

**SAP HANA SETUP GUIDE**

**The Below requirements are needed to establish a connection sap hana.**

**Prerequisites**

Prerequisiteslink  
To connect your SAP HANA account to Fivetran, you need:  
  
SAP HANA  
SAP HANA Schema (Database) name that you want to connect with  
A Fivetran-specific schema (for example, FIVETRAN\_DB)  
A Fivetran-specific SAP HANA user with read and write permissions  
Password for the user you are using to connect  
IP (for example, 172.16.254.2) or host (for example, your.server.com)  
Port (for example, 30215)  
  
  
Read SAP's Connections for Multitenant Database Containers documentation to identify the port in multitenant database containers.  
  
  
Allow Fivetran's IPs direct access to your SAP HANA database  
  
  
To connect using SSH tunnel, see our SSH connection documentation.

**Setup Guide**

1. Choose connection method

* First, decide whether to connect your generic 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. Follow Microsoft's TLS setup instructions to enable TLS on your database.
* Fivetran connects directly to your database instance. This is the simplest and most secure connection method.
* To connect directly, configure your firewall and/or other access control systems to allow incoming connections to your SQL server host and port (usually 1433) from Fivetran's IPs for your database's region. How you do this will vary based on how your SQL Server database is hosted (cloud platform, on-premises, etc.)

1. Connect using SSH (TLS optional)

* 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.
* To connect using SSH, do the following:
* In your connector setup form, select Connect via an SSH tunnel to expose Fivetran's public SSH key. Copy the key by clicking the blue clipboard icon:
* Add the public key to the authorized\_keys file of your SSH server. The key must be all on one line, so make sure that you don't introduce any line breaks when cutting and pasting.
* If you want Fivetran to tunnel SSH over TLS, follow Microsoft's TLS setup instructions to enable TLS on your database.

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. Allow TCP/IP protocol

* Verify that your database server is configured to allow TCP/IP connections. If your database instance does not have TCP/IP protocol enabled, do the following:
* Open SQL Server Configuration Manager.
* In the tree pane, click SQL Server Network Configuration to expand it.
* Click Protocols for YourInstanceName. If you specified the default instance during installation, the instance name will be MSSQLSERVER.
* In the Status column, verify that TCP/IP is Enabled.
* TIP: If Disabled appears, right-click TCP/IP, then click Enable.
* Right-click TCP/IP, then select Properties.
* Go to the IP Addresses tab and scroll all the way down.
* In the IPAll section, enter your database's port number (usually 1433) for the TCP Port, then click Apply.
* Click OK in the warning dialog box that pops up.
* Click OK in the CP/IP Properties dialog box.
* In the tree pane, click SQL Native Client Configuration to expand it, then click Client Protocols.
* In the right-hand column, verify that Enabled appears next to TCP/IP.
* TIP: If Disabled appears, right-click TCP/IP, then click Enable.
* Right-click TCP/IP, then select Properties.
* Verify that the Default Port is 1433 and that Yes appears next to Enabled.
* Click OK to exit the TCP/IP Properties dialog box.
* In the tree pane, click SQL Server Services.
* In the right pane, right-click SQL Server (YourInstanceName), then click Restart.

1. Create user

* Create a database user for Fivetran's exclusive use. The Fivetran user must be a SQL database user, not an Active Directory user.
* Connect to your SQL Server database as an admin user.
* Create a user for Fivetran by executing the following SQL commands. 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

* Grant the Fivetran user SELECT permission for the databases, 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

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. Depending on whether you are connecting Fivetran to your primary instance or an availability group replica, you may be limited in the mechanism you can choose. See our Supported Configurations documentation for more information.
* 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 CT 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 Fivetran to sync:
* 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 your database host's IP (for example, 1.2.3.4) or domain (for example, your.server.com).
* Enter your database instance's port number. The port number is usually 1433.
* Enter the Fivetran-specific user that you created in Step 3.
* Enter the password for the Fivetran-specific user that you created in Step 3.
* Enter the name of your database (for example, your\_database).
* 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 SQL Server 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 generic SQL Server 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.

