finPOWER Connect 3
Web Services Installation and Configuration

Version 3.13

5th July 2021

Table of Contents

Disclaimer

This document contains information that may be subject to change at any stage.

All code examples are provided "as is".

Version History

Date	Version	Name	Changes
09/01/2014	1.00	PH	Created.
18/02/2014	1.01	PH	Updated to detail configuration interface.
27/02/2014	1.02	PH	Updated from AM feedback.
04/03/2014	1.03	PH	Updated to include more installation details.
07/03/2014	1.04	PH	Updated after feedback from support.
10/03/2014	1.05	PH	Detailed installation of a test certificate for HTTPS.
14/03/2014	1.06	PH	Removed hyperlinks to localhost.
19/03/2014	1.07	PH	Added Security section.
26/03/2014	1.08	PH	Updated to assist installation on a proper Windows Server.
07/04/2014	1.09	PH	Added Web Server Time Zone section.
15/05/2014	1.10	PH	Updated troubleshooting guide for address database issues.
08/07/2014	1.11	PH	Added note regarding SQL Server licencing.
03/12/2014	1.12	PH	Updated system requirements.
26/06/2015	1.13	PH	Updated troubleshooting section.
04/07/2016	3.00	PH	Updated for version 3.
19/09/2016	3.01	PH	Fixed typo to administration URL.
23/11/2016	3.02	PH	Updated Web Configurations information.
07/03/2017	3.03	PH	Updated Troubleshooting section.
02/02/2018	3.04	PH	Updated for release 3.1.
04/02/2019	3.05	PH	System requirements updated and centralised configuration file detailed.
07/02/2019	3.06	PH	Multi-Sever and Server Farms section added.
13/02/2019	3.07	PH	Immediate Application Startup section added.
10/02/2020	3.08	PH	Updated
26/05/2020	3.09	PH	Reviewed and updated for 3.03.02 release.
07/08/2020	3.10	PH	Removed reference to IE 11.
17/05/2021	3.11	PH	Updated system requirements relating to .NET 4.7.2
28/06/2021	3.12	PH	Rolled back .NET 4.7.2 requirement and added more Application Pool information.
05/07/2021	**3.13**	**PH**	**Updated to .NET 4.8**

Introduction

This document describes the steps to be taken to install and configure the finPOWER Connect Web Services.

finPOWER Connect Web Services is a Web application that runs under Microsoft's Internet Information Services (IIS) Web Server software.

Installation and configuration should only be undertaken by a network administrator who should be familiar with both IIS configuration and network security.

System Requirements

- Please ensure the PC onto which the Web Services are being installed has the following:
  - Windows Server 2012 or above or Windows 7 or above for test purposes.
  - The Microsoft .NET framework 4.8 or above.
  - Microsoft Internet Information Services (IIS) version 6 or above.
    - ASP.NET must also be installed (version 4 or above).
    - A SSL certificate must be installed for production use.
- For the Web Services to function correctly, please also ensure:
  - The finPOWER Connect database that the Web Services will connect to is available to the Web Server.
    - A SQL Server database must be used in production.
      - Version 2008 or above.
      - This should, if possible, be configured to use mixed mode authentication (SQL Server and Windows Authentication mode).
      - If this is not possible, a Windows domain account will need to be created for the IIS Application Pool to use to access the database; this is outside of the scope of this document.
    - NOTE: MS Access databases should be used for test purposes only.
- The finPOWER Connect database must be licensed for the **Web Services and Automation** Add-On and also the **Enterprise Edition** (which allows SQL Server databases to be used).
- Any sites wishing to consume the Web Services must have access to the Web Server either via the Internet, Intranet, VPN or other method. Configuration of any of these is outside of the scope of this document.

NOTE: The Microsoft licence required for running SQL Server for finPOWER Connect, including Web Services, is outside of the scope of this document.

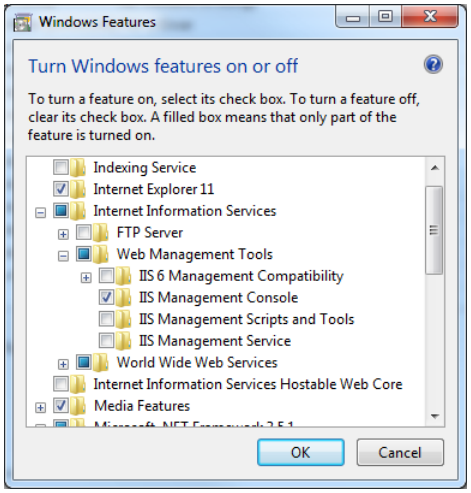
Contact your Microsoft dealer who can explain the best licensing options available for your site.

Installing IIS for Testing

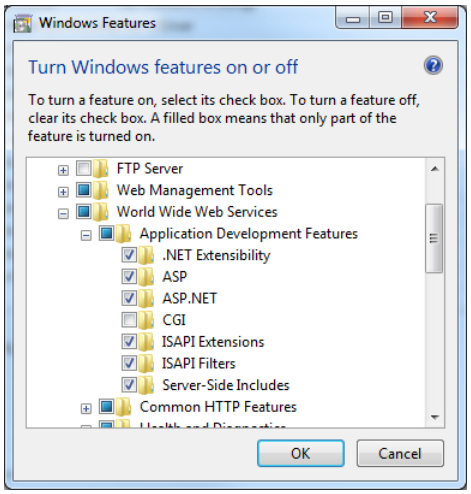
These steps detail installation of IIS on a non-server version of Windows 7/8 and are provided for testing purposes only.

In a non-testing environment (e.g. staging or production), this should be performed by a network administrator with the relevant skills. See Production Setup and Configuration for more information.

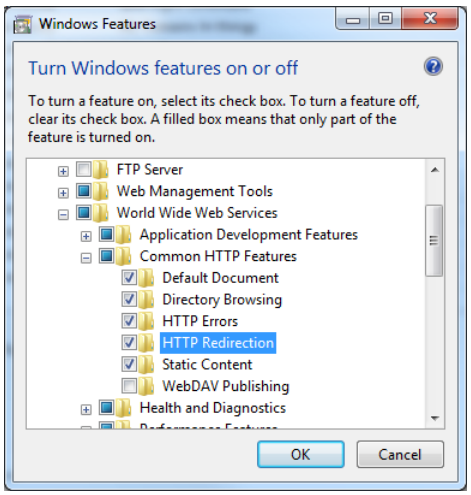
- Ensure you are logged into Windows as an Administrator.
- Option **Control Panel** and select **Programs**, **Turn Windows features on or off**.
  - WARNING: Do not uncheck any options not shown as checked in the screenshots below since they may have been configured by other applications)
- From the **Windows Features** dialog, ensure the following are selected (these may vary slightly between different versions of Windows):
  - **Internet Information Services**, **Web Management Tools**
    - Ensure **IIS Management Console** is checked.



- **Internet Information Services**, **World Wide Web Services**, **Application Development Features**
  - Check all items except CGI.



- **Internet Information Services**, **World Wide Web Services**, **Common HTTP Features**
  - Check all items except WebDAV Publishing.



- Click **OK** to complete installation.

Installing ASP.NET 4 and .NET 4.8

Installation of ASP.NET 4 is essential to ensure that all of the correct Application Pools are set up under IIS and all of the necessary features installed that are required by the Web Services, e.g. Microsoft MVC and Web API.

- Open a Windows Command Prompt as an Administrator.
- Type **cd C:\Windows\Microsoft.NET\Framework\v4.0.30319** and press **Enter**.
- Type **aspnet_regiis.exe -ir** and press Enter.

finPOWER Connect 3.4.1 and above targets the .NET framework 4.8. Therefore this must also be installed on the Web Server hosting the Web Services:

- This can be downloaded from: https://dotnet.microsoft.com/download/dotnet-framework/net48

Windows Firewall Configuration for Testing

Installation of IIS for testing purposes (as detailed above) allows the Web Services to be tested from the local PC but it is often desirable to test from another PC or device (e.g., an iPhone or Android phone).

To allow this, you may need to configure the Windows Firewall as follows:

- Open **Windows Control Panel**.
- Select **System and Security** and then **Windows Firewall**.
- Select the **Allow a program of feature through Windows Firewall**.
- Ensure the **World Wide Web Services (HTTP)** is checked.
  - Select the desired options, e.g., **Domain** and **Home/Work (Private)**.
- Click **OK**.
- This should allow the Web Services to be accesed via the PC name, e.g.:
  - **http://MyPC/WebServices2**
  - NOTE: Some devices, e.g., Android phone, may have trouble resolving the DNS. In these cases you may need to use the IP address of the PC, e.g.:
    - **http://192.168.16.120/WebServices2**
    - You can find the IP address of a PC by opening a command prompt and typing **ipconfig** and pressing Enter. Use the **IPv4 Address**.

Setup File

- The Web Services are deployed as a zip file (**finPOWERConnectWS3.zip**). The latest version can be obtained from Intersoft Systems.
- The zip file contains a **Readme.htm** file detailing the version and any Web Services-specific Knowledge Base articles.
    - NOTE: Since the Web Services use the finPOWER Connect business layer, most additions and fixes will be listed in the Knowledge Base under finPOWER Connect and not the Web Services.
- The zip file contains a **finPOWERConnectWS3** folder which contains the entire Web Services Web application.
- This setup file should be extracted to a folder on either the Web Server or some other media which can then be used to copy the files to the Web Server, e.g., a USB flash drive or network location.

Web Server Time Zone

As at version 3.0.0.0, Time Zone support was added to finPOWER Connect.

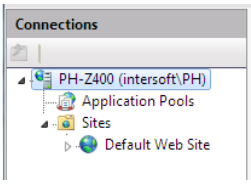
Most dates with a time portion, e.g., Log dates are stored in UTC format in the database along with Time Zone information.

Since a Web Server may exist in a different Time Zone to the user (or be configured to use a different Time Zone), certain dates that are formatted server-side may appear in a different Time Zone.

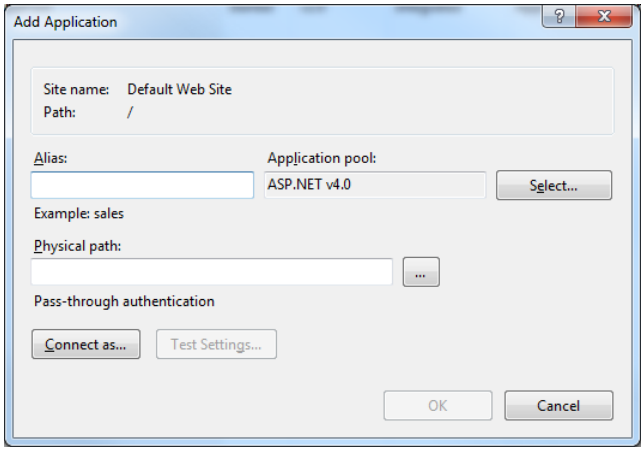
Generally, it is advisable that the Web Server hosting the Web Services is configured to use the same time zone that the majority of Users reside in which is typically the Time Zone defined under Global Settings in finPOWER Connect.

New Installation

- Start the **Internet Information Services (IIS) Manager**.
  - If you are using Windows 7, you can start this quickly by clicking the **Start** button and typing **IIS** in the search box.
- Expand the computer node and then the **Sites** node in the **Connections** pane.



- Right-click on **Sites**, **Default Web Site** and select **Add Application**. The following dialog is displayed:

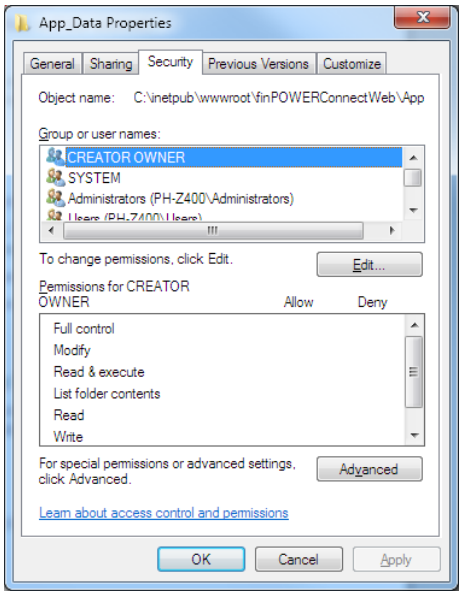


  - Enter an Alias for the application, e.g., **finPOWERConnectWS3**.
  - Enter the Physical path (the folder where the Web application files will be stored):
    - Click the **...** button.
    - Create or locate a folder to store the files.
      Generally you would create a folder in the **c:\inetpub\wwwroot** folder with the same name as your Web application, e.g.,
      c:\inetpub\wwwroot\finPOWERConnectWS3.
    - Ensure the **ASP.NET v4.0** or **.NET v4.5** Application Pool is selected or, create a new Application Pool as described in the **Application Pool Configuration** section.
  - Click the **OK** button.
  - You have now created a Web application.
  - Using Windows Explorer, copy the files from the setup's finPOWERConnectWS3 folder into the new Web application folder.
- Select the new Web application node in the **Connections** pane of the IIS Manager.
- At this stage you should now be able to access the Web Services login form from a Web browser, e.g.,
  http://localhost/finPOWERConnectWS3/WebAdmin/Login

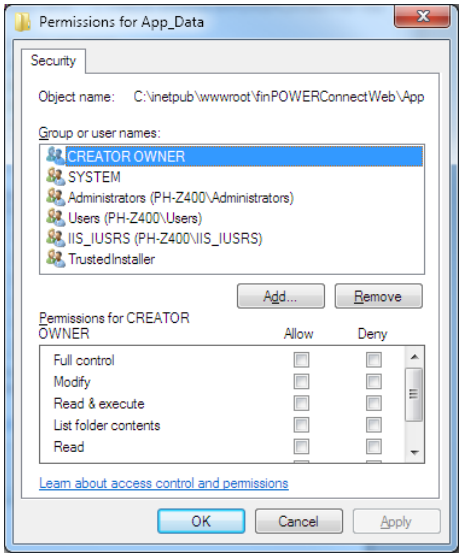
Allowing Access to Files in the App_Data folder

Configuration information is stored in the App_Data folder of the Web application. You must ensure that the Web application has read and write to this folder.

- Locate the **App_Data** folder using Windows Explorer, e.g., **c:\inetpub\wwwroot\finPOWERConnectWS3\App_Data.**
- Right-click on the folder and select **Properties** and the click on the **Security** tab.



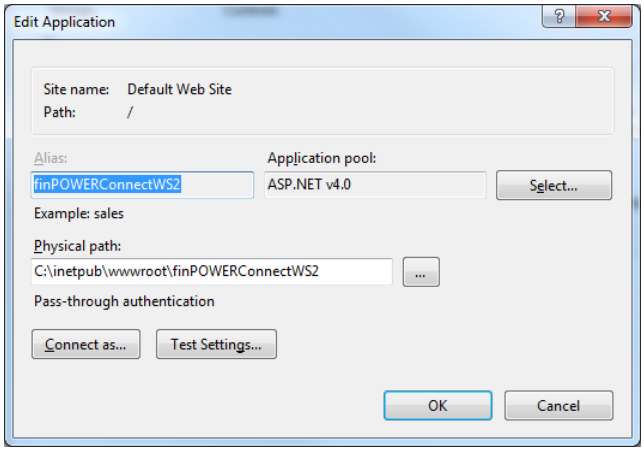
- Click the **Edit** button.



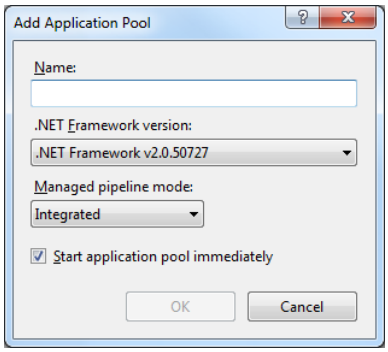
  - You should see a group called **IIS_USRS** and it is this group that you must grant the correct permissions to. Ensure that the following have the **Allow** box checked (checking Modify should check all items listed below):
    - Modify
    - Read & execute
    - List folder contents
    - Read
    - Write

Application Pool Configuration

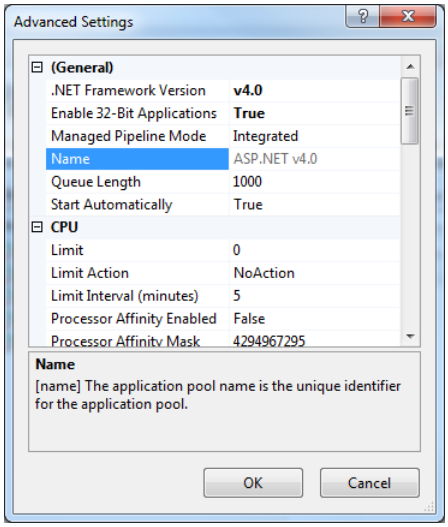
- finPOWER Connect 3 targets the .NET framework 4.8. Therefore this must be installed on the Web Server hosting the Web Services:
  - This can be downloaded from: https://dotnet.microsoft.com/download/dotnet-framework/net471
- Each Web site or Web application within IIS uses an Application Pool. To see which Application Pool a Web application is using or change the application pool, click on the site or application in the **Connections** pane of the **Internet Information Services (IIS) Manager** and select **Basic Settings** in the Actions pane:



  - The **Select...** button allows a different Application Pool to be used.
- To view an Application Pool's settings or add a new Application Pool, click the **Application Pools** node in the **Connections** pane of the **Internet Information Services (IIS) Manager**.
  - If other Web sites or applications are using the same Application Pool as your Web application, it may be advisable to create a new Application Pool as follows:
    - Right click the **Application Pools** node and select **Add Application Pool...**.



    - Give the Pool a name, e.g., **finPOWERConnectWS3** and click **OK**.
  - To edit the settings of an existing (including the newly added) Application Pool, right-click the Application Pool in the Application Pools grid and select **Advanced Settings...**



- Ensure the following Advanced Settings are configured:
  - .NET Framework Version: **v4.0**
    - In Windows 8 and other, later, versions of Windows this is:
      - .NET CLR Version: **v4.0.30319** (or similar)
  - Managed Pipeline Mode: **Integrated**
  - Enable 32-Bit Applications: **True**
    - Only required if testing against an MS Access database, otherwise, set to **False**.

- Edit the Basic Settings of your Web application and select the new Application Pool you have just created.

IMPORTANT: If you are running finPOWER Connect Cloud and Web Services on the same machine, ensure each is using its own, independent IIS Application Pool

Updating an Existing Installation

This section assumes that all of the steps listed in the **New Installation** section were followed when first installing the Web Services.

- Take a backup copy of your existing configuration files **config.xml** (and optionally, **config.redirect**)in the **App_Data** folder**.**
- Use Windows Explorer to remove all folders under the existing Web Services Web Application folder.
- Using Windows Explorer, copy the files from the setup's finPOWERConnectWS3 folder into the Web application folder.
- Copy your backed up configuration files back into the **App_Data** folder.
- Ensure IIS has access to the **App_Data** folder as per the **Allowing Access to Files in the App_Data folder** section.

WARNING: Failure to take a backup copy of your existing configuration file will result in the Web Services having to be re-configured.

Enforcing HTTPS for Secure Access

When running a Web application dealing with sensitive data, it is important that users can only access the site via the HTTPS protocol which encrypts data going to and from the application.

This means that a certificate must be installed under IIS.

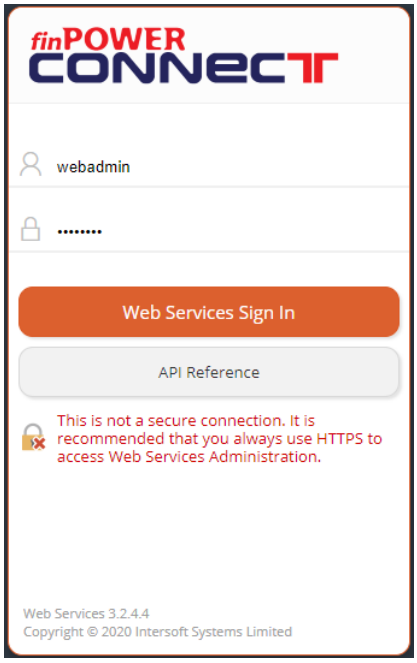
The only situations in which you might not need to use HTTPS in a production environment are:

- The Web Services are installed on the same physical server as the Web application using them.
- The Web Services are on the same private network as the Web application using them and the network has been configured so that only the Web server hosting the Web application can view and access the Web Services server.

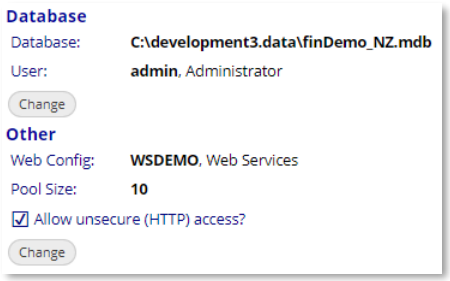
Enforcing HTTPS from the Web Services Administration Facility

HTTPS access can be enforced from within the Web Services Administration facility as follows:

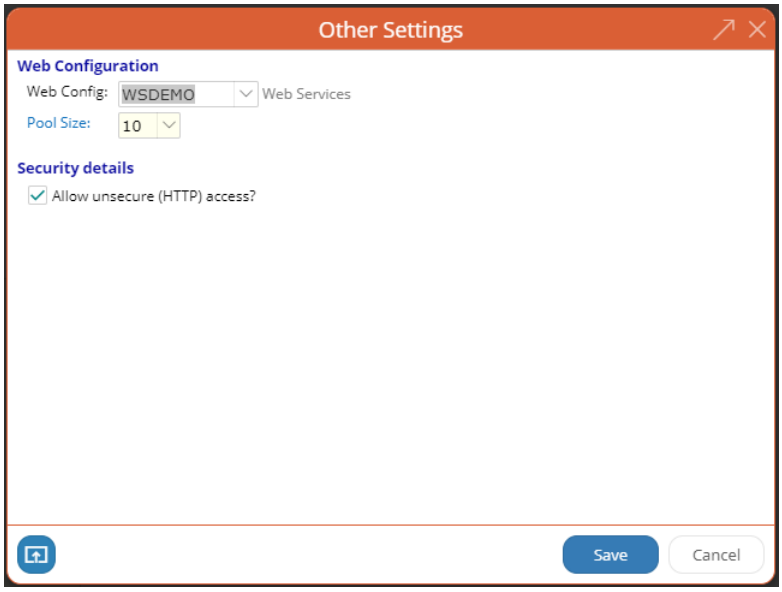
- Sign in to the Web Services Administration facility.
  - For a new installation, the Web Administration User Id is **webadmin** and the Password is **password**.



- From the **Configuration** page, under the **Other** heading, select **Change**.



- Uncheck the **Allow unsecure (HTTP) access** box:



- Click the **Save** button.

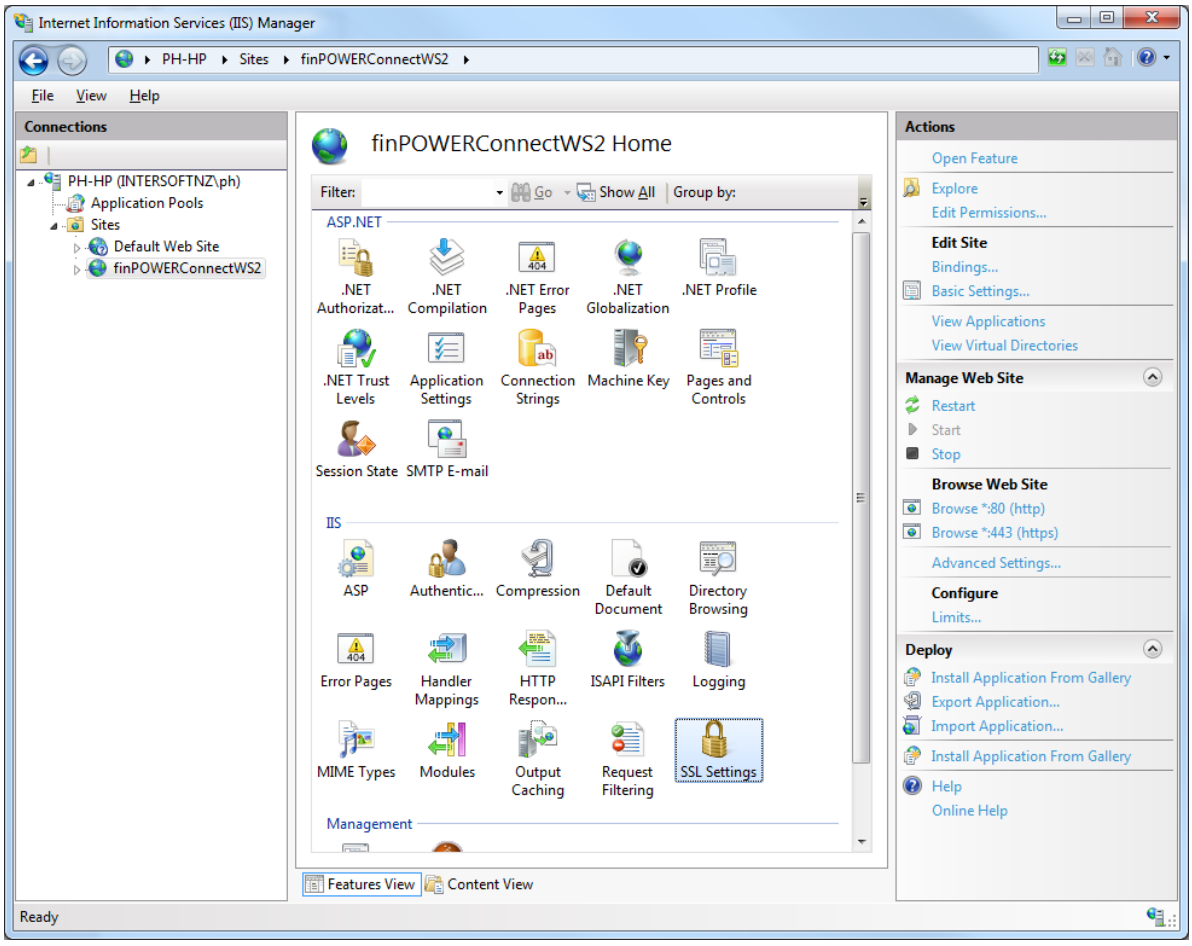
WARNING: The Save button will be disabled is the configuration file is read-only. This is usually due to the incorrect Windows permissions being applied to the App_Data folder.

NOTE: This still allows unsecure (HTTP) access when signing in locally to the Web Server.

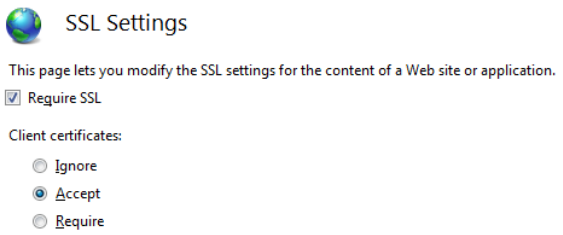
Enforcing HTTPS from IIS

HTTPS access can also be enforced from within IIS as follows:

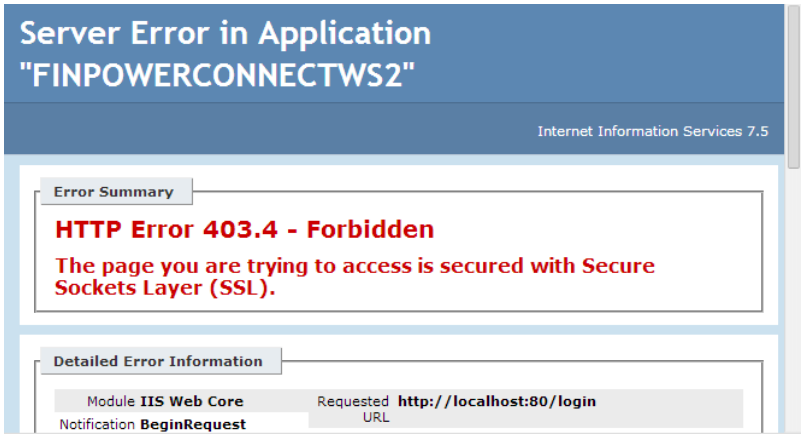
- Launch **Internet Information Services (IIS) Manager**.
- Locate and select the finPOWER Connect Web Services application in the **Connections** explorer.
- Select the **SSL Settings** item.



- Right-click **SSL Settings** and select **Open Feature**.



- Check **Require SSL** and under Client certificates, select **Accept**.
  - NOTE: If this checkbox is disabled, you will need to install a certificate as outlined in the next section.
- Click **Apply** in the **Actions pane.**
- Attempting to login using the HTTP protocol should now return a response similar to the following:


Server Error in Application "FINPOWERCONNECTWS2"
Internet Information Services 7.5
Error Summary
HTTP Error 403.4 - Forbidden
The page you are trying to access is secured with Secure Sockets Layer (SSL).
Detailed Error Information
Module IIS Web Core
Notification BeginRequest
Requested URL http://localhost:80/login

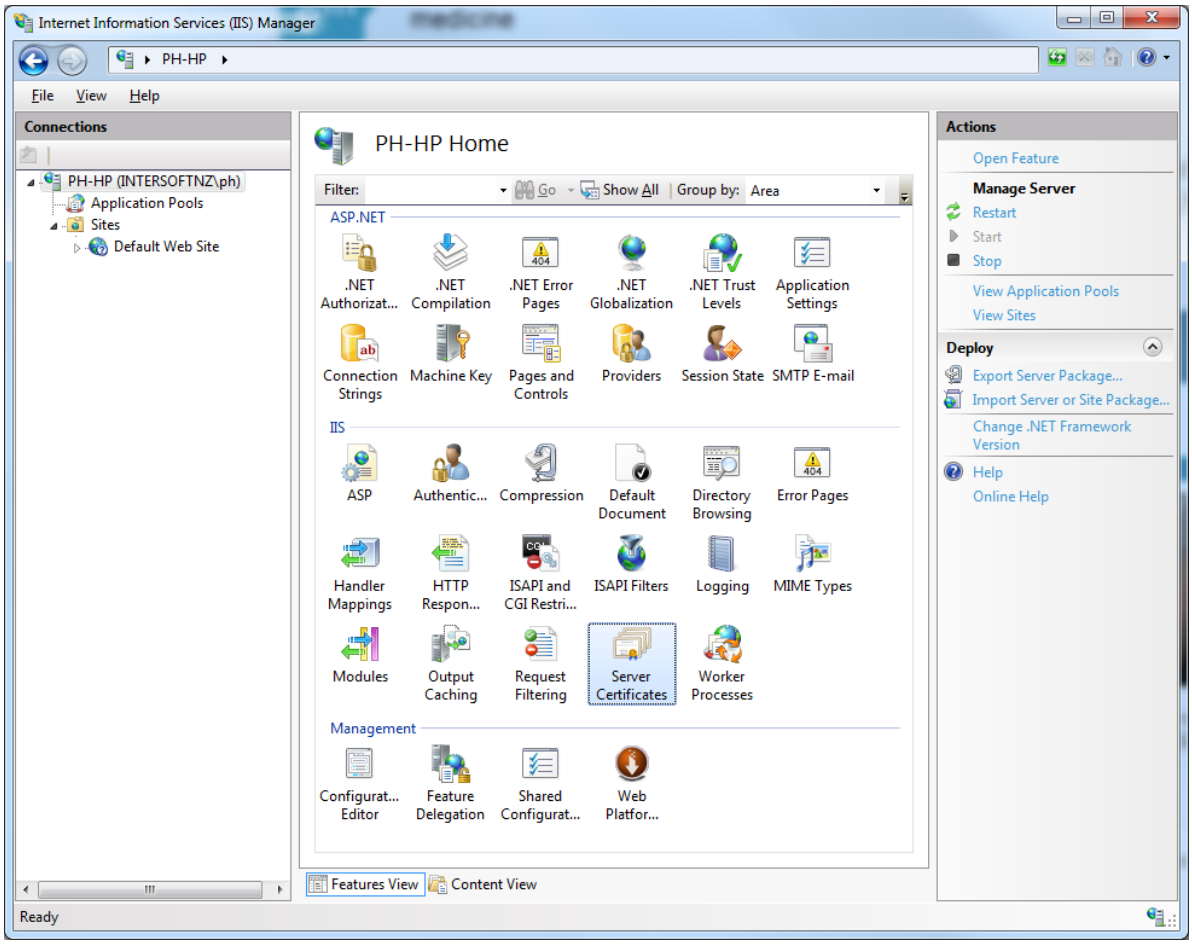
Installation of a Self-Signed Certificate for Testing

For testing purposes it is useful to be able to use HTTPS to access the Web Services.

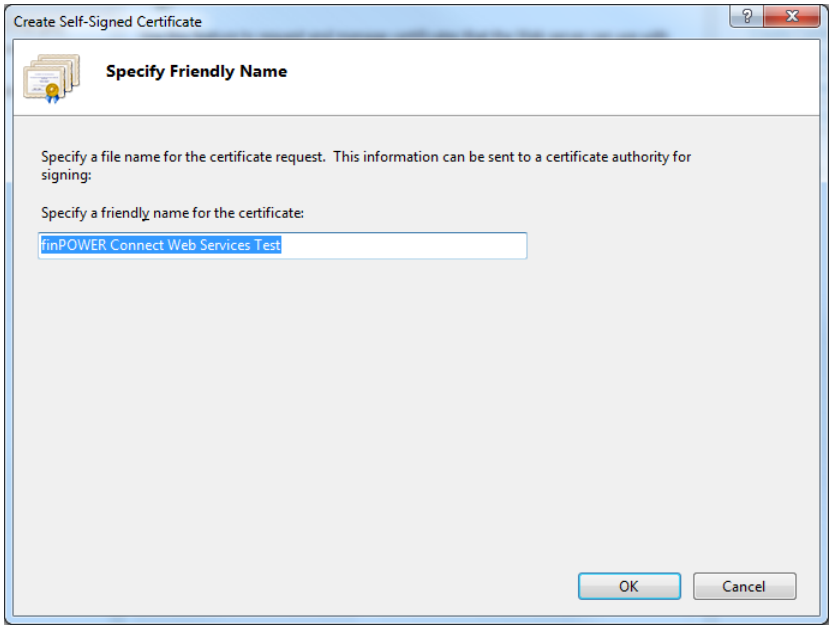
Acquiring a 'real' certificate and configuring IIS to use this certificate should be left to a system administrator. However, for testing purposes, a self-signed certificate can be used and this section details creating and installing such a certificate.

Create a Self-Signed Certificate

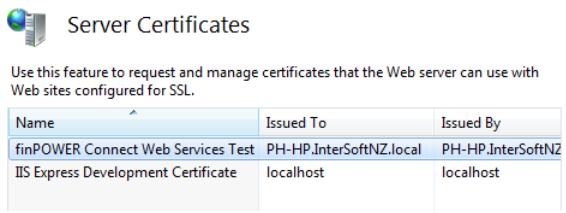
- Launch **Internet Information Services (IIS) Manager**.
- Click the root node in the **Connections** explorer.
- Select the **Server Certificates** item.



- Right-click **Server Certificates** and select **Open Feature**.
- In the **Actions** pane, select **Create Self-Signed Certificate...**

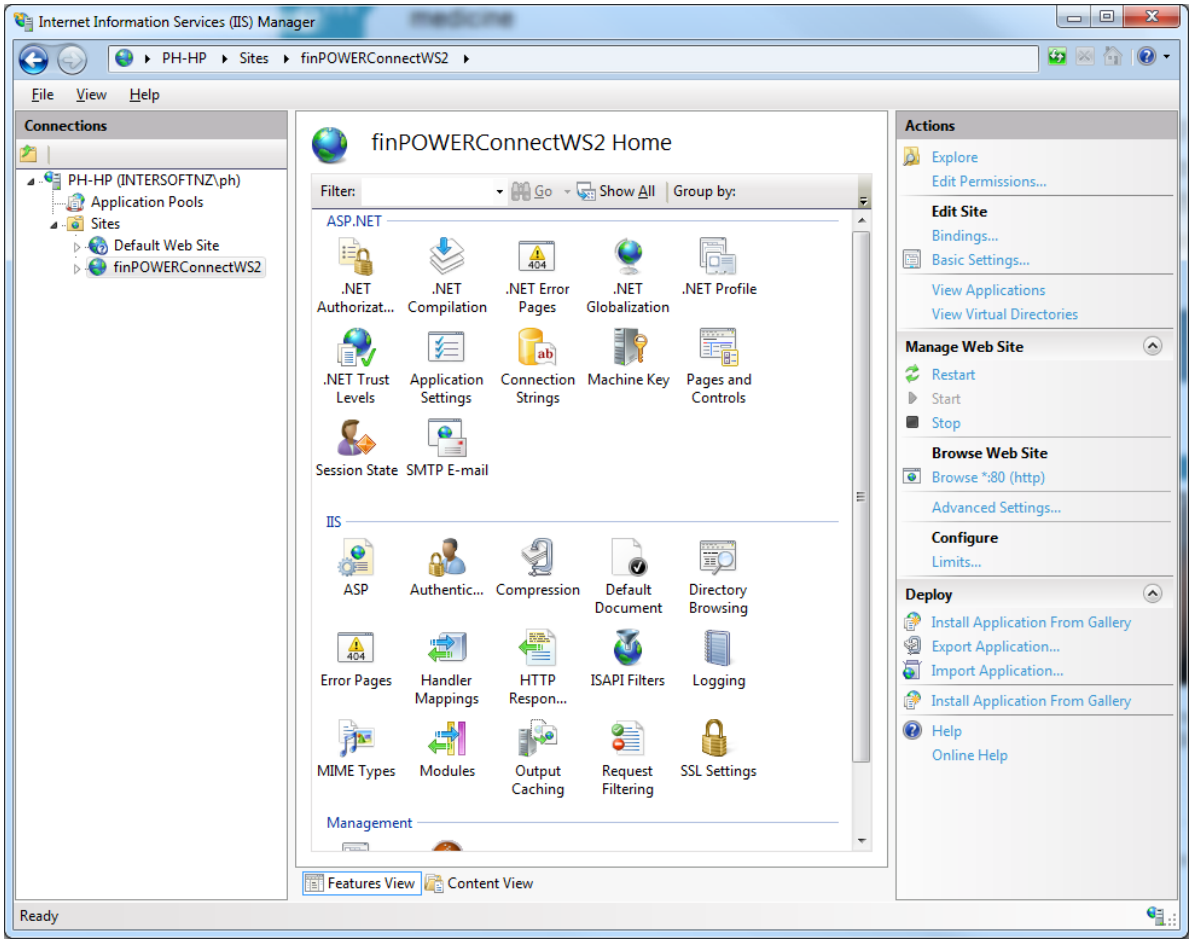


- Enter a friendly name, e.g., **finPOWER Connect Web Services Test**.
- Click the **OK** button.
- IIS creates a new self-signed certificate, e.g.

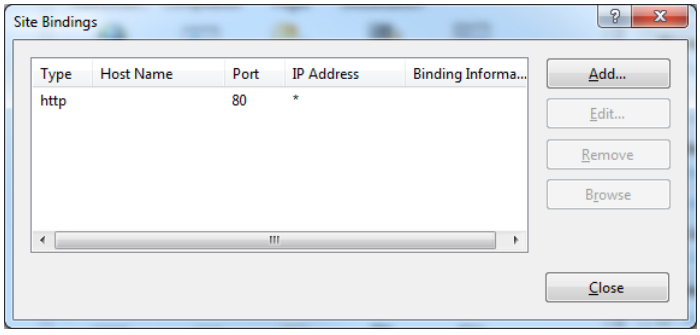


Enabling HTTP Bindings for Web Services

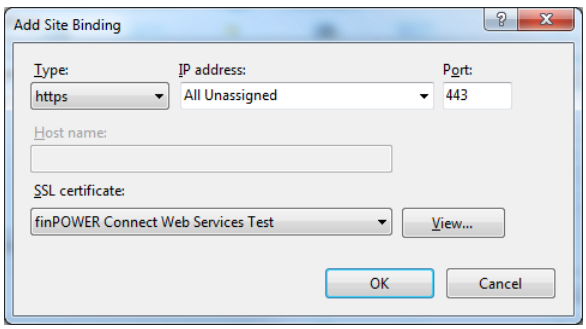
- Launch **Internet Information Services (IIS) Manager**.
- Locate and select the finPOWER Connect Web Services application in the **Connections** explorer.



- In the **Actions** pane, under the **Edit Site** heading, select **Bindings...**



- Click the **Add...** button.

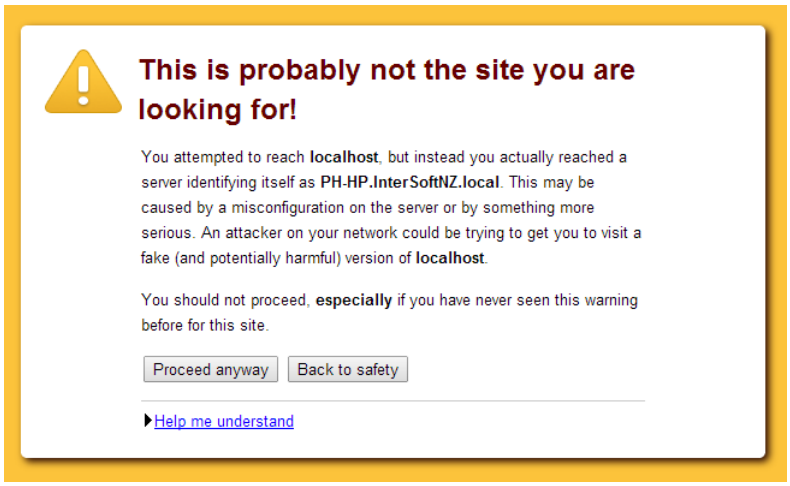


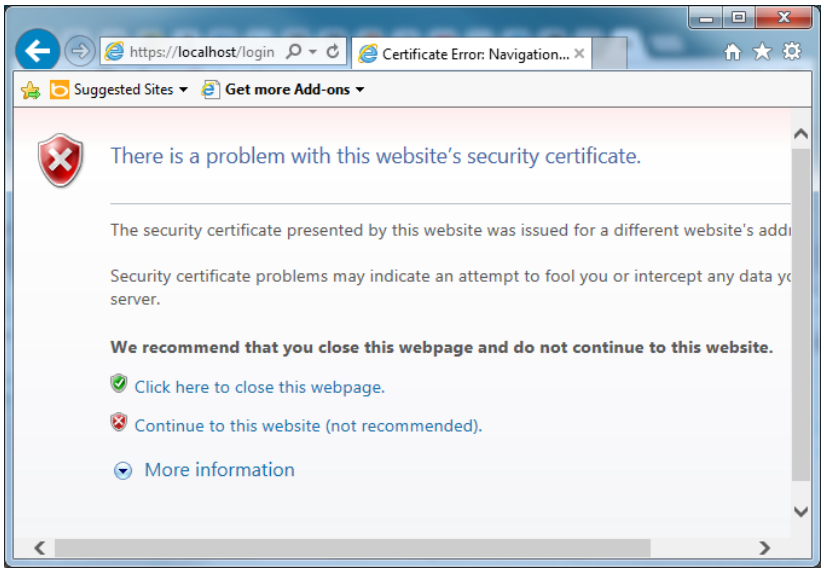
Set the following:

- Type: https
- Port: 443

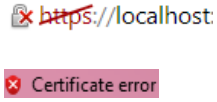
- SSL certificate: finPOWER Connect Web Services Test

- Click the **OK** button.
- SSL has now been enabled for the Web Services.
- Since this is a self-signed certificate, you will receive a warning when navigating to the Web Services Administration login page, e.g.





- Click the **Proceed anyway** button (Chrome) or the **Continue to this website (not recommended)** link (Internet Explorer).
- Note that whilst you are testing with a self-signed certificate, the Web browser will display a warning alongside the URL, e.g.



Configuration

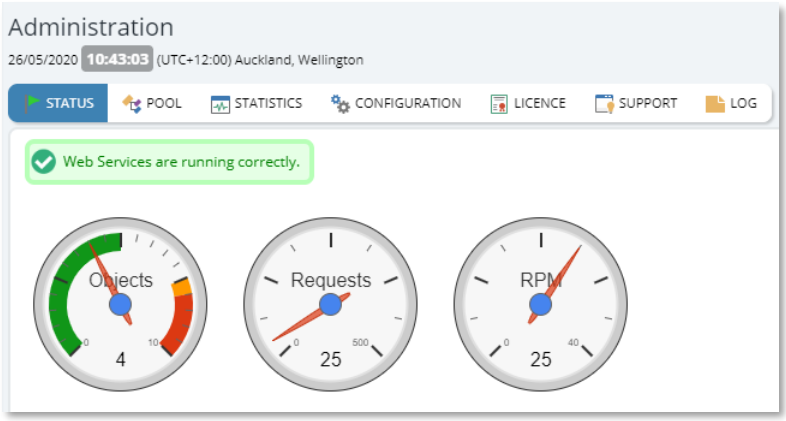
Configuration details are stored in the **App_Data/config.xml** file. Note that this file is not included with the setup but is created when settings are first configured.

NOTE: See the next section, Centralised Configuration for Multi-Server Setups if you have more than one web server.

An administration facility is provided to allow updates to this file.

The administration facility uses session state to keep the user logged in.

The Status page allows you to quickly see the current state of the Web Services.



NOTE: When a new Web Services installation is first performed, the configuration file will not exist in the App_Data folder.

Upon first saving the configuration file, e.g., by setting Database Connection details, the IIS application may restart resulting in a 401 error in the status bar. Simply sign out and sign back in again if this happens.

Centralised Configuration for Multi-Server Setups

By default, configuration information is stored in the **App_Data/config.xml** file.

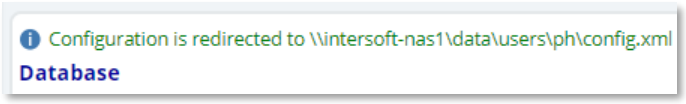
If however you have more than one web-server, or are running a server farm, you may wish to centralise configuration.

This is achieved by adding a **config.redirect** file to the **App_Data** folder.

If this file exists and contains text then this is used as the path of the configuration file, e.g.:

```
\\intersoft-nas1\data\webconfig\config.xml
```

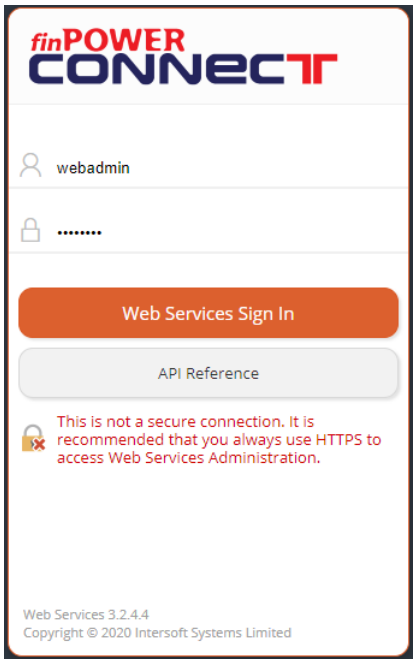
Both the Web Services default page and the Configuration page show special information if a redirected configuration is used:



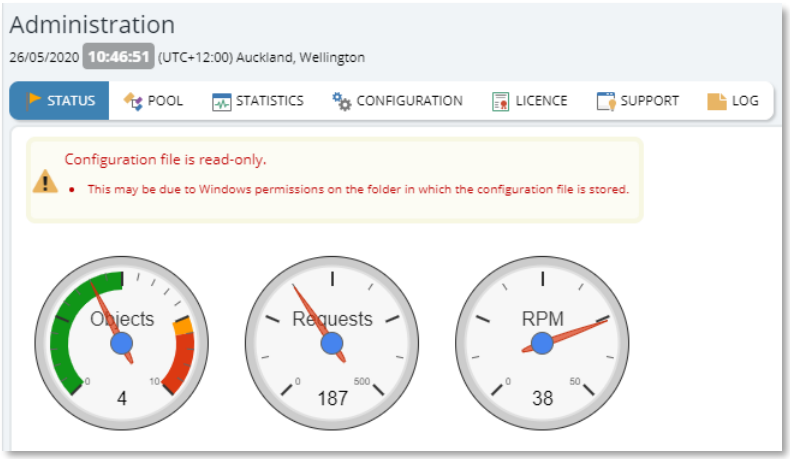
The "Servers" view allows you to see all Web Servers that are accessing the configuration file as described in Multi-Server and Server Farms.

Signing In to the Administration Facility

- Using a modern Web Browser (e.g., Google Chrome, the latest Microsoft Edge browser), navigate to the **/WebAdmin** page.
- Sign in using a Web Administration User Id or **webadmin** and a Password **password**.

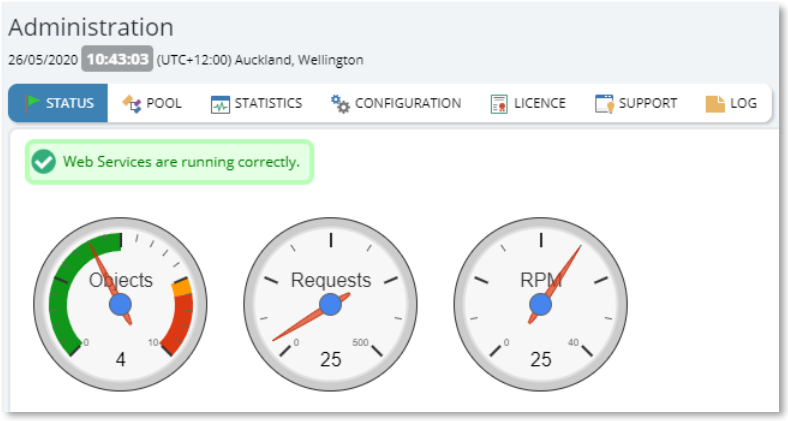


- If this is a new installation of the Web Services, the **Status** widget's heading will be pink and the widget will display a warning, e.g., "Configuration file does not exist."
  - This warning can be ignored since the configuration file (App_Data/config.xml) will be created as soon as any of the settings, e.g., the Database Connection) are first edited and saved.
- Other warnings should not be ignored, e.g., if the App_Data folder has the incorrect Windows permissions:

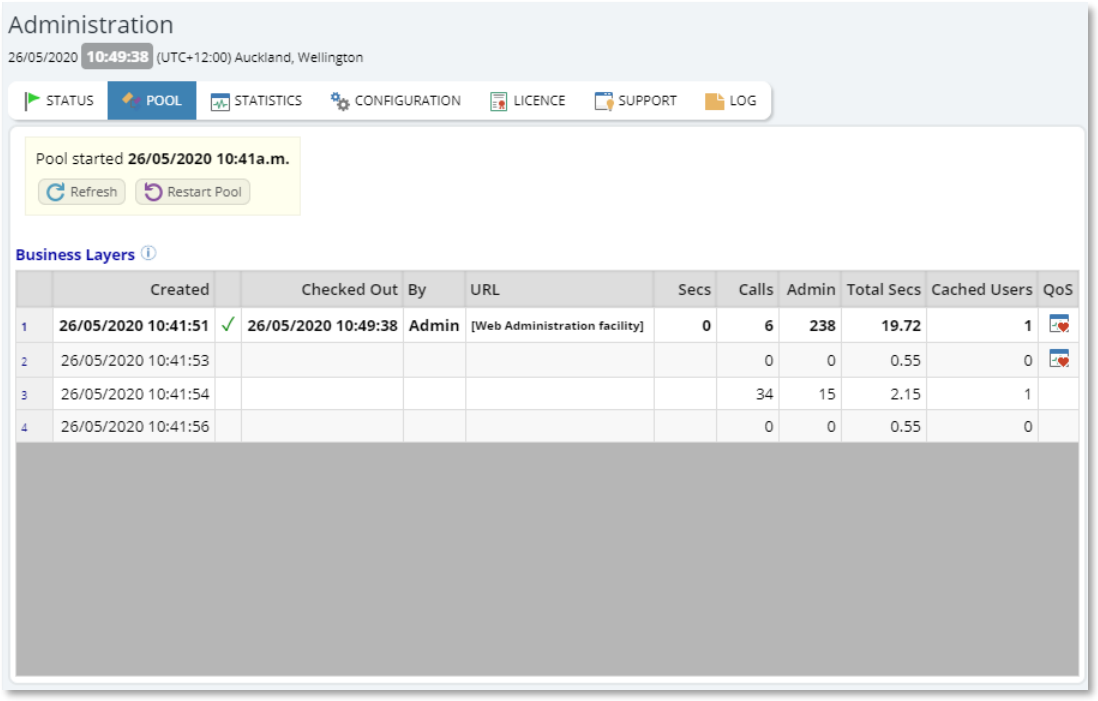


Business Layer Pool

- The Status page shows an overview of Business Layer Pool activity in the form of three gauges:

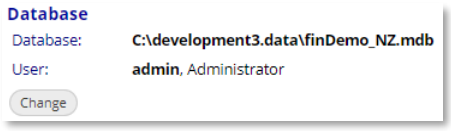


- More information about the business layer pool can be viewed from the **Pool** page:

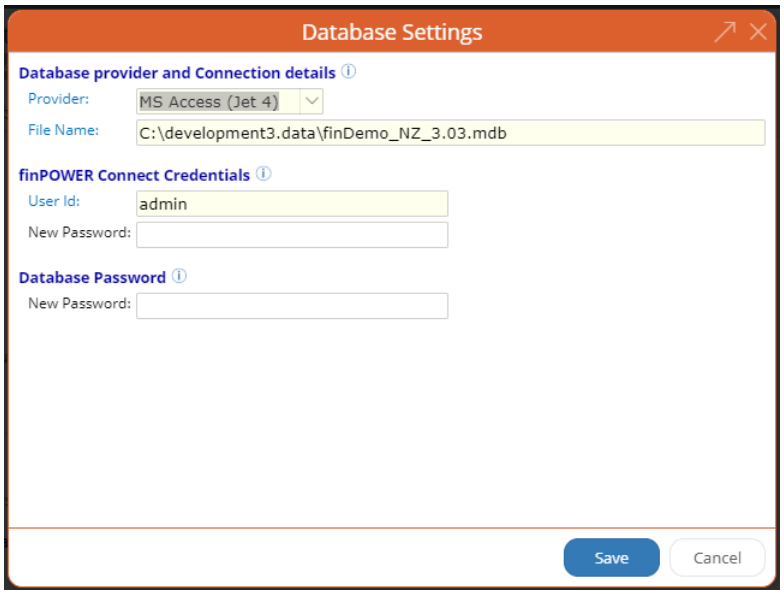


Database Connection

- The database to which the Web Services are connected can be configured via the **Configuration** page or via the **Database Settings** menu item:



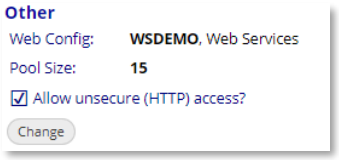
- This displays the **Database Settings** form:



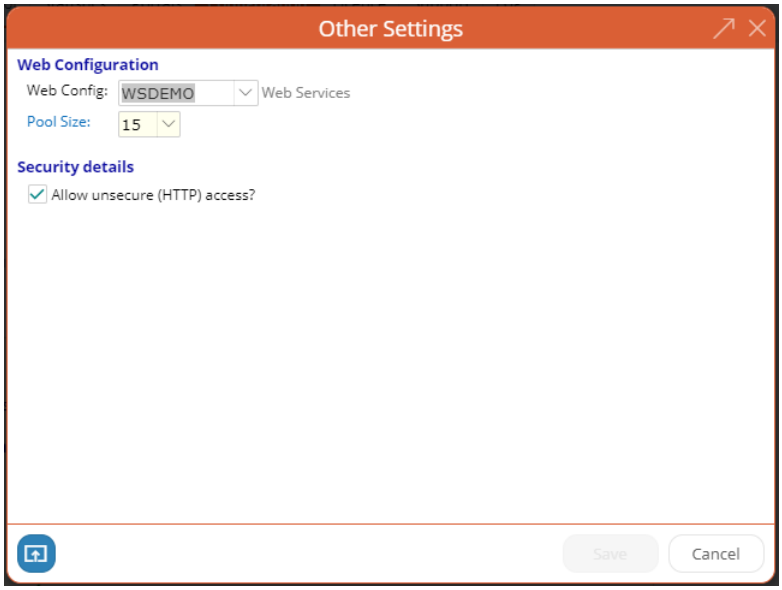
  - **Database provider and Connection details**
    - Always use SQL Server in a production (i.e., non-testing) environment.
      - SQL Server should be configured to use mixed-mode security. The login credentials can then be specified.
        - If this is not possible then IIS will need to be configured to use an Application Pool that specifies a Windows Domain user in order for the SQL Server to be accessed.
        - Using the SQL Server **sa** password is fine for testing on a local copy of SQL Server but should never be used in a production environment.
      - The Port is only necessary if SQL Server is listening on a non-standard port, i.e., not port 1433.
    - For testing purposes, an MS Access database can be used but:
      - The IIS Application Pool must be configured to 'Enable 32-bit Applications' as detailed under Application Pool Configuration.
      - The MS Access database must be at a location accessible to the Web Server, e.g., on the same PC in a C:\data folder.
        - Because IIS does not (by default) use a Windows domain User Account, it will not have access to any network drive mappings.
  - **finPOWER Credentials**
    - Specify a valid finPOWER Connect User and their password.
    - These credentials are used when initialising the business layer and also for an administration tasks (e.g., maintaining Web Subscribers). They are also used for Client access.

Other Settings

- Other Web Service settings are configured via the **Other** section on the **Configuration** page of the **Other Settings** menu item:



- This displays the **Other Settings** form:



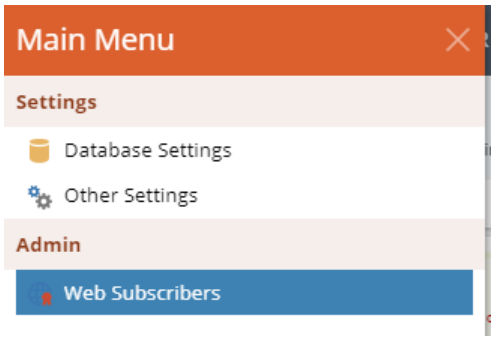
  - **Web Configuration**
    - Specify the Web Configuration to use and the maximum number of objects that can exist in the business layer pool.
      - Web Configurations are defined within the finPOWER Connect Windows interface under the **Tools** menu, **Web**, **Web Configurations**.
      - A Web Configuration allows services to be configured for use from a Web Server as opposed to using the Global Settings or User Preferences defined within finPOWER Connect.
      - See the finPOWER Connect Web Configurations section for more information.
  - **Security details**
    - Allows you to specify that unsecure (HTTP) access is allowed.

WARNING: Production systems should always use secure (HTTPS) access.

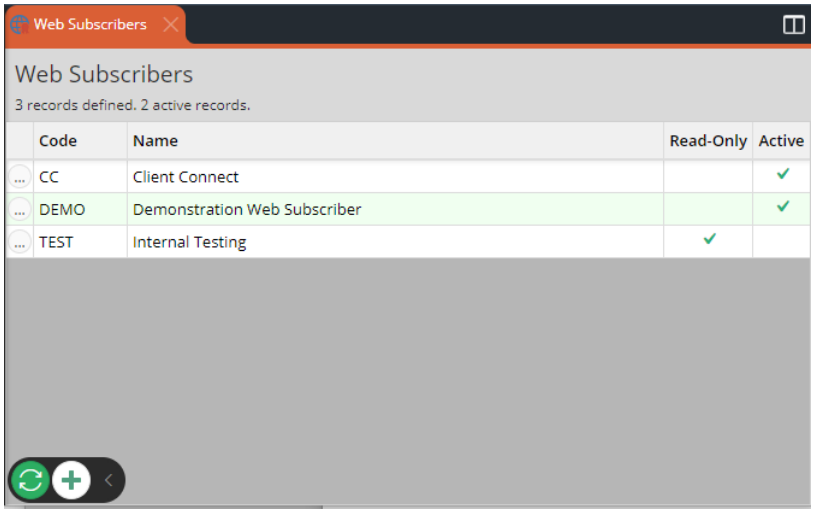
Accessing the administration facility from the Web server itself, i.e., via localhost, always allows unsecure access.

Web Subscribers

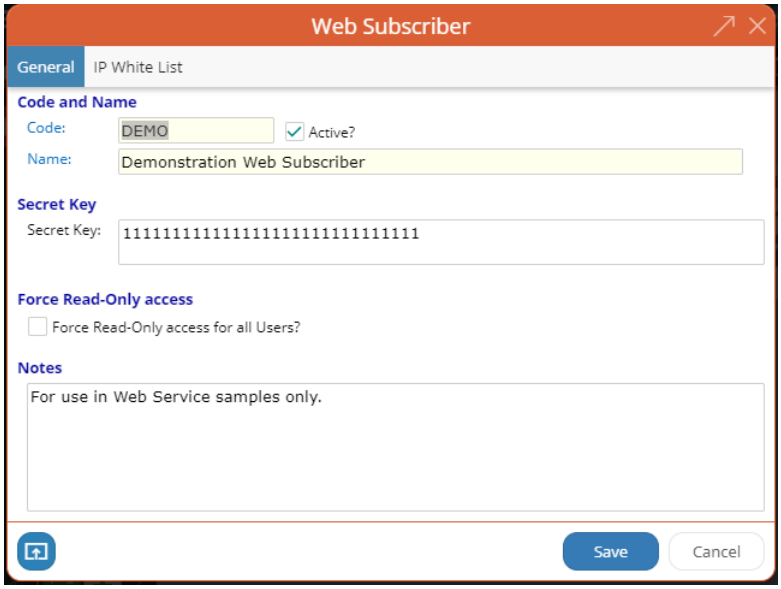
- Web Subscribers are external applications that require access to the Web Services. Each external application must have its own Web Subscriber record to enable it to access the Web Services.
- Select the **Web Subscribers** menu option.



- This displays a list of all available Web Subscribers records:

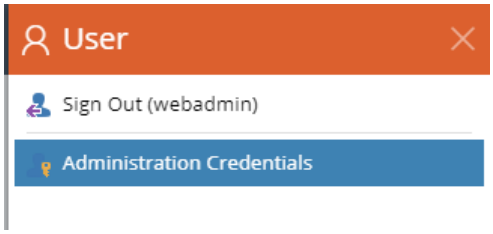


- From here you can add new Web Subscribers or edit existing ones without having to use the finPOWER Connect Windows interface.

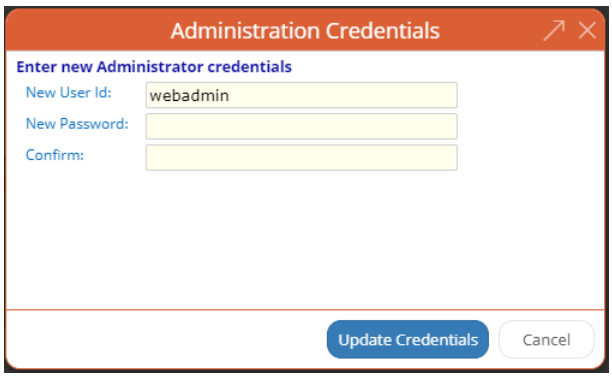


Changing Administration Credentials

- From the User menu, select **Administration Credentials**.



- You can change the Administration User Id from the default value of **webadmin** and also update the password from the default of **password**.



WARNING: The menu option will be disabled is the configuration file is read-only. This is usually due to the incorrect Windows permissions being applied to the App_Data folder.

NOTE: If you forget the administration credentials, you can reset them to the defaults (webadmin and password) by manually editing the App_Data/config.xml file and removing the following nodes:

WebAdminUserId
WebAdminPassword

finPOWER Connect Web Configurations

The Web Services Administration facility allows a Web Configuration to be specified via the "Other Settings" form.

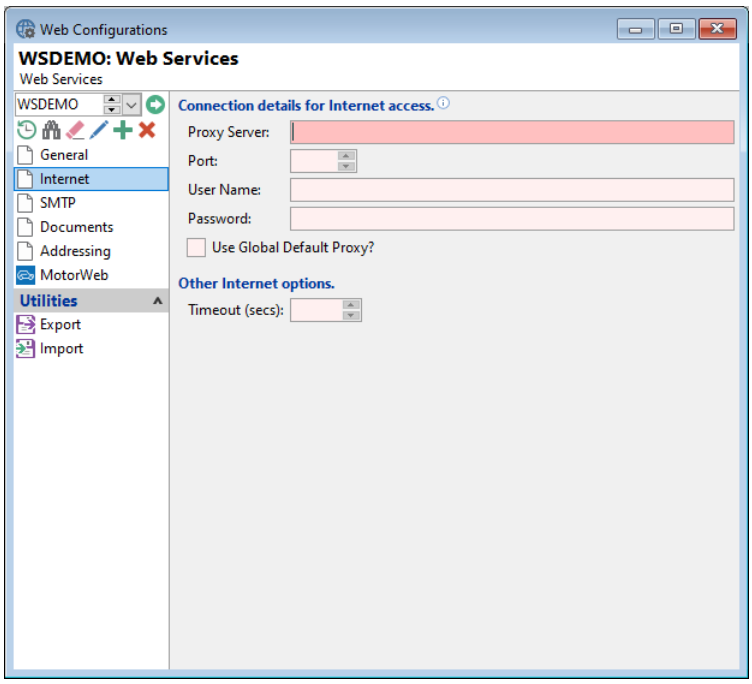
Web Configurations are defined within finPOWER Connect and contain settings to use that either replace or can be used to override any Global Settings defined within finPOWER Connect.

For example, you may wish to use a different SMTP Server to send Emails from Web Services (or, in turn, finPOWER Connect Cloud).

The Web Configurations form is available within finPOWER Connect via Tools, Web, Web Configurations. The following sections detail some of the more common Web Configuration settings.

Internet

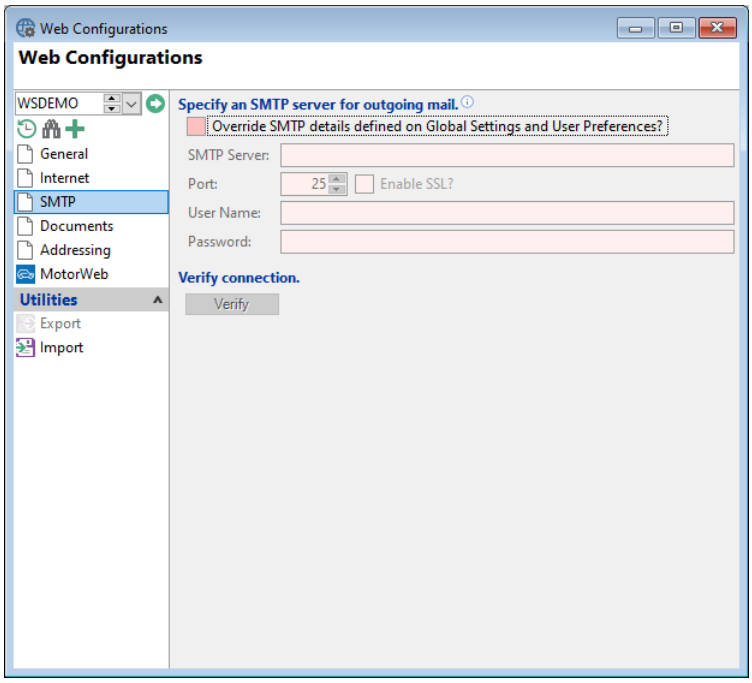
This page allows overriding proxy server details to be used by Web Services. These will override any Internet settings defined on either Global Settings or User Preferences:



NOTE: The "Use Global Default Proxy?" setting has nothing to do with Global Settings. It refers to the globally defined Windows Proxy Server settings.

SMTP

An SMTP server must be configured to enable Emails to be sent via Web Services.



By default, the currently signed in User's User Preferences will be used to determine the SMTP Server to use. If these are not defined, the SMTP settings defined under Global settings will be used.

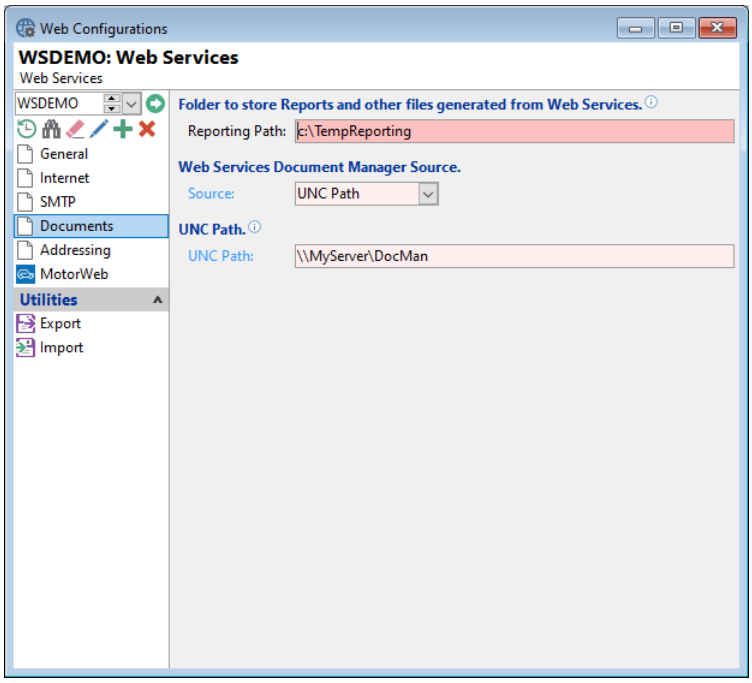
SMTP Server details can be overridden, e.g., the Web Server hosting the Web Services might also have its own SMTP Server installed which would be more efficient (and secure) to use than an externally hosted SMTP Server.

WARNING: Certain external SMTP Servers may be configured to only allow Emails to be sent from the currently signed in User which can make sending Emails from a standard business Email address problematic.

Microsoft Office 365 is one such example.

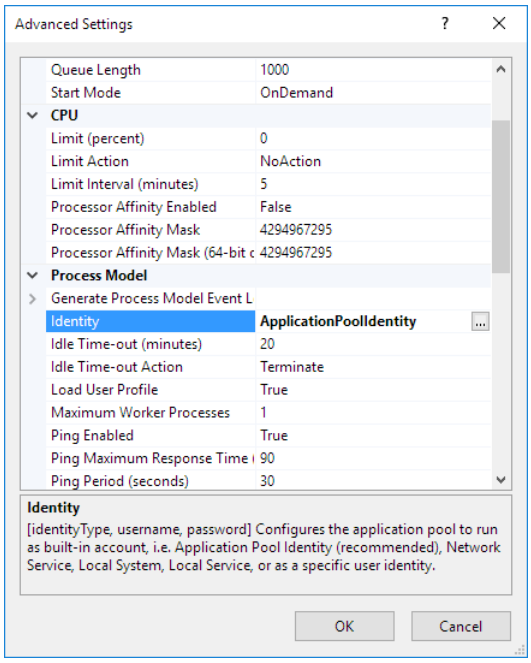
Document Manager

By default, no Document Manager functionality is available to Web Services. A Web Configuration MUST be used to enable Document Manager functionality such as accessing an Account's files.

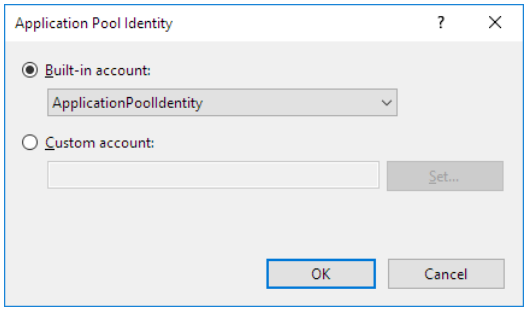


For Web Services to access the Document Manager, a UNC path must be specified.

This UNC path must be accessible by the IIS Application Pool. This may mean that IIS may need to be configured to run in the context of a Windows User. This is configured via the Application Pools, Advanced Settings form in IIS:



The Process Model, Identity field allows a Windows User to be defined:



NOTE: Configuration of IIS Application Pools and security is outside of the scope of this document; always use a qualified Network Engineer.

Production Setup and Configuration

When moving to a production environment, setup of the Windows Server hosting the Web Services must be performed by a qualified network administrator familiar with the installation and configuration of Windows Server, IIS and network security.

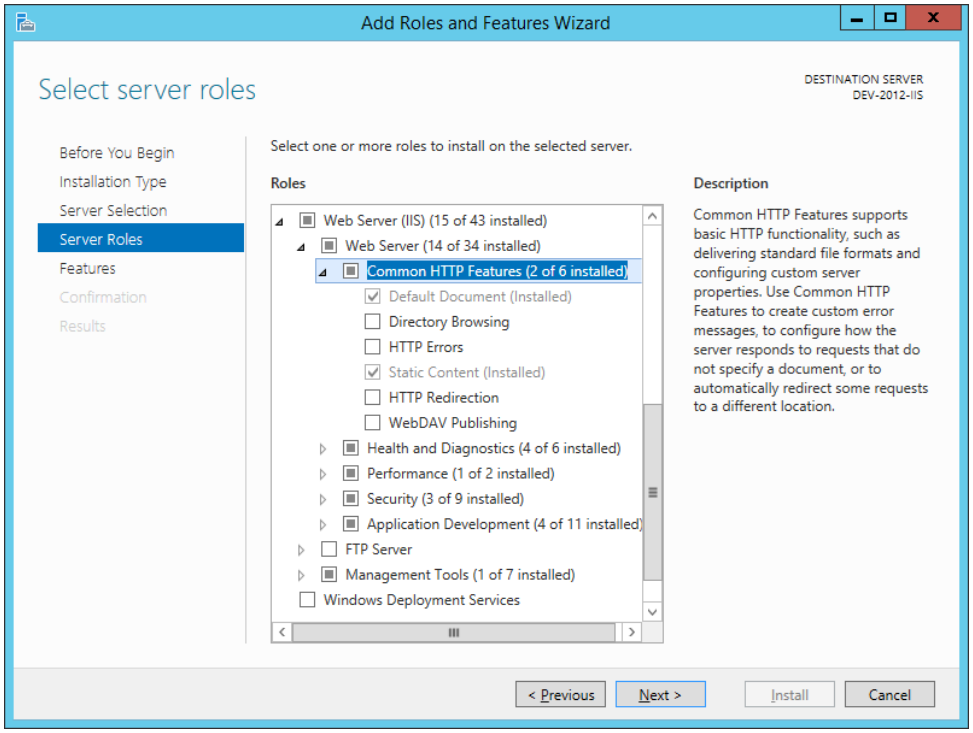
This section provides information that might prove useful when setting up and configuring the finPOWER Connect Web Services for production use.

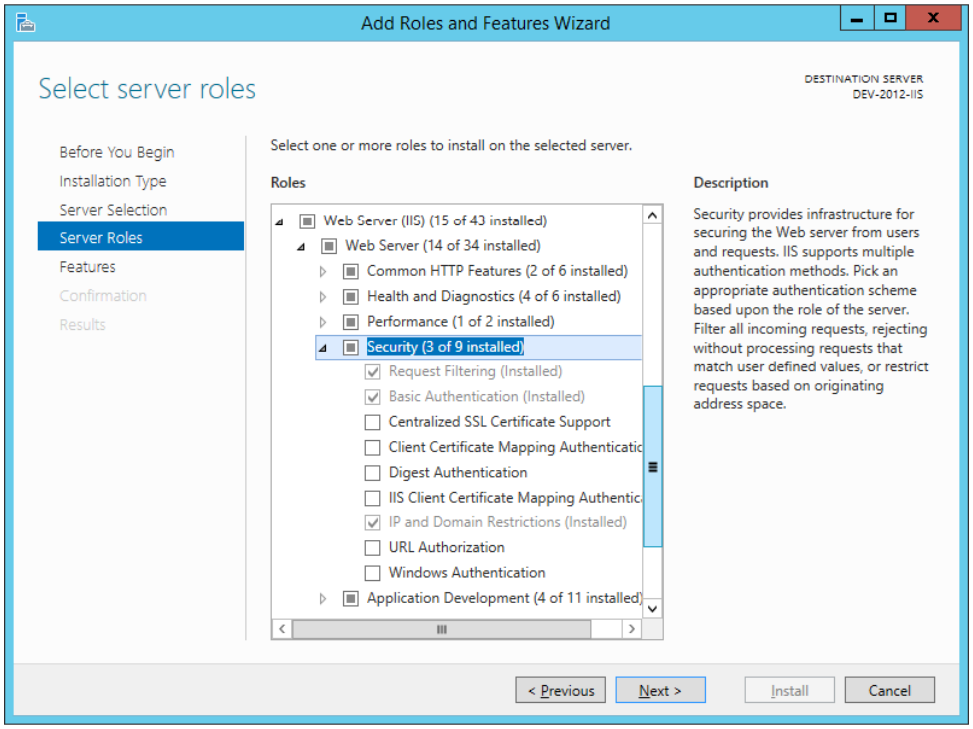
NOTE: This section is provided for informational purposes only and not as a guide for setting up a Web Server for use in a live, production environment.

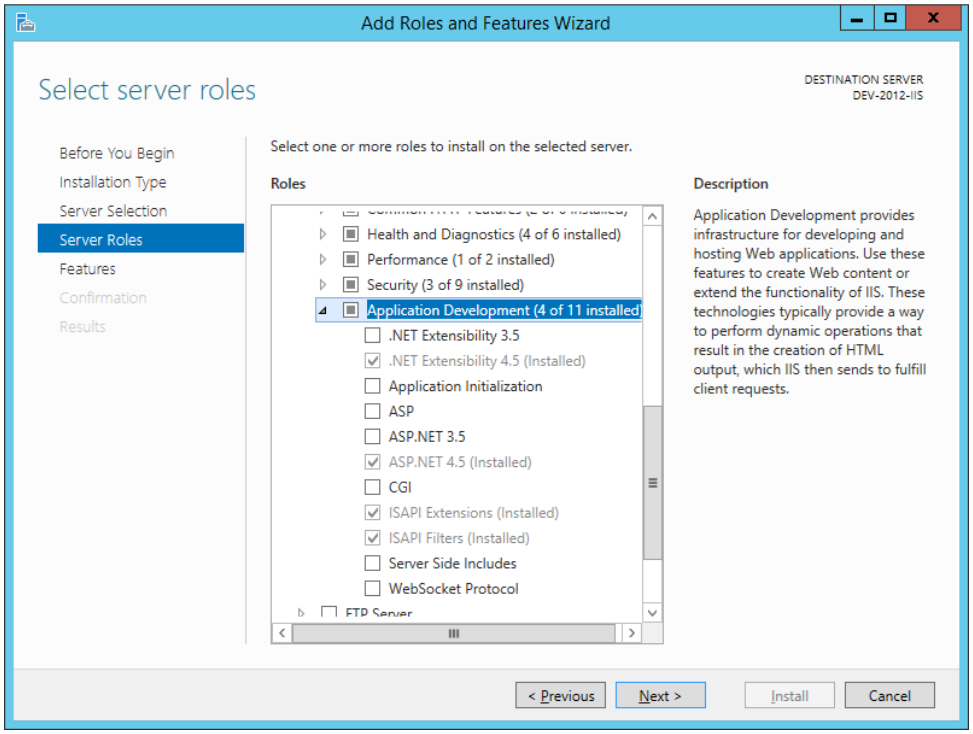
IIS Configuration

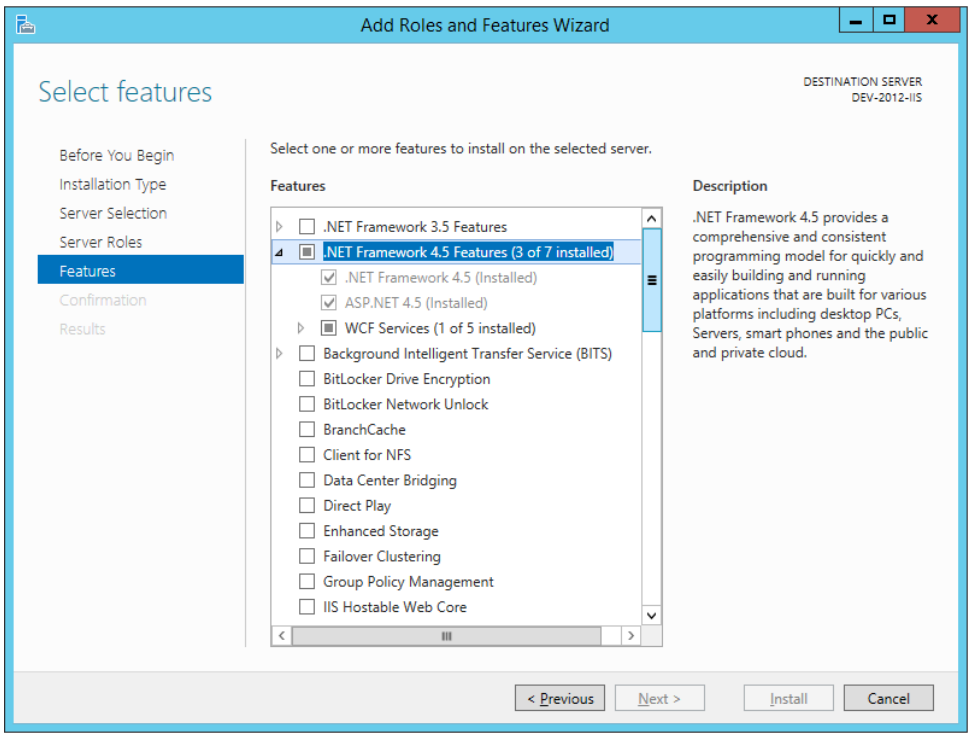
IIS Installation and configuration under Windows Server is quite different from desktop Windows and is outside of the scope of this document however, this section provides information on what the finPOWER Connect Web Services require from IIS; other applications running on the Web Server may require other options.

All screenshots are from the Windows Server 2012 **Add Roles and Features wizard** from the **Server Roles** and **Features** pages.






Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
DEV-2012-IIS
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Health and Diagnostics (4 of 6 installed)
Performance (1 of 2 installed)
Security (3 of 9 installed)
Application Development (4 of 11 installed)
.NET Extensibility 3.5
.NET Extensibility 4.5 (Installed)
Application Initialization
ASP
ASP.NET 3.5
ASP.NET 4.5 (Installed)
CGI
ISAPI Extensions (Installed)
ISAPI Filters (Installed)
Server Side Includes
WebSocket Protocol
FTP Server
Description
Application Development provides infrastructure for developing and hosting Web applications. Use these features to create Web content or extend the functionality of IIS. These technologies typically provide a way to perform dynamic operations that result in the creation of HTML output, which IIS then sends to fulfill client requests.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Select features
DESTINATION SERVER
DEV-2012-IIS
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.5 Features (3 of 7 installed)
.NET Framework 4.5 (Installed)
ASP.NET 4.5 (Installed)
WCF Services (1 of 5 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering
Group Policy Management
IIS Hostable Web Core
Description
.NET Framework 4.5 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.
< Previous
Next >
Install
Cancel

Security

In addition to ensuring that the Web Services are always called via a secure, HTTPS connection, the network administrator configuring the Web Server should also consider the following (configuration or which is outside of the scope of this document):

IP Address Restrictions

If the applications requiring access to the finPOWER Connect Web Services reside on servers with static IP addresses, IP Address Restrictions can be added in IIS to prevent servers other than these from accessing the Web Services.

This is performed via through **Internet Information Services (IIS) Manager** via, depending on the version of IIS, either:

- **IPv4 Address and Domain Restrictions**
- **IP Address and Domain Restrictions**

NOTE: If this tool is not available then it will need to be enabled from the Add Roles and Features wizard (or, in a non-Server version of Windows, the Windows Features tool described earlier in this document).

Firewall

Ensure the Web Server has a firewall installed and configured and that this firewall allows HTTPS (and, if necessary, HTTP) access to the Web Services.

Immediate Application Startup

By default, Web Services will only start upon the first request being received.

This can lead to a startup delay, particularly when the business layer pool is being populated with several entries.

IMPORTANT: If running Scheduled Processes, it is imperative that your Web Server is running for this processing to take place.

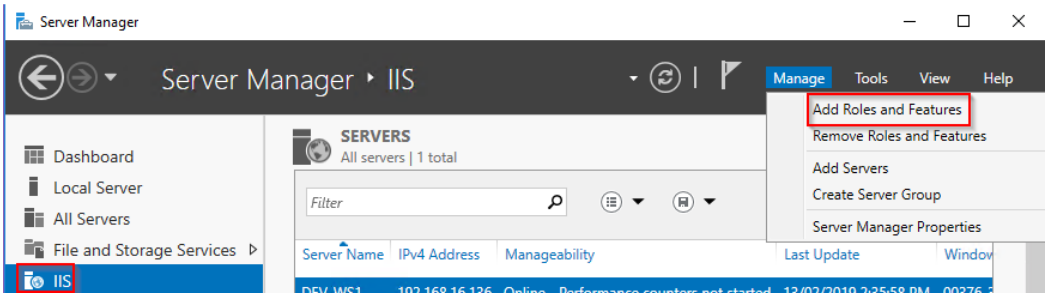
You can however enable IIS Application Initialization as detailed at:

https://docs.microsoft.com/en-us/iis/get-started/whats-new-in-iis-8/iis-80-application-initialization

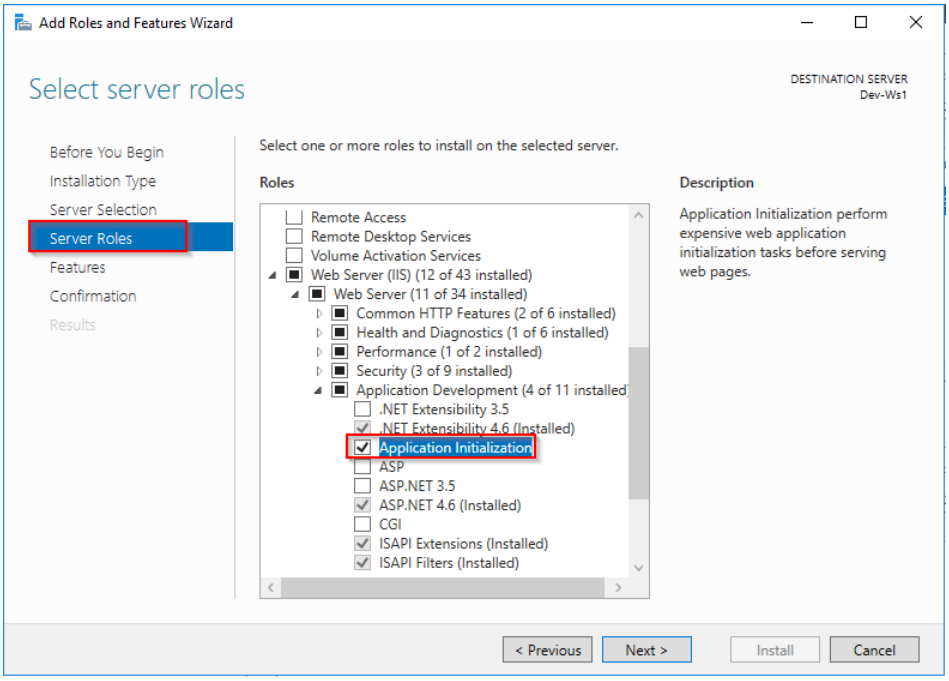
The following steps are required:

1. **Enable the IIS Application Initialization feature**

    a. From Server Manager, select IIS and then, from the Manage menu, select "Add Roles and Features":

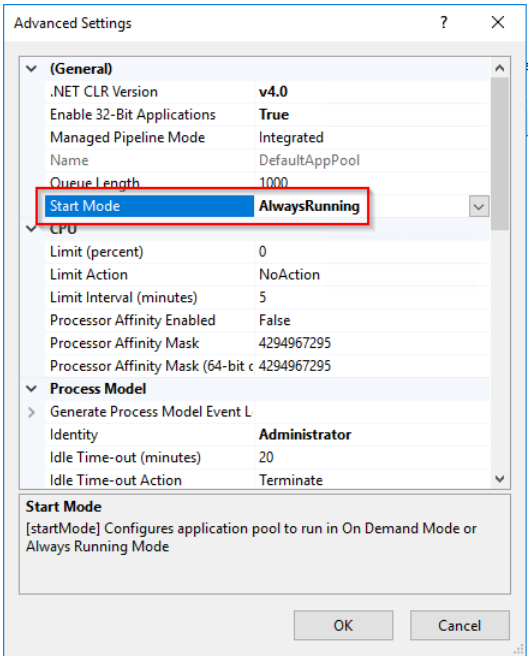


    b. Install the "Application Initialization" Server Role:



2. **Ensure the Application Pool is always running**

    a. The Application Pool that Web Services are using should have a "Start Mode" set to "AlwaysRunning". This is set under the Application Pool's Advanced Settings dialog:



3. Modify the applicationHost.config file

a. Run Notepad as an Administrator.
b. Load the applicationHost.config file from %WINDIR%\SYSTEM32\INETSRV\CONFIG
c. Locate the <sites>, <application> entry for Web Services and add a preloadEnabled="true" attribute:

4. Restart the Web Server

Multi-Server and Server Farms

The centralised configuration section details maintaining a LAN-based configuration file when using more than one web server.

This simply defines a **config.redirect** file to the **App_Data** folder which holds the UNC path of a centeralised configuration file, e.g.:

```
\\intersoft-nas1\data\webconfig\config.xml
```

When enabled, the default Web Services page shows a special icon and message:

To allow centralised configuration, the config.xml file must be updateable by all web servers. This might involve using a Windows User for the Web Services Application Pool to run under, something that will probably have been configured anyway if you want to use a LAN-based Document Manager folder.

NOTE: It is also recommended that the folder containing the config.xml file has permissions to allow each of the web servers to read, update and create files.

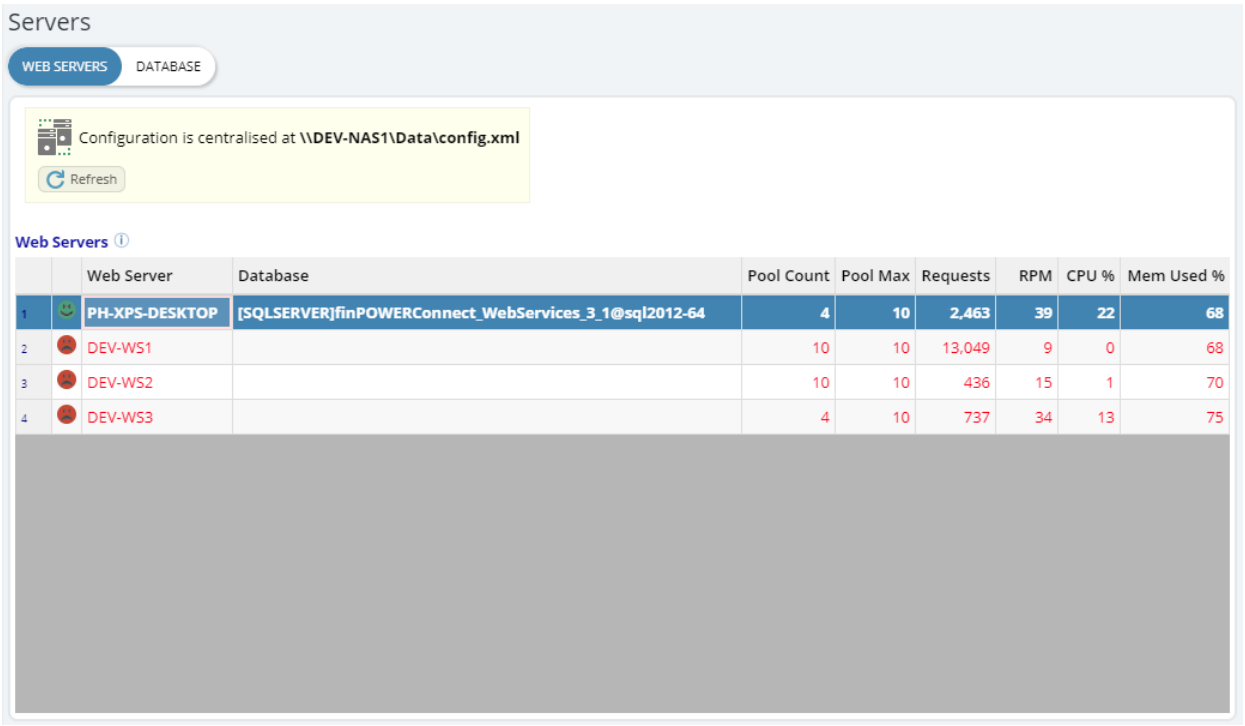
This allows a 'heart beat' file to be created and updated by each web server.

IMPORTANT: When running multiple Web Services, ensure each is set to immediately startup as details in the Immediate Application Startup section.

Monitoring Multiple Web Servers

When a centralised configuration file is being used, all Web Servers accessing this will write a "heartbeat" file to the folder containing the configuration file.

This allows the Servers view of the Web Services Administration facility to show details of all Web Servers, e.g.:



		Web Server	Database	Pool Count	Pool Max	Requests	RPM	CPU %	Mem Used %
1		PH-XPS-DESKTOP	[SQLSERVER]finPOWERConnect_WebServices_3_1@sql2012-64	4	10	2,463	39	22	68
2		DEV-WS1		10	10	13,049	9	0	68
3		DEV-WS2		10	10	436	15	1	70
4		DEV-WS3		4	10	737	34	13	75

Any Web Servers showing in red may mean there is an issue with this Web Server since its "heartbeat" file is out of date (more than 2 minutes old).

This may simply be because the Web Service has not received a request since starting (or restarting its Application Pool). This can be addressed by following the steps in the Immediate Application Startup section.

Troubleshooting

Cannot View IIS Application remotely

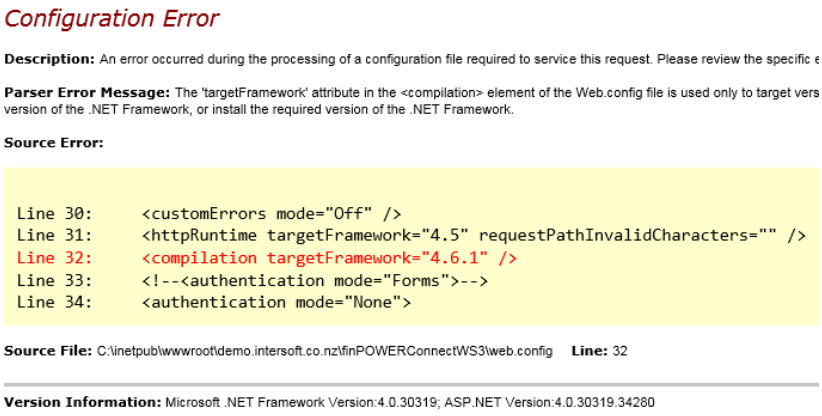
The following message may be displayed after first installing Web Services:

The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons)

This may indicate the Web Services causing an internal error that cannot be displayed on the remote browser.

To trouble-shoot this, navigate to the Web Services from a Web browser installed on the Web Server.

This allows the actual error to be displayed, e.g.:



This particular error is explained in the next section.

The 'targetFramework' attribute in the <compilation> element of the Web.config file is used only to target version 4.0

finPOWER Connect 3 targets the .NET framework 4.6.1.

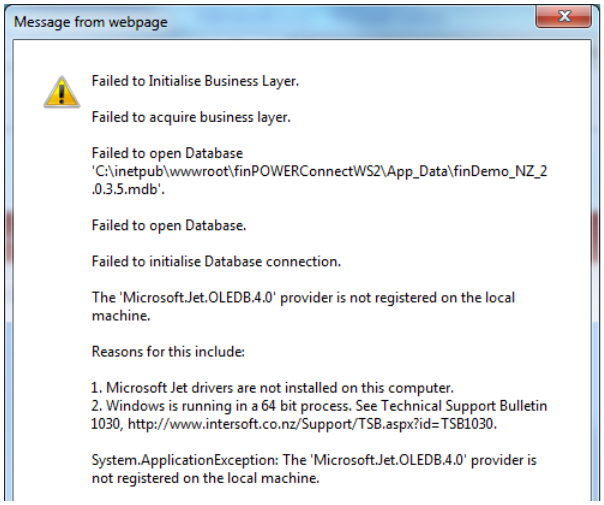
Therefore, the IIS Application Pool used by Web Services must also use this version.

This is covered in the Application Pool Configuration section.

Failed to acquire business layer using an MS Access database

A message similar to the following may be displayed when using an MS Access database.

This occurs when running on a 64-bit version of Windows when the Application Pool is not configured to Enable 32-bit Applications.


Message from webpage
Failed to Initialise Business Layer.
Failed to acquire business layer.
Failed to open Database 'C:\inetpub\wwwroot\finPOWERConnectWS2\App_Data\finDemo_NZ_2.0.3.5.mdb'.
Failed to open Database.
Failed to initialise Database connection.
The 'Microsoft.Jet.OLEDB.4.0' provider is not registered on the local machine.
Reasons for this include:
1. Microsoft Jet drivers are not installed on this computer.
2. Windows is running in a 64 bit process. See Technical Support Bulletin 1030, http://www.intersoft.co.nz/Support/TSB.aspx?id=TSB1030.
System.ApplicationException: The 'Microsoft.Jet.OLEDB.4.0' provider is not registered on the local machine.

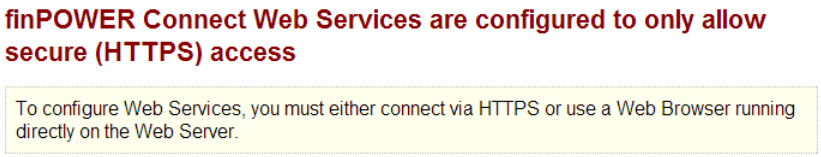
403 - Forbidden: Access is denied

This message might appear when viewing the Login page of the Web Administration facility. This might be due to the following:

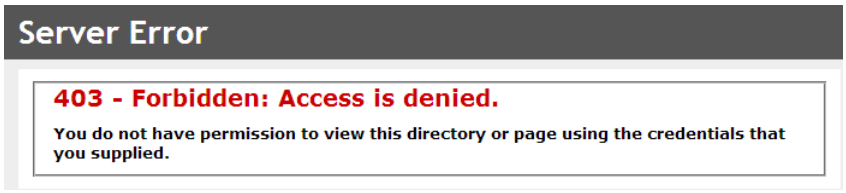
Page is being accessed by HTTP rather than HTTPS

In the Web Administration facility, **Settings**, **Other Settings**, **Security**, the option to **Allow unsecure (HTTP) access** might be unchecked. This means that attempting to sign in from anything but a Web browser running on the Web Server itself will be denied.

Usually, the page below will be displayed:



But, in certain configurations, IIS may deliver a generic error page such as this:



Timeout when Authenticating Client

A timeout error when attempting to authenticate a Client via the Authentication/AuthenticateClient service may be due to the following:

Misconfigured Address Database

If the Address database being used by the finPOWER Connect business layer is not available, attempting to connect to it may cause a time out.

This may be an issue when attempting to authenticate as a Client since the response from this service includes formatted Branch address details which involves accessing the Addressing interface which will always attempt to initialise a connection to the Address database when first accessed.

Server Error: <compilation targetFramework="4.5" />

If the .NET framework version 4.5 is not installed on the Web Server, an error similar to the following will be shown:

Configuration Error

Description: An error occurred during the processing of a configuration file required to service this request. Please review the specific error details below and modify your configuration file appropriately.

Parser Error Message: The 'targetFramework' attribute in the <compilation> element of the Web.config file is used only to target version 4.0 and later of the .NET Framework (for example, "<compilation targetFramework="4.0">"). The 'targetFramework' attribute currently references a version that is later than the installed version of the .NET Framework. Specify a valid target version of the .NET Framework, or install the required version of the .NET Framework.

Source Error:

```
Line 16:   <system.web>
Line 17:     <httpRuntime targetFramework="4.5" requestPathInvalidCharacters="" />
Line 18:     <compilation targetFramework="4.5" />
Line 19:     <!--<authentication mode="Forms">-->
Line 20:     <authentication mode="None">
```

To resolve this:

- Download the .NET Framework 4.5 from Microsoft and install it:
  - https://www.microsoft.com/en-nz/download/details.aspx?id=42643
- Ensure ASP.NET is installed correctly as detailed in the Installing ASP.NET 4 section.
- Check the Application Pool used for the Web Services is configured correctly as detailed in the Application Pool Configuration section.

Slow Requests/ Slow Initial Request

Web Services use the finPOWER Connect business layer which is a "stateful" object, i.e., it maintains information such as global collections between requests.

Therefore, initialising the business layer can be an expensive (i.e., slow) process, particularly for databases with large global collections such as External Parties.

This is why the Web Services use a Business Layer Pooling mechanism.

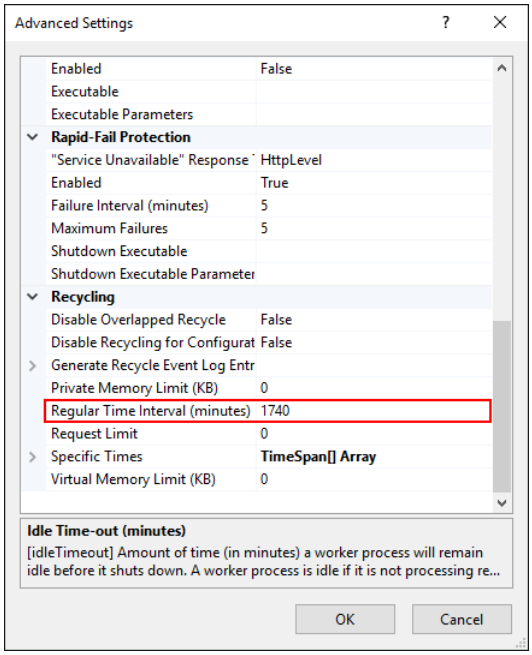
Certain actions can cause the finPOWER Connect business layer to be dropped from the Business Layer Pool, e.g.:

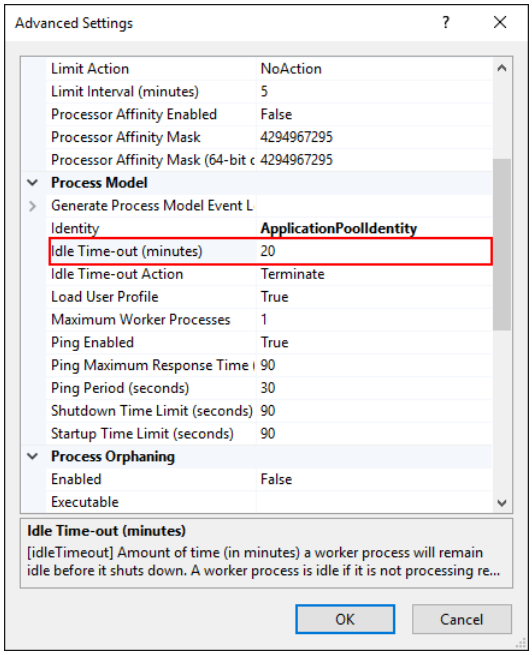
- A fatal error occurs on the business layer, e.g., a connection with the database was lost.
- As of version 3.00.00, any changes to global collections, global settings or permissions will cause the business layer to be dropped from the pool.
    - This ensures that Web Services always have the most up-to-date information in memory and that any security changes are enforced immediately.

Certain actions can cause the entire Business Layer Pool to be restarted, e.g.:

- IIS may recycle the Application Pool under which the Web Services are running.
    - By default, this will occur every 1740 minutes (29 hours) and helps with any memory leakages that may occur in Web applications.
    - However, if the Application Pool is set to recycle regularly, e.g., every 20 minutes (or after 20 minutes of inactivity), this could have performance implications.

Application Pool recycling and idle timeout is administered via the "Internet Information Services (IIS) Manager", Advanced Settings dialog for the Application Pool under which Web Services is running, e.g.:





X509Certificate Error using MotorWeb or PPSR G2B

Custom Web Services attempting to access MotorWeb or the PPSR G2B services may fail with an error relating to an 'X509Certificate', e.g.:

```
at
System.Security.Cryptography.CryptographicException.ThrowCryptographicException(
Int32 hr)

   at
System.Security.Cryptography.X509Certificates.X509Utils._LoadCertFromBlob(Byte[]
rawData, IntPtr password, UInt32 dwFlags, Boolean persistKeySet,
SafeCertContextHandle&amp;amp; pCertCtx)

   at
System.Security.Cryptography.X509Certificates.X509Certificate.LoadCertificateFro
mBlob(Byte[] rawData, Object password, X509KeyStorageFlags keyStorageFlags)

   at
System.Security.Cryptography.X509Certificates.X509Certificate2..ctor(Byte[]
rawData, String password)

   at Intersoft.ISRuntime3.ISWebUtilities.GetCertificateFromBase64String(String
certificateText, String certificatePassword, X509Certificate2&amp;amp; certificate)
```

To resolve this, update the 'Load User Profile' setting on the Application Pool to True: