

# SQL Server version 2016

CONFIGURATION, INSTALLATION AND SETUP GUIDE

## Contents

|   |    |
|---|----|
| Enterprise Edition (including SQL Server) .....                 | 3  |
| SQL Server Database Modifications.....                          | 3  |
| Backwards Compatibility .....                                   | 3  |
| Windows Server Configuration .....                              | 4  |
| Add the POWER series Group .....                                | 4  |
| To add the POWER Security Group.....                            | 4  |
| Assign users to the Group .....                                 | 5  |
| To assign Users to the security Group .....                     | 5  |
| Installation .....  | 6  |
| SQL Server 2016 Configuration .....                             | 6  |
| To configure SQL Server.....                                    | 6  |
| Authentication Mode .....                                       | 6  |
| Model database .....  | 7  |
| Intersoft Login .....   | 10 |
| To add the Intersoft Login .....                                | 10 |
| Security Group Login .....                                      | 12 |
| To add the Login .....  | 12 |
| SQL Data .....  | 13 |
| Configure the Windows Firewall to Allow SQL Server Access ..... | 13 |
| To open a port in Windows Firewall for TCP/IP access .....      | 13 |
| To open access to SQL Server when using dynamic ports .....     | 14 |
| To change sharing options for different network profiles.....   | 14 |
| Network mapping to the new server .....                         | 15 |

## **Enterprise Edition (including SQL Server)**

The Enterprise Edition Add-On adds support for Microsoft SQL Server

In emPOWER, fdPOWER and finPOWER there is a "SQL Server Upsize" utility to upgrade Access databases to SQL Server.

In finPOWER Connect there is a "Copy Database" utility to upgrade Access databases to SQL Server.

**Please be warned this is a significant change and should be carefully implemented, especially when making sure your backups are working correctly.**

Please carefully read and follow all of the instructions contained within this document.

## **SQL Server Database Modifications**

Unlike Access databases, where database access is tightly controlled by Intersoft, SQL Server **System Administrators** have full control over all aspects of SQL Server and everything within it, including database structure and the data contained in each table.

In other words there is nothing specifically stopping the System Administrator from altering the database structure or the information contained in the database. However, altering the database structure or information stored in the database may stop emPOWER, fdPOWER, finPOWER or finPOWER Connect from working correctly, and even corrupt information!

It may be tempting to log in as the System Administrator to change information or add an extra column to a table etc – BUT this will invalidate your software licence:

The Licensor may immediately terminate this Agreement if any attempt is made by the Licensee to decompile, disassemble, reverse engineer or in any way modify the System, including database structure or data, without the written consent of the Licensor, except as required by law.

## **Backwards Compatibility**

Once a SQL Server database has been upgraded to SQL Server 2016 there is no way to run it on the old SQL Server platform.

This means you should carefully test your systems in a SQL Server test environment before moving them to production. It also means you should ensure you have suitable backups before transferring to SQL Server 2016.

**ONCE A DATABASE HAS BEEN LOADED AND USED ON SQL SERVER 2016 IT CANNOT BE RESTORED BACK TO A PREVIOUS SQL SERVER VERSION.**

## Windows Server Configuration

For security purposes you need to create a Security Group and assign to it those users that will require access to POWER series Database respectively. This is the "top most" level of security and uses inbuilt Operating System security.

If running finPOWER and emPOWER etc. you can optionally create a Security Group for each application, or one to cover both applications.

### Add the POWER series Group

The Security Group allows you to quickly assign new Users to this group, giving them access to all POWER series databases respectively – rather than assigning individual Users to the database.

Note: If using separate Security Groups we suggest you use "finPOWER" for finPOWER and finPOWER Connect.

### To add the POWER Security Group

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, double-click the domain node, ie double-click the Server to expand it.
3. Open, ie click, the **Users** folder.
4. From the **Action** menu, point to **New** and click **Group**.
5. In the New Object wizard enter the **Group Name** as required, set **Group scope** as **Global** and **Group type** as **Security**.

The screenshot shows the 'New Object - Group' wizard. The 'Create in' field is 'INTERSOFT.CO.NZ/Users'. The 'Group name' and 'Group name (pre-Windows 2000)' fields are both 'finPOWER'. The 'Group scope' section has 'Global' selected. The 'Group type' section has 'Security' selected. The 'Next >' button is highlighted.

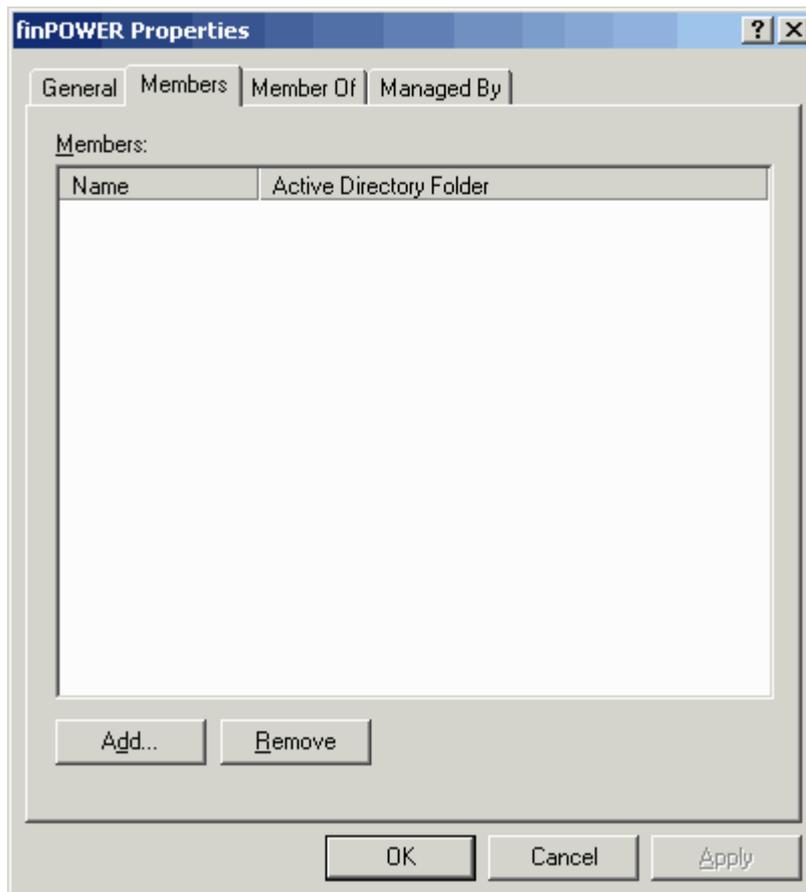
6. Click **Next**.
7. Do not create an Exchange email address, ie uncheck the **Create an Exchange e-mail address** if checked.
8. Click **Next**.
9. Click **Finish** to create the new Group.

## Assign users to the Group

Next you will need to add the users that have permission to open databases.

### To assign Users to the security Group

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, double-click the domain node, ie double-click the Server to expand it.
3. Open, ie click, the **Users** folder.
4. Right click the Security Group and click **Properties**.



5. Click on the **Members** tab.
6. Click **Add** and add the Users required.
7. Click **OK**.

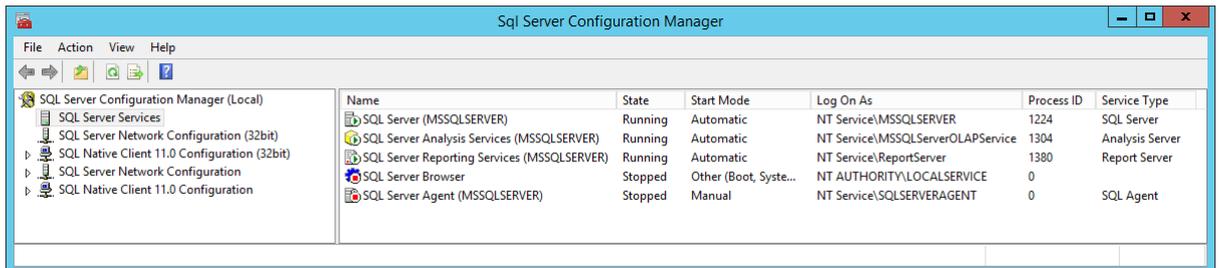
## Installation

Install SQL Server 2016 and then configure it as per below. Some steps like the SQL Server Properties can be completed as part of the install and if that is the case don't need to be changed again later.

## SQL Server 2016 Configuration

### To configure SQL Server

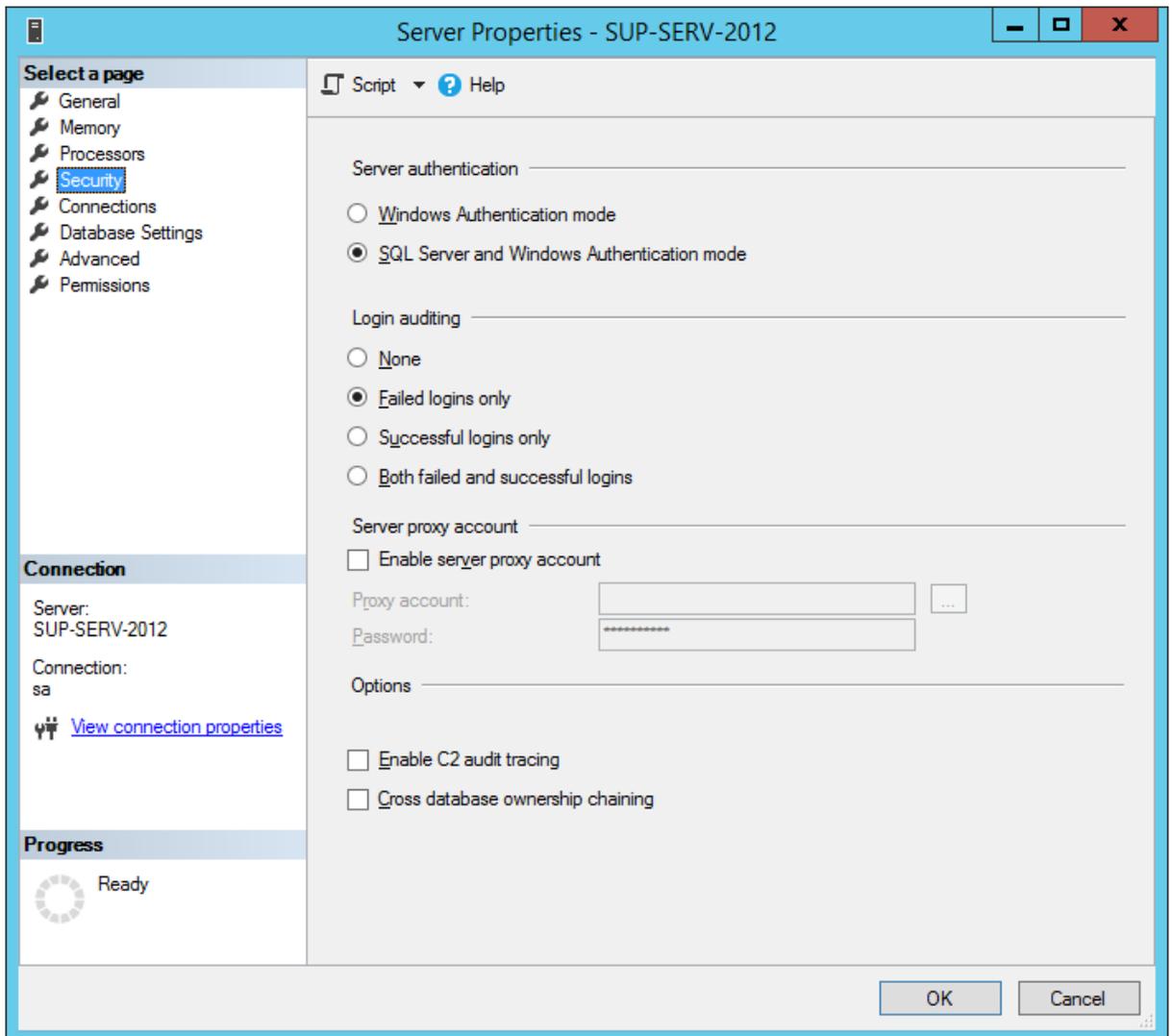
- Open **SQL Server 2016 Configuration Manager**. This can be found from the **Start** menu under **All Programs, Microsoft SQL Server 2016, Configuration Tools**.
- Click on the SQL Server Services node.



- Make certain both **SQL Server** and **SQL Server Agent** are both running and have a Start Mode of **Automatic**.
- The SQL Server Agent is required to automate backups.

### Authentication Mode

- Open **SQL Server Management Studio**. This can be found from the **Start** menu under **All Programs, Microsoft SQL Server [version]**.  
*\* Note: The screenshots below use v17.2 and your version might be different (from 2015 MS has released versions of Management Studio independently to the database components like Configuration Manager).*
- Logon using **Server Type** 'Database Engine', **Server Name** '[server network logon name]', **Logon, Password**, settings.
- Right click on the server and select **Properties**.



- Under **Server Authentication**, make sure that **SQL Server and Windows Authentication mode** is checked.
- Click **OK**.
- At this point you may be asked to Restart SQL Server – do so now.

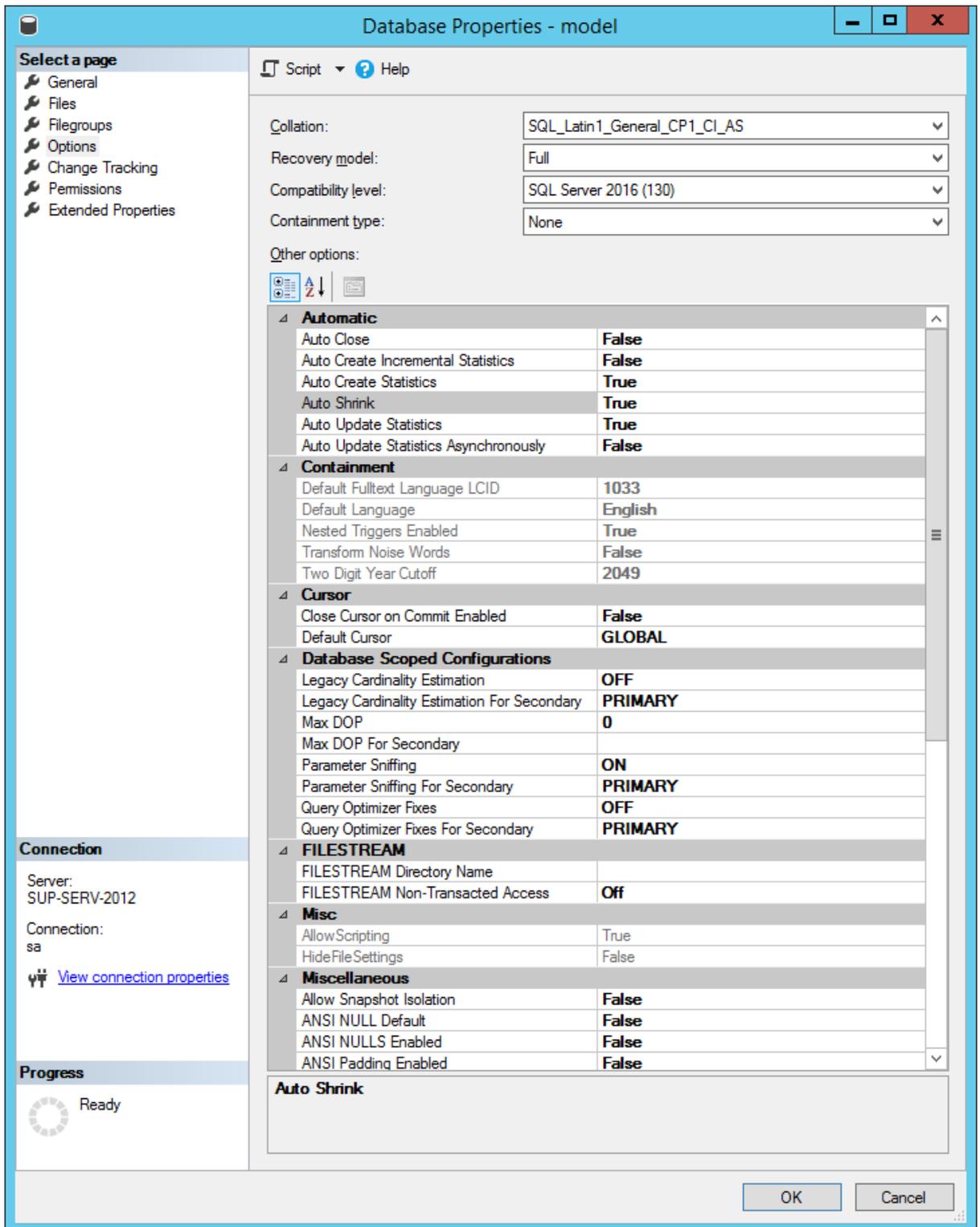
## Model database

Within SQL Server there are several "system" databases, including the **master**, **tempdb**, **model** and **msdb** databases.

The **model** database is used as the template for all databases created, and it is strongly recommended that this is correctly setup prior to doing anything else.

### To check Model database options

- Open Microsoft SQL Server Management Studio.
- Expand your server.
- Expand **Databases**.
- Expand **System Databases**.
- Right click the **model** database, then click **Properties**.
- Select the **Options** page.



- Ensure the following options are set:

|                        |      |
|------------------------|------|
| Auto Create Statistics | True |
| Auto Shrink            | True |
| Auto Update Statistics | True |

|                   |       |
|-------------------|-------|
| ANSI NULL Default | False |
|-------------------|-------|

- Click **OK**.

Although the above is what we suggest, it may be that you wish to set the default **Recovery** model to another option.

## Intersoft Login

**Note:** This is not required for finPOWER Connect.

The Intersoft Login is required so that the POWER Series can have System Administrator rights to the SQL Server, for example to create a new database.

### To add the Intersoft Login

- Open Microsoft SQL Server Management Studio.
- Expand your server.
- Expand **Security**.
- Right-click on **Logins** and click **New Login...**
- On the General page set Login Name as **intersoft**, change Authentication to **SQL Server Authentication** and set the password.

**Get the password for your client id from your Intersoft Dealer. Enter without spaces.**

- Uncheck **Enforce password policy**.

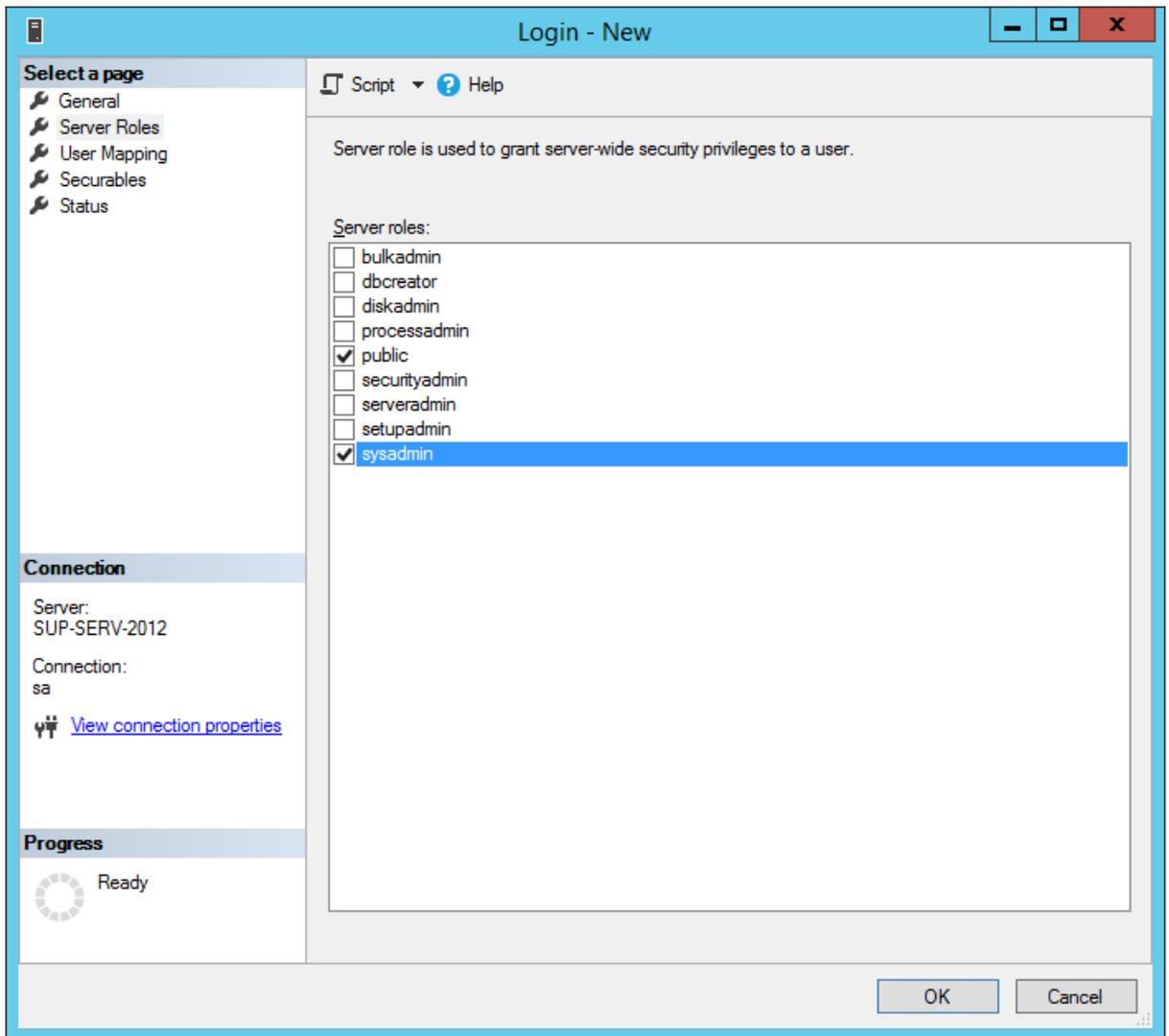
The screenshot shows the 'Login - New' dialog box with the following configuration:

- General** page selected.
- Login name: intersoft
- Authentication:  SQL Server authentication
- Password: [masked]
- Confirm password: [masked]
- Specify old password
- Old password: [empty]
- Enforce password policy
- Enforce password expiration
- User must change password at next login
- Mapped to certificate
- Mapped to asymmetric key
- Map to Credential
- Mapped Credentials table is empty.
- Default database: master
- Default language: <default>
- Buttons: OK, Cancel

On the left sidebar:

- Select a page:** General, Server Roles, User Mapping, Securables, Status
- Connection:** Server: SUP-SERV-2012, Connection: sa, View connection properties
- Progress:** Ready

- Click on the **Server Roles** page. Check the **sysadmin** Server Role. Note the 'public' role will already be selected automatically and this cannot be unselected.



- Click **OK**.
- If asked, confirm the Login password.

## Security Group Login

The login is required for general day to day use of the POWER series databases, rather than using the **Intersoft** login which has full System Administrator rights. This maps directly to the Windows Security Group defined on the Windows Server. Details of group creation can be found above.

### To add the Login

- Open Microsoft SQL Server Management Studio.
- Expand your server.
- Expand **Security**.
- Right-click on **Logins** and click New **Login....**
- On the General page set **Login name** as required ensuring that the name is prefixed with your domain name and make sure that **Windows Authentication** is checked.

Alternatively you can use the "**Search...**" button next to the **Login Name** field to lookup the Windows Security Group.

The screenshot shows the 'Login Properties' dialog box for the login 'INTERSOFTNZ\finPOWER'. The 'General' tab is active. The 'Login name' is 'INTERSOFTNZ\finPOWER'. The 'Windows authentication' radio button is selected. The 'Password' and 'Confirm password' fields are empty. The 'Specify old password' checkbox is unchecked. The 'Enforce password policy', 'Enforce password expiration', and 'User must change password at next login' checkboxes are also unchecked. The 'Mapped to certificate', 'Mapped to asymmetric key', and 'Map to Credential' options are all unchecked. The 'Mapped Credentials' table is empty. The 'Default database' is set to 'master' and the 'Default language' is set to 'English'. The 'OK' and 'Cancel' buttons are at the bottom right.

- On Server Roles page check "Public".
- Click **OK**.

## SQL Data

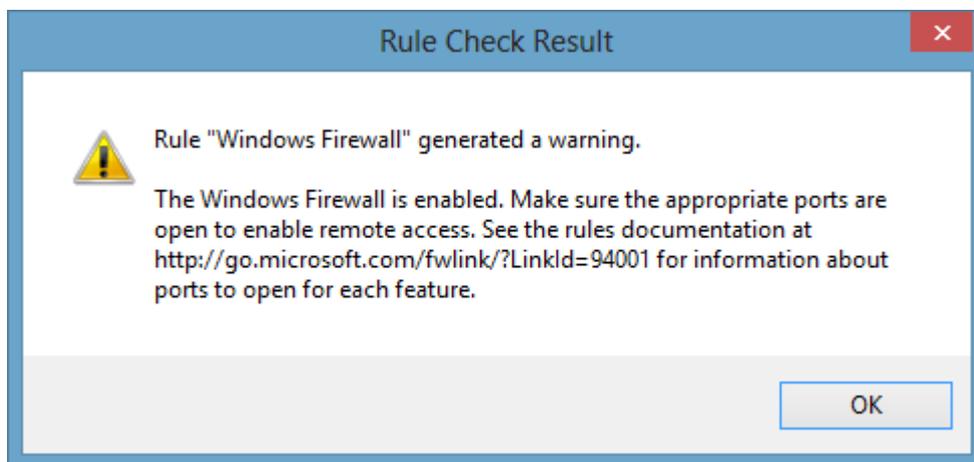
There needs to be a network available folder created to store the SQL Data for Clients and test databases.

1. If no other specific drive is being used then create a folder 'C:\SQLData' and share this folder on the network to everyone.
2. Everyone will then need to map this network location on their own computers.

## Configure the Windows Firewall to Allow SQL Server Access

Firewall systems help prevent unauthorized access to computer resources. If a firewall is turned on but not correctly configured, attempts to connect to SQL Server might be blocked.

To access an instance of the SQL Server through a firewall, you must configure the firewall on the computer that is running SQL Server to allow access. Windows Firewall is a component of Microsoft Windows. You can also install a firewall from another company. This topic discusses how to configure Windows Firewall, but the basic principles apply to other firewall programs.



<https://msdn.microsoft.com/en-us/library/cc646023.aspx>

Applies to Windows Vista, 7, 8 or 10, and Windows Server 2008, 2008 R2, 2012, 2012 R2 and 2016.

The following procedures configure Windows Firewall by using Windows Firewall with Advanced Security Microsoft Management Console (MMC) snap-in. Windows Firewall with Advanced Security only configures the current profile.

### To open a port in Windows Firewall for TCP/IP access

- On the **Start** menu, click Run, type WF.msc, and then click OK.
- In the Windows Firewall with Advanced Security, in the left pane, right-click Inbound Rules, and then click New Rule in the action pane.
- In the Rule Type dialog box, select Port, and then click Next.
- In the Protocol and Ports dialog box, select TCP. Select Specific local ports, and then type the port number of the instance of the Database Engine, such as 1433 for the default instance. Click Next.
- In the Action dialog box, select Allow the connection, and then click Next.

- In the Profile dialog box, select any profiles that describe the computer connection environment when you want to connect to the Database Engine, and then click Next.
- In the Name dialog box, type a name and description for this rule, and then click Finish.
- 

### To open access to SQL Server when using dynamic ports

- On the **Start** menu, click Run, type WF.msc, and then click OK.
- In the Windows Firewall with Advanced Security, in the left pane, right-click Inbound Rules, and then click New Rule in the action pane.
- In the Rule Type dialog box, select Program, and then click Next.
- In the Program dialog box, select This program path. Click Browse, and navigate to the instance of SQL Server that you want to access through the firewall, and then click Open. By default, SQL Server is at (32 bit) C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Binn\Sqlservr.exe. Click Next.
- In the Action dialog box, select Allow the connection, and then click Next.
- In the Profile dialog box, select any profiles that describe the computer connection environment when you want to connect to the Database Engine, and then click Next.
- In the Name dialog box, type a name and description for this rule, and then click Finish.

### To change sharing options for different network profiles

- On the **Start** menu, click Control Panel, select Network and Sharing Center.
- In the left pane, click on Change advanced sharing settings.
- Under Network discovery. Tick 'Turn on network discovery' button.

#### Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Private  

Guest or Public  

Domain (current profile)  

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.

Turn on network discovery

Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

Turn on file and printer sharing

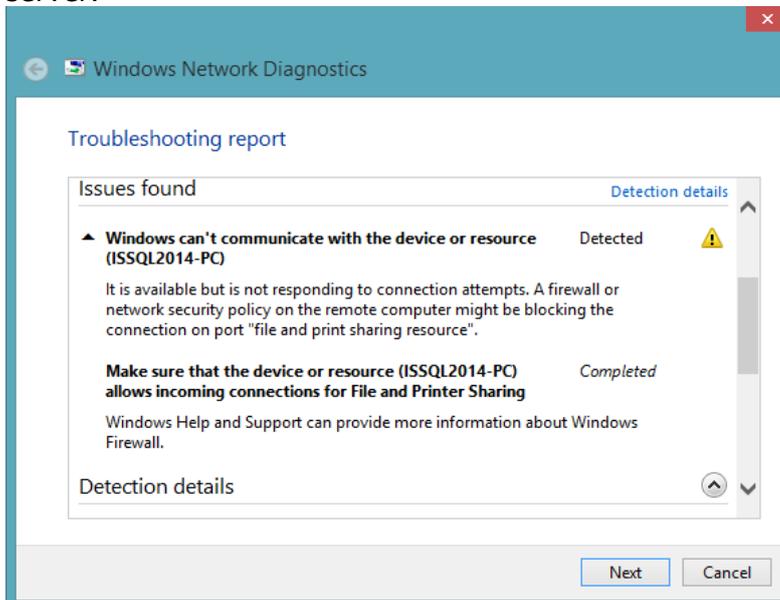
Turn off file and printer sharing

All Networks  

- Click Save changes.

## Network mapping to the new server

- You may experience the following error message when trying to map to the new server.



- You may have to enable rules under Windows Firewall, Advanced Settings, Inbound/Outbound Rules. Enable File and Printer Sharing.

| Windows Firewall with Advanced Settings |   | Inbound Rules             |            |         |         |
|---|---|---------------------------|------------|---------|---------|
|   |   | Name                      | Group      | Profile | Enabled |
| <input checked="" type="checkbox"/>     | Core Networking - Router Advertisement (ICMPv6-I...   | Core Networking           | All        | Yes     |         |
| <input checked="" type="checkbox"/>     | Core Networking - Router Solicitation (ICMPv6-In)     | Core Networking           | All        | Yes     |         |
| <input checked="" type="checkbox"/>     | Core Networking - Teredo (UDP-In)                     | Core Networking           | All        | Yes     |         |
| <input checked="" type="checkbox"/>     | Core Networking - Time Exceeded (ICMPv6-In)           | Core Networking           | All        | Yes     |         |
| <input type="checkbox"/>                | Distributed Transaction Coordinator (RPC)             | Distributed Transactio... | Private... | No      |         |
| <input type="checkbox"/>                | Distributed Transaction Coordinator (RPC)             | Distributed Transactio... | Domain     | No      |         |
| <input type="checkbox"/>                | Distributed Transaction Coordinator (RPC-EPMAP)       | Distributed Transactio... | Private... | No      |         |
| <input type="checkbox"/>                | Distributed Transaction Coordinator (RPC-EPMAP)       | Distributed Transactio... | Domain     | No      |         |
| <input type="checkbox"/>                | Distributed Transaction Coordinator (TCP-In)          | Distributed Transactio... | Domain     | No      |         |
| <input type="checkbox"/>                | Distributed Transaction Coordinator (TCP-In)          | Distributed Transactio... | Private... | No      |         |
| <input type="checkbox"/>                | File and Printer Sharing (Echo Request - ICMPv4-In)   | File and Printer Sharing  | Private... | No      |         |
| <input checked="" type="checkbox"/>     | File and Printer Sharing (Echo Request - ICMPv4-In)   | File and Printer Sharing  | Domain     | Yes     |         |
| <input checked="" type="checkbox"/>     | File and Printer Sharing (Echo Request - ICMPv6-In)   | File and Printer Sharing  | Domain     | Yes     |         |
| <input type="checkbox"/>                | File and Printer Sharing (Echo Request - ICMPv6-In)   | File and Printer Sharing  | Private... | No      |         |
| <input checked="" type="checkbox"/>     | File and Printer Sharing (LLMNR-UDP-In)               | File and Printer Sharing  | Domain     | Yes     |         |
| <input type="checkbox"/>                | File and Printer Sharing (LLMNR-UDP-In)               | File and Printer Sharing  | Private... | No      |         |
| <input type="checkbox"/>                | File and Printer Sharing (NB-Datagram-In)             | File and Printer Sharing  | Private... | No      |         |
| <input checked="" type="checkbox"/>     | File and Printer Sharing (NB-Datagram-In)             | File and Printer Sharing  | Domain     | Yes     |         |
| <input checked="" type="checkbox"/>     | File and Printer Sharing (NB-Name-In)                 | File and Printer Sharing  | Domain     | Yes     |         |
| <input type="checkbox"/>                | File and Printer Sharing (NB-Name-In)                 | File and Printer Sharing  | Private... | No      |         |
| <input checked="" type="checkbox"/>     | File and Printer Sharing (NB-Session-In)              | File and Printer Sharing  | Domain     | Yes     |         |
| <input type="checkbox"/>                | File and Printer Sharing (NB-Session-In)              | File and Printer Sharing  | Private... | No      |         |
| <input type="checkbox"/>                | File and Printer Sharing (SMB-In)                     | File and Printer Sharing  | Private... | No      |         |
| <input checked="" type="checkbox"/>     | File and Printer Sharing (SMB-In)                     | File and Printer Sharing  | Domain     | Yes     |         |
| <input type="checkbox"/>                | File and Printer Sharing (Spooler Service - RPC)      | File and Printer Sharing  | Private... | No      |         |
| <input checked="" type="checkbox"/>     | File and Printer Sharing (Spooler Service - RPC)      | File and Printer Sharing  | Domain     | Yes     |         |
| <input checked="" type="checkbox"/>     | File and Printer Sharing (Spooler Service - RPC-EP... | File and Printer Sharing  | Domain     | Yes     |         |