

**SQL SERVER AZURE MANAGED SETUP GUIDE**

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

**Prerequisites**

Prerequisiteslink  
To connect your Azure SQL managed instance 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 3342)  
(If you want to connect using SSH) An SSH server

**Setup Guide**

1. Choose a connection method

* First, decide whether to connect your SQL Server database directly, using an SSH tunnel, or using AWS PrivateLink.

1. Connect directly (TLS required)

* IMPORTANT: You must have TLS enabled on your database to connect directly to Fivetran.
* Fivetran connects directly to your database instance. This is the simplest and most secure connection method.
* To connect directly, create a security rule to allow access to Fivetran's IP.

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.
* Before you proceed to the next step, you must follow our SSH connection instructions to give Fivetran access to your SSH tunnel.
* To connect using SSH, configure your VPC Security Groups and Network Access Control Lists (ACLs) to allow incoming connections to your SQL server host and port (usually 1433) from your SSH tunnel server's IP address.

1. Connect using AWS PrivateLink BETA

* IMPORTANT: You must have a Business Critical plan to use AWS PrivateLink.
* AWS PrivateLink allows VPCs and AWS-hosted or on-premises services to communicate with one another without exposing traffic to the public internet. Learn more in AWS’ PrivateLink documentation.
* Follow our AWS PrivateLink setup guide to configure PrivateLink for your database.

1. Enable access

* Configure a server firewall to grant Fivetran's data processing servers access to your database.

1. Configure security group

* Note: These instructions assume that your instance is in a VPC.
* Click on your SQL instance to expand the view, then go to the Configuration Details tab.
* A panel of details for your read replica appears. Verify that the Publicly Accessible value is Yes if you choose to connect directly. You do not have to make your database publicly accessible if you choose to connect using SSH.
* Write down the read instance's port number. You will need this later.

1. Click the to the read instance's Security Group.

* In the security group panel, select the Inbound tab.
* Click Edit.
* Click Add Rule. This creates a new Custom TCP Rule at the bottom of the list with a blank space for a Port Range and a Source IP address.
* Enter your Port Range and Source IP address values.
* In the Port Range field, enter your instance's port number that you wrote down in Step 3 of this section (usually 1433).
* In the Custom IP field, enter Fivetran's IP if you are connecting directly or {your-ssh-tunnel-server-ip-address}/32 if you are connecting through an SSH tunnel.
* Click Save.

1. Configure Network ACLs

* Return to the RDS Dashboard and click on your instance.

1. Click the to the instance's VPC.

* Select the VPC.

1. In the Summary tab, click the Network ACL .

* You will see tabs for Inbound Rules and Outbound Rules. You need to edit both.

1. Edit inbound rules

* Select Inbound Rules.
* If you have a default VPC that was automatically created by AWS, the settings already allow all incoming traffic. To verify that the settings allow incoming traffic, confirm that the Source value is 0.0.0.0/0 and that the ALLOW entry is listed above the DENY entry.
* If your inbound rules don't include an ALL - 0.0.0.0/0 - ALLOW entry, edit the rules to allow {your-ssh-tunnel-server-ip-address}/32 to access the port number of your read replica (usually 1433). For additional help, see AWS's Network ACLs documentation.

1. Edit outbound rules

* Select Outbound Rules.
* If your outbound rules don't include an ALL - 0.0.0.0/0 - ALLOW entry, edit the rules to allow outbound traffic to all ports 1024-65535 for destination {your-ssh-tunnel-ip-address}/32.
* Enter host and port in setup formlink
* In your Fivetran setup form, enter your host and port.
* For the Host, enter the URL from the Endpoint field in RDS dashboard, without the port.
* For the Port, enter the port from the Endpoint field in RDS dashboard (1433 is the default).

1. Create user

* Create a database user for Fivetran's exclusive use.
* Connect to your SQL Server database as an admin user.
* Execute the following SQL commands to create a user for Fivetran. 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 LOGIN <username> WITH PASSWORD = '<password>';
* CREATE USER <username> FOR LOGIN <username>;
* content\_copy

1. Grant user permissions

* Once the Fivetran user is created, grant it SELECT permission for the set of databases, schemas, tables, or specific columns you would like 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
* Enter user, password, and database in setup formlink
* In your Fivetran setup form, enter your user, password, and database name.
* For the User, enter the username you created.
* For the Password, enter the password you set when you created the user.
* For the Database, enter the database you want to replicate from.

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.
* NOTE: You cannot enable CT or CDC on a read replica. If you enable CDC on your primary database, it applies to your read replica. However, if you enable CT on your primary database, it does not apply to your read replica.
* 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:
* EXEC msdb.dbo.rds\_cdc\_enable\_db [<database>];
* 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. Choose schema prefix

* Each database from your source will be mapped to a schema in the destination by adding a prefix to the source database name. For example, if your source database names are "foo" and "bar" and if you choose the prefix "source1", then you will get schemas "source1\_foo" and "source1\_bar" in the destination.

1. Setup tests

* Fivetran performs the following tests to ensure that we can connect to your SQL Server RDS 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.

