Bravura Security Fabric Implementation: Configuring ACLs

This document includes:

- Requirement
- Solution
- Use case: Creating an individual product administrator
- Use case: Defining a product administrator group
- Use Case: Defining help desk rules

Terminology

The following terms are introduced in this unit:

User groups Define a segment of *Bravura Security Fabric* users whose permissions are determined by an access control list. They do not necessarily refer to target system account groups, although they can be mapped to them via user classes.

Access control Used to allow or deny permission to view or change objects, or to request access changes. They can be applied to all or some user profiles, resources, or policies.

Privileges Actions that individual *Bravura Security Fabric* administrators or groups of administrators can take.

1 Requirement

To prevent unauthorized users from accessing sensitive data, while allowing those same users to access the data they need, organizations have a requirement to create access control lists.

2 Solution

Hitachi ID Bravura Security Fabric controls what a given user ID – whether it belongs to a human being or an automated agent – can see and do using user access rules, or ACLs (access control lists).

Access rules may be explicitly assigned to users or implicitly acquired by users, for example by associating access rules with groups on a system such as LDAP or Active Directory.

3 Use case: Creating an individual product administrator

In this use case you will create a product administrator who has limited access to product features. You will create a profile ID with a password that is verified against the *Hitachi ID Bravura Security Fabric* database only; the user will *not* have an account on a target system.

This use case assumes that:

- *Bravura Security Fabric* is installed.

Create the product administrator

To create a product administrator:

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Security** → **Access to product features** → **Individual administrators**.
3. Click **Add new...**
4. Enter the following values:

   ID `admin1`
   Name `admin1`
   Password / **Confirm password** *<password>*
5. Select the **Password never expires** checkbox.
6. Select "All" **Allowed privileges**.
7. Click **Add** at the bottom of the page to add the user.

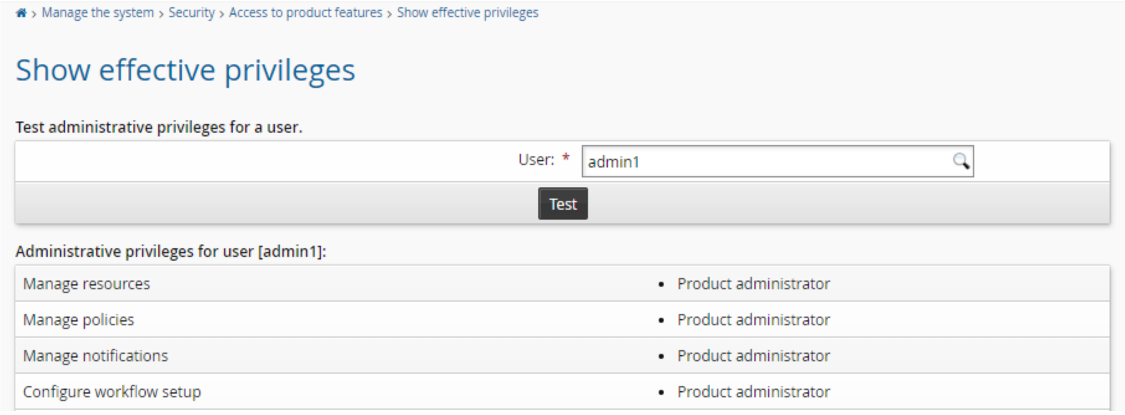
This creates a user who can only perform administrative tasks (console-only access). Because the ID is not mapped to accounts on target systems, the user cannot access the self-service or help desk menus.

Test the administrative privileges

The **Show effective privileges** function allows you to view the product administrator privileges for any user. To do this:

1. Click **Manage the system** → **Security** → **Access to product features** → **Show effective privileges**.
2. Type the ID of the **User** you just created, `admin1`.
3. Click **Test**.

   Hitachi ID Bravura Security Fabric displays the results of the test.



› Manage the system › Security › Access to product features › Show effective privileges

Show effective privileges

Test administrative privileges for a user.

User: * admin1

Administrative privileges for user [admin1]:

Manage resources	• Product administrator
Manage policies	• Product administrator
Manage notifications	• Product administrator
Configure workflow setup	• Product administrator

Login as the product administrator

1. Log in to *Bravura Security Fabric* as `admin1`.
2. Note that the privileges this user has are the same as the superuser account.

4 Use case: Defining a product administrator group

In this use case you will define a product administrator group of auditors who have limited access to product features. You will use the built-in REPORT_READERS administrator group, and include users who also have accounts on target systems.

This use case assumes that:

- *Hitachi ID Bravura Security Fabric* and *Hitachi ID Connector Pack* are installed.
- There is an Active Directory target system set up as a source of profiles.
- An Active Directory group called AUDIT-GENERAL exists and is managed.
- The user JANET exists and is a member of the AUDIT-GENERAL group.

Define the product administrator group

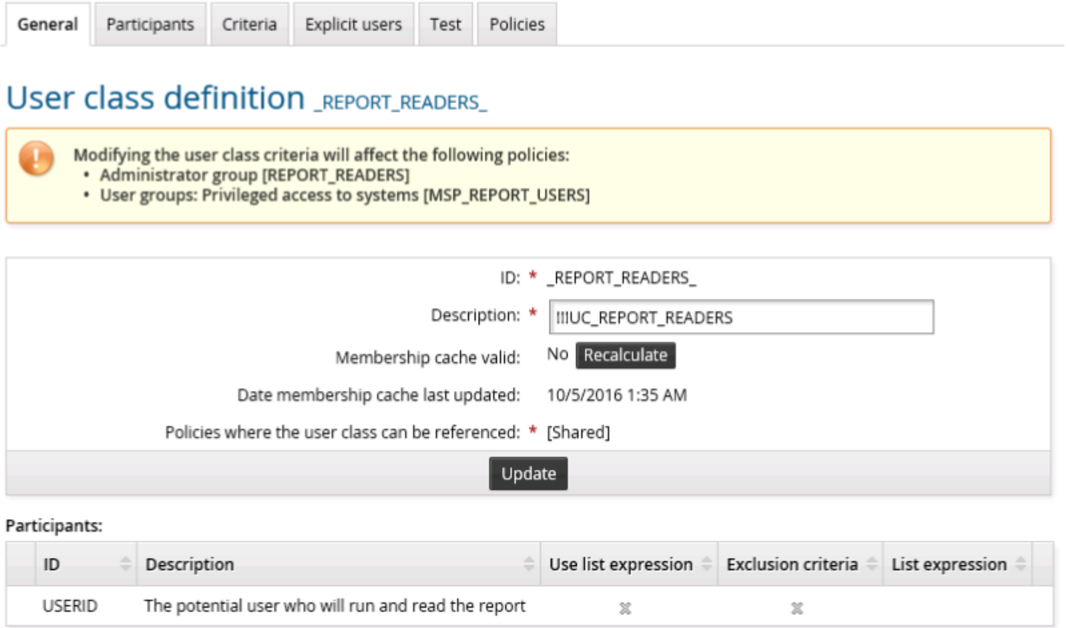
To define a product administrator group:

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Security** → **Access to product features** → **Administrator groups**.
3. Select ▶ REPORT_READERS.

   Leave the default settings. This group has the following allowed privileges:

   - Manage reports
4. Click the **Membership criteria** tab.

   The membership of the REPORT_READERS administrator group is defined by the _REPORT_READERS_ user class.
5. Click the edit icon ✎ next to _REPORT_READERS_.



User class definition _REPORT_READERS_

Modifying the user class criteria will affect the following policies:

- Administrator group [REPORT_READERS]
- User groups: Privileged access to systems [MSP_REPORT_USERS]

ID: * _REPORT_READERS_

Description: * !!!UC_REPORT_READERS

Membership cache valid: No

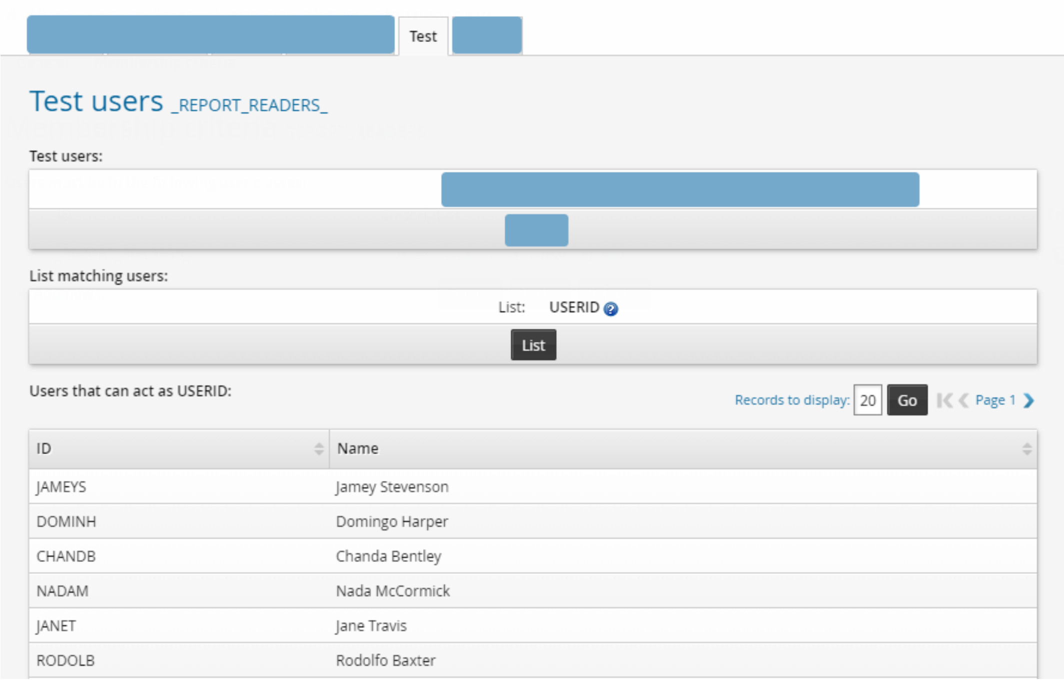
Date membership cache last updated: 10/5/2016 1:35 AM

Policies where the user class can be referenced: * [Shared]

Participants:

ID	Description	Use list expression	Exclusion criteria	List expression
USERID	The potential user who will run and read the report	✗	✗	

6. In the user class configuration pop-up window, click the **Criteria** tab.
7. In the group memberships table, click **Add new…**
8. In the **Target system** field, enter `AD`.
9. Search for and select ▶ the AUDIT-GENERAL group.
10. Click **Add**.
11. Click the **Test** tab and click **List** to see the users that are now members of the _REPORT_READERS_ user class.



Test users _REPORT_READERS_

Test users:

List matching users:

List: USERID

Users that can act as USERID:

Records to display: 20 Go Page 1

ID	Name
JAMEYS	Jamey Stevenson
DOMINH	Domingo Harper
CHANDB	Chanda Bentley
NADAM	Nada McCormick
JANET	Jane Travis
RODOLB	Rodolfo Baxter

12. Return to the **General** tab and next to the option for **Membership cache valid** click **Recalculate**.
13. Close ✖ the user class configuration window.
14. Click the **General** tab of the REPORT_READERS administrator group.
15. If the **Membership cache valid** value is "No", click **Recalculate**.
16. Click **Update**.

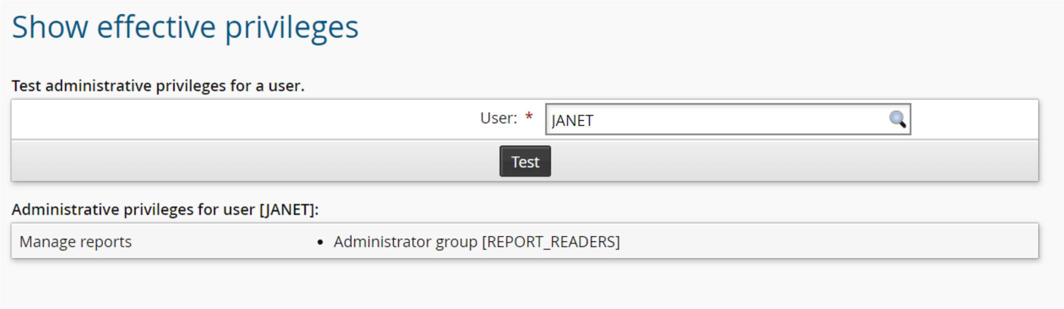
This puts members of the AUDIT-GENERAL group in the REPORT_READERS administrator group. These users can perform some administrative tasks, and can also access the self-service menus.

Test the administrative privileges

To test the administrative privileges:

1. Click **Manage the system** → **Security** → **Access to product features** → **Show effective privileges**.
2. Type `JANET` in the **User** field since we know she is in the AUDIT-GENERAL group that we added to the _REPORT_READERS_ user class.
3. Click **Test**.

   Hitachi ID Bravura Security Fabric should list "Manage reports" as a privilege for this user.



Show effective privileges

Test administrative privileges for a user.

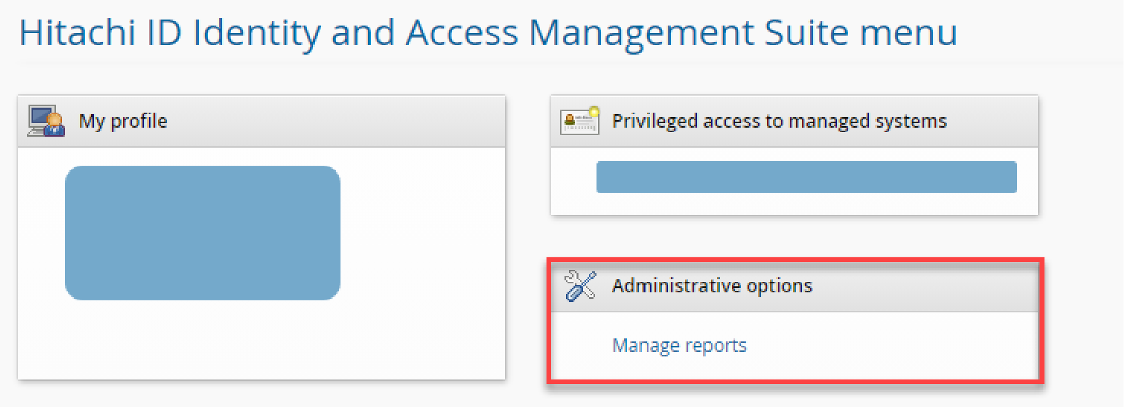
User: * JANET

Administrative privileges for user [JANET]:

Manage reports	• Administrator group [REPORT_READERS]

Login as a REPORT_READERS administrator group member

Log in to *Bravura Security Fabric* as `JANET`. You should see that the user now has access to the **Manage reports** option in the **Administrative options** section.



Hitachi ID Identity and Access Management Suite menu
My profile
Privileged access to managed systems
Administrative options
Manage reports

5 Use Case: Defining help desk rules

In this use case, we will provide a group of users the appropriate access so they can assist users to change their passwords.

This use case assumes that:

- *Hitachi ID Bravura Security Fabric* and *Hitachi ID Connector Pack* are installed.
- The installation includes a *Bravura Pass* license.
- There is an Active Directory target system set up as a source of profiles.
- A user group on Active Directory has been mapped to the `_GLOBAL_HELP_DESK_` user class in *Bravura Security Fabric*.

Use the ***Access to user profiles*** page to define global help desk rules:

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Security** → **Access to user profiles**.
3. Click **Global help desk rules** – these rules control what help desk users can do for all other users.
4. Select ▶ the `GLOBAL_HELP_DESK` user access rule.

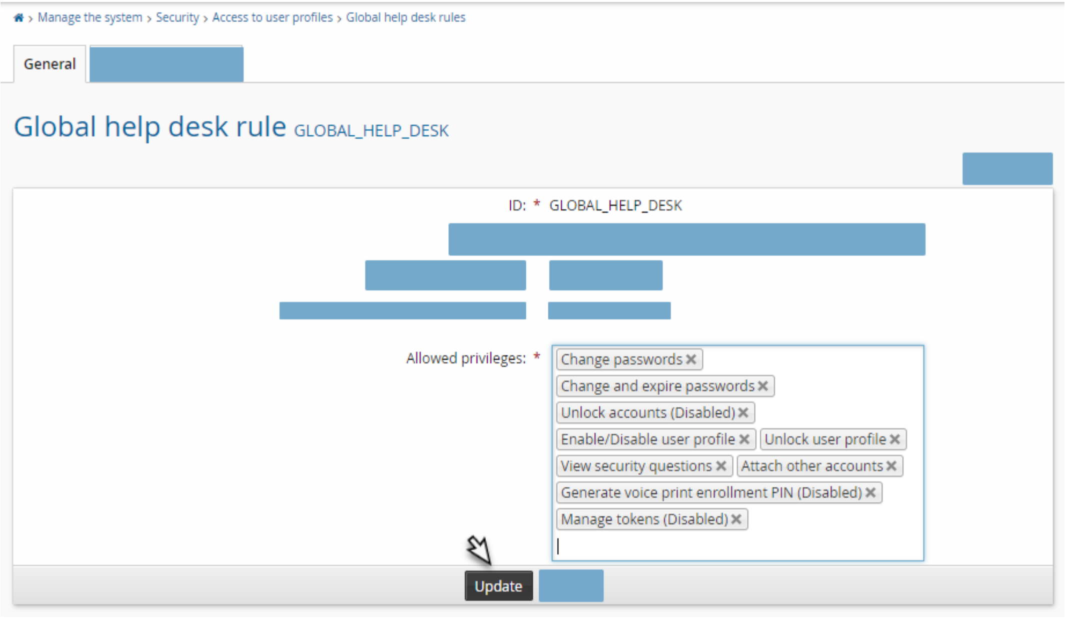
   This rule defines privileges for basic, front-line help desk users. By default, the following privileges are enabled:

   - Change passwords
   - Change and expire passwords
   - Unlock accounts
   - Enable/Disable user profile
   - Unlock user profile
   - Attach other accounts
   - Generate voice print enrollment PIN
   - Manage tokens

   > **Note:** The **Unlock accounts**, **Manage tokens** and **Generate voice print enrollment PIN** privileges all require configuration. If not yet configured, "(Disabled)" is displayed next to their name.
   >
   > The **Update security questions**, **View security questions**, and **Bypass security questions** privileges have "(Disabled)" displayed next to their name, when the *Update security questions* (PSQ) module is disabled.

5. Click in the field next to **Allowed privileges** and select **View security questions**.

   This will allow help desk users to see the user's security questions.


Manage the system › Security › Access to user profiles › Global help desk rules
General
Update

Global help desk rule GLOBAL_HELP_DESK

ID: * GLOBAL_HELP_DESK

Allowed privileges: * Change passwords ✕ | Change and expire passwords ✕ | Unlock accounts (Disabled) ✕ | Enable/Disable user profile ✕ | Unlock user profile ✕ | View security questions ✕ | Attach other accounts ✕ | Generate voice print enrollment PIN (Disabled) ✕ | Manage tokens (Disabled) ✕

6. Click **Update**.
7. Click the **Membership criteria** tab.

   This page allows you to select or create user classes that define the membership rules to have these access rights. By default, the membership criteria for this user access rule is defined by the `_GLOBAL_HELP_DESK_` user class.
8. Click the **General** tab and click **Recalculate** for `Membership cache valid:`.

See also:

- For more detail on setting up security and in particular, access control lists, see the *Bravura Security Fabric* Documentation .