Installation

Quick Start Guide

Software revision:	12.2.4
Document revision:	30072
Last changed:	2022-03-01

Contents

Database and Database Client Software 1

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*.

1.1 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”.

1.2 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.

1.3 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).

1.3.1 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 (p5).
3. *Optional:* Create a dedicated database, user, and schema (p6). You can allow *Bravura Security Fabric* **`setup`** to do this for you, as described in Using setup to create a new dedicated database user.

4. *Optional:* Create a dedicated report database user (p9). You can allow *Bravura Security Fabric* `setup` to do this for you, as described in SSRS settings.

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.

1.3.2 Installing Microsoft SQL Server

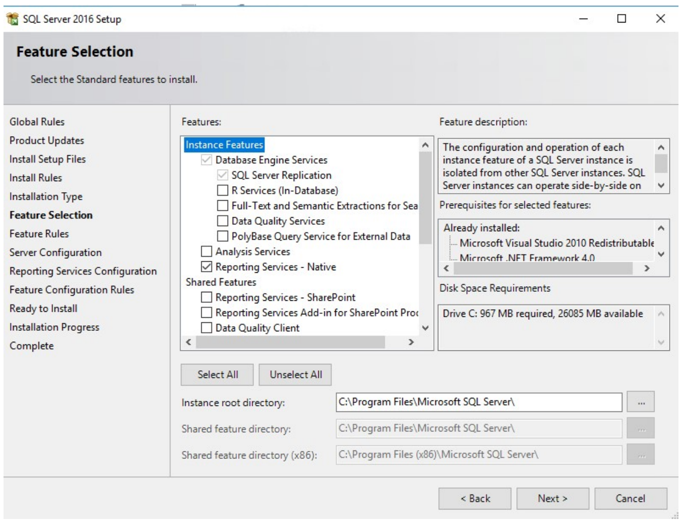
It is recommended that you install Microsoft SQL Server on Windows Server 2012 R2, 2016 or 2019.

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



SQL Server 2016 Setup

Feature Selection

Select the Standard features to install.

Global Rules
Product Updates
Install Setup Files
Install Rules
Installation Type
Feature Selection
Feature Rules
Server Configuration
Reporting Services Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete

Features:

Instance Features
- ☑ Database Engine Services
  - ☑ SQL Server Replication
  - ☐ R Services (In-Database)
  - ☐ Full-Text and Semantic Extractions for Sea
  - ☐ Data Quality Services
  - ☐ PolyBase Query Service for External Data
- ☐ Analysis Services
- ☑ Reporting Services - Native

Shared Features
- ☐ Reporting Services - SharePoint
- ☐ Reporting Services Add-in for SharePoint Proc
- ☐ Data Quality Client

Feature description:

The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL Server instances can operate side-by-side on

Prerequisites for selected features:

Already installed:
- Microsoft Visual Studio 2010 Redistributable
- Microsoft .NET Framework 4.0

Disk Space Requirements

Drive C: 967 MB required, 26085 MB available

Instance root directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

   - **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 (p5).
- If you decide to install SQL Server Reporting Services after installing SQL Server, complete SSRS post-installation steps (p6).

1.3.3 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`.

1.3.4 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.

1.3.5 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 Using setup to create a new dedicated database user, 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.

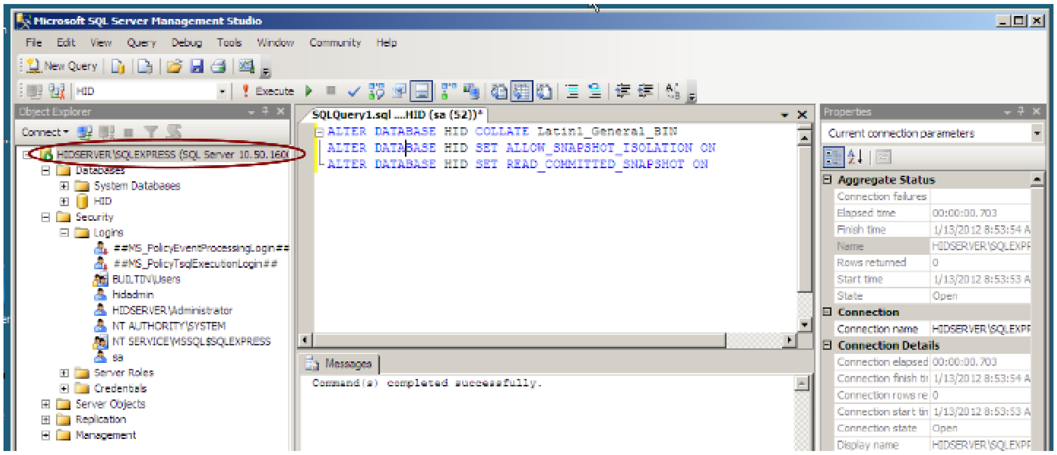
   (e) Set the **Default schema** to the schema you created in step 5.

   (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.


Microsoft SQL Server Management Studio
File Edit View Query Debug Tools Window Community Help
New Query
HID
Execute
Object Explorer
Connect
HIDSERVER\SQLEXPRESS (SQL Server 10.50.160
Databases
System Databases
HID
Security
Logins
##MS_PolicyEventProcessingLogin##
##MS_PolicyTsqlExecutionLogin##
BUILTIN\Users
hidadmin
HIDSERVER\Administrator
NT AUTHORITY\SYSTEM
NT SERVICE\MSSQL$SQLEXPRESS
sa
Server Roles
Credentials
Server Objects
Replication
Management
SQLQuery1.sql ....HID (sa (52))*
Messages
Properties
Current connection parameters

```
ALTER DATABASE HID COLLATE Latin1_General_BIN
ALTER DATABASE HID SET ALLOW_SNAPSHOT_ISOLATION ON
ALTER DATABASE HID SET READ_COMMITTED_SNAPSHOT ON
```

```
Command(s) completed successfully.
```

Aggregate Status	
Connection failures	
Elapsed time	00:00:00.703
Finish time	1/13/2012 8:53:54 A
Name	HIDSERVER\SQLEXPI
Rows returned	0
Start time	1/13/2012 8:53:53 A
State	Open
Connection	
Connection name	HIDSERVER\SQLEXPI
Connection Details	
Connection elapsed	00:00:00.703
Connection finish ti	1/13/2012 8:53:54 A
Connection rows re	0
Connection start tin	1/13/2012 8:53:53 A
Connection state	Open
Display name	HIDSERVER\SQLEXPI

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*.

See also:

- Advanced configuration for advanced configuration options.
- Working with multiple installations for information about working with multiple installations.
- Troubleshooting for troubleshooting tips.

1.3.6 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 SSRS settings, 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>*

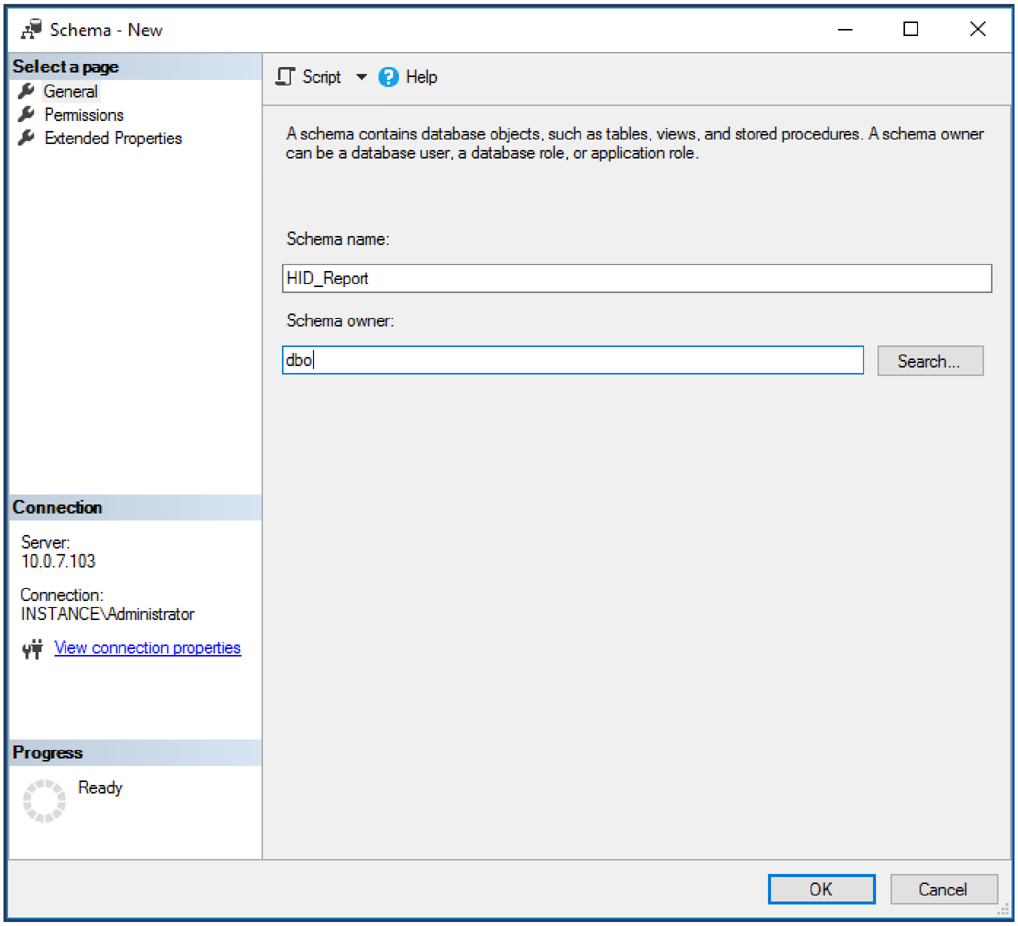
   Click **Connect**.
3. Create a new schema in the database:

   (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`.



A schema contains database objects, such as tables, views, and stored procedures. A schema owner can be a database user, a database role, or application role.

Schema name: HID_Report

Schema owner: dbo

Server:
10.0.7.103

Connection:
INSTANCE\Administrator

(e) Click **OK**.

4. Create a new login:

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

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

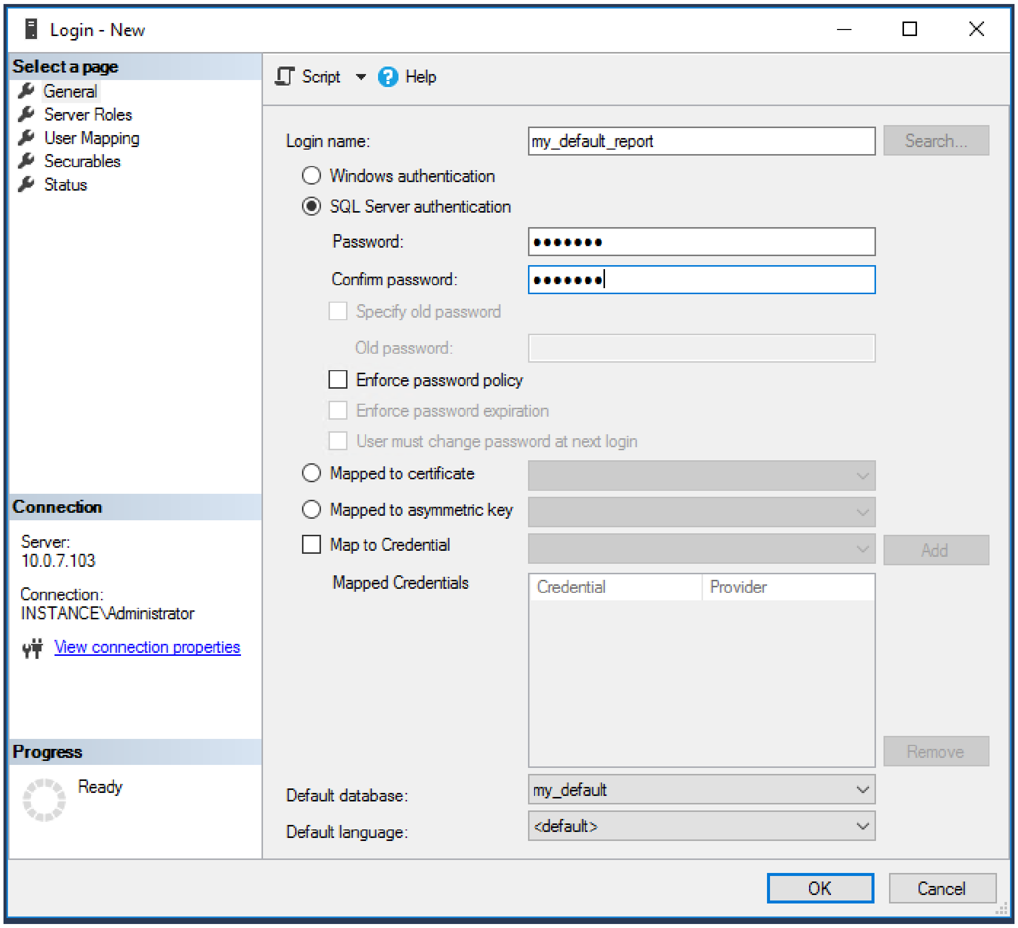
   (c) On the **General** page, type the **Login name**.

   (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.



Login - New

Login name: my_default_report

○ Windows authentication

● SQL Server authentication

Password: •••••••

Confirm password: •••••••

□ Specify old password

Old password:

□ Enforce password policy

□ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Mapped Credentials

Credential	Provider

Default database: my_default

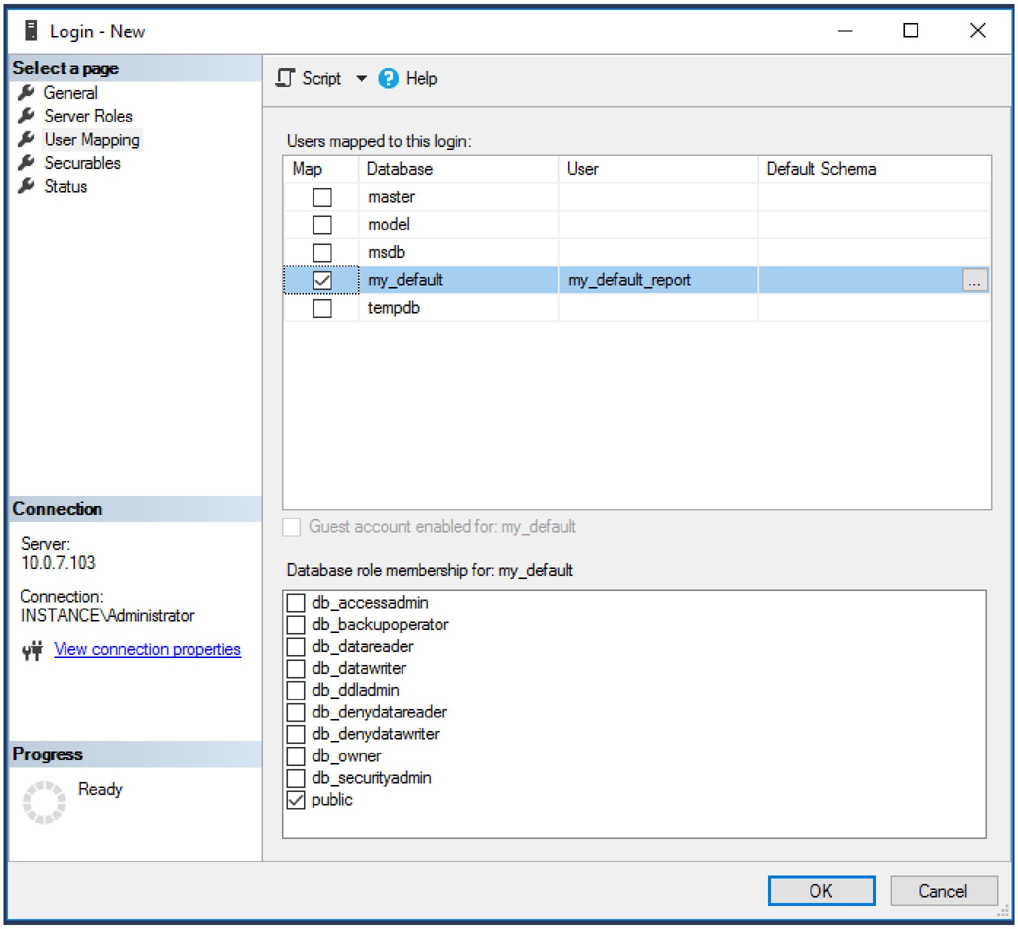
Default language: <default>

Server:
10.0.7.103

Connection:
INSTANCE\Administrator

(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.



Users mapped to this login:

Map	Database	User	Default Schema
☐	master		
☐	model		
☐	msdb		
☑	my_default	my_default_report	...
☐	tempdb		

☐ Guest account enabled for: my_default

Database role membership for: my_default

☐ db_accessadmin
☐ db_backupoperator
☐ db_datareader
☐ db_datawriter
☐ db_ddladmin
☐ db_denydatareader
☐ db_denydatawriter
☐ db_owner
☐ db_securityadmin
☑ public

Server:
10.0.7.103

Connection:
INSTANCE\Administrator

View connection properties

Ready

(j) Click **OK**.

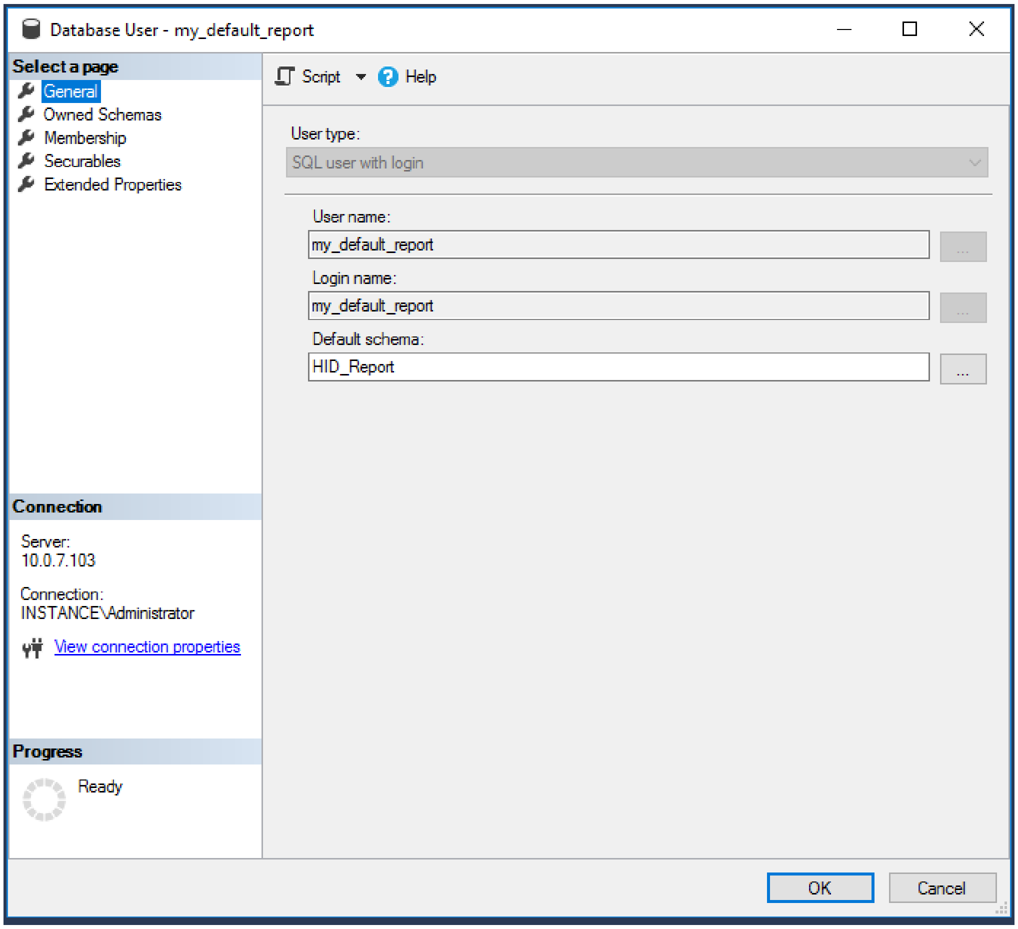
5. Set the user in the database:

   (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.



User type: SQL user with login

User name: my_default_report

Login name: my_default_report

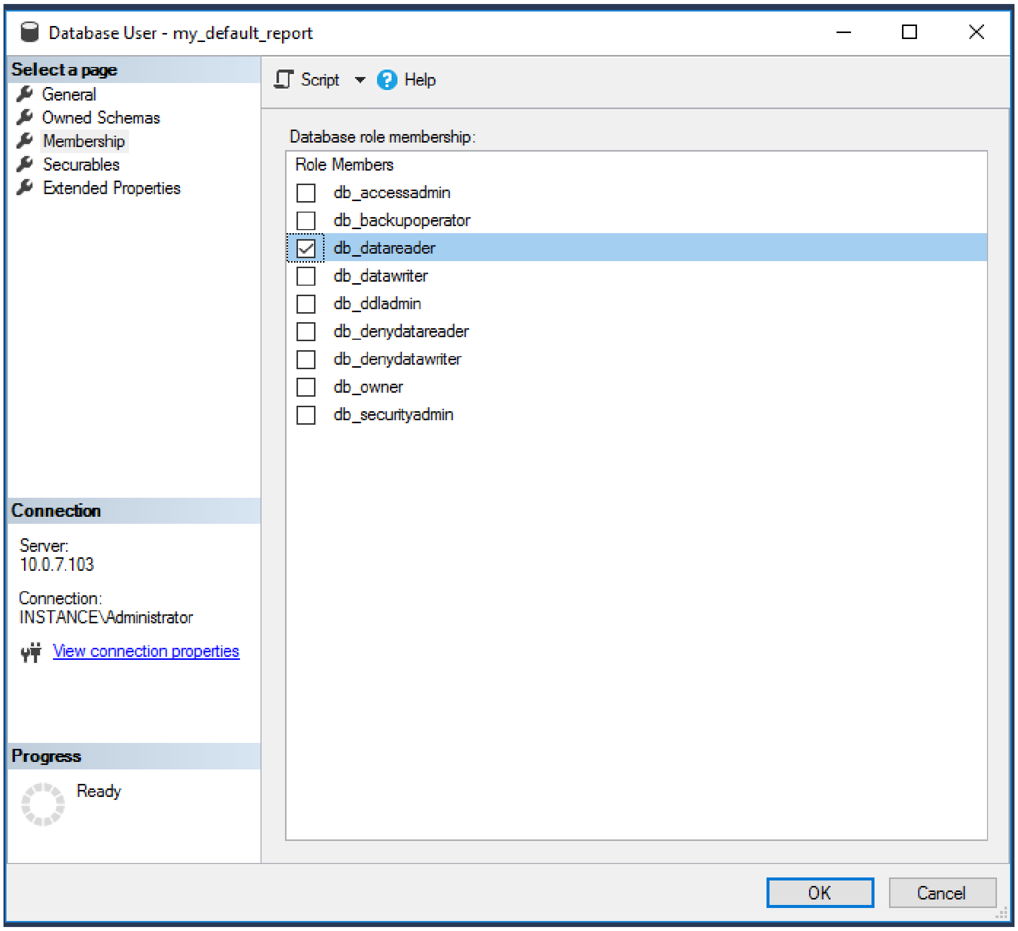
Default schema: HID_Report

Server: 10.0.7.103

Connection: INSTANCE\Administrator

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

- db_datareader



Database role membership:

Role Members

☐ db_accessadmin
☐ db_backupoperator
☑ db_datareader
☐ db_datawriter
☐ db_ddladmin
☐ db_denydatareader
☐ db_denydatawriter
☐ db_owner
☐ db_securityadmin

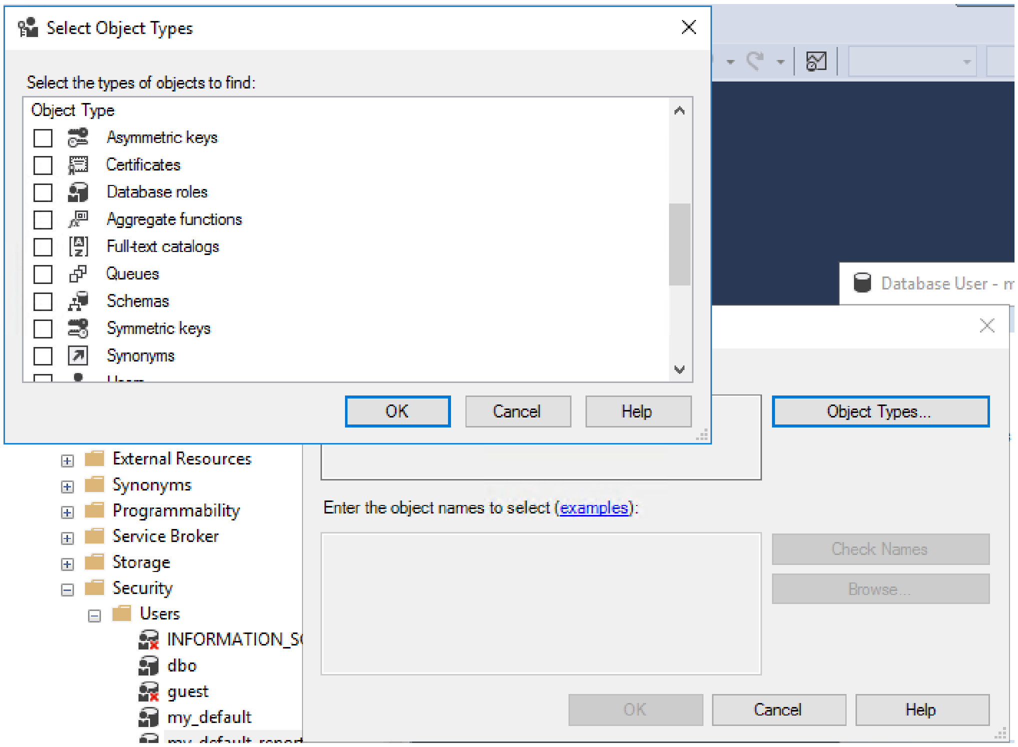
Server:
10.0.7.103

Connection:
INSTANCE\Administrator

Ready

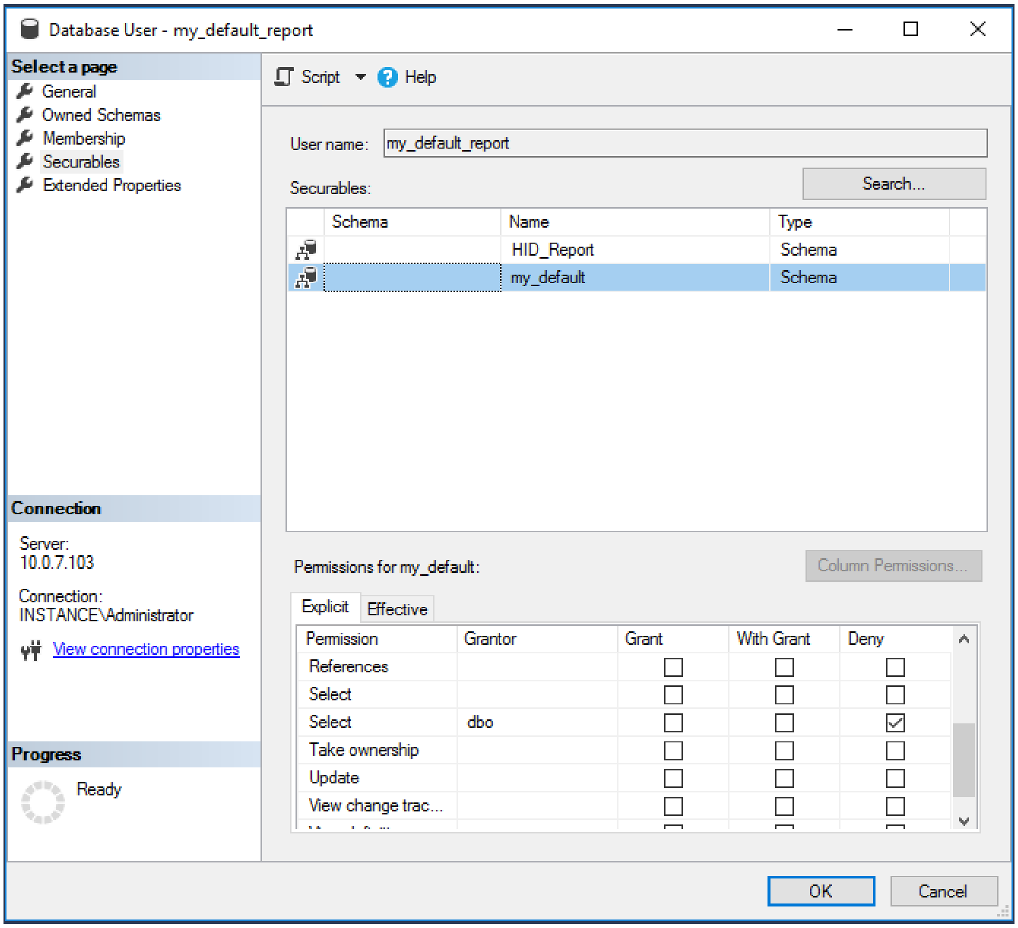
(f) Click **Securables** on the left.

(g) Search and select Schema object types.



(h) Select the instance databases' schema.

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



User name: my_default_report

Securables:

Schema	Name	Type
	HID_Report	Schema
	my_default	Schema

Server:
10.0.7.103

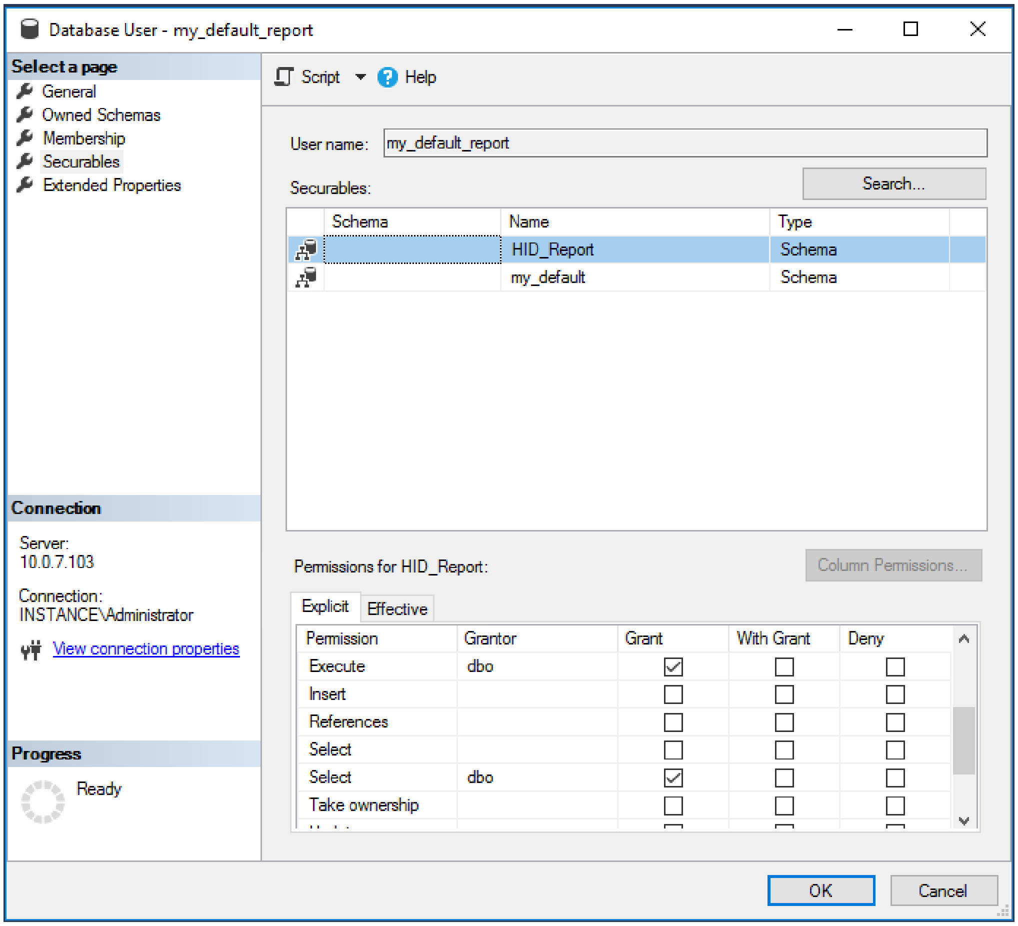
Connection:
INSTANCE\Administrator

Permissions for my_default:

Permission	Grantor	Grant	With Grant	Deny
References		□	□	□
Select		□	□	□
Select	dbo	□	□	☑
Take ownership		□	□	□
Update		□	□	□
View change trac...		□	□	□

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

(k) Grant Execute and Select permissions.



Connection

Server:
10.0.7.103

Connection:
INSTANCE\Administrator

Progress

Ready

User name: my_default_report

Securables:

Schema	Name	Type
	HID_Report	Schema
	my_default	Schema

Permissions for HID_Report:

Permission	Grantor	Grant	With Grant	Deny
Execute	dbo	☑	□	□
Insert		□	□	□
References		□	□	□
Select		□	□	□
Select	dbo	☑	□	□
Take ownership		□	□	□

(l) Click **OK**.

1.3.7 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 (p6).

   (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**.

Connector Pack 2

This chapter describes system requirements and steps for installing *Hitachi ID Connector Pack*.

2.1 Requirements

- Windows Server 2019, 2016, or 2012 Standard R2
- Python 3.7.3+

> **Note:** Python 3.8.x or later is not currently supported.

> **Note:** Ensure that Python is installed for all users. 3.7.3+ installs in the context of the current user by default. You must choose to do a custom install, then select "all users" when the selection becomes available. This will allow the *Bravura Security Fabric* service user (psadmin) account to have appropriate access to the Python installation.

> **Note:** It is recommended to add Python to the system PATH. This may also be added by selecting the option for "Add Python 3.7 to PATH" during the Python installation.

2.2 Installing the global *Connector Pack*

This chapter shows you how to install a global connector pack for use with *Bravura Security Fabric*, for demonstration or testing purposes. When planning a major deployment, it is **strongly** recommended that you read the planning and setup chapters of the Connector Pack Integration Guide. The Connector Pack Integration Guide also explains the difference between a global and instance-specific *Hitachi ID Connector Pack*.

The global *Connector Pack* is useful if you have multiple instances of the *Bravura Security Fabric* installed on a server, and you want them all to use the same group of connectors.

CAUTION: If a server is hosting multiple proxy instances of *Bravura Security Fabric*, it is recommended that you do *not* install the global *Connector Pack*. The multiple instances may use different versions of the *Connector Pack*. Unexpected results may occur when the proxies try to synch their connectors with the master servers.

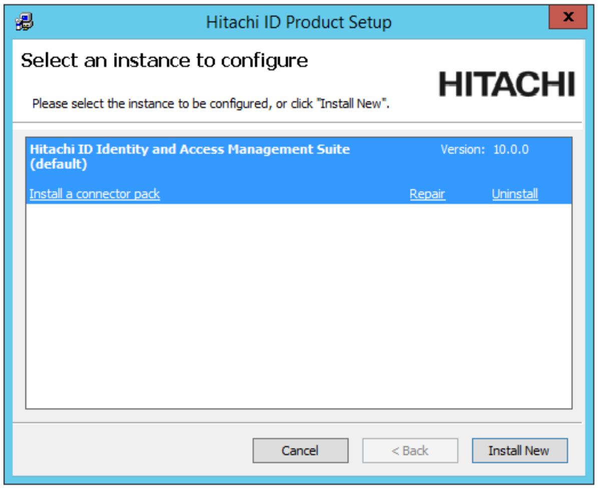
The *Connector Pack* is installed using the **`setup`** file distributed with the **`connector-pack-x64.msi`**.

Note: It is best practice to **not** install the *Connector Pack* or other software on the system (C:\) drive.

To install a global *Connector Pack*:

1. Log into the host Windows server as a member of the Administrators group.
2. Run **`setup`** from the main software installation package.

   The **`setup`** program displays the ***Select an instance to configure*** page.



Hitachi ID Product Setup

Select an instance to configure

Please select the instance to be configured, or click "Install New".

HITACHI

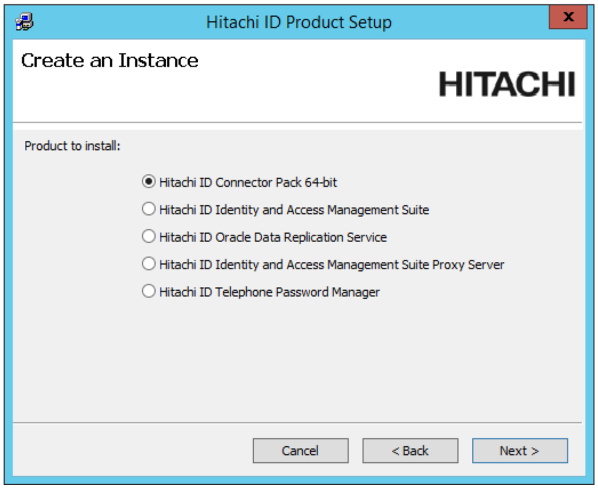
Hitachi ID Identity and Access Management Suite (default) Version: 10.0.0

Install a connector pack Repair Uninstall

Cancel < Back Install New

3. Click **Install New**.

   The **`setup`** program displays the ***Create an instance*** page.



Hitachi ID Product Setup

Create an Instance

Product to install:

● Hitachi ID Connector Pack 64-bit

○ Hitachi ID Identity and Access Management Suite

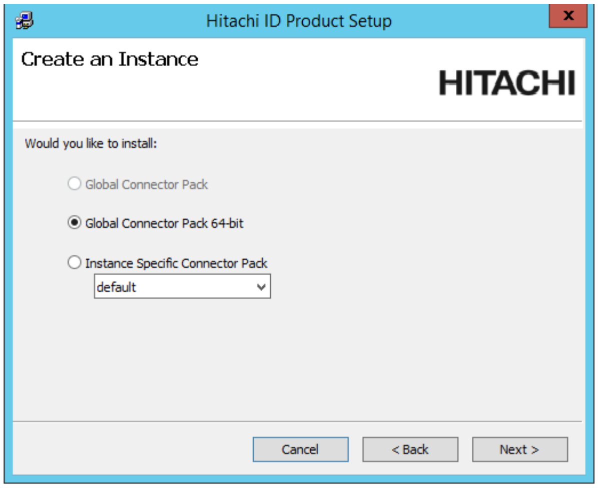
○ Hitachi ID Oracle Data Replication Service

○ Hitachi ID Identity and Access Management Suite Proxy Server

○ Hitachi ID Telephone Password Manager

4. Choose **Connector Pack**.

   Click **Next**.



Hitachi ID Product Setup

Create an Instance

Would you like to install:

○ Global Connector Pack

● Global Connector Pack 64-bit

○ Instance Specific Connector Pack

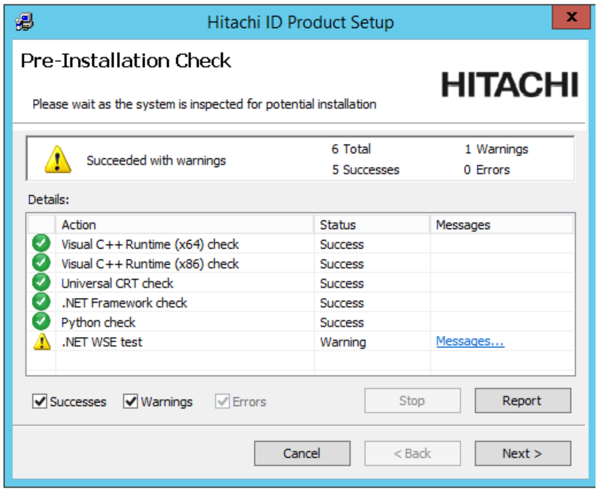
default

5. Choose **Global Connector Pack**.

   Click **Next**.

   The **`setup`** program performs a pre-installation check and verifies all of the requirements for installation.

> **Note:** Starting from *Connector Pack* 3.1+, **`setup`** checks for Visual C++ Runtime (x64) and Visual C++ Runtime (x86). If either are missing, **`setup`** attempts to install them.



Hitachi ID Product Setup

Pre-Installation Check

Please wait as the system is inspected for potential installation

Succeeded with warnings

6 Total
5 Successes
1 Warnings
0 Errors

Details:

	Action	Status	Messages
✓	Visual C++ Runtime (x64) check	Success	
✓	Visual C++ Runtime (x86) check	Success	
✓	Universal CRT check	Success	
✓	.NET Framework check	Success	
✓	Python check	Success	
⚠	.NET WSE test	Warning	Messages...

☑ Successes ☑ Warnings ☑ Errors

6. If all of the checks are successful, click **Next** to proceed with the installation.

> **Note:** If any of the pre-install checks produce warnings or errors, click **Report** for details.

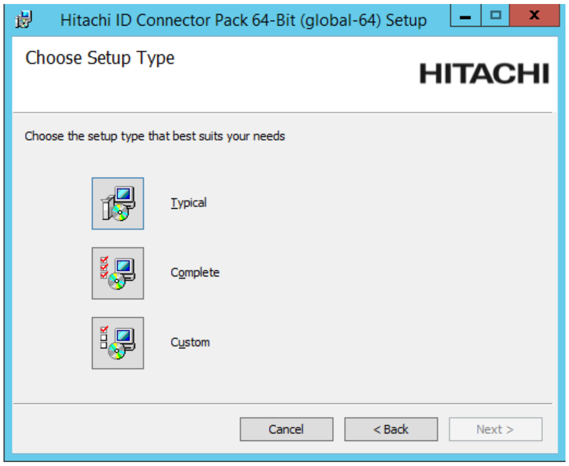
The **setup** program displays the ***Welcome to the Hitachi ID Systems* Connector Pack *(global) Setup Wizard*** page.

7. Click **Next**.

8. Read and accept the license agreement.

   Click **Next**.

9. Choose the setup type that best suits your needs:



Hitachi ID Connector Pack 64-Bit (global-64) Setup

Choose Setup Type

Choose the setup type that best suits your needs

- Click **Typical** to install all connectors, but no sample files.

  Or,

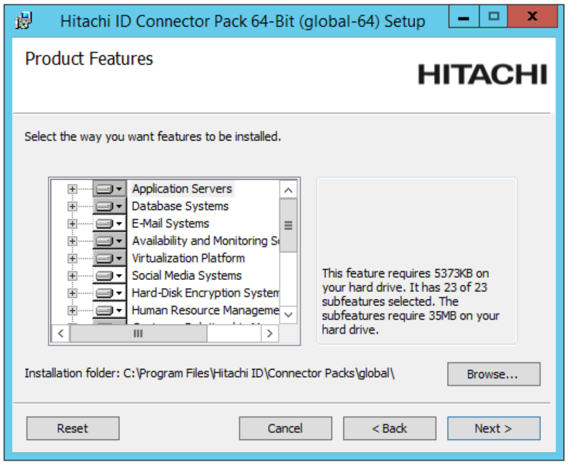
- Click **Complete** to install all connectors and sample files.

Or,

- Click **Custom** to select which connectors, sample files or other programs to install.

  Select only the items you want to install. All connectors are selected by default. Sample files are **not** selected by default.

> **Note:** Ticket management connectors (interface programs) are listed under **IT Service Management Systems**, with titles suffixed by `(Ticket)`.



Hitachi ID Connector Pack 64-Bit (global-64) Setup

Product Features

Select the way you want features to be installed.

This feature requires 5373KB on your hard drive. It has 23 of 23 subfeatures selected. The subfeatures require 35MB on your hard drive.

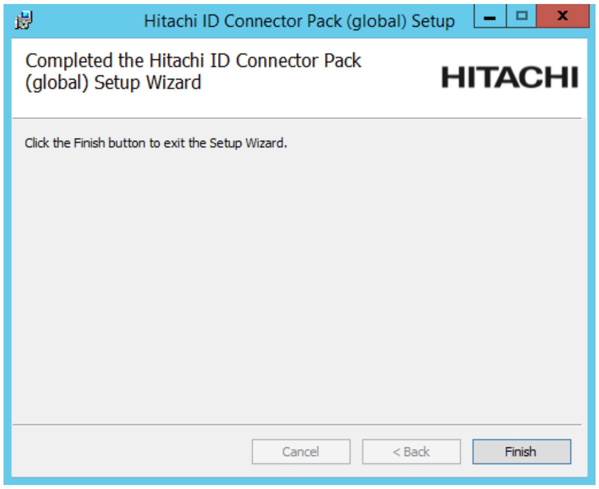
Installation folder: C:\Program Files\Hitachi ID\Connector Packs\global\

Click **Next**.

10. Click **Install** to start the installation.

11. Wait until you receive the message that the *Connector Pack* (global) has been successfully installed.

    Click **Finish**.



Hitachi ID Connector Pack (global) Setup

Completed the Hitachi ID Connector Pack (global) Setup Wizard

Click the Finish button to exit the Setup Wizard.

The post-installation tasks begin. Once the post-installation tasks are complete, you can click **Report** to see a list of connectors that have been installed by the *Connector Pack*, including any customized connectors.

CAUTION: Do not stop the post-installation tasks. The installer is loading connectors. Wait until the status changes to *success*, then click **Finish**. If you stop this process, or if it is unsuccessful, see the troubleshooting section of the Connector Pack Integration Guide.

The installer automatically generates and installs new skins.

Bravura Security Fabric Server Software 3

This chapter describes system requirements and provides instructions for installing software on *Hitachi ID Bravura Security Fabric* servers.

3.1 Server requirements

The *Hitachi ID Bravura Security Fabric* server and any replicated servers must be installed on a Windows Server operating system. Windows 2016 is recommended at the current release level of *Bravura Security Fabric*, and will be mandatory in the next major release.

Installing on Windows Server enables *Bravura Security Fabric* to leverage client software that is available only on the "Wintel" platform. In turn, this makes it possible for *Bravura Security Fabric* to manage passwords and accounts on target systems without installing a server-side agent.

Bravura Security Fabric stores all of its data in an *external database*. The database and its corresponding client software must be installed and configured before the *Bravura Security Fabric* server software can be installed.

If you are installing the *Bravura Security Fabric* on the same server as the database, ensure you take into consideration the server requirements for the database software when calculating the requirements for the *Bravura Security Fabric* server.

Each *Bravura Security Fabric* application server must also be configured with a web server. The *Bravura Security Fabric* installer is aware of and can automatically configure IIS web servers for use with *Bravura Security Fabric*.

The *Bravura Security Fabric* server is a security server, and should be locked down accordingly. See Locking Down a *Bravura Security Fabric* Server (**`server-hardening.pdf`**) for more information.

Bravura Security Fabric servers to learn how to do this. In short, most of the native Windows services can and should be removed, leaving a very small attack surface, with exactly one inbound TCP/IP port (443):

1. No ASP, JSP or PHP are used, so such code interpreters should be disabled.
2. Web-facing .NET is not used and should be disabled (some connectors require it, due to .NET API bindings).
3. No ODBC or DCOM are required inbound, so these services should be filtered or disabled at the web server. As with .NET, ODBC is sometimes needed to connect to target systems.

4. Inbound file sharing should be disabled.
5. Remote registry services should be disabled.
6. Inbound TCP/IP connections should be firewalled, allowing only port 443, remote desktop services (to configure the software) and a handful of ports between *Bravura Security Fabric* servers, mainly for data replication.

Each *Bravura Security Fabric* server requires a database instance. Microsoft SQL 2016 is the recommended choice. Microsoft SQL 2014 and 2012 are also supported. Oracle database was supported on versions up to 9.0.x and is *not* supported on 10.0 or later releases.

Bravura Security Fabric is compatible with 64-bit Windows Servers:

1. The core software is compiled as 64-bit binaries.
2. Components that execute in the context of the core OS, such as password synchronization triggers, event hooks, etc. are available in both 64- and 32-bit versions for compatibility.

3.1.1 Primary server requirements

Each *Hitachi ID Bravura Security Fabric* server is configured as follows:

- **Hardware requirements:**
  - Intel Xeon or similar CPU. Multi-core CPUs are supported and leveraged. Dual core is a minimum.
  - At least 16GB RAM – 32GB or more is leveraged and is typical for a server.
  - At least 600GB of HD storage, preferably in an enterprise RAID configuration for reliability and preferably larger for retention of more historical and log data.

    More space is always better, to increase log retention.
  - At least one Gigabit Ethernet NIC.

  Ensure you take into consideration the hardware requirements of any other software that may share the *Bravura Security Fabric* server; for example, database storage requirements.

  See Support for virtual machines for more information about support for virtual machines.

- **Operating system:**
  - Windows Server 2012 R2.
  - Windows Server 2016.
  - Windows Server 2019.

  It is recommended that the server is not a domain controller.

  In addition to the above editions, core mode on Server 2012 R2 and Server 2016 is also supported.

- **Networking:**

  - TCP/IP networking, with a static IP address and DNS name entry
  - Cryptographic certificate
  - Microsoft .NET Framework 3.5 and 4.5+
  - Web Service Enhancements (WSE) 2.0 SP3 for Microsoft .NET
  - Web server (IIS) with the following:
    - HTTP redirection
    - The IIS URL Rewrite module from:

      `http://www.iis.net/downloads/microsoft/url-rewrite`
    - CGI
    - Dynamic Compression
    - Static Compression

Modified in version 10.1.0

- **Database / connectivity software:**
- A Microsoft SQL Server 2016 (recommended), 2014 or 2012 instance is required to host the *Bravura Security Fabric* schema:
  - Normally one database instance per application server.
  - The SQL Server database software can be deployed on the same server as the *Bravura Security Fabric* application, as this reduces hardware cost and allows application administrators full DBA access for troubleshooting and performance tuning purposes. See Where to install the software for more information.
  - If the database software is deployed on a separate server, it is recommended that you install the client software that corresponds to the database backend.

  Seethe *Bravura Security Fabric* Documentation for details.
- ***Hitachi ID Connector Pack***:
  - The *Connector Pack* contains connectors which integrate *Bravura Security Fabric* with target systems.
  - It is recommended, but not required, that you install the *Connector Pack* after the *Bravura Security Fabric*. This allows you to select instance-specific or global installation.

    See the Connector Pack Integration Guide for details.
- **Installed and tested software:**
  - Native clients for the systems that *Bravura Security Fabric* will interface with

    Refer to the Connector Pack Integration Guide for information specific to each type of target system.
  - Python 3.7.3+

> **Note:** Python 3.7.3+ *must* be installed before installing *Bravura Security Fabric* or *Connector Pack*. It is required for certain *Bravura Security Fabric* components, including the Python IDMLib library used to help create plugin programs, Health check monitor, and reference builds.
>
> Ensure that Python is installed for all users to allow the *Bravura Security Fabric* service user (psadmin) account to have appropriate access to the Python installation.

> **Note:** It is recommended to add Python to the system PATH. This may also be added by selecting the option for "Add Python 3.7 to PATH" during the Python installation.

> **Note:** Python 3.8.x or later is *not* currently supported.

See Installing Python to learn how to install Python to meet these requirements.

- Microsoft Visual C++ 2015 Redistributable (x64)

  Microsoft Visual C++ 2015 Redistributable Package (x64) is required for *Bravura Security Fabric* 10.0 and higher. It is required for certain *Bravura Security Fabric* run-time components that use Visual C++ libraries. This is automatically installed during **`setup`**, if prerequisites are met.

  > **Note:** The installer checks prerequisites for C++ runtime and universal CRT. Before these two can be installed, the system requires the KB2919355 update (this is a set of patches, which has to be installed in order by clearcompressionflag.exe, KB2932046, KB2959977, KB2937592, KB2938439, KB2934018). KB2938439 must be patched before KB2919355 can be patched. During the installation of patches, if a Windows dialog box displays the message: "The update is not applicable to your computer" and you are sure that you installed the patch that matches your operating system, it is likely that there are other prerequisites that need to be installed before the current patch.

- At lease one web browser (such as Chrome), and PDF viewer (to read the documentation)
- A Git client (for revision control)

3.1.2 Installing Python

Python 3.7.3+ *must* be installed before installing *Hitachi ID Bravura Security Fabric* or *Hitachi ID Connector Pack*. It is required for certain *Bravura Security Fabric* components, including the Python IDMLib library used to help create plugin programs, Health check monitor, and reference builds.

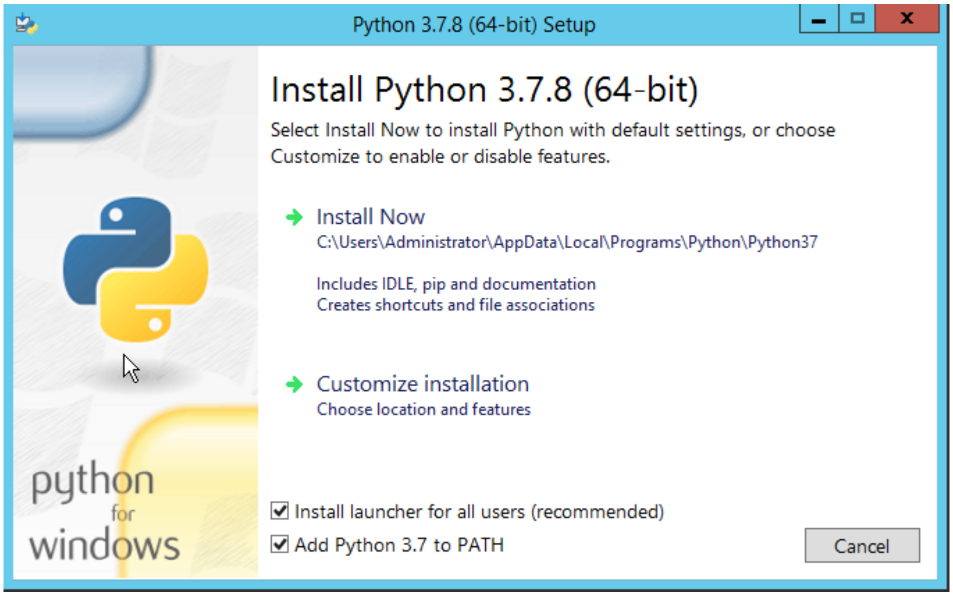
Ensure that you install the 64-bit version of Python.

Ensure that Python is installed for all users to allow the *Bravura Security Fabric* service user (psadmin) account to have appropriate access to the Python installation.

> **Note:** Python 3.8.x or later is *not* currently supported.

To install Python 3.7.3+:

1. Download and run the 64-bit installer from `python.org`.
2. On the first screen, check the **Add Python 3.7 to PATH** option.



Python 3.7.8 (64-bit) Setup

Install Python 3.7.8 (64-bit)

Select Install Now to install Python with default settings, or choose Customize to enable or disable features.

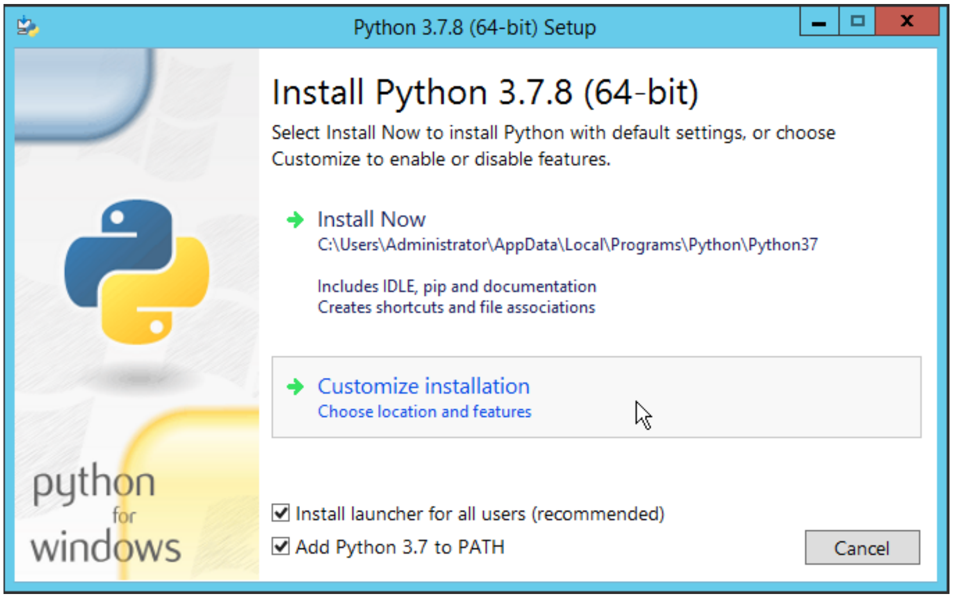
→ Install Now
C:\Users\Administrator\AppData\Local\Programs\Python\Python37

Includes IDLE, pip and documentation
Creates shortcuts and file associations

→ Customize installation
Choose location and features

☑ Install launcher for all users (recommended)
☑ Add Python 3.7 to PATH

3. Click **Custom installation**.



Python 3.7.8 (64-bit) Setup

Install Python 3.7.8 (64-bit)

Select Install Now to install Python with default settings, or choose Customize to enable or disable features.

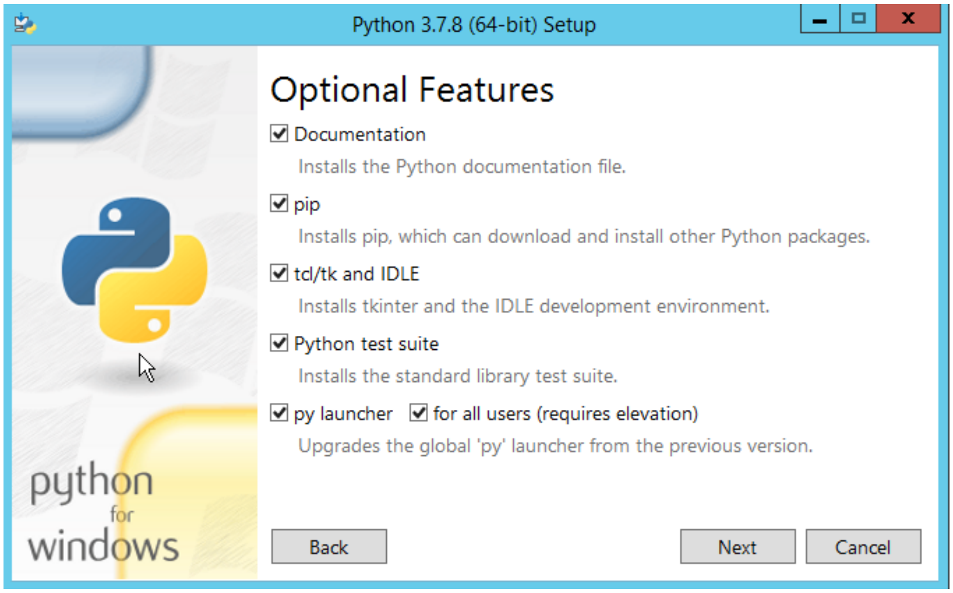
→ Install Now
C:\Users\Administrator\AppData\Local\Programs\Python\Python37

Includes IDLE, pip and documentation
Creates shortcuts and file associations

→ Customize installation
Choose location and features

☑ Install launcher for all users (recommended)
☑ Add Python 3.7 to PATH

4. Use all **Optional Features**.



Python 3.7.8 (64-bit) Setup

Optional Features

☑ Documentation
Installs the Python documentation file.

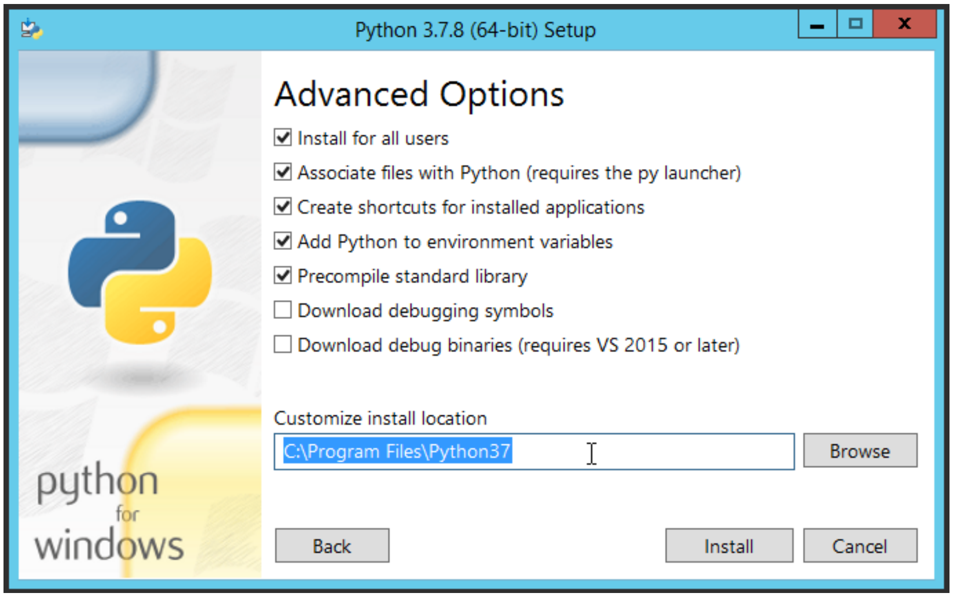
☑ pip
Installs pip, which can download and install other Python packages.

☑ tcl/tk and IDLE
Installs tkinter and the IDLE development environment.

☑ Python test suite
Installs the standard library test suite.

☑ py launcher ☑ for all users (requires elevation)
Upgrades the global 'py' launcher from the previous version.

5. On the ***Advanced Options*** screen, select **Install for all users**, and ensure that the path is correct in the **Custom install location**.



Python 3.7.8 (64-bit) Setup

Advanced Options

☑ Install for all users
☑ Associate files with Python (requires the py launcher)
☑ Create shortcuts for installed applications
☑ Add Python to environment variables
☑ Precompile standard library
☐ Download debugging symbols
☐ Download debug binaries (requires VS 2015 or later)

Customize install location
C:\Program Files\Python37

6. Click **Install**.

3.1.3 Support for virtual machines

Hitachi ID Bravura Security Fabric is compatible with VMware, Xen Project, Microsoft Hyper-V and Oracle VirtualBox virtual machine platforms. It can also be deployed on IaaS, including AWS. It generally works well with other virtualization platforms, but Hitachi ID Systems primarily tests with these. Hitachi ID Systems officially supports running *Bravura Security Fabric* on these virtual servers and will make a best effort to support customers who run on other hypervisors.

So long as the database server that hosts the *Bravura Security Fabric* back-end has access to reasonably fast I/O (e.g., NAS or similar) and so long as connectivity between the *Bravura Security Fabric* application sever and the database is fast and low latency (e.g., 1Gbps/1ms) there should is no adverse performance impact when comparing *Bravura Security Fabric* installed on hardware vs. *Bravura Security Fabric* installed on a similarly-equipped virtual server.

The key point above is to ensure sufficient I/O capacity for the database (MSSQL). If the database server is virtualized, using network attached storage (NAS) is recommended, as virtualized I/O (files such as VMDK's emulating an HDD image) is often substantially slower than physical I/O.

Even where customers choose to deploy the main *Bravura Security Fabric* servers on raw hardware, virtual machines are an excellent platform for proxy servers, test servers, development servers and model PCs.

A related question is often "how large can the deployment get before we have to move from a VM to hardware?" Unfortunately, there is no simple, universal answer:

1. Virtual servers vary in capabilities – they may have a 32-bit or a 64-bit CPU, may have 1, 2, 4 or 8 CPU cores allocated, may have different amounts of memory and may link to different types of storage infrastructure.
2. The load created by the application also varies – is there complex business logic? Do users access the application at random times or all at once? Are there just a few or thousands of integrations?

This variability means that the safest bet is to use benchmark results, using a configuration as similar as possible to the production setup, to gauge the performance of *Bravura Security Fabric* on representative physical and virtual servers.

As a general standard, the ratio of vCPU to CPU (core) is 3:1. Therefore the actual vCPU performance will be 33% of the actual CPU. If the *Bravura Security Fabric* is deployed in a virtualized environment, and the general ratio on the hypervisor is 3:1, then a virtualized setup would require 6vCPU to match the minimal 2 CPU physical CPU requirement.

3.1.4 Domain requirements

While *Hitachi ID Bravura Security Fabric* servers are capable of operating as domain members, we suggest you take the following into consideration:

- Security / limited accessibility:

  If the *Bravura Security Fabric* server is part of the domain, then other administrative users from the domain (who may not be *Bravura Security Fabric* administrators) can gain administrative logon access to the server and can then access (encrypted) credentials for target systems other than the domain.

  A policy of segregation of duties suggests that it is preferable to eliminate the ability of administrators of one system to access privileged accounts for another system and since *Bravura Security Fabric* houses such credentials, it makes sense to avoid domain membership.

- Secure service account:

  Bravura Security Fabric requires a service account which *Bravura Security Fabric* services will run as. It is recommended to restrict the service account's abilities to interactively log on to networks when a domain account is used. This is a recognized industry best-practice and it can be configured by using group policy.

  See Creating a secure service account for more details.

- Windows credential conflicts:

  To change/verify passwords on an Active Directory domain, *Bravura Security Fabric* uses ADSI, which may connect a named pipe to a share on a domain controller, such as the NETLOGON share.

  If an administrative user logs into the *Bravura Security Fabric* server console and makes a similar connection but using his personal credentials (not those encoded into *Bravura Security Fabric*), then the Windows network provider may produce a credential conflict error. This can interrupt *Bravura Security Fabric*'s ability to manage user objects on the domain, for the duration of the interactive login session.

  If *Bravura Security Fabric* is not a domain member, then the set of administrators who are able to inadvertently cause this error condition is significantly reduced and so *Bravura Security Fabric* operation is more reliable (less prone to human-induced errors).

- Password randomization

  Credential problems can also occur if the *Hitachi ID Bravura Privilege* server is also a Domain Controller, and *Bravura Privilege* is used to manage the administrator account used to target the system. When the administrator account has its password randomized, the target system administrator credentials may not be updated.

3.1.4.1 Creating a secure service account

The following steps for creating a secure service account are demonstrated on Windows 2019 server:

1. Launch **Active Directory Users and Computers**.
2. Create an OU.
3. In the OU, create an account as the service account as well as a security group.
4. Add the service account as a member of the security group.
5. Launch **Group Policy Management Console (GPMC)**.
6. Create a new group policy.
7. Right click on the group policy, then click on **Edit...** to launch **Group Policy Management Editor**, configure the group policy with following settings:
   - Navigate to **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **User Rights Assignments**
     - Select **Deny log on locally** and enter the security group created previously.

  - Select **Deny log on through remote desktop services** and enter the security group created previously.

- Exit from **Group Policy Management Editor**.

8. Back to **Group Policy Management Console (GPMC)**, click on **Scope** tab to ensure the GPO is set to authenticated users.
9. Link the GPO to any OUs containing machines which you want to stop the service account from being able to log on to interactively, or the domain level for all machines.
10. If you have more than one domain, you can put groups from the trusted domain in the GPO. However, you might want to make a GPO like this on both sides (in case of two-way trusts).
11. Reboot or run command "gpupdate.exe /force" on the machines to apply the GPO.
12. Test to ensure the service account is not allowed to log on the machines where the GPO is applied.

3.1.5 Database server

Hitachi ID Bravura Security Fabric requires MS SQL Server 2019 or 2016, typically with one database instance per application server. In most environments, the Microsoft SQL Server software is installed on the same hardware or VM as the *Bravura Security Fabric* software, on each *Bravura Security Fabric* server node. This reduces hardware cost, eliminates network latency and reduces the security surface of the combined solution.

Be sure to install the following components that come with Microsoft SQL Server 2019 and 2016:

- Database Engine Services
- Client Tools Connectivity
- Management Tools - Basic
- Management Tools - Complete

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.

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.

Seethe *Bravura Security Fabric* Documentation for details.

3.1.6 Proxy servers

In some cases, the connection to a target system may be slow, insecure or blocked. This may be because the connection spans multiple data centers or uses an insecure network protocol.

To address such connectivity problems, *Hitachi ID Bravura Security Fabric* includes a connector proxy server. When a proxy server is deployed, the main *Bravura Security Fabric* server ceases to make direct connections to some target systems and instead forwards all communication to those systems through one or more connector proxies, which are co-located with the target systems in question.

Communication from the main *Bravura Security Fabric* server to the connector proxy is encrypted and works well even when there is low bandwidth or high packet latency. It uses a single, arbitrarily-numbered TCP port number. Connections are established from the main *Bravura Security Fabric* application server to the proxy server. A single TCP port supports an arbitrarily large number of target systems at the connector proxy's location.

It is simple for firewall administrators to open a single TCP port per proxy server. Since connections are efficient and encrypted, there are usually no objections to doing so.

Communication between the proxy server and target systems continues to use whatever protocol each system supports natively. This communication is confined to a physically secure data center with a high-bandwidth, low-latency local network.

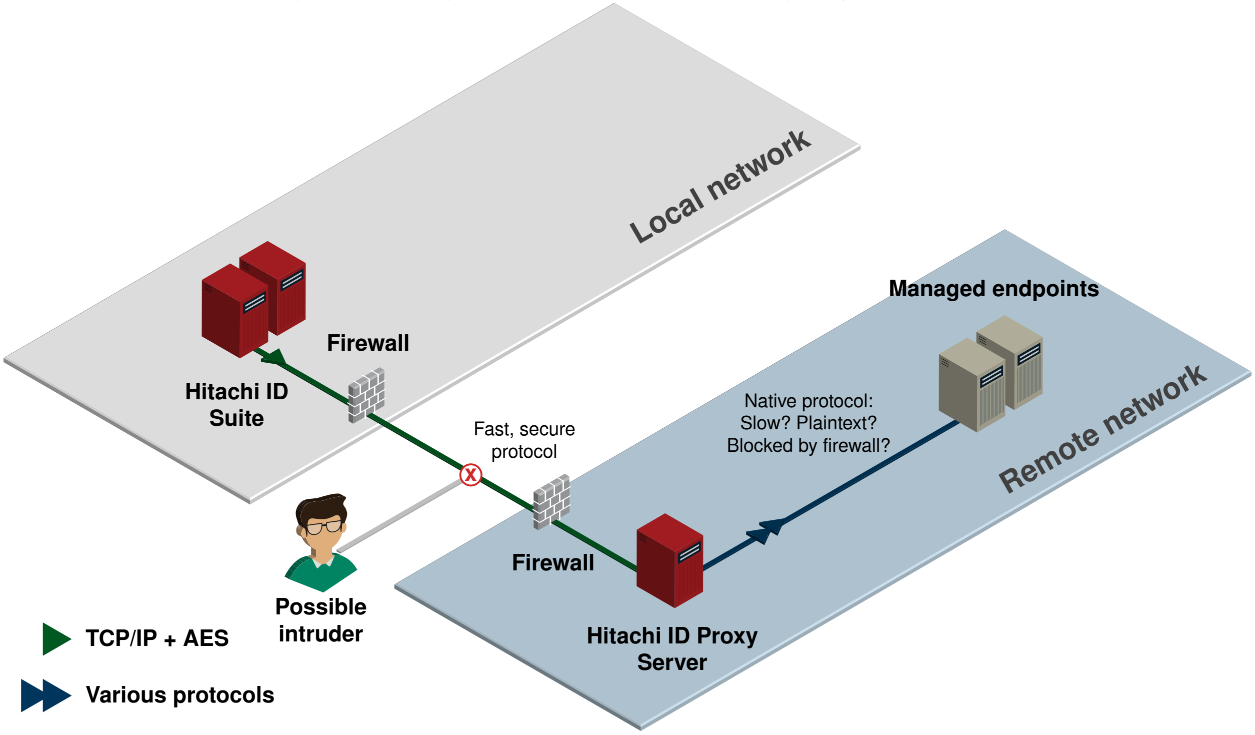
Deployment of the secure *Bravura Security Fabric* proxy server is illustrated in Figure 3.1.

See the *Bravura Security Fabric* Documentation for more information.

3.1.7 Browser support

The following browsers are supported:

Figure 3.1: Target systems connected through a proxy server



- Internet Explorer 11 or later *(recommended)*.
- Microsoft Edge.
- Edge Chromium.
- Latest versions of Mozilla Firefox and Google Chrome.

Font downloads must be enabled in the browser to allow *Hitachi ID Bravura Security Fabric* to use Font Awesome.

Some plugins require that you configure ActiveX security.

3.1.7.1 HTTPS settings

As of version 12.1.1 *Bravura Security Fabric* adds the "Strict-Transport-Security" header to IIS for all resources. What this means is that if you have configured your site to use SSL and if you have accessed your site using HTTPS protocol, the browser will cache that the site supports HTTPS and prevents the browser from using HTTP. This keeps your site secure but occasionally in testing there will be a need to downgrade the browser security to allow accessing your site via HTTP. In order to do this you must clear the HSTS settings in the browsers.

These links show how to clear the HSTS settings in the browsers:

- `https://www.thesslstore.com/blog/clear-hsts-settings-chrome-firefox/`
- `https://tinsleynet.co.uk/2017/hsts/`

3.2 Using setup to install *Bravura Security Fabric*

You can use **`setup`**, located at the root of the distribution folder, to install one or more *Hitachi ID Bravura Security Fabric* instances. For example, you can have *Bravura Security Fabric* instances representing target systems and users in different geographical regions, or have separate instances with different password rules for different sets of users or clients.

The **`setup`** program requires Windows Installer version 3.0.1 or later. This program should be run by a member of the Windows Administrators group.

CAUTION: Before you begin, ensure that the server that will host *Bravura Security Fabric* meets the minimum system requirements and that all required software is installed. See the *Bravura Security Fabric* Documentation for details.

CAUTION: Ensure that your back-end database and *dedicated user* are set up according to the *Bravura Security Fabric* Documentation .

Note: If you are installing multiple instances on the same machine, you may be prompted to either reboot the system, or to shut down and restart the file replication service before continuing the installation. This is because the file replication service keeps certain DLL files open. You can avoid having to do this during installation by shutting down all file replication services before you begin.

3.2.1 Preparation for Management Suite Server Installation

Gather the following information about your database server configuration:

- IP address or DNS name of the database server.

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

- Name and password of a database administrator (DBA) (such as sa or SYS).
- The SQL database instance name.
- If you are using an existing database, you will also need:

  - The name of the *Bravura Security Fabric* database.
  - TCP port number (such as 1521) that the database is listening on.
  - Name and password of the SQL dedicated user.

If you are installing the *Analytics* app, gather the following information:

- The server name where SQL Server Reporting Services (SSRS) resides
- Report Server Web Service URL
- Name and password of service account
- If you are using an existing report server database you will need that database name
- If you are using an existing report server user you will need that username and password

3.2.2 Starting the Management Suite Server Installation

To install *Hitachi ID Bravura Security Fabric* products and features on a primary server or replicated server:

1. Log into the host Windows server as member of the Administrators group.

   > **CAUTION:** If you plan to use a preconfigured database using windows authentication, the installation of *Bravura Security Fabric* needs to be performed by the same account ID that will run the *Bravura Security Fabric* service(s).

2. If required, download and unzip the *Bravura Security Fabric* distribution folder.

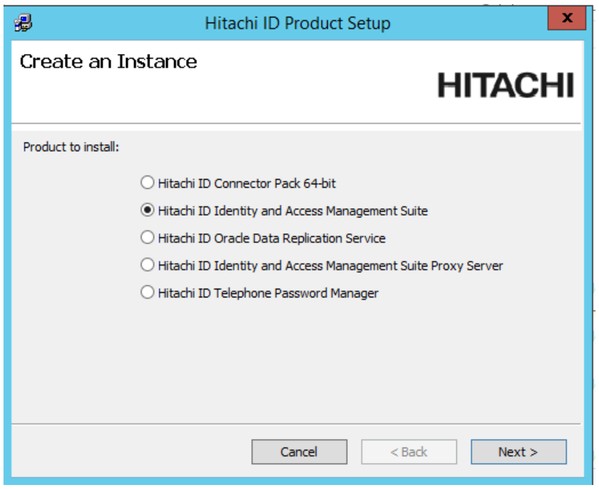
   Contact your Hitachi ID account representative for details.

3. Launch the **`setup`** program located at the root of the distribution folder.

4. If you already have an *Bravura Security Fabric* instance installed on the Windows server, **`setup`** displays the ***Select an instance to configure*** page.

   Click **Install New** to proceed.

   A list of available products is displayed.



Hitachi ID Product Setup

Create an Instance

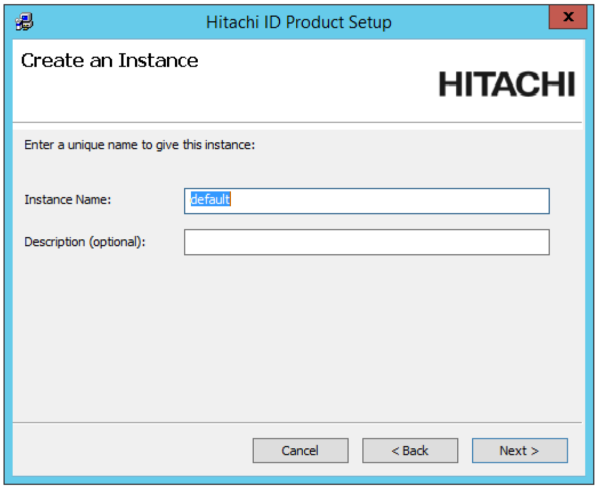
HITACHI

Product to install:

○ Hitachi ID Connector Pack 64-bit
● Hitachi ID Identity and Access Management Suite
○ Hitachi ID Oracle Data Replication Service
○ Hitachi ID Identity and Access Management Suite Proxy Server
○ Hitachi ID Telephone Password Manager

5. Select ***Bravura Security Fabric***, then click **Next**.

   The **`setup`** program displays a page to gather initial instance information.



Hitachi ID Product Setup

Create an Instance

HITACHI

Enter a unique name to give this instance:

Instance Name: default

Description (optional):

6. Type a unique instance name, and optionally a description.

   Note: All replicated servers must have the same instance name.

   Note: Instance names cannot contain whitespace or the following characters: `% \ / : ; ' ` , * ? " < > | & $`

   Click **Next**.

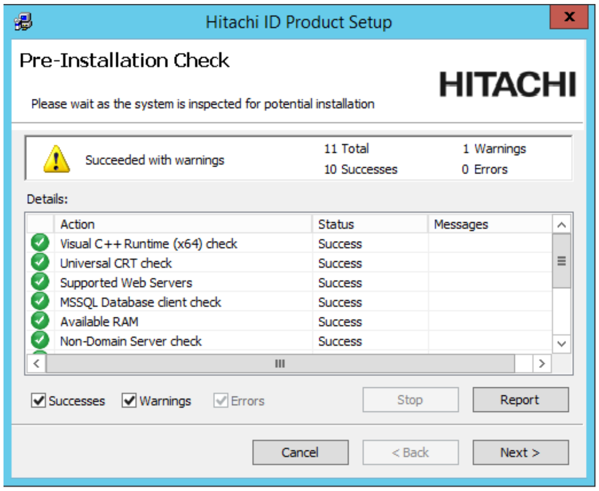
   The **`setup`** program performs a pre-installation check and verifies all of the requirements for installation.

   If any of the pre-install checks produce warnings or errors, click:

- **Report** for details on all pre-install checks
  Or,
- **Messages...** for details on a specific pre-install check

See the *Bravura Security Fabric* Documentation for additional troubleshooting information.

> **Note:** The installer checks for Visual C++ Runtime (x64) and Visual C++ Runtime (x86). If either are missing, `setup` attempts to install them. See the *Bravura Security Fabric* Documentation for more information.



Hitachi ID Product Setup

Pre-Installation Check

Please wait as the system is inspected for potential installation

Succeeded with warnings

11 Total	1 Warnings
10 Successes	0 Errors

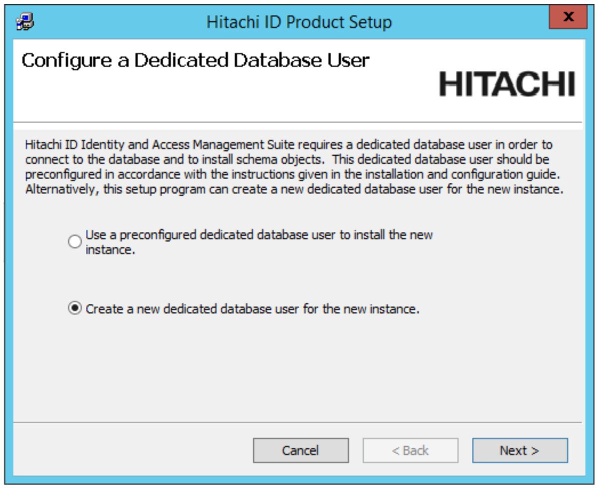
Details:

Action	Status	Messages
✓ Visual C++ Runtime (x64) check	Success	
✓ Universal CRT check	Success	
✓ Supported Web Servers	Success	
✓ MSSQL Database client check	Success	
✓ Available RAM	Success	
✓ Non-Domain Server check	Success	

☑ Successes ☑ Warnings ☑ Errors

7. If all of the checks are successful, click **Next** to proceed with the installation.

   The ***Configure a Dedicated Database User*** page is displayed.



Hitachi ID Product Setup

Configure a Dedicated Database User

Hitachi ID Identity and Access Management Suite requires a dedicated database user in order to connect to the database and to install schema objects. This dedicated database user should be preconfigured in accordance with the instructions given in the installation and configuration guide. Alternatively, this setup program can create a new dedicated database user for the new instance.

○ Use a preconfigured dedicated database user to install the new instance.

● Create a new dedicated database user for the new instance.

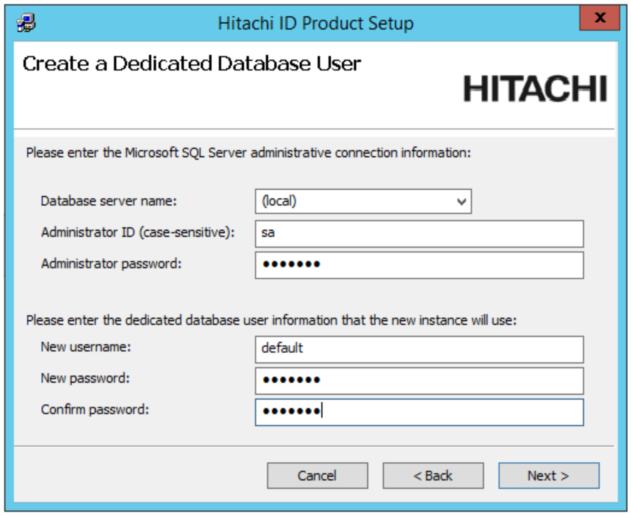
8. Choose your database user setup option, then click **Next**.

   If you want `setup` to create and configure a New Dedicated Database user, proceed to Using setup to create a new dedicated database user.

If you already have a dedicated database user created and configured, proceed to Configuring the software installation.

3.2.3 Using setup to create a new dedicated database user

On the ***Configure a Dedicated Database User*** page, when you select **Create a new dedicated database user for the new instance**, **`setup`** displays the database user and connection information page depending on your database system.



Please enter the Microsoft SQL Server administrative connection information:

Database server name: (local)
Administrator ID (case-sensitive): sa
Administrator password: •••••••

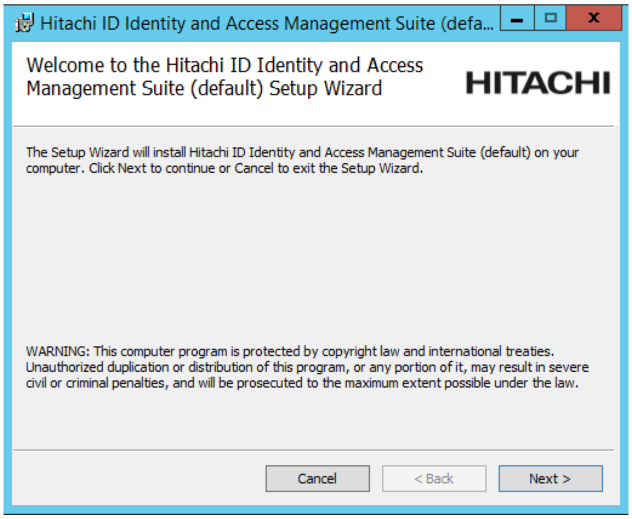
Please enter the dedicated database user information that the new instance will use:
New username: default
New password: •••••••
Confirm password: •••••••

Enter the database connection and user information, then click **Next**. The **`setup`** program creates the new database user.

Proceed to Configuring the software installation.

3.2.4 Configuring the software installation

The **`setup`** program launches **`idm.msi`** to configure the software installation. The welcome page is displayed:



Hitachi ID Identity and Access Management Suite (defa...

Welcome to the Hitachi ID Identity and Access Management Suite (default) Setup Wizard

The Setup Wizard will install Hitachi ID Identity and Access Management Suite (default) on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

To configure software installation:

1. Read and accept the license agreement.

   Click **Next**.

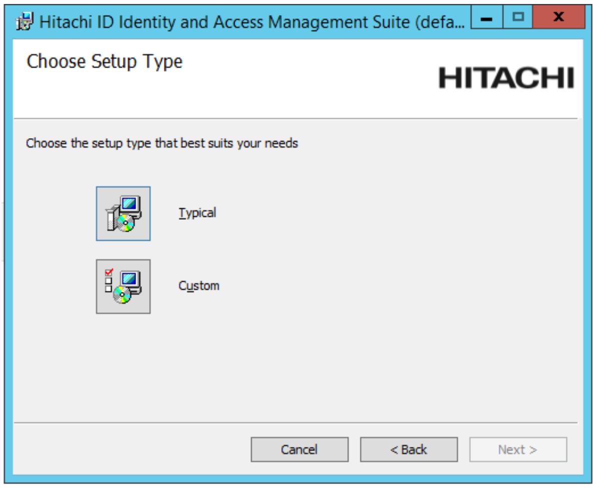
2. Type the location of the license file.

   Alternatively, you can use the **Browse** button to select the location of your license file.

   > **Note:** It is recommended that all replicated servers use the same license file.

   Click **Next**.

   The installer displays setup types for you to select from.



Hitachi ID Identity and Access Management Suite (defa...

Choose Setup Type

Choose the setup type that best suits your needs

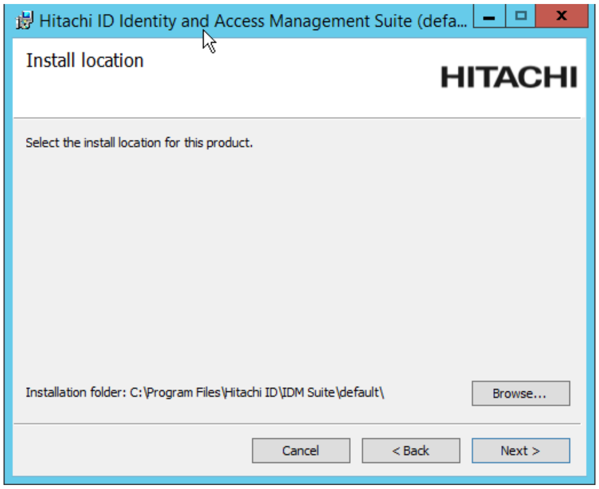
3. Select:

   - **Typical** to install with default settings for file locations, ports, and web site. Proceed to Step 6.

Or,

- **Custom** to customize settings.

> **Note:** Files for all products are installed; however only those for licensed products are enabled for use.



Hitachi ID Identity and Access Management Suite (defa...

Install location

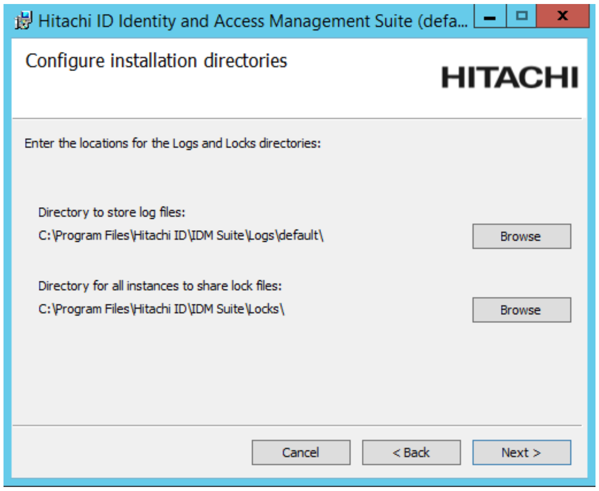
Select the install location for this product.

Installation folder: C:\Program Files\Hitachi ID\IDM Suite\default\

4. If you chose a custom installation, choose the **Install location**.

> **Note:** It is recommended that you do *not* change the install location.

Click **Next**.



Hitachi ID Identity and Access Management Suite (defa...

Configure installation directories

Enter the locations for the Logs and Locks directories:

Directory to store log files:
C:\Program Files\Hitachi ID\IDM Suite\Logs\default\

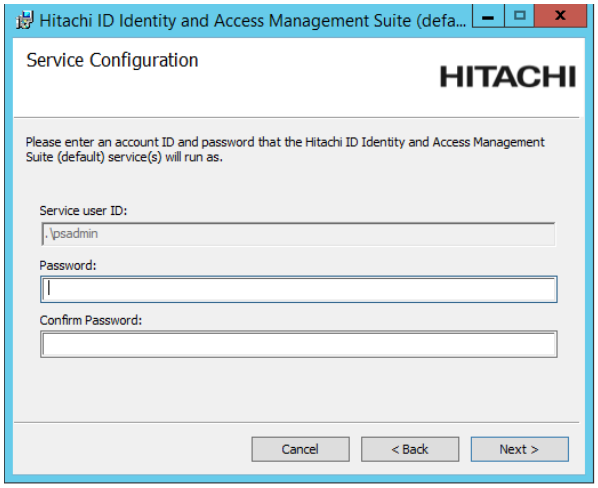
Directory for all instances to share lock files:
C:\Program Files\Hitachi ID\IDM Suite\Locks\

5. If you chose a custom installation, choose the locations for the:

Directory to store log files This directory should be *unique* for each instance. The default is <*Program Files path*>\Hitachi ID\IDM Suite\Logs\<*instance*>\.

Directory for all instances to share lock files This directory should be *shared* by all instances. The default is <*Program Files path*>\Hitachi ID\IDM Suite\Locks\.

Click **Next**.



Service Configuration

Please enter an account ID and password that the Hitachi ID Identity and Access Management Suite (default) service(s) will run as.

Service user ID: .\psadmin

Password:

Confirm Password:

6. Type the **Service user ID** and **Password**.

   This is the account *Hitachi ID Bravura Security Fabric* services will run as. If IIS is selected as your Web server, this is also the anonymous user for web access.

   You can use either a local or domain account for the **Service user ID**. The **Password** can be up to 64 characters long.

   The default is *psadmin*. If you use the default account and the account does not already exist, the installer will create it with the specified password on the *Bravura Security Fabric* instance server. If a domain account is specified, the installer validates the account and password before proceeding. An error message will display if the domain account can not be found or the password is incorrect.

   Note: Denying interactive log-on for service account is a recognized industry best-practice which is also suggested by *Bravura Security Fabric*. See Domain requirements for more details on how to create a secure service account.

   Click **Next**.

   See also:

   Refer to serviceacct in the Bravura Security Fabric *Reference Manual* for information about the **`serviceacct`** utility, used to make updates in cases where the *psadmin* account is changed.

7. Type the **communication key** that will be used to encrypt communication between the *Hitachi ID Bravura Security Fabric* server and other *Bravura Security Fabric* components on the network.

   The key must only contain hexadecimal digits (0-9, a-f).

   You can also click **Random Key** to generate a random key.

   Note: The same *communication key* must be applied to all components that share communication. It is strongly recommended that you note this key in a safe location.

Click **Next**.

8. Type the **database encryption key** that will be used to encrypt sensitive data stored in the *Bravura Security Fabric* database; for example, *Bravura Security Fabric* uses the database encryption key to encrypt passwords.

   The key must only contain hexadecimal digits (0-9, a-f).

   You can also click **Random Key** to generate a random key.

   > **Note:** The same database encryption key must be applied to all *Bravura Security Fabric* servers in a replication environment and all components that share communication. It is strongly recommended that you note this key in a secure location.

   Click **Next**.

9. Type the **workstation authentication encryption key** that will be used to initialize the communication of untrusted *Bravura Security Fabric* components to *Bravura Security Fabric* servers on the network. The **workstation authentication encryption key** is used by the workstation component for either initial registration or key re-negotiation.

   The key must only contain hexadecimal digits (0-9, a-f).

   You can also click **Random Key** to generate a random key.

   > **Note:** The same workstation authentication encryption key must be applied to all *Bravura Security Fabric* servers in a replication environment and all components that share communication. It is strongly recommended that you note this key in a secure location.

   Click **Next**.

10. Type the **Connector encryption key** that will be used to encrypt sensitive data for communication with the connectors; for example, *Bravura Security Fabric* uses the Connector encryption key to encrypt and decrypt passwords and administrative credentials used by connectors and exit traps as well as all communication and operations run by the connectors.

    The key must only contain hexadecimal digits (0-9, a-f).

    You can also click **Random Key** to generate a random key.

    > **Note:** The same Connector encryption key must be applied to all *Bravura Security Fabric* servers in a replication environment and all components that share communication. It is strongly recommended that you note this key in a secure location.

    Click **Next**.

11. Type the **IDMLib encryption key** that will be used to encrypt sensitive data generated in IDMLib.

    The key must only contain hexadecimal digits (0-9, a-f).

    You can also click **Random Key** to generate a random key.

    > **Note:** The same IDMLib encryption key must be applied to all *Bravura Security Fabric* servers in a replication environment and all components that share communication. It is strongly recommended that you note this key in a secure location.

Click **Next**.

12. If you want to install the *Analytics* app, configure options to connect with SQL Server Reporting Services (SSRS); proceed to SSRS settings

    Click **Skip** if you do *not* want to install this component.

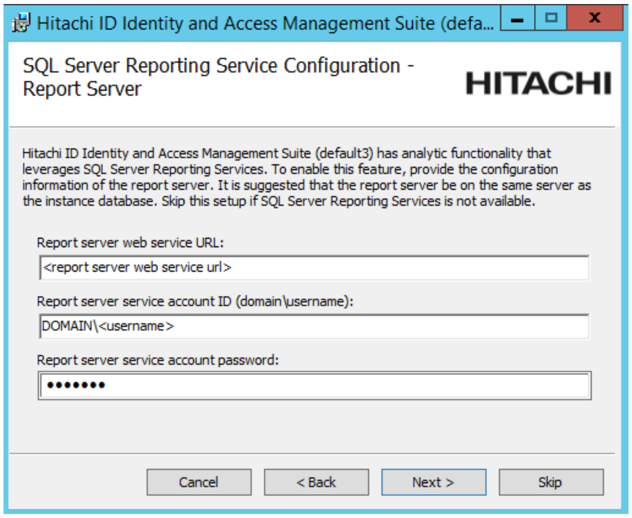
    - If you chose a typical installation, and used **`setup`** to create a new dedicated database user, skip to Completing the installation process.
    - If you chose a typical installation, and chose to use a preconfigured database user, **`setup`** displays SQL Server connection settings; proceed to Microsoft SQL Server connection details.
    - If you chose a custom installation, **`setup`** displays port settings; proceed to Custom port and web server settings

    See also:

    You must have access to SQL Server Reporting Services to use this component. See Preparation for Management Suite Server Installation for requirements.

    If you skip SSRS setup now you can set it up after installing Bravura Security Fabric software, as documented in the Reports User Guide (**`reports.pdf`**).

3.2.4.1 SSRS settings



SQL Server Reporting Service Configuration - Report Server

Hitachi ID Identity and Access Management Suite (default3) has analytic functionality that leverages SQL Server Reporting Services. To enable this feature, provide the configuration information of the report server. It is suggested that the report server be on the same server as the instance database. Skip this setup if SQL Server Reporting Services is not available.

Report server web service URL: <report server web service url>

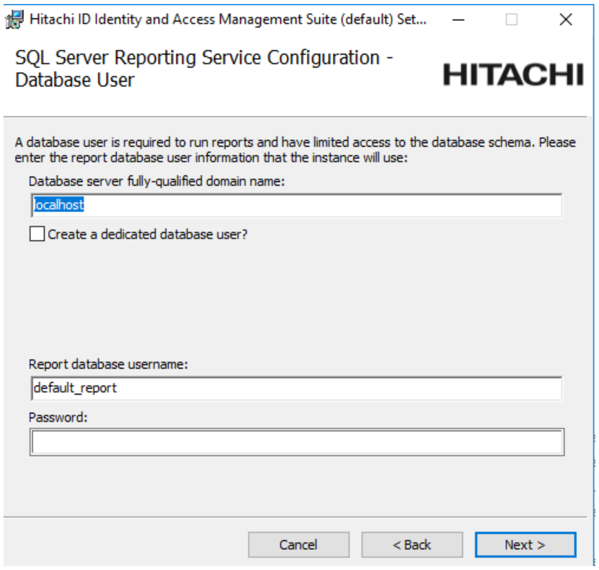
Report server service account ID (domain\username): DOMAIN\<username>

Report server service account password: •••••••

To configure the *Analytics* app connection to SSRS:

1. Enter the Report Servers web service URL.
2. Enter the SSRS service username and password.
3. Click **Next**.

   The ***SQL Server Reporting Service Configuration - Database User*** page is displayed.



Hitachi ID Identity and Access Management Suite (default) Set...

SQL Server Reporting Service Configuration - Database User

A database user is required to run reports and have limited access to the database schema. Please enter the report database user information that the instance will use:

Database server fully-qualified domain name: localhost

□ Create a dedicated database user?

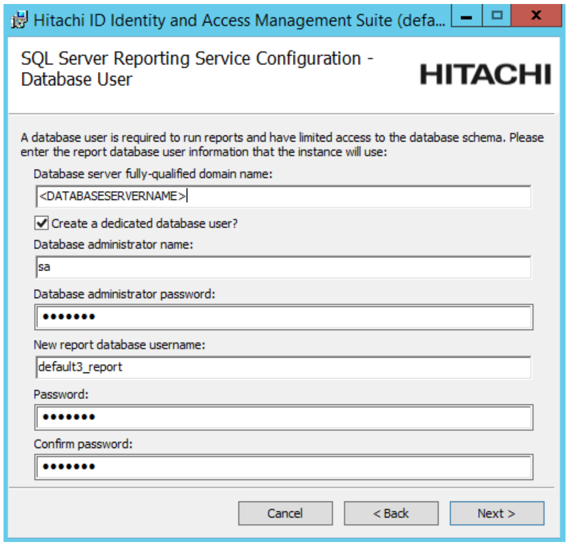
Report database username: default_report

Password:

4. Enter the name of server where your instance database resides.

5. Choose your report database user option.

   (a) If you want **`setup`** to create and configure a new dedicated database user that can query the instance database, enable the **Create a dedicated database user?** option.



Hitachi ID Identity and Access Management Suite (defa...

SQL Server Reporting Service Configuration - Database User

A database user is required to run reports and have limited access to the database schema. Please enter the report database user information that the instance will use:

Database server fully-qualified domain name: <DATABASESERVERNAME>

☑ Create a dedicated database user?

Database administrator name: sa

Database administrator password: •••••••

New report database username: default3_report

Password: •••••••

Confirm password: •••••••

   Enter the database administrator name and password so the installer can create the new dedicated database user.

   (b) If you already have a dedicated database user created and configured, enter those details and click **Next**, otherwise, add a password for the new dedicated database user.

6. Click **Next**.

- If you chose a typical installation, and used **`setup`** to create a new dedicated database user, skip to Completing the installation process.
- If you chose a typical installation, and chose to use a preconfigured database user, **`setup`** displays SQL Server connection settings; proceed to Microsoft SQL Server connection details.
- If you chose a custom installation, **`setup`** displays port settings; proceed to Custom port and web server settings

3.2.4.2 Custom port and web server settings

If you chose a custom installation, after configuring keys and SSRS settings:

1. Define port settings:

   Database Service TCP port that the Database Service (iddb) will listen on, for database replication. The default is `5555` unless that port is already in use by another *Bravura Security Fabric* instance.

   File Replication Service TCP port number that the File Replication Service (idfilerep) will listen on, for file replication. The default is `2380` unless that port is already in use by another *Bravura Security Fabric* instance.

   Workflow Manager Service TCP port number that the Workflow Manager Service (idwfm) will listen on. The default is `2240` unless that port is already in use by another *Bravura Security Fabric* instance.

   Transaction Monitor Service TCP port that Transaction Monitor Service (idtm) will listen on. The default is `2234` unless that port is already in use by another *Bravura Security Fabric* instance.

   Password Manager Service TCP port that the Password Manager service (idpm) will listen on. The default is `3334` unless that port is already in use by another *Bravura Security Fabric* instance.

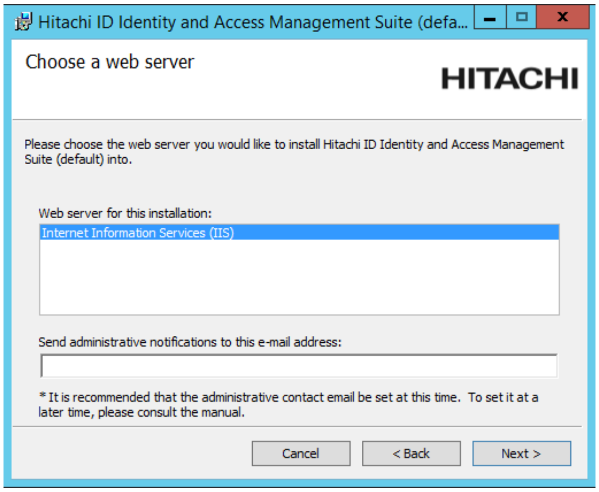
   Session Monitoring Package Generation Service TCP port that session monitoring modules will listen on. The default is `2340` unless that port is already in use by another *Bravura Security Fabric* instance.

   Discovery Service TCP port that the Discovery service will listen on. The default is `2540` unless that port is already in use by another *Bravura Security Fabric* instance.

   Privileged Access Manager Service TCP port that the Privileged Access Manager Service (idarch) will listen on. The default is `6190` unless that port is already in use by another *Bravura Security Fabric* instance.

   Persistent Connector Service TCP port that the Persistent Connector Service (agtsvc) will listen on. The default is `4567` unless that port is already in use by another *Bravura Security Fabric* instance.

   Click **Next**.



Choose a web server

Please choose the web server you would like to install Hitachi ID Identity and Access Management Suite (default) into.

Web server for this installation:

Internet Information Services (IIS)

Send administrative notifications to this e-mail address:

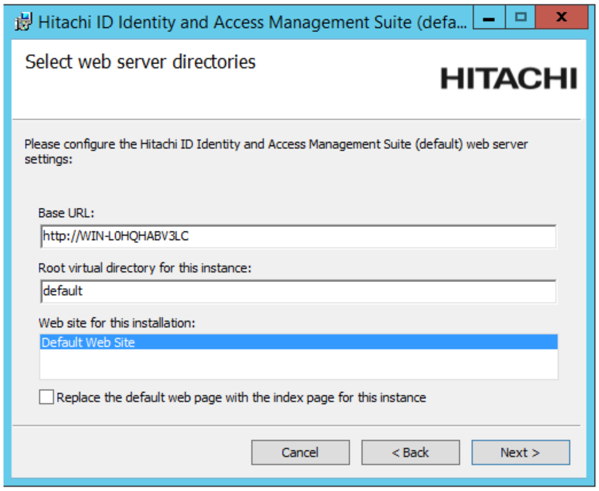
* It is recommended that the administrative contact email be set at this time. To set it at a later time, please consult the manual.

2. Select a **Web server for this installation**.

   If multiple web servers are installed on your *Hitachi ID Bravura Security Fabric* server, select the one on which you want to install *Bravura Security Fabric*. IIS web servers are automatically detected and configured.

   Type an email address to receive administrative notifications.
   You can use the *Manage the system* (PSA) module to set or change this later by modifying the RECIPIENT EMAIL option.

   Click **Next**.



Select web server directories

Please configure the Hitachi ID Identity and Access Management Suite (default) web server settings:

Base URL:

http://WIN-L0HQHABV3LC

Root virtual directory for this instance:

default

Web site for this installation:

Default Web Site

□ Replace the default web page with the index page for this instance

3. Configure the following options for your web server:

   Base URL This is the URL of the *Bravura Security Fabric* server. The installer automatically detects the server name.

   Root virtual directory for this instance This is the name of the virtual directory that points to the physical \<*instance*>\cgi-bin\ directory.

   > **Note:** Virtual directory paths cannot contain whitespace or the following characters:
   > % \ / | @ ! # $ ^ & * < > ; : ” ’ ? , [ ] { } + = ` .

   The default value is the name of the instance.

   Web site for this installation If the web server for this installation is IIS, select the web site you want *Bravura Security Fabric* to use.

   Replace the default web page with the index page for this instance Enable this checkbox if you want to replace the default web page with the index page for this instance. The index page automatically redirects users to the Front-end (PSF).

   Click **Next**.

   - If you chose to use **setup** to create a new dedicated database user, skip to Completing the installation process.
   - If you chose to use a preconfigured database user, proceed to Microsoft SQL Server connection details.

3.2.4.3 Microsoft SQL Server connection details

If you chose to use a preconfigured database user at the beginning of the installation process, choose an authentication mode that the SQL Server ID should use. You can choose either SQL Server authentication or Windows authentication. If you choose Windows authentication, ensure that the login exists on the SQL Server database server for the account ID that the *Hitachi ID Bravura Security Fabric* services will run as.

Click **Next**.

Enter connection information as follows:

Database server name Type the name of the server hosting the database:

```
<dbserver>
```

If the database is installed on your *Bravura Security Fabric* server, use . (period), localhost, or the server name.

If you installed SQL Server with the non-default instance name, you must include a backslash followed by the instance name:

```
<dbserver>\<instance>
```

For the express edition, the instance is normally SQLEXPRESS.

If SQL Server is using a custom port, the syntax is:

```
<dbserver>,<port>[\<instance>]
```

Database name Type the name of the database hosting the schema.

Database server user ID If using SQL Server authentication, type the ID of the dedicated user that you created for *Bravura Security Fabric*. This field is not visible for Windows authentication.

You must use a different dedicated user for each *Bravura Security Fabric* instance.

Database server user password If applicable, type the password for the above user.

> **Note:** If a change has been made to the database server credentials, use the `iddbadm` program to update the database information.
>
> See iddbadm in the *Reference Manual* for more information.

Advanced configuration

If you want to modify how *Hitachi ID Bravura Security Fabric* installs the database schema, click **Advanced** on the ***Database Server configuration*** page and configure the following:

Install schema Clear this checkbox if you do *not* want *Bravura Security Fabric* to install the schema because it has already been installed by your database administrator, or you are using a shared schema.

Populate default data Clear this checkbox if you do *not* want *Bravura Security Fabric* to populate default data; for example where you want to install to a shared schema.

Schema install user ID (Optional) If using SQL Server authentication, type the ID of the user to install the schema as. This field is not visible for Windows authentication.

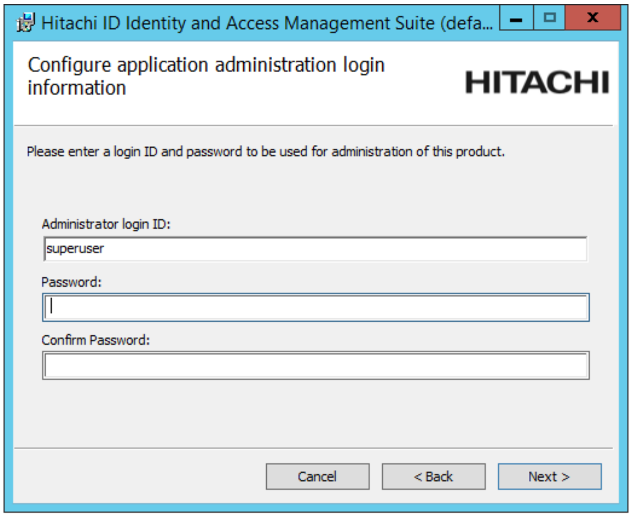
This user must be able to create schema objects. If not specified, *Bravura Security Fabric* uses the **Database server user ID**.

Schema install password If applicable, type the password for the above user.

The password is only required if **Install schema** is selected and **Schema install user ID** is specified.

3.2.5 Completing the installation process

Once you have configured the software installation and determined how you will connect to the database, complete the setup process:



Hitachi ID Identity and Access Management Suite (defa...

Configure application administration login information

Please enter a login ID and password to be used for administration of this product.

Administrator login ID: superuser

Password:

Confirm Password:

1. Type the login ID and password for the *Hitachi ID Bravura Security Fabric application administrator*. The default login ID is superuser. The password can be up to 64 characters long.

   Note: Be sure to remember this login ID and password. You will need them to log into *Bravura Security Fabric*.

   Click **Next**.

2. Click **Install** to start the installation.

   The installer begins copying files to your computer. The ***Completed the* Bravura Security Fabric *(<instance>) Setup Wizard*** page appears after the *Bravura Security Fabric* features have been successfully installed.

3. Click **Finish** to exit.

   The post-installation tasks begin.

   CAUTION: Do not stop the post-installation tasks. The installer is attempting to load connectors from the *Connector Pack*, language tags, and reports.

   If you install the *Bravura Security Fabric* before a *Connector Pack* has been installed, a warning appears at this stage that no connectors could be found. It is safe to proceed.

   If any of the post-installation tasks produce warnings or errors, click:

   - **Report** for details on all post-installation tasks
     Or,
   - **Messages...** for details on a specific post-installation task

   Otherwise, wait until the status changes to *success*, then click **Finish**.

   If connectors (agents) were not installed successfully, see “Troubleshooting” in the Connector Pack Integration Guide.

WARNING!: If the server is going to be used for replication, it is important that the server is configured for replication before any modification or configuration of the *Bravura Security Fabric* software occurs. Replication configuration must be completed first. Refer to the Replication and Recovery (**`replication.pdf`**). This only applies to servers being used for replication.

See also:

- INSTALLATION TOOLS in the *Reference Manual* for additional information about **`setup`** and **`idm.msi`**.

Index