Bravura Security Fabric Implementation: Installing Database Software

1 Requirement

Hitachi ID Bravura Security Fabric requires an external database backend to store its data. You must have a working installation of one of the supported database management systems before you can install *Bravura Security Fabric*.

2 Solution

This document shows you:

3 Supported database management systems

Hitachi ID Bravura Security Fabric works with any of the following database management systems:

- Microsoft SQL Server 2019
- Microsoft SQL Server 2016 SP2
- Microsoft SQL Server 2014 SP3

Both 32-bit and 64-bit versions of these databases will work.

Note: The **Compatibility level** on the Microsoft SQL Server database must be set to a minimum value of **SQL Server 2012 (110)**.

Note: If you are installing SQL Server Reporting Service (SSRS) to use the *Analytics* app, ensure the server is not a Domain Controller.

Express editions should *only* be used for evaluation purposes. Hitachi ID Systems strongly recommends that, whenever possible, you use an enterprise or standard edition, rather than the express database edition.

Database I/O performance on a virtualized filesystem (e.g., VMDK or equivalent) is slow. If the database server software runs on a VM, please use a fast, nearby NAS or SAN to store the actual data files.

WARNING!: Clustered backend databases can lose data during or after cluster failover. Hitachi ID Systems recommends using *Bravura Security Fabric*'s application-level replication rather than clustered databases whenever possible. If your company policy requires the use of clustered databases, have database cluster nodes available as close as possible on the network to the *Bravura Security Fabric* nodes to target directly. See Installing with a shared schema for setting up the *Bravura Security Fabric* nodes in shared schema.

Bravura Security Fabric can leverage an existing database server cluster, but Hitachi ID Systems recommends a dedicated database server instance, preferably one per *Bravura Security Fabric* application server, installed on the same OS image as the core application.

1. The data managed by *Bravura Security Fabric* is extremely sensitive, so it is desirable to minimize the number of DBAs who can access it (despite use of encryption).

2. SQL Server has limited features to isolate workloads between database instances on the same server. This means that a burst of activity from *Bravura Security Fabric* (as happens during auto-discovery) would cause slow responses in other applications. Conversely, other applications experiencing high DB load would slow down *Bravura Security Fabric*.

3. *Bravura Security Fabric* already includes real-time, fault-tolerant, WAN-friendly, encrypted database replication between application nodes, each with its own back-end database. Use of an expensive DB server cluster is neither required nor beneficial.

4. Deploying the database to localhost has performance advantages (minimal packet latency from the application to its storage).

5. Allowing *Bravura Security Fabric* administrators full control over the database simplifies performance and related diagnostics and troubleshooting, especially when we consider that database administrators in most organizations are few in number and very busy.

6. Eliminating reliance on shared database infrastructure also eliminates the need to coordinate events such as database version upgrades, which involve reboots. Some Hitachi ID Systems customers who leverage a shared database infrastructure have experienced application disruption due to unscheduled and un-communicated database outages and restarts.

For more information about choosing a database configuration design, see the whitepaper: “Best Practices for *Bravura Security Fabric* Database Configuration”.

4 Where to install the software

Hitachi ID Bravura Security Fabric can be installed on the same server as the database, or on a separate server.

If *Bravura Security Fabric* is installed on physical hardware, deploying the database on the same server can have the following advantages:

- Reduce total hardware cost.
- The same performance will be achieved, assuming the database server meets the minimum requirements for the database product.

> **Note:** By default, the Microsoft database engine will only use one CPU core, due to license restrictions – the ability to use more CPU cores costs more money.

- Network latency between *Bravura Security Fabric* and the Database Management Server (DBMS) is reduced to zero.
- The backup process can be simplified by taking a snapshot of the complete server, as opposed to making separate backups of multiple servers. This makes the restore process much simpler.
- Both Microsoft SQL Server and *Bravura Security Fabric* require a Windows server as their host operating system.

If *Bravura Security Fabric* and the DBMS are installed on a virtual machine, ensure the database is deployed on a disk with high-speed I/0 (not a vmdk file).

Note that two or more *Bravura Security Fabric* instances may share database schema.

5 Installing and configuring Microsoft SQL Server

This section provides basic instructions for use with a Microsoft SQL Server database and the corresponding client software. These instructions are based on a "standard" configuration. If you want to use a non-standard configuration, or if you experience errors, consult the documentation provided with the SQL Server software.

> **WARNING!:** When setting up SQL Server, avoid using non-alphanumeric characters in your server name, users' passwords, or in any other names (instance, database, schema).

5.1 Overview for setting up Microsoft SQL Server

The following is an overview of required and optional tasks for setting up Microsoft SQL Server to work with *Hitachi ID Bravura Security Fabric*. The tasks are detailed in the sections that follow.

> **Note:** Hitachi ID Systems recommends the enterprise version of SQL Server for a production installation. The express version should *only* be used for evaluation purposes.
>
> Read Supported database management systems and Where to install the software to determine appropriate version for your organization.

To set up Microsoft SQL Server :

1. Install the SQL Server software (p4) if you haven't already.
2. Gather information about your database server that will be required during *Bravura Security Fabric* installation (p6).
3. *Optional:* Create a dedicated database, user, and schema (p7). You can allow *Bravura Security Fabric* **`setup`** to do this for you, as described in the *Bravura Security Fabric* Documentation .
4. *Optional:* Create a dedicated report database user (p10). You can allow *Bravura Security Fabric* **`setup`** to do this for you, as described in the *Bravura Security Fabric* Documentation .
5. *Optional:* Remove public/guest permissions (p18).
6. If you will be using multiple *Bravura Security Fabric* instances or servers (replication), read Working with multiple installations for additional considerations

> **Note:** Ensure you follow Microsoft's best practice guide when setting up your SQL server.

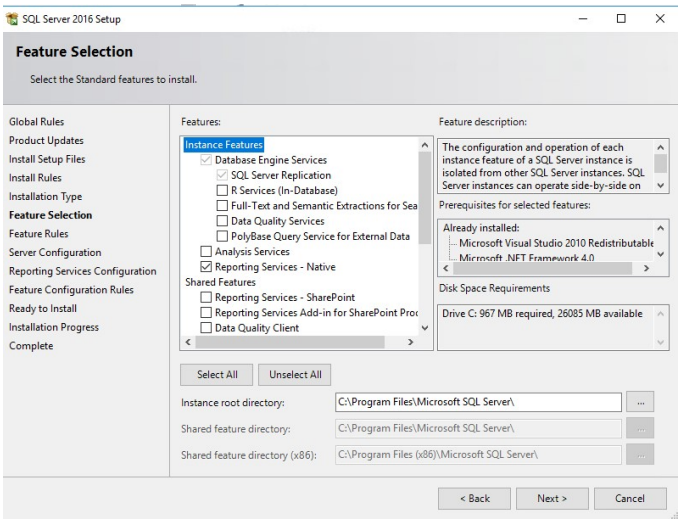
5.2 Installing Microsoft SQL Server

It is recommended that you install Microsoft SQL Server on Windows Server 2012 R2, 2016 or 2019.

1. Install Microsoft SQL Server with the following settings:

   - **Feature Selections**
     - Database Engine Services
     - *Optional:* Reporting Services - Native

       This feature is a requirement to use the *Analytics* app.
     - Client Tools Connectivity
     - Management Tools - Basic
     - Management Tools - Complete



   - **Server Configuration**
     - **SQL Server Agent** NT AUTHORITY\SYSTEM (not available in Microsoft SQL Server Express Edition)
     - **SQL Server Database Engine** NT AUTHORITY\SYSTEM
     - **SQL Server Browser** NT AUTHORITY\LOCAL SYSTEM
     - **SQL Server Reporting Services** NT SERVICE\ReportServer

       (Only available if you chose to install reporting services)
   - **Startup Type** Automatic for all services

     Note: The server collation type must be SQL_Latin1_General_CP1_CI_AS, and the database collation type must be set to Latin1_General_BIN when the database is created later.

   - **Database Engine Configuration** Mixed Mode (SQL Server authentication and Windows authentication).

     Enter and confirm the password. Optionally, you can specify SQL Server Administrators, which use Windows authentication to manage SQL Server.

2. *If you chose to install reporting services*, click **Install and configure** on the ***Reporting Services Configuration*** page.

   This removes the need for the SSRS post installation steps.

3. Verify the features to be installed on the ***Ready to install*** page.

4. Click **Install**.

> **Note:** Consult Microsoft's documentation for detailed installation instructions.

Next:

- Gather information needed for *Hitachi ID Bravura Security Fabric* installation (p6).
- If you decide to install SQL Server Reporting Services after installing SQL Server, complete SSRS post-installation steps (p6).

5.3 SQL Server information required for *Bravura Security Fabric* installation

You need the following information about your SQL Server database before installing *Hitachi ID Bravura Security Fabric*:

- IP address or DNS name of the server that SQL Server is installed on.

  You should verify that you can reach this address from the machine that will host *Bravura Security Fabric*.

  For Microsoft SQL Server Express Edition this is usually `localhost`.

- SQL Server instance name.

  Typically, SQL Server is installed in the default instance, and the instance name is `MSSQLSERVER`.

  Clients that connect to the default instance, including *Bravura Security Fabric*, do not require `\MSSQLSERVER` in their server address lines.

  For Microsoft SQL Server Express Edition this is usually `SQLEXPRESS`.

- Name and password of a system administrator (sysadmin role) login.

  For Microsoft SQL Server Express Edition this is usually `sa`.

5.4 SQL Server Reporting Services post installation

The SQL Server Reporting Services feature is a requirement to use the *Analytics* app in *Hitachi ID Bravura Security Fabric*. The following steps are only required if you add the SSRS feature *after* you have already installed SQL Server; you do not need to do these steps if you installed SSRS during the SQL server install.

> **Note:** The version of SSRS must be the same version as the SQL Server for the instance. For example; SQL Server 2016 and SSRS 2016.

1. Launch Reporting Services Configuration Manager.
2. Click the **Web Service URL** button on the left. Change settings if required.
3. Click **Apply** (whether you change the settings or not).
4. Take note of the Report Server Web Service URL. You will need this when you install *Bravura Security Fabric*.
5. Click the **Database** button on the left.
6. If you do not have a database:
   (a) Click **Change Database**
   (b) Select **Create a new report server database**
   (c) Click **Next**
   (d) Follow the prompts to create a database.

> **Note:** This initial database will not be used; however, SSRS requires an initial database to connect to as part of the install process.

5.5 Creating a dedicated database, user, and schema

Hitachi ID Bravura Security Fabric requires a dedicated database, user and schema in SQL Server in order to connect to a database and install schema objects.

You can allow *Bravura Security Fabric* `setup` to do this for you, as described in the *Bravura Security Fabric* Documentation , or use the following instructions to set up the user and schema yourself.

To create the user and configure its permissions:

1. Start Microsoft SQL Server Management Studio.
2. Connect to the server as a system administrator (sysadmin role).

   You can do this using SQL Server authentication and the sa account, or using Windows authentication if the Windows user has the sysadmin role.

   For example, to connect to the server using the sa account, set:

   Server type to "Database Engine"
   Server name <*host name or IP address*>\<*instance*>
   Authentication to "SQL Server authentication"
   Login to `sa`
   Password to <*password for sa*>

   Click **Connect**.

3. Create a new database for *Bravura Security Fabric*:

   (a) In the **Object Explorer** (left) pane, right-click **Databases**, then click **New Database...**.

   (b) Type the **Database name**.

   (c) Click **Options**.

   (d) Select **Recovery model** and choose **Simple**.

   > **Note:** Ensure that an appropriate database backup policy is in place. See `http://technet.microsoft.com/en-us/library/ms189275.aspx` for more information.

   (e) Select **Compatibility level** and ensure that this is set to a minimum value of **SQL Server 2012 (110)**. The compatibility level for the installed version of Microsoft SQL Server is suitable.

   (f) Select **Auto Create Statistics** and choose **True**.

   (g) Select **Auto Update Statistics** and choose **True**.

   (h) Select **Auto Update Statistics asynchronously** and choose **False**.

   (i) Click **OK**.

4. Create a new login:

   (a) In the **Object Explorer** pane, expand **Security**.

   (b) Right-click **Logins**, then click **New Login...**.

   (c) On the **General** page, type the **Login name**.

   (d) Select:

   - **SQL Server Authentication**

     Type and confirm the password for the new login. Deselect the **User must change password at next login** and **Enforce password expiration** checkboxes.

     Or

   - **Windows authentication**

     Pick a local or domain account or group.

   (e) Set **Default database** to the database that you created in step 3.

   (f) Click **OK**.

5. Create a new schema in the database:

   (a) In the **Object Explorer** pane expand **Databases** → **<*New database*>** → **Security**.

   Where <*New database*> is the database that you created in step 3.

   (b) Right-click **Schemas**, then click **New Schema...**.

   (c) Type the **Schema name**.

(d) Click **OK**.

6. Set the user in the database:

   (a) In the **Object Explorer** pane, expand **Databases** → **<*New database*>** → **Security**.

   Where <*New database*> is the database that you created in step 3.

   (b) Right-click **Users**, then click **New User...**

   (c) Type the **User name**.

   (d) Set the **Login name** to the user you created in step 4.

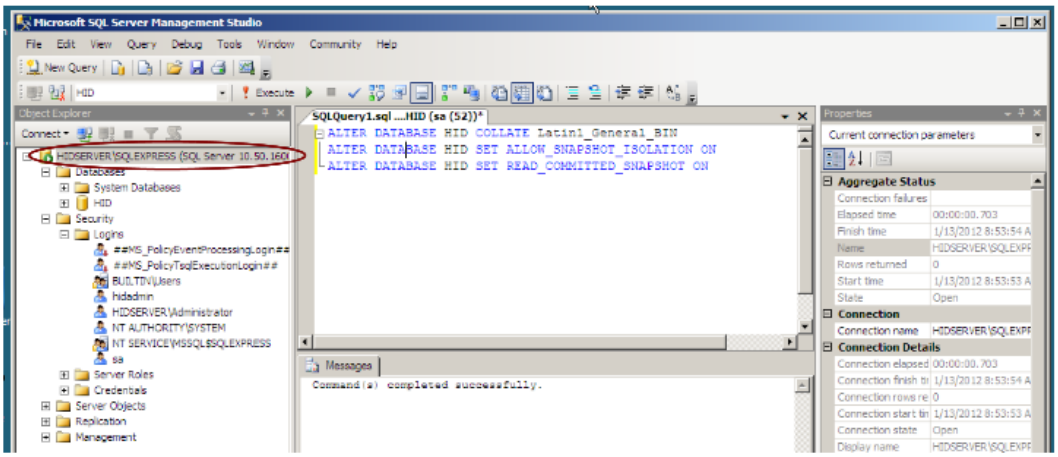
   (e) Set the **Default schema** to the schema you created in step 5.

   (f) In the **Database role membership** area, enable:

   - db_datareader
   - db_datawriter
   - db_ddladmin
   - db_owner

   (g) Click **OK**.

7. Close the connection to the schema by collapsing the database tree and highlighting the root of the SQL Server management interface.



This ensures that the database can be locked to perform the following operation.

8. Alter the database collation:

   (a) In the toolbar, click **New Query**.

   (b) In the new query window, type the following:

```
ALTER DATABASE <database name> SET SINGLE_USER WITH ROLLBACK IMMEDIATE
ALTER DATABASE <database name> COLLATE Latin1_General_BIN
ALTER DATABASE <database name> SET ALLOW_SNAPSHOT_ISOLATION ON
ALTER DATABASE <database name> SET READ_COMMITTED_SNAPSHOT ON
ALTER DATABASE <database name> SET MULTI_USER
```


Note: If the database name is "default", enclose it in square brackets: `[default]`.

Click **Execute**.

9. Exit SQL Server Management Studio.

Note the database name, and the name and password of the login that you create. You will need these values, as well as the information you gathered earlier, when you install *Bravura Security Fabric*.

5.6 Creating a dedicated report database user and schema

The *Analytics* app requires a dedicated report database user and schema.

You can allow *Hitachi ID Bravura Security Fabric* **`setup`** to do this for you, as described in the *Bravura Security Fabric* Documentation , or use the following instructions to set up the user and schema yourself.

To create the report user and schema and configure permissions:

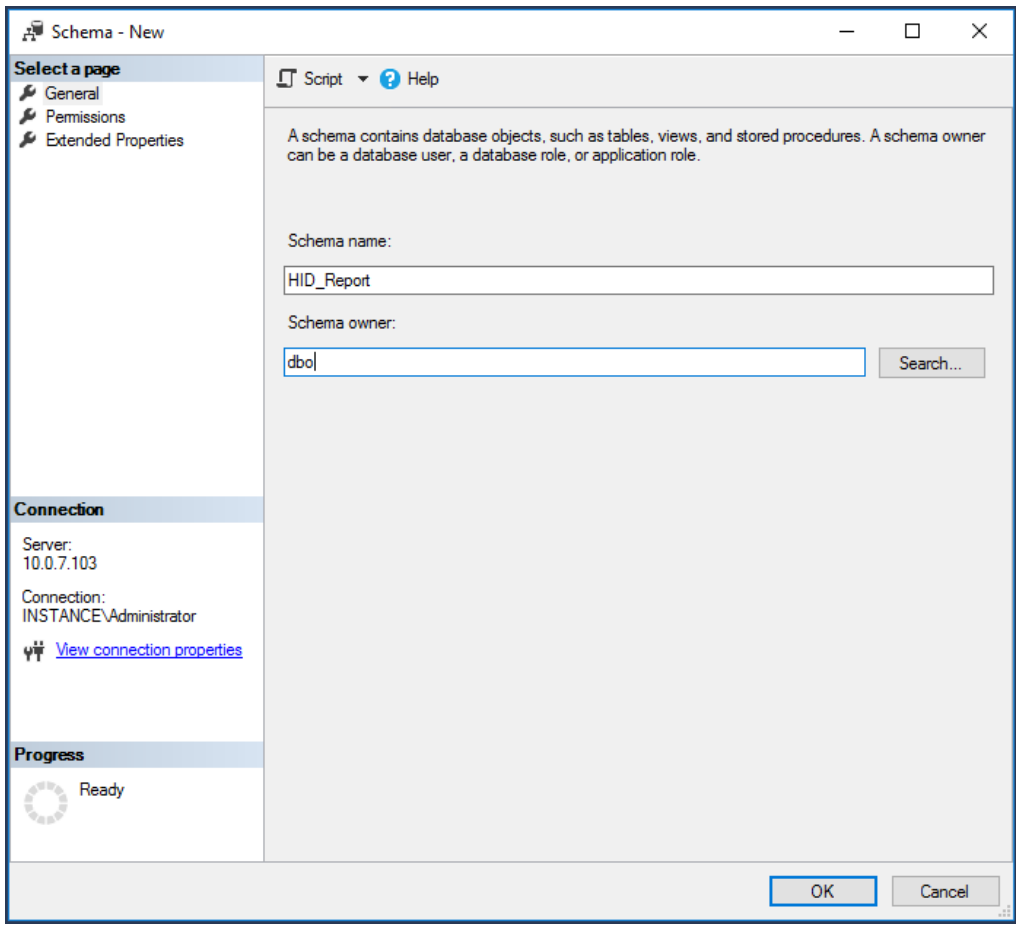
1. Start Microsoft SQL Server Management Studio.
2. Connect to the server as a system administrator (sysadmin role).

   You can do this using SQL Server authentication and the sa account, or using Windows authentication if the Windows user has the sysadmin role.

   For example, to connect to the server using the sa account, set:

   Server type to "Database Engine"
   Server name <*host name or IP address*>\<*instance*>
   Authentication to "SQL Server authentication"
   Login to `sa`
   Password to <*password for sa*>

   Click **Connect**.
3. Create a new schema in the database:
   (a) In the **Object Explorer** pane expand **Databases** → **<instance database>** → **Security**.
   (b) Right-click **Schemas**, then click **New Schema...**.
   (c) Type the **Schema name**.
   (d) Set the Schema owner to `dbo`.



(e) Click **OK**.

4. Create a new login:

   (a) In the **Object Explorer** pane, expand **Security**.

   (b) Right-click **Logins**, then click **New Login...**.

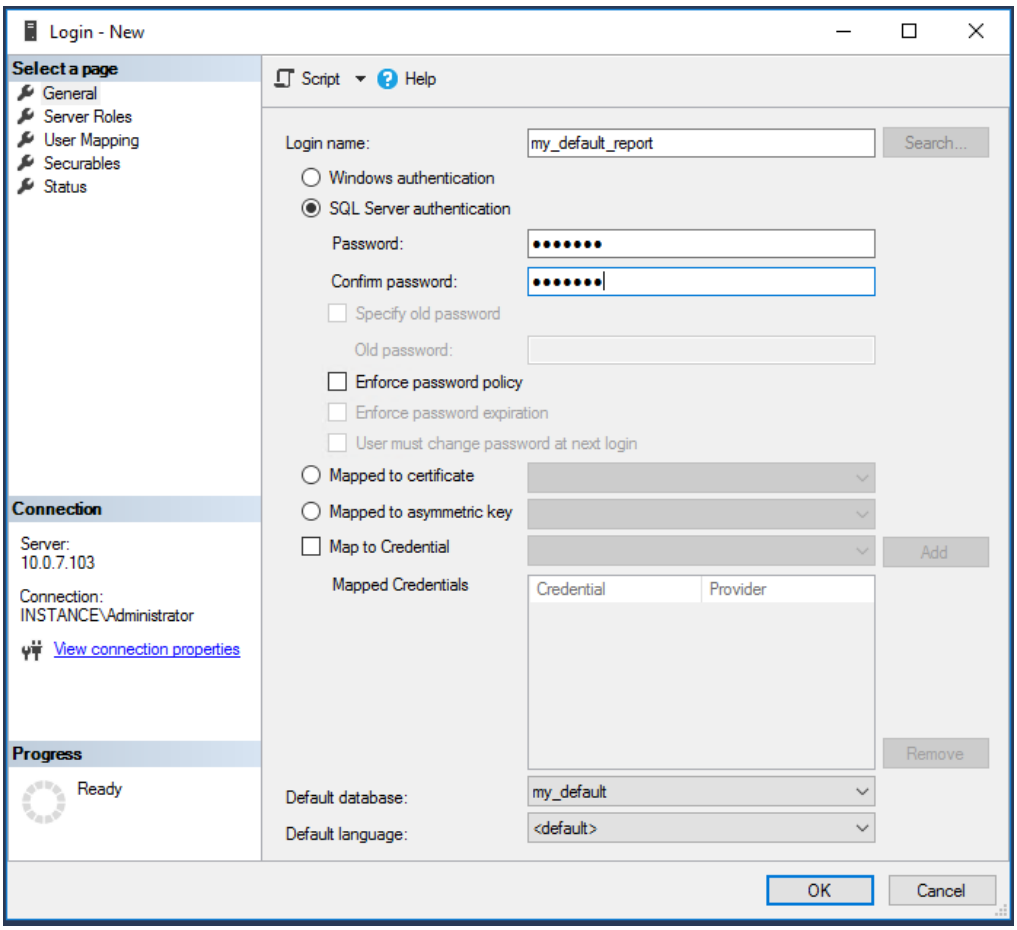
   (c) On the **General** page, type the **Login name**.

   (d) Select **SQL Server Authentication**.

   (e) Type and confirm the password for the new login.

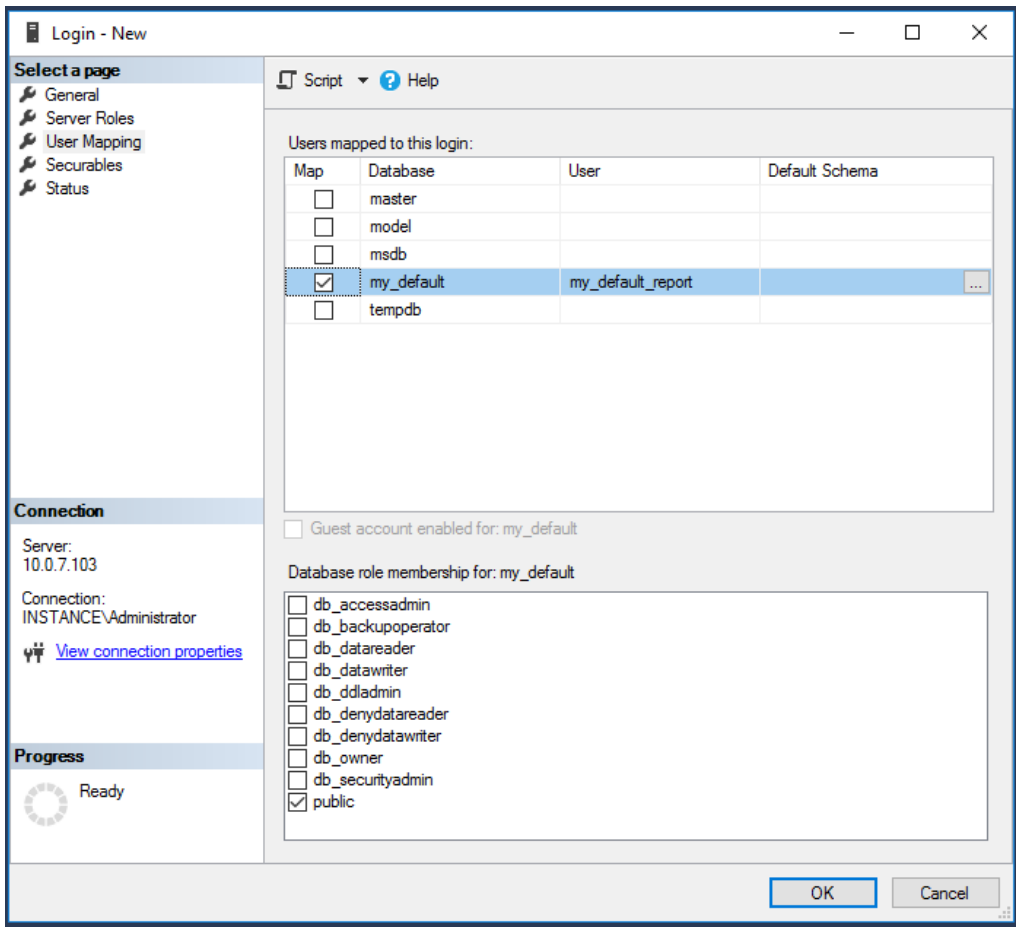
   (f) Deselect the **User must change password at next login** and **Enforce password expiration** checkboxes.

   (g) Set **Default database** to the instance database created either in a previous install or in step 3.



(h) Click **User Mapping** on the left.

(i) Map the <instance database> to this new user and set the default schema to the schema created in the previous step.



(j) Click **OK**.

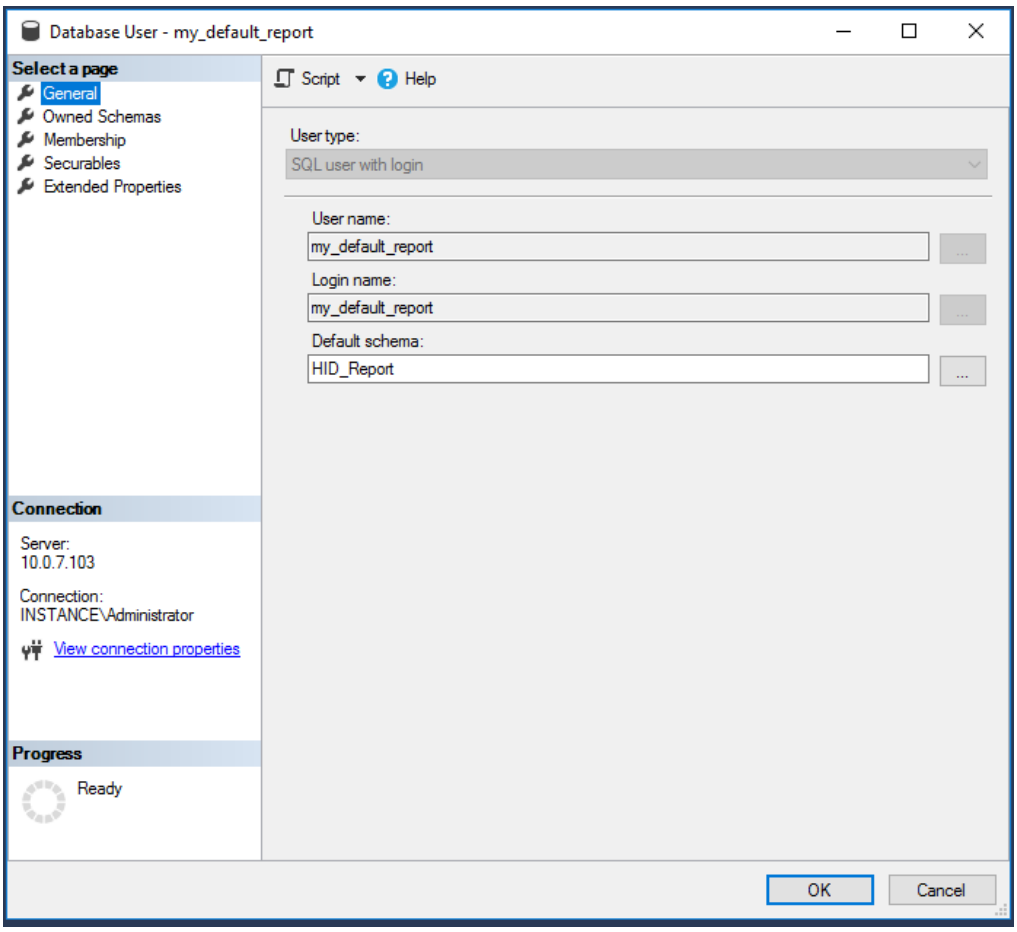
5. Set the user in the database:

   (a) In the **Object Explorer** pane, expand **Databases** → **<instance database** → **Security** → **Users**.

   (b) Right-click the user created in 4 and click **Properties**.

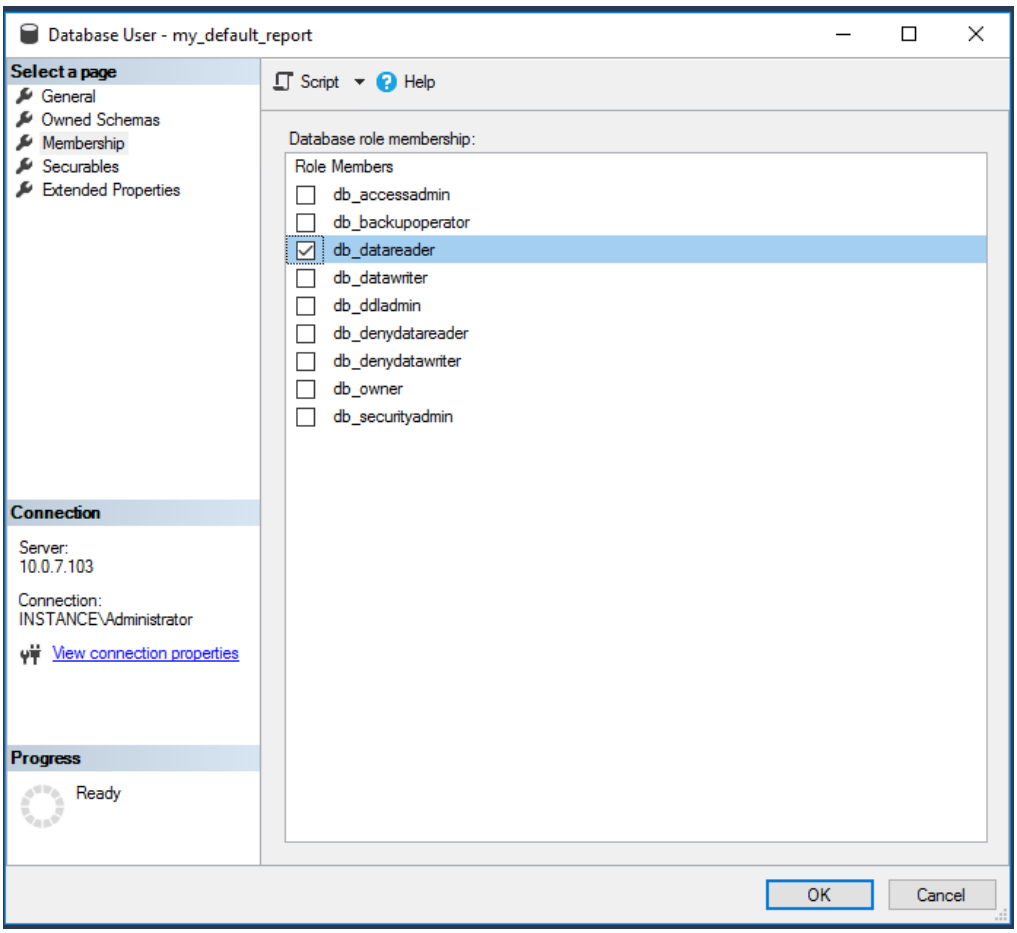
   (c) Click **General** on the left.

   (d) Set the **Default schema** to the schema you created in step 3.



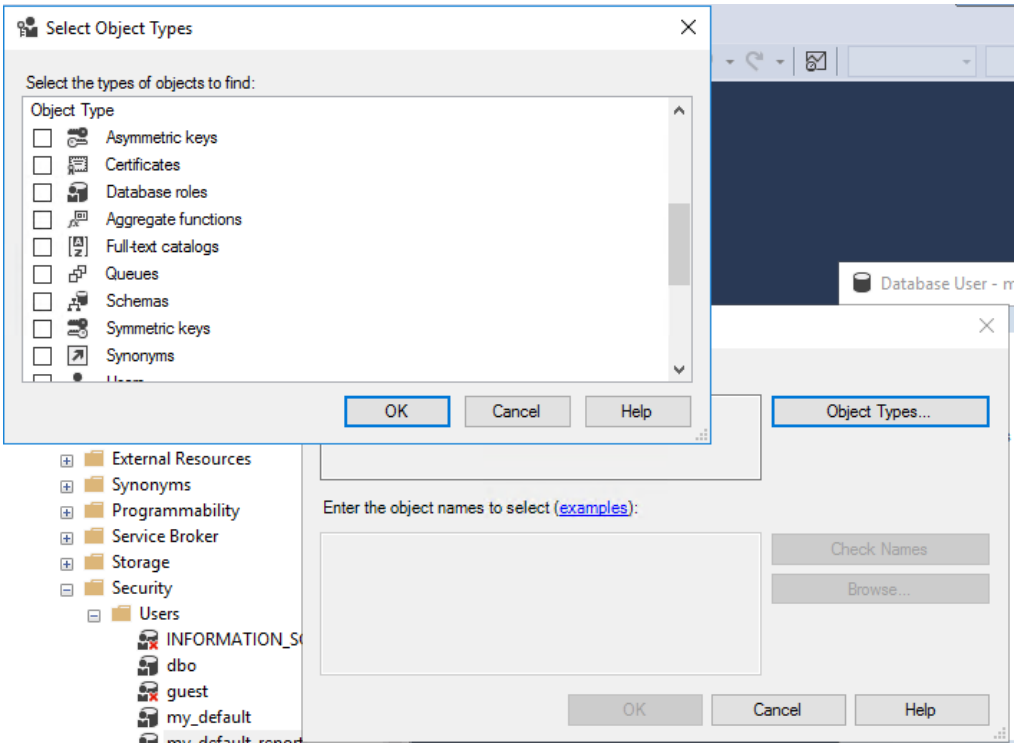
(e) In the **Membership** area, enable:

- db_datareader



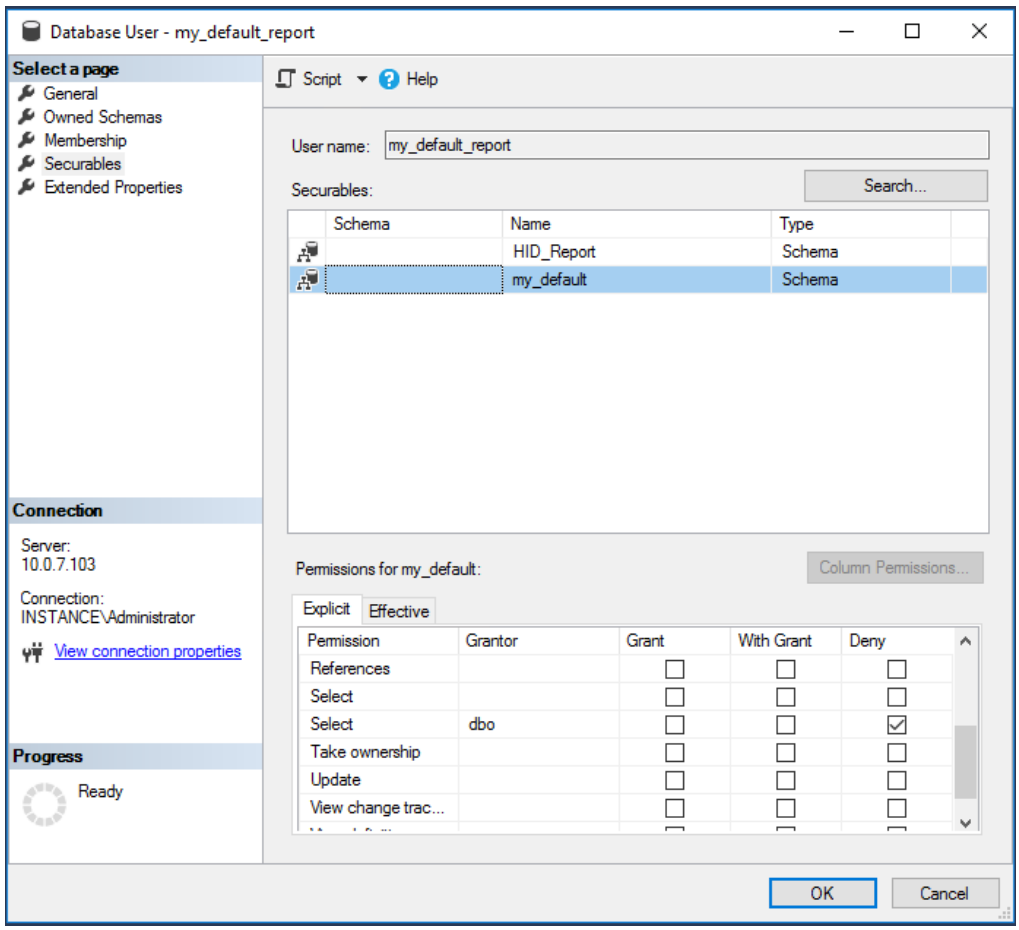
(f) Click **Securables** on the left.

(g) Search and select Schema object types.



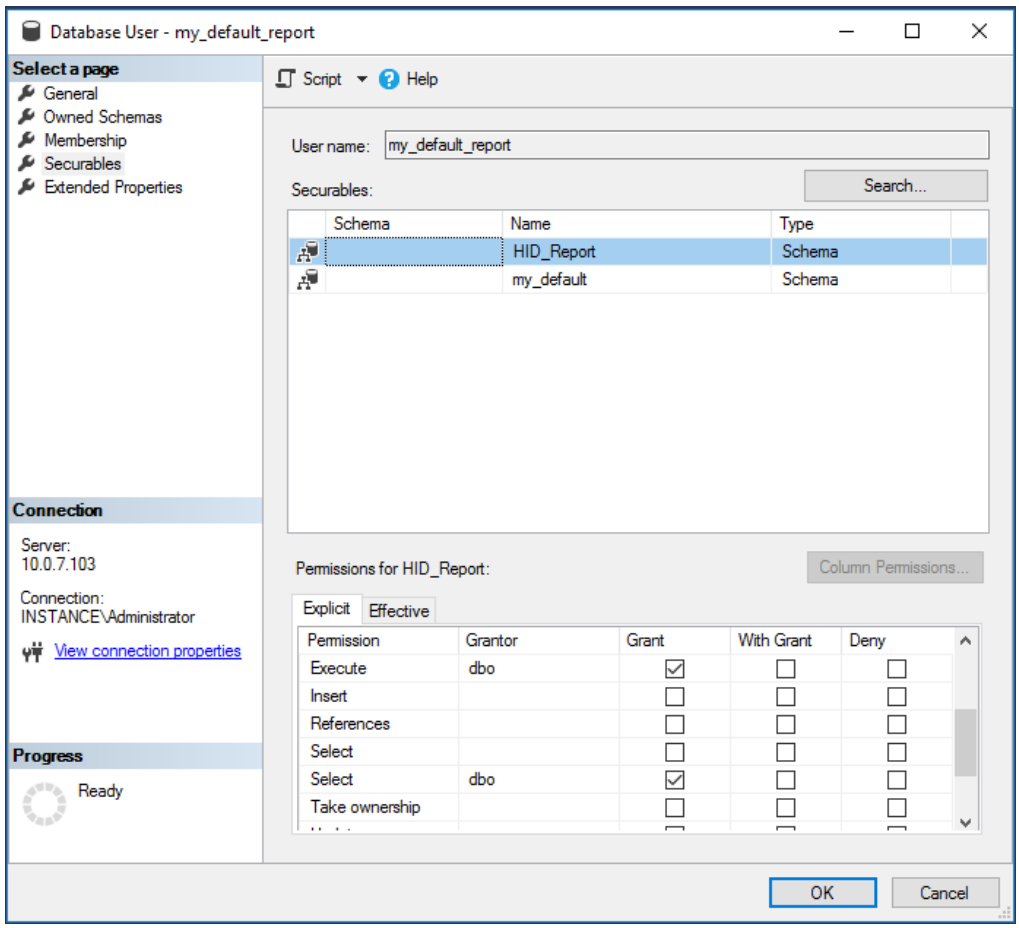
(h) Select the instance databases' schema.

(i) Deny this user access to the instance databases' schema.



(j) Search and select the report schema you created in step 3.

(k) Grant Execute and Select permissions.



(l) Click **OK**.

5.7 Removing public/guest permissions

By default, in SQL Server, most objects have public permissions granted. If you remove the default public and guest permissions from your database, for example in SQL server 2012 and after, you must ensure the following steps are performed to ensure *Hitachi ID Bravura Security Fabric* operates correctly:

1. Start Microsoft SQL Server Management Studio.
2. Connect to the server as a system administrator (sysadmin role).

   For example, to connect to the server using the sa account, set:

   Server type to **Database Engine**
   Server name *<host name or IP address>\<instance>*
   Authentication to **SQL Server Authentication**
   Login to `sa`
   Password to *<password for sa>*

then click **Connect**.

3. Create a new user:

   (a) In the **Object Explorer** (left) pane, expand **Databases** → **System Databases** → **master** → **Security**, right-click **Users**, then select **New User...**.

   (b) Type the **User name**.

   (c) Select **Login name** created in previous section (p7).

   (d) Select **Default schema** (for example, **`sys`**).

   (e) Select **Securables** to search and grant select permission on schemas sys and INFORMATION_SCHEMA.

   (f) Click **OK**.

4. Create a new database role for **`sp_describe_first_result_set`**:

   (a) In the **Object Explorer** (left) pane, expand **Databases** → **System Databases** → **master** → **Security** → **Roles**, right-click **Database Roles**, then select **New Database Role...**.

   (b) Type the **Role name**.

   (c) Add user created in previous step to **Role Members**.

   (d) Select **Securables** page, and click **Search**.

   (e) Select **`sp_describe_first_result_set`** (Extended Stored Procedures).

   (f) Grant **Execute** permission, and click **OK**.

5. Repeat last step to create a new database role for **`sp_executesql`**.

6. For upgrade or migration, repeat to create a new database role for **`sp_rename`**.

7. For upgrade or migration, ensure your login user can connect:

   (a) In the **Object Explorer** (left) pane, expand **Security** → **Logins**, and select your login user.

   (b) Select **Securables** page, and click **Search**.

   (c) Select your server.

   (d) Under the `Permissions for <server>` check the following permissions:

   - Connect SQL
   - Control server
   - Create any database
   - Create availability group
   - Create DDL event notification
   - Create endpoint

- Create server role
- Create trace event notification
- External access assembly
- View any definition
- View server state

(e) Click **OK**.

Advanced configuration

If you require that the dedicated user works with fewer permissions, you can do one of the following:

- Modify installation options so that *Hitachi ID Bravura Security Fabric* installs to a named schema owned by a different user.

  The "schema install user" requires all of the roles described in the above procedure.
- Modify installation options so that *Bravura Security Fabric* does not install the schema, and instead uses a schema already set up by your database administrator.
- Remove extra permissions from the dedicated user after *Bravura Security Fabric* is installed.

In the above cases, the dedicated user requires at least the db_datareader and db_datawriter database roles, as well as permissions to the schema objects. This includes: EXECUTE permission on the stored procedures, VIEW DEFINITION permission on the stored procedures and views. To learn how to grant permissions to schema objects, contact your database administrator or refer to your database documentation.

5.8 Working with multiple installations

Instances

If you are installing multiple *Hitachi ID Bravura Security Fabric* instances, ensure that you create and use a separate database and user for each instance.

Database replication

If you will be using *Hitachi ID Bravura Security Fabric* database replication, ensure that you create and use a separate database and user for each replicated server installation.

Schema

During installation, you can modify options so that *Hitachi ID Bravura Security Fabric* does not install the schema, if:

- The schema is set up by your database administrator ahead of time.

  In this configuration, you must set up database replication between instances.

- The schema is shared from a previous installation.

  This means both instances work against the same schema and no database replication is required between them.

5.9 Modifying database connection details

If a change has been made to the database server credentials, (database server name, database name, database server user ID, or database server user password) use the **`iddbadm`** program to update the database information.

See iddbadm in the Bravura Security Fabric *Reference Manual* for more information.

5.10 Required database maintenance

The auto discovery process replaces the entire data in some large tables whenever it is scheduled; that can lead to very large transaction and/or temp files showing up overnight.

The data, transaction and log file locations of every *Hitachi ID Bravura Security Fabric* node's backend database have to be monitored so they don't run out of space:

- If the database engine is configured to clean up, the files could be much smaller when inspected after the clean-up.
- Ensure that you have at least 50% free space on the drives, shares or SAN's that host those files. This ensures that the database always has enough space to function as expected. Hitachi ID Systems recommends at least 500gb of hard drive storage for a *Bravura Security Fabric* server.

Do not schedule database maintenance, clean-up procedures or table reindexing at the time auto discovery, automated user administration (**`idtrack`**), automatic resource assignment (**`autores`**) or other long, database-intensive *Bravura Security Fabric* processes are scheduled.

- If database maintenance lasts more than a few minutes, schedule the *Bravura Security Fabric* nodes that use that database to be taken out of the load balancer.
- It is a good idea to perform maintenance (for example OS upgrades) on the *Bravura Security Fabric* node itself at the same time as it is done on its database (if so, take down the *Bravura Security Fabric* node before the database one, and bring up the database before the *Bravura Security Fabric*)

In case *Bravura Security Fabric*'s stored procedures fail for any reason, the date/time stamp, sproc name, its arguments, and the failure reason will be recorded in the *Bravura Security Fabric* instance's db\iddb-failed-procs-*.log files; for example:

- These log files are created whenever a new node is added. The failure logs for receive and send queues are created as empty (0 bytes) files. They are created by the Database Service (iddb) and data is appended to them by the Database Service.
- These log files are not rotated with the rest of the *Bravura Security Fabric* logs: they are there for maintenance, and if non-empty, they must be read by an administrator who will decide if corrective action is needed (when an unfamiliar sproc fails, open an issue with support@Hitachi-ID.com to determine if action is needed).
- Some sproc failures are benign; for example, an error in updating an account during auto discovery could well be made obsolete by the next auto discovery.
- Hitachi ID Systems recommends that the content of those files be emptied as soon as the reason for failure is solved, but that content should be kept elsewhere (outside the *Bravura Security Fabric* instance folder), in case later troubleshooting sessions require them.

5.11 Troubleshooting

Errors

If you experience errors, verify that:

- You can connect to SQL Server using the login that you created.

  You can verify the connection using the SQL Server Command Line Tool.

  If the login uses SQL Server authentication:

  ```
  sqlcmd.exe -S <server name>\<instance> -U <login ID> -P <password>
  ```

  If the login uses Windows authentication, and the current Windows user is the same as the SQL Server login:

  ```
  sqlcmd.exe -S <server name>\<instance>
  ```

- Your system meets the recommended installation requirements.

  For example, 1 GB RAM is recommended (512 MB is the minimum) for Microsoft SQL Server .

If you continue to experience errors with Microsoft SQL Server :

- Ensure that the server is set up to allow remote connections.

- If you are connecting to a named instance, try specifying the TCP port number along with the server and instance name: `<server name>\<instance>,<port>`.

  For example, using sqlcmd.exe:

  ```
  sqlcmd.exe -S sqlserver\mycorp2,1433 -U sa -P letmein!
  ```

If you continue to experience errors with Microsoft SQL Server 2008 Express Edition with Advanced Services, try the following:

1. Start the SQL Server Configuration Manager (**Start** → **All Programs** → **Microsoft SQL Server 2008** → **Configuration Tools**)
2. Select **SQL Server Network Configuration** → **Protocols for <*SQL Server instance*>** and enable Shared Memory, TCP/IP, and Named Pipes protocols.
3. Select **SQL Native Client Configuration** → **Client Protocols** and enable protocols with the following order:

Name	Order
Shared Memory	1
TCP/IP	2
Named Pipes	3

4. Restart the server to apply your settings.

Services

Under certain circumstances, *Hitachi ID Bravura Security Fabric* services may fail to start after a server reboot. This problem may occur if the database is unavailable, or the database services and/or other dependent services have not started completely when the *Bravura Security Fabric* services attempt to start. There are two methods for resolving this problem.

Method 1:

Manually start the services

If *Hitachi ID Bravura Security Fabric* services fail to start, you can manually start all required services. To do this:

1. Before you begin, ensure the database is available.
2. Log on to the affected server.
3. On the **Start** menu, click **Run**, type `services.msc`, Click **OK**.
4. In the results pane, find the **Hitachi ID Logging Service**.
5. Right-click the service, then select **Restart**.
6. In the results pane, find the **Hitachi ID Database Service**.

7. Right-click the **Service**, then select **Start**.
8. Repeat steps 6 and 7 for all Hitachi ID services that did not start.

Method 2:

Set *Hitachi ID Bravura Security Fabric* services to Automatic (Delayed Start)

To ensure that the database and all required services have started completely before the *Bravura Security Fabric* services have started, you can set them to **Automatic (Delayed Start)**. To do this:

1. Log on to the affected server.
2. On the **Start** menu, click **Run**, type `services.msc`, Click **OK**.
3. In the results pane, find the Hitachi ID services.
4. Right-click the service, then select **Properties. . .** .
5. Change the **Startup Type** to **Automatic (Delayed Start)**.
6. Click **Apply**, then click **OK**.
7. Repeat steps 4-6 for all Hitachi ID services that are installed.
8. Restart the server.