

**TDSi** UK

INNOVATE · INTEGRATE · INSPIRE

# GARDiS Installation Guide

SM007 – Issue 17

 Part of the  
Vita **protech** Group

## Scope

Copyright © 2022 TDSi. All rights reserved.

Time and Data Systems International Ltd operate a policy of continuous improvement and reserves the right to change specifications, colours or prices of any of its products without prior notice.

## Guarantee

For terms of guarantee, please contact your supplier.

## Trademarks

Copyright © 2022 Time and Data Systems International Ltd (TDSi). This document or any software supplied with it may not be used for any purpose other than that for which it is supplied, nor shall any part of it be reproduced without the prior written consent of TDSi.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

All other brands and product names are trademarks or registered trademarks of their respective owners.

## Cautions and Notes

The following symbols are used in this guide:



**CAUTION!** This indicates an important operating instruction that should be followed to avoid any potential damage to hardware or property, loss of data, or personal injury.



**NOTE.** This indicates important information to help you make the best use of this product.

## Document Control

Issue	Date Issued	Change Summary	Issued By
1	25/10/17	Initial Release	RT
2	05/11/17	Content and Format Changes	RT
3	27/02/18	Content Update of installer and troubleshoot section	RT
4	28/02/18	Removed all Prerequisites	RT
5	08/03/18	Added Prerequisites back into TS Section	RT
6	19/07/18	Added Section 5.3 and 5.4 in TS	RT
7	10/10/18	Added HTTPS TS section along with other updates requested by DS	RT
8	09/11/18	Updated styling from FM's proof read	RT
9	21/03/19	Updated with upgrade section. .Net Framework is updated from 4.6.1 to 4.7.2. SQL Server version is updated from 2014 Express to 2014 SP2 Express.	TBA
10	02/05/19	Revised branding	FM
11	23/09/20	Updated pc requirements	TBA
12	30/07/21	Update GARDiS Requirements to reflect Windows Server 2019 and SQL Server 2019. Removed references to Windows 7, 8.1 and Windows Server 2012	TBA
13	02/03/22	Update GARDiS Requirements. Update to remove references to unsupported operating systems. Updated section 7.5.1, 7.5.2 and 7.5.3 to collate the windows features to enable	TBA
14	10/11/2022	Updated section 3 to specify where to run setup.exe from.	TBA
15	28/04/2023	Update Default SQL Version and tested operating systems	TBA

16	18/12/2024	Updated for v3. Configuration tool UI changes during installer. Set username and password during configuration tool stage.	TBA
17	21/11/2025	General document formatting. Updated supported environments. Updated firewall section for Server 2025 UI. Removed Windows Features section.	

## Table of Contents

1.	Introduction .....	7
2.	GARDiS Requirements .....	8
2.1	Minimum System Requirements.....	8
2.2	Recommended System Requirements .....	8
2.3	Supported Operating Systems.....	8
2.4	Supported Database Engines.....	8
2.5	Supported Browsers .....	8
3.	Installer .....	10
3.1	Launching the Installer.....	10
3.2	Initial Configuration .....	15
3.3	Launching the Web Interface.....	19
4.	Firewall Access for Server PC.....	21
4.1	Accessing Inbound and Outbound Port Rules.....	21
4.2	Inbound Rules .....	23
4.3	Outbound Rules.....	26
5.	Upgrading GARDiS .....	30
5.1	Uninstall the Previous Version.....	30
5.2	Install the New Version .....	30
6.	Troubleshooting .....	31
6.1	Installing on a Domain Controller.....	31
6.2	SQL Installation Failure .....	31
6.3	Troubleshooting – Windows Features.....	31

6.3.1	Windows Server Features .....	32
6.3.2	Window Features to Enable.....	37
6.4	Login Button Error .....	37
6.5	Unable to log in .....	39
7.	HTTPS.....	42
7.1	Enabling HTTPS.....	42
8.	VPN and WAN .....	43

## 1. Introduction


This manual will show you the installation steps required, depending on the Windows version you're working on.

This guide contains walkthroughs relating to Windows 11, Server 2019, 2022 and 2025.

Before installing GARDiS on your system there are certain prerequisites that need to be enabled first.

**NOTE:** We no longer support Windows 10.

## 2. GARDiS Requirements

 The computer name must be 15 characters or less.

### 2.1 Minimum System Requirements

Intel i7, 8GB RAM, 40GB\* free hard drive space, Windows 11 Professional

### 2.2 Recommended System Requirements

Intel i7 or above, 16GB RAM, 80GB\* free hard drive space.

### 2.3 Supported Operating Systems

#### **GARDiS CANNOT BE INSTALLED ON A DOMAIN CONTROLLER**

- Windows Server 2025 Standard + Datacentre
- Windows Server 2022 Standard + Datacentre
- Windows Server 2019 Standard + Datacentre
- Windows Server 2016 Standard + Datacentre
- Windows 11 Pro

### 2.4 Supported Database Engines

- SQL 2025 Express + Standard
- SQL 2022 Express + Standard
- SQL 2019 Express + Standard
- SQL 2017 Express + Standard + Enterprise
- SQL 2016 Express + Standard + Enterprise

GARDiS software will be installed with **Microsoft SQL 2022 Express**.

### 2.5 Supported Browsers

- Google Chrome
- Mozilla Firefox
- Edge

**PLEASE NOTE:**

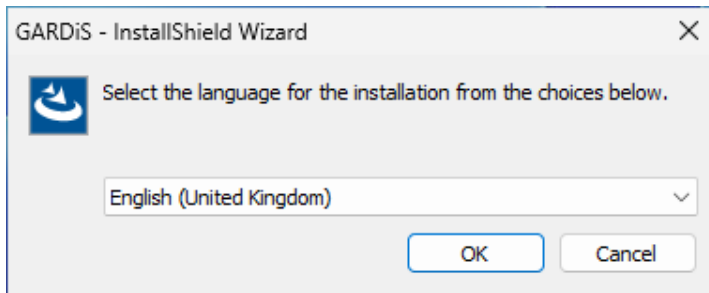
- Domain controllers or child domains are not supported by TDSi.
- All environments are x64 unless stated otherwise.
- (\*) Size of hard disk depends on how many backups and events are to be stored by the system.

## 3. Installer

### 3.1 Launching the Installer

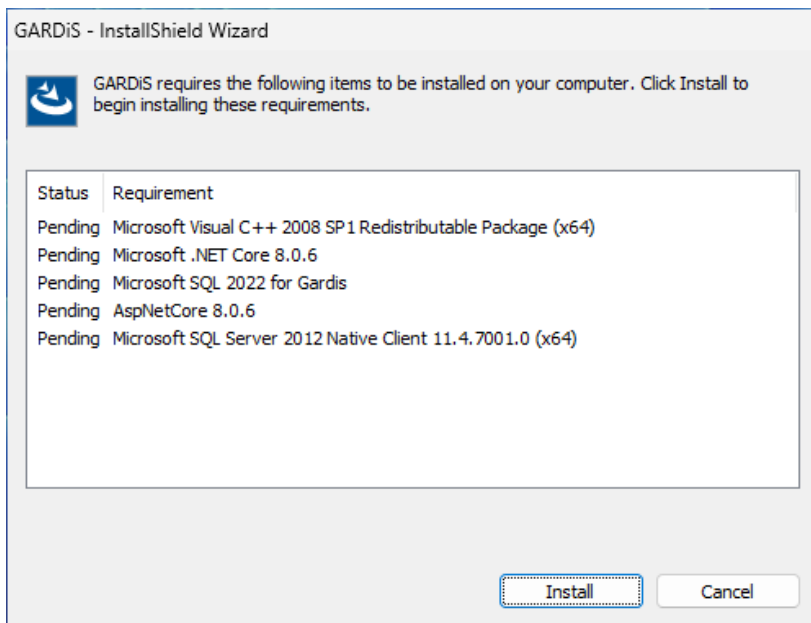
Run the '**Setup.exe**' file.

**Language Selection** – Select the required language. This will also affect the database language.



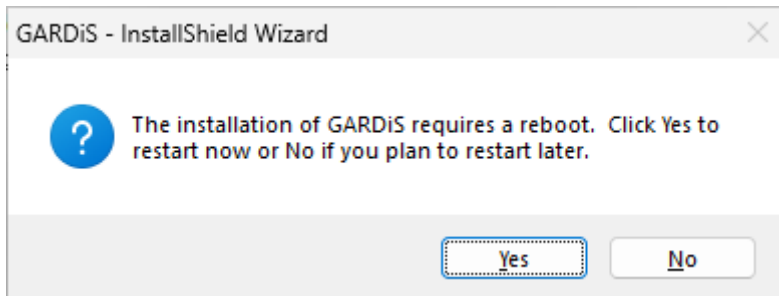
An InstallShield pop-up window may appear, prompting you to install any prerequisites required.

Click '**Install**'.



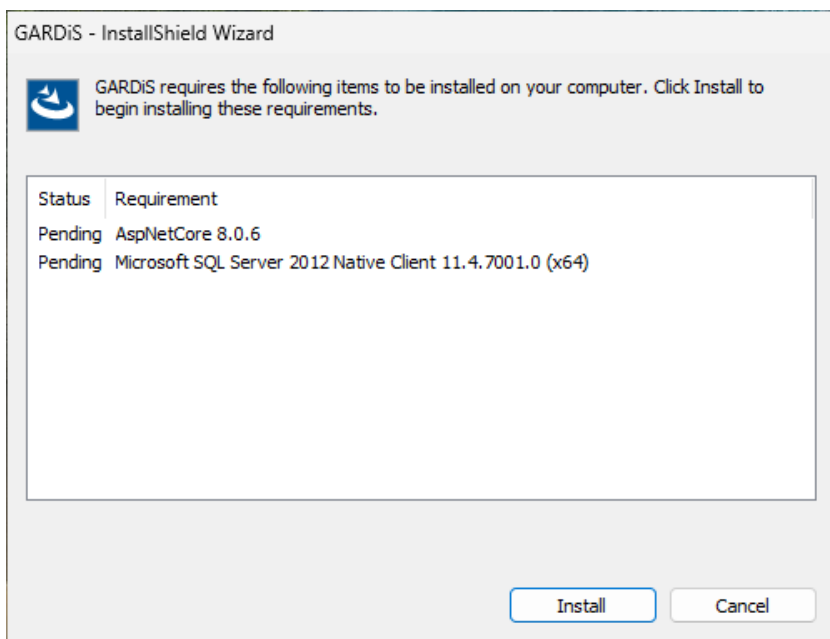
Wait while the required software is installed.

If prompted, click '**Yes**' to restart your computer.

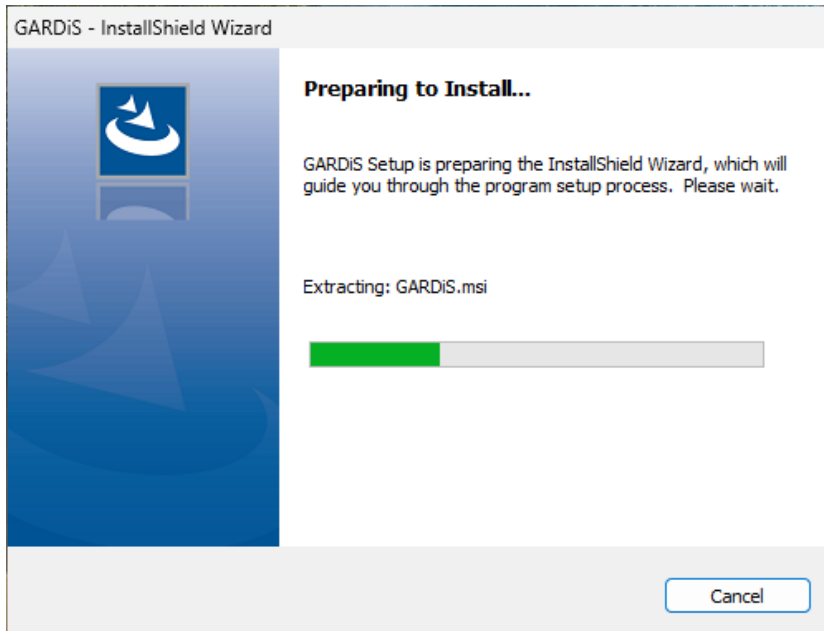


Resume the setup by clicking setup.exe once your computer has restarted and you've logged back in. This will start at language selection as before. Click '**OK**'.

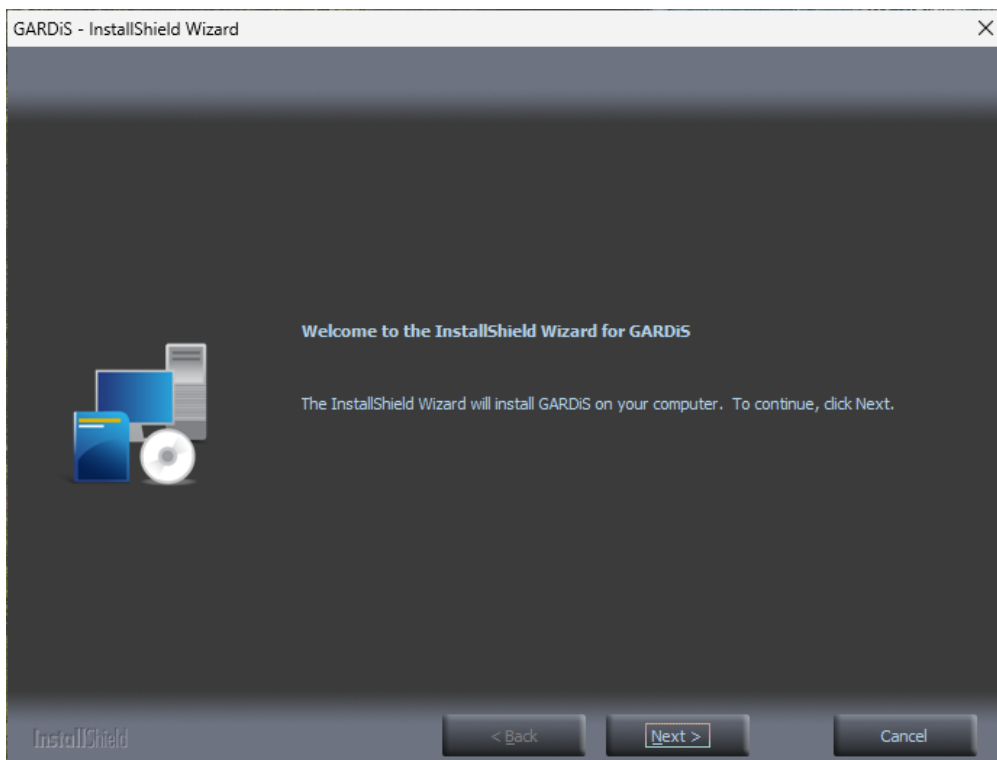
Click '**Install**' to continue any further prerequisites required.



Once prerequisite installation is complete, the installer will prepare to install GARDiS.

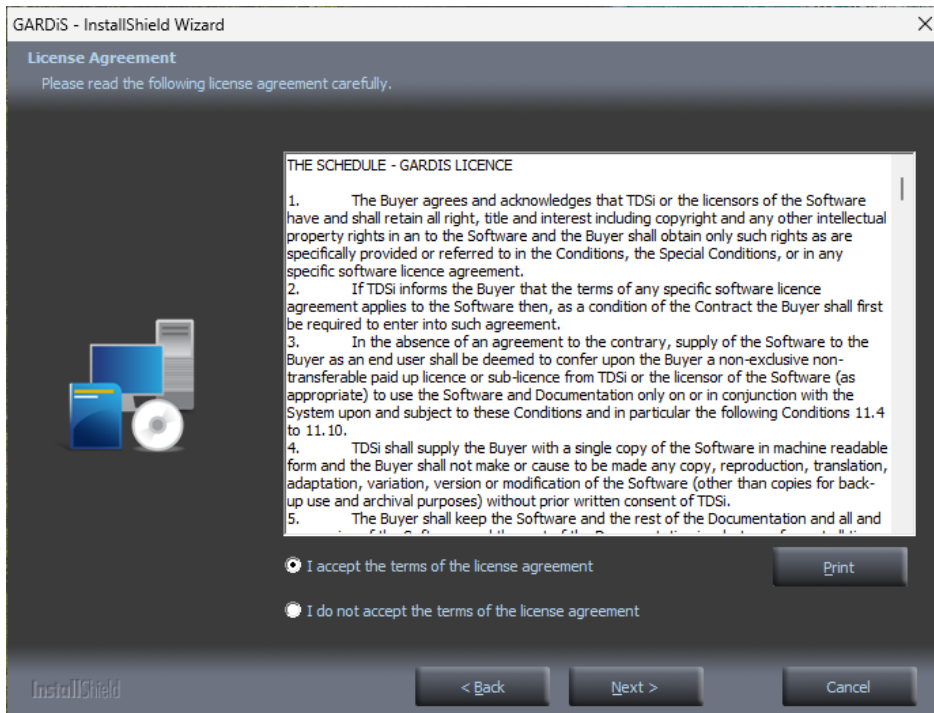


The installer window will now appear. Click '**Next**'.

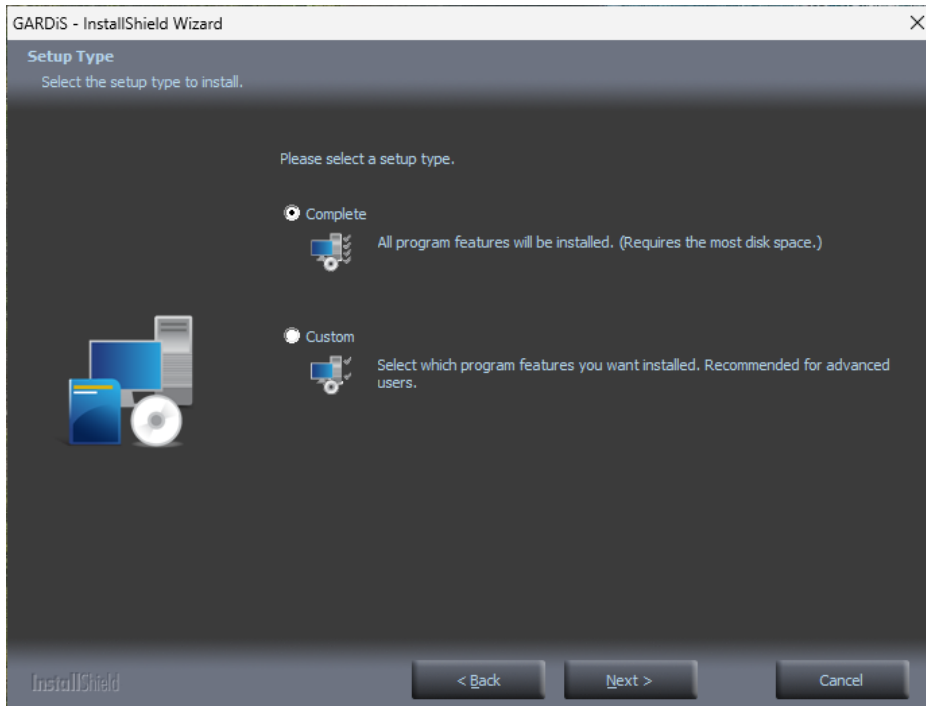


Read the User License Agreement then click '**I accept**'.

To continue, click '**Next**'.

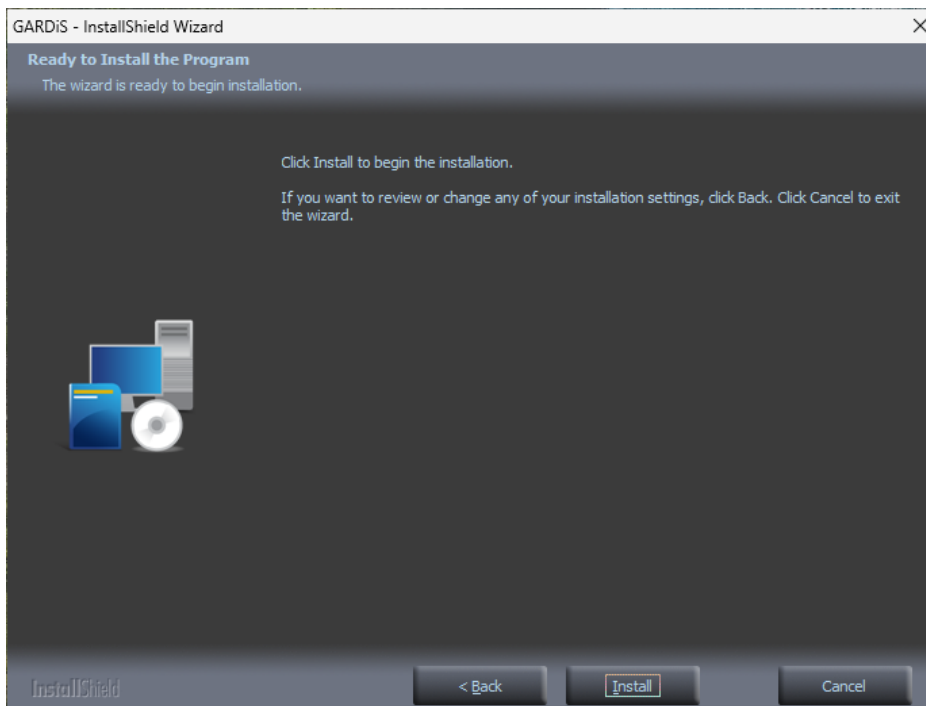


Click the required setup type. It's recommended that you select '**Complete**', but to customise your install, click '**Custom**'.

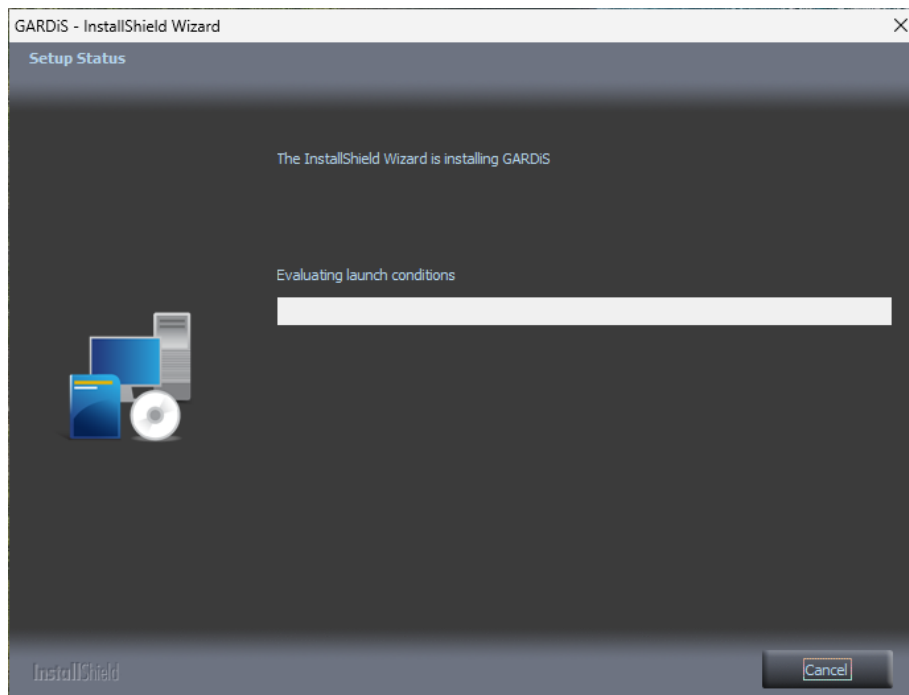


To continue, click '**Next**'.

Click '**Install**'.



Installation shall commence with evaluation and computing space requirements.



## 3.2 Initial Configuration

You will now see the 'Setup' window appear.

Select the IP address of the PC to allow access to the system from browsers on other machines.

If you wish to use/access GARDiS on your PC only select 'This PC only'.

The screenshot shows a 'Setup' window with two main sections: 'Connection Details' and 'Initial Login'. In the 'Connection Details' section, there are two radio buttons: 'This PC only' (unselected) and 'Network' (selected). Next to the 'Network' radio button is a dropdown menu showing the IP address '192.168.5.114'. Below this is a checked checkbox for 'Use Default Ports'. A text label reads 'Connect to GARDiS using the following URL' followed by the URL 'http://192.168.5.114:80'. The 'Initial Login' section contains four text input fields: 'Initial Software Username', 'Initial User Password', 'Confirm Password', and 'Initial User Email Address'. The password fields have eye icons to toggle visibility. A warning icon and text at the bottom of this section state: 'Please make a note of this password as if you forget it you will need to create a new database.' A 'Confirm' button is located at the bottom right of the window.

**Radio buttons:**

- 'Network' for connecting from other machines to the GARDiS PC >> drop down box to choose IP address from those listed on the PC, it may have two or more network cards, you will need to select which one will be listened to.
- 'This PC only' will display the URL that will only work on the PC itself.

These radio buttons do NOT change the operation of the GARDiS service, it's only to indicate to the installer what the desired URL will be following installation.

Use Default Ports – Leave this ticked if you do not have restrictions on the following ports:

- **80:** Used for main website.
- **8715:** Used for login and security.
- **8716:** Used by API to retrieve data from server.
- **8730+:** Ports used internally to the server for sending messages between services.

**NOTE:** If you're accessing GARDiS from a remote PC, you may need to allow these default port numbers in Windows firewall settings as a rule.

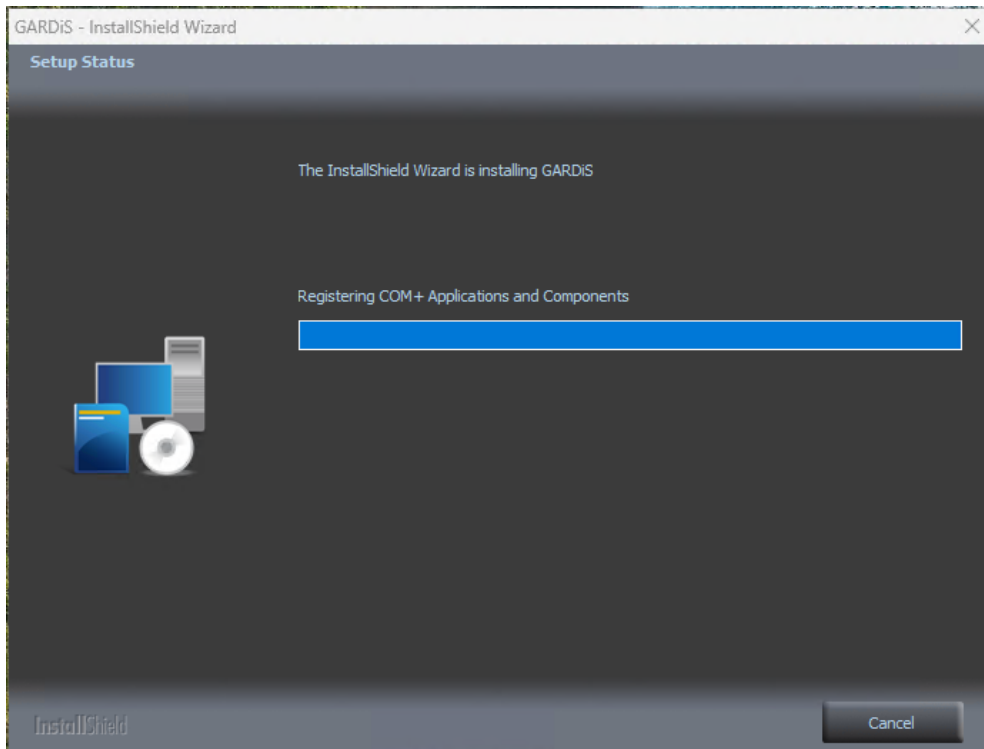
See [Section 4](#) for information on how to set up firewall rules.

**Initial Login** – Enter username and password that will be first used to log into the software.

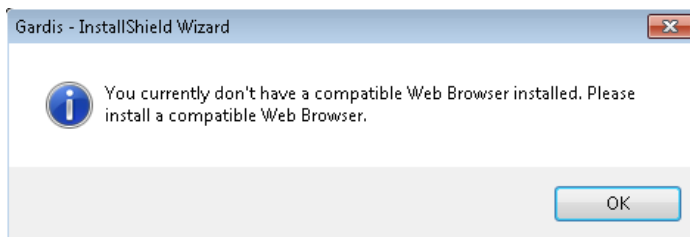
The screenshot shows a 'Setup' window with two main sections: 'Connection Details' and 'Initial Login'.  
**Connection Details:**  
- Radio buttons for 'This PC only' and 'Network' (selected).  
- A dropdown menu showing the IP address '192.168.5.114'.  
- A checkbox for 'Use Default Ports' which is currently unchecked.  
- Four port configuration rows, each with a text input, a refresh icon, and a checkbox:  
 - Security Token Service Port: 8715  
 - GARDiS API Port: 8716  
 - GARDiS Website Port: 80  
 - Message Queue Port: 8730 - 8790  
- A text label: 'Connect to GARDiS using the following URL' with the URL 'http://192.168.5.114:80' below it.  
**Initial Login:**  
- 'Initial Software Username' text box containing 'Installer'.  
- 'Initial User Password' text box with masked characters and a visibility icon.  
- 'Confirm Password' text box with masked characters and a visibility icon.  
- 'Initial User Email Address' text box containing 'Installer@company.com' and a 'Test\$2024' button.  
- A warning icon and text: 'Please make a note of this password as if you forget it you will need to create a new database.'  
- A 'Confirm' button at the bottom right.

Once complete, click '**Confirm**'.

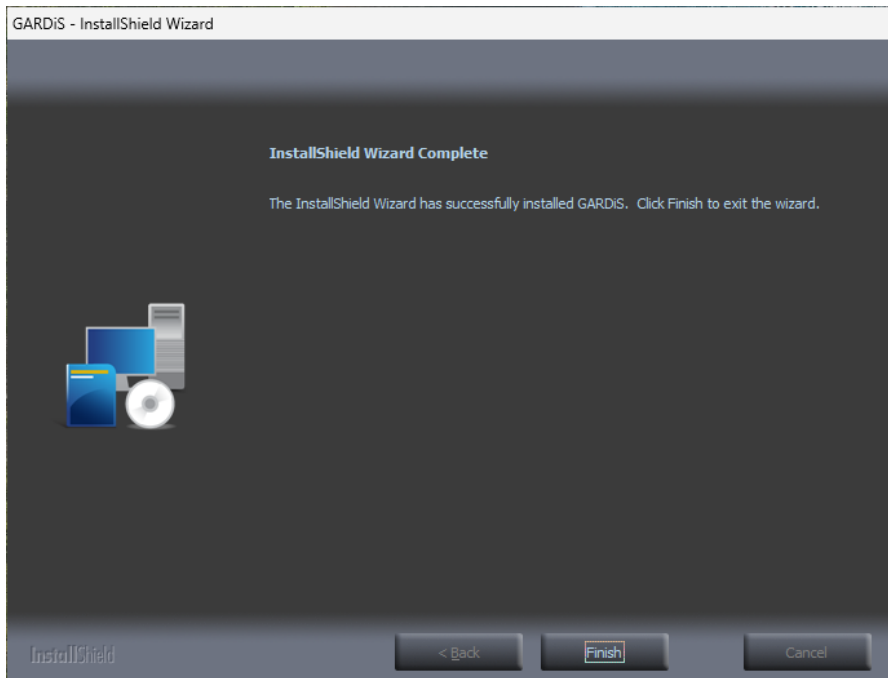
Installation then continues.



**NOTE:** If you do not have one of the internet browsers listed in [Section 2.5](#), you will see this message:



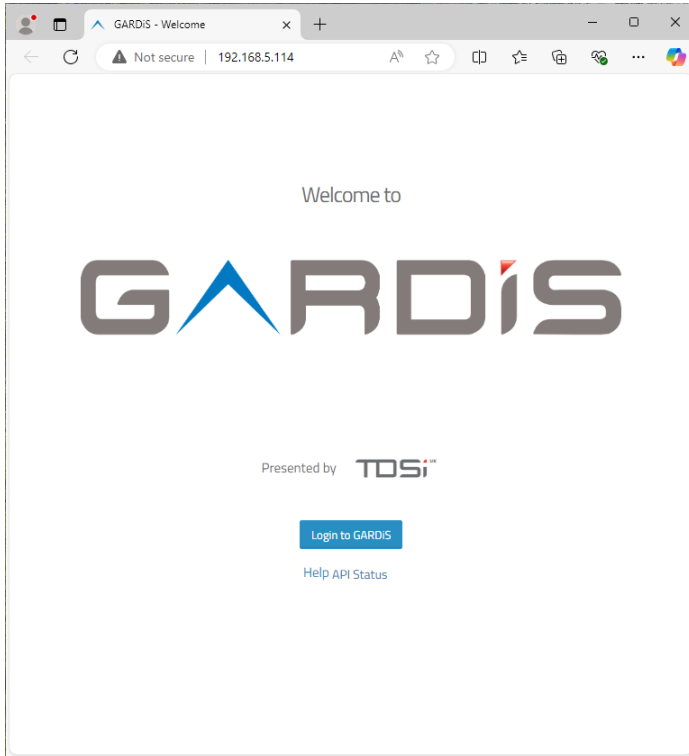
Once the setup completes, click **'Finish'**



### 3.3 Launching the Web Interface

Navigate to the address you previously set in the configuration application. You do not need to include a port number if left at the default of port 80.

E.g. 192.168.5.114



Click '**Log In**' on the landing screen, then you will now be able to log into GARDiS using your username and password entered during the setup screen.

**NOTE:** The username and password are case sensitive.



## Login

Username

Password

Login

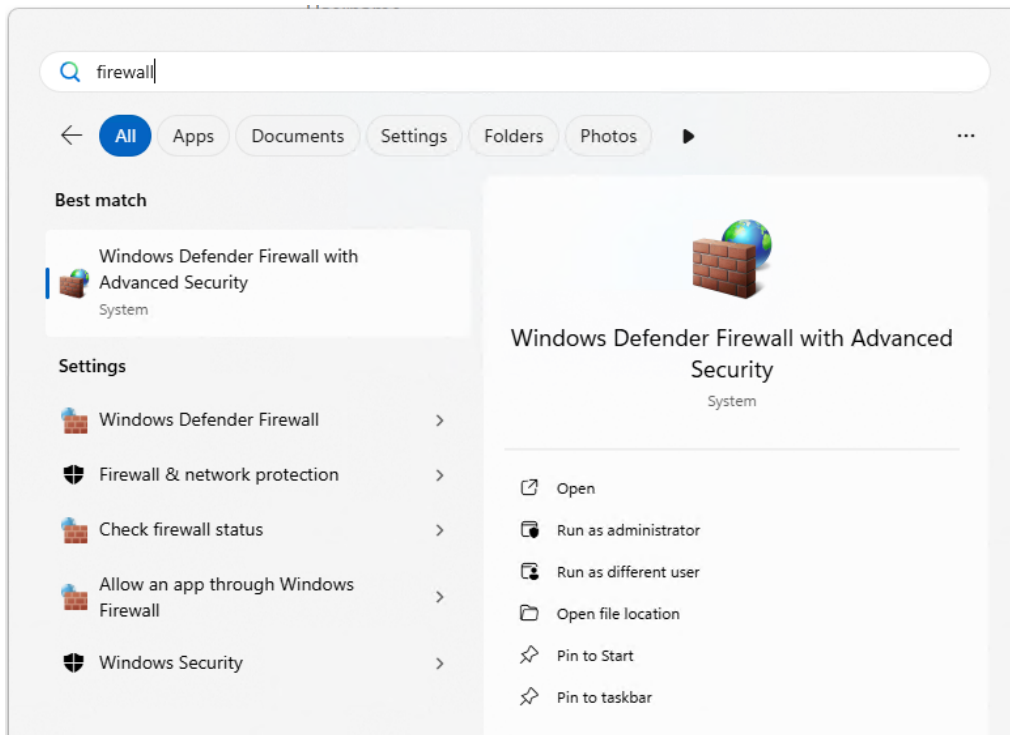
[Reset Your Password](#) [Help](#)

## 4. Firewall Access for Server PC

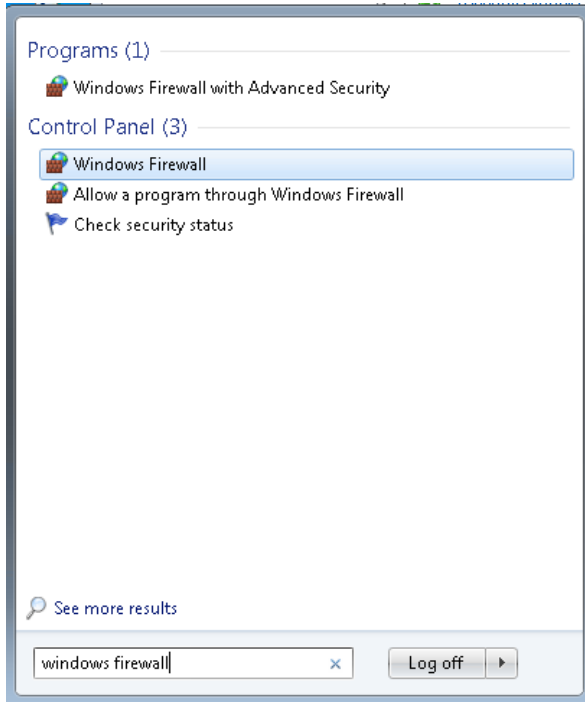
### 4.1 Accessing Inbound and Outbound Port Rules

To access GARDiS on a browser from a remote PC you need to allow the GARDiS ports through the firewall on the Server PC.

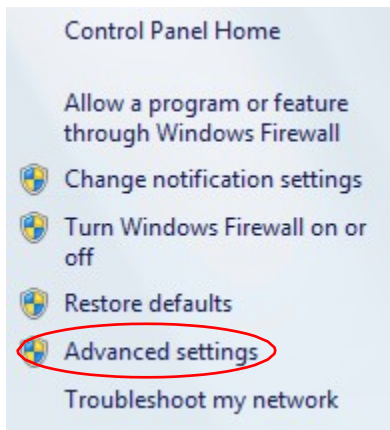
In the start menu, search for '**Windows Firewall**' and click on "**Windows Defender Firewall with Advanced Security**" for Windows 11 or Server 2025.



For Windows 10 or Server 2019 and older, in the start menu, search for '**Windows Firewall**' and click on it.



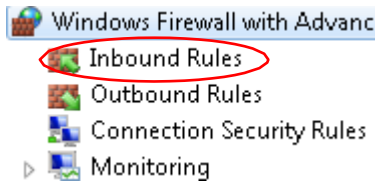
Look to the left hand panel and click '**Advanced settings**'.



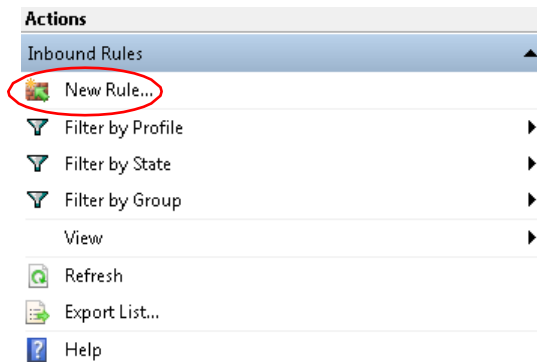
**NOTE:** For Windows 11 and Server 2025, this can be skipped.

## 4.2 Inbound Rules

In the left hand menu click 'Inbound Rules'.



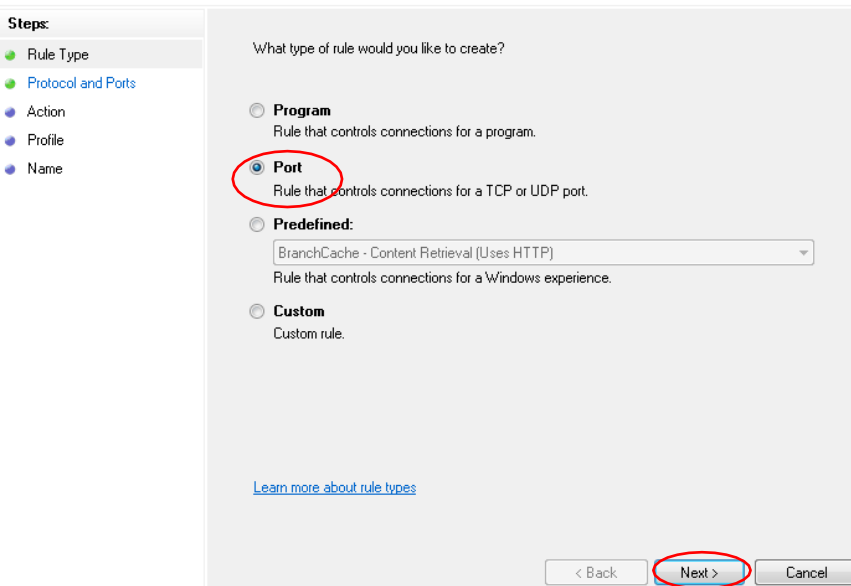
In the right hand menu click 'New Rule...'



Make sure 'Port' is selected, then click 'Next'.

### Rule Type

Select the type of firewall rule to create.



Make sure TCP is selected, then click the '**Specific Local Ports**' box and enter:

- 80
- 8715
- 8716

**NOTE:** Each port number must be followed by a comma.

Then click '**Next**'.

**Protocol and Ports**

Specify the protocols and ports to which this rule applies.

Make sure you've selected '**Allow the Connection**' then click '**Next**'.

**Action**

Specify the action to be taken when a connection matches the conditions specified in the rule.

By default Domain, Private and Public are ticked. Change as required then click **'Next'**.

**Profile**

Specify the profiles for which this rule applies.

**Steps:**

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

When does this rule apply?

**Domain**  
Applies when a computer is connected to its corporate domain.

**Private**  
Applies when a computer is connected to a private network location.

**Public**  
Applies when a computer is connected to a public network location.

[Learn more about profiles](#)

< Back   Next >   Cancel

Give the new rule a name and enter a description if required, then click **'Finish'**.

**Name**

Specify the name and description of this rule.

**Steps:**

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

Name:  
GARDIS Ports

Description (optional):

< Back   Finish   Cancel

## 4.3 Outbound Rules

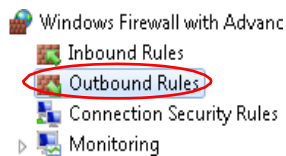
If using TDSi legacy controllers such as EX-Series and MG-Series, you may wish to place communication servers on other machines. This uses port 10001.

The online license activation also requires an outbound rule to allow:

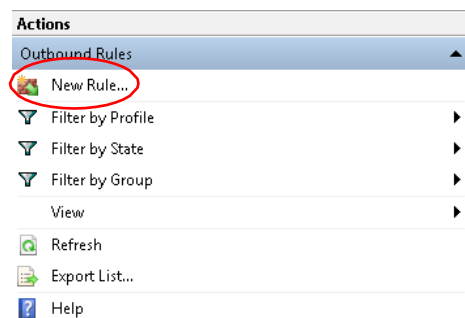
<https://tdsi-product-registration.com:8201>

One of the port numbers also needs to be entered into an **Outbound Rule**.

Windows Firewall Advanced Settings should still be open, click '**Outbound Rules**' in the left menu.



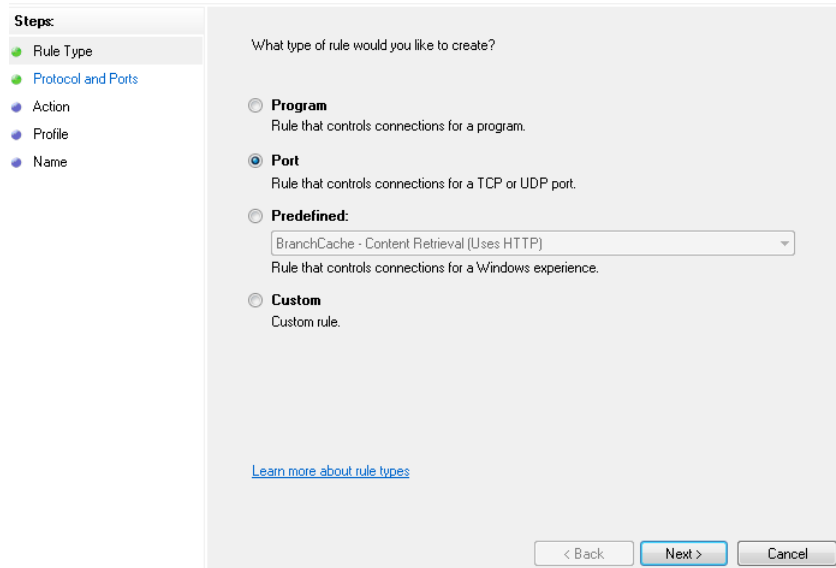
Click '**New Rule...**' in the right hand menu.



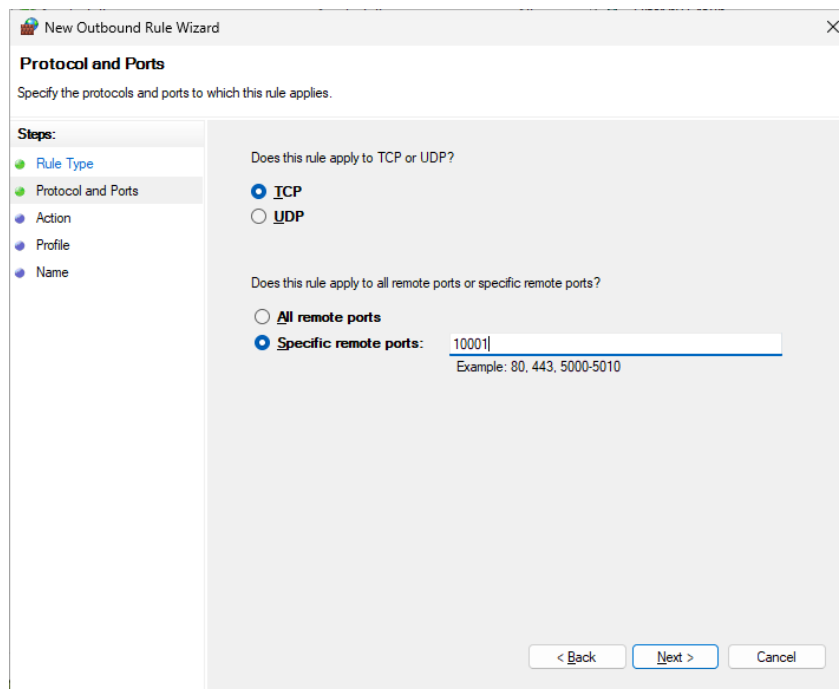
Select '**Port**' then click '**Next**'.

**Rule Type**

Select the type of firewall rule to create.



Make sure '**TCP**' is selected, then enter '**10001**' in the specific remote ports box. Then click '**Next**'.



Make sure **'Allow the Connection'** is selected, then click **'Next'**.

#### Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

**Steps:**

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

What action should be taken when a connection matches the specified conditions?

**Allow the connection**  
This includes connections that are protected with IPsec as well as those are not.

**Allow the connection if it is secure**  
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

**Block the connection**

[Learn more about actions](#)

< Back   Next >   Cancel

By default Domain, Private and Public are ticked. Change as required then click **'Next'**.

#### Profile

Specify the profiles for which this rule applies.

**Steps:**

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

When does this rule apply?

**Domain**  
Applies when a computer is connected to its corporate domain.

**Private**  
Applies when a computer is connected to a private network location.

**Public**  
Applies when a computer is connected to a public network location.

[Learn more about profiles](#)

< Back   Next >   Cancel

Name the rule as required then click '**Finish**'.

**Name**

Specify the name and description of this rule.

**Steps:**

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

Name:

Description (optional):

< Back   Finish   Cancel

## 5. Upgrading GARDiS

### 5.1 Uninstall the Previous Version

Go to Control Panel -> Programs and Features. Right click on GARDiS from the list of programs and select "Uninstall".

The software will be removed and the configuration settings will remain.

### 5.2 Install the New Version

Install the new version by following the steps in [Section 3](#) (Installer) from this manual.

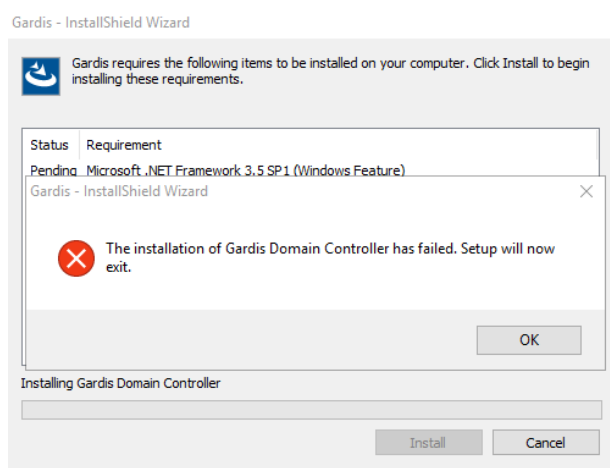
During the Configuration step, the previous settings will be displayed. Confirm and close.

The installer may ask to reboot the computer. This is recommended for successful software installation.

## 6. Troubleshooting

### 6.1 Installing on a Domain Controller

GARDiS cannot be installed on a domain controller. If you attempt to install on a domain controller you will see this error message:



### 6.2 SQL Installation Failure

If you encounter errors while installing SQL during the installation of GARDiS, open the 'Summary.txt' log file located here:

C:\Program Files\Microsoft SQL Server\120\Setup Bootstrap\Log\

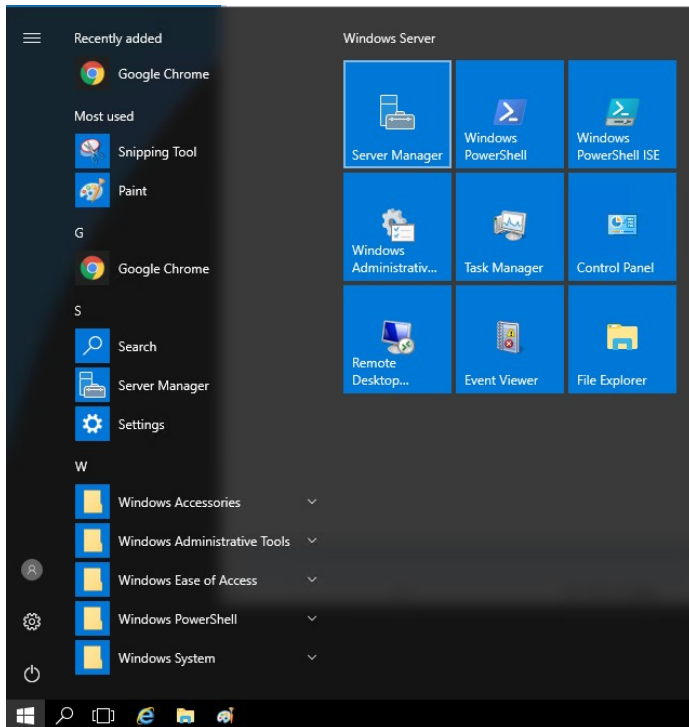
### 6.3 Troubleshooting – Windows Features

If you experience any issues while installing or running GARDiS, Windows may have been unable to automatically enable some of the Windows features. The following steps will show you how to enable all the required features depending on the version of Windows you are using.

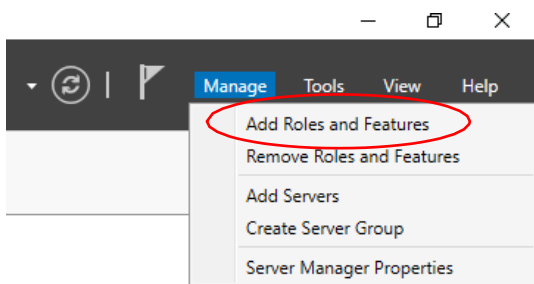
Make sure you check these Windows features.

### 6.3.1 Windows Server Features

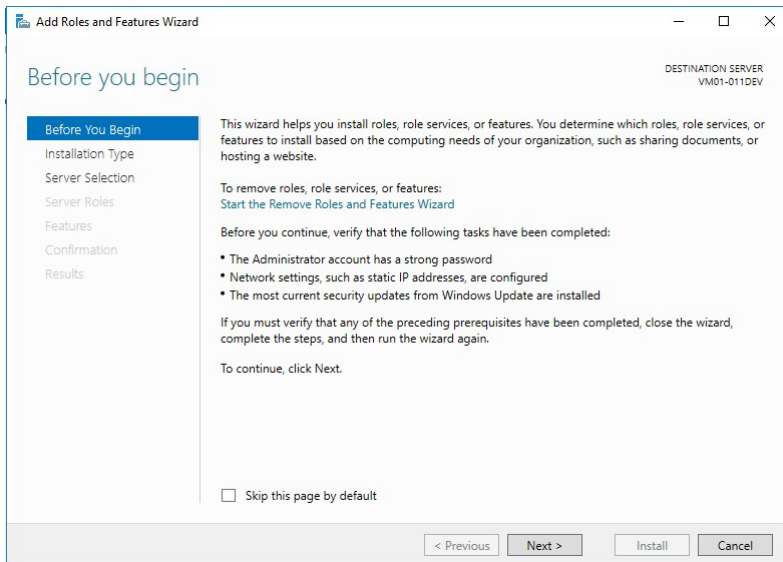
Windows features can be configured on (in this example) Windows Server 2016 by clicking the '**Start**' icon then clicking '**Server Manager**'.



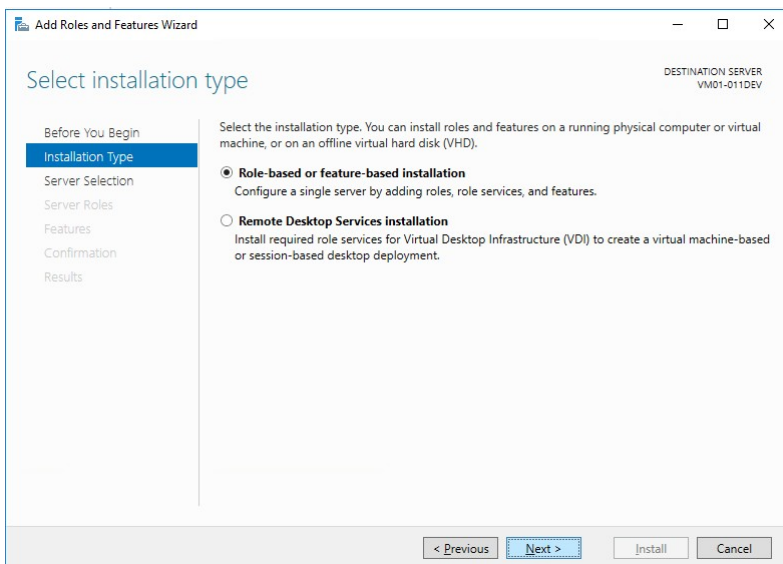
In the top right corner, click '**Manage**' then click '**Add Roles and Features**'.



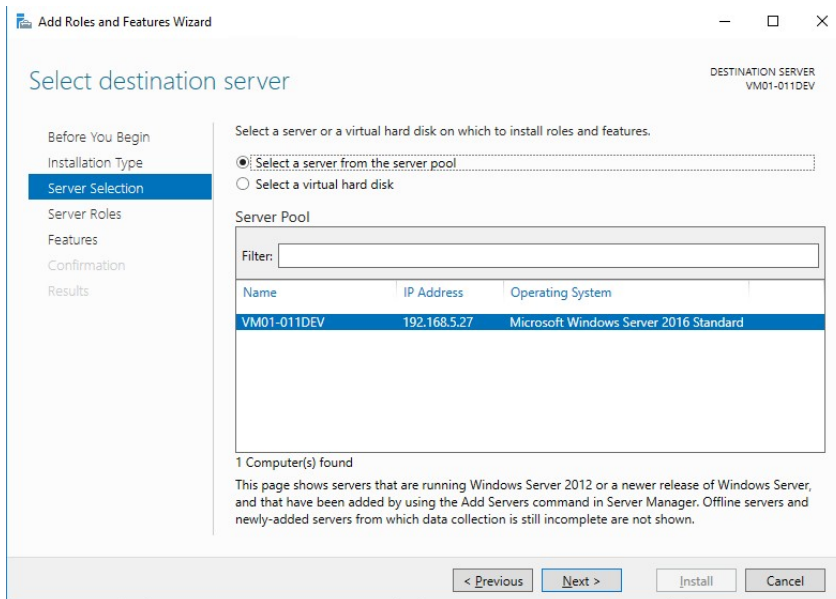
Click **'Next'**.



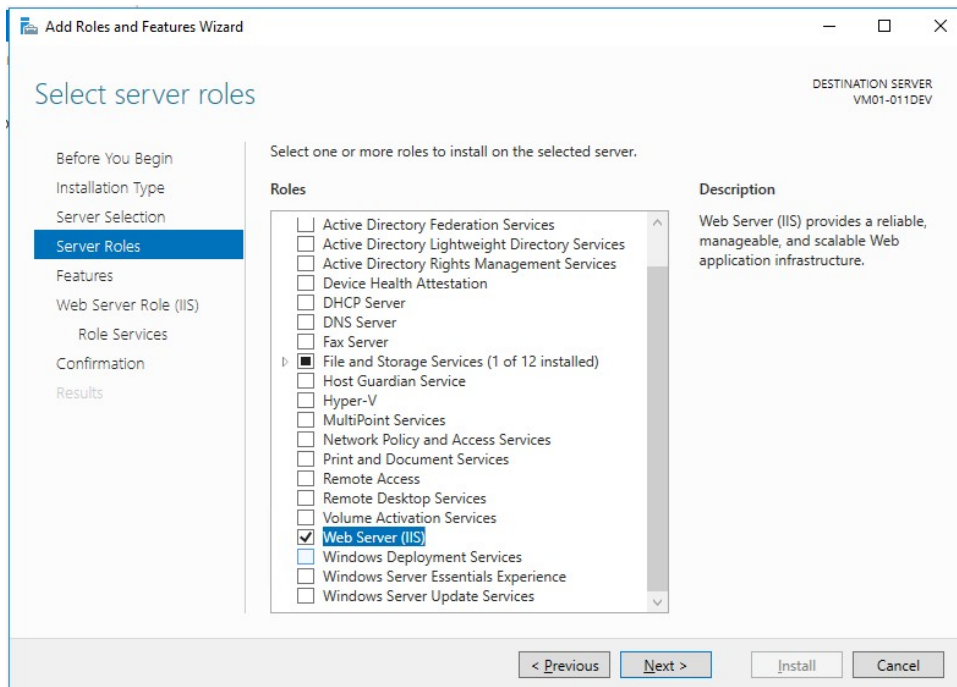
Select the required option then click **'Next'**.



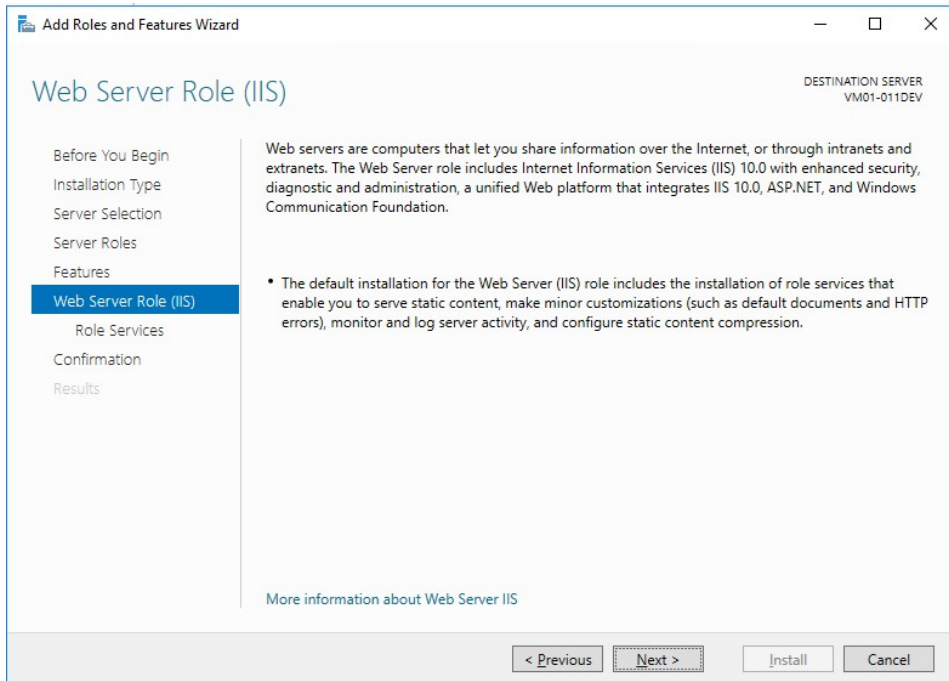
Click the required server then click '**Next**'.



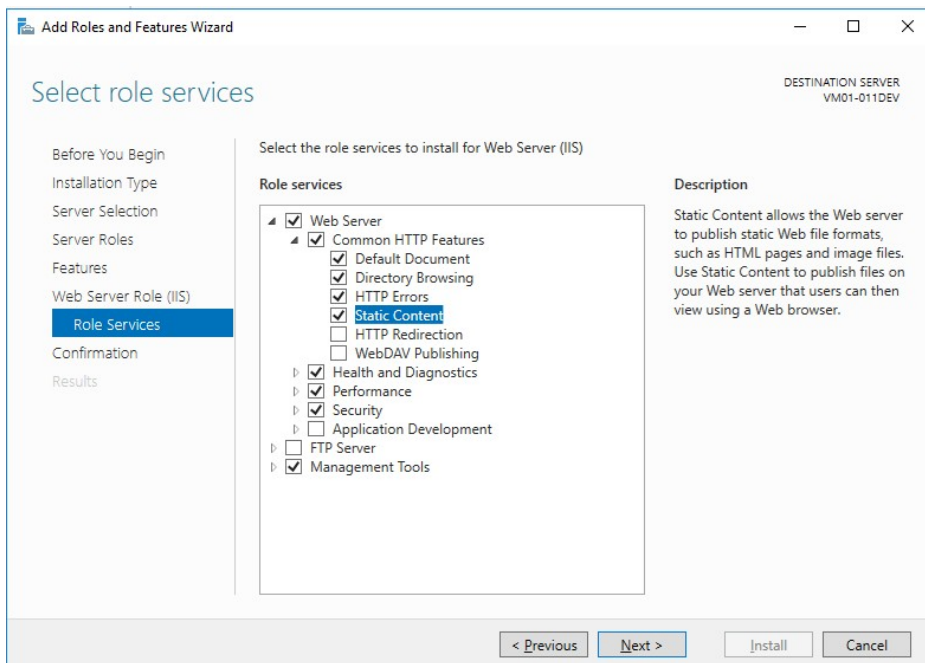
Scroll down the list to '**Web Server (IIS)**' then click to enable it. Then click '**Next**'.



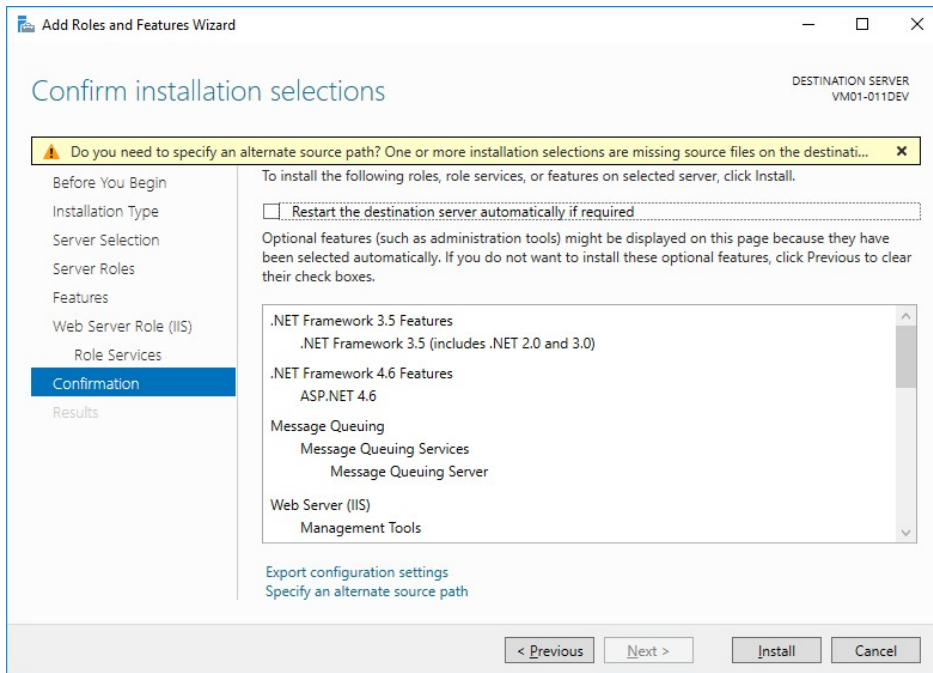
Select Web Server Role.



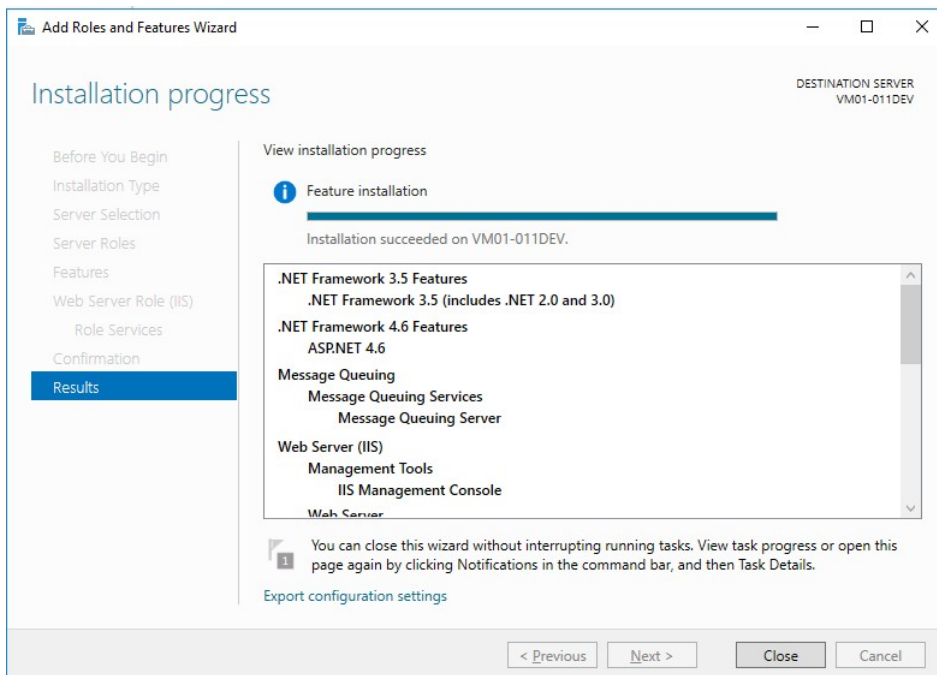
Select Role Services to begin editing the Windows Features. Go to [Section 7.5.3](#) for full details of the windows features to enable.



Click '**Next**' then '**Install**' to begin installing the windows features.



Wait for Windows to install the features, then once complete click '**Close**'.



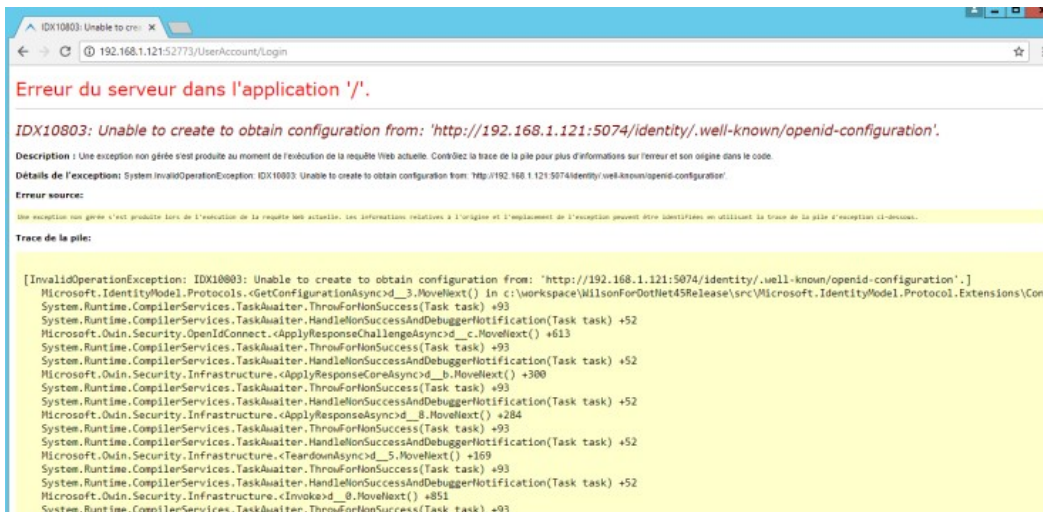
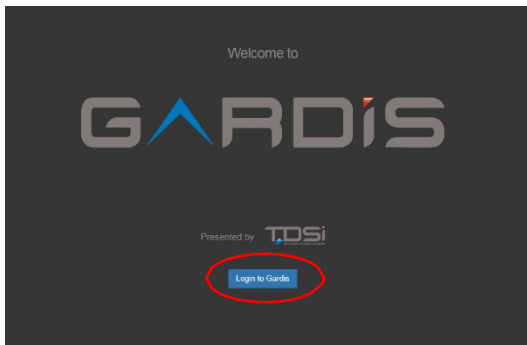
### 6.3.2 Window Features to Enable

**NOTE:** This section is no longer relevant from GARDiS v3.0 onward.

This legacy information can be obtained from Installation Guide Issue 16.

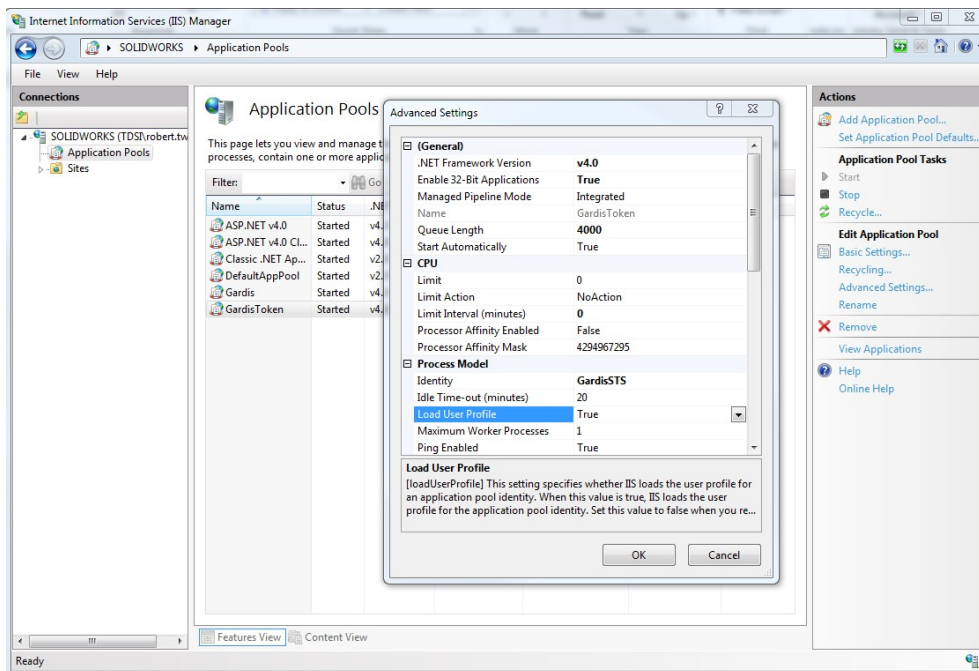
### 6.4 Login Button Error

**Symptom:** Can navigate to the login page, but when you click the **'Login'** button, the following screen appears with IDX10803 error.

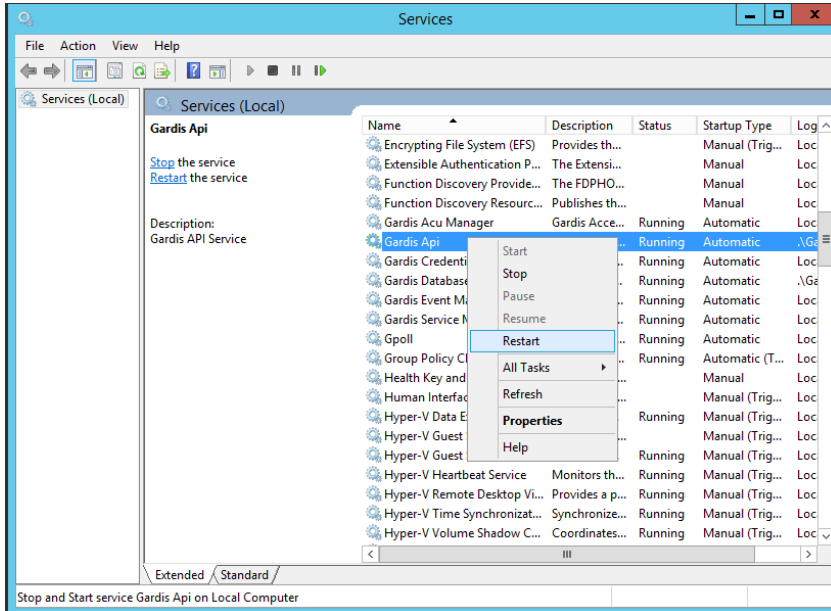


**Resolution:** Change the 'Load User Profile' setting in IIS to 'True'.

- Open 'Internet Information Services (IIS) Manager'.
- Find your computer in the connections menu on the left and click the '**Expand**' arrow.
- Click '**Application Pools**'.
- Left click 'GardisToken' then click 'Advanced Settings' in the right hand menu.
- Locate 'Load User Profile'.
- If it says false, click on it and change it to 'True'.



Once complete, open '**Services**' and find '**Gardis API**'. Right click it, then click '**Restart**'.

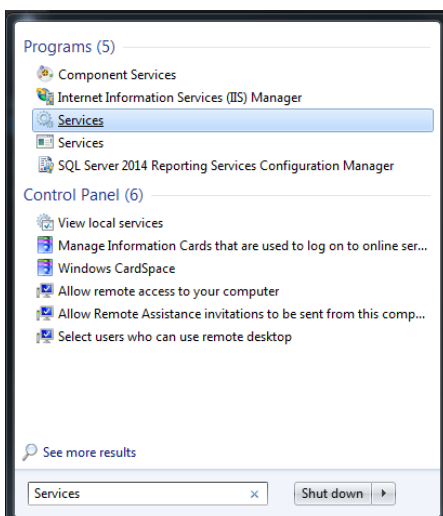


## 6.5 Unable to log in

The most likely cause of this issue is that the GARDiS services aren't running.

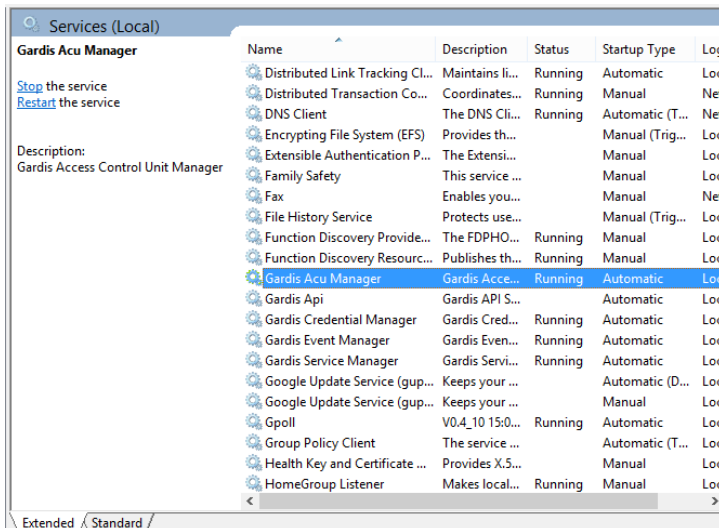
Once you've restarted your system after the install, GARDiS should start automatically within 3 minutes.

To check, open **'Services'**.

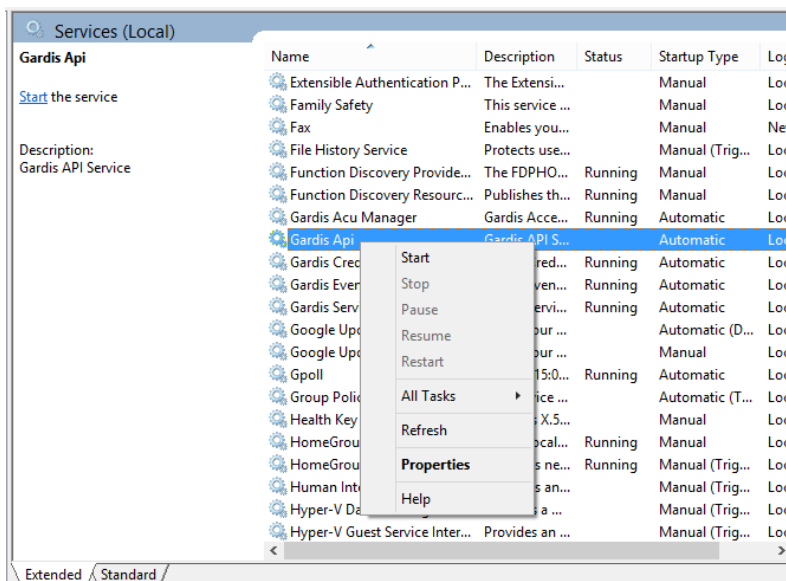


Make sure the following services are running.

- Gardis ACU Manager
- Gardis API
- Gardis Credential Manager
- Gardis Event Manager
- Gardis Service Manager
- SQL Server (GARDiS)
  - \*If SQL database is hosted on the same machine as the application



If the services aren't running, right click on it and click 'Start'.



Now you're sure the services are running, browse to:

**http://localhost:52773** or the IP address you've set previously during the installation.

You will now be able to log into GARDiS using your username and password.

## 7.HTTPS

The default protocol for GARDiS is HTTP. This is, in most cases, acceptable as all data is being transferred on a local area network. In a medium to large organisation, data protection and securing data will be more active. For this, the protocol needs to be configured to use Https, which encrypts all data between the client (Browser) and the server.

It is recommended to stop all GARDiS services until all tasks are complete.

### 7.1 Enabling HTTPS

First run the GARDiS configuration tool and select the Https option.

The screenshot shows the 'Service URLs' section of the configuration tool. It includes a radio button for 'Network' (selected) and a dropdown menu showing '10.0.9.123'. There are also radio buttons for 'Basic Mode' (selected) and 'Expert Mode'. Below this is the 'Protocol' section with radio buttons for 'Http' and 'Https' (selected).

Change the protocol from '**Http**' to '**Https**'.

Https has a default port of 443 and if this is the only website running on this PC (recommended), the website port can be set to this value.

The screenshot shows the 'Ports' section of the configuration tool. It contains three input fields, each with a refresh button: 'Security Token Service Port' (44310), 'Gardis API Port' (44311), and 'Gardis Website Port' (443). Below the fields is the text 'Connect to Gardis using the following URL'.

The '**Security Token Service**' and '**API**' can then be changed to any value and as an idea using a 443xx gives an indication they are also on a https. Finally click the '**Confirm**' button to save these settings.

If an error occurs at this point in updating the IIS settings, this can be ignored as changes are required to be set in the IIS.

## 8.VPN and WAN

GARDiS will not work internally as the VPN network cannot be accessed on the same WAN.

# TDSi<sup>UK</sup>

Part of the  **Vita**protech Group

 [tdsi.co.uk](https://tdsi.co.uk)

 [sales@tdsi.co.uk](mailto:sales@tdsi.co.uk)

 +44(0)1202 723 535

Unit 10 Concept Park, Innovation Close,  
Poole, Dorset, BH12 4QT, UK