aims

advice + information management system

aims azure sql server installation

Document Version: 4.3
October 2020

CONTENTS

AIMS Installation Guide

With the Azure SQL Server version of AIMS you do not need to host your own SQL Server and database, instead you connect to Microsoft's SQL Server service in the cloud. All you need is a subscription to the Microsoft Azure cloud service and a reliable internet connection. Your team could be based in the same location or at opposite ends of the country, it doesn't matter.

Make sure you use the AIMS installer shown on your licence certificate. The licence number on the certificate will not activate any other version of the software.

PLEASE READ THE CONFIGURATION GUIDE CAREFULLY AFTER YOU INSTALL THE SOFTWARE

AIMS is a complex case management database. To make best use of it, there are several configuration issues to consider before you start entering data.

Azure SQL Server

AIMS requires a high-quality internet connection to the Azure cloud service. Intermittent connectivity is likely to cause problems and maybe even loss of data.

The AIMS Team do not provide support for any technical issues relating to Azure, we are only able to provide support for AIMS users in their day-to-day usage of AIMS i.e. on how to do things within AIMS.

Please refer to the AIMS support contract for more information.

If you are not sure if Azure AIMS is suitable for you, please contact us either by email at aims@rightsnet.org.uk or by telephone on 020 7377 2806.

Microsoft Azure configuration

Use the Microsoft Azure portal to create a new, empty database, and make a note of the server name, the administrator username and administrator password.

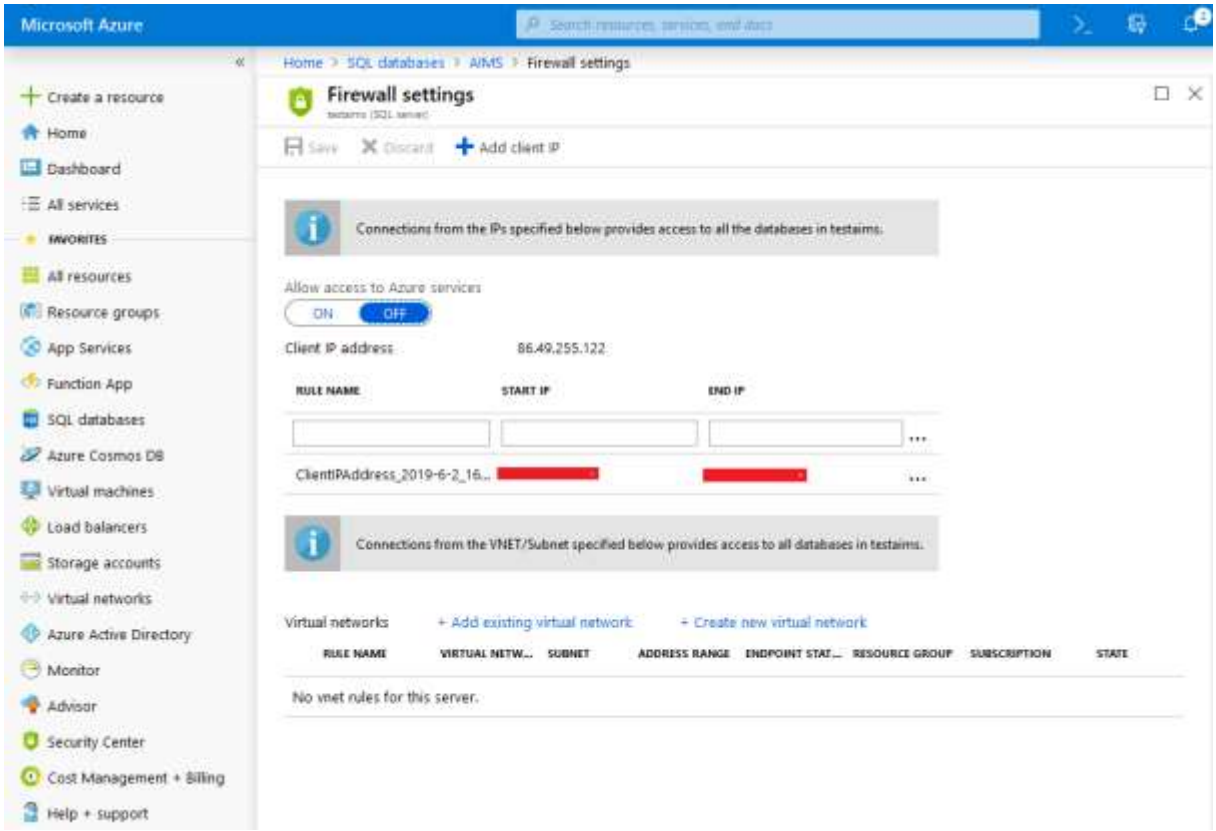
There are many pricing models in Azure, and it is beyond the scope of this document to go into detail about which to use. Fortunately, with Azure you can start small and grow as required, depending how intensively you use AIMS. After installation, with no client data added, the AIMS database occupies about 8 MB space. You should probably allocate about 16 MB to allow for it to grow as you add data.

Azure Server Firewall

Make sure that the Azure server firewall will allow the machine that you are using to run the AIMS Azure installation program to connect to the Azure database.

In the Azure portal, on the Overview page for your AIMS database, you should see a button “Set Server Firewall”. Click it.

Assuming you are accessing the portal from the machine you will run the installation on, simply click on the “Add Client IP” button to add your current external IP address. Then click on the “Save” button.



Later, you will need to unblock access for all the client machines that will be using AIMS.

Installing the AIMS Software

Installation

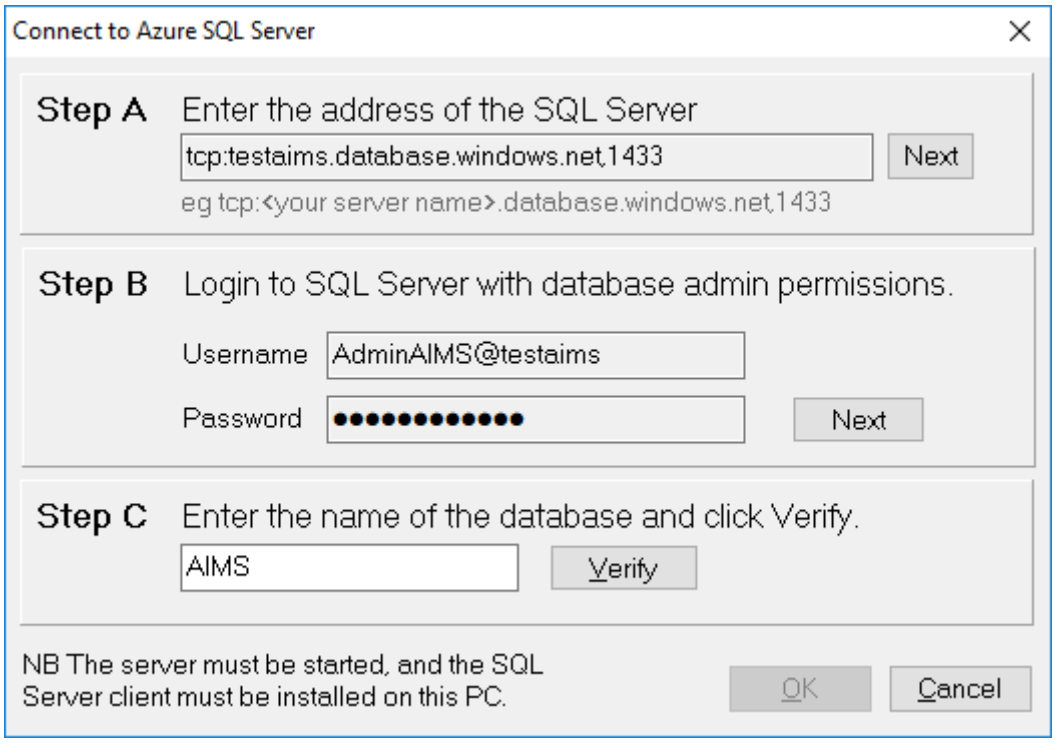
To install the AIMS software, simply download the AIMS Installer and run it, following the on-screen instructions.

You will reach a screen like the one shown below, where you must supply:

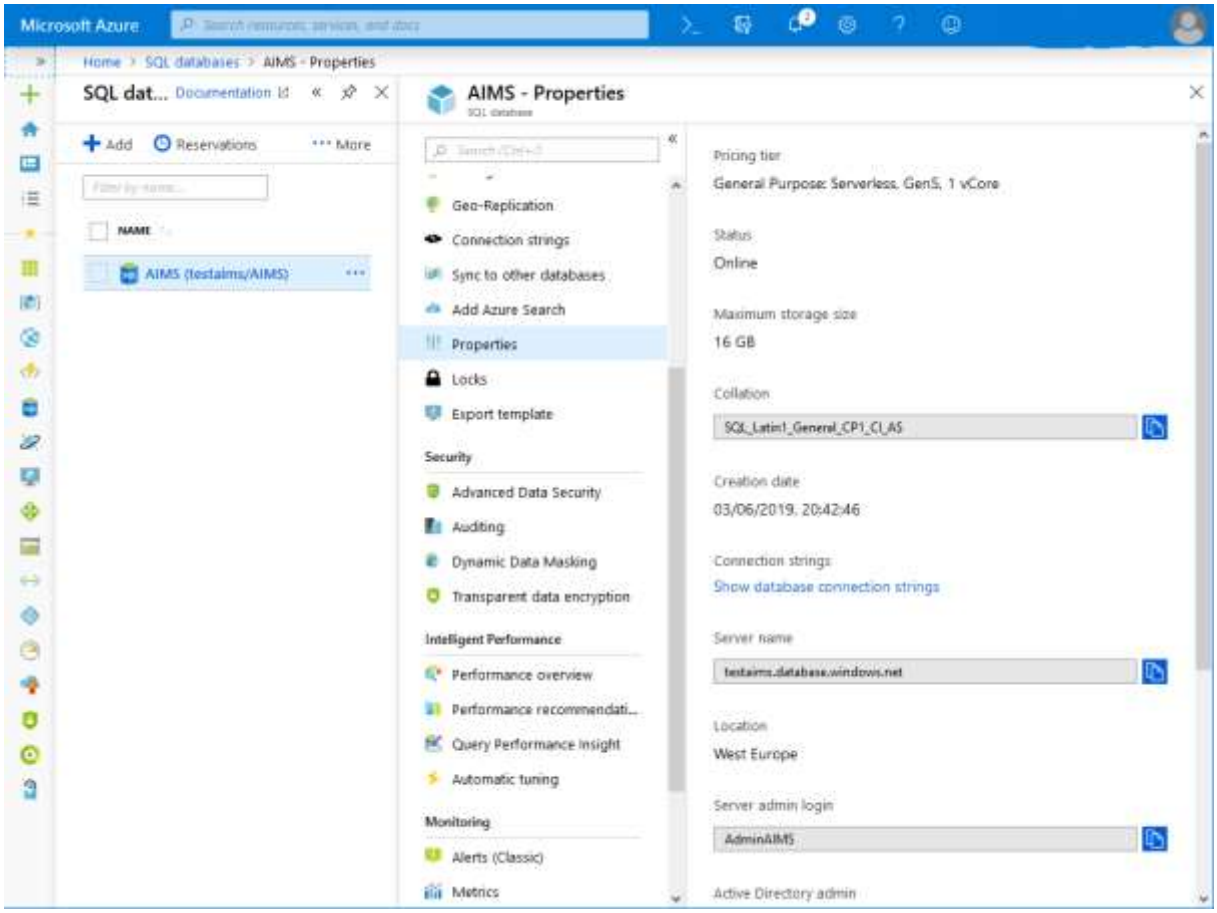
A. The address of your Azure server, usually in the form “tcp:<your server name>.database.windows.net,1433”. Where <your server name> should be replaced with the name of your Azure SQL Server. In the example below, the server is called “testaims”. Click “Next” to proceed to step B.

B. The administrator username and password. Remember the username should be <username>@<your server name>. Click “Next” to proceed to step C.

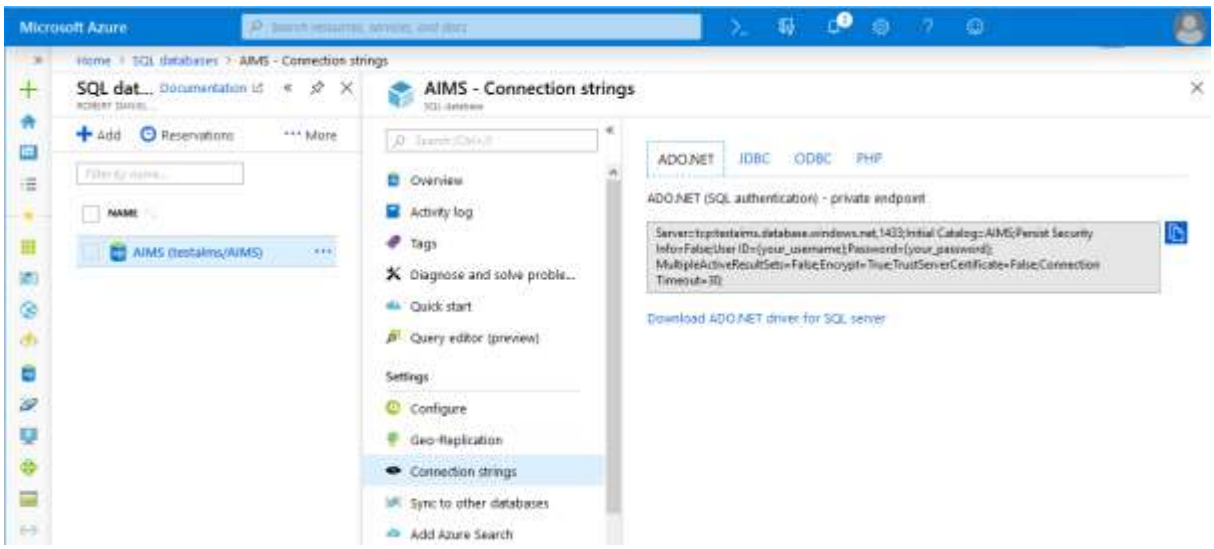
C. The name of the database that you created in Azure for use with AIMS.



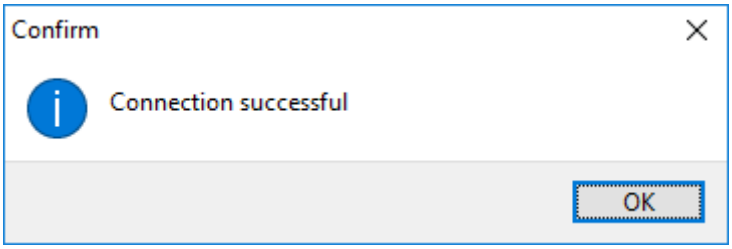
Use the Azure Portal to check the details if you are not sure – select your database in the portal and then select Properties to see an overview of your database settings. “Server name” and “Server admin logon” are the important ones. See the screenshot below for an example.



You can also click on the “Connection strings” option to confirm the full server address. See that the first part says “Server=tcp:testaims.database.windows.net,1433” this is the server address we need.

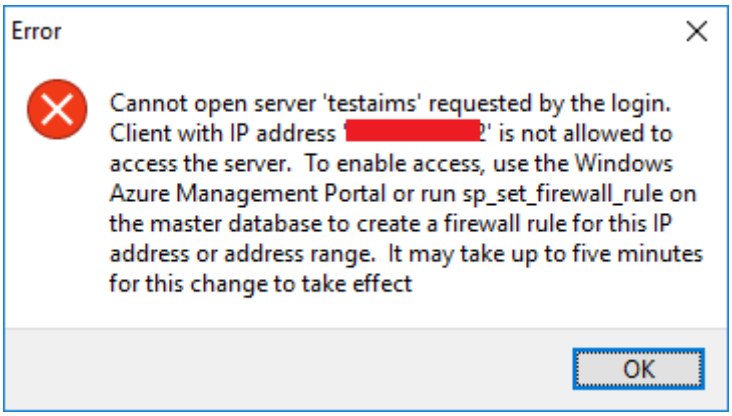


In Step C of the main connection dialog, when you click on the “Verify” button, after a short pause, you should see the “Connection successful” message.



Click OK to close the message, then click OK on the main dialog to complete the setup.

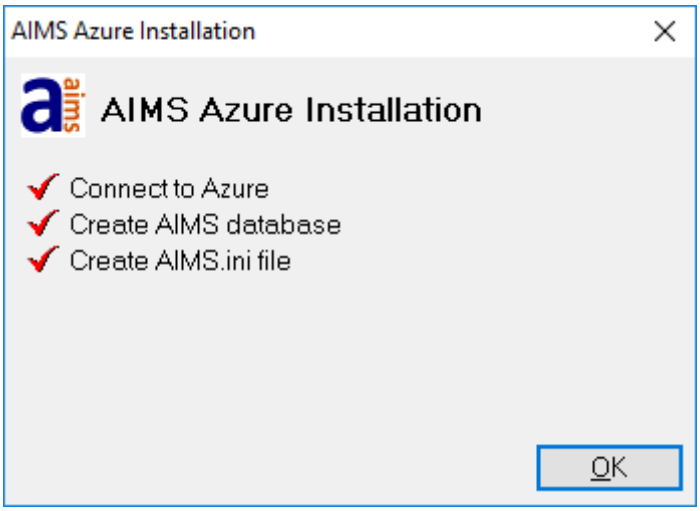
If you see a message like the one below that says “Client with IP address <your IP address> is not allowed to access the server”, then you forgot to open the Firewall in Azure. See the notes on the *Azure Server Firewall*.



The AIMS Azure Installation performs the following tasks:

- Connects to the Azure SQL Server database
- Populates the AIMS database
- Creates the AIMS.ini file
- Installs the AIMS application AIMS.exe and documentation

When the setup has completed successfully, you should see this dialog.



By default, the AIMS software will be installed in “C:\Program Files\AIMS”, or “C:\Program Files (x86)\AIMS” if you have a 64 bit version of Windows. You can change this location during the installation process. AIMS users will need read-only access to the installation directory, in order to be able to run the software and see the documentation.

Shortcuts

The installation will place an AIMS icon on your desktop, to launch the software, and it will create shortcuts on the start menu, in a folder called AIMS.

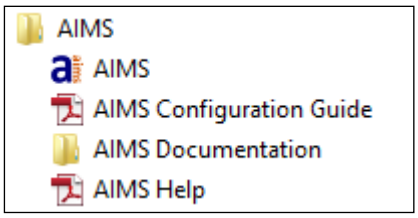


Figure 1: Start Menu Shortcuts

AIMS – Use this link to launch the AIMS software.

AIMS Configuration Guide – This guide leads you through the process of configuring the software, helping you decide which options are best for your organisation.

AIMS Documentation – This link takes you to where the AIMS documentation is stored on disk.

AIMS Help – This link opens the full AIMS help guide. You can also open this guide from within the software using the Help menu, or by pressing the F1 key.

You will probably want to copy these shortcuts on all the AIMS client machines.

Directory Structure

The installation creates a number of folders within the location you specified during the installation process.

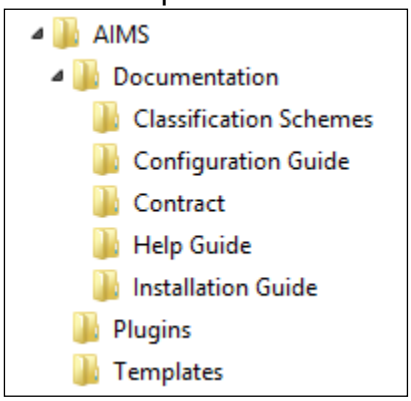


Figure 2: Directory Structure

Documentation - This folder contains all the AIMS documentation, divided in to subdirectories.

Classification schemes - These are the subject classifications that are available for use as the main description of problems brought to you by clients.

Templates - This folder contains example Word mailmerge templates.

Running AIMS for the first time

When the setup is completed, the client workstations can be configured. We recommend you complete the client installation on one machine and test it before configuring the remaining clients. If your client cannot connect to AIMS, see the troubleshooting section of this document.

1. Although modern versions of Windows come with SQL Server client software built in, only the latest drivers fully support Azure SQL Server. Download and install *Microsoft® OLE DB Driver 18 for SQL Server®* Version 18.2.1 or later and install it on each machine where you want to run AIMS. Do not forget to allow each client machine through the Azure Firewall.

To connect to Azure SQL Server, you must be using *Microsoft® OLE DB Driver 18 for SQL Server®* Version 18.2.1 or later. Download this driver from the Microsoft website.

https://www.microsoft.com/en-us/download/details.aspx?id=56730

2. On the Windows desktop, create a shortcut to the AIMS.exe file on your server. You should also create a shortcut to the AIMS Help pdf file on the server.

   You should now be able to open AIMS successfully. Double click the shortcut to the 'AIMS.exe' on the desktop to check that this is so. If AIMS has not been opened before, clicking the shortcut should take you to the 'AIMS - licence Key' screen otherwise the 'AIMS - Login' screen will be displayed.

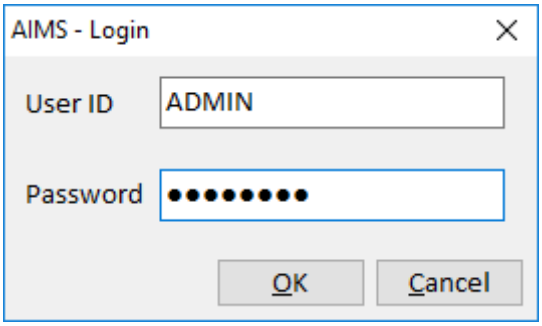
.

The SQL version of AIMS requires two different keys to be added to activate the system. The licence key switches the system on and the subscription key activates the reports module.

See the final section of this document **Activating the License and Subscription Keys** for details of how to enter your subscription key

Do not enter any data until you have read the pre-configuration guide.

3. When AIMS starts, you will be asked to log in.



The default user is User ID = Admin, Password = password. Later, you can avoid this step by configuring Windows Authentication – see Windows Authentication later.

Next you will be prompted to enter the username and password for the Azure database. You can use the administrator details you used to create the database, or another database login if you have one. See Azure SQL Server Authentication

AIMS supports three types of security when connecting to Azure SQL Server.

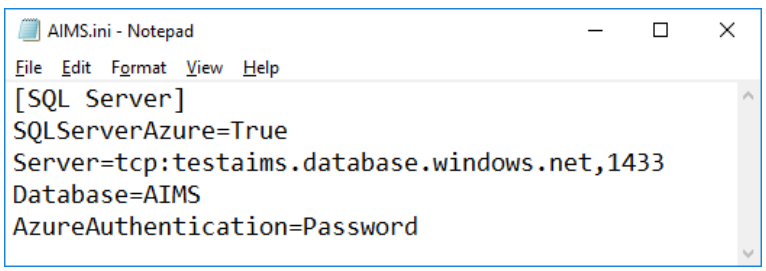
1. SQL Server Password Authentication – this is the default mechanism. It means that in order to connect to the database, users must enter an Azure SQL Server username and password. You may wish to use this mode if you already have Azure SQL Server usernames created.

2. Azure Active Directory Password Authentication – in this mode, users need to enter an Azure Active Directory username and password. You may wish to use this mode if you already have Azure Active Directory usernames created, for example as part of your overall IT security, or as part of an Office 365 setup.

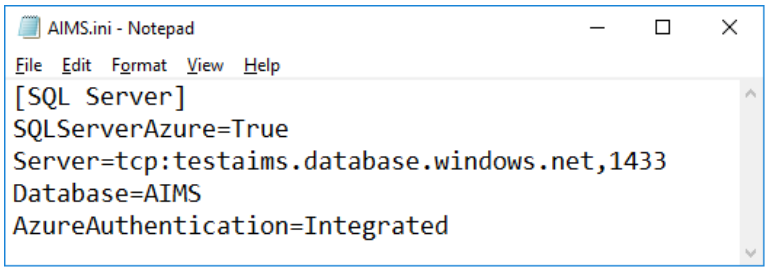
3. Azure Active Directory Integrated Authentication – in this mode, users do not need to enter an additional username and password, Windows supplies the necessary authentication automatically. To use this mode you need to have the Azure Active Directory configured correctly and be using your Azure Active Directory username and password to log in to Windows.

The mode that AIMS uses is controlled by entries in the AIMS.ini file.

To enable Azure Active Directory Password Authentication, add an entry “AzureAuthentication=Password” to your ini file and restart AIMS. For example:



To enable Azure Active Directory Integrated Authentication, add an entry "AzureAuthentication=Integrated" to your ini file and restart AIMS. For example:



To use SQL Server Password Authentication, remove the "AzureAuthentication" line from the ini file.

Remember to install the latest Microsoft OLE DB Driver 18. Azure Active Directory Authentication is only supported in Version 18.2.1, released in February 2019, and later versions.

To connect to Azure SQL Server, you must be using *Microsoft® OLE DB Driver 18 for SQL Server®* Version 18.2.1 or later. Download this driver from the Microsoft website.

https://www.microsoft.com/en-us/download/details.aspx?id=56730

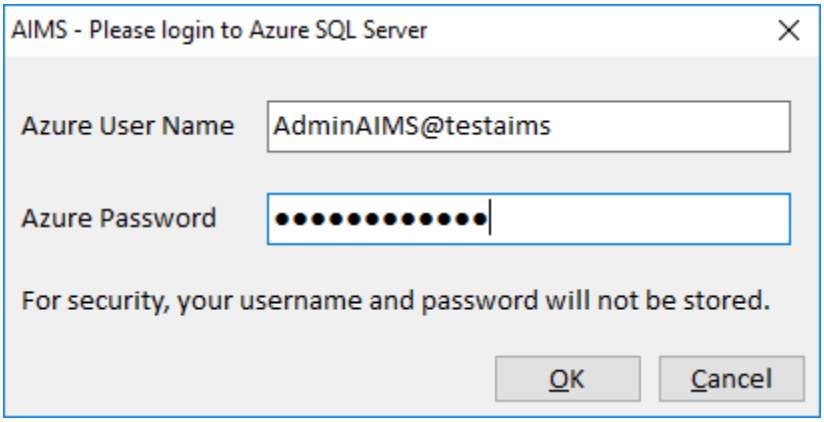
Azure SQL Server and AIMS Database Permissions

Azure SQL Server database users are given different levels of permissions, or database roles. The Azure SQL Server administrator user has full control or ownership of the database. Day to day use of AIMS only requires read and write access to data – the db_datareader and db_datawriter roles in SQL Server terms.

The only exception is when the administrator in AIMS wants to create or delete user-defined fields. This requires the permission to modify table structures, in other words database owner permissions or membership of the db_owner role.

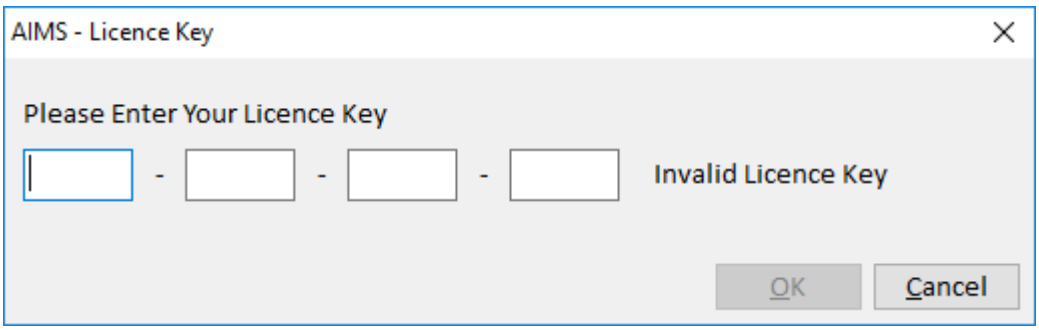
If you are using Azure Active Directory Authentication, we recommend you create two Active Directory groups. One for AIMS administrators and one for normal AIMS users. In the AIMS database you can grant permissions to those two Active Directory groups, and then make Active Directory users members of one of those groups.

4. for more details.



For now, you will need to enter the Azure username and password every time you start AIMS. We hope to be able to implement integrated security to omit this step soon.

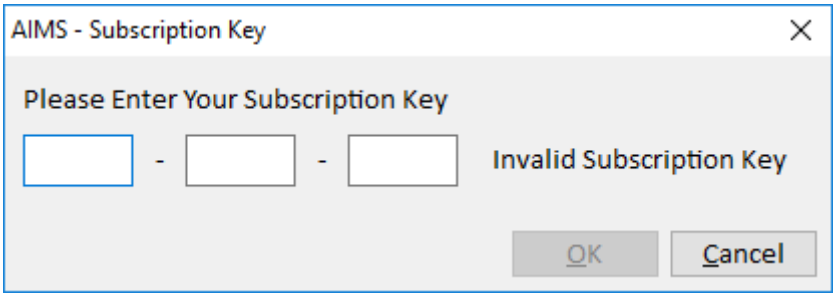
5. Now you will be asked to provide a 12 character Licence Key to activate it. This switches AIMS on and allows you to start configuration. Please read the Configuration Guide carefully as certain choices cannot be changed once any data is entered.



Do not add any test data until you have read the pre-configuration guide.

6. You also need to enter an annually renewable subscription Key. Your 9 character Subscription key can be found on the invoice and in the box at the bottom of the renewal letter. The Subscription Key only works in conjunction with the correct AIMS Licence Key which will already have been encoded.

   To input your Subscription Key you will need to be logged into AIMS as an administrator. **Make sure no-one else is in the database**. Go to the Admin drop down from the main menu bar and select Subscription Key.

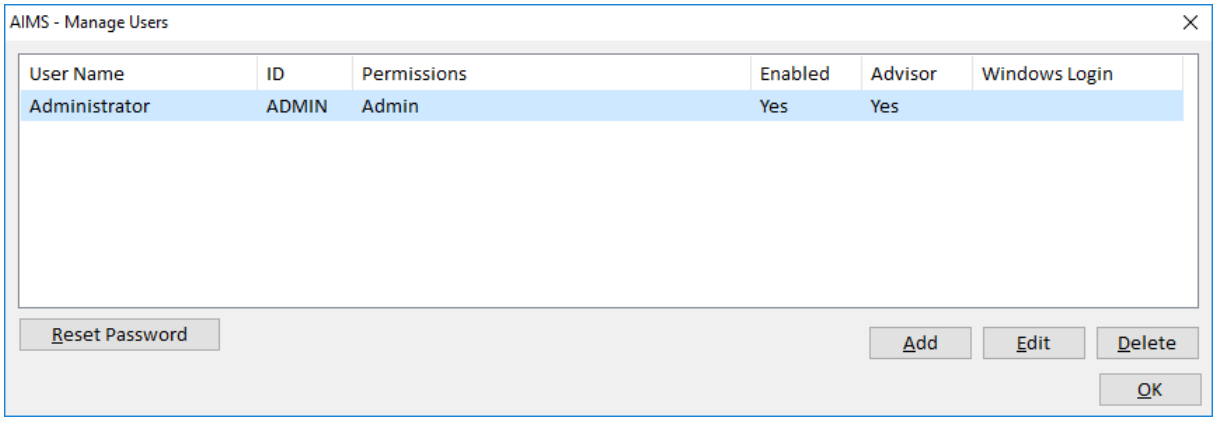


Now fill in the boxes putting three characters in each box. Or if updating with a subsequent years subscription renewal, over write the existing key details. The subscription expiry date will be updated the next time you log in to AIMS.

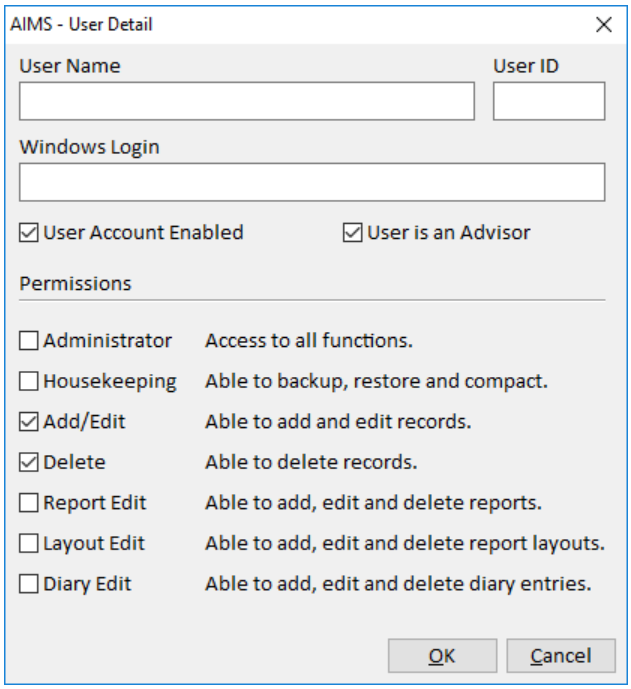
AIMS Users and Windows Authentication

AIMS Users

To distinguish different users in AIMS, create a unique user ID for each one. From the main menu, select Admin and then Manage Users.

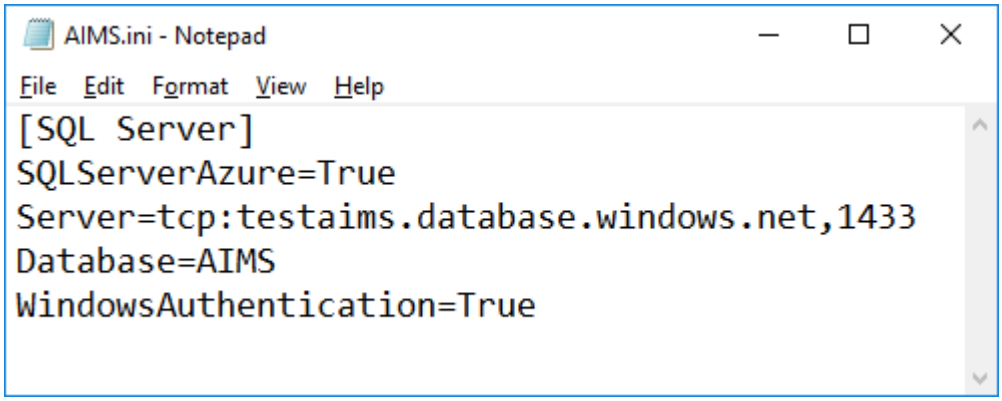


To add a new user, click the “Add” button and fill out the user details. You can restrict what the user is allowed to do by ticking or unticking the permissions boxes. For more inforation, refer to the main AIMS help guide.

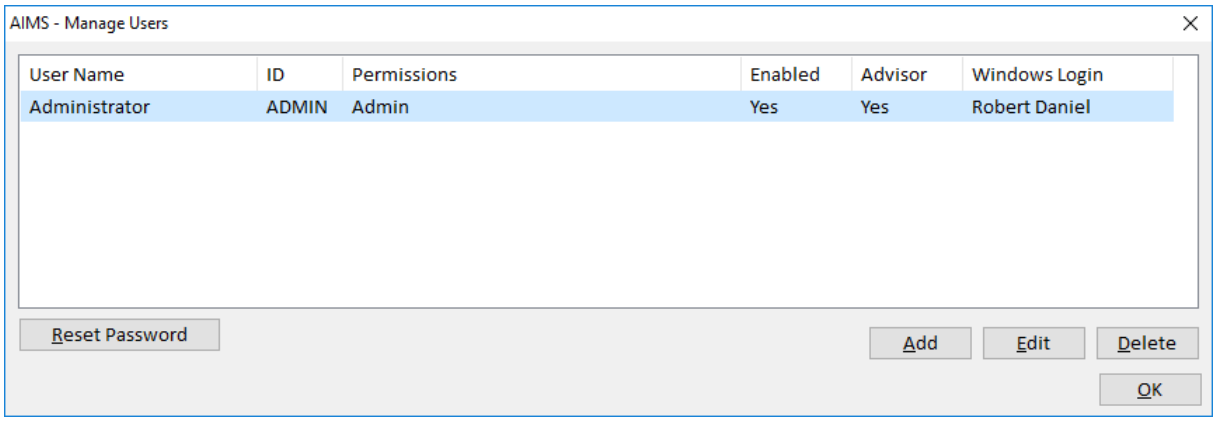


Windows Authentication

Enabling Windows Authentication enables AIMS to deduce your AIMS user id from your Windows login details. In the above screens you will notice a field for “Windows Login”. If you do not see that field, you need to edit the AIMS.ini file and add the line “WindowsAuthentication=True”. You need to restart AIMS for it to take effect.



Now, enter your Windows user name (check in Windows Settings, Accounts if you are not sure what it is) and enter the full user name. For example:



Exit AIMS and then re-start it. AIMS will read the Windows Login name “Robert Daniel” and look for it in the list of users. If it finds that Windows Login, it will automatically log in the corresponding AIMS user, in this example “ADMIN”.

Obviously you should only use this feature in environments where each user has their own Windows Login and they do not leave the computers logged in and unattended.

To disable Windows Authentication, delete the entry “WindowsAuthentication=True” from the AIMS.ini file, or change it to “WindowsAuthentication=False”.

Azure SQL Server Security, Users and Logins

Azure SQL Server Authentication

AIMS supports three types of security when connecting to Azure SQL Server.

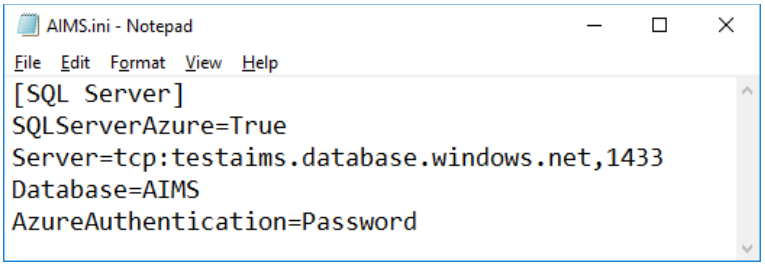
4. SQL Server Password Authentication – this is the default mechanism. It means that in order to connect to the database, users must enter an Azure SQL Server username and password. You may wish to use this mode if you already have Azure SQL Server usernames created.

5. Azure Active Directory Password Authentication – in this mode, users need to enter an Azure Active Directory username and password. You may wish to use this mode if you already have Azure Active Directory usernames created, for example as part of your overall IT security, or as part of an Office 365 setup.

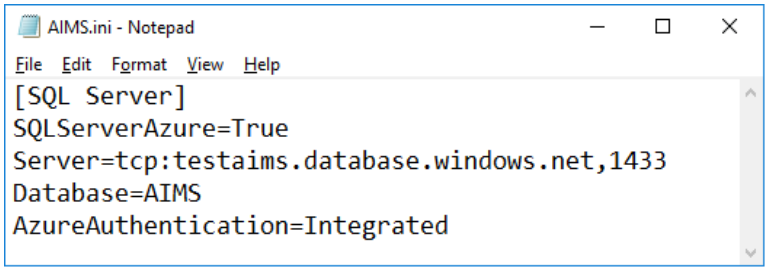
6. Azure Active Directory Integrated Authentication – in this mode, users do not need to enter an additional username and password, Windows supplies the necessary authentication automatically. To use this mode you need to have the Azure Active Directory configured correctly and be using your Azure Active Directory username and password to log in to Windows.

The mode that AIMS uses is controlled by entries in the AIMS.ini file.

To enable Azure Active Directory Password Authentication, add an entry “AzureAuthentication=Password” to your ini file and restart AIMS. For example:



To enable Azure Active Directory Integrated Authentication, add an entry “AzureAuthentication=Integrated” to your ini file and restart AIMS. For example:



To use SQL Server Password Authentication, remove the “AzureAuthentication” line from the ini file.

Remember to install the latest Microsoft OLE DB Driver 18. Azure Active Directory Authentication is only supported in Version 18.2.1, released in February 2019, and later versions.

To connect to Azure SQL Server, you must be using *Microsoft® OLE DB Driver 18 for SQL Server®* Version 18.2.1 or later. Download this driver from the Microsoft website.

https://www.microsoft.com/en-us/download/details.aspx?id=56730

Azure SQL Server and AIMS Database Permissions

Azure SQL Server database users are given different levels of permissions, or database roles. The Azure SQL Server administrator user has full control or ownership of the database. Day to day use of AIMS only requires read and write access to data – the db_datareader and db_datawriter roles in SQL Server terms.

The only exception is when the administrator in AIMS wants to create or delete user-defined fields. This requires the permission to modify table structures, in other words database owner permissions or membership of the db_owner role.

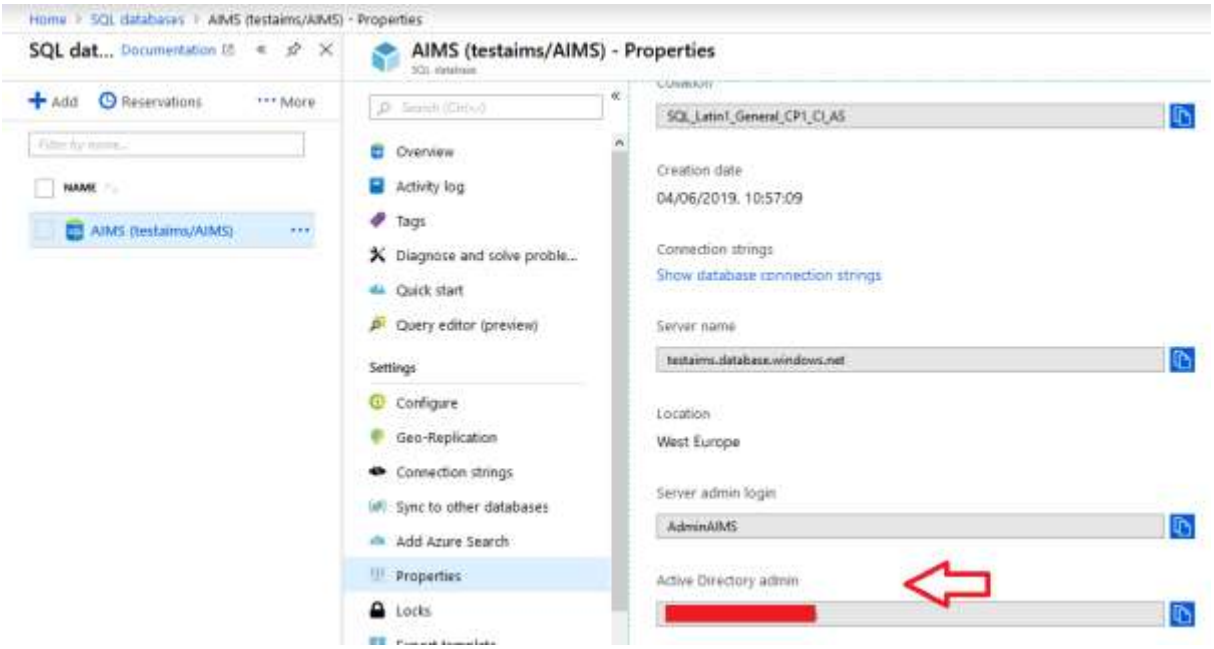
If you are using Azure Active Directory Authentication, we recommend you create two Active Directory groups. One for AIMS administrators and one for normal AIMS users. In the AIMS database you can grant permissions to those two Active Directory groups, and then make Active Directory users members of one of those groups.

Creating an Active Directory Group

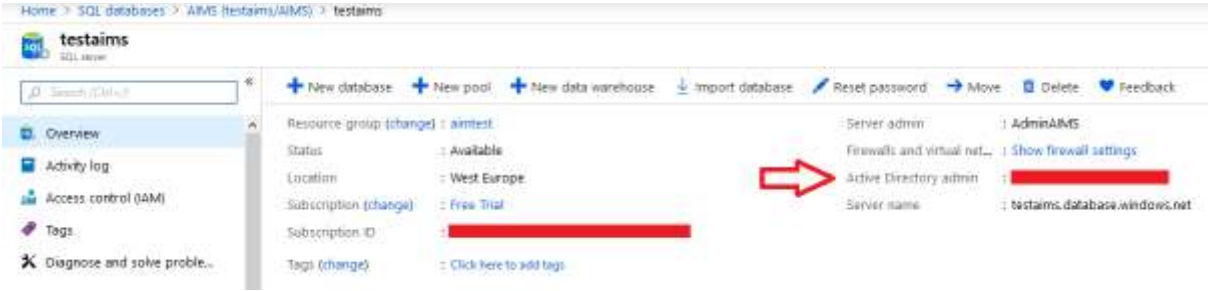
In the Azure Portal, select Azure Active Directory. Then look for Manage… Groups. In the Groups screen, find and click the “New Group” button.
Give the group a name, for example “AimsUsers”. Fill in the other details and click the “Create” button. See below:

Adding an Active Directory Group to the AIMS Database

Before you can use Active Directory in the AIMS database, ensure that the Active Directory admin for the database has been set. Go to the database Properties page and check the Active Directory admin field.

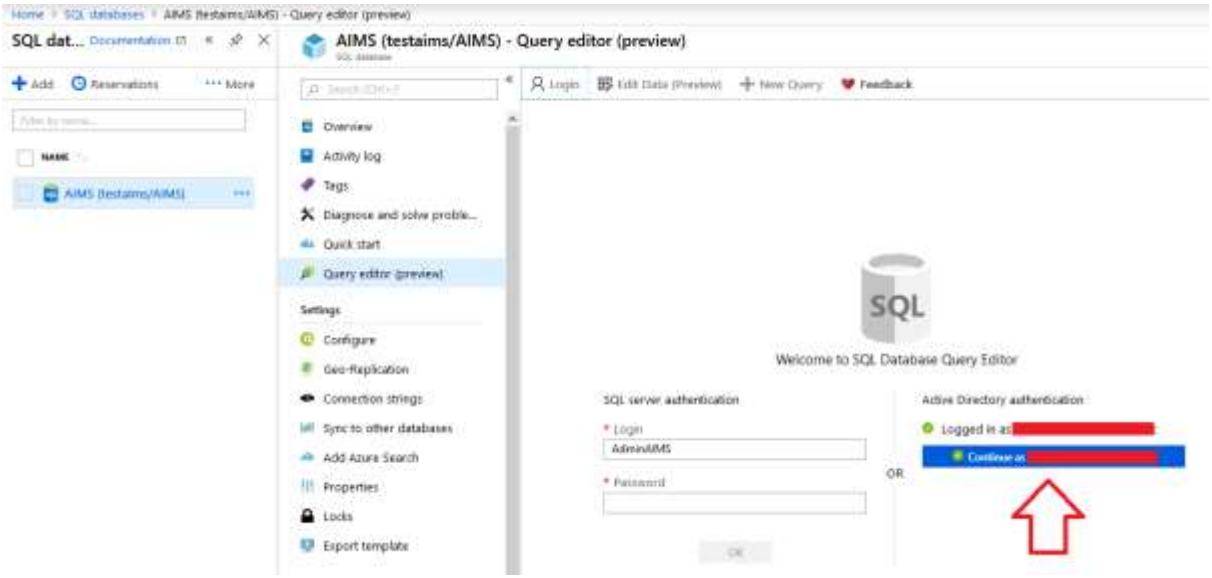


If the Active Directory admin is not set, go the SQL Server page (not SQL databases) for the database and set the admin there.



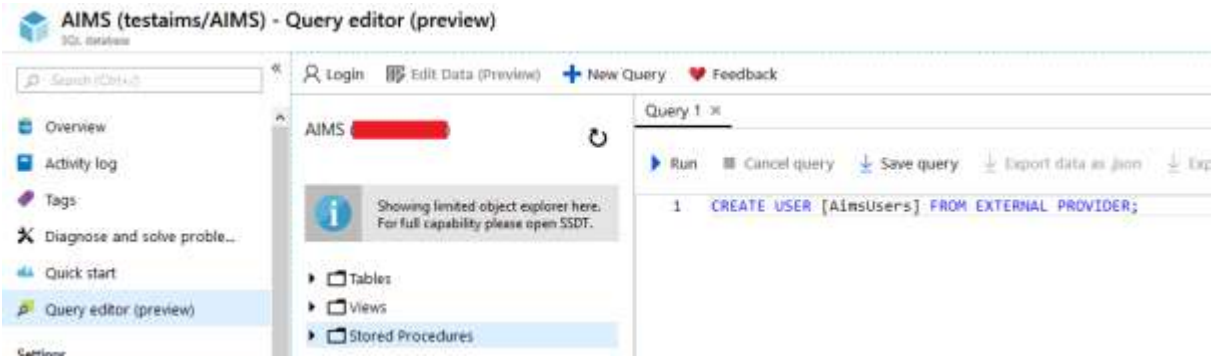
Now you can add the Active Directory group to your Azure SQL Server database. Unfortunately, there is no easy way to do this in the Azure Portal. You have to use SQL commands. If you are familiar with the Microsoft SQL Server Management Studio tool, you can use that. Alternatively, you can use the Query Editor tool in the Azure Portal, which is in preview at the time of writing.

When you log in to the Query Editor, use the Active Directory authentication method. Otherwise you cannot perform operations involving Active Directory. You may also need to allow the Query Editor tool through the database firewall – it has its own IP address. It will prompt you if it is not allowed through.



In the tool, enter the command “CREATE USER [<group name>] FROM EXTERNAL PROVIDER;” where <group name> is the name of the Active Directory group you wish to create as a user in the AIMS database. In our example, below, the group is “AimsUsers”.

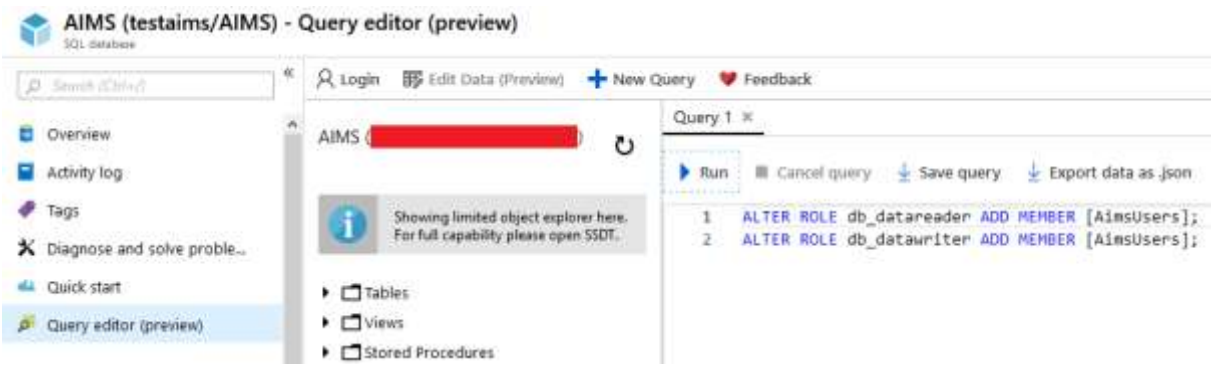
Click the “Run” button and check the messages section below the query window. It should say “Query succeeded”.



Now that you have created the user, you can give it some permissions. For normal day to day AIMS usage, that means db_datareader and db_datawriter. The command required is “ALTER ROLE db_datareader ADD MEMBER [<group name>];” and “ALTER ROLE db_datawriter ADD MEMBER [<group name>];”.

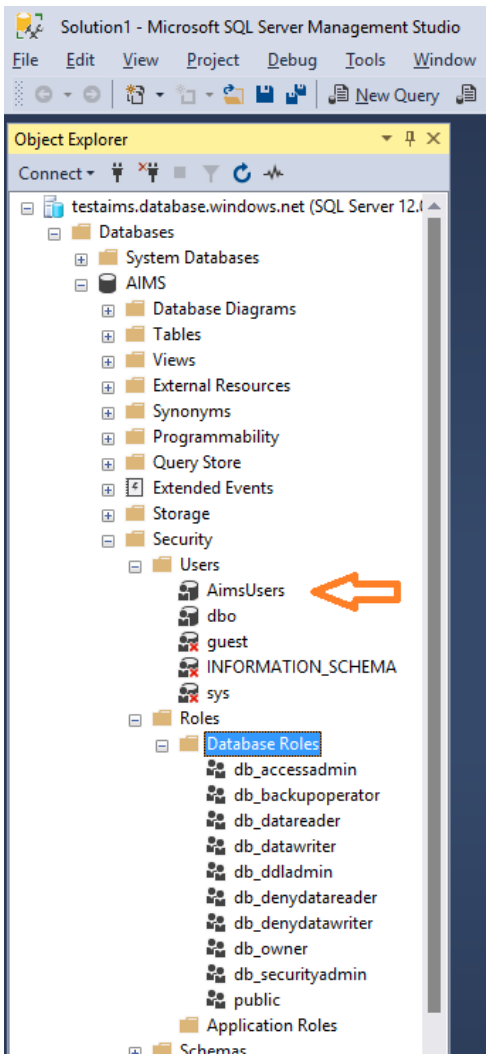
Again, <group name> is the name of your Active Directory group, in our example it is “AimsUsers”. You can run both commands at once, as shown.

Click on the “Run” button and check that the message says “Query succeeded”.



If you are familiar with Microsoft SQL Server Management Studio you can confirm that we have created a user in the AIMS database, called “AimsUsers”. See below.

Any Active Directory user that is a member of the AimsUsers group should now be able to connect to the AIMS database using the Active Directory username and password. Just make sure you set the AIMS.ini file as described in Azure SQL Server Authentication above.



Troubleshooting

If you have any problems setting up AIMS, please read this section before contacting the AIMS team.

The AIMS installation is designed to be as simple and flexible to install and maintain as possible. The AIMS software, manuals and client installation programs are installed on the network file server so they are accessible from each client workstation.

Client machines simply use a shortcut link to the AIMS program file (AIMS.exe) on the server in order to run AIMS. This means that if you need to upgrade the program at some future time, you only need to it in one place. Information about the database connection is kept in a text file, AIMS.ini, installed in the same location as AIMS.exe. This file should have been generated for you by the installation program.

If you have problems getting AIMS to run and connect to the database, please follow the steps below.

On the client machine:

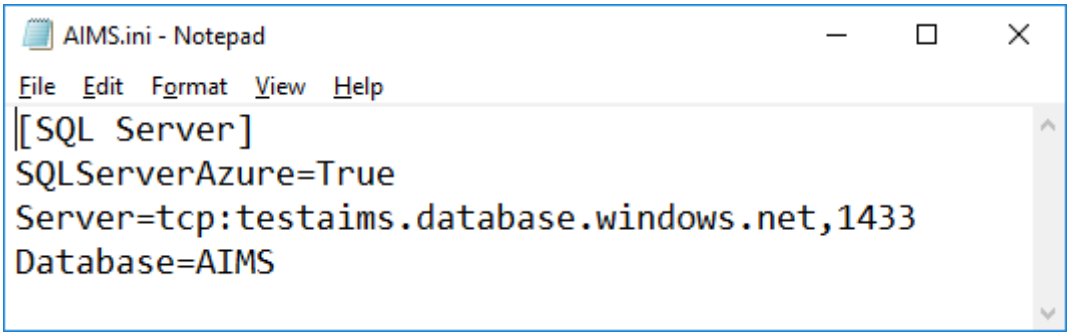
1. Check that the shortcut to the AIMS.exe is pointing to the AIMS.exe file installed on your server. There should not be an AIMS.exe file on the client machine.

2. If AIMS runs but is unable to connect to the database, ensure you have the SQL Server native client installed on the client machine, it is usually pre-installed as part of Windows. Also, check the contents of the AIMS.ini file on the server

On the server machine:

1. Check the **AIMS.INI** file. This file is automatically configured during the installation of the AIMS application, on the server.

   Browse to the folder where you installed the AIMS program (AIMS.exe) and you should find the AIMS.ini file there. Open it using Notepad or another plain text editor. It should look similar to the example below:



The first line should say “SQLServerAzure=True”. Then there should be an entry “Server=tcp:<your server name>.database.windows.net,1433” where <your server name> must be the correct name for the Azure server hosting the database.

The line “Database=” must have the correct name of the AIMS database on the Azure SQL Server.

Save any changes you make to the AIMS.ini file, taking care that Notepad does not save the file as “AIMS.ini.txt”. There is no need to re-start the SQL Server, just re-start AIMS on a client machine.

End.