Connecting Database Indexer to Azure SQL Database

Set up Firewall

To connect Database Indexer to an Azure SQL Database, a firewall policy must be created to allow Database Indexer to connect to the database.

It is recommended to use a trusted server with a static IP address to index an Azure SQL Database for the purpose of security and ease of firewall management.

Another more advanced option is to use a Virtual Network Firewall rule

Option 1. Create an IP Firewall Rule

1. Go to the Azure SQL Server Firewall Rules Page
    a. Log into the Microsoft Azure Portal from the server/computer running Database Indexer.
    b. From *All Resources* select your *SQL Server*
    c. Under *Security* select *Firewalls and virtual networks*
2. Create a new Firewall Rule
    a. Copy the displayed Client IP Address of the computer.
    b. Paste it into the 'Start IP' and 'End IP'
    c. Add a name for the rule.
3. Click *Save* to save the Firewall Rule.

Refer to:

Create a virtual network using the Azure portal

Create a Site-to-Site connection in the Azure portal

Ensure your SQL Server has had the new Virtual Network added to its firewall rules.

Connect Database Indexer

1. Open Database Indexer and select *Add Database*.
2. Use the MSSQL Database type and fill in the fields using the SQL Database Information provided to you by Azure.
3. Click *Save*