CAUTION: Ensure you read the "Pre-Installation" (**`pre-installation.pdf`**) and "Installing Database Software" (**`sql-server.pdf`**) documents before you start.

CAUTION: This document is suitable for a demonstration or evaluation installation. There are many factors to consider before beginning an installation in a production environment; consult the *Bravura Security Fabric* Documentation for details.

1 Bravura Security Fabric software

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 "Pre-Installation" (**`pre-installation.pdf`**) for details.

CAUTION: Ensure that your back-end database and *dedicated user* are set up according to "Installing Database Software" (**`sql-server.pdf`**).

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.

1.1 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

2 Use case: Installing Bravura Security Fabric software

This use case shows you how to install the *Hitachi ID Bravura Security Fabric* software in a typical demonstration environment.

Requirements

This use case assumes that:

- The environment has been set up as described in “Pre-Installation” (**`pre-installation.pdf`**).
- The SQL Server has been set up according to “Installing Database Software” (**`sql-server.pdf`**).

  In this case the **`setup`** program will create a new dedicated database user for this instance.
- You have downloaded the license and installation files.

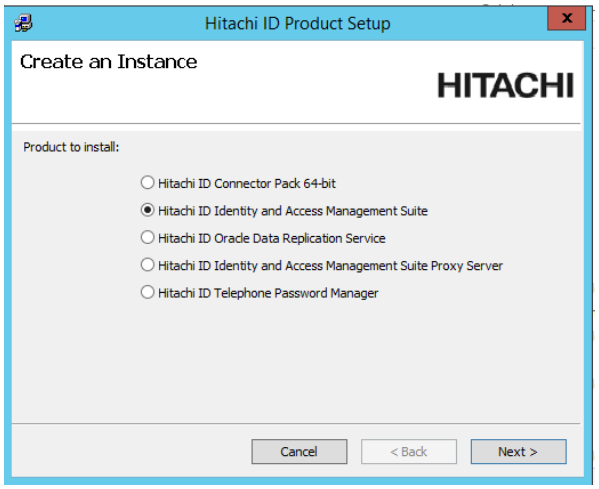
  If you don’t already have a license file, contact your account representative or instructor to request the *Hitachi ID Bravura Security Fabric* license file. Download the license to your *Bravura Security Fabric* server, to the same location as the **`idm.msi`** and **`setup`** files.
- You are logged into your Windows server with elevated privileges (administrator).

Run setup

> **Note:** The screenshots may vary from your server type and product installation.

1. Navigate to the folder containing the setup program for *Hitachi ID Bravura Security Fabric*.

2. Double-click **`setup`** to start the setup wizard.



Hitachi ID Product Setup

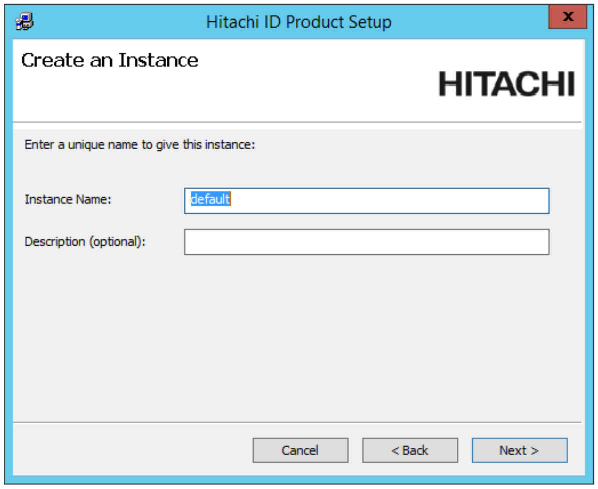
Create an Instance

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

3. Select **Hitachi ID Bravura Security Fabric**, then click **Next**.

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



Hitachi ID Product Setup

Create an Instance

Enter a unique name to give this instance:

Instance Name: default

Description (optional):

4. Accept the `default` instance name in the **Instance Name** field.

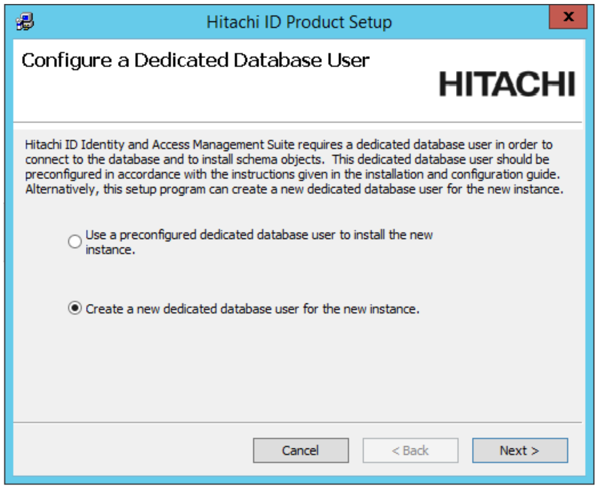
> **Note:** In a production environment, this could be any instance name. All replicated servers must have the same instance name.

5. Click **Next**.

   The **`setup`** program performs a pre-installation check. There should be no errors. Warnings are fine. In this case, you are installing *Bravura Security Fabric* only so connector pack warnings will appear. Notice that the Visual C++ 2015 Runtime libraries were installed automatically.

6. Click **Next** to go ahead with the installation.

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



Hitachi ID Product Setup

Configure a Dedicated Database User

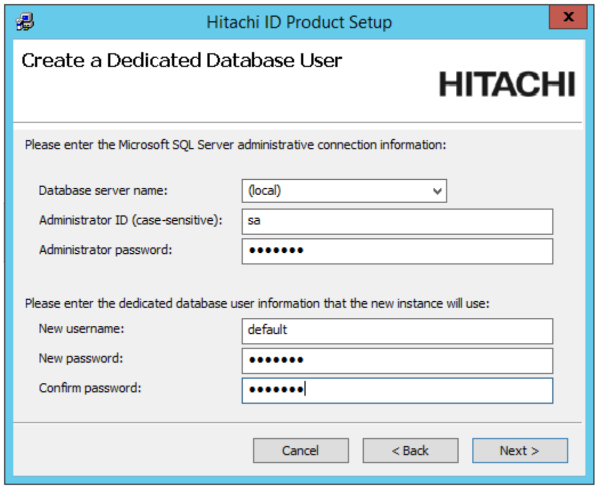
HITACHI

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.

7. Choose **Create a new dedicated database user for the new instance** and click **Next**.



Hitachi ID Product Setup

Create a Dedicated Database User

HITACHI

Please enter the Microsoft SQL Server administrative connection information:

Database server name: (local)

Administrator ID (case-sensitive): sa

Administrator password: •••••••

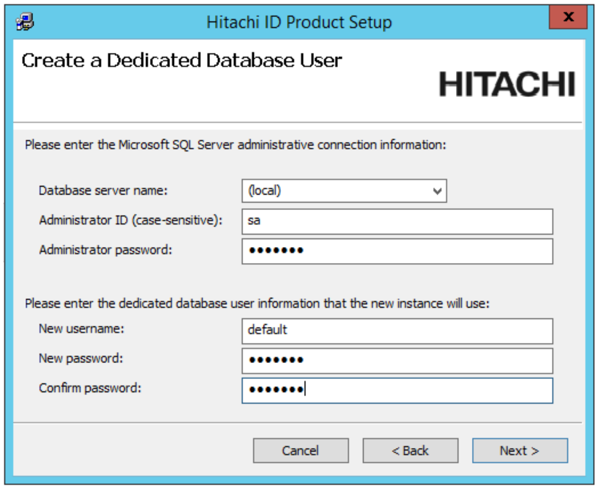
Please enter the dedicated database user information that the new instance will use:

New username: default

New password: •••••••

Confirm password: •••••••

8. Enter the database details.



Hitachi ID Product Setup

Create a Dedicated Database User

HITACHI

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:

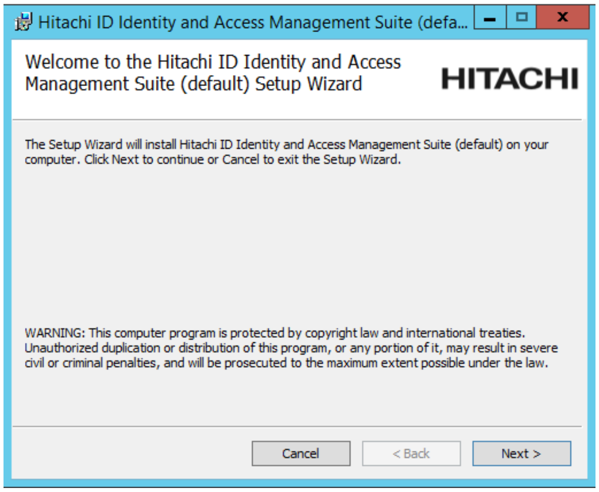
New username: default

New password: •••••••

Confirm password: •••••••

9. Click **Next**.

   The `setup` program creates the new database user and launches `idm.msi`.



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.

10. Click **Next**.

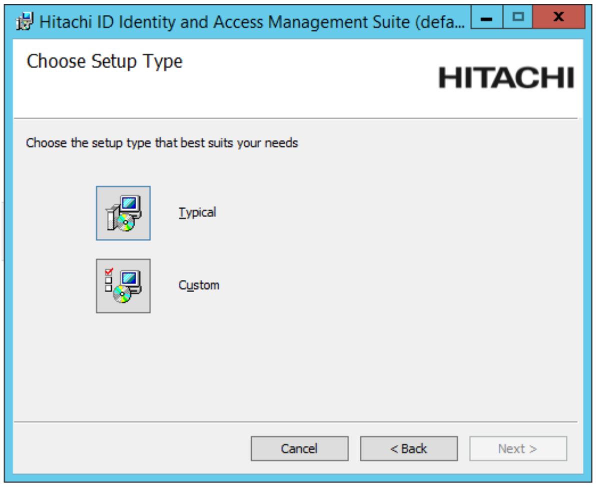
11. Read the license agreement, select the checkbox to accept it, then click **Next**.

    The installer automatically selects the license file located in the same directory as the MSI file.

12. Click **Next** to continue.

> **Note:** All of your replicated servers should use the same license file.

13. The installer displays setup types for you to select from.



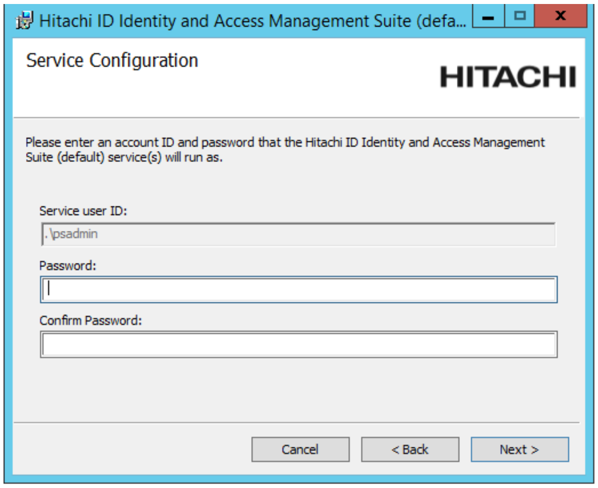
Hitachi ID Identity and Access Management Suite (defa...

Choose Setup Type

Choose the setup type that best suits your needs

14. Select **Typical** to install with default settings for file locations, ports, and web site.

> **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...

Service Configuration

HITACHI

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:

15. Enter the service user ID and password.

    The default is *psadmin*. If the account does not already exist, the installer will create it with the specified password. The password can be up to 64 characters long.

    This is the account *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 ID. The password can be up to 64 characters long.

    If you use the default *psadmin* account and the account does not already exist, the installer will create it with the specified password.

    Click **Next**.

16. Type the **communication key** that will be used to encrypt communication between the *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: If you lose track of this key, you can copy the `idmsetup.inf` file from <*instance*>\psconfig\ on the *Bravura Security Fabric* server to the same location as the installer. The installer will extract the communication key value from the file. Alternatively, you can use the `resetkey` program to reset it.

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

17. Click **Next**.

18. 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**.

19. 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.

    > **Note:** This key is not currently used in *Bravura Identity*-only licenses.

    Click **Next**.

20. 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**.

21. 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.

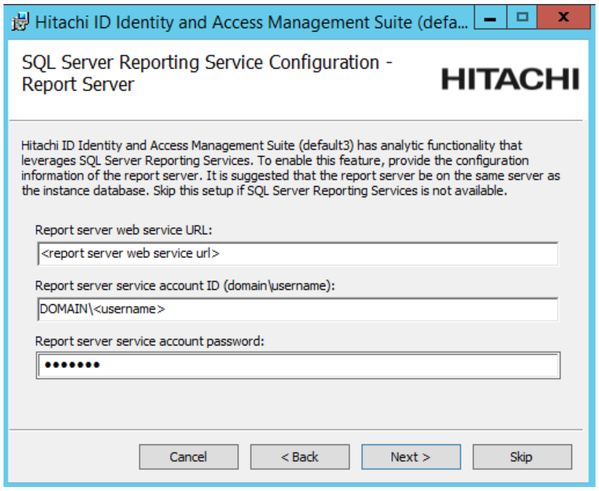
    Click **Next**.

22. If you want to install the *Analytics* app, configure options to connect with SQL Server Reporting Services (SSRS); proceed to Step 23

    You must have access to SQL Server Reporting Services to use this component.

    Click **Skip** if you do *not* want to install this component now; skip to Step 24.

    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`).



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>

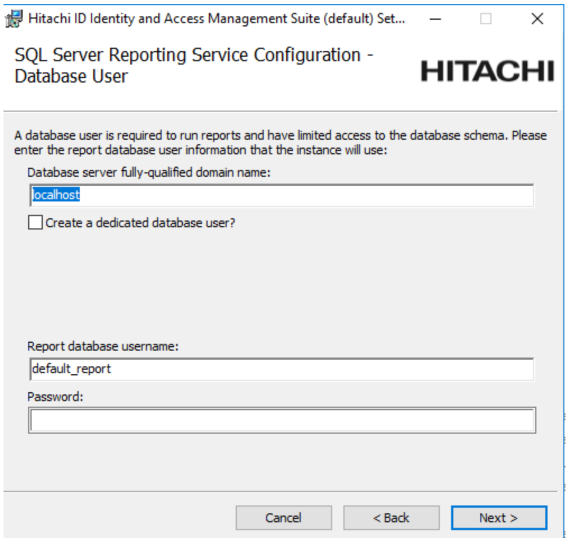
Report server service account password: •••••••

23. To configure the *Analytics* app connection to SSRS:

    (a) Enter the Report Servers web service URL.

    (b) Enter the SSRS service username and password.

    (c) Click **Next**.
    The ***SQL Server Reporting Service Configuration - Database User*** page is displayed.


Hitachi ID Identity and Access Management Suite (default) Set...
HITACHI
Cancel
< Back
Next >

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?

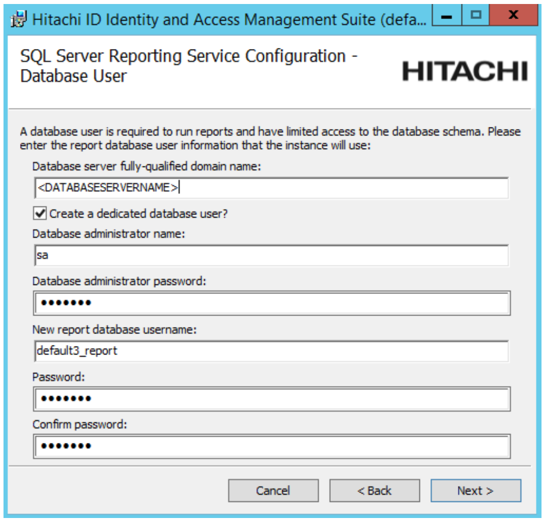
Report database username: default_report

Password:

    (d) Enter the name of server where your instance database resides.

    (e) Choose your report database user option.

    - 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.

- 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.

Click **Next**.

24. Type the login ID and password for the *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**.

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

26. Once *Bravura Security Fabric* is successfully installed, click **Finish** to start the post-installation tasks.

    CAUTION: Do not stop the post-installation tasks. The installer is loading connectors from the *Connector Pack*, language tags, and reports. As the *Connector Pack* is not installed yet you will receive a warning that the *Connector Pack* could not be loaded. This warning is safe to ignore at this time.

27. Click **Finish** to complete the installation.

    To validate the installation, open a browser and type `localhost/default`. The *Bravura Security Fabric* login page will be displayed.

    Note: The address above is composed of the host name and the virtual directory which is created using the instance name. If you installed a new instance called `passwords`, the address would be `localhost/passwords`.

2.1 idmsetup.inf

When you install *Hitachi ID Bravura Security Fabric* on the main server, an **`idmsetup.inf`** file is created in the \\<*instance*>\\psconfig\\ directory. You can use the file to aid in the installation of proxy servers, backup servers, and add-on software. It is a recommended best practice to use this file during migration projects. It acts as an "answer file" for the installer, by populating instance specific configuration parameters and encryption keys at every step during the setup process.

See also:

- INSTALLATION TOOLS in the Bravura Security Fabric *Reference Manual* for information about command-line tools and configuration files, including how to script the installer for silent installations.

3 Connector Pack

Connectors are programs that enable software to integrate with target systems. The Hitachi ID Systems *Hitachi ID Connector Pack* is released independently from the *Hitachi ID Bravura Security Fabric* software.

The *Connector Pack* can be implemented as either a global *Connector Pack* or an instance-specific *Connector Pack*. The global *Connector Pack* only needs to be installed once per machine. All instances of the *Bravura Security Fabric* running on that machine can share the same global *Connector Pack*. The instance-specific *Connector Pack* installs directly into and is only used by the specified instance.

Bravura Security Fabric uses connectors, also referred to as *agents*, to perform operations on a target system. Connectors also allow *Bravura Security Fabric* to set or validate passwords or other authenticators on a target system. The connectors also harvest information about accounts from target systems during the auto discovery process.

Connectors may include:

- An *agent* binary located in the *Bravura Security Fabric* instance's agent directory. Product administrators can use their process names to troubleshoot functionality by finding them in *Bravura Security Fabric* logs or the Windows' list of running processes.
- Any libraries used by the agent. This may include libraries in CommonFiles\\Hitachi-ID, Windows or VisualC++ libraries and the various target libraries, SDKs, Python interpreter, and so on.
- In some cases, such as Unix systems, a listener installed on the target system.

Each connector is designed to target a specific type of system; for example, the Active Directory connector (**`agtaddn`**) is used to interact with an Active Directory system. Some connectors, such as the flexible SSH connector (**`agtssh`**), require a script to define interaction between *Bravura Security Fabric* and the target system.

Connectors are installed on the *Bravura Security Fabric* server itself (in the agent directory) and use a remote administration software protocol understood by the target system. For some target systems, such as RSA Access Manager and SAP, client software must be installed on the *Bravura Security Fabric* server.

The individual actions that connectors take on a target system are referred to as connector *operations*. Note that not all target systems are capable of supporting all connector operations, and that some operations are not yet available through the *Bravura Security Fabric* web interface. See Connector Operations in the *Connector Pack Integration Guide* for a full list and explanation of each connector operation.

See also:

See the Connector Pack Integration Guide for details about *Hitachi ID Connector Pack*.

4 Use case: Installing a Connector Pack

This use case shows you how to install an instance-specific *Hitachi ID Connector Pack*.

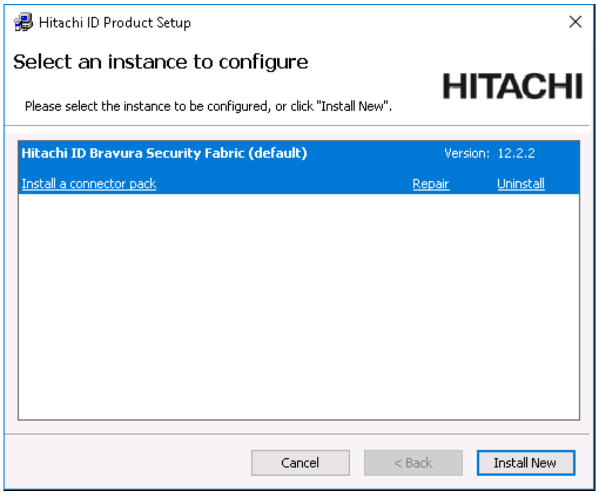
Requirements

This use case assumes:

- You have already installed *Hitachi ID Bravura Security Fabric*.
- You are logged into your Windows server with elevated privileges (administrator).

Run setup

1. Navigate to the folder containing the setup program for *Hitachi ID Bravura Security Fabric*.
2. Double-click **`setup`** to start the setup wizard.
   In this case, you should see that *Bravura Security Fabric* is already installed.
3. Select your instance so that the installer displays options, and click **Install a connector pack**.

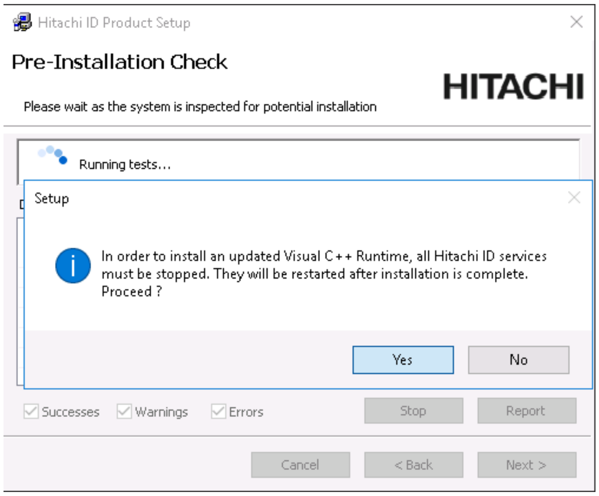
   Select an instance to configure

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

   Selecting this option installs an instance-specific connector pack. In order to select a global connector pack, you would click **Install new** to see that option.
4. Choose **Connector Pack 64-bit**

5. Click **Next**.

   A Setup confirmation message appears: `In order to install an updated Visual C++ Runtime, all Hitachi ID services must be stopped.  They will be restarted after installation is complete.  Proceed?`



Hitachi ID Product Setup

Pre-Installation Check

Please wait as the system is inspected for potential installation

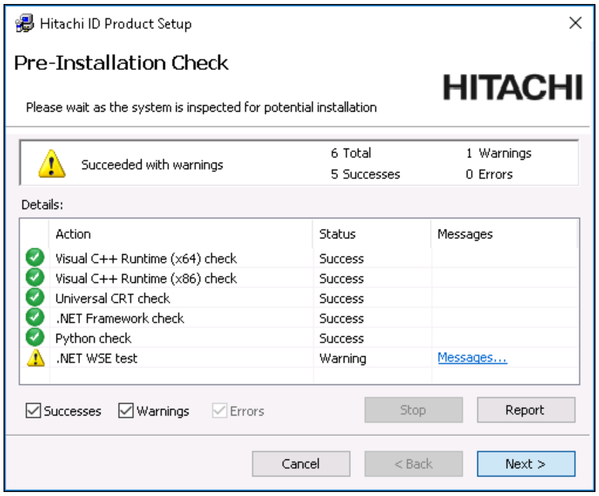
Running tests…

Setup

In order to install an updated Visual C++ Runtime, all Hitachi ID services must be stopped. They will be restarted after installation is complete. Proceed ?

6. Click **Yes**.

   The **`setup`** program performs a pre-installation check. There should be no errors. A warning may be shown for some components, such as .NET WSE test, that are required for certain target systems, such as SOAP applications. This would only be a concern if you are planning on targeting those systems. The installation can proceed without it.



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

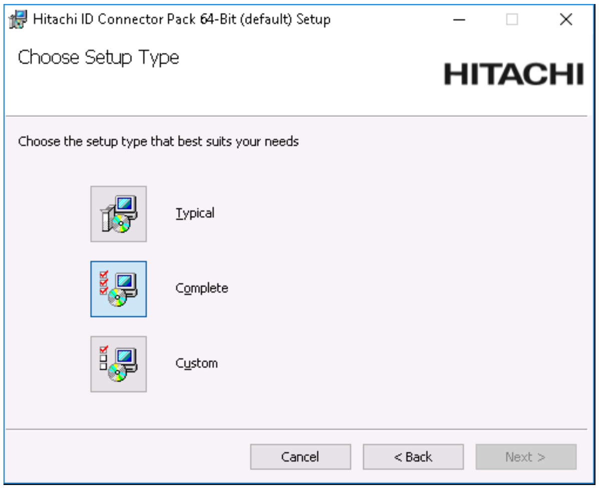
Details:

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…

7. Click **Next**.

8. Click **Next** to start the setup wizard.

9. Select the **I accept the terms in the License Agreement** checkbox, then click **Next**.



Choose Setup Type

Choose the setup type that best suits your needs

10. Click **Complete**.

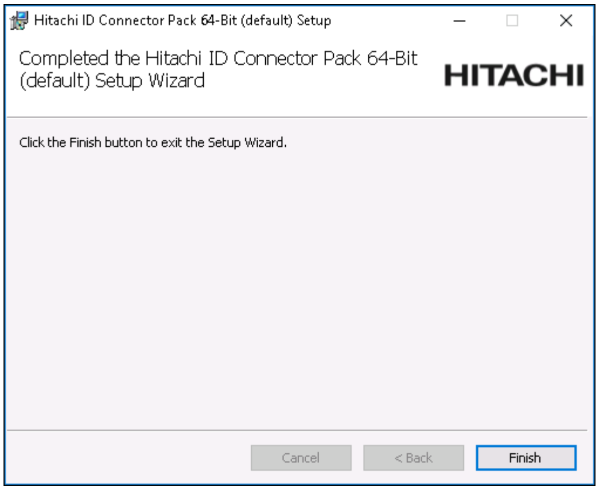
> **Note:** In test, development and production environments, it is recommended that you choose **Complete** and install all of the connectors. This is so that if you were to add a new system later on you already have the connector installed.

11. Click **Install**.

    You may be notified that the system will need to reboot to complete the installation. If you do, click **OK** to continue.

    After a period of time, the installation should complete.

12. Click **Finish**.



Completed the Hitachi ID Connector Pack 64-Bit (default) Setup Wizard

Click the Finish button to exit the Setup Wizard.

    The installer will take some time to complete all of the installation tasks.

13. Click **Finish** when prompted to complete the installation.

5 Troubleshooting

5.1 Security policy pre-installation check fails

The pre-installation check reports that the “Security Policy check” fails if the Windows option **Default owner for objects created by members of the Administrators group** is not set to **Administrators groups**. This setting is located in **Administrative Tools** → **Local Security Policy** → **Security Settings** → **Local policies** → **Security options**.

To work around this issue:

1. Create a user called `psadmin` as part of the Administrators group, with the **Password never expires** setting.
2. Log into the Windows server and install *Hitachi ID Bravura Security Fabric* as the psadmin user.

5.2 Database connectivity pre-installation check fails

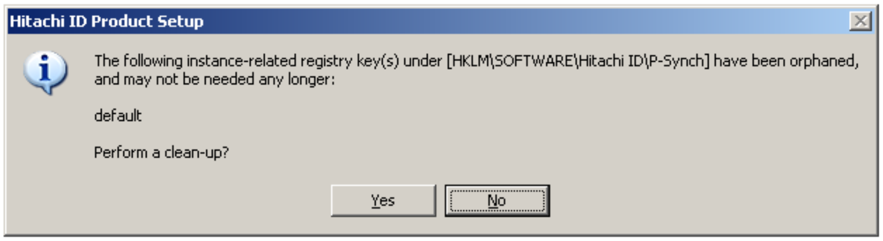
The pre-installation check reports that “Database connectivity” fails if it cannot detect the appropriate Microsoft SQL Server client software. To correct this issue, see Installing database and database client software to learn how to set up your back end database and client software.

If the pre-installation check still fails, check your PATH environment variable. For example, if you have installed the SQL Server Express client, PATH should contain:

```
C:\Program Files\Microsoft SQL Server\90\Tools\binn\
```

5.3 Setup detects orphaned instances

If the **`setup`** program detects that there are registry entries for improperly installed or uninstalled instances on the current server, it displays a dialog:



Hitachi ID Product Setup

The following instance-related registry key(s) under [HKLM\SOFTWARE\Hitachi ID\P-Synch] have been orphaned, and may not be needed any longer:

default

Perform a clean-up?

where `default` is the orphaned instance name. Click **Yes** if you want to remove the registry entries for the orphaned instance.

Connector Pack check fails

Hitachi ID Bravura Security Fabric needs a valid *Hitachi ID Connector Pack* before it can manage any systems. If the **`setup`** program does not detect an installed *Connector Pack*, then a warning ⚠ appears next to the *Connector Pack* check during the pre-installation check.

Click **Messages...** to view the details of the warning, which includes the minimum *Connector Pack* version required for the product you are installing.

After you finish installing all instances of *Bravura Security Fabric*, you should install the *Connector Pack*. See the Connector Pack Integration Guide for details on global and instance-specific *Connector Pack*s.