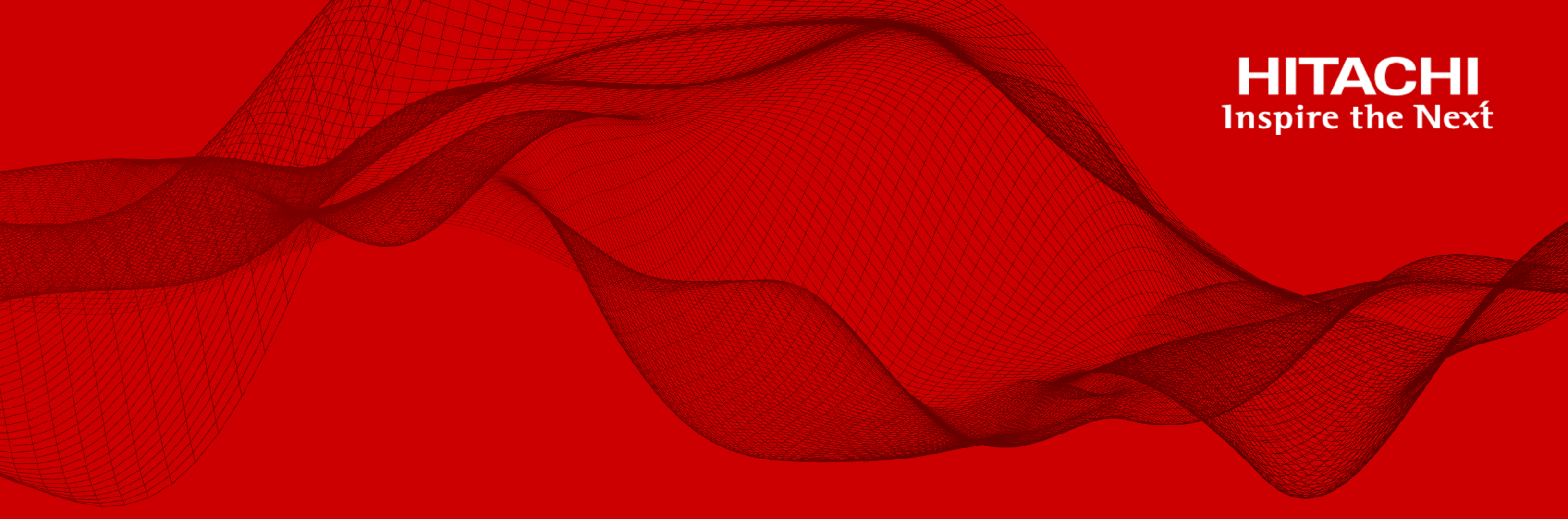


Hitachi ID Systems Shell Extension

Configuration Guide

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

Contents

About This Document 1

This document provides information about the installation and configuration of Hitachi ID Systems Shell Extension on an enterprise network. It supplements the *Hitachi ID Bravura Group* documentation. It is intended for network or IT administrators.

1.1 Conventions

This document uses the following conventions:

This information . . .	displayed in . . .
Variable text (substituted for your own text)	<*angle brackets*>
Non-text keystrokes – for example, **[Enter]** key on a keyboard.	**[brackets]**
Terms unique to *Hitachi ID Bravura Security Fabric*	*italics*
Button names, text fields, and menu items	**boldface**
Web pages (names)	***italics and boldface***
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

1.2 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.

If you require technical assistance with *Hitachi ID Bravura Group*, contact support@Hitachi-ID.com.

Introduction 2

The Hitachi ID Systems Shell Extension works in conjunction with *Hitachi ID Bravura Group* to allow efficient access to protected network resources, for example – folders/shares, managed Microsoft Active Directory groups, printers, etc.

Once installed, the *Shell Extension* is embedded into the operating system. Instead of logging into *Bravura Group*, requesting access is as simple as a right-click or double click on the protected resource.

Using the *Shell Extension* facilitates a simpler user experience. Users are led directly to the *Bravura Group* page for the network resource to which they want to request access. Previously, users needed a better working knowledge of *Bravura Group* in order to perform the same task.

Hitachi ID Systems Shell Extension integrates seamlessly with the operating system and is a transparent addition to *Bravura Group*.

> **Note:** All shared resources will reveal the "Request Access" option when opening the context menu by right-clicking the resource.

Before the *Shell Extension* can be installed, you must have the following installed:

- *Bravura Group* – see the *Bravura Security Fabric* Documentation
- "Windows Active Directory DN" connector (**`agtaddn`**) from the *Hitachi ID Connector Pack* – see the Connector Pack Integration Guide
- Active Directory – see the Connector Pack Integration Guide

Hitachi ID Systems Shell Extension supports both 32 bit and 64 bit systems, including Windows 7/Vista and newer.

Installing and Configuring *Shell Extension* 3

You can install the Hitachi ID Systems Shell Extension software:

- Manually using the MSI installer (p4)
- Automatically using a group policy object (p6)

3.1 Manually installing the *Shell Extension*

1. Download the **hidshext.msi** installer to the client workstation. If the client workstation is running 64-bit Windows, use **hidshext-x64.msi** instead.

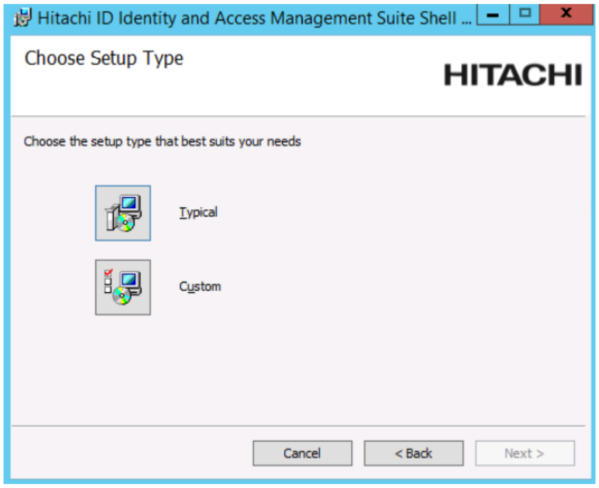
   The installer is located in the addon directory. If it is not, ensure that the add-ons subfeature of *Hitachi ID Bravura Group* was selected during installation, or run the *Hitachi ID Bravura Security Fabric* installer again, modify the installed instance, and select it.

2. Launch the MSI installer with administrator privileges.

   Click **Next**

3. Read and accept the license agreement. Click **Next**.

   The installer displays setup types for you to select from.



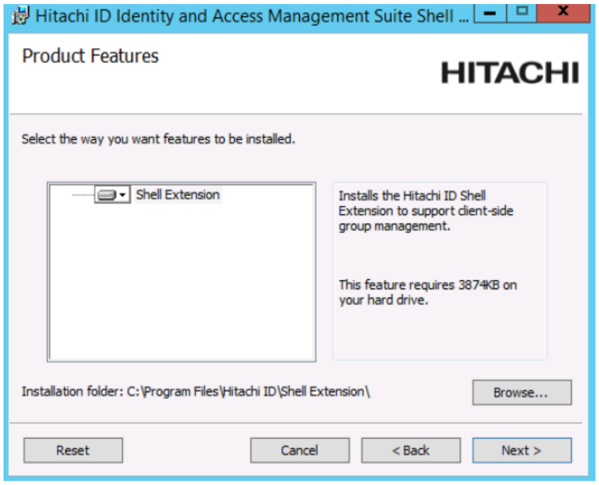
Hitachi ID Identity and Access Management Suite Shell ...

Choose Setup Type

Choose the setup type that best suits your needs

4. Select:
   - **Typical** to install with the default settings.

     Or,
   - **Custom** to customize the installation directory.



Select the way you want features to be installed.

Installs the Hitachi ID Shell Extension to support client-side group management.

This feature requires 3874KB on your hard drive.

Installation folder: C:\Program Files\Hitachi ID\Shell Extension\

   Click **Next**.

5. Configure the connection to the *Bravura Security Fabric* server:
   - **Hitachi ID Management Suite URL:** the URL of the *Bravura Security Fabric* server instance.
   - **Active Directory Target System ID:** the name of your Active Directory target within the *Bravura Security Fabric*.

   Click **Next**.

6. Click **Install** to start the installation.
7. Click **Close** to complete when installation has finished.

   You are prompted to restart your system.

3.2 Installing automatically

You can easily deploy Hitachi ID Systems Shell Extension to a group of users or computers using a Windows group policy to automate the installation of the client software. If you want the MSI installer to install automatically with no end-user interaction, you must set installation options by applying a Windows Installer Transform file (.mst) or by modifying the MSI installer with an MSI editor. See the section on Customizing the *Shell Extension* client installer (p8) for more information. The installer must be run with administrative privileges.

For information about installer command-line options, visit:
`https://docs.microsoft.com/en-us/windows/win32/msi/standard-installer-command-line-options`

3.2.1 Configuring a group policy for unattended software installation

The following steps outline the general procedure for configuring a group policy to deploy an installer package to computers in a domain (see your Windows help for more information). You must perform these steps using administrator privileges:

> **Note:** The following steps are for Active Directory 2012R2, installed on Windows Server 2012R2. Details may vary depending on your version of Windows.

1. Log into a domain controller.
2. Copy the installer package and any transform files you have created to a shared folder with access granted to all target machines.
3. Launch Server Manager.
4. Click **Tools** → **Group Policy Management**.
5. If necessary, create a new group policy. To do this, right click on the container where you wish to create the group policy; for example, the container in which the computers reside.
6. Select **Create a GPO in this domain, and Link it here...**, and type a unique name for the policy. For example, `IDM Suite software policy`.
7. Click **OK**.
8. Ensure the group policy is applied only to the appropriate users, computers, or groups:
   (a) On the left hand side, select the policy you just created. You may need to expand the tree before you can view the new policy.
   (b) Select the **Delegation** tab.
   (c) Click the **Advanced. . .** button.
   (d) Select the Authenticated Users group.
   Under the permissions for this group, clear the **Allow** checkbox for the **Apply Group Policy** permission.
   (e) Click **Add**, type name of the users, computers, or groups to add, then click **OK**.

   (f) Select each user, computer, or group for which you want to apply the group policy. Under the permissions for this object, select the **Allow** checkbox for the **Apply Group Policy** permission.

   (g) Click **OK** to return to the **Group Policy Management** snap-in.

9. Select the group policy you want to modify, then click **Edit. . .** .

   The **Group Policy Management Editor** snap-in displays.

10. Expand **Computer Configuration** → **Policies** → **Software Settings**.

11. Right-click **Software installation** and select **New** → **Package. . .** .

    The **Open** dialog box appears.

12. Browse to the shared folder (UNC path) where you copied the MSI, select the file, then click **Open**.

    The **Deploy Software** dialog appears.

13. Choose **Advanced**, then click **OK**.

    The properties dialog for the package appears.

14. Select the **Modifications** tab. Click **Add**. In the Open dialog box, browse to the transform file (**.mst**), then click **Open**.

15. Click **OK**.

    The package is assigned immediately. The installation is performed when it is safe to do so, typically when the computer starts up.

16. Close the **Group Policy Management Editor** and the **Group Policy Management** snap-in.

3.2.2 Customizing the *Shell Extension* installer

The following options for the Hitachi ID Systems Shell Extension client installer can be set on the command-line (quiet install), contained in a Windows Installer Transform file, or modified with an MSI editor such as Orca.

Table 3.1: *Shell Extension* custom install options

Option	Description
SHEXTURL	URL path, including server information, to the root virtual directory on the *Hitachi ID Bravura Group* server (http://<*server*>/<*instance*>/).
SHEXTTARGET	Name of the Active Directory target system in *Bravura Group*.

Example silent install command

```
msiexec /i hidshext.msi SHEXTURL=http://<server>/<instance>/ SHEXTTARGET=AD
/quiet
```

Modifying the installation properties with an MSI editor

Obtain an MSI editor such as Orca. Orca is a table editing tool that can be used to edit .msi files. Information on how to use Orca and where to download it can be found at: `https://docs.microsoft.com/en-us/windows/desktop/msi/orca-exe`.

To modify the properties with an MSI editor:

1. Use the editor to open the MSI installer.
2. Select the Property table.
3. If the property already exists, select it and edit its value. If the property does not exist, add the property and set its value.
4. Save the MSI installer package.

3.3 Advanced configuration

In the Windows registry, there are two registry entries to control the Hitachi ID Systems Shell Extension:

- IDAccessURL (p8)
- DisableHidShExt (p9)

WARNING!: Ensure that you are comfortable and knowledgeable in the mechanics of the registry before you attempt to change any configuration settings.

3.3.1 config

The *Shell Extension* gives you the option to change the URL for the Front-end (`PSF`) module.

To change the URL, modify the following registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Hitachi ID\IDM Suite\Shell Extension`

The registry key contains an entry named `IDAccessURL`. If you modify this entry, the change takes effect once you log out and log back into the workstation.

Entry name	Shell Extension
Value Data	IDAccessURL
Data Type	REG_SZ

Default Value `http://<server>/<instance>/?LANG=en-us&JUMPTOCGI=IDR&LINK= → NETWORKRESOURCES&NETRES_HOSTID=<AD name>`

For Example:

```
http://10.0.61.5/idmsuite/?LANG=en-us&JUMPTOCGI=IDR&LINK= →
NETWORKRESOURCES&NETRES_HOSTID=AD
```

3.3.2 disable

You have the option to disable the *Shell Extension* without removing the software.

To disable, modify the following registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Hitachi ID\IDM Suite\Shell Extension`

The registry key contains an entry named `DisableHidShExt`. If you modify this entry, the change takes effect once you log out and log back into the workstation.

Entry name `DisableHidShExt`

Value Data 0|1

- If set to 0 (false) *Shell Extension* is enabled
- If set to 1 (true) *Shell Extension* is disabled

Data Type REG_DWORD

Default Value 0

Using the *Shell Extension* 4

This chapter shows you how to use the Hitachi ID Systems Shell Extension to easily request access to network shares and network printers via *Hitachi ID Bravura Group*.

Requirements

Ensure that network resources within Microsoft Active Directory are set up according to the “Active Directory DN” chapter of the Connector Pack Integration Guide.

Bravura Group can only manage shares that have a network resource configured. The *Shell Extension* automatically creates a network resource if one does not exist when you request access to a network share. Network resources can also be manually created and modified.

For details on manual configuration, see the “Network Resources” and “Managed Groups” chapters in the *Bravura Security Fabric* Documentation .

For shares in Windows Server 2016 (and some versions of 2012) or higher, the **Enable access-based enumeration** option is on by default. You must disable this option in order to see the subfolders underneath and gain access.

To do this:

1. As domain administrator, open Server Manager.
2. Click **File and Storage Services** from the left panel.
3. Click **Shares**.
4. Right click the shares you want to manage and select **Properties**.
5. Click **Settings**.
6. Uncheck the **Enable access-based enumeration** option.

You can also disable this option via group policy.

4.1 Requesting access to a network share

To request access to a network share from your workstation:

1. Navigate to the network share to which you want to gain access.
2. Choose one of the following ways to request access:
   - Right-click the share and click **Smart Open**, or simply double-click the share. A message opens asking if you want to request permission. Click **Yes**.
   - Right-click the share and click **Request Access**.

   The *Hitachi ID Bravura Security Fabric* launches.
3. Enter your password and click **Login**.
4. Click the network share to which you want access.
5. If there are multiple groups available, check the box next to the group you want to join.

   Click **Continue**.
6. Click **OK** in the pop-up window to confirm submitting the request.

   Hitachi ID Bravura Group displays a notification stating that your request was successfully submitted. Click the **View request** link next to the message to view changes in the request.

If your request is approved by the authorizer, then you can access the network resource.

Appendices

File Locations A

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

- *Hitachi ID Bravura Security Fabric* (p13)
- *Hitachi ID Connector Pack* (p18)

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

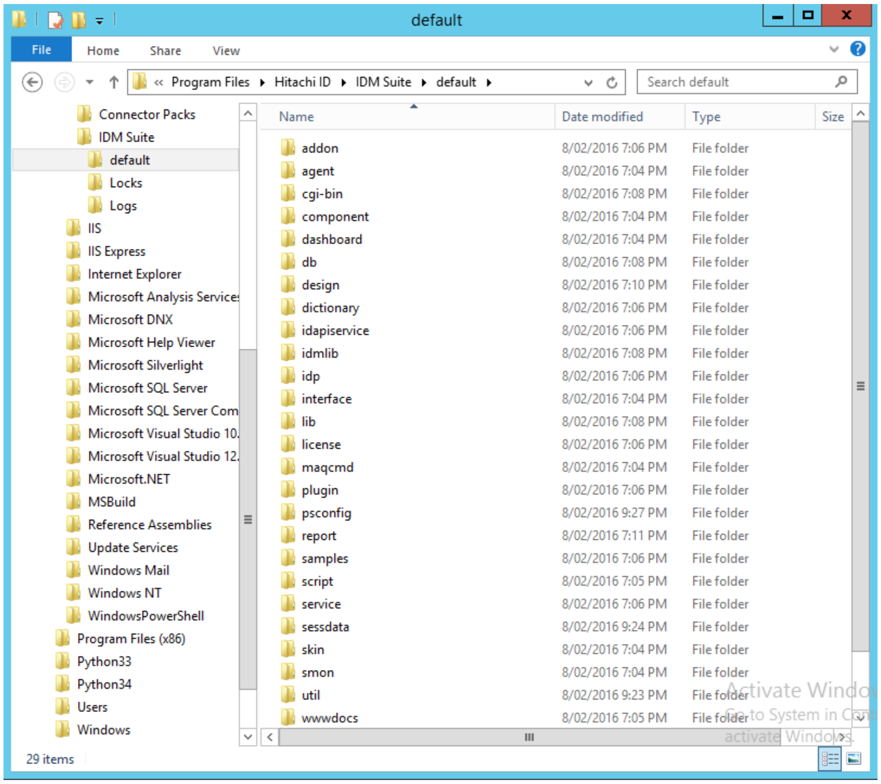
C:\Program Files\Hitachi ID\

A.1 *Bravura Security Fabric* directories and files

There are three main directories that are created when you install *Bravura Group* 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.



Name	Date modified	Type	Size
addon	8/02/2016 7:06 PM	File folder	
agent	8/02/2016 7:04 PM	File folder	
cgi-bin	8/02/2016 7:08 PM	File folder	
component	8/02/2016 7:04 PM	File folder	
dashboard	8/02/2016 7:04 PM	File folder	
db	8/02/2016 7:08 PM	File folder	
design	8/02/2016 7:10 PM	File folder	
dictionary	8/02/2016 7:06 PM	File folder	
idapiservice	8/02/2016 7:06 PM	File folder	
idmlib	8/02/2016 7:08 PM	File folder	
idp	8/02/2016 7:06 PM	File folder	
interface	8/02/2016 7:04 PM	File folder	
lib	8/02/2016 7:08 PM	File folder	
license	8/02/2016 7:06 PM	File folder	
maqcmd	8/02/2016 7:04 PM	File folder	
plugin	8/02/2016 7:06 PM	File folder	
psconfig	8/02/2016 9:27 PM	File folder	
report	8/02/2016 7:11 PM	File folder	
samples	8/02/2016 7:06 PM	File folder	
script	8/02/2016 7:05 PM	File folder	
service	8/02/2016 7:06 PM	File folder	
sessdata	8/02/2016 9:24 PM	File folder	
skin	8/02/2016 7:04 PM	File folder	
smon	8/02/2016 7:04 PM	File folder	
util	8/02/2016 9:23 PM	File folder	
wwwdocs	8/02/2016 7:05 PM	File folder	

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 Group* 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 Group* 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. Some files, required to target Netegrity SiteMinder, are installed by *Connector Pack*. If you installed a global *Connector Pack*, these files are contained in the *Connector Pack* global directory.
⋆ agent	Instance-specific user management connectors (agents). If you installed a global *Connector Pack*, user management connectors are contained in the *Connector Pack* global directory.
⋆⋆ analytics	*Analytics* 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 *Analytics* app. Within these folders are **`*.rdl`** files which are Report Definitions. The folders need to be added to the **CUSTOM ANALYTIC CATEGORIES** system variable to be visible. These reports are then visible to the end-users in the *Analytics* app.
cgi-bin	The user web interface modules (**`*.exe`** CGI programs).
db	The *Bravura Group* database SQL scripts.
db\cache	Search engine temporary search results. These files are cleaned up nightly by **`psupdate`**.
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 *Connector Pack*. If you install a global *Connector Pack*, files related to connectors are located in the global design directory. See the *Bravura Security Fabric* Documentation for details.
dictionary	A flat file, **`words.dat`**, that contains dictionary words. *Bravura Group* 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 *Connector Pack*, ticket management connectors are contained in the *Connector Pack* global directory.
lib	Contains the **`pslangapi.dll`**.
license	The license file for *Bravura Group*.
plugin	Plugin programs executed by *Bravura Group*.
psconfig	List files produced by auto discovery and the **`idmsetup.inf`** file.

. . . continued on next page

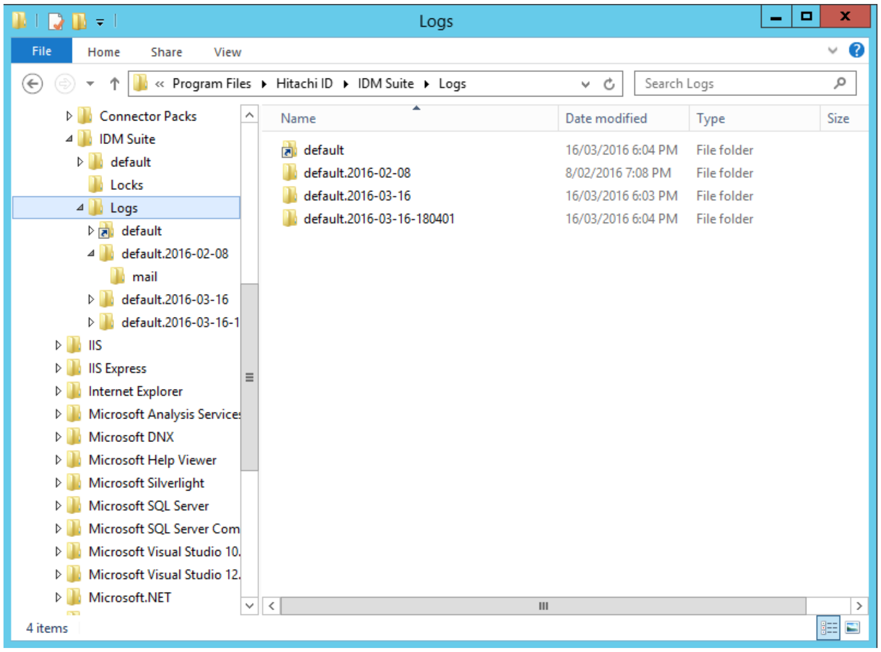
Table A.1: Instance directory files (Continued)

Directory	Contains
report	Files and programs for report generation.
† ⋆ samples	Instance-specific sample scripts and configuration files. If you installed a global *Connector Pack*, connector-related sample files are contained in the *Connector Pack* global directory.
script	Configuration files and scripts used by connectors, **psupdate**, 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).
⋆ util	Command-line programs and utilities. If you install a global *Connector Pack*, tools related to connector configuration are located in the global util directory.
⋆ unix	The **psunix** archive, which is required to install the Unix Listener and supporting files on a Unix-based target system. If you installed a global *Connector Pack*, this directory is created in the *Connector Pack* global directory.
wwwdocs	Images and static HTML pages used by *Bravura Group*.

A.1.2 Log directory

Any operation that is run by *Bravura Group* 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 Group* 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.



Name	Date modified	Type	Size
default	16/03/2016 6:04 PM	File folder	
default.2016-02-08	8/02/2016 7:08 PM	File folder	
default.2016-03-16	16/03/2016 6:03 PM	File folder	
default.2016-03-16-180401	16/03/2016 6:04 PM	File folder	

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 Group* 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 Group* 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	*Connector Pack*-related files necessary to make modifications to the GUI; for example target system address help pages. See the *Bravura Security Fabric* Documentation for details.
interface	Ticket management connectors (exit trap programs)
samples	Sample scripts and configuration files
unix	The **psunix** 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