Bravura Security Fabric Implementation: Manage Groups - Admin

This document provides an introduction to the way that *Hitachi ID Bravura Security Fabric* manages groups on target systems.

This document contains:

Terminology

The following terms are used in this document:

Group owner a user that is responsible for the management of a group, and who can directly modify the list of group members and (possibly) group owners.

Group authorizer A user who has the responsibility to decide who should belong to a particular group.

Groups app allows users to request changes to group membership, or to create or update groups if they have assigned privileges.

1 Requirement

Enterprises need automatic and manual management of groups and group memberships from a source of profiles such as an Active Directory domain.

2 Solution

A managed group is a group of accounts defined on a target system, whose membership is monitored and managed in *Hitachi ID Bravura Security Fabric*. On some target systems this can include groups inside groups. An unmanaged group is simply a group whose membership is not monitored and managed in *Bravura Security Fabric*.

During auto discovery, *Bravura Security Fabric* lists all available groups from supported target systems, then loads the group information into its database. By default, *Bravura Security Fabric* only lists group membership for managed groups. This option can be modified on the ***Target system information*** page.

When a group is managed:

- Users can submit requests to join or leave the group.
- The group can be included in roles, so that when a requester selects a role, the request automatically includes group membership.
- Group owners can manage membership and ownership.
- The group can be included in segregation of duties (SoD) rules so that users' membership can be examined when identifying possible access conflicts.
- The group can be included in certification campaigns so that users' memberships can be reviewed.
- The group's membership can be used to segment users into user classes.

2.1 Group membership

Hitachi ID Bravura Security Fabric lists discovered groups for each target system in the **Resources** → **Groups** menu in the *Manage the system* (PSA) module. Group owner information is included if it is available.

Generally, groups managed by *Bravura Security Fabric* can be:

- Open – no approval is required to change their membership
- Moderated – Changes to membership must be approved by an authorizer
- Closed – No membership changes are allowed via *Bravura Security Fabric*

You can configure groups individually, or you can configure *Bravura Security Fabric* so that it automatically manages groups on a target system and assigns the owner as the group authorizer.

To manage groups automatically, configure the option to **Automatically manage groups to be moderated by owners** on the applicable ***Target system information*** page. This option applies to Microsoft Active Directory, Oracle Database, or Domino Server Script target system types. Select one of the following:

- **(Disabled)**: When this value is selected, groups on this target system will *not* be automatically managed. This is the default setting for this option.
- **Only groups with owners, moderated by owners**: Only manage groups that have an owner. Assign the owner as the group authorizer.
- **All groups, approval required**: Manage all groups on the target system. If a group has an owner, then the owner is assigned as the group authorizer. If a group has no owner, then no authorizer is assigned. Groups without authorizers require manual configuration.
- **All groups, no approval required**: Manage all groups on the target system. No authorizers are required by default.

Note: The approval settings only apply when *Bravura Identity*, *Bravura Privilege*, or *Bravura Group* is licensed.

Alternatively, use the **`managegrp`** program to configure managed groups in batches. The program reads entries from a file and configures all the specified groups as moderated managed groups. See managegrp in the Bravura Security Fabric *Reference Manual* to learn how to use this program.

3 Use Case: Manage a group

In this use case you will view listed groups for the Active Directory target, then manage a single group on that target.

This use case assumes that:

- *Hitachi ID Bravura Security Fabric* and *Hitachi ID Connector Pack* are installed.
- An Active Directory target system is added as a source of profiles.

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Resources** → **Groups**.
3. Select ▶ the Active Directory target system to view its listed groups.

   Note that the groups are listed but their membership is not, because the target system is configured to only list membership for managed groups.
4. Select ▶ one of the groups.
5. Click **Manage** at the bottom of the page.
6. If available, click the **Authorization** tab.

Note: This step does not apply when only *Bravura Pass* is licensed.

7. Click **Select...** in the **Authorizers** table.
8. Select the checkbox for the user you want to make authorizer for this group, then click **Select**.

Run auto discovery to calculate membership

You now need to run auto discovery to calculate user membership to newly added group.

1. In the *Manage the system* (PSA) module, navigate to **Maintenance** → **Auto discovery** → **Execute auto discovery**.
2. Click **Continue**.
3. Click the Refresh ↻ until the page states that "Auto discovery is not running".
4. Confirm the auto discovery successfully listed group members by running the groups report:

   (a) Click Home ⌂ → **Manage reports** → **Reports** → **Roles and groups** → **Membership**.

   (b) Click **Run**.

   If auto discovery is successful, this report lists the group you managed and its members.
5. Navigate back to the groups list page for the Active Directory target system.
   You will notice that the account membership is now listed for the managed group.

4 Use Case: Manage groups

In this use case you will manage all groups on the Active Directory target, then view the results.

This use case assumes that:

- *Hitachi ID Bravura Security Fabric* and *Hitachi ID Connector Pack* are installed.
- An Active Directory target system is added as a source of profiles.

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Resources** → **Target systems** → **Manually defined**.
3. Select ▶ the Active Directory target system.
4. Set the **Automatically manage groups** field to "All groups, no approval required".

Note: The request-and-approval workflow engine that supports the "Only Groups with owners, moderated by owners" and "All groups, approval required" options is available in *Bravura Group*, Bravura Identity, or Bravura Privilege.

5. Click **Update**.
6. Click **Run discovery** to automatically manage groups.

   Auto discovery, in this case, will tell the product to manage all of the groups indicated by the Active Directory target address. In order to pull in members of the managed groups auto discovery must be run a second time.

Run auto discovery a second time to calculate membership

You now need to run auto discovery a second time to calculate user membership of the newly managed groups.

1. In the *Manage the system* (`PSA`) module, navigate to **Maintenance** → **Auto discovery** → **Execute auto discovery**.
2. Click **Continue**.
3. Click the Refresh 🔄 until the page states that "Auto discovery is not running".

View managed groups

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Resources** → **Groups**.
3. Select ❯ the Active Directory target system to view its listed groups.
4. Select ❯ one of the groups and take note of its settings.

   You'll see that it is in a managed state.