

finPOWER Connect Azure SQL Database Configuration

Version 1.00

15 January 2021

Table of Contents

Disclaimer	3
Version History	4
Introduction	5
Azure SQL Database Modifications	6
SQL Server Databases versus Azure SQL Databases	7
Microsoft Azure Portal	8
Microsoft SQL Server Management Studio	8
finPOWER Connect Overview	9
Creating a New Database	10
Indirect Database Authentication	11
Create Indirect Database Login	11
Configure finPOWER Connect to use Indirect Database Login	11
Users	13

Disclaimer

This document is for informational purposes only.

All information contained in this document, including code samples, are provided "as is" without warranty of any kind, and Intersoft accepts no liability for any decisions made on the basis of this information.

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

Copyright Intersoft Systems Ltd, 2021.

Version History

[illegible]

Introduction

The finPOWER Connect Enterprise Edition incorporates support for Microsoft's industrial strength database engine "SQL Server", which is designed to handle hundreds of simultaneous users and very large databases.

It also includes a "beta" database provider for Microsoft Azure SQL Databases.

WARNING: This is a BETA database provider. This means you should be cautious using it. It may also be updated in the future to improve its functionality.

Microsoft Azure SQL Databases provide a fully managed platform as a service (PaaS) database engine that handles most of the database management functions such as upgrading, patching, backups, and monitoring without user involvement.

Microsoft Azure SQL Databases are always running on the latest stable version of the SQL Server database engine and patched OS with 99.99% availability.

Because the database is in the cloud, you should consider where your finPOWER Connect application will run. The closer the application is to the database the better your performance will be.

NOTE: Parts of this document reference functionality introduced in finPOWER Connect version 3.3.5.

WARNING: Make sure your backups are working correctly before using your finPOWER Connect database.

Azure SQL Database Modifications

Azure SQL **System Administrators** have full control over all aspects of the SQL Server and everything within it, including the database structure and the data contained in each table.

This means there is nothing specifically stopping the System Administrator from altering the database structure or the data contained in the database. However, altering the database structure or information stored in the database may stop finPOWER Connect from working correctly, and even corrupt information.

WARNING: 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.

Under Software Warranty section

This Warranty is also subject to the additional condition that it immediately becomes void if any attempt by the Licensee to decompile, disassemble, reverse engineer or in anyway modify the System, database structure or data is made without written consent of the Licensor.

Under Termination section

The Licensor may immediately terminate this Agreement if any attempt by the Licensee to decompile, disassemble, reverse engineer or in anyway modify the System is made without written consent of the Licensor.

SQL Server Databases versus Azure SQL Databases

There are a number of differences between a SQL Server Database and an Azure SQL Database, however for the most part they are identical and use the same SQL Query syntax.

- Trusted Connections
 - Azure SQL Databases can use Trusted connections via an Azure Active Directory, but this is more complicated to configure and authenticate
 - For now, finPOWER Connect does not support Trusted Connections for Azure SQL Databases
- Application Roles
 - Azure SQL Databases support Application Roles
 - However, unlike the finPOWER Connect SQL Server provider, Applications Roles are not used. This is related to Trusted Connections not being used
- Hardware
 - Azure Databases can be configured and reconfigured from very small and low cost options to very high specified and costly options

NOTE: It is recommended that configuration of Azure SQL Databases is undertaken by a technically able person.

This document is not intended for beginners, i.e., it assumes a certain level of existing knowledge.

Microsoft Azure Portal

The web-based portal provides management of your Azure services including Azure SQL databases.

- <https://portal.azure.com/>
- Open your Azure "SQL Server" resource
- Under Overview you will find:
 - Server Name, e.g., **intersoft.database.windows.net**
 - Server Admin, e.g., **intersoft_administrator**
- Firewall Configuration
 - Under the Firewall page you should update options and create a Client Rule if necessary
 - Note, when connecting via Microsoft SQL Server Management Studio it may prompt you to add a rule, shortcutting this process (see below)

Microsoft SQL Server Management Studio

We recommend you install the latest version of Microsoft SQL Server Management Studio.

Next, test that you can connect to your Server via SQL Server Management Studio.

- Open Microsoft SQL Server Management Studio
 - From the menu click **File** and click **Connect**
 - Enter details as follows:
 - ✧ Server Type = **Database Engine**
 - ✧ Server Name = Server Name as above, e.g., **intersoft.database.windows.net**
 - ✧ Authentication = **SQL Server Authentication**
 - ✧ Login = Server Admin as above, e.g., **intersoft_administrator**
 - Click **Connect**
 - You may be prompted to create a New Firewall Rule
 - ✧ **Click Sign In...** and login to your Azure Account
 - ✧ Confirm the new rule, adding the IP Address or range

finPOWER Connect Overview

The notes below cover the suggested method of configuring finPOWER Connect to open an Azure SQL Database.

- Remember, finPOWER Connect does not support:
 - Trusted Connections
 - Application Roles
- Therefore, the flow when logging into finPOWER Connect and an Azure SQL Database is as follows:
 - User logs into finPOWER Connect using their User Name and Password
 - ✦ The User Name and Password must be the same for finPOWER Connect and the Azure SQL Database
 - ✦ These credentials are used to open the Azure SQL Database Engine with the minimum permission required to read information
 - The credentials defined under Global Settings "Indirect Database Authentication credentials" are then used to re-authenticate the login
 - ✦ This requires two steps, as we need to read the database configuration to retrieve the indirect database authentication details
 - Finally, the User Name and Password is used to validate the User within finPOWER Connect
- For this to work correctly
 - The Azure SQL Database Login must be kept in sync with finPOWER Connect
 - The Azure SQL Database Login should NOT have write access to the database
 - ✦ This is dangerous and a security issue

Creating a New Database

When creating a new Database, you must use the Azure SQL Database's Server Admin Account.

- Open finPOWER Connect
- From the **File** menu, click **New Database...**
 - Enter Database Type as **MS SQL Azure**
 - Enter the Server Name, e.g., **intersoft.database.windows.net**
 - Optionally enter the port, normally **1433**
 - Enter a Database Name
 - ✦ This must begin with **finPOWERConnect_**
 - ✦ E.g., **finPOWERConnect_Demonstration**
 - Enter your Azure Server Admin Name and Password, e.g., **intersoft_administrator**
 - Click **Next**, **Next** and finally **Finish**

Once the Database has been successfully created you can view it under the Microsoft Azure Portal.

- Review and update Pricing Tier

NOTE: It is important that you select the correct pricing tier for your needs.

WARNING: Make sure you do not have any open connections to your database when changing Pricing Tiers as this will invalidate any open connections.

Indirect Database Authentication

The Azure SQL Server Admin should not be used in day-to-day processing.

Additionally, the "User" Logins should only have very basic Read-Only, i.e., SELECT, access to the database. If these logins had full read/ write rights to the database and the User opened the database in other tools, they could alter the data or even database structure - and this would invalidate the Software Licence Agreement – not to mention potentially corrupt the database or the relationships within the database.

Breaking either of these rules is a major security and data integrity risk.

Therefore, the only way to write to an Azure SQL Database should be via a special "**Indirect Database**" Login that you create.

The next step is to create a new Login for "Indirect Database Access", e.g., "finPOWER_Administrator".

Create Indirect Database Login

To do this, open your Azure Database Engine under Microsoft SQL Server Management Studio.

- Create the Administrator Login
 - Expand Security and Logins
 - ✧ Right-click and select **New Login...**
 - ✧ You can use the template script created, or replace the query with

```
CREATE LOGIN finPOWER_Administrator WITH PASSWORD = '1StrongPassword'  
  
CREATE USER finPOWER_Administrator FOR LOGIN finPOWER_Administrator  
  
EXEC sp_addrolemember 'loginmanager', 'finPOWER_Administrator'
```

- ✧ The first command adds the Login
 - Make sure you use a strong password and record it in a safe place
 - E.g., dPKB5qYaFV015kuDFsKghQii84dCdfuT4j3PxK71Zd
 - ✧ The second command adds a User
 - ✧ The third command gives the User permission create and delete logins
 - This is used to keep Users in finPOWER Connect in-sync with Logins and Users in the Azure SQL Database
- Next add the User to the finPOWER Connect Database
 - Expand Databases, your finPOWER Connect Database, Security and Users
 - Right-click and select **New User...**
 - Replace the query with

```
CREATE USER finPOWER_Administrator FOR LOGIN finPOWER_Administrator  
  
EXEC sp_addrolemember 'db_owner', 'finPOWER_Administrator'
```

- The first command creates the User
 - The second command grants permissions to the User
- For more information on database level roles see
 - <https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/database-level-roles?view=sql-server-ver15>

Configure finPOWER Connect to use Indirect Database Login

- Open finPOWER Connect

- From the File menu, click **Open Database...**
 - Enter Database Type as **MS SQL Azure**
 - Click **Next**
 - Enter the Server Name, e.g., **intersoft.database.windows.net**
 - Optionally enter the port, normally **1433**
 - Enter the Database Name, e.g., **finPOWERConnect_Demonstration**
 - Click **Finish**
- You will then see the finPOWER Connect Login screen
 - Enter your finPOWER Connect User Id and Password, e.g., Admin and Admin
 - Click **Advanced**
 - Check **"Using the following Credentials"**
 - Enter your Indirect Database Login Credentials, e.g., **finPOWER_Administrator** and **1StrongPassword**
 - ✧ Note, we use this to test the Login has been setup correctly
 - Check **"Force direct database authentication?"**
 - Click **Login**
 - ✧ You should see a warning "WARNING: Your login credentials allow write access to the database. This is not recommended and may invalidate your Software Licence Agreement." - this can be ignored.
 - ✧ However, if you see this message logging in as a normal User you should check Permissions are setup correctly
- From the menu click **Tools** and click **Global Settings...**
 - Under the **General** group, **Database** page, at the bottom of the page enter your **Indirect database authentication details**
 - ✧ These are the same values you just logged in with, e.g., **finPOWER_Administrator** and **1StrongPassword**
- Before closing finPOWER Connect you should add or change the default Admin User with finPOWER Connect if its Id is "**Admin**".
 - This is because "Admin" is a reserved Login Name and therefore cannot be used
 - From the menu click **Tools, User Security** and **Users**
 - Select the "Admin" User and click **Edit**
 - On the **General** page change the User Id, e.g., to **finAdmin**
 - On the **Login** page, under **Login Password** click **Change**
 - ✧ Enter a Password
 - Make sure you use a strong password and record it in a safe place
 - ✧ Click **OK**
 - Click **Save**

Users

- finPOWER Connect does not support Trusted Connections
 - This is the main difference between the finPOWER Connect SQL Server Database provider and the Azure SQL Database provider
 - ✦ finPOWER Connect logs a User into a SQL Server database using a Trusted Connection (which has read-only permissions) and then switches to an Application Role that has permissions to write to the database
- Instead, finPOWER Connect will:
 - Create, update and delete Logins and Users within the Azure SQL Database as you add, edit and delete Users in finPOWER Connect
 - Update Login passwords as you change passwords in finPOWER Connect
 - These Logins will only have the permissions assigned to the "public" role, i.e., SELECT
- You cannot have a User with a name of "Admin", "Administrator", "sa" or "root"
 - Trying to add a Login with a restricted login name will return the error:
 - ✦ '[Name]' is not a valid login name in this version of SQL Server
- Manually adding and deleting Azure SQL Database Logins and Users
 - Whilst you can manually add and delete Logins and Users in your Azure SQL Database, finPOWER Connect will do this automatically for you – as noted above
 - You can manually add and delete Azure SQL Database Logins/ Users via the Tools, User Security, Users form
 - ✦ **NOTE: This is not necessary, but provides a way of fixing any issues**
 - ✦ Under Actions, there is an "Azure SQL Database" group
 - Open the User you wish to update
 - Click "Add" to add the Login/ User
 - You will be prompted to re-enter the User's password. This is necessary as finPOWER Connect does not store the Password in a reversible format
 - Note, you can also force the Login/ User to be re-added by updating the User's password
 - Click "Delete" to delete the Login/User
 - Note, if the User Id or Password changes in the future the Login/ User will automatically be added again