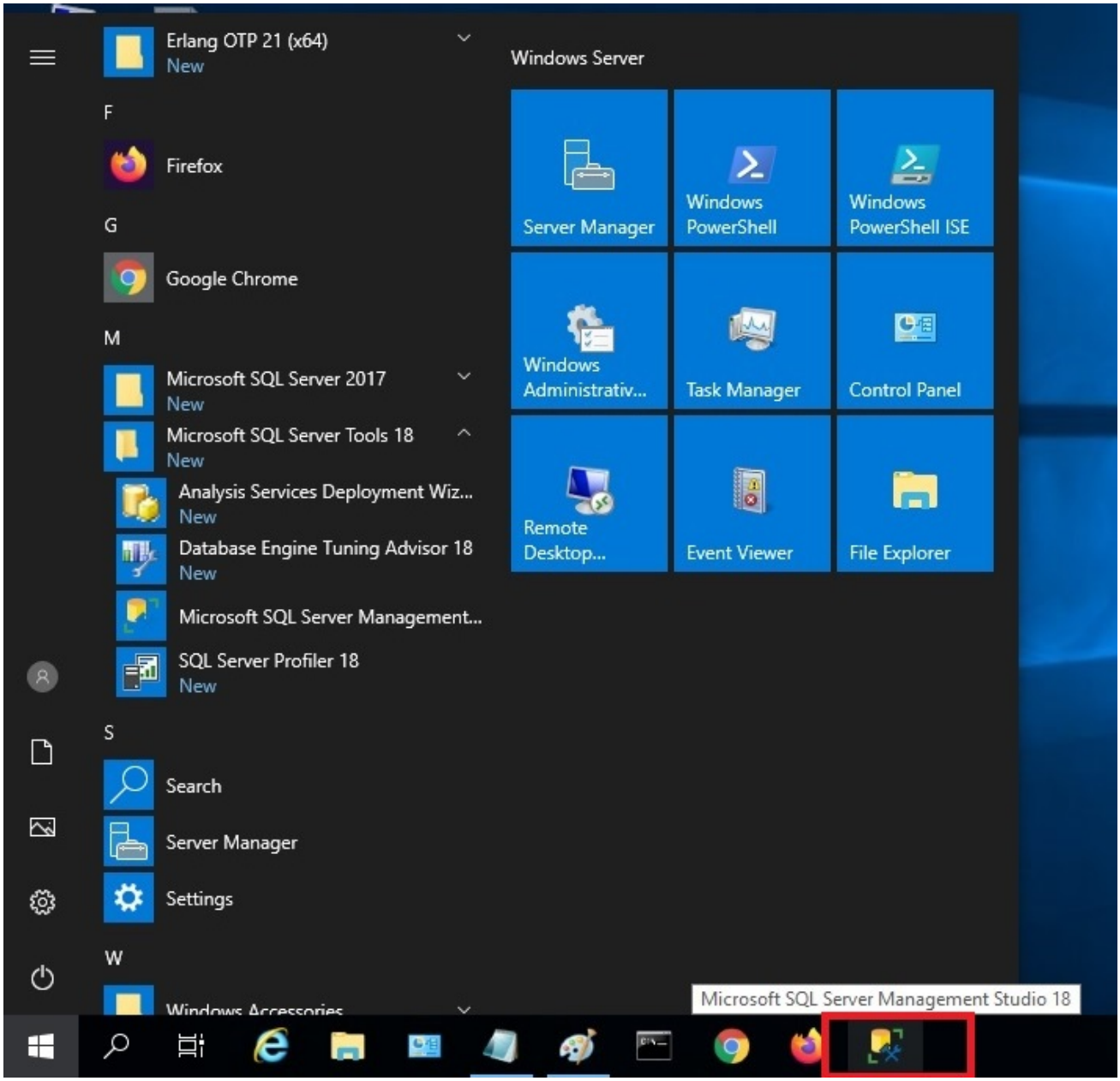
17. Locate 'Microsoft SQL Server Management Studio 18'.



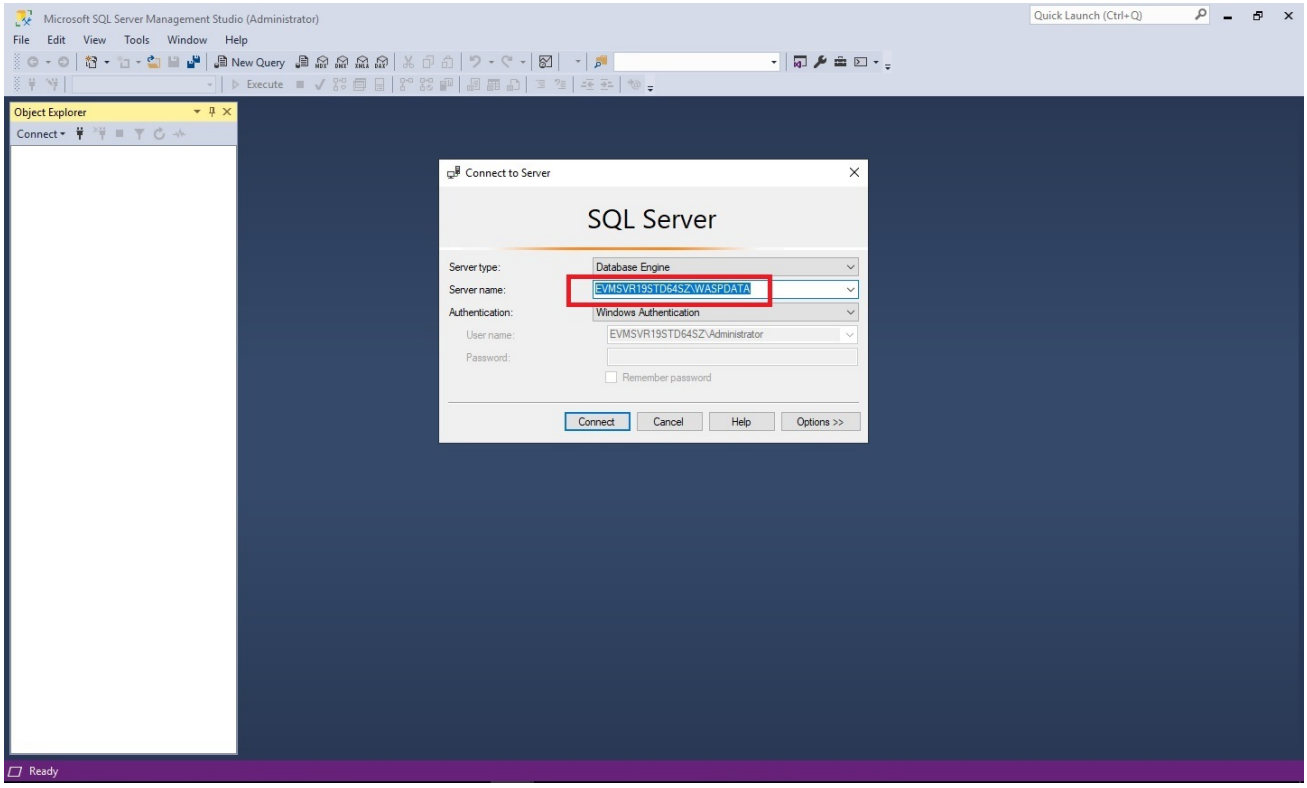
18. Right-click on 'Microsoft SQL Server Management Studio 18' and select More & Pin to Taskbar.



19. The 'Microsoft SQL Server Management Studio 18 (SSMS) icon appears on the Taskbar.

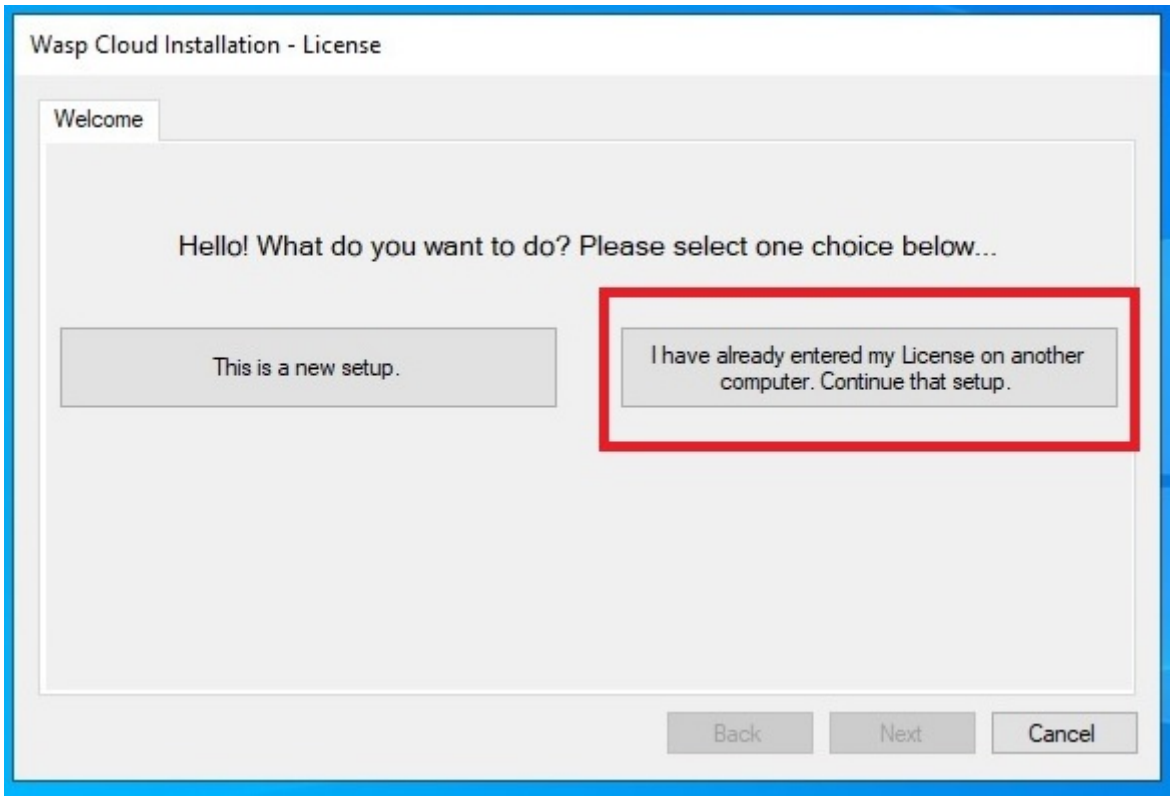


20. Click on the SSMS icon in the taskbar. **Note down the Server name which can be used to install the On-Premise software on other computers.**

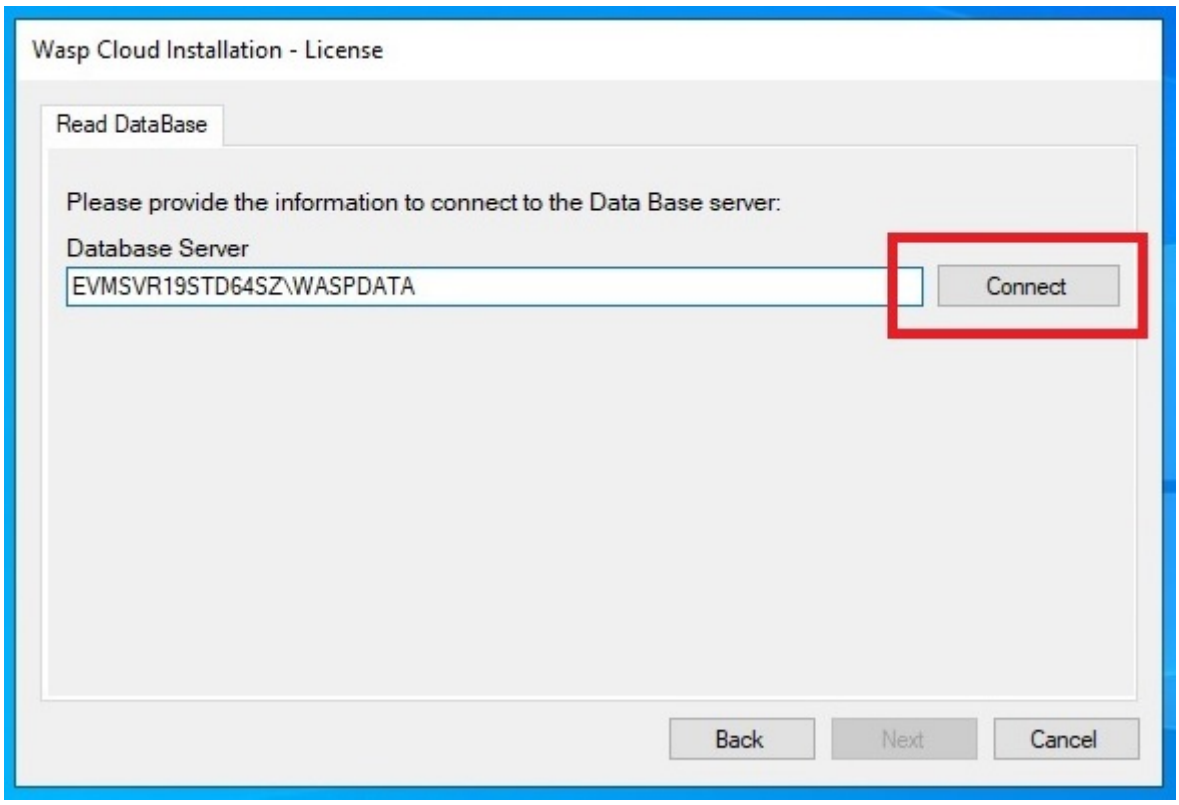


I have already entered my License on another computer. Continue that setup – Consider that we are installing the last 4 features on another computer and the license is already entered into another computer.

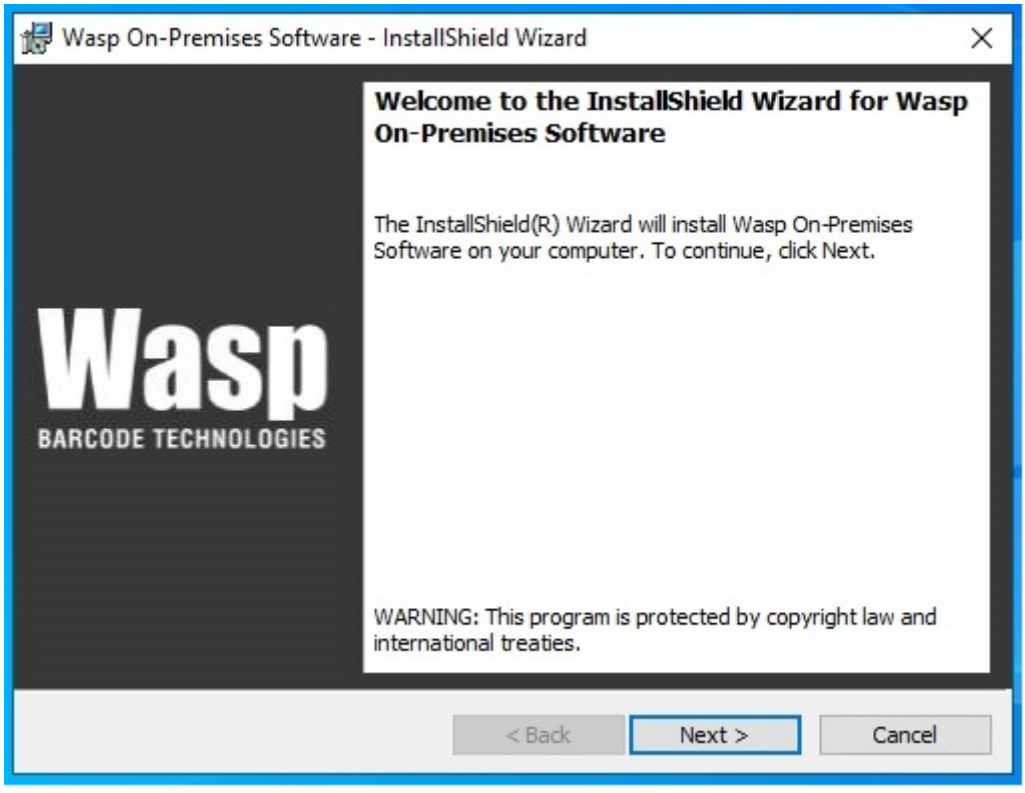
21. Select ***'I have already entered my License on another computer. Continue that setup**.'*.



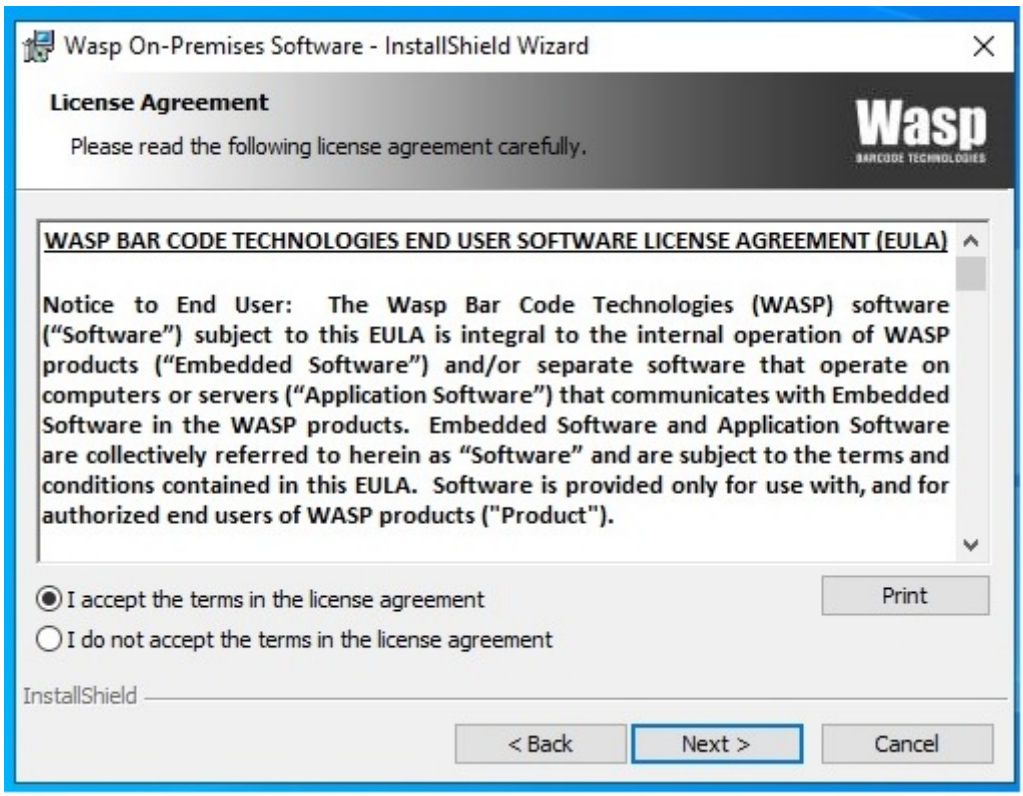
22. Add the Database Server you copied from **Step 20** while installing the new setup. Click **Connect**.



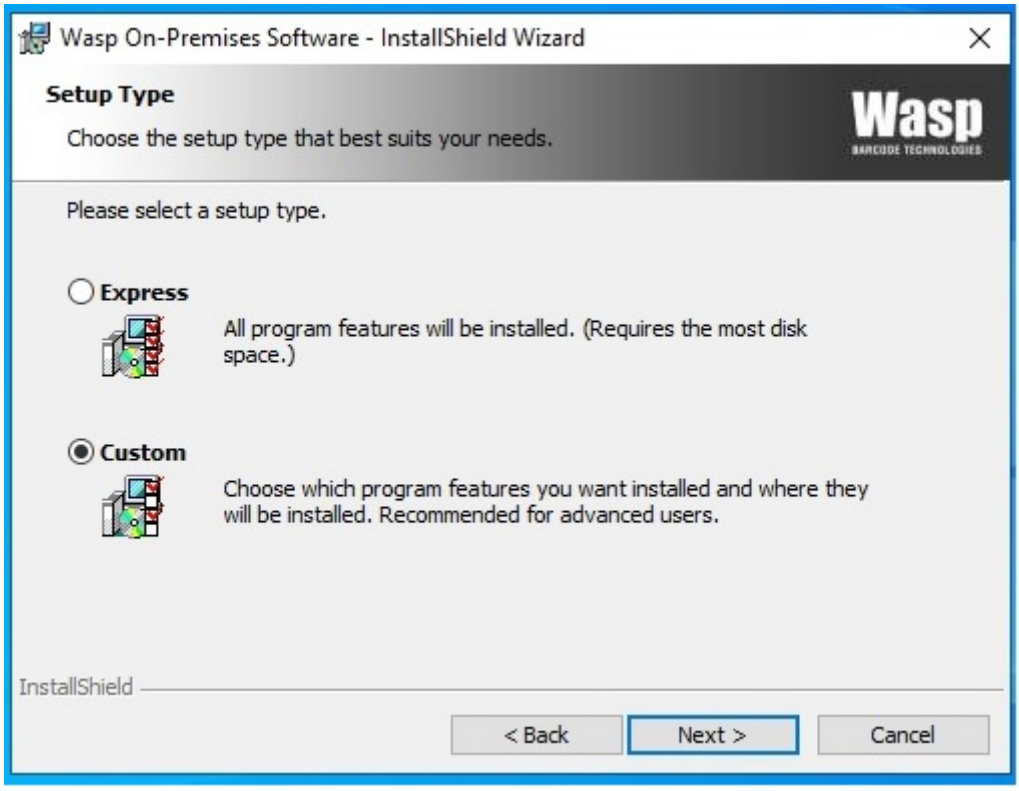
23. Wasp On-premise Software – Installshield Wizard will appear which also indicates the successful connection of the Database Server. It will install Wasp On-premise Software on your computer. Click **Next**.



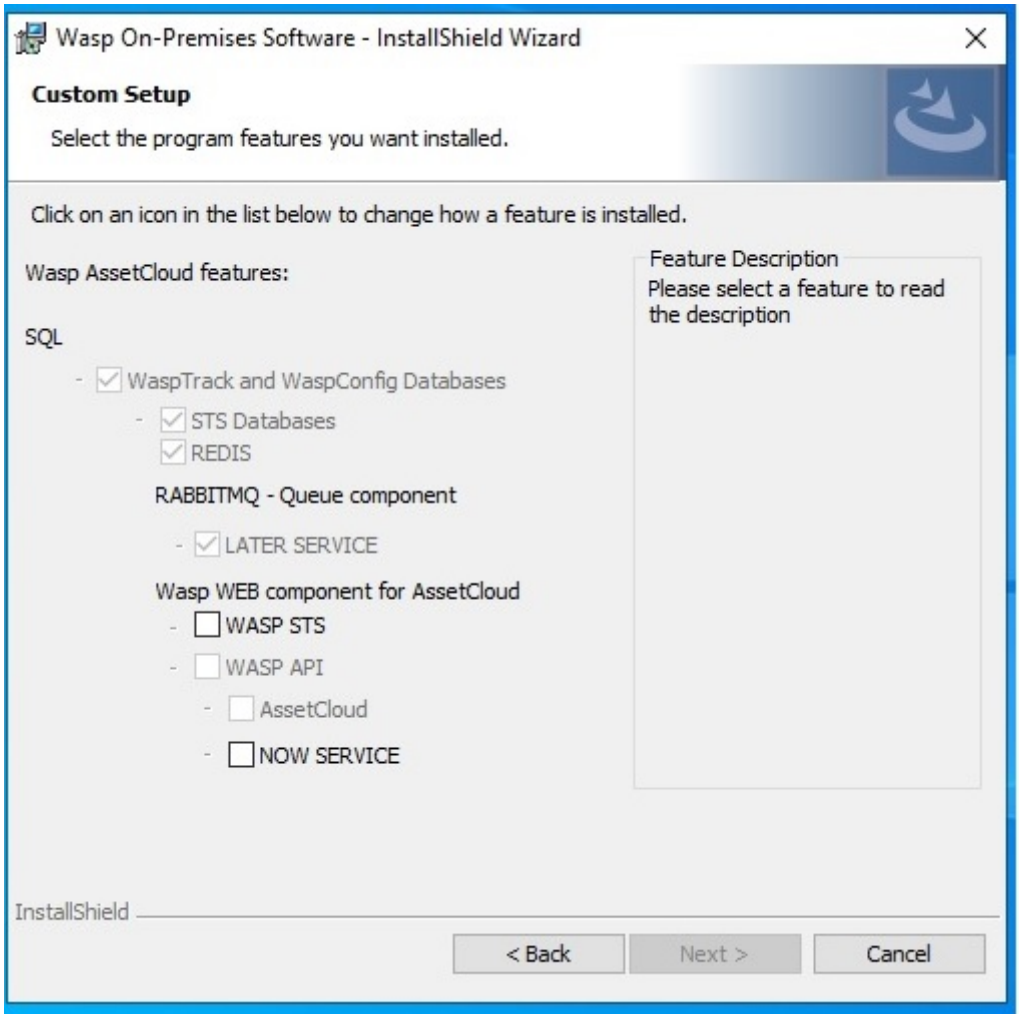
24. To proceed with the setup, you must accept the terms in the License Agreement. Please read the license agreement carefully and click on the radio button and then click **Next**.



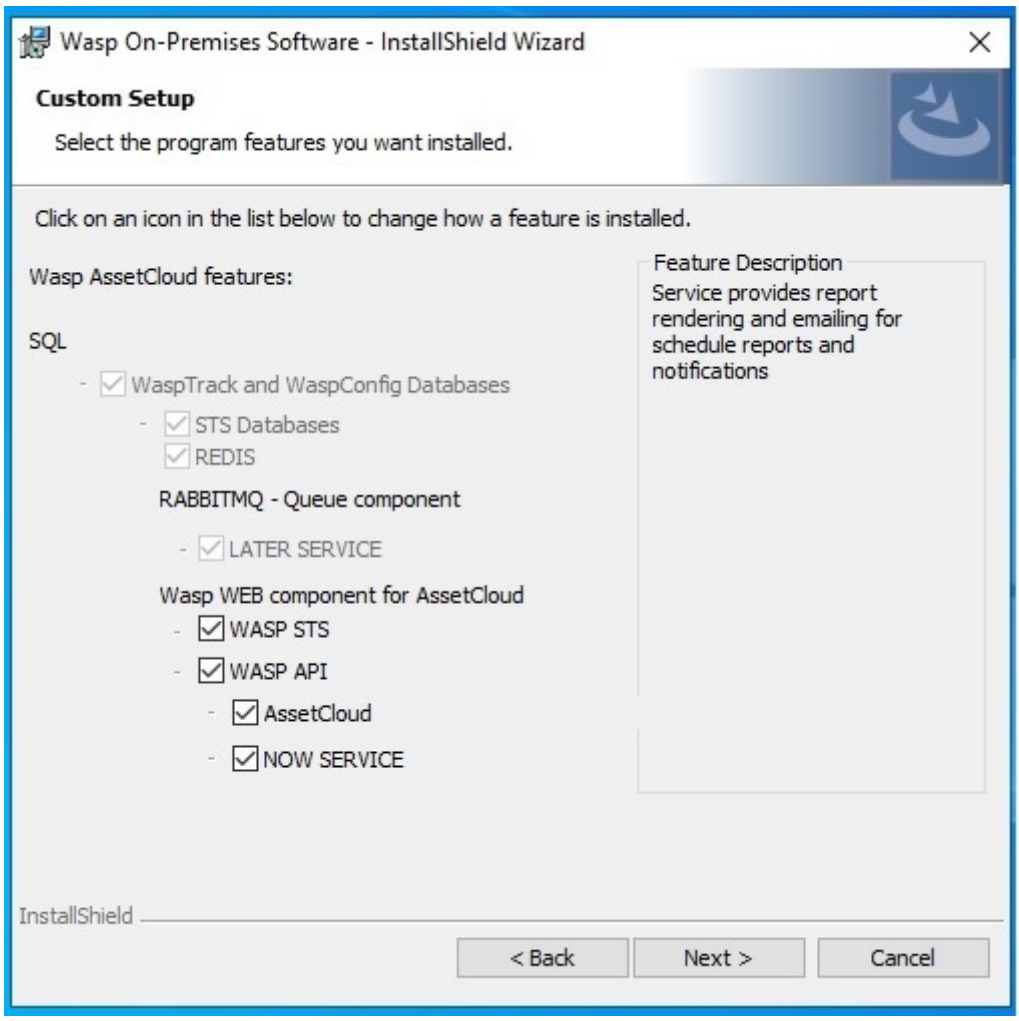
25. Select **Custom** and click **Next**.



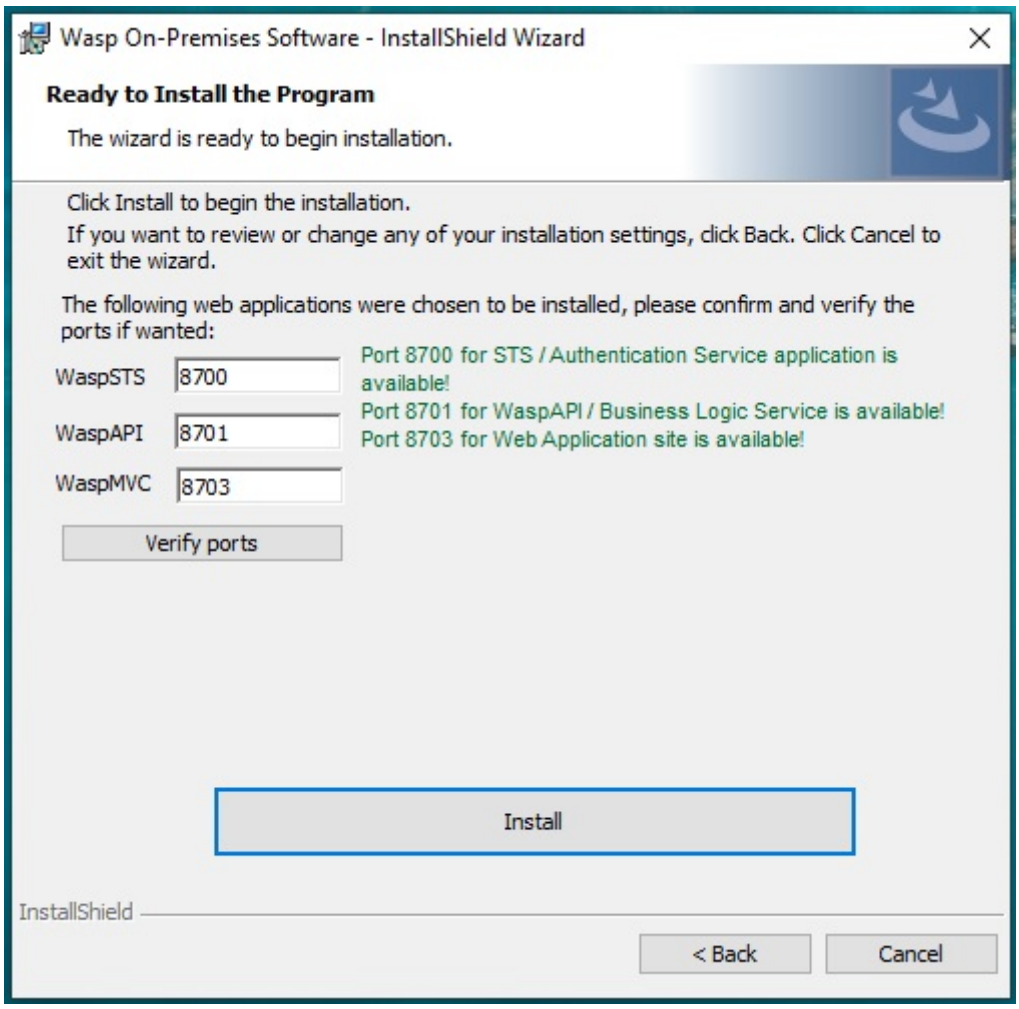
26. Select the program feature that you want to install. Note - Features screen shows 1st 4 features were pre-selected as it already installed.



27. Select the last 4 features and click **Next**.

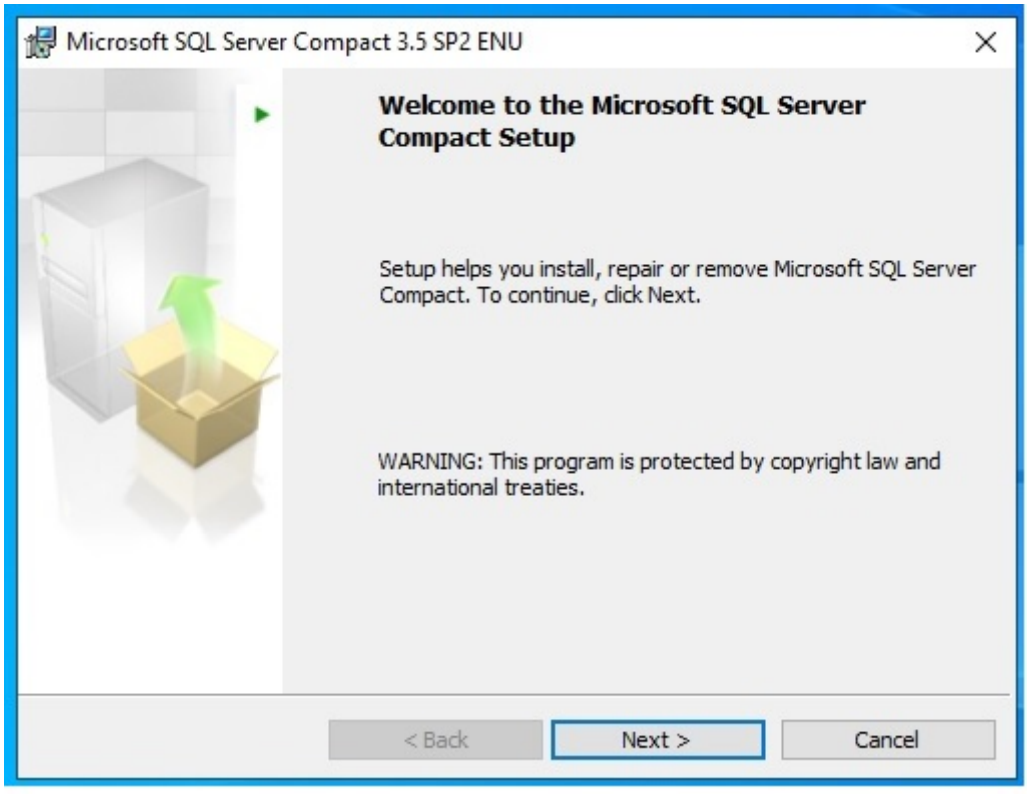


28. The Ports screen shows next. Click **Install**.

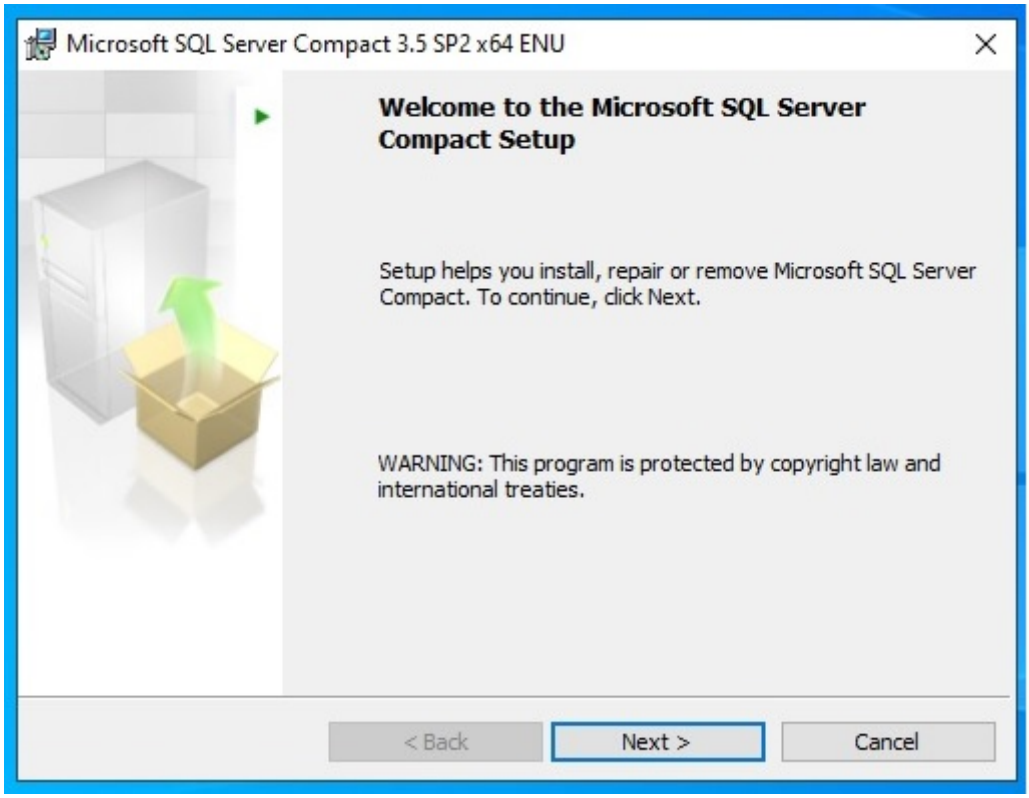


29. Click **Next** in the Microsoft SQL Server Compact 3.5 SP2 ENU screen. The setup helps to install, repair or remove Microsoft SQL Server Compact.

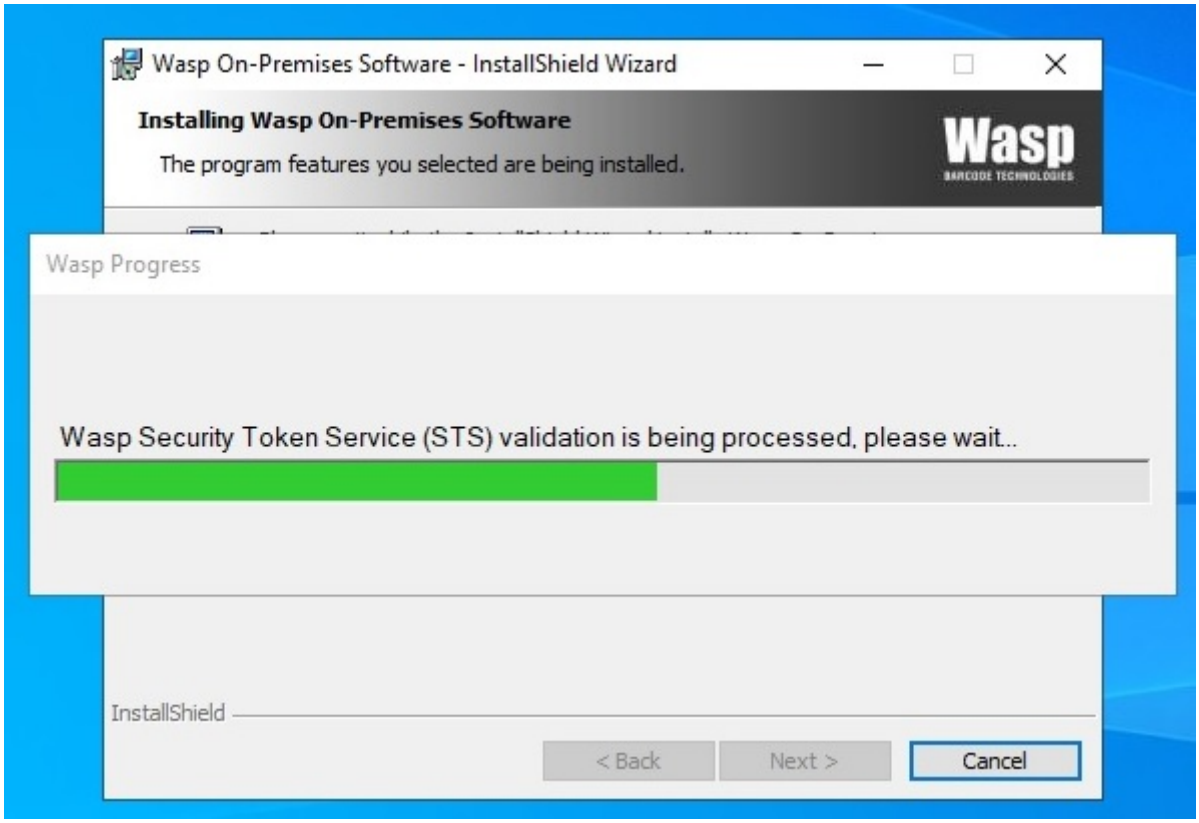
    Note: The Microsoft SQL Server Compact 3.5 could take up to 30 minutes to complete the installation. During installation, when you click on the Next button, the screen might hang. If you choose to click Cancel/Close button, a prompt will appear indicating the operation is not yet complete. We would recommend waiting for 30 minutes to complete the installation and to view the Finish screen.



30. Click **Next** in the Microsoft SQL Server Compact 3.5 SP2 x64 ENU screen. The setup helps to install, repair or remove Microsoft SQL Server Compact

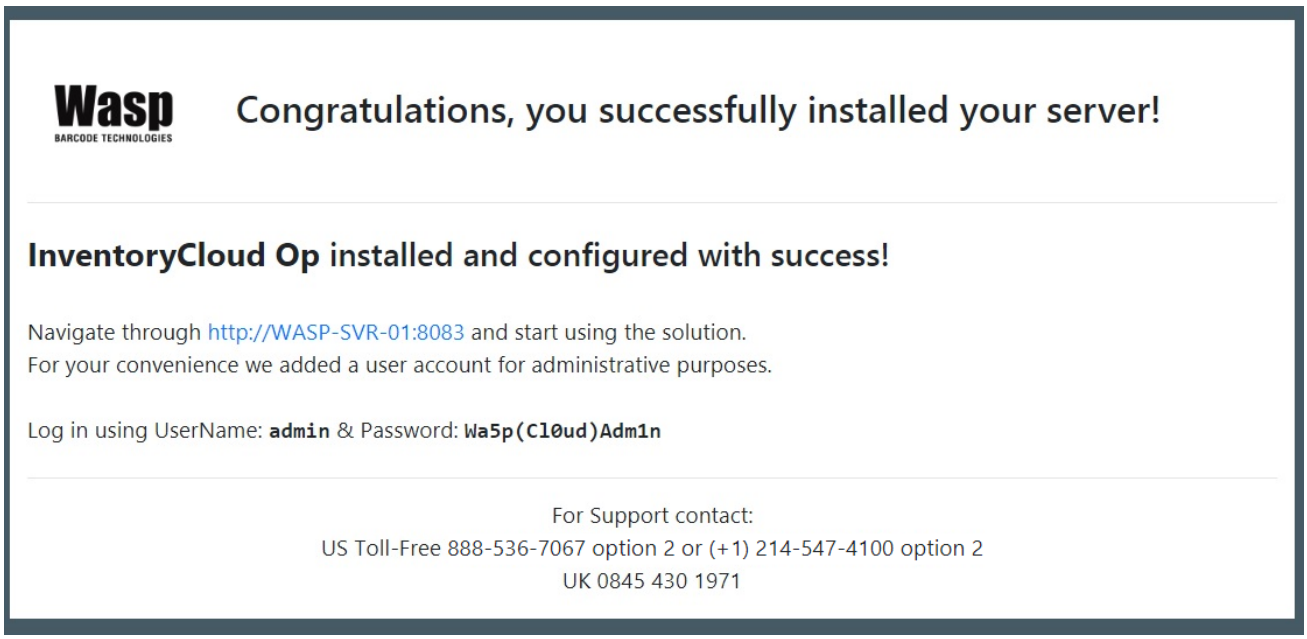


31. Wasp Security Token Service (STS) validation is processed towards the end of the installation.



32. The Congratulations screens will appear and click **Finish**.

    Note - Make sure to note down the URL, Username, and Password.



Once the Cloud On-Premise installation completes successfully but when you attempt to browse to the login page, the username and password fields are left-justified, and the product logo does not appear. Then the problem is certain IIS features were not enabled: Server-Side Includes, Static Content, and Static Content Compression and the solution is to enable these features, refer **IIS Settings Prerequisites** and then refresh the browser.

After the Cloud On-Premise software is installed successfully and you have confirmed you can log in successfully, make the changes in IIS Manager to improve performance. Refer **IIS Application Pool Settings**.