

***Bravura Security Fabric* Training:**

Product Administration

:

Product administrators can use the *Hitachi ID Bravura Security Fabric* user interface to:

- Manage access rights
- Manage profiles
- Configure settings
- Manage other product administrators
- Manage resources

This document contains:

- [The *Bravura Security Fabric* URL](#)
- [Front-end login](#)
- [Use case: Logging in](#)
- [Use case: Changing the Administrator Password](#)
- [Finding Things](#)

Terminology

The following terminology is used in this document:

Module A part of the *Bravura Security Fabric* software that provides a specific set of functionality. Modules may be CGI programs or web apps. Some modules, such as the *Manage the system* (PSA) module, are used by analysts or administrators, and others are used by end users. Sometimes administrative modules are referred to as consoles. Modules may be CGI programs or web apps.

Front-end (PSF) module Provides an authentication and task selection point for all *Bravura Security Fabric* users.

***Manage the system* (PSA) module** Provides a means for product administrators to carry out core configuration and administration tasks from a web interface. This includes configuring *Bravura Security Fabric* objects and environment, managing processes and options, configuring individual features and functionality, and administering security.

Profile ID A unique identifier for a user in *Bravura Security Fabric*.

Regular user A user who has at least one account on a target system, and can log into *Bravura Security Fabric*. Regular users can be end users and/or product administrators.

End user A regular user who uses *Bravura Security Fabric* as self-service user, help desk user, workflow manager, or authorizer.

Product administrator A user who has been granted administrative privileges in *Hitachi ID Bravura Security Fabric*. The privileges control the access to administrative modules and the *Bravura Security Fabric* API. You can make a regular user a product administrator, or create dedicated accounts that are only used to manage the product. A product administrator is sometimes called a *console user*.

Superuser A product administrator who has all administrative privileges. You create the first superuser when you install *Bravura Security Fabric*. A superuser *cannot* be a regular user; that is, they cannot access self-service menus.

1 The *Bravura Security Fabric* URL

You can access the login page for the Front-end (PSF) by including the full path to the virtual directory in the URL:

Modified in
version 10.0.0

```
http[s]://<host name>/<virtual directory>
```

where:

http[s] If your web server is configured to use a secure connection type `https`. If not, type `http`.

Note: For security purposes, HTTPS should be used at all times. This is especially recommended for production environments.

<host name> This is your domain name, or *Hitachi ID Bravura Security Fabric* server name or IP address.

<virtual directory> If *Bravura Security Fabric* was installed using the default instance name, this is `default`; otherwise, this is the non-default instance name.

You can supply additional arguments, such as language preference, by including a question mark (?) in the *Bravura Security Fabric* URL. Separate multiple arguments using an ampersand (&). For example:

```
https://idm-server/default/?LANG=fr-ca&USERID=bobsmith
```

Note: For security reasons, arguments other than language and skin will be only be acknowledged when included in URLs for the root virtual directory or in URLs that redirect the user to the root virtual directory. In all other URLs, all arguments except language and skin will be ignored.

If the index page for your *Bravura Security Fabric* instance is set up (during installation) as your web server's default web page, you can access the Front-end (PSF) login page simply by typing the web server's URL in a browser. For example:

```
https://idm-server.example.com
```


2 Front-end login

You can customize the login and authentication process for product administrators and end users in many ways. In general, the front-end login process for *product administrators* works as follows:

1. Navigate to the [URL \(p2\)](#) for the front-end login page in a browser.

On your *Hitachi ID Bravura Security Fabric* server, you can also access the login page through the **Start** menu by searching for **Self Service Login**.

Hitachi ID Identity and Access Management Suite: Login



2. At the login page, type a profile ID.

If you have not yet set up any additional product administrators, superuser is the only profile ID you can use as an *application administrator*.

3. Click **Continue**.
4. Type your password then click **Verify password**.

Depending on licensing and permissions, product administrators have access to the following main menu options:

Table 1: Administrative options

Option	Description
Manage the system	Configure <i>Bravura Security Fabric</i> objects and environment, administer security, and run reports.
Manage certification process	Create, save, and start access certification campaigns. This feature requires a <i>Bravura Identity</i> or <i>Bravura Privilege</i> license.
Manage the OrgChart	Manually change the OrgChart structure or start Org building rounds.
View dashboards	View graphical summary reports of <i>Bravura Security Fabric</i> operations and usage. This feature requires a <i>Bravura Identity</i> , <i>Bravura Privilege</i> or <i>Access Certifier</i> license.

... continued on next page

Table 1: Administrative options (Continued)

Option	Description
Configure Login Manager	Manage installation licenses, create installation packages, and configure <i>Login Manager</i> options.
Manage reports	enables product administrators to view, run, save, and schedule reports.
Analytics	When configured, enables product administrators to view reports that exist on a Microsoft's SQL Server Reporting Services (SSRS) server.
Manage external data store	enables product administrators to view and update data in the External data store.
Change product administration password	Change your product administrator password. This option is available only if your password is stored in <i>Bravura Security Fabric</i> , and not verified against a target system.
Manage components	Manage <i>Bravura Security Fabric</i> components.

3 Use case: Logging in

In this use case you will log into your *Hitachi ID Bravura Security Fabric* instance and change the default inactivity timeout for a login session.

Requirements

This use case assumes that:

- You have installed *Hitachi ID Bravura Security Fabric*.
- You have installed *Hitachi ID Connector Pack*.
- You are logging in from the product server, to the instance named `default`.

Note: For the use cases within this document we will be using the **Chrome** Internet browser. You may use other Internet browsers, but some security settings and extension installation instructions may differ.

Log in

To log into the Front-end (PSF):

1. On the *Hitachi ID Bravura Security Fabric* server, open the Chrome browser and type:

`localhost/default`

This will automatically redirect you to the login page for *Bravura Security Fabric*.

2. At the Front-end (PSF) login page enter `superuser` as the account.
3. Click **Continue**.
4. Enter the password that you set up for superuser during installation.
5. Click **Log in**.

You are directed to the main menu . Note that as superuser you only have access to administrative options. Product administrators who do not have an account on a target system *cannot* access self-service options.

6. Click **Manage the system** to go to the *Manage the system* (PSA) module.
7. Click **Modules** in the top menu.
The **Modules** menu allows you to configure the behavior of all, or individual modules.
8. Click **Options** at the bottom of the menu.
9. Locate the **DEFAULT EXPIRY SECONDS** field, and change this setting to a timeframe that suits your organization.
By default, *Bravura Security Fabric* logs a user out after 600 seconds of inactivity.
In a test or learning environment it is helpful to extend this time.

WARNING!: In a real-life production environment, the DEFAULT EXPIRY SECONDS value should remain close to the default. A shorter time period prevents users from leaving the browser open for extended periods of time and limits the opportunity for others to gain unauthorized access to the user's accounts.

10. Press **[Enter]** or click **Update** at the bottom of the options table to save the changes.

CAUTION: Changes are not auto saved. You must save your changes before navigating away from the page.

11. Click Home .

This returns you to the front-end menu.

4 Use case: Changing the Administrator Password

There are two ways that you can change a product administrator's password. You can change it using the *Hitachi ID Bravura Security Fabric* web interface or by using the `adm_set` program in the `<instance>\util\` directory.

If you forget the password for your *Bravura Security Fabric* superuser, then using `adm_set` is by default the only way to reset the product administrator's password.

Note: The `adm_set` utility can also be used to unlock the superuser or another product administrator account.

This use case will guide you through changing the product administrator's password using the *Bravura Security Fabric* UI and then changing it back to the original password using the `adm_set` utility.

Requirements

This use case assumes that:

- You have installed *Hitachi ID Bravura Security Fabric*.
- You have installed *Hitachi ID Connector Pack*.

Change the password using the web UI

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Change product administration password**.
3. Enter the following:

Your current password `<password>`

Your new password `Iwantin2`

Confirm your new password `Iwantin2`

4. Click **Change my password**.
The password has now been changed.
5. Log into the Front-end (PSF) using `Iwantin2` as the password to verify the password has been changed successfully.

Change the password using the adm_set utility

1. Open a Windows command prompt (cmd.exe) as administrator.
2. Change directory to the location of the **adm_set** utility using the following command:
3. Change the password of the superuser using the **adm_set** utility using the following command:

```
cd c:\Program Files\Hitachi ID\IDM Suite\default\util
```

```
adm_set.exe -user superuser -pass <password>
```

Note: If you are prompted to make changes to the computer, click **Yes**.

4. Log into the Front-end (PSF) with the updated password and verify that superuser can log in successfully.

5 Finding Things

This explains:

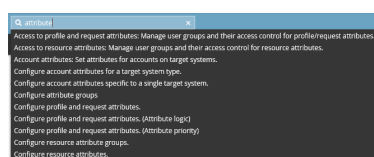
- Searching on actions
- Searching within a page
- Saved searches

5.1 Searching on actions

You can do a quick search on actions that you can perform in *Hitachi ID Bravura Security Fabric*. The action search facility is located at the top left above the navigation bar.



When you start to type a word, suggestions will start appearing matching the current search string. To select a suggestion, either click on it or use the arrow keys to select the suggestion then press **[Enter]**.



5.2 Searching within a page

When you perform a task that requires you to select an object, such as a user, group, or target system, you may need to narrow down the list to find the object you are looking for.

5.3 Saved searches

If you have a lot of records to search through, and you complete the same search regularly, you may find it useful to save your own filters as a saved search and re-use it.

There are many cases where users can do a search, save it, then re-use it either to find stuff again quickly, or in terms of controlling other business logic, such as being able to easily find:

- Target systems of a certain type
- Subordinates of a user
- Users in a certain department
- Users of a certain team

5.3.1 Types of saved search

Saved searches can be:

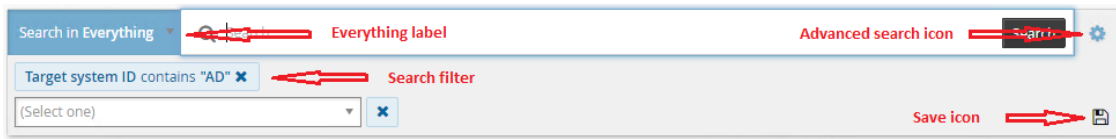
- **My Searches** – Users can create saved searches from the user interface. My saved searches *cannot* be shared across users.
- **Searches** – Product administrators can use plugin to create saved searches. Searches can be shared for all users.

5.3.2 Saved search logic

Saved searches are shared across all engines that derived from the same base engine; for example, saved searches for accounts are shared across all engines that derived from the account base engine class.



Saved search works with advanced search. Any search engine that supports advanced search will support saved searches except for some (older style) advanced search pages in the *Manage reports* (RPT) module. In addition, saved search that are shared across engines will be disabled if the criteria within the saved search is missing in the engine; for example, if one account engine can search on First Name and another cannot, then any saved search containing First Name will be disabled on the second engine. This functionality works the same for criteria that have been removed from the system entirely; for example, profile attributes and resource attributes.

The pre-defined label "Everything" is the default for all search engines that support saved searched. When a user selects another saved search and then switches back to "Everything", all results will be returned in the page.




5.3.3 Creating and deleting My Searches

To save an advanced search query:

1. On the object list page, click the advanced search icon  next to the **Search** button.
2. Enter your search criteria.
See [Advanced searching](#) for details.
3. Click the "Save search"  icon.
4. Enter a name for the new search.
5. Click **Create**.

Once it is saved, you will see it from the saved search drop-down list in the **My Searches** section.

You can delete your saved search at any time by clicking the saved search drop-down list and clicking the "trash can" icon  on the right of the saved search. You will be prompted to confirm the deletion.

5.3.4 Creating and deleting Searches


Product administrators can use a plugin program to add or remove saved searches for users, based on the type of search engine. See [Saved search](#) in the Bravura Security Fabric *Reference Manual* for details on how to write and configure this plugin.

5.3.5 Use Case: General usage of saved search

The following examples demonstrate how users can create a saved search, delete a saved search as well as add more filters to an existing saved search and save as a new saved search.

Create a saved search

To create a saved search:


1. As an end user, from the main menu , click **View and update profile** under **Other users**.
2. On the users page, click the advanced search icon  next to the **Search** button.
3. Create some search filters.
4. Click **Save search** and enter a name for saved search.

5. Click **Create**.

The saved search named `User name contains psadmin` is created.

Delete a saved search


To delete a saved search:

1. As an end user, from the main menu , click **View and update profile** under **Other users**.
2. Select the drop-down list and click the "trash can" icon .
3. Click the **OK** button.


The save search is deleted.

Modify a saved search


To add more filters to an existing saved search and save as a new saved search:

1. As an end user, from the main menu , click **View and update profile** under **Other users**.
2. Select a saved search.
3. Click the advanced search icon .
4. Add more filters to the search.
5. Click **Save search**.
6. Click **Save as** and enter a name for saved search.
7. Click **Create**.

To add more filters to an existing saved search and save as current saved search:

1. As an end user, from the main menu , click **View and update profile** under **Other users**.
2. Select a saved search.
3. Click the advanced search icon .
4. Add more filters to the search.
5. Click **Save search**.
6. Click **Update**.

To create a saved search and override an existing one:

1. As an end user, from the main menu , click **View and update profile** under **Other users**.
2. On the users page, click the advanced search icon  next to the **Search** button.

3. Create some search filters.
4. Click **Save search** and enter the name of a existing saved search which you want to override.
5. Click **Create**.
6. Click **Yes**.

See also:

- For more detail about administration of *Hitachi ID Bravura Security Fabric* see the [Bravura Security Fabric Documentation](#) .