

# ***Bravura Security Fabric***

---

## **Upgrade Reference Manual**

- |                                     |                                     |
|-------------------------------------|-------------------------------------|
| <input checked="" type="checkbox"/> | <b>Hitachi ID Bravura Pass</b>      |
| <input checked="" type="checkbox"/> | <b>Hitachi ID Bravura Privilege</b> |
| <input checked="" type="checkbox"/> | <b>Hitachi ID Bravura Identity</b>  |
| <input checked="" type="checkbox"/> | <b>Hitachi ID Bravura Group</b>     |

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

# Contents

<b>I</b>	<b>INTRODUCTION</b>	<b>1</b>
<b>1</b>	<b>About the Documentation</b>	<b>2</b>
1.1	This document . . . . .	2
1.2	Conventions . . . . .	3
1.3	Feedback and help . . . . .	3
<b>2</b>	<b>About Upgrades</b>	<b>4</b>
2.1	Use cases . . . . .	4
2.1.1	Patch use case . . . . .	4
2.1.2	Upgrade use cases . . . . .	4
2.2	Component compatibility . . . . .	6
2.3	Interceptor compatibility . . . . .	6
2.4	Login Assistant compatibility . . . . .	7
2.5	Connector pack compatibility . . . . .	8
<b>II</b>	<b>PREPARATION</b>	<b>9</b>
<b>3</b>	<b>Research and Analysis</b>	<b>10</b>
3.1	Taking inventory . . . . .	10
3.2	Product considerations . . . . .	11
3.2.1	Databases . . . . .	12
3.2.2	Analytics . . . . .	13
3.2.3	Replication configuration . . . . .	13
3.2.4	Scripts, plugins, and configuration files . . . . .	14
3.2.5	Services . . . . .	15

3.2.6	Reports . . . . .	15
3.2.7	Product customizations and fixes . . . . .	15
3.2.8	Client tools . . . . .	16
3.2.9	Web interface modifications . . . . .	16
3.2.10	Language packs . . . . .	17
3.2.11	Supporting systems . . . . .	17
3.2.12	Python . . . . .	17
3.2.13	Connector pack compatibility . . . . .	17
3.2.14	Hitachi ID Mobile Access applications . . . . .	18
3.2.15	Proxy Servers . . . . .	18
3.2.16	Release notes . . . . .	18
3.2.17	Operating system updates . . . . .	18
3.2.18	Product password . . . . .	18
3.2.19	<i>Bravura Privilege</i> . . . . .	19
<b>4</b>	<b>Planning</b>	<b>20</b>
4.1	Test plan . . . . .	20
4.2	Production change control plan . . . . .	22
4.3	Communications plan . . . . .	22
<b>III</b>	<b>UPGRADING</b>	<b>23</b>
<b>5</b>	<b>Upgrading an Instance Using Setup</b>	<b>24</b>
5.1	Preparation . . . . .	24
5.2	Upgrade using installer . . . . .	28
5.2.1	SSRS settings . . . . .	32
5.2.2	Completing the upgrade process . . . . .	33
5.3	Troubleshooting . . . . .	34
5.4	Post upgrade . . . . .	35
5.4.1	Post upgrade steps . . . . .	35
5.4.2	Additional steps to consider . . . . .	37
5.4.3	Verifying the upgrade . . . . .	37
5.4.4	Remove old installation files . . . . .	38

5.4.5	Post upgrade notes . . . . .	38
<b>6</b>	<b>Upgrading Connector Pack</b>	<b>41</b>
<b>7</b>	<b>Upgrading Local Workstation Service software</b>	<b>43</b>
<b>8</b>	<b>Upgrading Guacamole</b>	<b>44</b>
<b>9</b>	<b>Upgrading the Login Assistant Software</b>	<b>45</b>
9.1	Running the installer . . . . .	45
9.2	Command line upgrade . . . . .	51
<b>10</b>	<b>Upgrading the Proxy Server</b>	<b>52</b>
<b>11</b>	<b>Upgrading components</b>	<b>54</b>
<b>IV</b>	<b>UTILITY REFERENCE</b>	<b>56</b>
<b>12</b>	<b>getfileinfo</b>	<b>57</b>
<b>13</b>	<b>instdump</b>	<b>58</b>
<b>14</b>	<b>loadplatform</b>	<b>60</b>
14.1	Requirements . . . . .	60
14.2	Usage . . . . .	61
14.2.1	Examples . . . . .	61
14.3	Loading a new scripted target system type . . . . .	62
14.4	Loading a new platform category . . . . .	63
14.5	Loading default attributes . . . . .	64
14.6	Loading a new or modified discovery template . . . . .	64
<b>15</b>	<b>migratedata</b>	<b>66</b>
15.1	Prerequisites for the older version . . . . .	66
15.2	Prerequisites for the current version . . . . .	67
15.3	Data migration process . . . . .	68
15.3.1	Exporting data from the older (source) version . . . . .	68
15.3.2	Importing data to the current (destination) version . . . . .	70

- 15.4 Items to verify after the data migration . . . . . 72
- 16 upgradetest 75
  - 16.1 Usage . . . . . 75
  - 16.2 Examples . . . . . 75
- A File Locations 77
  - A.1 Bravura Security Fabric directories and files . . . . . 77
    - A.1.1 Instance directory . . . . . 78
    - A.1.2 Log directory . . . . . 80
    - A.1.3 Locks directory . . . . . 81
  - A.2 Connector pack directories and files . . . . . 82

## **Part I**

# **INTRODUCTION**

# About the Documentation

---

# 1

## 1.1 This document

This document shows you:

- How to *upgrade* an existing instance of *Hitachi ID Bravura Security Fabric* by using the **setup** program.
- How to apply a same-version, no-data-loss *patch* when Hitachi ID Systems developers provide custom fixes or enhancements.

[About Upgrades](#) [About Upgrades](#) explains the use cases for an upgrade or patch, compared to a more complicated migration, which involves manual steps of migrating from one instance to another.

[Research and Analysis](#) [Research and Analysis](#) describes important information that you need to gather, and analysis that is crucial before starting an upgrade or patch.

[Planning](#) [Planning](#) provides an outline for planning the upgrade or patch.

While the upgrade process is relatively simple, it is recommended that you read these chapters fully and from the beginning.

[getfileinfo](#) to [upgradetest](#) provide detailed usage information on utilities that are commonly used during upgrading.

This guide compliments the [Bravura Security Fabric Documentation](#) and the *Bravura Security Fabric Reference Manual* shipped with the latest version of *Bravura Security Fabric*.

**Note:** This document may be updated after a release, after migrations have been carried out. Check the Hitachi ID Systems portal or contact [support@Hitachi-ID.com](mailto:support@Hitachi-ID.com) for the latest version.

## 1.2 Conventions

This document uses the following conventions:

This information ...	displayed in ...
Variable text (substituted for your own text)	<code>&lt;angle brackets&gt;</code>
Non-text keystrokes – for example, <b>[Enter]</b> key on a keyboard.	<b>[brackets]</b>
Terms unique to <i>Hitachi ID Bravura Security Fabric</i>	<i>italics</i>
Button names, text fields, and menu items	<b>boldface</b>
Web pages (names)	<b><i>italics and boldface</i></b>
Literal text, as typed into configuration files, batch files, command prompts, and data entry fields	monospace font
Wrapped lines of literal text (indicated by the → character)	Write this string as a →single line of text.
Hypertext links – click the link to jump to a section in this document or a web site	Purple text
External document – click the link to jump to a section in another document. The links only work if the documents are kept in the relative directory path.	Magenta text

## 1.3 Feedback and help

If you have feedback about this document or wish to report an omission or error, please contact [doc-feedback@Hitachi-ID.com](mailto:doc-feedback@Hitachi-ID.com).

If you require technical assistance with *Hitachi ID Bravura Security Fabric*, contact [support@Hitachi-ID.com](mailto:support@Hitachi-ID.com).



# About Upgrades

# 2

## Terminology

This document uses the following terms:

**Patch** replacing or modifying existing files when Hitachi ID Systems provides fixes or enhancements.

**Upgrade** deploying a newer version of *Bravura Security Fabric* in place of an older version using **setup**. In the **setup** program and in this document, the term *upgrade* can also refer to *patch*.

**Manual Upgrade** involves a manual process such as migration of data from old servers to new servers at the same time as the upgrade.

**Migration** copying configuration files and raw data from one instance to another. For information about the migration process, see the *Bravura Security Fabric* Migration Reference Manual

This document is about the process for supported versions of *Hitachi ID Bravura Security Fabric*. To check the latest support status see:

<https://hitachi-id.com/support/support-for-older-releases.html>.

## 2.1 Use cases

The following outlines cases for patching, upgrading. If you are unsure which method you should use, contact [support@Hitachi-ID.com](mailto:support@Hitachi-ID.com) for advice.

### 2.1.1 Patch use case

Hitachi ID Systems may provide a customer with a same-version, no-data-loss patch. Installing an in-place patch provides fixes and minor enhancements and is usually achieved by running **setup**, but may include some manual steps. After installing a patch the build number will be updated.

### 2.1.2 Upgrade use cases

#### 2.1.2.1 Upgrade using setup

An upgrade using **setup** is usually sufficient to take advantage of feature improvements and performance enhancements in a newer version. Completing an upgrade is much easier than carrying out a migration.

You still need to be concerned with issues such as a compatibility of plug-ins, custom binaries or other customization; however the work on the databases is done by **setup**.

### 2.1.2.2 Manual upgrade

There may be situations where the upgrade involves a migration of data from old servers to new servers at the same time as the upgrade. A *manual upgrade* is recommended where:

- If you have a lot of customizations
- If you are upgrading your hardware at the same time
- If you are upgrading from a non-supported version of the product
- Your upgrade is going to be complicated

A manual upgrade ensures the current production version of *Hitachi ID Bravura Security Fabric* remains available as long as possible during the change of versions.

When performing a manual upgrade, you must install a second instance that will become the new version. Then you can manually copy or migrate configuration files and data from the databases to this new version instance.

It is possible to perform a manual upgrade on a single server. The only limitations are that the second instance – the new version – must have a unique instance name and all the port numbers of the services for the second instance must be changed from their default values. Thus, you will need to modify any configuration parameters that contain the instance name or port numbers. This includes both the *Bravura Security Fabric* server, targets with local agents, or transparent password synchronization triggers, and clients with *Bravura Security Fabric* components. It is recommended that you use two servers to perform all manual migrations to avoid these complications.

Manual upgrades, including those that are migrating to a new instance at the same time, involve many complex components that require an in-depth knowledge of *Bravura Security Fabric*. It is highly recommended you contact [support@Hitachi-ID.com](mailto:support@Hitachi-ID.com) for assistance.

See the *Bravura Security Fabric* Migration Reference Manual (**migration.pdf**) to achieve this outcome.

## 2.2 Component compatibility

During the upgrade process, new component functionality is made available with automated upgrade to the components.

Updates to the components can include:

- New policies
- Updates to policy tables in *Manage external data store* (DBE) module
- Updates to configuration objects
- Deprecation in favor of new components
- Updates to static HTML files
- Updates to configured *Hitachi ID Bravura Security Fabric* objects

See [Upgrading components](#) for notes about possible issues.

## 2.3 Interceptor compatibility

Below is a compatibility matrix that should be taken into consideration when upgrading *Hitachi ID Bravura Pass* services (**idpm/pushpass**) or interceptors. **Y** denotes that the versions are compatible and **N** denotes that the versions are not compatible.

Table 2.1: *Bravura Pass* interceptor compatibility

Interceptor version	Service version						
	10.0.x	10.1.x	11.0.x	11.1.x	12.0.x	12.1.x	12.2.x
6.4.9	Y	Y	Y	Y	Y	Y	Y
7.3.1	Y	Y	Y	Y	Y	Y	Y
8.2.8	Y	Y	Y	Y	Y	Y	Y
9.0.x	Y	Y	Y	Y	Y	Y	Y
10.0.x	Y	Y	Y	Y	Y	Y	Y
10.1.x	Y	Y	Y	Y	Y	Y	Y
11.0.x	Y	Y	Y	Y	Y	Y	Y
11.1.x	Y	Y	Y	Y	Y	Y	Y

Table 2.1: *Bravura Pass* interceptor compatibility (Continued)

Interceptor version	Service version						
	10.0.x	10.1.x	11.0.x	11.1.x	12.0.x	12.1.x	12.2.x

... continued on next page

12.0.x	Y	Y	Y	Y	Y	Y	Y
12.1.x	Y	Y	Y	Y	Y	Y	Y
12.2.x	Y	Y	Y	Y	Y	Y	Y
CP 3.0.x (unix)	Y	N	N	Y	Y	Y	Y
CP 3.1.x (unix)	Y	N	N	Y	Y	Y	Y
CP 3.2.x (unix)	Y	Y	Y	Y	Y	Y	Y
CP 3.3.x (unix)	Y	Y	Y	Y	Y	Y	Y
CP 4.0.x (unix)	Y	Y	Y	Y	Y	Y	Y
CP 4.1.x (unix)	Y	Y	Y	Y	Y	Y	Y

Also review the access control list for the **Comma-delimited list of IP addresses with CIDR bitmask that are allowed to send socket requests** setting for the Password Manager service (idpm). Password synchronization interceptors that need to access **idpm** must be defined in this field.

For more information about Password Manager service see [Password Manager Service \(idpm\)](#).

## 2.4 Login Assistant compatibility

Below is a compatibility matrix that should be taken into consideration when upgrading *Hitachi ID Bravura Pass* as well as *Login Assistant* on the workstations.

**Y** denotes that the versions are compatible and **N** denotes that the versions are not compatible.

Table 2.2: *Bravura Pass* Login Assistant compatibility

Instance version	Login Assistant version									
	7.3.1	8.2.8	9.0.6	10.0.x	10.1.x	11.0.x	11.1.x	12.0.x	12.1.x	12.2.x
12.2.x	N	N	N	N	Y	Y	Y	Y	Y	Y

## 2.5 Connector pack compatibility

Table 2.3: *Connector Pack* compatibility

Instance version	Connector Pack version									
	3.0.x	3.1.x	3.2.x	3.3.0	3.3.1	3.3.2	4.0.0	4.0.1	4.0.2	4.1.x
10.1.x	N	N	Y	Y	Y	Y	Y	Y	Y	Y
11.0.x	N	N	N	Y	Y	Y	Y	Y	Y	Y
11.1.x	N	N	N	N	Y	Y	Y	Y	Y	Y
12.0.x	N	N	N	N	N	N	Y	Y	Y	Y
12.1.x	N	N	N	N	N	N	N	N	Y	Y
12.2.x	N	N	N	N	N	N	N	N	N	Y

The format in which the *Connector Pack* gathers information by each connector during auto discovery has been modified for *Connector Pack* 3.2.0 and *Bravura Security Fabric* 10.1.0 to support a new listing format when listing users, accounts, groups, group memberships, servers, and subscribers.

See <https://docs.hitachi-id.net/#/home/4198/10/11> for the formats used for the list files generated during auto discovery.

When planning an upgrade to *Bravura Security Fabric* 12.2.4, it is recommended you uninstall the previous *Connector Pack* and then install *Connector Pack* 4.1.5.

See:

- [Upgrade using installer](#) for more information on upgrading *Bravura Security Fabric*
- [Upgrading Connector Pack](#) for specific connector pack upgrade information

## **Part II**

# **PREPARATION**

# Research and Analysis

# 3

Before you start, gather information about your environment to ensure the feasibility of an upgrade and to help you plan the change.

Your research and analysis should include:

- An inventory of affected systems and installed *Hitachi ID Bravura Security Fabric* components
- An analysis of *Bravura Security Fabric* configuration and files, including customizations

## 3.1 Taking inventory

Carry out a complete inventory of potentially affected systems to determine the location of all *Hitachi ID Bravura Security Fabric* components that need to be upgraded, including:

- ☐ *Bravura Security Fabric* servers
  - ☐ Primary server
  - ☐ Replica servers
  - ☐ Proxy servers
- ☐ Target systems
  - ☐ Targets with listeners, such as, Unix, OS/390 mainframe
  - ☐ Targets with transparent password synchronization triggers, such as, Windows, LDAP Directory Service, Unix, OS/390, IBM OS/400
- ☐ Managed resources – Local service installations
- ☐ Systems that have *Bravura Security Fabric* software components installed on them. Examples include:
  - ☐ *Bravura Security Fabric* API installations
  - ☐ Local Kiosk software installed on user workstations and laptops
  - ☐ Domain Kiosk software installed on domain netlogon shares, called from domain policies
  - ☐ GINA or Credential Provider software installed on user workstations
  - ☐ Password expiry client or notification client software installed on domain netlogon shares
  - ☐ Password Manager Local Reset Extension installed on user workstations
  - ☐ Lotus Notes Extension DLL installed on user workstations
- ☐ Other technologies that support *Bravura Security Fabric*
  - ☐ Network load balancers deployed for high availability and/or redundancy

- ☐ Reverse web proxy servers to expose the user interface to other networks
- ☐ Backup servers for disaster recovery

## 3.2 Product considerations

Carefully analyze configuration parameters and files to determine what will be affected. Consider the following:

- ☐ Databases
- ☐ Analytics
- ☐ Replication configuration
- ☐ Scripts, plugins, and configuration files
- ☐ Services
- ☐ Reports
- ☐ Product customizations and fixes
- ☐ Client tools
- ☐ Web interface modifications
- ☐ Language packs
- ☐ Supporting systems
- ☐ Python
- ☐ Connector pack compatibility
- ☐ Hitachi ID Mobile Access applications
- ☐ Proxy Servers
- ☐ Release notes
- ☐ Operating system updates
- ☐ Product password
- ☐ *Bravura Privilege*



### 3.2.1 Databases

Each significant version of Hitachi ID Systems software is likely to have different requirements for its database tables, table schema or data encoding.

*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.

Upgrades are not supported for SQL Server Express.

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.

#### 3.2.1.1 Check available database space

If the upgrade will change the instance's database schema, verify there is at least two and half times the total database size free on each database server where the temp.db files are stored, for example:

1. Using MSSQL Management Studio check the size of the database file(s).
2. In Windows Explorer, look at the free space available where the temp.db file(s) are located.
3. If the free space is less than two and half times the size of the database, allocate more disk space. Failure to do so may result in the installer failing to update the database schema.

## 3.2.2 Analytics

If you are installing the new *Analytics* app feature as part of the upgrade you must install Microsoft's SQL Reporting Services.

After installing Microsoft's SQL Reporting Services 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

See the Reports User Guide ([reports.pdf](#)) for more information on this feature.

## 3.2.3 Replication configuration

Establish a window of time to perform the upgrade when all replication nodes can be offline. Before performing an upgrade, you need to stop services, except the logging service, on all replication nodes, then upgrade each node. During an upgrade, **setup** automatically starts services. Ensure that you stop them again until all nodes have been upgraded. This prevents data and files from becoming unsynchronized.

In shared schema or hybrid replication one or more application servers (nodes) using the same backend database. All application nodes using the same backend database are collectively referred to as a single database node.

- If backups can be created and the restore process has been previously tested and proven reliable in your environment, it is safe to begin patching with the primary node.
- If backups can not be created or the restore process has not been reliably tested, begin by patching the least critical node.
- Backups must be performed on all application nodes before the patch or upgrade is applied on any of the nodes.

If hybrid database replication is used:

- All application nodes that are using the same database as backend have to be patched at the same time, or as close to each other as possible, or;
- Only one application node must be patched per database node. The other application nodes will get their changes through file replication .

**Note:** File and registry replication behaves, and is implemented differently than database replication, however, neither process provides notification in the WebUI when the process has ended. Check the log file of the target node(s) to determine when the process ends.

**CAUTION:** Hitachi ID Suite file synchronization *must not* be triggered from the time the patching process starts until all nodes are patched (automatic file replication from the primary is disabled) and file replication can resume.

### 3.2.4 Scripts, plugins, and configuration files

When configuring Hitachi ID software, various files may have been added or modified in order to implement various features or customizations.

Carefully analyze and test all scripts, plugins, and configuration files; for example:

- Customized auto discovery scripts
- Target integration configuration files
- External interface program configuration files
- Plugin scripts
- Language and user interface modifications
- Customized password strength dictionary file
- Filters
- Access controls, including user classes
- Service configuration

Note the following for custom scripts, plugins, and configuration files:

- The directory structure may have changed between versions; verify any hard-coded directory PATH details. See [File Locations](#) for current file locations.
- The names of *Hitachi ID Bravura Security Fabric* programs may have changed; verify all references to those programs.
- The command line usage of *Bravura Security Fabric* programs may have changed; verify all arguments being passed into those programs.
- Scripts written in the PSLANG language are being migrated to Python scripts. You may want to examine any scripts to determine if new build-in functions or versions written in Python are available to optimize your code.

- The capability of connectors and external interface programs may have been enhanced (possibly by changes to the target address line or additional options in its configuration file); you may need to review your integrations to reflect those changes.
- New built-in connectors may have been written for integrations you previously scripted using flexible connectors; you may want to re-implement those targets using the new connector.
- Multiple connectors may have been consolidated into a single connector (for example, the Domino and Lotus Notes connectors were combined in connector pack 1.3); you will need to redo any integrations using either of those connectors.
- If you have your own compiled binaries for custom interfaces, plugins or authentication chains, you must recompile them as 64-bit.
- Changes to wfreq plugins as of 12.0.0 mean almost any custom wfreq extensions likely need to be re-written or have logic changed to meet new restrictions on when the plugin runs.
- Custom loadadb or idtrack scripts written prior to 12.0.0 should be tested. Care has been taken to maintain backwards compatibility but some edge cases may not work or require refactoring; for example, differential listing works differently to older versions.

### 3.2.5 Services

After an upgrade, service configuration is reset to the default. If you have set the startup type of a service (for example, if you have set a service to delayed start), this change must be made again after upgrading.

### 3.2.6 Reports

Reports in *Hitachi ID Bravura Security Fabric* version earlier than 9.0 were saved as flat files. In 9.0 or later they are SQLite databases. Saved reports will not be preserved when upgrading from earlier versions. After the upgrade, scheduled reports can be viewed on the **Manage the system** → **Maintenance** → **Scheduled jobs** page, but cannot be run or modified.

### 3.2.7 Product customizations and fixes

In addition to configuration files, it is possible that your *Hitachi ID Bravura Security Fabric* instance may contain custom binaries and/or schema. These could include web modules, connectors, plugin programs, external interface programs, and so on.

Identify custom binaries by right clicking the binary in Windows Explorer and check the versions tab. Alternatively you can check it using the [getfileinfo](#) program (p57).

Once custom binaries are identified, the purpose for them should be determined in order to decide whether they are still necessary. For example, if the custom binary was created to resolve a product deficit, it is likely the deficit was resolved in the base product. Similarly, if the purpose for the binary was to add custom functionality, it is also possible that feature was added to the base product.

Read the release notes to determine whether a custom binary is necessary, or list all the binary versions by running the following command from each of the folders below:

```
for
%i in (*.exe) do (%~ni -v>>versions.txt & echo %~ni>>versions.txt)
```

- <Program Files path>\Hitachi ID\IDM Suite\<instance>\agent
- <Program Files path>\Hitachi ID\IDM Suite\<instance>\cgi-bin
- <Program Files path>\Hitachi ID\IDM Suite\<instance>\interface
- <Program Files path>\Hitachi ID\IDM Suite\<instance>\lib
- <Program Files path>\Hitachi ID\IDM Suite\<instance>\report
- <Program Files path>\Hitachi ID\IDM Suite\<instance>\service
- <Program Files path>\Hitachi ID\IDM Suite\<instance>\util

If it is still not obvious, contact [support@Hitachi-ID.com](mailto:support@Hitachi-ID.com) for assistance.

Only in very specific cases will an older binary be usable in a newer product. A previous service engagement or product fixes on an existing instance (including binary and/or schema) might require assistance from Support to either initiate a new service engagement, verify the fixes provided in a previous release, or indicate new feature/functionality that supersedes fixes in older functionality.

### 3.2.8 Client tools

As of 9.0, *Bravura Security Fabric* is completely 64-bit, so it requires any target tools (for example database clients, SDKs or any software our product loads directly in order to integrate with targets), to also be installed as 64-bit versions. This means that for fresh installs (including replication migrations), the 64-bit clients must be installed, and for cloned migration, the 32-bit clients must be uninstalled, and the 64-bit client installed. Refer to the Connector Pack Integration Guide for details on any targets which require the use of target clients or tools.

### 3.2.9 Web interface modifications

All custom web interface modifications should be reviewed. Some existing modifications will require modification or deletion, while new modifications may need to be added.

The best method to address this issue is to go through every file in the custom directory in the source instance and confirm the same file exists in the destination instance src directory. If a file does not exist in the new instance, the custom version of the file can probably be deleted. If a file does exist, go through the entire file and search for each tag or KVGroup in the new instance. If the tag or KVGroup does not exist, it can probably be deleted from the file. If it does exist, compare the custom version to the default version in the new instance and figure out what if any modification will need to be made to the custom version.

Finally, test all the web pages and verify that the desired modifications have been migrated properly. Also look for new web interface constructs that may require new modifications.

See the [Bravura Security Fabric Documentation](#) for more information.

### 3.2.10 Language packs

Check the Hitachi ID Systems portal or contact [support@Hitachi-ID.com](mailto:support@Hitachi-ID.com) to find out what language packs are available for the new version. The lack of a language pack might cause delays in the migration project if it does not yet exist.

### 3.2.11 Supporting systems

As mentioned in [Taking inventory](#), there are a number of potentially related supporting systems to consider in addition to the *Bravura Security Fabric* servers themselves. These systems fall into two categories; systems with *Bravura Security Fabric* software components installed on them, and other technologies that support the *Bravura Security Fabric* server.

### 3.2.12 Python

Verify the minimum Python requirements for the upgrade. The latest *Bravura Security Fabric* requires Python 3.7.3+ 64-bit. Python must be installed for all users.

The upgrade in support to Python 3.7 as of *Bravura Security Fabric* 12.0.0 may cause issues with some scripts.

### 3.2.13 Connector pack compatibility

Table 3.1: *Connector Pack* compatibility

Instance version	Connector Pack version									
	3.0.x	3.1.x	3.2.x	3.3.0	3.3.1	3.3.2	4.0.0	4.0.1	4.0.2	4.1.x
10.1.x	N	N	Y	Y	Y	Y	Y	Y	Y	Y
11.0.x	N	N	N	Y	Y	Y	Y	Y	Y	Y
11.1.x	N	N	N	N	Y	Y	Y	Y	Y	Y
12.0.x	N	N	N	N	N	N	Y	Y	Y	Y
12.1.x	N	N	N	N	N	N	N	N	Y	Y
12.2.x	N	N	N	N	N	N	N	N	N	Y

The format in which the *Connector Pack* gathers information by each connector during auto discovery has been modified for *Connector Pack* 3.2.0 and *Bravura Security Fabric* 10.1.0 to support a new listing format when listing users, accounts, groups, group memberships, servers, and subscribers.

See "Auto Discovery" in the [Bravura Security Fabric Documentation](#) for the formats used for the list files generated during auto discovery.

When planning an upgrade to *Bravura Security Fabric* 12.2.4, it is recommended to do one of the following:

- Upgrade the *Connector Pack* to 4.1.5 prior to upgrading *Bravura Security Fabric*.
- Uninstall the *Connector Pack* and then install *Connector Pack* 4.1.5. This step is required if the *Connector Pack* is prior to 3.2.2.

### 3.2.14 Hitachi ID Mobile Access applications

Hitachi ID Bravura One App must be the same version as the instance so ensure this is included in your upgrade plan. For more information about the Hitachi ID Bravura One App see the "Hitachi ID Mobile Access Configuration Guide" ([mobile.pdf](#)).

Upgrading from *Bravura Security Fabric* version 10.1.4 or below will require that the Hitachi ID Bravura One App be registered again from the mobile devices if two factor authentication has been enabled to scan a QR Code for mobile authentication for phone assisted login.

### 3.2.15 Proxy Servers

Hitachi ID Systems Proxy servers can be upgraded in any order after the application nodes are upgraded, as long as it is done before [file changes are propagated](#) (p35).

### 3.2.16 Release notes

Review the release notes to identify changes that might affect expected product behavior.

Pay particular attention to:

- Script changes for plugins and exit traps.
- Access controls.
- Features that have been added or revoked.

### 3.2.17 Operating system updates

Verify there are no pending Windows updates to be installed, and verify that no server restarts are scheduled before starting the upgrade or patching process.

### 3.2.18 Product password

Ensure that you know the *Bravura Security Fabric* service user (psadmin) password. This will be required to upgrade existing systems.

For information resetting the service user password, with **serviceacct**, see the Reference Manual.

### 3.2.19 Bravura Privilege

Review the following:

- Managed system policies. Ensure that no single account belongs to more than one policy.

**WARNING!:** As of version 12.0.0, *Bravura Privilege* does not allow for a managed account to belong to more than one policy. If an account is a member of multiple policies at the time of the upgrade, it will be removed from all policies, except from the managed system's primary policy.

- Session monitoring privileges, for both managed system policies, and self-service rules.

**WARNING!:** Session monitoring privileges have changed as of 12.0.0. All managed system policy and self-service rules will be cleared upon upgrade. You will need to reconfigure them after the upgrade.

- *Hitachi ID Bravura Pattern: Privileged Access Edition* trustee privileges. Trustee privileges changed in 12.0.0. The upgrade script should maintain any existing rules so they work how they used, but authmod rules should be reviewed in case different behavior is desired.



Use the documented information you gathered in [Research and Analysis](#) to develop:

- ☐ A *test plan* that can measure whether or not the old and new instances behave as expected
- ☐ A *backup and recovery plan*
- ☐ A *change control plan* to minimize downtime of the production system
- ☐ A *communications plan* to prevent calls to the help desk during the process

## 4.1 Test plan

Write a test plan that systematically identifies use cases covering the required capability of the system. This test plan should cover all automated processing expectations, all end-user self-service cases, all help desk assisting user cases, and so on.

Test the plan on the current production system to ensure it is operating as expected.

The Hitachi ID Systems suite of products has the potential to interact with nearly every other piece of computing equipment in the enterprise, and as such, the test plan ought to be comprehensive and well maintained.

After an upgrade, systematically test the use cases on the newly upgraded system.

Develop test cases around all the various components of the system that you have implemented; for example:

- ☐ End-user use of the self-service web interface, and help-desk-user use of the web interface to assist others to perform all possible operations, such as:
  - ☐ Identification of the profile during login
  - ☐ Authentication of the profile using each method
  - ☐ Resetting passwords for yourself and others
  - ☐ Unlocking accounts for yourself and others
  - ☐ Claiming unassociated accounts to your profile
  - ☐ Managing tokens, SmartCard, and/or hard disc encryption keys
  - ☐ Requesting access to a privileged account

- ☐ Approving a request for access to a privileged account
- ☐ Accessing a privileged account
- ☐ Checking in access to a privileged account
- ☐ Randomizing a password
- ☐ Randomizing a local service
- ☐ Assigning access and membership via user classes
- ☐ Requesting a new account on a target system
- ☐ Requesting attribute changes
- ☐ *Phone Password Manager* functionality
- ☐ Telephone interface for performing operations
- ☐ Target system integrations
  - There should be a test for each operation that is possible on each target system.
- ☐ Ticket / issue tracking system integrations
  - There should be a test for each operation that is possible on each ticketing or issue tracking system.
- ☐ Technologies deployed on user workstations, such as:
  - ☐ Self Service, Anywhere (SSA) / *Login Assistant* (formally Credential Provider / GINA) interface for domain attached users
  - ☐ Other local kiosk solutions for remote and/or local users
  - ☐ Lotus Notes ID file delivery mechanism
  - ☐ Cached credential controls for external users
  - ☐ *Login Manager* client software
- ☐ Technologies deployed on other servers
  - ☐ Transparent synchronization triggers
  - ☐ Target system agent listeners
  - ☐ Hitachi ID Systems proxy servers that run connectors for targets
  - ☐ Notification service clients that run in user domain logon scripts
  - ☐ Reverse proxy servers that allow the web interface to be reached from external networks
- ☐ High availability technologies
  - ☐ Load balancers that direct traffic to multiple Hitachi ID Systems servers either based on load or simple round robin
- ☐ Redundancy technologies
  - ☐ Hitachi ID Systems replication servers
  - ☐ Third party systems that make periodic backups of the files and registry on the servers
  - ☐ Third party systems that make backups of the databases that the Hitachi ID Systems servers use
- ☐ Automation and scheduled events

- ☐ Nightly scheduled update
- ☐ Automatically scheduled tasks such as auto discovery and log rotation.
- ☐ Automated report generation and delivery
- ☐ Notification of soon-to-expire and other bulk email events
- ☐ Notifications delivered via plugin points or "exit traps" which trigger when certain conditions are met or actions are performed.

## 4.2 Production change control plan

Consider the following points to help reduce the production service outage:

- Since production change control windows are usually small, and are typically scheduled during off-hours, extra attention to detail is required to compensate for the late hours and disruption of routine. Upgrade plans should be both explicitly documented and easy to follow. For each step:
  - Describe exactly what to do in clear, plain language, so the person implementing that step does not have to take time to analyze the wording.
  - Include a quick test to verify that this step was completed.
  - Include contingency procedures describing how to troubleshoot failure, back out the change, or redo the change.
  - Describe conditions to help the team decide if the entire migration has reached a critical impasse and must be backed out.

## 4.3 Communications plan

Developing a communication plan that advises end-users well in advance of the upgrade and what to expect when the new version of the software is up-and-running is an important step. This can help reduce call volume from concerned end-users following the upgrade, and set expectations for what they can and can not do during the upgrade window. Ensure that you notify your help desk so that they know how to handle calls from any users who still have questions or concerns. The nature and amount of end-user or even product administrator communication required will depend on whether the new version of the software has changed the user interface in a dramatic way, significantly altered or added new functionality.

This could include telling users that the web interface will not be available during that time; however they can still reset their passwords directly on the target systems if necessary. You could also need to advise users that their passwords may not be synchronized automatically when changed directly on the target systems, and advise them that they can re-synchronize their passwords at a later time.

Ensure that you notify your help desk so that they know how to handle calls from any users who did not get the first messages.

**Note:** Due to time format changes from Unix time to ISO date strings, there may be time skews in reports and active access requests.

## **Part III**

# **UPGRADING**

# Upgrading an Instance Using Setup

# 5

This section shows you how to use **setup** to upgrade from *Hitachi ID Bravura Security Fabric* version 10.x/11.x to 12.x, or apply a patch provided to you by Hitachi ID Systems support.

**Note:** Unless specified, *upgrade* can also refer to **patch**.

**CAUTION:** In cases where your instance contains data or schema customizations the installer doesn't expect, and **setup** rolls back the installation. You may have to perform a version migration process. See the *Bravura Security Fabric Migration Reference Manual* for more information.

It is strongly recommended that you work with Hitachi ID Systems professional services in these cases. Contact your account manager to arrange this.

## 5.1 Preparation

Before you start the upgrade or patching process:

1. Do a complete audit of your environment to ensure upgrading or patching would be successful.  
See [Research and Analysis](#).
2. Design plans for testing, change control, and communication.  
See [Planning](#).
3. Copy the installation package to all application servers.
4. Ensure that pre-upgrade checks pass on each node:
  - (a) Run **setup** with the 12.x MSI.
  - (b) Select the instance you want to upgrade or patch, then click the **Upgrade** link for that instance.
  - (c) Confirm that pre-upgrade checks pass.The database configuration check verifies:
  - The current windows user is the same user that is used for Windows authentication by the instance.
  - The SQL server login for the windows user still has the same default database that is used by the instance.

- The connectivity to the database that the instance uses.

(d) Abort the upgrade.

If the instance you want is not listed, ensure the **instance.cfg** file exists in the root folder of the instance on the disk. This file is a text file containing the following entries, which you would have to modify to fit your own instance:

```
[Config]
INSTANCENAME=pm1200
INSTANCEDESCRIPTION=HiPM 12.0.0 with MSSQL Standard backend
REGISTRY=SOFTWARE\Hitachi ID\IDM Suite\default
```

5. Ensure all health checks pass on all nodes. Confirm that:

- Windows updates are applied.
- There are no critical problems in the Windows event log.
- There are no critical problems in *Hitachi ID Bravura Security Fabric* health checks.
- The node has at least 50GB free.
- The database server has at least 50GB free.
- The database server has at least 25GB free for the transaction log.

6. Restrict access to the IIS server to only a local IP address and the loopback interface by using the IP and Domain Restrictions IIS feature.

**Note:** You may need to install the IP and Domain Restrictions security feature for IIS.

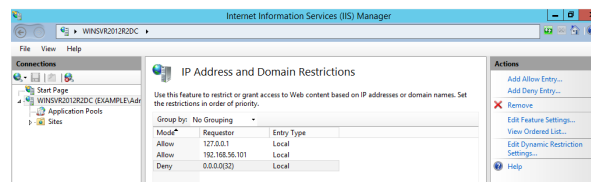


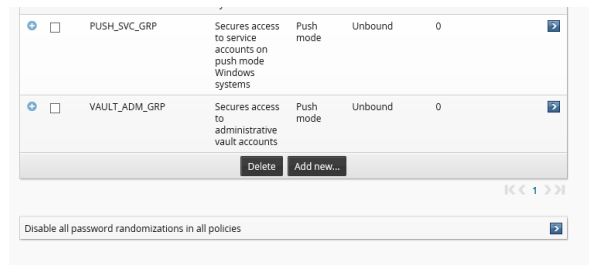
Table 5.1: IP and Domain Restriction settings

Mode	Requestor	Entry type
Allow	127.0.0.1	Local
Allow	Local IP address of IIS server	Local
Deny	0.0.0.0/32	Local

**Note:** If a load balancer or round-robin DNS has been configured in front of the *Bravura Security Fabric*, remove all application nodes from availability to the load balancer to stop new user sessions from being created (and avoid interrupting them when services go down). Optionally, redirect users to a static web page that mentions the cause and duration of the outage (and can be updated with notes if the outage takes longer than expected)

7. Disable all automatic password randomization.

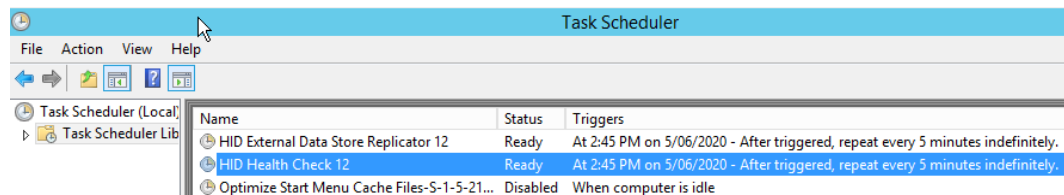
- (a) Log in to *Bravura Security Fabric*.
- (b) Click **Manage the system** → **Privileged access** → **Managed system policies**.
- (c) Scroll to the bottom of the page.
- (d) Select **Disable all password randomizations in all policies**.
- (e) Click **OK** to confirm the selection.



Replication will propagate the disabled password randomization policy to all other nodes automatically. It is recommended to double-check on each node manually or at least check the nodes which have managed system policies configured to run on them.

**Note:** This setting does not actually disable randomization inside each managed system policy; it simply stops any randomization from happening.

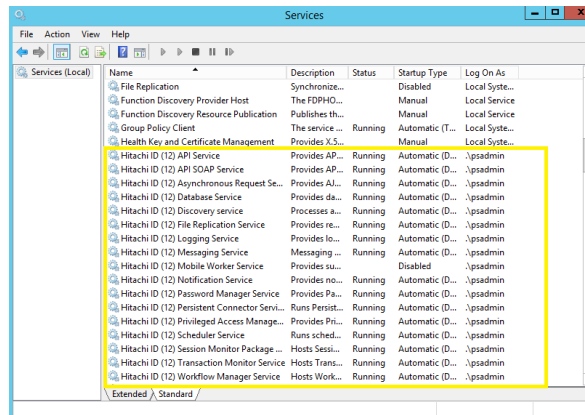
8. Disable Hitachi ID Systems tasks in the OS task scheduler.



9. Verify Hitachi ID Systems processes are no longer running.

While logged into each application node, use Task Manager and verify no processes are running under the Hitachi ID service user (psadmin), other than the Hitachi ID instance services; in particular, **psupdate**, **idtrack** and **autores** should not be running.

10. Stop and disable *Bravura Security Fabric* services on all shared schema or replicated nodes, except for Database Service (iddb) and Logging Service (idmlogsvc).



- Take note of which services are configured as "Manual" or "Disabled" so they can be returned to the same state after the .
- Verify no processes are running under the *Bravura Security Fabric* service user (psadmin) account other than **iddb** and **idmlogsvc**.
- Leave the Database Service running to allow flushing of the replication queue. This will also allow all gathered requests and other database activity to finish trickling through from one node to another, so all source of operations are removed. Verify that the queue has been flushed. See Replication and Recovery ([replication.pdf](#)) for details.

**WARNING!:** Do not set the database replication mode to "Disabled" when patching. Disabling replication will prevent application nodes from queuing replication events for other replicated nodes. (potentially resulting in node desynchronization for data and configuration)

**Note:** The **setup** program does automatically stop services when it starts; however it is important that all nodes share the upgraded schema before services are started again.

It is recommended that each server be upgraded sequentially to prevent overlap of database updates.

#### 11. Stop the remaining Database Service.

All product services other than the Logging Service should be stopped at this point. The Logging Service can remain on during the upgrade.

**Note:** Ensure that you close the services.msc console after stopping all services. If you don't, it can hold a lock on one or more services, preventing them from being uninstalled.

**Note:** All services other than the Logging Service depend on the Database Service. Disabling the Database Service and the other services will ensure that nothing other than the installer will be able to start the service before the patch is over. The Logging Service is left running so that any errors or attempts to start binaries will be logged.

#### 12. Backup all nodes and proxies.

**Virtualized servers** If you are using a virtualization solution to run your *Bravura Security Fabric* nodes as virtual machines, create a snapshot of each of node. Create a snapshot of each node's corresponding database server if the application and database are not on the same server.



**Physical servers** If you are running the application and database nodes on bare-metal, image the server disks, including all disks where *Bravura Security Fabric* and its backend database files are stored. To determine the paths you can check in the Windows registry:

- HKLM\Software\Hitachi ID\IDM Suite\<instance-name>\PsInstallDir
- HKLM\Software\Hitachi ID\IDM Suite\<instance-name>\PsTempDir

### 13. Backup the database.

Regardless of the chosen backup strategy, create an explicit SQL backup. A database backup provides additional flexibility in some recovery scenarios, and can potentially allow an administrator to quickly re-run a patch after fixing issues that may have caused it to fail.

If the database is hosted on a SAN or a shared database cluster where a snapshot or disk image is not possible, create a database backup to accompany the snapshot or disk image made for the application.

### 14. Install Python 3.7.3+.

**Note:** Keep the old version of Python to uninstall the old version of *Bravura Security Fabric*. If the old version of Python is removed, then Python 3.7.3+ location must be added into system path.

### 15. Upgrade *Hitachi ID Connector Pack* if necessary. See [Upgrading Connector Pack](#).

If *Connector Pack* is 3.1.x or older, you need to uninstall the old *Connector Pack*, and install a new one.

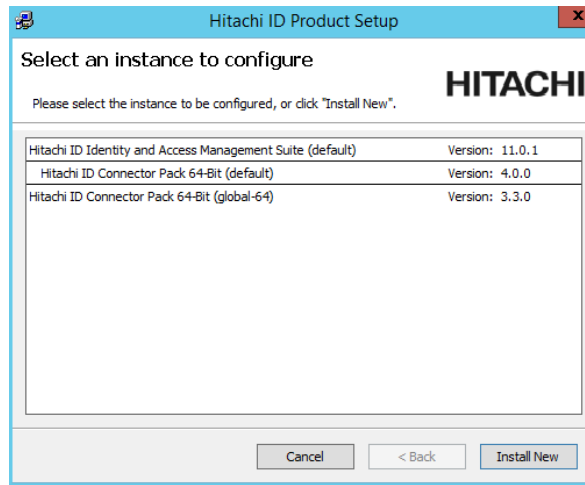
**Note:** The `loadplatform` program may fail, since the Database Service has been stopped; however the program will run as part of the post-installation tasks once *Bravura Security Fabric* has been upgraded.

## 5.2 Upgrade using installer

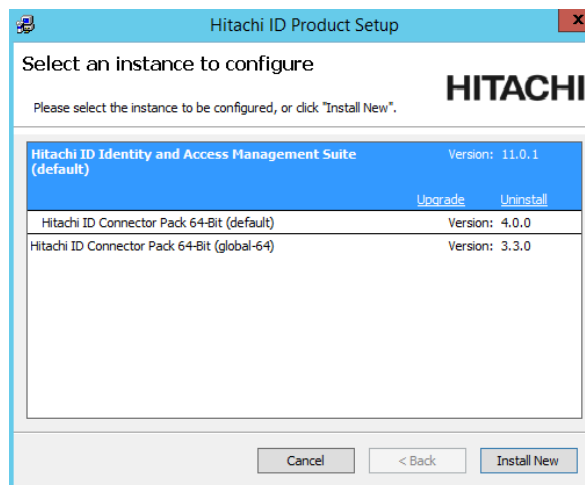
To run the installer:

1. Run **setup** as an Administrator with the 12.x MSI and upgrade the instance on each node, starting with the least critical node first.

The **setup** program shows you the list of existing instances on the server.

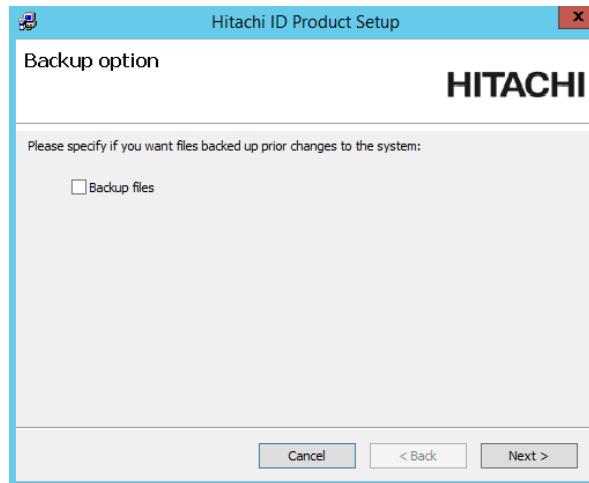


2. Select the instance you want to upgrade or patch, then click the **Upgrade** link for that instance.

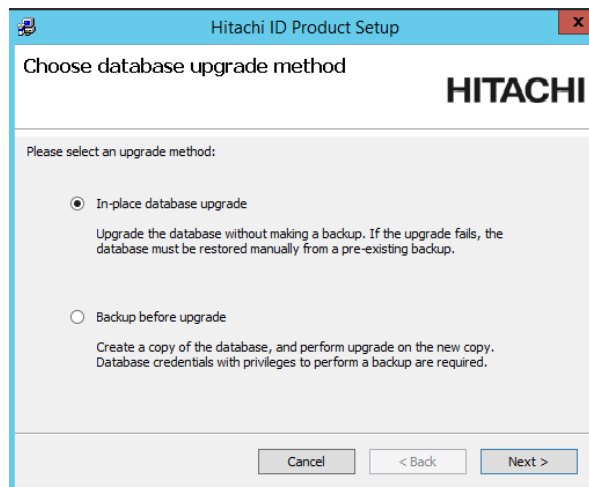


If the instance you want is not listed, refer to [Preparation](#).

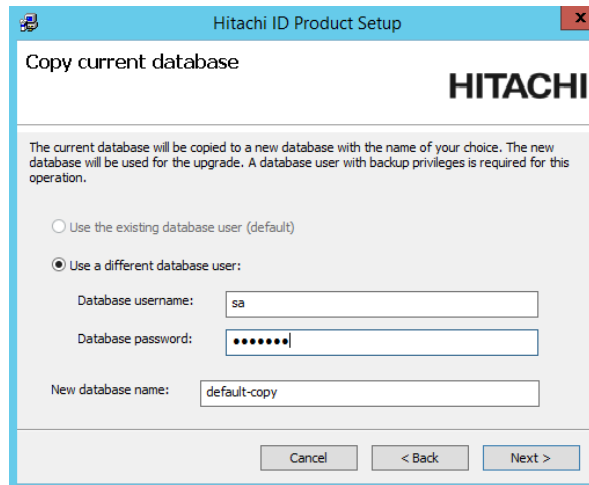
3. Read the product setup warning and click **Yes** to continue.
4. Enter the **psadmin** credentials.
5. Click **Next** after the pre-installation check.
6. Select **Backup files** if you want the installer to backup the files.



7. Choose if you want the installer to backup the database before the upgrade.



8. If you chose to do a database backup, enter the database user's password and a name for the backup database.



**Hitachi ID Product Setup**

### Copy current database

The current database will be copied to a new database with the name of your choice. The new database will be used for the upgrade. A database user with backup privileges is required for this operation.

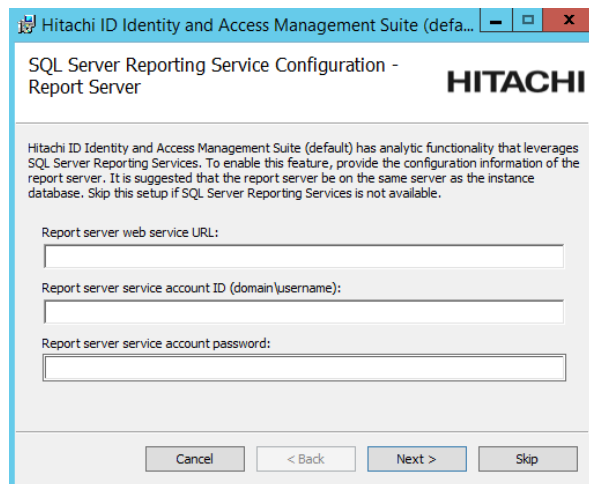
☐ Use the existing database user (default)
   
☒ Use a different database user:

Database username:

Database password:

New database name:

9. During the upgrade, if prompted, update or add new encryption keys.  
*Hitachi ID Bravura Security Fabric* uses several encryption keys to ensure your data is secure.
10. 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 and proceed to [Completing the upgrade process](#).



**Hitachi ID Identity and Access Management Suite (default)**

### SQL Server Reporting Service Configuration - Report Server

Hitachi ID Identity and Access Management Suite (default) 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 service account ID (domain\username):

Report server service account password:

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

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

## 5.2.1 SSRS settings

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

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 service account ID (domain\username):

Report server service account password:

Cancel < Back Next > Skip

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... HITACHI

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:

☐ Create a dedicated database user?

Report database username:

Password:

Cancel < Back Next >

4. Enter the name of server where your instance database resides.
5. If you want **set up** 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 (default)

### SQL Server Reporting Service Configuration - Database User

**HITACHI**

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:

☒ Create a dedicated database user?

Database administrator name:

Database administrator password:

New report database username:

Password:

Confirm password:

Cancel    < Back    Next >

6. Enter the database administrator name and password so the installer can create the new dedicated database user.
7. 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.

## 5.2.2 Completing the upgrade process

1. Enter a valid license for the upgrade if prompted.
2. Click **Install** to start the upgrade.

The installer begins copying files to your computer. The **Completed the Hitachi ID 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 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*.

## 5.3 Troubleshooting

- Do not execute the installer from a network share.
- If the installer opens a window with an error like "You did not provide a database name", contact [support@Hitachi-ID.com](mailto:support@Hitachi-ID.com).
- If the installer does not provide the option to upgrade and instead shows setup screens for a new install, start **setup** from the command line:

```
setup -opts PREVIOUSVERSIONFOUND=11.1.0
```

- If the Hitachi ID Systems service account is a domain account and you are not currently logged into the server using the service account directly, use the following command:

```
runas /user:<domain\BS{ }service-account> setup -opts PREVIOUSVERSIONFOUND=11.1.0
```

- If the upgrade introduces database changes and stored procedures made it into the **iddb** queues before patching started, any resulting failed stored procedures will show up after the database service **iddb** is started:
  - As a summary in the instance's db\iddb-failed-procs\*.log files.
  - With details, in <instance>\logs\<instance-name>\idmsuite.log.
- If the upgrade fails on any node collect the upgrade log and send it to [support@Hitachi-ID.com](mailto:support@Hitachi-ID.com) or reply to a related open Zendesk ticket.
  - The **setup.log** can be found in the same directory as the installer (**setup**). Inside **setup.log** file there is a **msiexec** command that specifies the exact location of the patch installer log is located.
  - Do *not* run **setup** a second time, as it may overwrite the patch installer log containing the original issue details. If the upgrade fails again, it will leave the node in an unknown state.
  - If the upgrade failed with a database error, make a backup of that database on the affected node before reverting the instance. Hitachi ID Systems developers may need to inspect the database state at the time of the error to provide a fix or workaround. Name the backup file "backup-failed-<node-designation>-<timestamp>.bak"; do not send the database backup file to Hitachi ID Systems support unless requested.
  - If the upgrade failed on a production instance, revert it using the [backups](#) (p27).
  - If the upgrade failed on a test instance, leave it as is (make sure the services are off and the Database Service (iddb) is disabled), in case Hitachi ID Systems developers need to look at it.
  - If a node could not be backed up completely in Step 12 in [Preparation](#), it could be restored from a database backup. This is the least recommended recovery version, because it involves re-installing the instance, its prerequisites, and all target system client software. Contact [support@Hitachi-ID.com](mailto:support@Hitachi-ID.com) for help with this.

## 5.4 Post upgrade

### 5.4.1 Post upgrade steps

During the upgrade process, the installer starts all services and tasks. After installer has successfully completed an upgrade on a node:

1. Return the node to the inactive state before continuing to other nodes:
  - Disable Hitachi ID Systems scheduled tasks again as illustrated in Step 8 in [Preparation](#).
  - Stop all services, including the Database Service (iddb), and set to "Manual" as described in Step 10 and Step 11 in [Preparation](#).
2. Once all nodes are upgraded, return all services to their original state and manually start them to bring the system back online. Do *not* enable or start services which were originally disabled before the patch or upgrade.

3. Propagate file changes.

If hybrid or shared schema database replication is configured:


- (a) Log in to *Bravura Security Fabric* on the primary node.
- (b) Click **Manage the system** → **Maintenance** → **File synchronization** to send the new files to the other application nodes and proxies.




Busy files like services, other running binaries and the files these keep open/locked, will not be replaced, but will be left as either `<filename>.busy` or `<filename>.<random digits>`.



- Login to the other nodes to verify if that is the case.
  - If shared or hybrid schema is used, search the instance directory on the servers where the installer was not run (and its subdirectories) for \*.busy files.
  - Sort the files alphabetically in affected directories (where the busy files are found), to identify any more recent copies of the same filename with different extensions.
  - If such files are found, stop the affected services, remove the old binaries and rename the most recent ones with the same filename to give them the correct extension (.exe, .dll, etc); use the file's timestamp in the OS to determine which file version is newer.
4. If sample scripts from previous versions are used, review the new sample scripts and update the currently-used scripts.
  5. Enable Hitachi ID Systems tasks in the OS task scheduler.
 





In the Windows Task Scheduler on all nodes re-enable the names of those tasks begin with "HID". The Data Store Replicator task should not be enabled on any node other than the PRIMARY application node.
  6. Re-enable password randomization.
    - (a) Log in to *Bravura Security Fabric*.
    - (b) Click **Manage the system** → **Privileged access** → **Managed system policies**.
    - (c) Scroll to the bottom of the page.




- (d) Select  **Allow policies to randomize passwords.**
- (e) Click **OK** to confirm the selection.

<input type="checkbox"/>	PUSH_ADM_GRP	Secures access to administrative accounts on push mode Windows systems	Push mode	Unbound	0	0	0	
<input type="checkbox"/>	PUSH_SVC_GRP	Secures access to service accounts on push mode Windows systems	Push mode	Unbound	0	0	0	
<input type="checkbox"/>	VAULT_ADM_GRP	Secures access to administrative vault accounts	Push mode	Unbound	0	0	0	

Allow policies to randomize passwords 

## 7. Load and patch components on the primary node:

- (a) From a command prompt, navigate to the instance directory.
- (b) Run the command:

```
instance.bat
```

- (c) run the command:

```
script\manage_components.py load --patch
```

Confirm they succeed.

## 8. Test local functionality.

On all nodes which have to be used remotely, test local functionality first, especially whatever was changed by the new build, if it's feasible locally.

See [Verifying the upgrade](#) for more detail.

## 9. *Optional:* Reduce "IP Address and Domain Restrictions" rules.

If there is any remote functionality that was changed and requires testing, only open access to the specific IP of the workstation(s) or other server(s) from where the testing will be done.

## 10. Test remote functionality.

From a workstation or other server, attempt instance administration and the other remote features that may be configured: Login Assistant (SKA), API automation, disclosure, LWS connectivity, and so on.

## 11. Remove all "IP Address and Domain Restrictions" rules added during the [pre-upgrade steps](#) (p25).

This is necessary in order for all staff to be able to access the product's web user interface, which is served by IIS.

## 12. Enable and start IIS on all nodes.

## 13. Run auto discovery and resynchronize local service mode systems to generate stable IDs if upgrading from pre-10.x.

## 14. Turn on incremental listing on the primary node.

## 15. Validate that replication is working.

## 16. Upgrade local workstation service software.

See [Upgrading Local Workstation Service software](#).

## 5.4.2 Additional steps to consider

There may be new features included in the upgraded version of the product that have not been enabled during the upgrade process, or may require additional configuration. If you require assistance, contact [support@Hitachi-ID.com](mailto:support@Hitachi-ID.com).

## 5.4.3 Verifying the upgrade

After running **setup** to upgrade to 12.x, verify that the was successful; for example:

- Verify that services are started.
- Verify that replication is working, and all replication nodes are replicating and are functional.
- Navigate the user interface.

**Note:** Check whether web interface customizations were applied. Design style files changed as of 10.0.2, and colors may be missing as a result of your customizations. You must reapply the customizations and reload the skin files.

- Follow an [upgrade plan](#) (p20) based on the configured capability of the old version.
- Verify that the following are correctly configured:
  - Target systems configuration
  - Target systems administrator credentials
  - Target system groups
  - Password policies
  - User classes
  - Authentication/identification priority
  - User notifications
  - Authentication chains
  - Product administrators
  - User access rules
  - Managed system policies
  - Import rules
  - Custom plugins and exit traps

- Verify email configuration.

**Note:** Links in emails sent prior to upgrade will no longer work in 12.x. Users will need to manually log into *Bravura Security Fabric* to view request details or perform actions.

- Confirm that:
  - Managed passwords have have been upgraded properly.
  - Scheduled password resets are still occurring normally for both push and local workstation service mode managed systems.
  - Managed accounts belong to the correct policy.
  - Session monitoring managed system policy and self-service rules are cleared.

## 5.4.4 Remove old installation files

Remove old installation files to avoid confusing with new upgrade/patch files. Hitachi ID Systems recommends keeping only the last two copies of installation files (previous install and current install).

## 5.4.5 Post upgrade notes

### Access to user profiles

By default, *View profile information* privilege is granted to *Access to user profiles* rules - ALLREQUESTERS, API\_REQUEST, and ALL\_SELF\_REQUEST. However, this privilege is not granted to rules created before upgrading.

### Privileged access to systems

By default, permission for users to *Request check-out to managed group sets* are granted to *Privileged access to systems* groups - ALLREQUESTERS and ALLRECIPIENT. However, this permission is not granted to managed system policies created before upgrading.

### Import rules

Managed account import rules created before the upgrade cannot be associated with local workstation service managed system policies. All newly created managed account import rules can be associated with local workstation service managed system policies.

### Local workstation service

You must uninstall the Privileged Access Manager Local Workstation Service (hipamlws) and re-install and re-register a 12.x version of the service.

### Managed accounts

As of 10.x, managed accounts can only belong to a single policy. Run the following report to verify if account are attached to multiple policies:

#### **Reports → Privileged access: Configuration → Managed systems and accounts -import method**

You will need to manually select which policy managed accounts should belong to.

If accounts still belong to more than one policy at upgrade, the following rules will be applied to them:

1. If an account belongs to only one policy, it will be left as a member of that policy.
2. If an account belongs to more than one policy, it will be removed from all policies and added to its managed system's primary policy.

In other words, 1) if you have a managed account on multiple policies, regardless of whether it's on the primary policy, it will be moved to the primary policy, and 2) if you have an account that belongs on a single policy, it will be left on that policy, regardless of whether it's the primary policy.

## Disclosure plugins

If upgrading from 9.x or older to 12.x, you must manually update the Remote Desktop access disclosure plugin. To do this, remove the legacy Remote Desktop disclosure plugin from existing managed system policies and replace it with the new one.

If you want to continue to use the legacy Remote Desktop disclosure plugin, you must update the following disclosure attributes:

- 'encryption' is now a boolean attribute type. Delete the existing 'encryption' disclosure attribute and replace it with the new attribute type. This value should be set to 'False' by default.
- 'host' should be updated to match that of the new Remote Desktop disclosure plugin. If there are managed systems that still follow the old format of '`\<server>`', leave this value untouched.
- 'multimon' and 'smartsizing' attributes are set to 'False'; however the values will only take effect when the **Update** button is clicked.

Uninstall any versions of Firefox native browser extensions 11.1.x or older on the instance server and client workstations, and install the latest version, which is located in the `\<instance>\addon\idarchive` directory.

## Guacamole

As of 12.x, previous versions of Guacamole will no longer work. You will need to upgrade Guacamole with the latest RPMs in the `idmunix*.tar.gz` file located in `\<instance>\addon\idmunix`. As well, you have the option of installing Guacamole using Docker.

When Guacamole is upgraded, you will no longer need to configure an API user or modify the `guacamole.properties` file.

## Database encryption

If upgrading from 9.x or older, you should run `update_db_crypto` on relevant tables. As of *Hitachi ID Bravura Security Fabric* 9.0, the database encryption key was updated from using AES-128 to AES-256 encryption. This will affect answers to security questions and other information.

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

## Detection of attribute names conflict

If name conflicts between resource attributes and profile attributes are detected, post upgrade steps should contain this message: "Resource attribute conflict resolution". The post upgrade report will contain this message about the resource attribute name changes: "Resource attribute `<resourceAttrName>` renamed to `<resourceAttrName_RESATTR>`".

## Hitachi ID Mobile Access applications

Upgrading from *Bravura Security Fabric* version 10.1.4 or below will require that the Hitachi ID Bravura One App be registered again from the mobile devices if two factor authentication has been enabled to scan a QR Code for mobile authentication for phone assisted login.

## Language packs

The upgrade process only upgrades the US English (en-us) language pack. If other language packs are installed before the upgrade, you must install the language packs again after the upgrade.

See the [Bravura Security Fabric Documentation](#) for more information regarding installing language packs.

## Browser caching

Using the same desktop browser that was used to log in to the instance prior to the upgrade and then logging in again after the upgrade is complete may sometimes not render correctly. For example, the user ID in the top right may have a dot where an icon should be and you cannot click on the user name (it does nothing).

You must refresh and reload the browser and then it will be displayed properly.

## Logging Service (idmlogsvc) configuration file

When upgrading *Bravura Security Fabric*, the `idmlogsvc.cfg` configuration file will be retained from the previous version. A new configuration file named `idmlogsvc.bak` will be created and will contain the configuration settings of `idmlogsvc.cfg` for *Bravura Security Fabric* 12.2.4.

This configuration file should be reviewed for any changes between `idmlogsvc.cfg` (configuration settings from the previous version) and `idmlogsvc.bak` (configuration settings for *Bravura Security Fabric* 12.2.4) after the upgrade is complete.

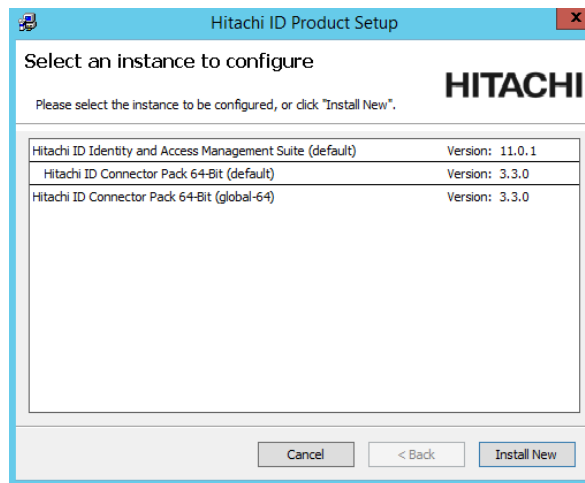
# Upgrading Connector Pack

# 6

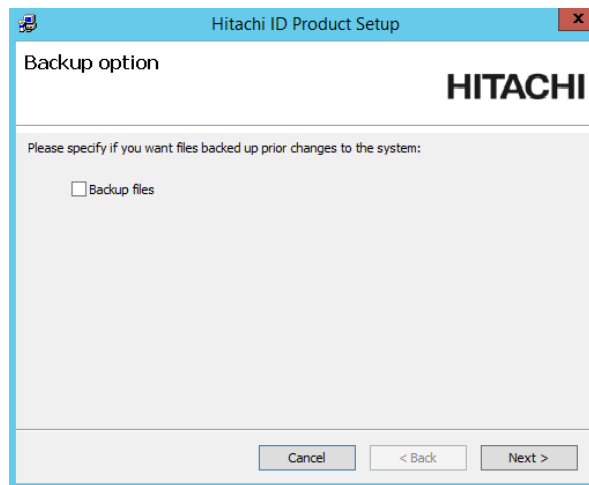
**Note:** When upgrading the connector pack, you must use the **setup** program that comes with the connector pack.

To upgrade *Hitachi ID Connector Pack* from 3.2.2 or later to 4.1.5 using the **setup** installer:

1. Run **setup** with the 12.x MSI. Setup shows you the list of existing *Connector Pack* installations on the server.



2. Select the *Connector Pack* you want to upgrade and click the **Upgrade** link.
3. During the upgrade, if prompted, click **Yes** to stop all services in order to install an updated Visual C++ Runtime.
4. Click **Next**.
5. Select **Backup files** if you would like the installer to do a backup.



6. Click **Next**.
7. Follow the prompts to finish the upgrade.

# Upgrading Local Workstation Service software

# 7

There are three ways to upgrade the Privileged Access Manager Local Workstation Service (hipamlws):

- Running the **hipamlws\*.msi** installer and going through the wizard pages.

This will look like a normal Local Workstation Service installation, where the server, proxy, initial delay and custom attribute file settings are retained.

- Running **hipamlws\*.msi** through commandline:

```
msiexec /l*v upgrade.log /i hipamlws-win-x64.msi REINSTALLMODE=amus ADDLOCAL=ALL  
UPGRADE=ALL
```

(include `/QUIET` for complete automation)

During upgrade, the installer will attempt to retain SERVER, PROXY, and CUST\_ATTR\_FILE properties from the original installation. These can be specified in the command if there is a need to replace them; for example:

```
msiexec /l*v upgrade.log /i hipamlws-win-x64.msi REINSTALLMODE=amus ADDLOCAL=ALL  
UPGRADE=ALL CUST_ATTR_FILE=full_path_and_file
```

If there is a need to clear any retained properties, you can first clear them from the `idmsetup.inf`, and then use `IGNORE_EXISTING_*`; for example:

```
msiexec /l*v upgrade.log /i hipamlws-win-x64.msi REINSTALLMODE=amus  
ADDLOCAL=ALL UPGRADE=ALL IGNORE_EXISTING_PROXY="1"  
IGNORE_EXISTING_CUST_ATTR_FILE="1" IGNORE_EXISTING_VERIFY_CERT="1"
```

- Uninstall the old client and install the new client with the **Re-register this workstation** option selected in the **Advanced** settings.



# Upgrading Guacamole

---

## 8

The steps covered in this section cover upgrading Guacamole through Docker. It is recommended that if Guacamole was installed directly on the server using RPM packages, to remove the RPM packages and install Guacamole using the Docker method instead.

1. On the Guacamole gateway, rename the `idmunix-rhel-el7.x64` directory to `idmunix-rhel-el7.x64.old`.
2. Copy over the new `idmunix-rhel-el7.x64.tar.gz` file from the `<instance>\addon\idmunix` directory to a temporary folder on the Guacamole gateway.
3. Unzip the `.tar.gz` file.
4. Open the `idmunix-rhel-el7.x64\docker` directory.
5. If behind a proxy server, ensure that the `DockerFile` in the `guacd` folder is updated with the proper proxy settings.
6. Build and run the Docker images:

```
docker-compose up --force-recreate --build -d
```

7. Remove the older images:

```
docker image prune -f
```

# Upgrading the Login Assistant Software

---

# 9

*Login Assistant* can be upgraded two ways:

- Running the `ska-x64.msi` or `ska.msi` installer and going through the wizard pages (p45)
- Running the `ska-x64.msi` or `ska.msi` through commandline (p51)

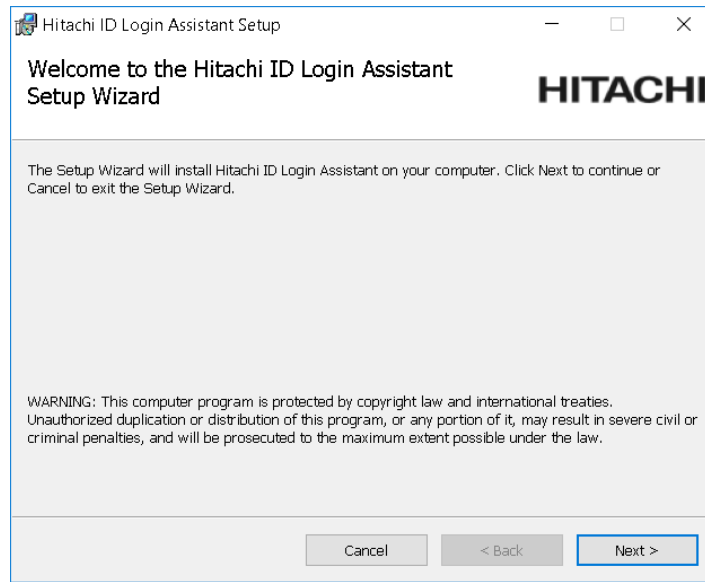
## 9.1 Running the installer

This section shows you how to manually install or upgrade *Login Assistant* on a workstation. See:

- [Installing add-on software](#) for general requirements for using a client MSI installer, and instructions for automatic installation using a group policy.
- [Add-on Installers](#) in the *Reference Manual* for more information about setting MSI properties in a transform file or from the command line.

To manually install or upgrade *Login Assistant* on a workstation:

1. Copy the `ska.msi` installer, or `ska-x64.msi` installer for 64-bit systems, from the `addon` directory to a scratch directory (C:\temp) on the local workstation or to a publicly accessible share.
2. Launch the installer.



Click **Next**.

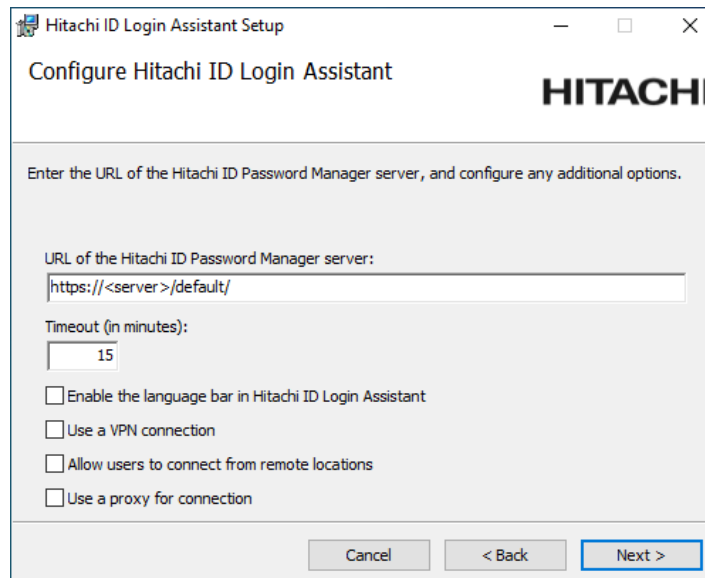
3. Read and accept the license agreement.

Click **Next**.

4. Click **Typical** to install the Credential Provider.

Click **Next**.

5. Configure the *Login Assistant*:



**URL of the Hitachi ID Bravura Pass server** The full path to the *Hitachi ID Bravura Pass* server. The URL can include skin name or other parameters. Do *not* set this URL to a redirect page.

**Timeout** This is the maximum amount of time the *Login Assistant* secure kiosk account can be used before it automatically closes. Default is 15 minutes.

**Enable the language bar in the Login Assistant** Select this option if you want users to be able to select a different language while using the *Login Assistant*.

**Use a VPN connection** Select this option if you want to establish a VPN connection before opening the *Bravura Pass* login page in a kiosk browser.

**Allow users to connect from remote locations** Select this option if you want users to be able to connect from remote locations, using direct connection, WiFi hotspot, or AirCard. This is generally used along with a VPN connection.

**Use a proxy for connection** Select this option if you want the secure kiosk account browser to use the Internet Explorer proxy server to connect to the *Bravura Pass* instance. You can configure settings for the proxy in Step 9.

Click **Next**.

#### 6. Set up the help account.

Type the **User ID** (default is `help`). The help account is used to login and launch `runurl`.

Use the format `<User ID>@<Domain>` or `<Domain>\<User ID>` if the help account is a domain user.

If the **Use random password for this account** checkbox is selected, you do *not* need to enter a password. A random password will be used instead. You must specify a password if you are only installing the *Login Assistant* and not the Credential Provider, or if you are using a domain account.

Click **Next**.

#### 7. Configure a VPN connection program if you selected that option in step 5:

**Connection program** Name and full path of the program to run in order to establish a VPN connection.

**Connection program arguments** Command-line arguments for the VPN connect program; for example `-u %USERID% -p %PASSWORD%`.

**Disconnection program** Name and full path of the program to run to disconnect from the VPN.

**Disconnection program arguments** Command-line arguments for the VPN disconnect program; for example `-u %USERID% -p %PASSWORD%`.

**User ID** To be used with the VPN connect and disconnect programs.

**Password** For the VPN user ID.

**Timeout** The period in seconds that the `runur1` program should wait before checking to see if connectivity has been established after the VPN connect program has run. Default value is 30.

**Retries** Number of times to test for connectivity after the VPN connect program has run. If this value is blank, there will only be one retry attempt. Default value is 3.

Click **Next**.

8. Configure the remote account access if you selected that option in step 5:

**External URL to test for connectivity** This will be the URL of a website that used to determine if the computer is connected to the Internet, or still behind a registration screen or captive portal. This defaults to `www.msftncsi.com/ncsi.txt`.

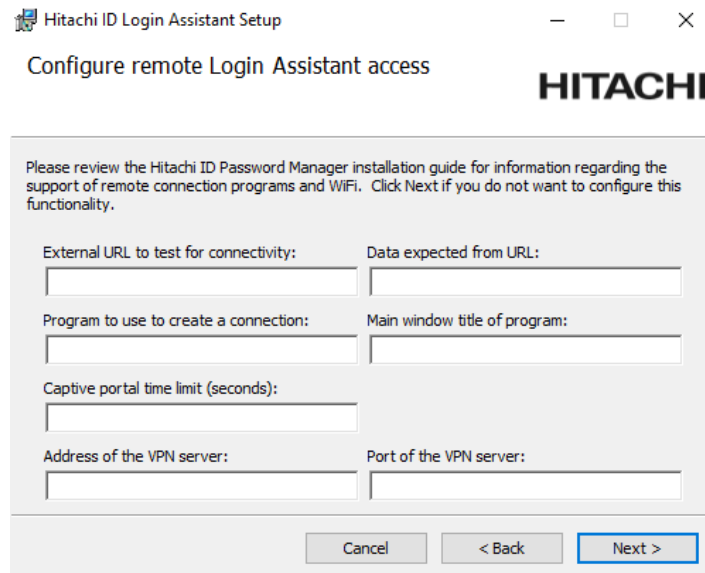
**Data expected from URL** This is a string that is expected from the above website. It should be unique enough to ensure that a registration page will not have the data, but always present on the external URL. The default is `Microsoft NCSE`.

**Program to use to create a connection** If users will be using an AirCard or Internet stick, this is the name of the program to run in order to connect. This program will be run from the *Login Assistant* to allow the user to connect.

**Main window title of program** If the **Program to use to create a connection** is used, this is the main window title of the program when run. In AirCard, this is listed under the **Task** column on the **Applications** tab.

**Captive portal time limit (seconds)** Specify the length of time to wait to see if a connection has been established by the captive portal used to create a connection. The time limit may be set between 0 and 600 seconds. The default is 300.

**Address of the VPN server / Port of the VPN server** If specified these allow the remote *Login Assistant* to test a connection to the VPN server to see if it can be accessed before starting the VPN. This can help with better diagnosis and faster connection times.



Hitachi ID Login Assistant Setup

Configure remote Login Assistant access

**HITACHI**

Please review the Hitachi ID Password Manager installation guide for information regarding the support of remote connection programs and WiFi. Click Next if you do not want to configure this functionality.

External URL to test for connectivity:	Data expected from URL:
<input type="text"/>	<input type="text"/>
Program to use to create a connection:	Main window title of program:
<input type="text"/>	<input type="text"/>
Captive portal time limit (seconds):	
<input type="text"/>	
Address of the VPN server:	Port of the VPN server:
<input type="text"/>	<input type="text"/>

Cancel < Back Next >

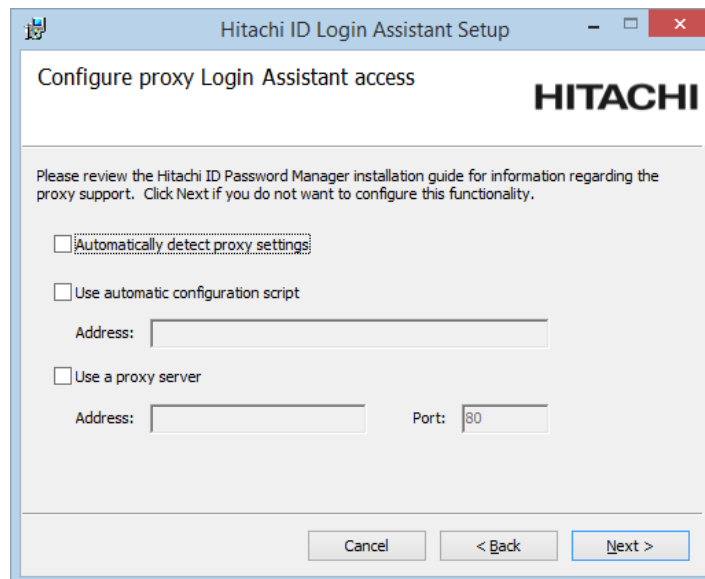
Click **Next**

- If you chose to use a proxy for connection in step 5, configure the Internet Explorer proxy server for the secure kiosk account. These settings match those set in Internet Explorer → Internet Options → Local Area Network (LAN) Settings:

**Automatically detect proxy settings** Sets Internet Explorer proxy server to "Automatically detect settings".

**Use automatic configuration script** Sets the proxy server to use "Use automatic configuration script".

**Use a proxy server** Sets proxy server to use a manually defined proxy server.



Hitachi ID Login Assistant Setup

Configure proxy Login Assistant access

**HITACHI**

Please review the Hitachi ID Password Manager installation guide for information regarding the proxy support. Click Next if you do not want to configure this functionality.

☐ Automatically detect proxy settings

☐ Use automatic configuration script

Address:

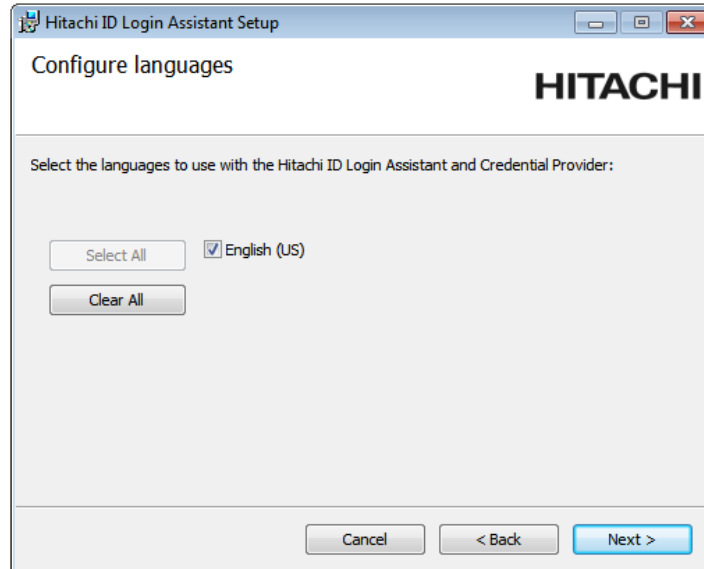
☐ Use a proxy server

Address:  Port:

Cancel < Back Next >

Click **Next**.

10. Select the languages to be displayed by the *Login Assistant*.



Click **Next**.

i

11. Once you have finished configuring the various installation options, you are prompted to start the installation.

Click **Install**.

The installer begins copying files to your computer. The ***Installation Complete*** dialog appears after the software has been successfully installed.

12. Click **Finish** to exit.

Depending on your installation options, you may be prompted to restart Windows.

## 9.2 Command line upgrade

*Login Assistant* can be upgraded from the command line using the following:

```
msiexec /i ska-x64.msi REINSTALLMODE=amus
```

### See also:

See the Self-Service Anywhere Implementation Guide (**self-service-anywhere.pdf**) for more information about installing and using *Login Assistant*.



# Upgrading the Proxy Server

# 10

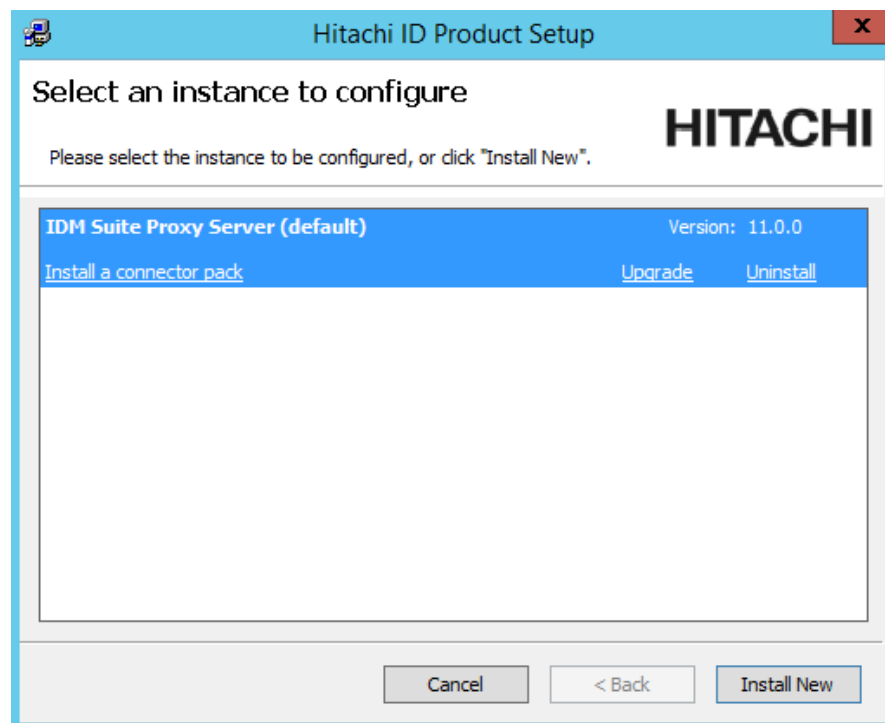
This chapter shows you how to upgrade a *Hitachi ID Bravura Security Fabric* proxy server using the **setup** installer.

**Note:** Currently you can only upgrade minor versions of the proxy server. For example, 11.1.2 to 11.1.3. Major version changes requires an uninstall of the previous version and a new install of the new version.

To upgrade a proxy server:

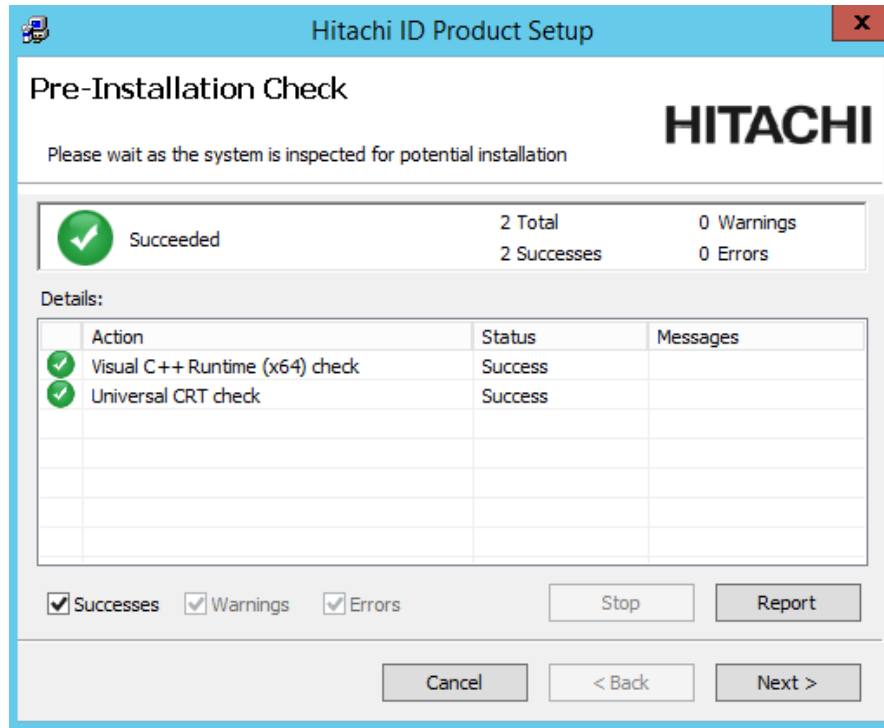
1. Run **setup** with the 12.x **msi**.

Setup shows you the list of existing instances on the server. Select the one you want to upgrade, then click the **Upgrade** link for that instance.



2. Click **Yes** to confirm.
3. Enter the password for the service account.

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



4. If all of the checks are successful, click **Next** to proceed with the upgrade.
5. Click **Next**.  
The proxy server will be upgraded.
6. Click **Finish** to exit.

# Upgrading components

# 11

This chapter contains notes about possible issues that may occur with the component framework when upgrading.

## Upgrade from 11.1.3 to 12.0.x fails with component error 'Failed: AUTO\_INSTALL for Scenario.hid\_authchain\_smspin\_email

In *Hitachi ID Bravura Security Fabric* 11.1.3 the `Scenario.hid_first_login` and `Functional.hid_authchain_2factor` components were changed from using the generic `Scenario.hid_authchain_smspin` to `Scenario.hid_authchain_smspin_celltrust` even though the replacement for `Scenario.hid_authchain_smspin` was logically `Scenario.hid_authchain_smspin_email`.

In 12.0.1 this changed back from celltrust to email, but those who installed 11.1.3 with this scenario will run into a conflict until *Bravura Security Fabric* includes the ability to specify multiple possible dependent components.

Work-around: To fix this, explicitly remove `Scenario.hid_authchain_smspin_celltrust` and reload the components, the conflict should resolve itself.

## Upgrade cannot compensate for custom components

An upgrade using the `setup` installer will not be able to compensate for custom components. For example if the manifest of a custom component depends on a component that has been deprecated, upgrade will not be able to properly load that custom component because of the deprecated dependency. If the custom component has a CSV that does not use newer columns this could cause a failure during upgrade.

Check custom components before upgrading.

## Entries in the external data store may not be upgraded properly

As of version 11.1.1, *Hitachi ID Bravura Security Fabric* no longer supports the use of wildcards in external data store entries. After upgrading to 12.2.4, any entries in the external data store that uses wildcards may not be updated properly. Those entries will need to be manually fixed.

## Update system vault addresses

After upgrading from a version 10.1.4 instance you must manually update the address of system vault types that were created before the upgrade as their address lines will still contain single quotes. If the address line is not updated the creation of vault accounts will not have set passwords.

## Upgrade cannot install all decoupled components

When a component is decoupled to multiple components, only one component will be installed during upgrade; others will need to be manually installed after upgrade.

For example: Component `Scenario.im_corp_onboard` was decoupled to components `Scenario.im_corp_onboard` and `Scenario.im_corp_automated_onboard` since 11.1.1. If component `Scenario.im_corp_onboard` was installed on a 10.0.4 instance, when upgrading to 11.1.3, the upgrade task will only upgrade the `Scenario.im_corp_onboard` component. `Scenario.im_corp_automated_onboard` won't be installed during upgrade.

The workaround is to manually install the component `Scenario.im_corp_automated_onboard` after upgrading.

## **Part IV**

# **UTILITY REFERENCE**

## Description

Use the **getfileinfo** program to return the build information for Hitachi ID-created binary files. This information is useful during support calls, or when diagnosing problems.

The program returns information about whether the file has been customized or upgraded, or contains debugging information.

## Usage

```
getfileinfo.exe <binary file name>
```

## Examples

The following is an example of the return for a regular build:

```
FileName:           <file path>\<filename>
MajorVersion:       4
MinorVersion:       0
BuildNumber:        1
RevisionNumber (QFE): 6552
FileFlags: 0x0
FileVersion:        4.0.1.06552
SpecialBuild:       not found
```

The following is an example of the return for a custom build:

```
FileName:           <filepath>\<filename>
File has been customized.
MajorVersion:       6
MinorVersion:       3
BuildNumber:        0
RevisionNumber (QFE): 2066
FileFlags: 0x20
FileVersion:        6.3.0.02121
SpecialBuild:       Custom build by <developer's name>
```

## Description

The **instdump** program is run at the end of the auto discovery process and writes a configurations summary to a file named `config-<yyyy>-<mm>-<dd>.kvg` in the `<Program Files path>\Hitachi ID\IDM Suite\Logs\<instance>\` directory. The file can be used by Hitachi ID Systems support to help provide assistance.

The **psupdate** program runs the **instdump** program when the **Maintenance** → **Options** → **PSUPDATE INSTDUMP** setting is enabled (disabled by default).

**Note:** Some arguments are dependent on the Hitachi ID Systems product license.

## Usage

```
instdump.exe [ <options> ] -outfile <outfile>
```

Table 13.1: instdump arguments

Argument	Description
-acl	Output ACL information.
-attrgrp	Output attribute group information. Requires <i>Bravura Identity</i> .
-authenidlist	Output authentication target system list information.
-authorizer	Output authorizer information. Requires <i>Bravura Identity</i> .
-binaryversion	Output binary version information.
-consoleuser	Output product administrator information.
-customfile	Output custom file information.
-exittrap	Output event action (exit trap) information.
-inventory	Output inventory information. Requires <i>Bravura Identity</i> .
-managedgrp	Output managed group information. Requires <i>Bravura Identity</i> .
-outfile <outfile>	File name for output (required).
-plugin	Output plugin information.
-profileattr	Output attribute information.
-registry	Output registry information.

... continued on next page

Table 13.1: instdump arguments (Continued)

Argument	Description
-role	Output role information. Requires <i>Bravura Identity</i> .
-service	Output service information.
-strength	Output strength information.
-system	Output system configuration variables.
-target	Output target information.
-targetattr	Output account attribute information.
-template	Output template information. Requires <i>Bravura Identity</i> .
-userclass	Output userclass information.
-verbose	Use a more readable format for output.



## Description

Use the `loadplatform` program to query connectors for their abilities and populate PLATFORM,OBJOPER and OBJREL database tables with the information; Also it sets the default attributes for the connector platforms by populating ATTRDEF and ATTRDEFVAL tables. This is particularly useful when custom connectors have been created and the target type needs to be available in the user interface.

*Hitachi ID Bravura Security Fabric* target systems types are displayed in **Type** drop-down list on the **Target system information** page. Target types in this list are displayed according to target system category.

## 14.1 Requirements

The client software required by the specified target systems must be installed or else the platform data for the connector will not be imported to the database.

The `loadplatform` program loads a binary executable (.exe), or a [scripted platform definition file \(.con\)](#) (p62) that calls a binary agent. If you do not specify an .exe or .con extension, the program looks for files with either extension. If both exist, `loadplatform` loads the .exe file.

To load and list official scripted connectors, both the scripted platform definition file (.con) and the configuration script specified within the .con file must be located in the agent directory.

## 14.2 Usage

```
loadplatform.exe -a <connector name> [-dry-run]
```

```
loadplatform.exe -target [-dry-run]
```

Table 14.1: loadplatform arguments

Argument	Description
-v, --version	Print out version and exit
-a, --agent <connector name>	Load the specified connector.
-target	Load all target system connectors.
-d, --dir <directory path>	Changes the directory to look for the agents and connectors in the specified path.
-32bit	Load 32-bit connectors.
-dry-run	Query the specified connectors but do not write the information to the database.
-force	Forcibly update attribute information if conflict exists.
-list-db-inserts	Include a list of all inserted database values.

### 14.2.1 Examples

1. To import information about the Unix connector into the database, type:

```
loadplatform.exe -a agtunix.exe
```

2. To see the operations supported by the Active Directory DN connector, type:

```
loadplatform.exe -dry-run -a agtaddn.exe
```

## 14.3 Loading a new scripted target system type

Some target system types listed on the **Target system information** page are defined by scripted platform definition files that call a binary agent such as the SSH scripted agent (**agtssh**) and specify a configuration script that defines supported operations.

Scripted platform definition files are written in the following format:

```
# KVGROUP-V2.0
<name> = {
  agent = <binaryToRun>;
  script = <script>;
  category = <category>;
  platform = <platformId>;
  description = <languageTagName>;
}
```

for example:

```
# KVGROUP-V2.0
agtssh-sample = {
  agent = agtssh.exe;
  script = sampleScript.cfg;
  category = SCRIPT;
  platform = AGTSSH-SAMPLE;
  description = !!!AGTSSH-SAMPLE-DESC;
}
```

**Note:** Official scripted connectors are only compatible with *Bravura Security Fabric* 10.0 and above.

The keys in the scripted platform definition file are all required, and are all case sensitive. The "category" must be a valid platform category. These are described in **platcat.csv** in the agent\dat directory.

To load a new scripted target system type:

1. Write a configuration script in the format described in **SCRIPT TYPES** in the *Script Systems Integration Guide* (**script-systems.pdf**).
2. Write a scripted platform definition file in the format described on this page.
3. Add both the configuration script and the .con file to the agent directory.
4. From the util directory, run:

```
loadplatform -a <con filename>.con
```

This loads the new target system type into the instance database.

Scripted platform definition files and configuration scripts can also be loaded from other directories outside the agent directory. To do this, place both the configuration script and the .con file into the desired directory and run loadplatform with the absolute or relative path to the .con file. For example:

```
loadplatform -a <con filename>.con -d "C:\path\to\agent"
```

SQL scripted connectors also support defining managed identities by using a configuration file in following format:

```
# KVGROUP-V2.0
<name> = {
  agent = <binaryToRun>;
  script = <script>;
  category = <category>;
  platform = <platformId>;
  description = <languageTagName>;
  objects = <object type>;
}
```

for example:

```
# KVGROUP-V2.0
agtoracustom = {
  agent = agtorascript.exe;
  script = agtoracustom.cfg;
  category = ATTAP;
  platform = ORACUSTOM;
  description = "Custom oracle target";
  system = false;
  objects = {ACCT;ASSET;GRP;ROLE;};
}
```

Providing managed identities in the configuration file allows connectors to be loaded with only operations related to the specified objects.

## 14.4 Loading a new platform category

*Hitachi ID Bravura Security Fabric* can load a new platform category dynamically. *Hitachi ID Connector Pack* 1.1 or later is required.

To load a new platform category:

1. Modify the `platcat.csv` from the `agent\dat` directory.
2. Add a new category to the `platcat.csv` file.
3. Add the language tag for this new category to the `en-errmsg.kvg` file.
4. Generate and install a new set of skins.
5. From the `util` directory, run:

```
loadplatform -target
```

This loads the new platform category into the `platcat` table.

## 14.5 Loading default attributes

*Hitachi ID Bravura Security Fabric* can load default attributes for connectors from attribute files located in `agent\dat` directory. The default attributes for connectors are defined in different files which may include account attributes file, group attributes file and object attributes file depending on the connector supported operations.

To load the default attributes:

1. Modify or create a new attribute file(s) in the `agent\dat` directory.
2. From the util directory, run:

```
loadplatform -a <agent>
```

This loads or modifies the default attributes for the connector platforms by populating `ATTRDEF` and `ATTRDEFVAL` tables.

You should be able to find default attributes for account and group under **Manage the system** → **Resources** → **Account attributes** or **Manage the system** → **Resources** → **Group attributes** then select the connector target system type or the connector target system.

## 14.6 Loading a new or modified discovery template

*Hitachi ID Bravura Security Fabric* can load target system discovery templates dynamically. *Hitachi ID Connector Pack* 3.1.0 or later is required. By default, they are located in the `agent\dat` directory.

Discovery template files are written in the following format:

```
KVGROUP-V2.0
templates = {
  <TARGET_TEMPLATE> = {
    name = <PSLang name description>
    address = <PSLang address description>
    <key> = <value>; # target system option
    ...
    ...
    <key> = <value>;
    Resources = {
    };
    TargetAttrs = {
    };
  };
}
```

for example:

```
# KVGROUP-V2.0
templates = {
  NT_TEMPLATE = {
    name = "$comp[\"dNSHostName\"] [0]";
```

```

address = "\"{server=}\" + $comp[\"dNSHostName\"] [0] + \";}\"";
runlist = true;
listattributes = true;
listgroups = true;
idarchivepush = true;
adminresethide = true;
selfresethide = true;
adminunlockhide = true;
selfunlockhide = true;
adminclaimhide = true;
selfclaimhide = true;
selfmanagehide = true;
listmembertype = A;
Resources = {
    ls_scmacct;
    ls_taskacct;
    ls_iisacct;
    ls_comacct;
    ls_normacct;
};
TargetAttrs = {
    ADDR_ATTR = "DNSHOSTNAME";
    DESC_ATTR = "DNSHOSTNAME";
};
};

```

The keys in the discovery template file are all required, and are all case sensitive. The name and address keys are written using PSLang expression based on account attributes discovered using auto discovery.

To load a discovery template:

1. Modify or create a new <target>-template.cfg file in the agent\dat directory.
2. From the util directory, run:

```
loadplatform -a <agent>
```

This loads the agent with the new/modified discovery template onto the instance. You should be able to find the discovery template under **Manage the system** → **Resources** → **Target systems** → **Discovery templates**.

Use the Hitachi ID Systems Data Migration Utility to migrate user data from an older version of *Hitachi ID Bravura Pass* to a current version.

## 15.1 Prerequisites for the older version

- Users have security questions populated for their question sets including user-defined as well as pre-defined question sets (built-in and optionally custom).
- Password policies are updated for password history enforcement if password history is being exported. Users need to have reset their passwords previously in order to have values populated for the password history.
- If attributes are to be exported, users have profile attributes populated, where those profile attributes are not listed from any target systems, although they may be associated with attributes on a target system.
- Users may have their profiles locked out (too many bad authentication attempts) or disabled (a help desk administrator has disabled a user's profile). For testing purposes these accounts should be noted and revisited after the migration.
- Users have mobile devices that have been registered. The mobile device registration data may be exported so that the users are not required to re-register their devices.
- Target system credentials can be exported from *Hitachi ID Bravura Security Fabric* version 8.2.0 or newer.
- Team management data can be exported from *Bravura Security Fabric* version 10.1.4, and versions 11.1.1 or newer.
- The following *Bravura Privilege* data cannot be exported using the utility:
  - managed accounts and systems not onboarded using team management
  - import rules and related data
  - managed system policies
  - archived data (\*\_hst tables)
  - inactive managed systems and accounts
  - active managed account check-outs

## 15.2 Prerequisites for the current version

- Target systems should be set up prior to data import. Accounts should be discovered, and profiles should already be created.
- Target systems should reflect existing configuration between the older version and the current version of *Hitachi ID Bravura Security Fabric*. For example you should use newer agents such as the Active Directory DN (**agtaddn**) rather than the older and mostly obsolete Active Directory (**agtad**).
- Target system credentials will only be imported for target systems that match the IDs from the older version. This will override any existing credentials already defined on the current version.
- Password policies are updated to the intended policy. Password history enforcement must be enabled if password history is being imported.
- Profile attributes must be created for any profile attribute values that will be imported.
- A dry run might generate some entries in log with !!!TAG complains, but they are minor and only related to a multilingual UI. Any !!!TAG (multilingual) values should be recreated on imported target systems to avoid missing translations if you are deploying in additional languages.
- Hitachi ID Bravura One is configured on the *Bravura Security Fabric* server and the Mobile Worker Service (mobworker) is configured for mobile access with the Hitachi ID Bravura One proxy server.

When migrating the mobile device registrations and the instance name has changed for *Bravura Security Fabric* and/or the company name has changed for the Hitachi ID Bravura One proxy server Apache configuration, the **Proxy server URL** address for the Mobile Worker Service may remain the same, however the rewrite rule in the Apache configuration on the Hitachi ID Bravura One proxy server will need to be modified.

This is to ensure that when one or both of these names have changed, that users will not be required to re-register their mobile devices. See the Hitachi ID Bravura One Configuration Guide for more information on the Apache configuration requirements.

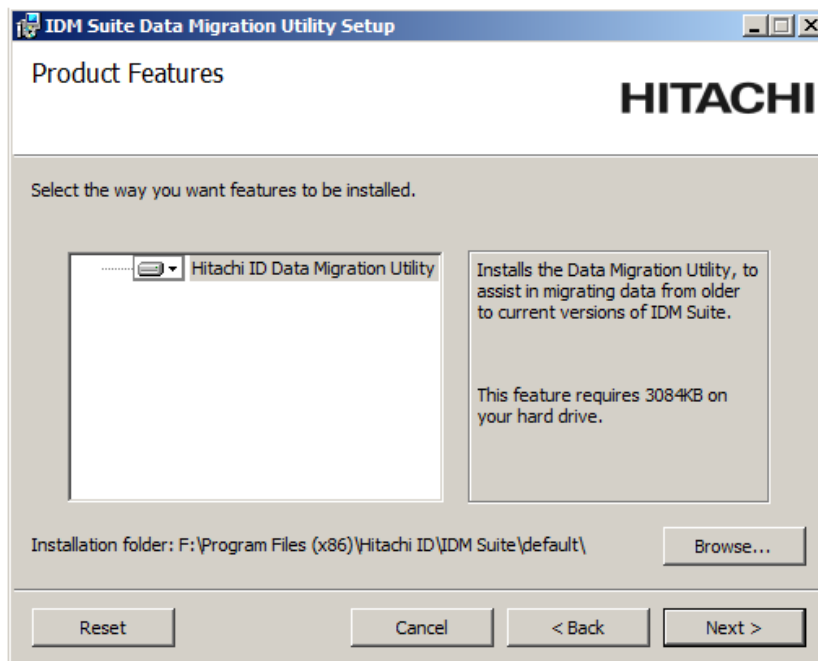
- Randomization must be disabled for all accounts. It is also recommended that all checked out accounts are checked in prior to data export.
- The same team management components installed in the older version must also be installed in the current version. This includes the following:
  - *Bravura Privilege* rebuild components (pam\_team\_management, pam\_team\_vault\_management)
  - system type scenario components (pam\_system\_type\_winnt, pam\_system\_type\_linux)
  - subscriber validation scenario component (pam\_subscriber\_validation)
  - personal admin scenario component (pam\_personal\_admin\_management)
- The same source of profiles target used in the older version must also be added and configured in the current version to list users and manage groups.
- If the target system credentials of onboarded systems are associated with a *Bravura Privilege* managed account, you will need to manually add the managed system the account is a part of. As well, you will also need to manually create the managed system policy the managed account was originally added to (if it doesn't already exist), and bind the account to the managed system policy.



## 15.3 Data migration process

### 15.3.1 Exporting data from the older (source) version

1. Obtain a copy of the `migratedata.msi` Windows installer from Hitachi ID.
2. Copy `migratedata.msi` to the computer where the older (source) instance is installed.
3. On the computer where the source instance is installed, run `migratedata.msi`.
4. On the **Product Features** page, ensure that **Installation folder** is set to the directory where the source instance is installed; for example, the following source instance is installed under `F:\Program Files (x86)\Hitachi ID\IDM Suite\default`:



5. Continue with the remaining wizard pages to install `migratedata`.  
If you do not have at least SQL Server Native Client 2008 installed, you will receive a warning and installation will not proceed until it is installed. Upon completion of the installation process, `migratedata.exe` will be available in the `\util` sub-directory of the location specified for **Installation folder**.
6. Open a command prompt and navigate to the directory where `migratedata` is located.
7. Run `migratedata` using the following parameters:

```
migratedata.exe -action export -file <dbfile> <datatype>
```

where:

- `<dbfile>` is the SQLite database file that will be created if it does not exist already, or opened if it already exists.

- `<datatype>` is one or more of the data types listed in Table 15.1.

8. Enter a password.

The password will be used to encrypt the data key of the instance.

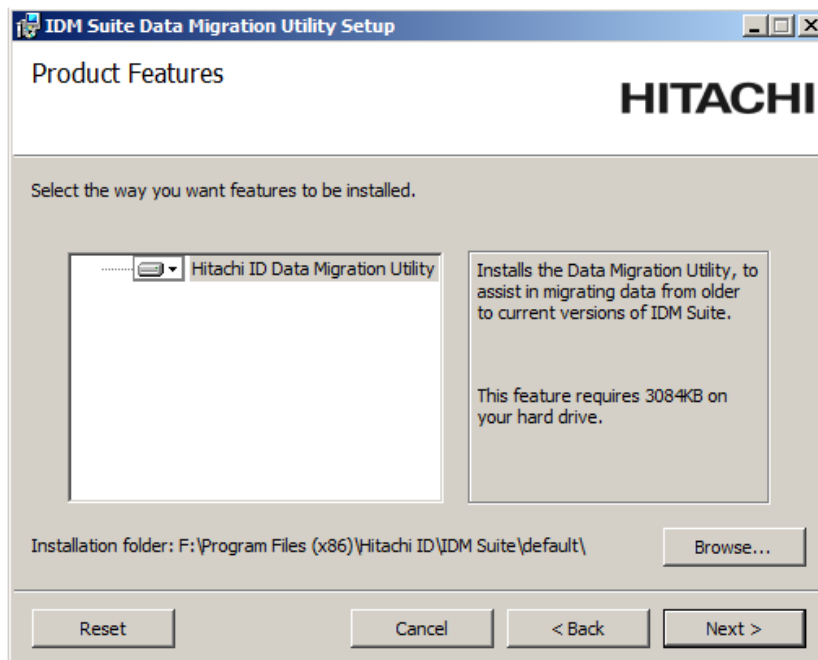
The **migratedata** utility will create the export SQLite database. If the SQLite database file already exists, then it will be updated but the password must match the one used to create the database file.

Table 15.1: migratedata data type arguments

Argument	Description
-qaconfig	Question set configuration (qdef+qset tables) Security question configuration settings and lists of custom questions.
-qadata	Question set data (response+responseq tables) Answers provided by the users for the security questions.
<b>Note:</b> -qaconfig is required when -qadata is specified.	
-madmin	Target system credentials (madmin table) Administrator credentials configured for target systems.
-mobilereg	Mobile registrations (usermobiledevice table) Mobile device registration data for users that have registered a Hitachi ID Bravura One App with the <i>Bravura Security Fabric</i> server.
-pamteam	<i>Bravura Privilege</i> team management data Configuration of teams, including team groups, members, privileges, systems and accounts
-force-pamteam-export	Force export of <i>Bravura Privilege</i> team management data, even if there are checked out managed accounts. Checked out managed accounts will be considered checked in.
-pwhistory	Password history (history table) List of passwords reset by users when password history is enforced in the password policy rules.
-userstat	Userstat tags (userstat table) Userstat tags/records and their values set for users for specific actions.
-userattr	Profile attributes that didn't come from a target (userattr table) Profile and request attributes that have values stored in the database and are not read in from any targets.
-userauth	Profile lockout/disabled-ness (userauth table) User profiles that have been locked out or disabled by the help desk.
-all	All of the above data types

### 15.3.2 Importing data to the current (destination) version

1. Locate a copy of the `migratedata.msi` Windows installer from Hitachi ID.
2. Copy `migratedata.msi` to the computer where the current (destination) instance is installed.
3. On the computer where the destination instance is installed, run `migratedata.msi`.
4. On the **Product Features** page, ensure that **Installation folder** is set to the directory where the destination instance is installed; for example, the following destination instance is installed under `F:\Program Files (x86)\Hitachi ID\IDM Suite\default`:



5. Continue with the remaining wizard pages to install `migratedata`.  
If you do not have at least SQL Server Native Client 2008 installed, you will receive a warning and installation will not proceed until it is installed. Upon completion of the installation process, `migrate-data.exe` will be available in the `\util` sub-directory of the location specified for **Installation folder**.
6. Copy the SQLite database file you created in [Exporting data from the older \(source\) version](#) to the computer where the *Hitachi ID Bravura Security Fabric* instance is located for the current version.
7. (Optional) Perform a dry run (i.e. not actually import data into the backend database used by the instance).

You can do this by running `migratedata` in the destination instance's `\util` sub-directory with the following parameters:

```
migratedata.exe -action dryrun -file <dbfile> <datatype> -log <logfile>
```

where:

- `<dbfile>` is the SQLite database file from Step 6.

- `<datatype>` is one of the data type values listed in [migratedata data type arguments](#) to be imported.
  - `<logfile>` is the file used to log the results.
8. (Optional) Enter the password used to encrypt the data key in the database file.
  9. (Optional) Review the dry run results for any errors.
  10. To import the data, run **migratedata** utility in the destination instance's \util sub-directory with the following parameters:  

```
migratedata.exe -action import -file <dbfile> <datatype> -log <logfile>
```

where:

    - `<dbfile>` is the SQLite database file from Step 6.
    - `<datatype>` is one of the data type values listed in [migratedata data type arguments](#) to be imported.
    - `<logfile>` is the file used to log the results.
  11. Enter the password used to encrypt the data key in the database file.
  12. Review the results of the migration and then proceed to verify the upgrade.

**Note:** If **migratedata** seems to hang on import, wait for its timeout (30min) before killing the process.

**Note:** Do *not* left-click on the command prompt screen when a console app is running, especially for apps like **migratedata** which takes a long time to complete.

If something is selected in the command console while **migratedata** runs, it may seem that the process is stuck, but in fact the command prompt is paused, waiting for the user to do something with the selection; in that case, press any key (e.g. **[Delete]**) to remove the selection and allow the prompt to continue processing.

## 15.4 Items to verify after the data migration

### Question set configuration

Confirm that:

- Any customized settings for the question sets such as for user-defined and pre-defined are present.
- Any custom pre-defined questions that existed in the older version are also now present in the current version after the data migration.

### Security questions

Confirm that:

- A user's security questions and answers match those from the imported data. For example, user-defined as well as pre-defined question sets for both built-in and custom security questions. Previously defined question sets for the account that existed on the current instance will be replaced.
- A user is able to authenticate to self-service using the security questions and answers from the imported data.
- A user is able to use the "Test mode" for all of their security questions successfully when valid answers from the imported data are provided.
- If configured to do so, a help desk administrator may see the list of the user's security questions and they are from the imported data.

### Password history

Confirm that:

- A user is unable to reset their password to a value that is in the password history from the imported data following the password policy.
- A user is able to reset their password to a new value that is not in the password history.
- A help desk administrator is unable to reset the password for a user to a value that is in the password history from the imported data.
- A help desk administrator is able to reset the password for a user to a new value that is not in the password history.

### Profile attributes

Confirm that:

- Values for a user's profile attributes are replaced with the values from the attributes in the imported data.

## Statutes for profile lockout and profile enabled/disabled

Confirm that:

- The status for whether or not a user's profile is locked out when a user has provided too many bad authentication attempts to self-service and has locked out their profile is replaced with the status from the imported data.
- The user will be unable to login to self-service if their profile is locked out.
- A help desk administrator is able to see whether or not a user's profile is locked out or not.
- The status for whether or not a user's profile has been disabled for when a help desk administrator has disabled their profile is replaced with the status from the imported data.
- The user will be unable to login to self-service if their profile is disabled.
- A help desk administrator is able to see whether or not a user's profile is disabled or not.

## Userstat tags

From the instance after the import is complete, locate and run the Userstat report. The Userstat report will include records for the users from the imported data. For example, the report output will show the PSQDONE userstat tag for users from the imported data that had completed their security questions profile.

## Target system credentials

Confirm that:

- Target system credentials are imported, assuming that the target systems exist on the current version and matches the target system IDs of the older version. If a target system exists on the current version and already have credentials defined, its password will be overwritten during import.
- Target system credentials are not exported if the target system does not exist on the current version.
- Target system credentials of onboarded systems are associated with the same *Bravura Privilege* managed account, if associated in the previous version.

## Mobile device registrations

Confirm that:

- A user is able to use the Hitachi ID Bravura One App on their mobile device to login to and access *Bravura Security Fabric* for devices that were previously registered.
- If configured, a user is also able to still authenticate successfully for Computer Login on the desktop for a mobile authentication chain to scan a QR code using the mobile device.
- The mobile devices are not required to be re-registered.

## Team management

Confirm that:

- The team admin from the previous version will still be able to create teams, manage group membership of teams, and delete teams.
- In versions 12.0 and newer, the trustee privilege is broken down into several trustee privileges, including Team trustee, System trustee, Account trustee, Vault trustee, OTP trustee, LC trustee and Subscriber trustee. By default, the trustee user from the previous version will have all of these privileges.

Refer to the [Bravura Security Fabric Documentation](#) for more information about trustee privileges.

- The same systems and accounts are present in the current version.
- The same team vaults and vault accounts are present in the current version.
- The same OTP API user accounts are present in the current version.
- Account settings, such as disclosure method, session monitoring, and randomize/override settings are unchanged.
- Managed account and vault account passwords are unchanged.
- Vaulted files can be downloaded as normal.
- Managed accounts previously checked out before migration are checked in, and can be requested and checked out as normal.
- Personal admins continue to have unrestricted access to the managed accounts they are entitled to.
- Users with Requesters, Approvers, Auto-approved, and Credential manager privileges in the previous version will continue to have the same access in the current version.
- Users that were help desk trustees before migration continue to have help desk privileges in the current version.
- Target system credentials of onboarded systems are associated with the same *Bravura Privilege* managed account, if associated in the previous version.

## Description

Use the **upgradetest** program to check for potential problems with updating the database. It runs all the necessary **patchdb** scripts to make sure there are no surprises from the database side. Before running this tool, you have to copy the production database to another server

## Preparation

Before running **upgradetest**:

1. Copy the instance database to another SQL server.
2. Set up an account that has access to it.
3. Copy the installation package to the new server.

## 16.1 Usage

```
upgradetest.exe -db <database> -s <server> [ -u <user> ] [ -windowsauth ]
```

Table 16.1: upgradetest arguments

Argument	Description
-db, --db <database>	Name of the database to upgrade (required)
-s, --server <server>	Address of SQL Server backend (required)
-u, --username <username>	User name to connect to SQL Server backend with
-windowsauth	Use Windows authentication using the current user (do not prompt for password)

## 16.2 Examples

```
upgradetest.exe -s sqlserver -db enterprisedb -u sqladmin
```



# **Appendix**

# File Locations

---

# A

This chapter provides details of the location and purpose of files installed by:

- *Hitachi ID Bravura Security Fabric* (p77)
- *Hitachi ID Connector Pack* (p82)

When you install any Hitachi ID Systems product, the default path for program files is:

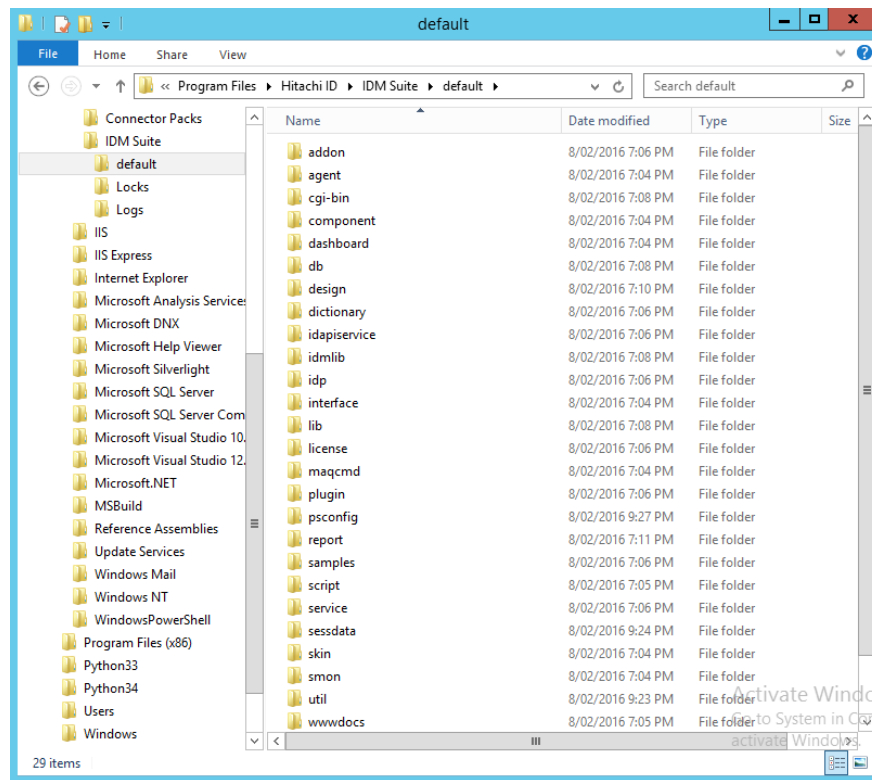
C:\Program Files\Hitachi ID\

## A.1 *Bravura Security Fabric* directories and files

There are three main directories that are created when you install *Bravura Security Fabric* instance:

- <Program Files path>\Hitachi ID\IDM Suite\<instance>\
- <Program Files path>\Hitachi ID\IDM Suite\Logs\<instance>\
- <Program Files path>\Hitachi ID\IDM Suite\Locks\

The contents of those directories are detailed in the following subsections.



It is recommended that you do *not* change these directory locations during the setup process. You cannot install any of the directories required for *Bravura Security Fabric* on a mapped drive.

### A.1.1 Instance directory

[Instance directory files](#) describes the function of directories that are created when an instance of *Bravura Security Fabric* is installed.

**Note:** Directories marked with ★ include files installed by *Connector Pack*.

Directories marked with ★★ include folders and files installed with the optional *Analytics* app.

Directories marked with † include optional files. They are only installed in a complete installation or if selected in a custom installation.

Table A.1: Instance directory files

Directory	Contains
† * addon	Files required for add-on software, such as Password Manager Local Reset Extension and secure kiosk account (SKA). Some files, required to target Netegrity SiteMinder, are installed by <i>Connector Pack</i> . If you installed a global <i>Connector Pack</i> , these files are contained in the <i>Connector Pack</i> global directory.
* agent	Instance-specific user management connectors (agents). If you installed a global <i>Connector Pack</i> , user management connectors are contained in the <i>Connector Pack</i> global directory.
** analytics	<i>Analytics</i> app specific folders
** analytics\DataSets	Contains *.rsd files which are Shared Dataset Definitions. These files are only used by SQL Server versions higher than Express. They contain datasets that are shared between reports.
** analytics\Hidden	Contains *.rdl files which are Report Definitions. These files are the drillthrough reports used by other reports. They are not visible to the end-user.
** analytics\ReportItems	This folder contains other folders. Each folder in this folder is a category in the <i>Analytics</i> app. Within these folders are *.rdl files which are Report Definitions. The folders need to be added to the <b>CUSTOM ANALYTIC CATEGORIES</b> system variable to be visible. These reports are then visible to the end-users in the <i>Analytics</i> app.
cgi-bin	The user web interface modules (*.exe CGI programs).
db	The <i>Bravura Security Fabric</i> database SQL scripts.
db\cache	Search engine temporary search results. These files are cleaned up nightly by <b>psupdate</b> .
db\replication	Stored procedure replication queues, and temporary replicated batch data.
* design	Files necessary to make modifications to the GUI. Some files are installed by <i>Connector Pack</i> . If you install a global <i>Connector Pack</i> , files related to connectors are located in the global design directory. See the <a href="#">Bravura Security Fabric Documentation</a> for details.
dictionary	A flat file, <b>words.dat</b> , that contains dictionary words. <i>Bravura Security Fabric</i> uses this file to determine if new passwords fail dictionary-based password-policy rules.
idapiservice	Files required to use the SOAP API.
* interface	Instance-specific ticket management connectors (exit trap programs). If you installed a global <i>Connector Pack</i> , ticket management connectors are contained in the <i>Connector Pack</i> global directory.
lib	Contains the <b>pslangapi.dll</b> .
license	The license file for <i>Bravura Security Fabric</i> .
plugin	Plugin programs executed by <i>Bravura Security Fabric</i> .

... continued on next page

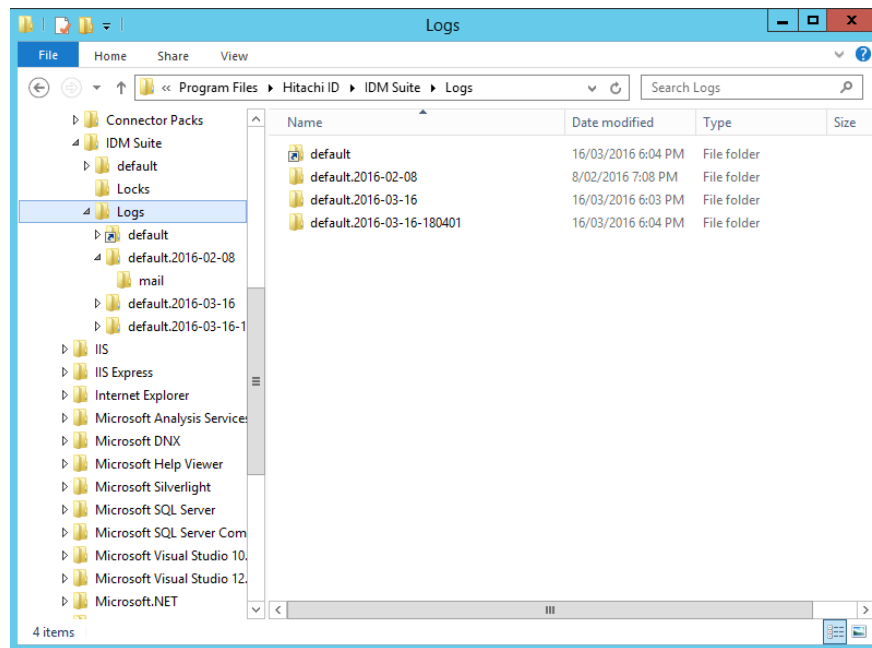
Table A.1: Instance directory files (Continued)

Directory	Contains
psconfig	List files produced by auto discovery and the <code>idmsetup.inf</code> file.
report	Files and programs for report generation.
† ★ samples	Instance-specific sample scripts and configuration files. If you installed a global <i>Connector Pack</i> , connector-related sample files are contained in the <i>Connector Pack</i> global directory.
script	Configuration files and scripts used by connectors, <code>psupdate</code> , plugins and interface programs.
service	Service programs.
sessdata	Session data. A scheduled program removed old data files nightly.
skin	Compiled GUI files used at run-time (HTML and *.z).
smon	Monitored session data. This location can be changed by <i>Recorded session management</i> (SMON) module options.
★ util	Command-line programs and utilities. If you install a global <i>Connector Pack</i> , tools related to connector configuration are located in the global util directory.
★ unix	The <code>psunix</code> archive, which is required to install the Unix Listener and supporting files on a Unix-based target system. If you installed a global <i>Connector Pack</i> , this directory is created in the <i>Connector Pack</i> global directory.
wwwdocs	Images and static HTML pages used by <i>Bravura Security Fabric</i> .

### A.1.2 Log directory

Any operation that is run by *Bravura Security Fabric* is logged. Those logs are invaluable when debugging an issue. The log directory by default is `C:\Program Files\Hitachi ID\IDM Suite\Logs\`. Each instance of *Bravura Security Fabric* that is installed will have at least one sub-directory within this directory.

The `rotatelog` scheduled job, which runs on a nightly basis, rotates the logs in to a new folder, to reduce disk space usage.



See the [Bravura Security Fabric Documentation](#) for more information.

### A.1.3 Locks directory

Certain target systems can only be accessed serially, such as Lotus Notes. This is a limitation of the API used to access the target system. In these cases *Bravura Security Fabric* drops a *lock file* in the locks directory when an operation is being performed that should only be performed serially. For this reason the locks directory *must* be the same for all instances of *Bravura Security Fabric* that are installed on the same server.

See the [Bravura Security Fabric Documentation](#) for more information.

## A.2 Connector pack directories and files

When you install *Hitachi ID Connector Pack*, files are placed in different locations depending on type of *Connector Pack*.

For an instance-specific connector pack, the installer, **connector-pack-x64.msi**, installs connectors and supporting files in:

`<Program Files path>\Hitachi ID\IDM Suite\<instance>\`

For a global connector pack, the installer, **connector-pack-x64.msi**, installs connectors and supporting files in:

`<Program Files path>\Hitachi ID\Connector Packs\global\`

[Connector Pack directory files](#) describes the function of directories that are created when a *Connector Pack* is installed:

Table A.2: Connector Pack directory files

Directory	Contains
addon	Files required to target Netegrity SiteMinder systems
agent	User management connectors (agents)
design	<i>Connector Pack</i> -related files necessary to make modifications to the GUI; for example target system address help pages. See the <a href="#">Bravura Security Fabric Documentation</a> for details.
interface	Ticket management connectors (exit trap programs)
samples	Sample scripts and configuration files
unix	The <b>psunix</b> archive, which is required to install the Unix Listener and supporting files on a Unix-based target system
util	Tools to support the configuration of various target systems