WMS Pro by tecom

WMS PRO INSTALLATION GUIDE

Version 3.3

ARITECH

BEFORE YOU BEGIN

Before upgrading an existing WMS Pro installation, please ensure that you have first applied an updated license to your installation.

As of WMS Pro 3.0, software upgrades are only available to customers with an active Software Maintenance Agreement (SMA). For more information on WMS Pro SMAs, please contact your local Tecom distributor.

Once you are ready to proceed, please skip ahead to the “Installation Process” section on page 2.

NEW INSTALLATIONS

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.

Note: SQL server version 2019 or newer is required for WMS Pro

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

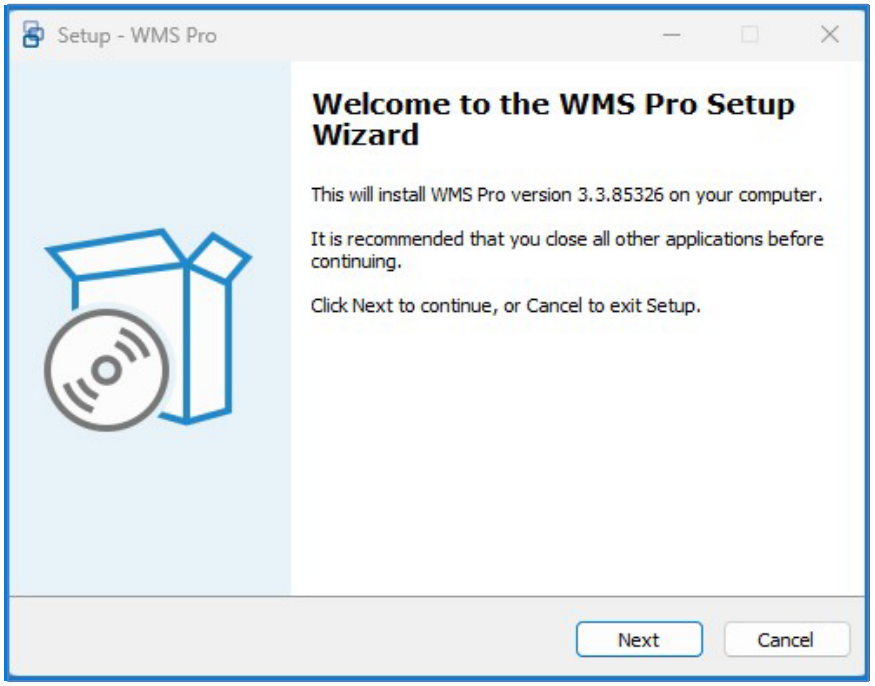
- Erlang*
- IIS URL Rewrite*
- RabbitMQ*
- Microsoft ASP.NET Core bundle

It is strongly recommended that you do **NOT** proceed if any of the starred (*) packages already exist on the server, as installation may be disrupted or cause interference with normal operation of these packages and any systems that may currently utilise them.

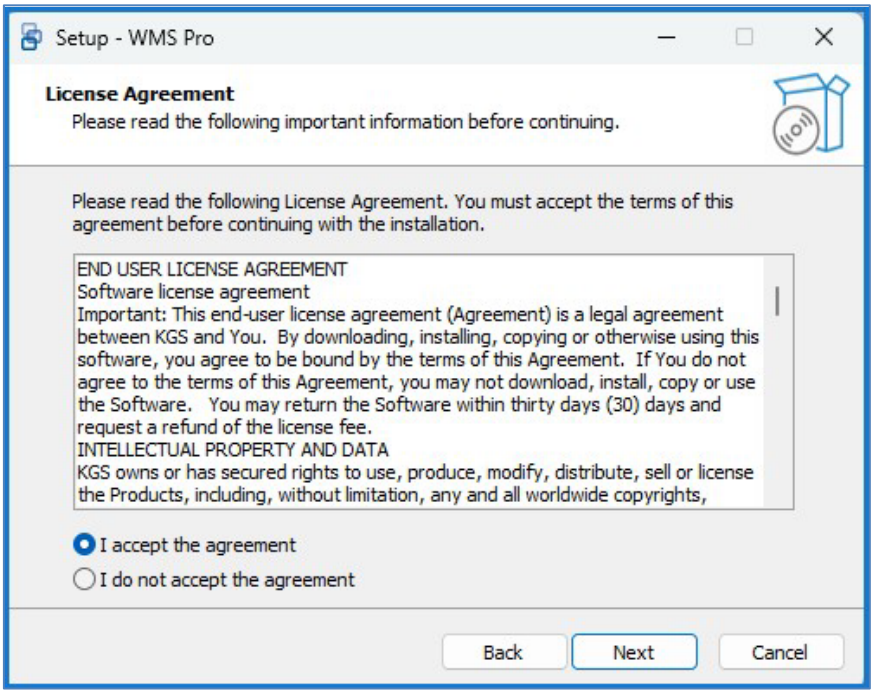
Ensure that there are no **Windows updates** currently in progress as it will interfere with the installation process.

INSTALLATION PROCESS

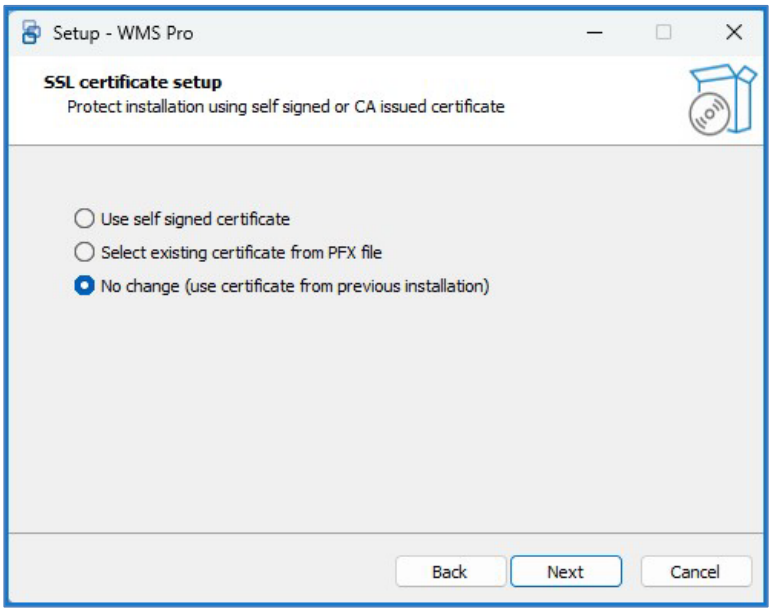
Download and run the WMS Pro installer executable on the Windows computer hosting the WMS Pro server.



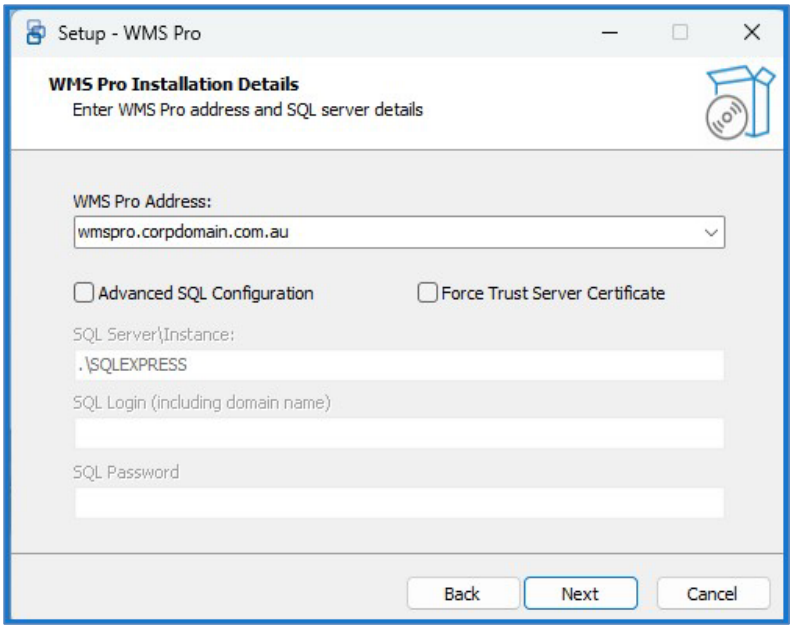
Click 'Next' to continue.



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



Select which certificate to use for the installation and click next to proceed. For existing installations or upgrades, you can choose 'No change' to leave the previous SSL configuration intact, or you can select the appropriate option if you need to modify these details. For example, if you were previously using the self-signed certificate and now wish to use a CA issued certificate, you can re-run the installation process and select the new option to maintain all other existing settings.

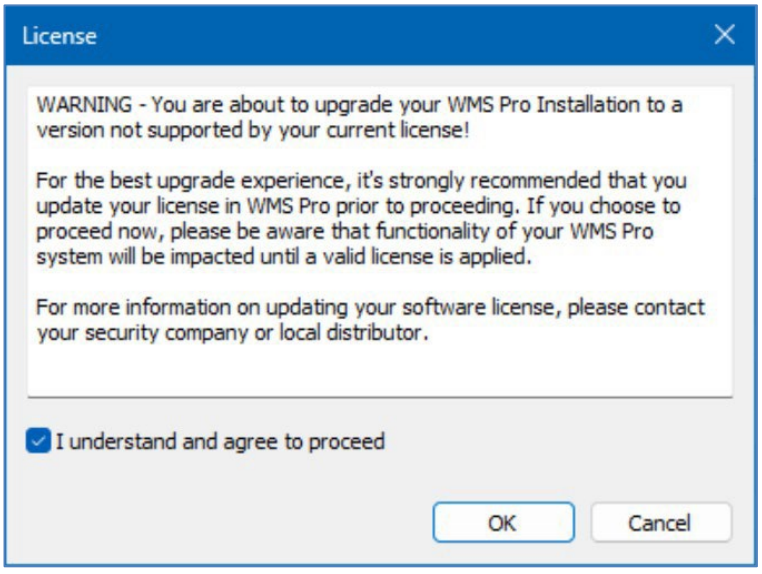


Enter the URL that customers will use to access the WMS Pro web interface in the WMS Pro Address field. For small installations, this will typically be either the IP address or the computer name, which will be populated in the dropdown menu for selection. Larger installations or customers who are using a CA issued SSL certificates should ensure that the fully qualified domain name used on the SSL certificate is manually entered instead.

If the server is using a standalone SQL Express installation, no further info should be required on this screen. However, if the SQL database is located on a different machine and/or instance name, or requires specific login credentials, these details may be entered by ticking the 'Advanced SQL Configuration' checkbox. Additional manual configuration may still be required, depending on the specific configuration being used on site. Please consult with your local IT department for assistance if required.

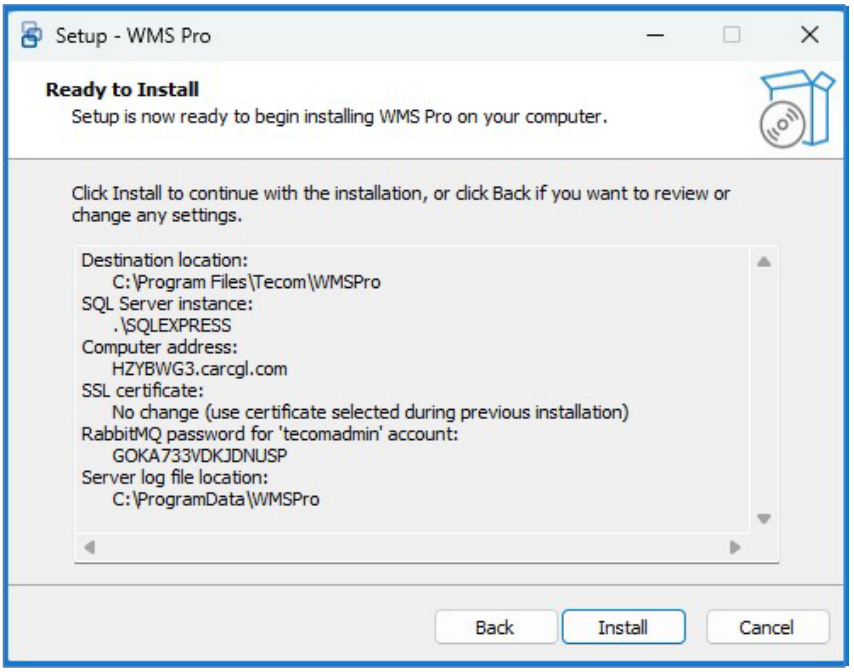
Ticking the checkbox 'Force Trust Server Certificate' will fix an issue where installations were not successfully connecting to SQL 2025 instances.

If you're upgrading an existing installation and have not yet applied a matching updated license to your system, you may be presented with the following warning:



You may choose to proceed regardless, however it's strongly recommended that an updated license be applied to your existing installation first. WMS Pro has been specially designed to accept newer version license keys in order to ensure a smooth upgrade process for existing customers, minimizing downtime and other disruptions that may negatively impact a currently operational system.

To apply an updated license to your current system, simply cancel the installation, request an updated license, and apply it on the Administration > About page once received. You can then restart the upgrade process, and should note that this warning no longer appears.

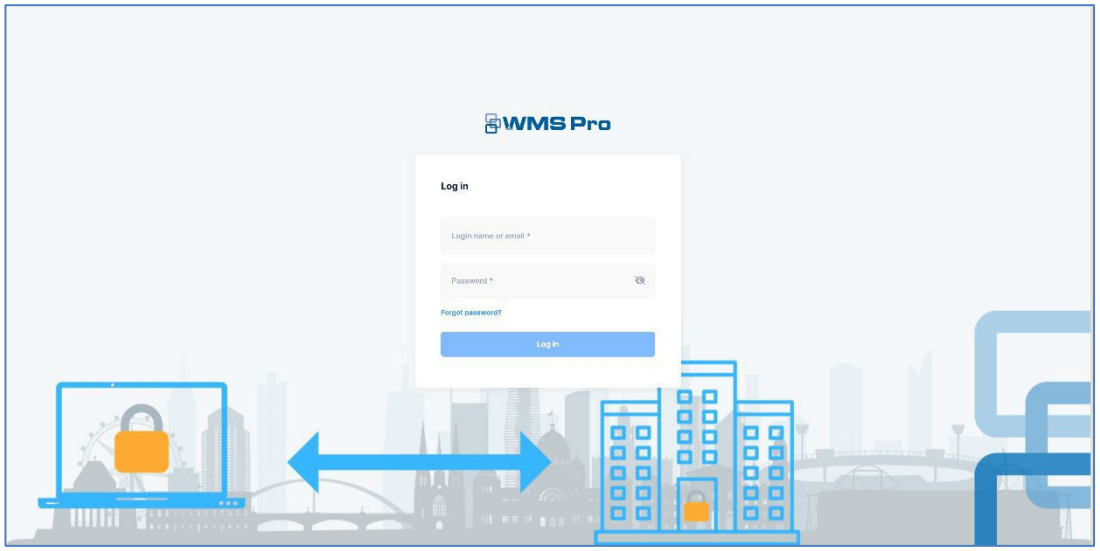


It's advised to save the **RabbitMQ** password in a secure location, as it may be required for future troubleshooting. If you're satisfied with the settings presented, click "**Install**" to start the installation process.

Assuming there were no issues with the installation, you should see the screen below confirming that installation has been completed.

Click “Finish” to exit the setup.

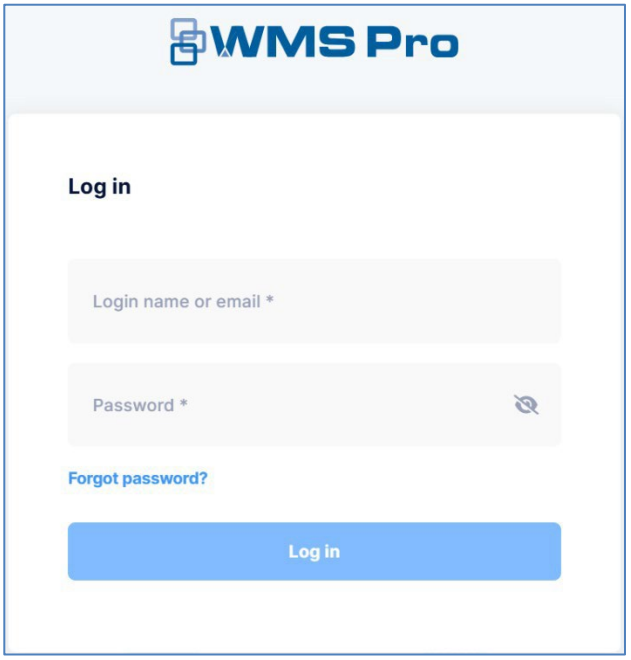
If the 'Launch WMS Pro server UI' checkbox was ticked, the WMS Pro client login page will be launched in the default browser.



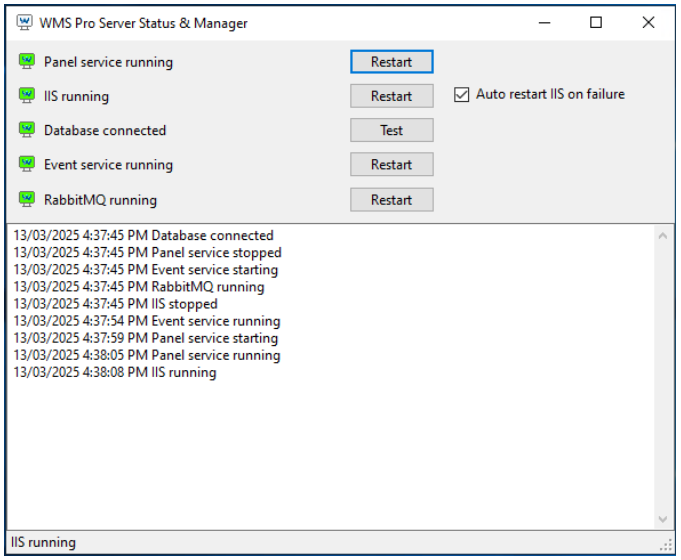
If you're using a **self-signed certificate**, you may receive a warning from the web browser when first accessing WMS Pro. This warning page is being displayed because the browser can't validate self-signed certificates, but should still give you an option to proceed.

This warning page is different for each browser and organisation, and it's strongly recommended to use certificates which have been issued by a trusted Certificate Authority (CA) with your WMS Pro server whenever possible.

Once the login window appears, enter your login details in the given fields. The default credentials can be found in the Quick Start Guide, available from the Aritech Support Portal to Tecom trained and registered installers.



WMS PRO SERVER STATUS AND MANAGER



WMS Pro has a Windows application (WMS Pro Server Status & Manager) which operates alongside your WMS Pro installation. With this app you can check the status of the following back-end dependencies:

- WMS Pro Comms Service
- IIS (Internet Information Services Manager)
- MSSQL Database
- Event service
- RabbitMQ

This allows a Windows administrator to perform some basic troubleshooting, such as restarting services and testing database connectivity, whilst also displaying a log of any events that affect these dependencies, such as when a service starts or stops.

The WMS Pro Server Status & Manager also acts as a watchdog for the IIS service, which may be affected by Windows Updates. Enabling the ‘Auto restart IIS on failure’ checkbox will ensure that this service is automatically restarted in the event that it stops unexpectedly.

This useful diagnostic tool ensures that your WMS Pro system stays up and running smoothly.

Congratulations!

Your installation is now complete.

Please refer to the Quick Start guide for next steps.

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
KGS Fire and Security
Australia Pty. Ltd.
Suite 4.01, 2 Ferntree
Place Notting Hill,
Victoria 3168 Phone:
1300 361 479
www.aritech.com.au

Specifications subject to change without notice.

Aritech Australia Pty Ltd

ARITECH