WMS Pro by tecom

WMS PRO INSTALLATION GUIDE

USER GUIDE

ARITECH

BEFORE YOU BEGIN

An installed SQL Server is required for WMS Pro to function. **SQL Express** can be downloaded for free on the Microsoft website (https://www.microsoft.com/en-au/sql-server/sql-server-downloads), however this would only apply for smaller sites. For larger sites seek advice from your company's IT expert.

If you are using TLS version 1.2, make sure your SQL server version is compatible otherwise you will get an error when the server attempts to connect to the database. SQL server versions 2016 or later will support TLS 1.2 natively.

As a part of the setup process the following third-party packages will also be installed:

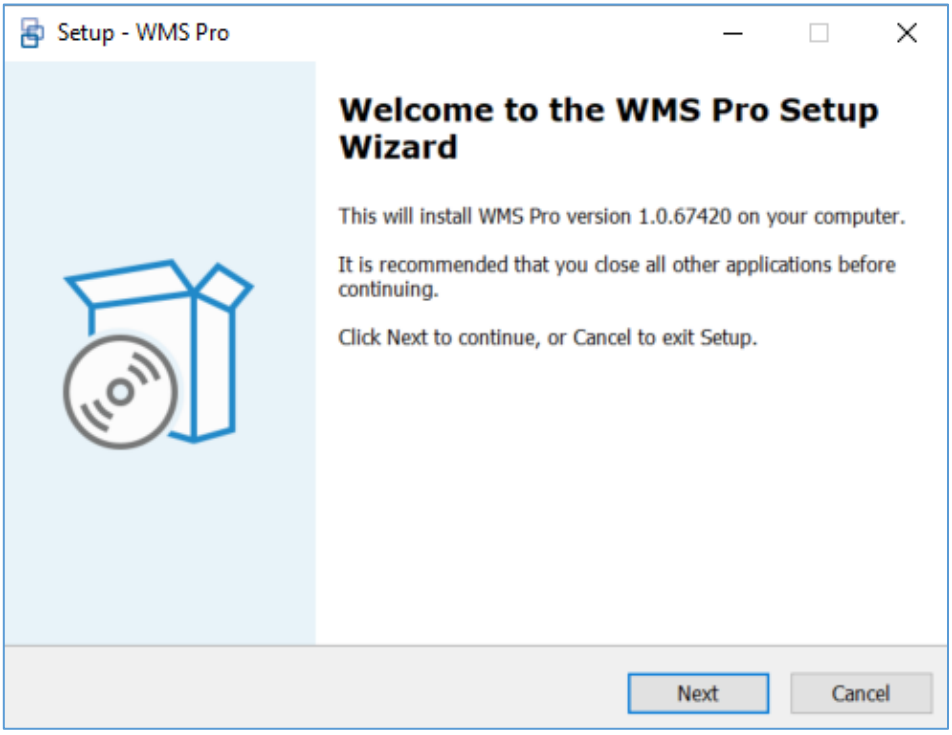
- Erlang
- IIS URL Rewrite
- RabbitMQ
- Microsoft ASP.NET Core bundle

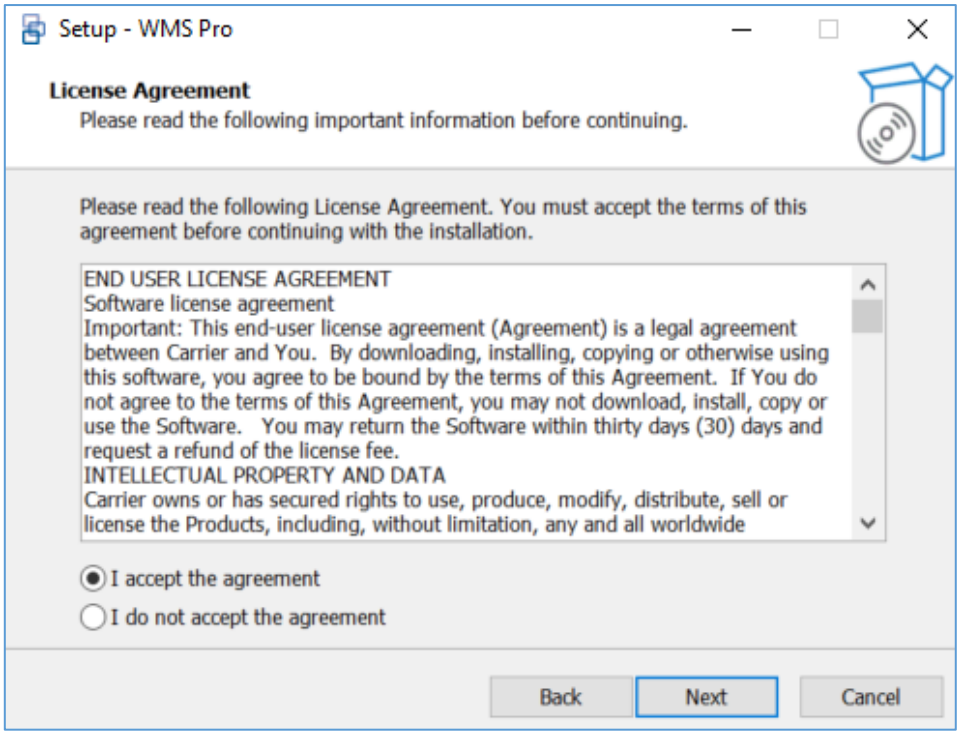
It is strongly recommended that the installation does **NOT** proceed if any of those packages already exist on the server, however ASP.NET Core is the exception. The installation may not succeed as those packages may interfere with the current operation of these systems.

The installation of WMS Pro by default installs a **Self-Signed SSL** certificate, there are steps on page 6 that should be followed if the users require a Signed SSL Certificate from a **Certification Authority** (CA) to access the WMS Pro server.

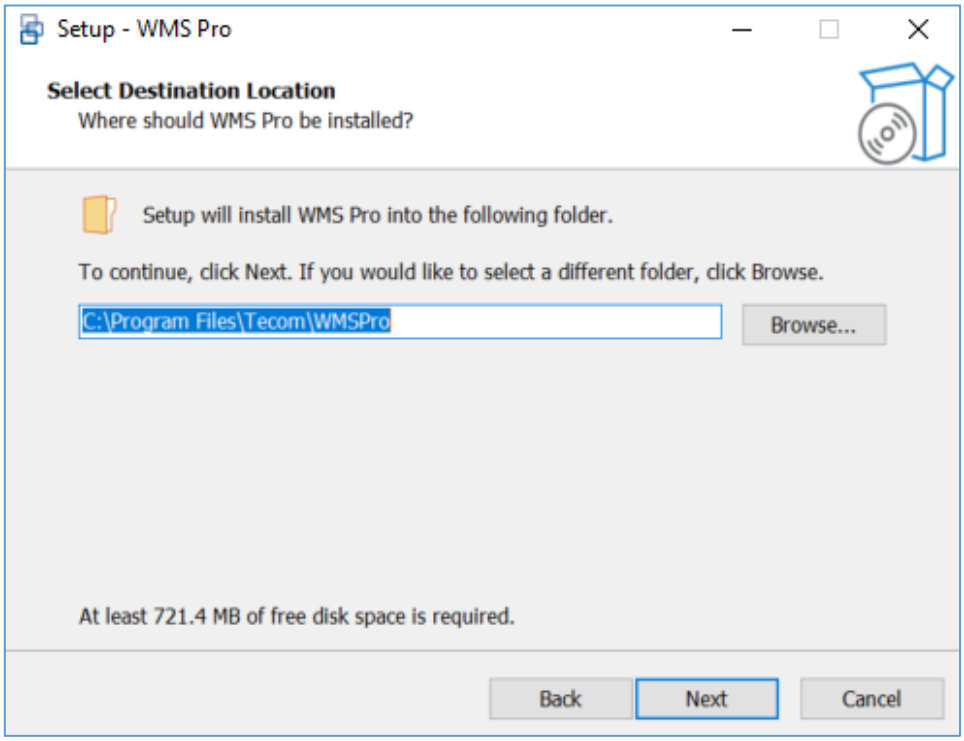
Ensure that there are no **Windows updates** currently in progress as it will interfere with the installation process.

INSTALLATION PROCESS

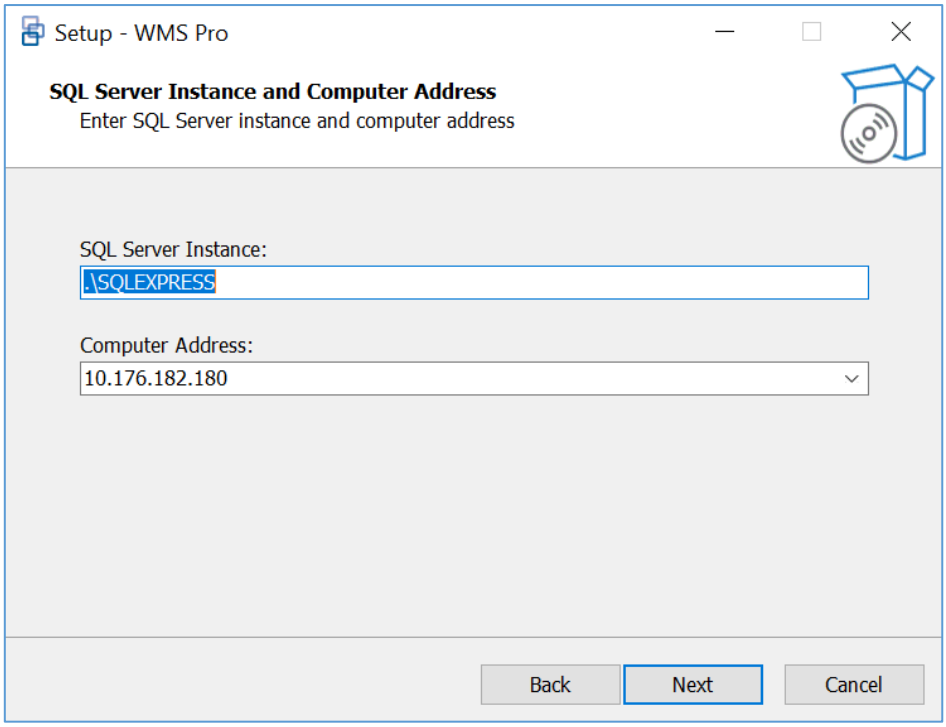




Read and accept the agreement to proceed to the next step.



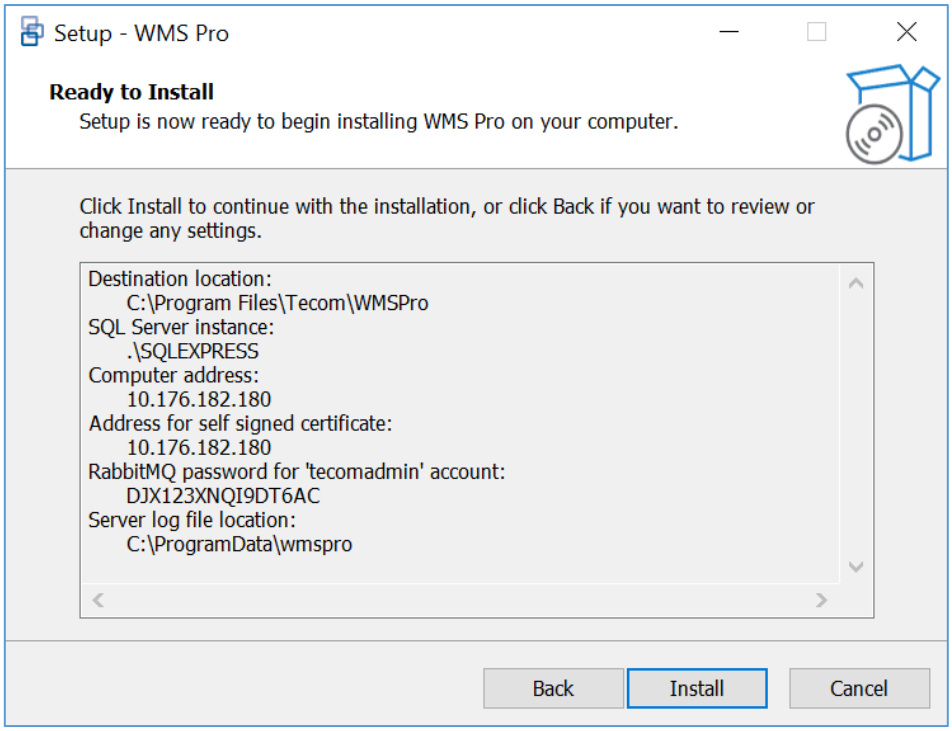
Select your desired folder location or leave it on the default option and proceed.



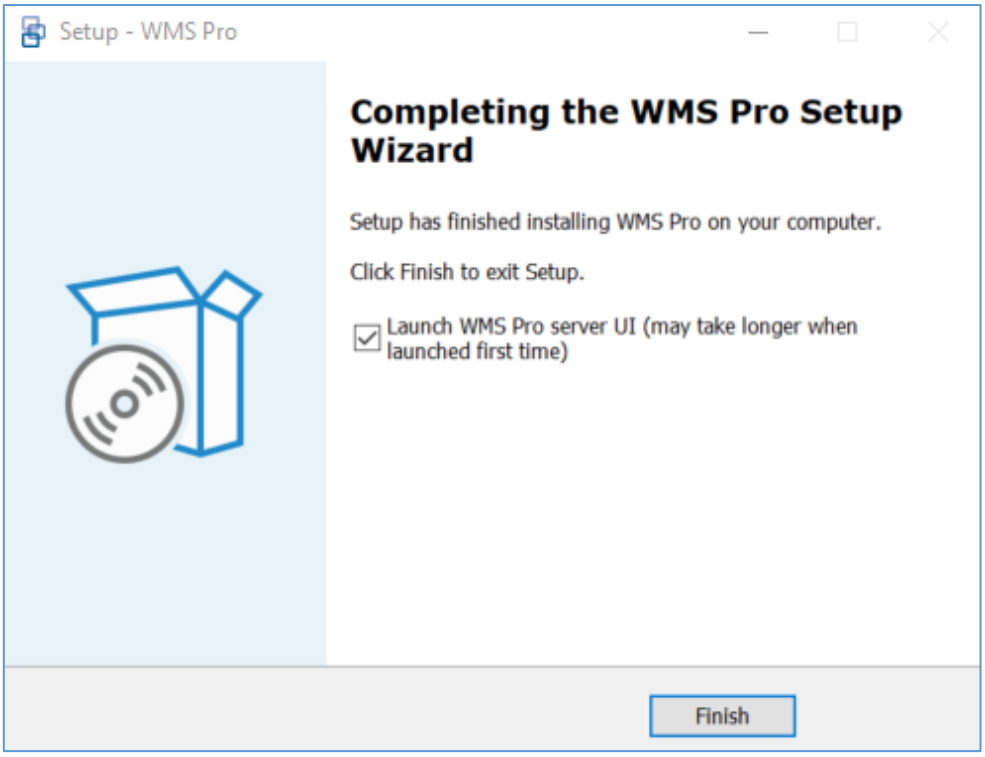
By default, the **SQL Server Instance** field will already be prepopulated for smaller installations that may be running SQL Express and WMS Pro on the same server. If the SQL server has been installed in a different machine and/or has a different instance name, then the correct SQL Server Instance details must be manually entered. Please consult with your local IT department if you are unsure what to enter here.

By default, the **computer address** field will have the IP address entered. The PC name can be selected instead from the drop-down list, or a different name can be manually inputted into the field. Once a computer address has been chosen, it will be the only address/domain name that can be used to connect to WMS Pro.

Note: If you are using a CA issued SSL certificate, please enter the appropriate address manually.



It is advised to save the RabbitMQ password in a secure location as it may be required for future troubleshooting. If you're satisfied with the chosen settings, click "**Install**" to start the installation process.



Click "**Finish**" to exit the setup. WMS Pro client login page will be launched with the default browser if the checkbox is ticked.

If you're using the self-signed certificate that was created during installation, your installation is now complete.

Please refer to the Quick Start guide for next steps.

The steps that follow are **optional** and will only be required for configuring a WMS Pro installation with a CA issued SSL certificate.

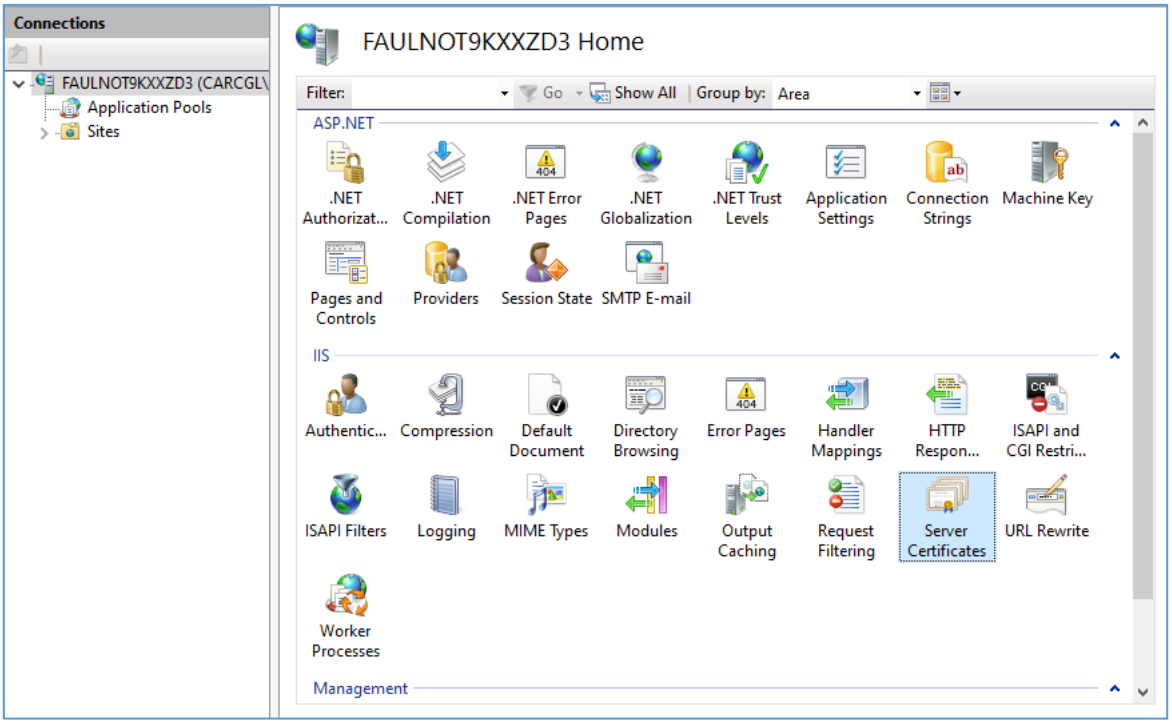
ENABLING WMS PRO SERVER TO USE A SIGNED SSL CERTIFICATE

INSTALLING A SIGNED SSL CERTIFICATE

The installation of WMS Pro by default installs a Self-Signed SSL certificate, the steps below should be followed if the users require a Signed SSL Certificate from a **Certification Authority** (CA) to access the WMS Pro server. Please ensure you have already entered the correct domain address from the installation steps found on page 3.

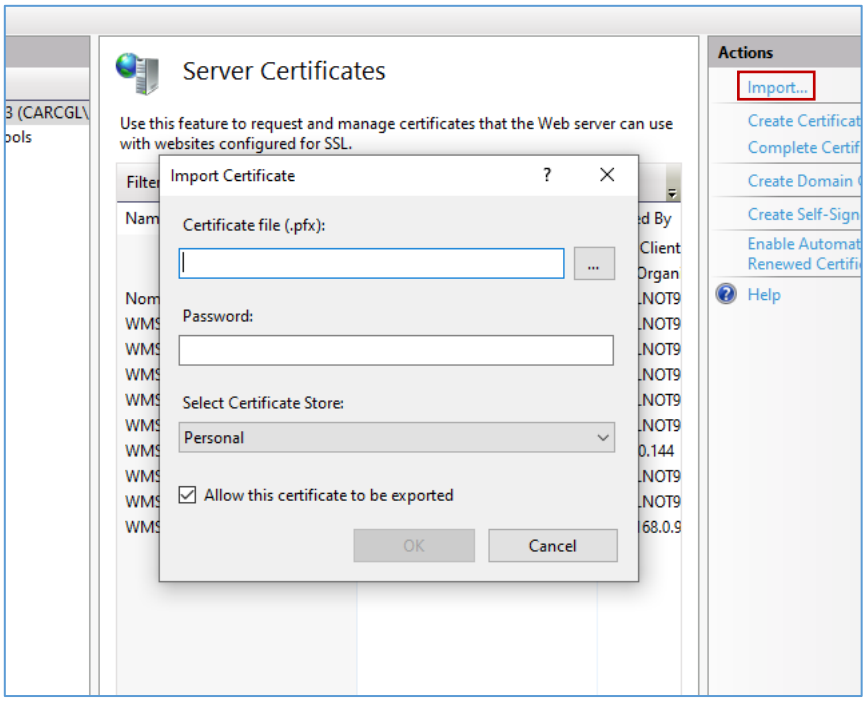
1. The Server certificates are typically managed on a Windows system using the Internet Information Services (IIS) Manager utility, which supports the file extension (.pfx). The IIS Manager can be found by typing in "**IIS**" in the Windows search bar.

2. Double click the "**Server Certificates**" option located under the IIS section. This will take you to a new page.



This is what the IIS Manager window looks like

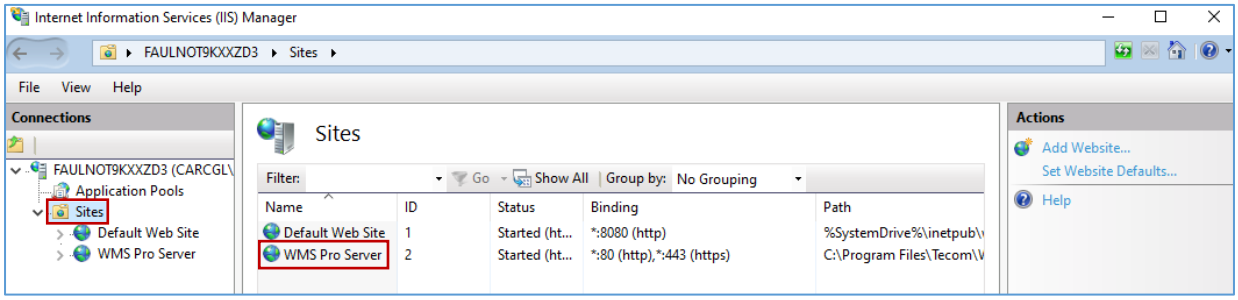
3. In the Server Certificates page click "**Import**" to open a new window (as seen below), upload the relevant file and fill in the required information in the given fields. For the **Certificate Store**, click on the arrow to open the drop-down menu and select "**Web Hosting**". Click "**OK**" to finalise the changes.



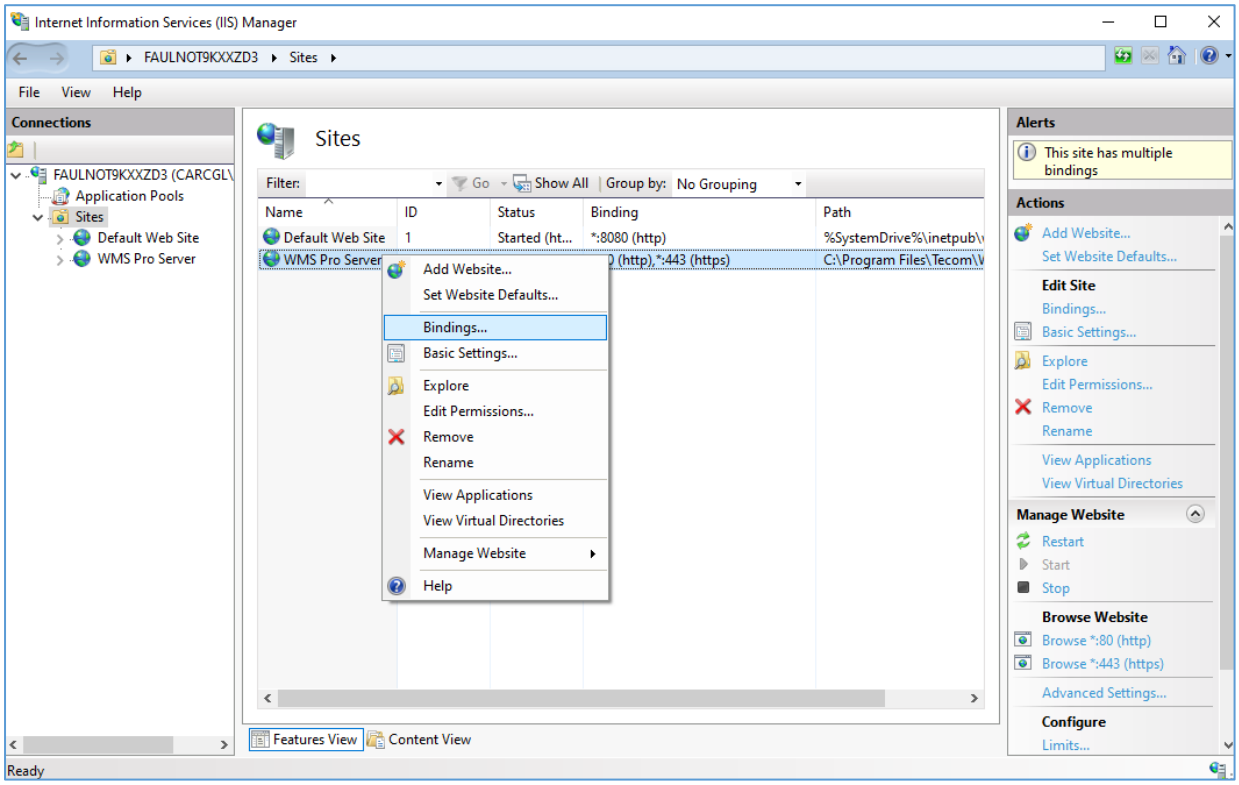
If further assistance is required, contact the person who supplied the SSL certificate for more information and troubleshooting.

BINDING THE WMS PRO SERVER TO USE THE SIGNED SSL CERTIFICATE

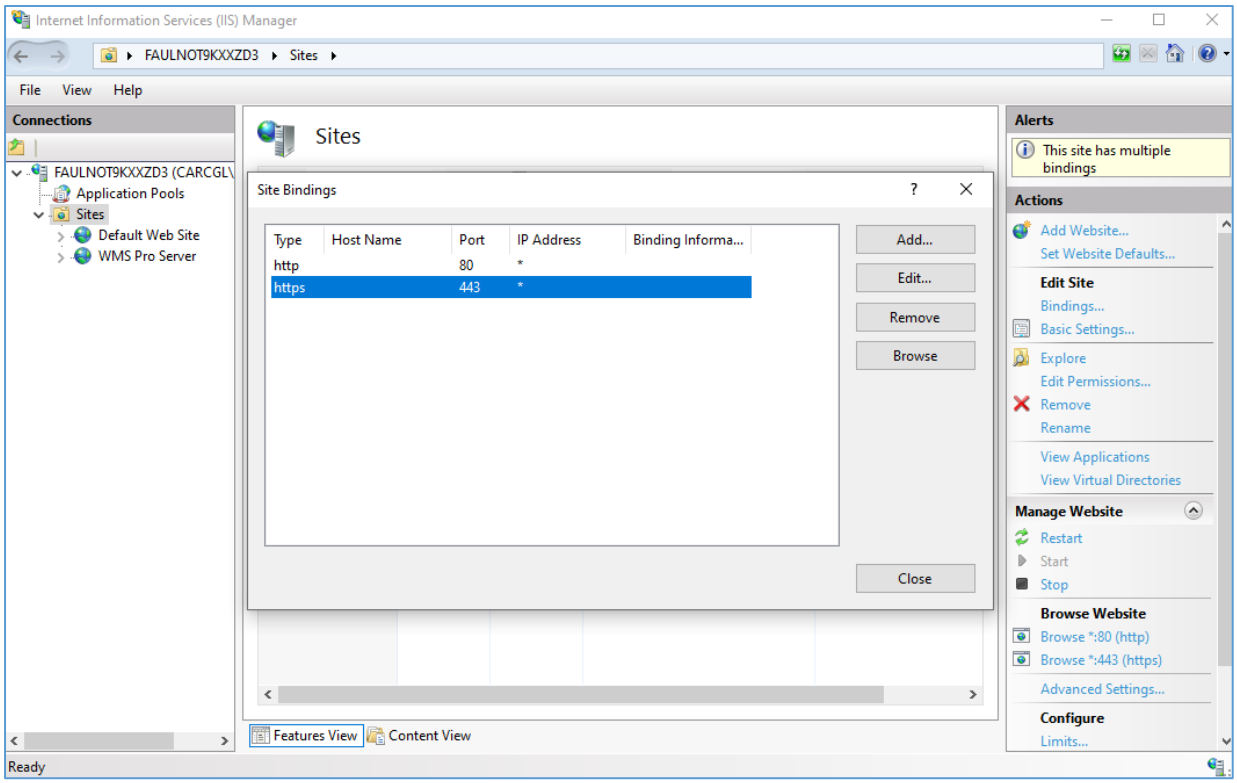
1. Open Windows IIS Manager. Select “**Sites”**, found on the left in the **Connections** section. The list should contain the WMS Pro Server Site as shown below.



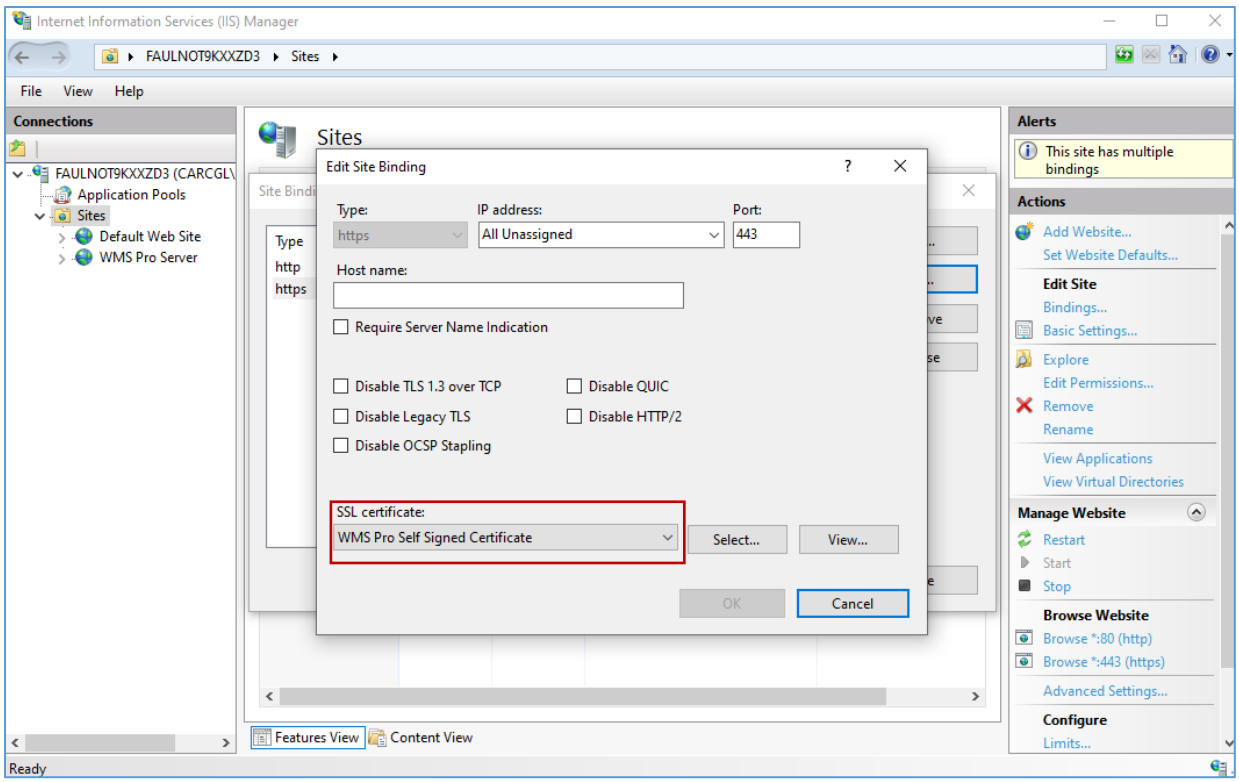
2. Right click on the WMS Pro Server and click “**Bindings**”.



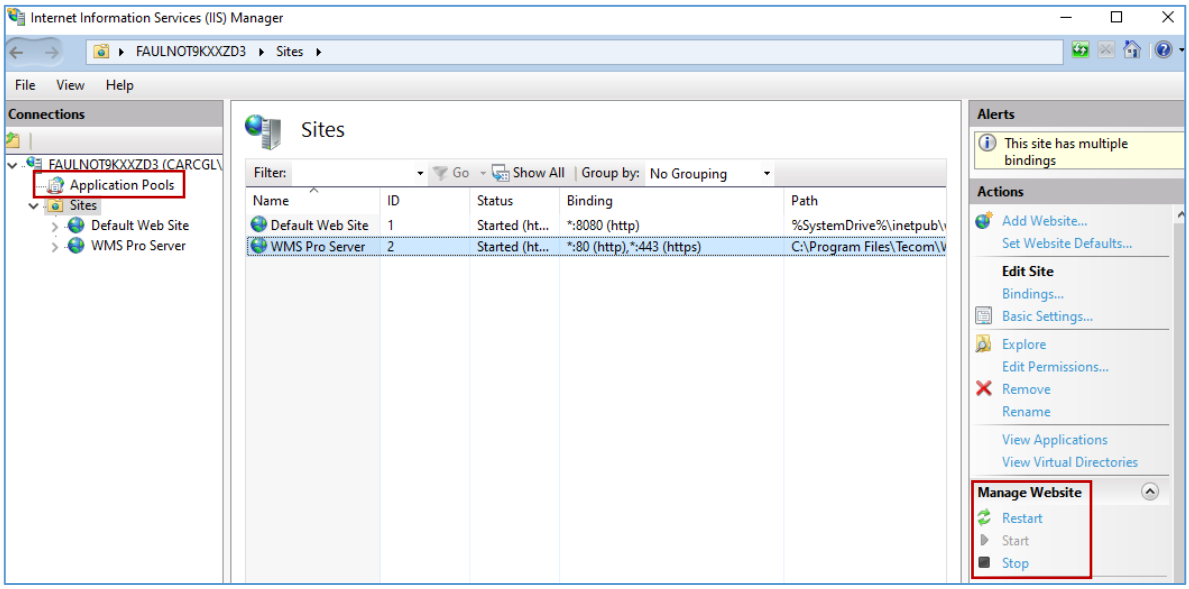
3. Select the **https** entry from the list and click "**Edit**".



4. Change the SSL certificate from the current 'WMS Pro Self Signed Certificate' to use the name of the installed Signed SSL Certificate from the drop-down list. Click "**Select**" to confirm the selection.



5. The IIS WMS Pro Server services will need to be restarted, including the ones found in the Application Pools. Make sure to have the WMS Pro server highlighted. Afterwards, under the "**Manage Website**" option in the IIS Manager window section, press the **Stop** button, wait a couple of minutes and then press the **Start** button.



UNINSTALLING WMS PRO

When uninstalling, it should be noted that some of the third party components installed with WMS Pro will have to be removed separately. Erlang and RabbitMQ can be optionally uninstalled during the uninstallation process. The list of third party packages that will require you to separately uninstall them is:

- IIS URL Rewrite
- Microsoft ASP.NET Core bundle

WMS Pro
by tecom

WMS Pro Security Solutions

SCAN ME

Aritech Australia Pty Ltd
10 Ferntree Place
Notting Hill, Victoria 3168
Phone: 1300 361 479
www.firesecurityproducts.com.au

Carrier

ARITECH

WMS_Pro_Installation_Guide_June23