

**SQL SERVER AZURE SETUP GUIDE**

**The Below requirements are needed to establish a connection sql server azure .**

**Prerequisites**

Prerequisiteslink  
To connect your SQL Server database to Fivetran, you need:  
  
SQL Server version 2012 or above  
An Azure account with a DB Owner, SQL Server Contributor, or SQL Security Manager role  
ALTER ANY USER permissions in your database server  
Your database host's IP (e.g., 1.2.3.4) or domain (e.g., your.server.com)  
Your database's port (usually 1433)  
(If you want to connect using SSH) An SSH server

**Setup Guide**

1. Choose a connection method

* First, decide whether to connect your Azure SQL managed instance directly or using an SSH tunnel.

1. Connect directly (TLS required)

* IMPORTANT: You must have TLS enabled on your database to connect directly to Fivetran. Follow Azure's TLS setup instructions to enable TLS on your database.
* Fivetran connects directly to your database instance. This is the simplest connection method.
* To connect directly, create a firewall rule to allow access to Fivetran's IPs for your database's region.

1. Connect using SSH

* Fivetran connects to a separate server in your network that provides an SSH tunnel to your database. You must connect through SSH if your database is in an inaccessible subnet on a virtual network.
* To connect using SSH, create a firewall rule to allow access to your SSH tunnel server's IP address.
* Before you proceed to the next step, you must follow our SSH connection instructions to give Fivetran access to your SSH tunnel. If you want Fivetran to tunnel SSH over TLS, follow Azure's TLS setup instructions to enable TLS on your database.

1. Enable access

* Configure a server firewall to grant Fivetran's data processing servers access to your database.
* Log in to the Azure console.
* On the Azure main page, select Azure SQL.
* Click the Azure SQL managed instance that you want to connect to Fivetran.
* On the instance overview page, find the host URL and make a note of it. You will need it to configure Fivetran.
* In the left menu, go to the Security section. Click Networking.
* Set the Public endpoint toggle to Enable.
* Click Save.
* In the left menu, click Overview.

1. Click the Virtual network/subnet .

* In the left menu, go to the Settings section. Click Subnets.
* On the Subnets page, find the security group and make a note of it.
* Return to the resource group that contains your managed instance. Click the network security group that you noted in the last step.
* In the left menu, go to the Settings section. Click Inbound security rules.
* On the Inbound security rules page, click Add to add a new firewall rule with a memorable name (for example, Fivetran). What you enter in the IP fields depends on whether you're connecting directly or using an SSH tunnel.
* If you are connecting directly, use the following settings:
* Source : Fivetran's IPs for your managed instance's region
* Source Port Range : \*
* Destination : Any
* Service: Custom
* Destination port ranges : 3342
* Protocol : TCP
* Action : Allow
* Priority : Set a higher priority than the deny\_all\_inbound rule.
* If you are connecting using an SSH tunnel, use the following settings:
* Source : Your SSH tunnel server's IP address
* Source Port Range : \*
* Destination : Any
* Service: Custom
* Destination port ranges : 3342
* Protocol : TCP
* Action : Allow
* Priority : Set a higher priority than the deny\_all\_inbound rule.
* Click Add.

1. Create user

* Create a database user for Fivetran's exclusive use.
* Open a connection to your Azure SQL database.
* Add a container database user by running the following command. Replace <database> with the name of your database, <username> with the username of your choice, and <password> with a password of your choice:
* USE [<database>];
* CREATE USER <username> WITH PASSWORD = '<password>';
* content\_copy

1. Grant user permissions

* Once you've created the Fivetran user, grant it SELECT permission for the database, schemas, tables, or specific columns you want Fivetran to sync. You can grant access to everything in a given database:
* GRANT SELECT on DATABASE::[<database>] to <username>;
* content\_copy
* or all tables in a given schema:
* GRANT SELECT on SCHEMA::[<schema>] to <username>;
* content\_copy
* or a specific table:
* GRANT SELECT ON [<schema>].[<table>] TO <username>;
* content\_copy
* or a set of specific columns in a table:
* GRANT SELECT ON [<schema>].[<table>] ([<column 1>], [<column 2>], ...) TO <username>;
* content\_copy
* or all but a set of specific columns in a table:
* GRANT SELECT ON [<schema>].[<table>] TO <username>;
* DENY SELECT ON [<schema>].[<table>] ([<column X>], [<column Y>], ...) TO <username>;
* content\_copy

1. Enable incremental updates

* We use one of SQL Server's two built-in tracking mechanisms for incremental updates: change tracking (CT) and change data capture (CDC). When enabled, both CT and CDC keep a record of the table rows that have changed in a certain window of time (the default window is the most recent 2 days). These mechanisms let Fivetran copy only the rows that have changed since the last data sync so we don't have to copy the whole table every time.
* Choose to enable either change tracking or change data capture. To learn more about CT and CDC, see our updating data documentation.

1. Change tracking

* Enable change tracking at the database level:
* ALTER DATABASE [<database>] SET CHANGE\_TRACKING = ON;
* content\_copy
* Enable CT for each table you want to integrate:
* ALTER TABLE [<schema>].[<table>] ENABLE CHANGE\_TRACKING;
* content\_copy
* Grant the Fivetran user VIEW CHANGE TRACKING permission for each of the tables that have change tracking enabled:
* GRANT VIEW CHANGE TRACKING ON [<schema>].[<table>] TO <username>;
* content\_copy

1. Change data capture

* Enable change data capture at the database level:
* USE [<database>];
* EXEC sys.sp\_cdc\_enable\_db;
* content\_copy
* Enable CDC for each table you want to integrate:
* EXEC sys.sp\_cdc\_enable\_table
* @source\_schema = [<schema>],
* @source\_name = [<table>],
* @role\_name = [<username>];
* content\_copy
* NOTE: Fivetran only supports tables with a single CDC capture instance. Our syncs only include tables and columns that are present in a CDC instance. If you add new tables or columns, you must create a new CDC instance that includes them and delete the old instance.

1. Finish Fivetran configuration

* In your connector setup form, enter a destination schema prefix. This prefix applies to each replicated schema and cannot be changed once your connector is created.
* In the Host field, enter the host you copied in Step 2.
* Enter your database instance's port number. The port number is usually 3342.
* For the User, enter <username>@<servername>. The <servername> is part of the Azure host URL you found in Step 2 (for example, <servername>.database.windows.net).
* For the Password, enter the password for the Fivetran-specific user that you created in Step 3.
* For the Database, enter the name of the database that you want to connect to Fivetran.
* Choose your connection method. If you selected Connect via an SSH tunnel, provide the following information:
* SSH hostname (do not use a load balancer's IP address/hostname)
* SSH port
* SSH user
* If you enabled TLS on your database in Step 1, set the Require TLS through tunnel toggle to ON.
* Click Save & Test. Fivetran tests and validates our connection to your Azure SQL managed instance database. Upon successful completion of the setup tests, you can sync your data using Fivetran.

1. Setup tests

* Fivetran performs the following tests to ensure that we can connect to your Azure SQL managed database and that it is properly configured:
* The Connecting to SSH Tunnel Test validates the SSH tunnel details you provided in the setup form. It then checks that we can connect to your database using the SSH Tunnel. (We skip this test if you aren't connecting using SSH.)
* The Connecting to Host Test validates the database credentials you provided in the setup form. It then verifies that the database host is not private and checks that we can connect to the host.
* The Validating Certificate Test generates a pop-up window where you must choose which certificate you want Fivetran to use. It then validates that certificate and checks that we can connect to your database using TLS. (We skip this test if you aren't connecting directly.)
* The Connecting to Database Test checks that we can access your database.
* The Checking Access to Schema Test checks that we have the correct permissions to access the schemas in your database. It then verifies that your database contains at least one table.
* The Validating Replication Config Test verifies that your database has an incremental update mechanism enabled (either CDC or CT).
* NOTE: The tests may take a few minutes to finish running.

