

Bravura Security Fabric

Upgrading

This document shows you how to deploy a newer version of *Hitachi ID Bravura Security Fabric* by using the **setup** program.

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

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

An upgrade using **setup** is usually sufficient to take advantage of feature improvements and performance enhancements in a newer version. 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. This document does not cover these cases.

WARNING!: Using **setup** to perform upgrades and patches is simple; however proper research, analysis, and planning is required to ensure that it works. This should be carried out by someone familiar with deploying *Bravura Security Fabric*. Contact support@Hitachi-ID.com for assistance.

See also:

- For more detail about upgrade use cases and processes, see the *Bravura Security Fabric* Upgrade Reference Manual.
- For information about the migration process, see the *Bravura Security Fabric* Migration Reference Manual.

1 Research and analysis

Before you start, gather information about your environment to ensure the feasibility of an upgrade or patch, and to help you plan the change. Carefully analyze configuration parameters and files to determine what needs to be upgraded, and how.

1.1 Inventory of systems

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 including:

- ☐ *Bravura Security Fabric* servers
- ☐ Target systems
- ☐ Managed resources – Local service installations
- ☐ Systems that have *Bravura Security Fabric* software components installed on them.
- ☐ Other technologies that support *Bravura Security Fabric*

1.2 Product considerations

- ☐ Databases

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

If the upgrade or patch 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.

- ☐ Analytics

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

- ☐ Replication configuration

Establish a window of time to perform the upgrade or patch when all replication nodes can be offline.

- ☐ 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.

- ☐ Services

After an upgrade or patch, 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 or patching.

☐ 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.

☐ 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.

☐ Language packs

Check the Hitachi ID Systems portal or contact 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.

☐ Web server configuration files

The *Bravura Security Fabric* server must have a running web server. Microsoft Internet Information Services (IIS) is supported for automatic configuration by *Bravura Security Fabric*'s installer.

☐ Supporting systems

Supporting systems can include systems with *Bravura Security Fabric* software components installed on them, and other technologies that support the *Bravura Security Fabric* server.

In particular, each local service will require redeployment for workstations to allow reintegrating to the new instance.

☐ Python

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

☐ Connector Pack compatibility

Bravura Security Fabric 12.1.x is only compatible with *Connector Pack* 4.0.2 or higher.

☐ Hitachi ID Bravura One App

Hitachi ID Bravura One App must be the same version as the instance so ensure this is included in your upgrade plan.

☐ 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](#) (p14).

☐ 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.

☐ 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 using **svcaccount**, see the *Bravura Security Fabric Reference Manual*

- *Bravura Privilege*

Review managed system policies, session monitoring privileges, trustee privileges.

See the *Bravura Security Fabric Upgrade Reference Manual* for more detailed information about researching for upgrades.

2 Planning

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

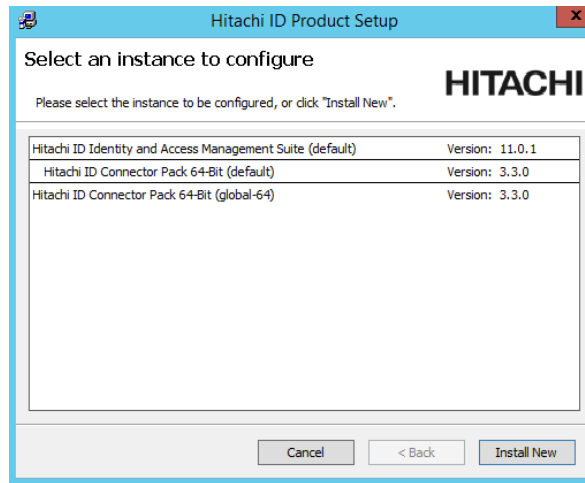
- A *test plan* that can measure whether or not the old and new instances behave as expected
- A *backup and recovery plan*
- A *change control plan* to minimize downtime of the production system
- A *communications plan* to prevent calls to the help desk during the process

3 Upgrading Connector Pack

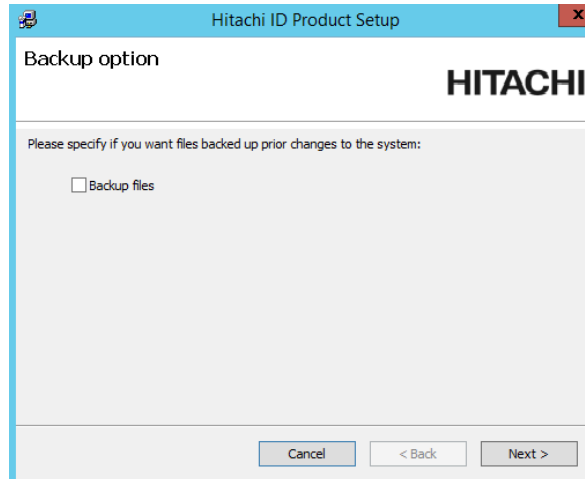
Note: When upgrading the connector pack, you must use the **setup** program that comes with the connector pack.

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.

4 Upgrading an instance

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.

4.1 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:
 - (a) Windows updates are applied.
 - (b) There are no critical problems in the Windows event log.
 - (c) There are no critical problems in *Hitachi ID Bravura Security Fabric* health checks.
 - (d) The node has at least 50GB free.
 - (e) The database server has at least 50GB free.
 - (f) 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.

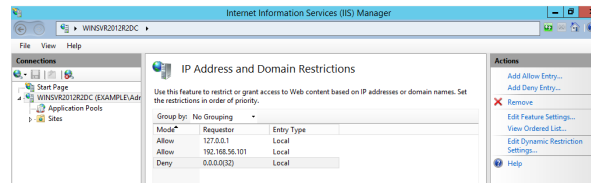



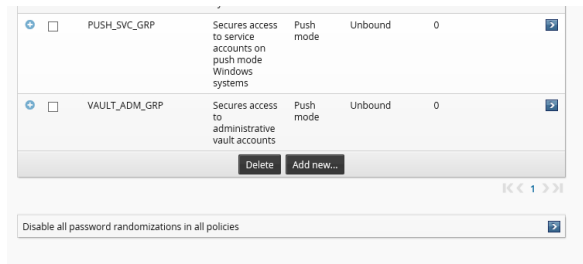
Table 1: IP and Domain Restriction settings

| 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**.

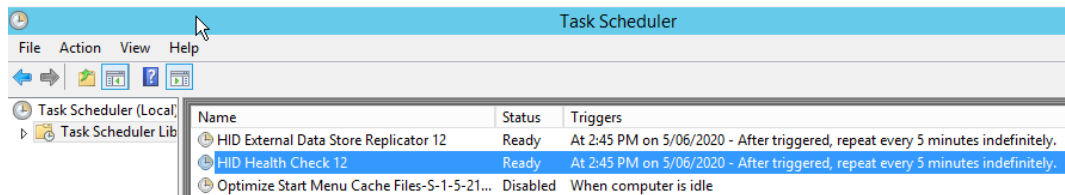
- (c) Scroll to the bottom of the page.
- (d) Select  **Disable all password randomizations in all policies.**
- (e) Click **OK** to confirm the selection.



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.

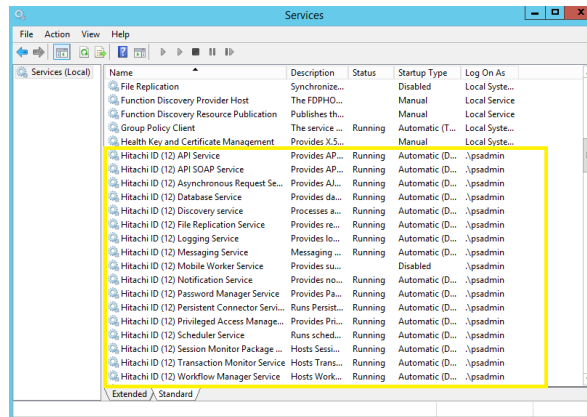
8. Disable Hitachi ID Systems tasks in the OS task scheduler.



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 patch.
- 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 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+.

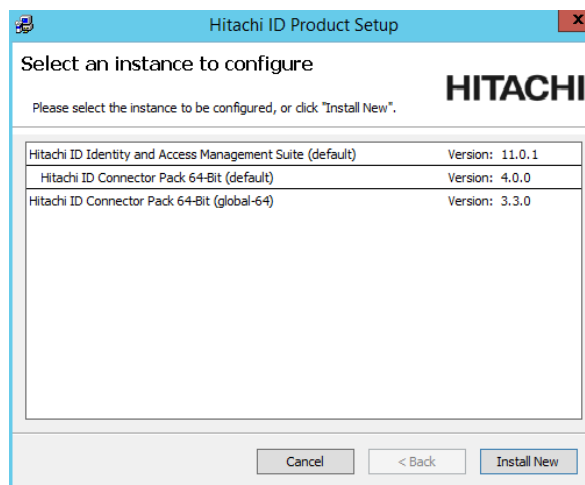
Note: Keep the old version of Python to uninstall the old version of *Bravura Security Fabric*. If the old version of Python is removed, then Python 3.7.3+ location must be added into system path.

4.2 Upgrade using installer

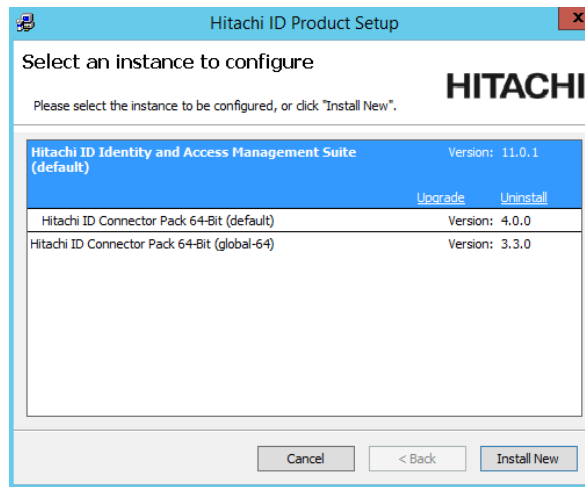
To run the installer:

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.

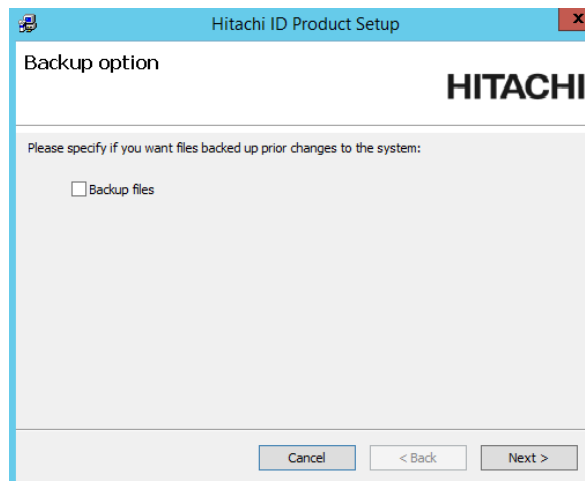


2. Select the instance you want to upgrade or patch, then click the **Upgrade** link for that instance.

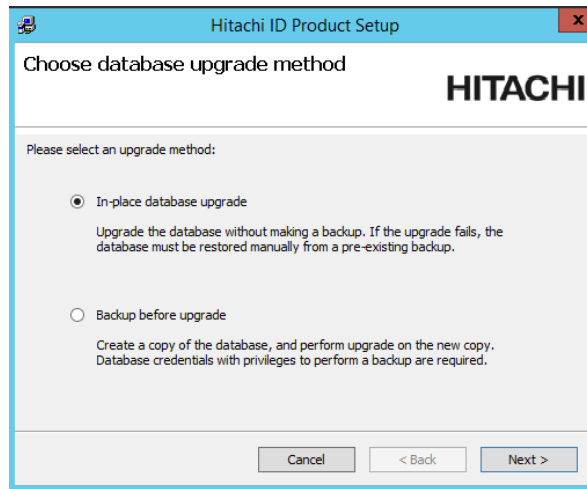


If the instance you want is not listed, refer to [Preparation](#).

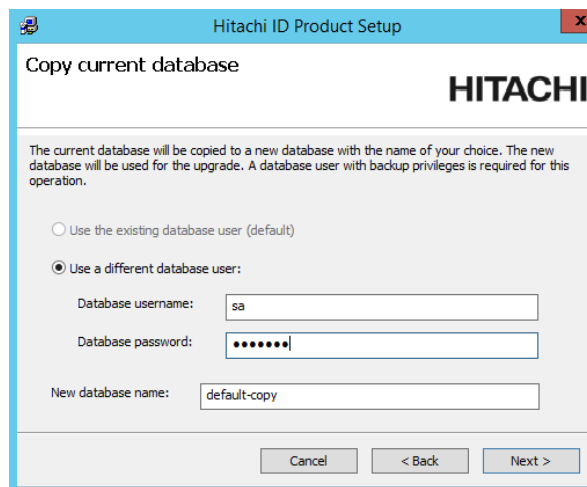
3. Read the product setup warning and click **Yes** to continue.
4. Enter the **psadmin** credentials.
5. Click **Next** after the pre-installation check.
6. Select **Backup files** if you want the installer to backup the files.



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



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



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.

4.2.1 Completing the upgrade process

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

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.

4.3 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.
- 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 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 fails on any node collect the upgrade log and send it to 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 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 failed on a production instance, revert it using the [backups](#) (p9).
- If the failed on a test instance, leave it as is (make sure the services are off and the Database Service 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 for help with this.

4.4 Post upgrade

4.4.1 Post upgrade steps

During the process, the installer starts all services and tasks. After installer has successfully completed 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, and set to "Manual" as described in Step 10 and Step 11 in [Preparation](#).
2. Once all nodes are , 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.

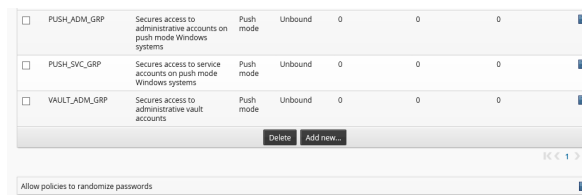
If hybrid or shared schema database replication is configured:

- (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.
- If sample scripts from previous versions are used, review the new sample scripts and update the currently-used scripts.
 - 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.
 - Re-enable password randomization.
 - Log in to *Bravura Security Fabric*.
 - Click **Manage the system** → **Privileged access** → **Managed system policies**.
 - Scroll to the bottom of the page.
 - Select  **Allow policies to randomize passwords**.
 - Click **OK** to confirm the selection.



- Load and patch components on the primary node:
 - From a command prompt, navigate to the instance directory.
 - Run the command:
`instance.bat`
 - 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](#) (p7).

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.

4.4.2 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.

4.4.3 Verifying the upgrade

After running **setup** to , 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](#) (p4) 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.

4.4.4 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).

4.4.5 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.

5 Upgrading Local Workstation Service software

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.

6 Upgrading the proxy server

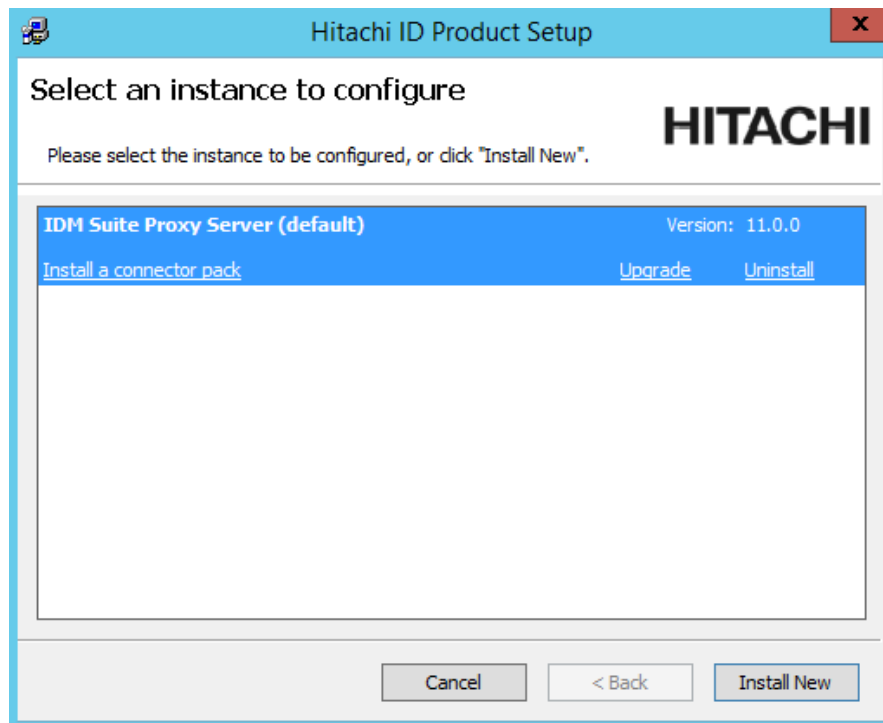
This chapter shows you how to a *Hitachi ID Bravura Security Fabric* proxy server using the **setup** installer.

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 a proxy server:

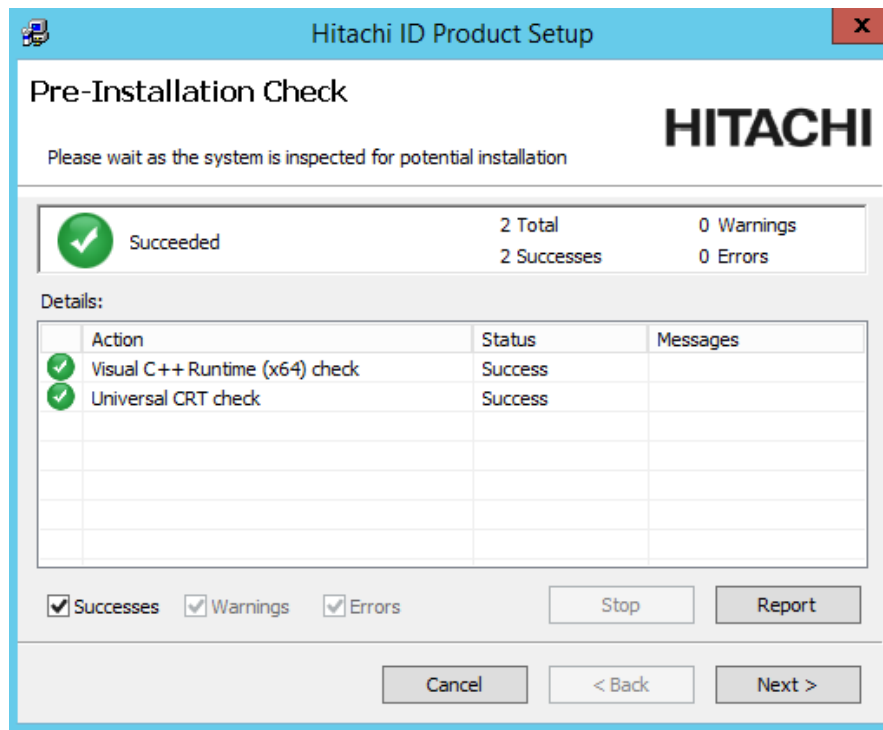
1. Run **setup** with the 12.x **msi**.

Setup shows you the list of existing instances on the server. Select the one you want to , 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 .
5. Click **Next**.
The proxy server will be .
6. Click **Finish** to exit.

See also:

- See the *Bravura Security Fabric Upgrade Reference Manual* for more detailed information about upgrades.
- See the *Bravura Security Fabric Migration Reference Manual* for detailed information about migrations.