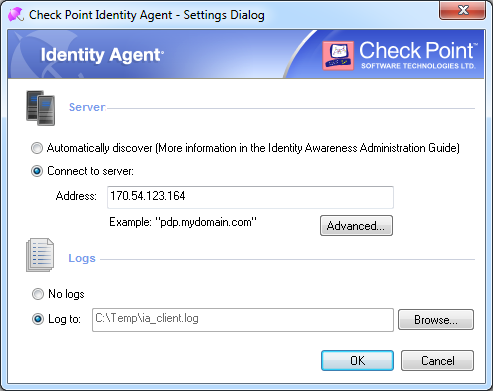
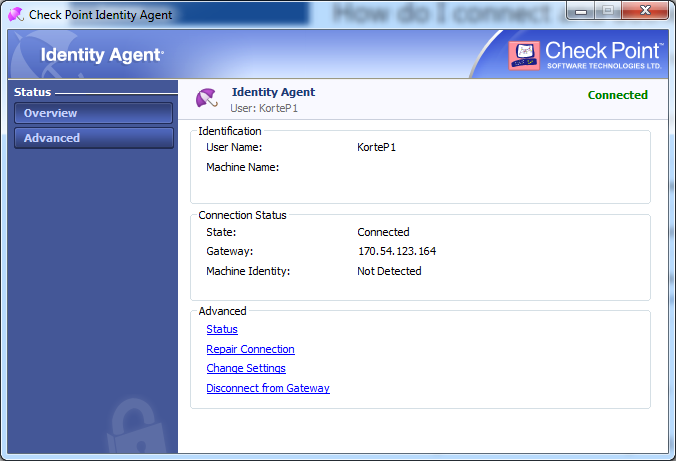
# How to Connect to Azure SQL Server, Azure MySQL or Azure PostgreSQL Databases

The ports used for communication by the databases Azure SQL Server (1433), Azure MySQL (3306), and Azure PostgreSQL (5432) are blocked by default for outbound on-premises traffic.

To communicate with these databases in Azure from on-premises you will need the following:

1. Have an account that has security privileges to the database (see details below for how to acquire for each type of database)
2. Be a member of the Active Directory group FW\_PHI\_AZURE\_SQL
   1. Request membership from [LanSec](mailto:LANSEC@pioneer.com) which will require your manager’s approval
3. Be connected using the Check Point Identity Agent software
   1. You can download the software [here](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk107415)
   2. Use the IP address 170.54.123.164





## How to Connect to Azure SQL Server with SQL Server Management Studio

If you are using SQL Server Management Studio to connect to your database here are a few tips to help you connect to your database.

First, ensure that you are in one of the Active Directory groups that are automatically applied to each SQL Server instance in Azure. The three groups offer different levels of access. They are -

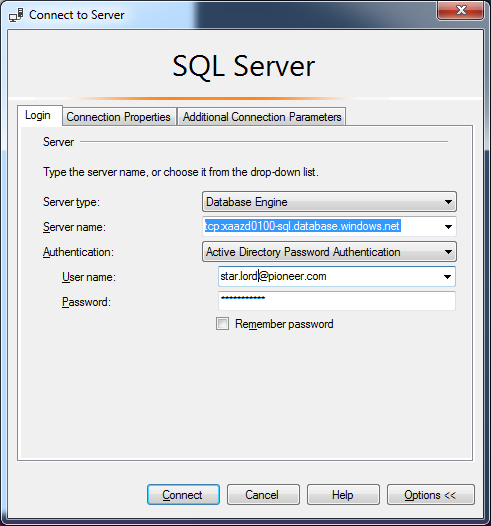
* <Resource Group Name>-SQL-ADMIN
* <Resource Group Name>-SQL-WRITE
* <Resource Group Name>-SQL-READ

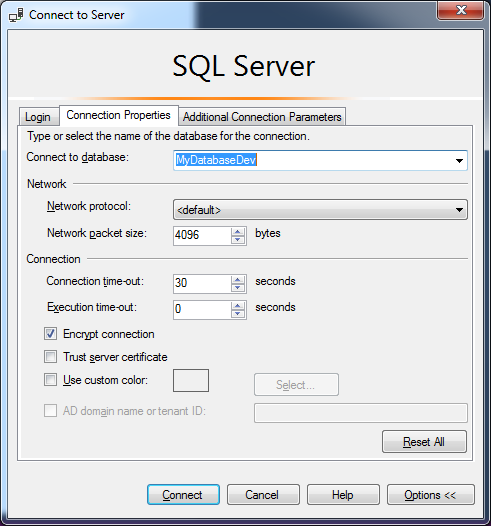
Requests to be added into one of the groups for your database can be sent to [LanSec](mailto:LANSEC@pioneer.com).

When setting up your connection make sure to do the following –

1. Use **tcp:** as a prefix to your server name This forces communication over TCP rather than Named Pipes or other legacy communication protocols.
   1. DO - use **tcp:**xaazd0100-sql.database.windows.net instead of xaazd0100-sql.database.windows.net
2. Use your logon name as your user name rather than your domain identity
   1. DO - use star.lord@pioneer.com instead of PHIBRED\lordst
3. You must provide the name of the database you are connecting to under the Connection Properties tab

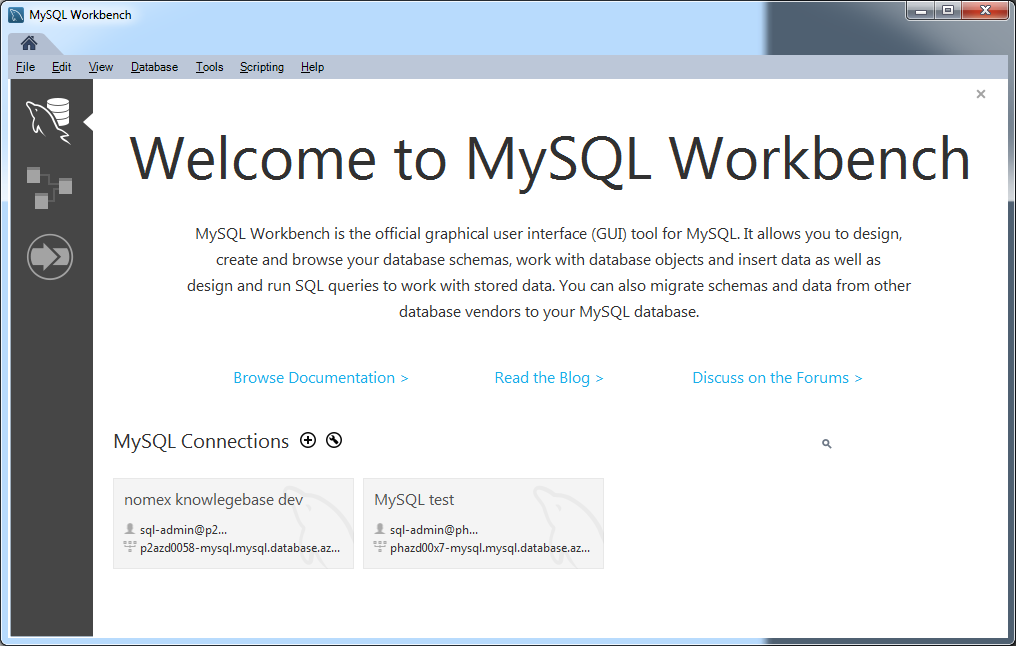
Your connection configuration should like below when you implement the tips above





## How to Connect to Azure MySQL with MySQL Workbench

This example uses the free MySQL Workbench management tool. If you don’t have the MySQL Workbench application you can download it [here](https://dev.mysql.com/downloads/workbench/) and follow the instructions to install.

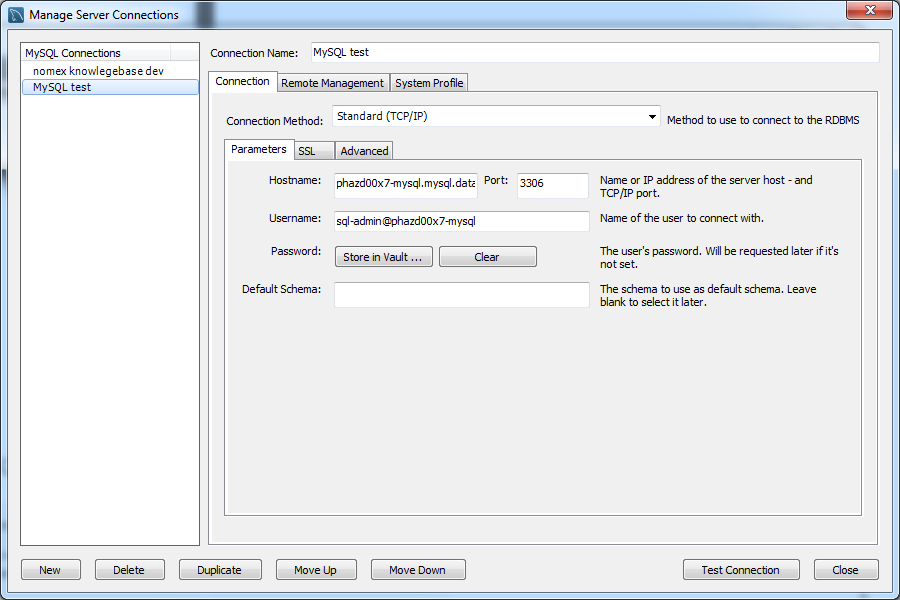


## Add MySQL Connection

MySQL uses internal server accounts and is not integrated with Active Directory. You can request a MySQL account by contacting the [Cloud Engineering team](mailto:DL-AzureSupport@pioneer.com). Please provide your user identity, the resource group name, and the access level requested – read, write, or admin. All requests for access must be approved by the resource group owner.

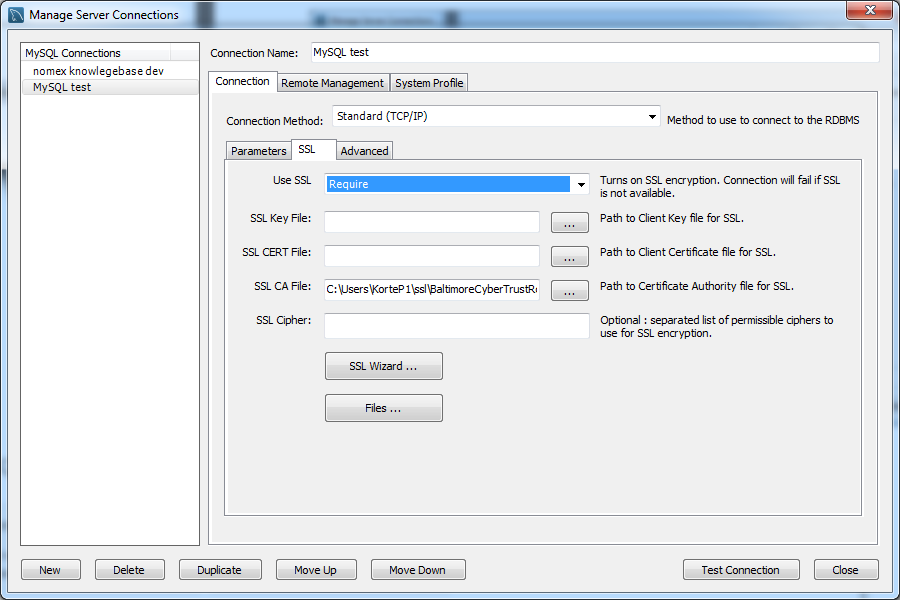
All communications between on-premises and Azure databases are encrypted. To enable SSL communications to Azure MySQL follow the instructions [here](https://docs.microsoft.com/en-us/azure/mysql/howto-configure-ssl) and download BaltimoreCyberTrustRoot.crt.pem.

Select the plus icon to the right of MySQL Connections to configure a connection to your Azure MySQL server database. Provide the hostname, username, and password.



Select the SSL tab and select Require SSL for Use SSL.

Provide the location to the BaltimoreCyberTrustRoot.crt.pem file you downloaded in the SSL CA File.



Select Test Connection. You should see a success message.

## How to Connect to Azure PostgreSQL with pgAdmin

This example uses the free PostgreSQL management tool pgAdmin. You can download the pgAdmin from [here](https://www.pgadmin.org/) and follow instructions to install.

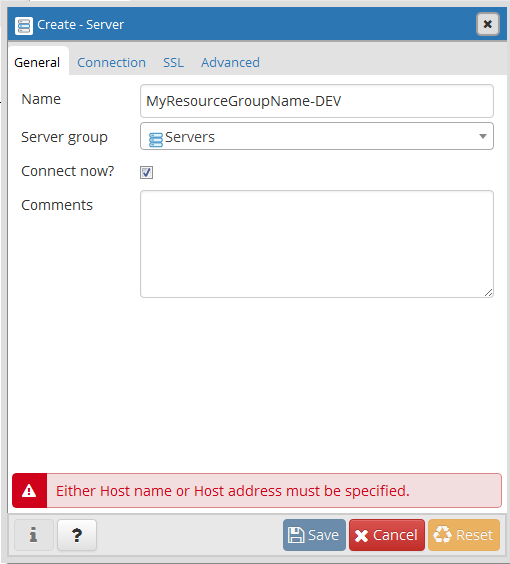
PostgreSQL uses role based security with privileges specifically granted to each role, or inherited by granting a role to another role. Azure PostgreSQL is not integrated with Active Directory. You can request a PostgreSQL role by contacting the [Cloud Engineering team](mailto:DL-AzureSupport@pioneer.com). Please provide your user identity, the resource group name, and the access level requested – read, write, or admin. All requests for access must be approved by the resource group owner.

All communications between on-premises and Azure databases are encrypted. To enable SSL communications to Azure PostgreSQL follow the instructions [here](https://docs.microsoft.com/en-us/azure/postgresql/concepts-ssl-connection-security). Once you have your root.crt, you are ready to connect.

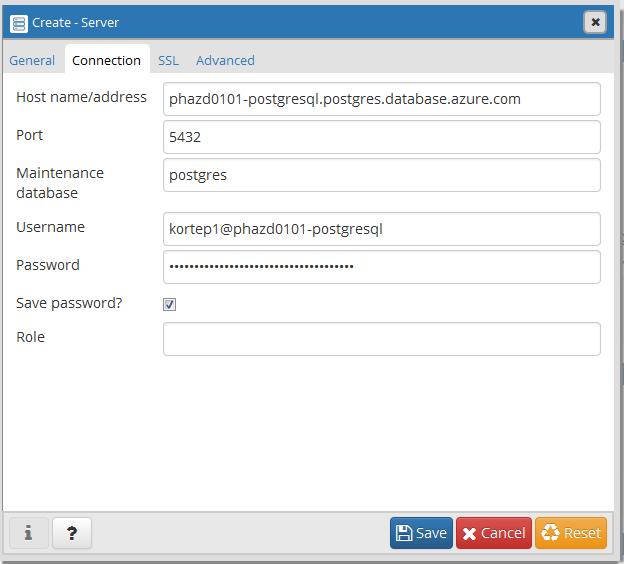
## Add PostgreSQL Connection

Right click on the Servers in the left pane, then select Create and then Server as shown below.

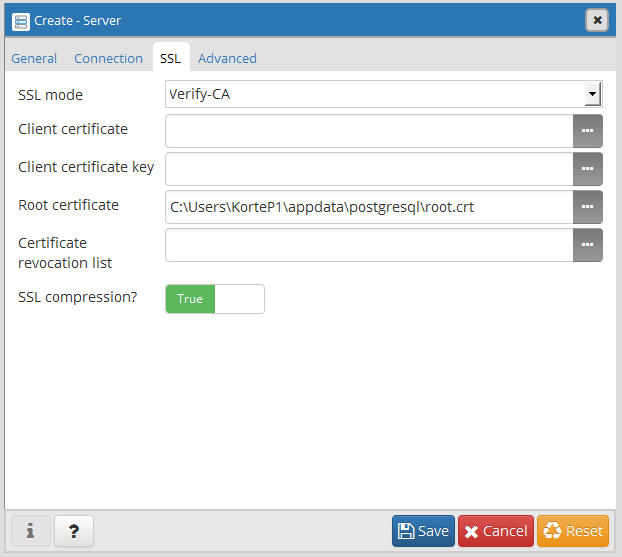




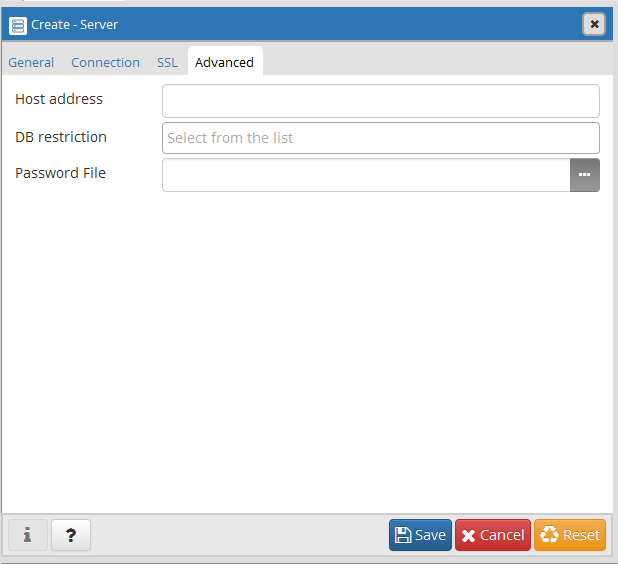
In the Create - Server dialog, choose a name to describe the database you’re connecting to.



On the Connection tab, enter the host name in Azure, user name, and the password that you received from the CET team.



On the SSL tab, select the SSL Mode of Verify-CA, select your root.crt file for Root certificate and then set the SSL compression value to True.



On the Advanced tab, there are no values needed.

Select Save and you should now be connected.