

# ***Bravura Security Fabric* Implementation:**

## **Configuring Workflow Authorization**

*Hitachi ID Bravura Security Fabric* provides a workflow authorization engine to receive, validate, and route access change requests to the appropriate individuals. This document explains the components of the workflow request and authorization process.

This unit contains:

- Workflow authorization logic and process
- Types of authorization
- Inheriting authorization configuration from the target system
- Configuring phased authorization
- Selecting authorizers using a plugin
- Use case: Configuring static authorization
- Use case: Configuring dynamic authorization
- Use case: Phased authorization

### **Terminology**

Within the workflow authorization process there are a number of actors including:

**Requester** The user submitting a request.

**Recipient** The user who will be affected by a request. This may be the same as the requester.

**Authorizer** The user responsible for reviewing a request. An authorizer may approve, deny, or change a request depending on their privileges.

In many organizations authorizers are typically managers, security staff, or application owners.

**Implementer** A “human agent” that manually fulfills requests. An implementer can accept or decline tasks, and mark them as completed or cannot be completed.

**Workflow manager** An authorizer who can approve, modify, deny, or cancel any authorization request.

**Delegate** (n) The person to whom another person's responsibilities have been delegated or escalated.  
(v) The act of manually transferring workflow responsibilities to someone else.

**Escalate** The automated process that causes your responsibilities on a specific request to be transferred to someone else. This is caused through inaction on a given request.

## 1 Workflow authorization logic and process

The Workflow Manager Service (*idwfm*) is responsible for implementing authorization logic and orchestrating workflow processes. In general, the workflow process operates as follows:

1. A user logs into the *Hitachi ID Bravura Security Fabric* web application and submits a change request. Alternatively, an automated process may submit the change request.
2. *Bravura Security Fabric* validates the input and forwards the request to the Workflow Manager Service (*idwfm*).
3. The *idwfm* service determines authorizers for the request using *static authorization* or *dynamic authorization* rules, and notifies them of their assignments by email.

**CAUTION:** Assigning too many authorizers could affect performance. When the number of authorizers assigned to a resource exceeds the value of MAX AUTH ALLOWED (default 20), the request is put on hold. If you increase this value, ensure that you test the configuration for performance issues.

4. Authorizers log into the *Bravura Security Fabric* web application, usually after following a URL embedded in the email, where they log in and either approve or deny the request.
5. If authorizers do not respond in a timely manner, *idwfm* can send reminder emails or take other actions like denying or escalating the request.
6. The *idwfm* service determines if input received from authorizers is sufficient to approve or deny the request. If the request is:
  - Denied, *idwfm* closes the request.
  - Approved, *idwfm* forwards the request to the Transaction Monitor Service (*idtm*) to carry out changes on target systems.The fulfillment engine can be configured to run connectors directly or to use human implementers.

The *idwfm* service also updates the *Bravura Security Fabric* database and informs the appropriate users.

## 2 Types of authorization

Two types of authorization are available within *Hitachi ID Bravura Security Fabric's* workflow engine:

**Static authorization** Requests involving resources (target systems, templates, roles, or groups) are routed to pre-defined authorizers mapped directly to the objects.

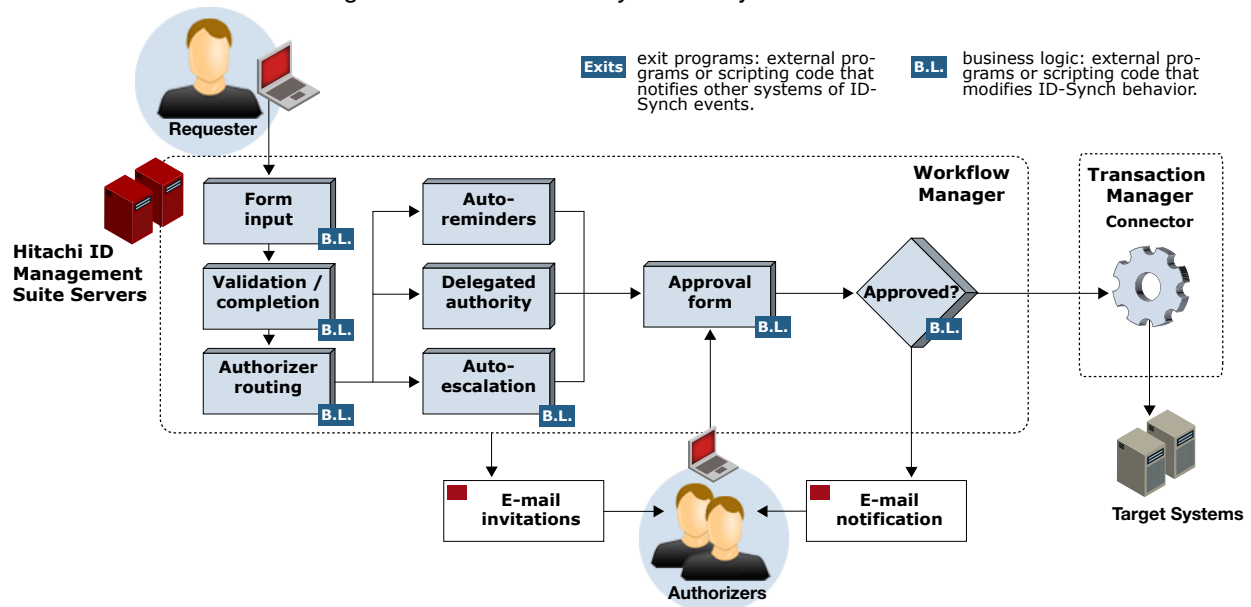
This type of authorization is static because the list of authorizers is configured in advance. It is generally not used in *Hitachi ID Bravura Privilege* implementations.

**Dynamic authorization** Authorizers are determined and assigned at the time the request is submitted, using criteria based on properties of the request (relationship to the recipient, value of a particular request attribute, access requested, and so on).

This type of authorization is dynamic because the list of authorizers changes depending on details of the request. Authorization for managed resources is generally determined by configuration at the resource object level.

Static authorization is simple to configure, but requires manual maintenance. In *Hitachi ID Bravura Identity* implementations, it is usually sufficient for small to medium-size organizations where a small number of employees are responsible for reviewing and authorizing requests to a resource. In *Bravura Privilege* implementations, *Hitachi ID Bravura Pattern: Privileged Access Edition* makes it easier to use team management (which uses dynamic workflow).

Figure 1: *Bravura Security Fabric* Dynamic Workflow



**BEST  
PRACTICE**

In *Bravura Identity* deployments where there are consistent change requests of the same type, there is a risk that authorizers develop "approval fatigue" and rubber-stamp all requests that reach them, without paying close attention to what is being asked.

Setting up appropriate workflow is important so that only requests that require human approval are sent to authorizers; for example an unusual number of terminations, or requests for resources that are outside a user's usual role. Other requests can be auto-approved based on pre-determined conditions.

### 3 Inheriting authorization configuration from the target system



You can configure target systems so that child resources, including templates and groups, inherit the authorization configuration of the target system.

To configure inheritance, enable **Default authorization for child resources, including templates and managed groups, will be inherited from the target system** on the *Target system information* page.


You can override the configuration at the group or template account level. To do this:

1. Navigate to the resources information page:

(a) For managed groups:

- i. Click **Manage the system** → **Resources** → **Groups**.
- ii. Select  the target system that the group belongs to.
- iii. and select  the managed group you want to configure authorization for.  
*Hitachi ID Bravura Security Fabric* displays the **Managed group information** page.

(b) For template accounts:

- i. Click **Manage the system** → **Resources** → **Template accounts**.
- ii. Select  the template account you want to configure authorization for.  
*Bravura Security Fabric* displays the **Template information** page.

2. Set **Override authorization configuration** to:

- Use only inherited configuration
- Do not inherit configuration
- Add to inherited configuration (default)

3. Click the **Authorization** tab:

- If you chose to use only inherited authorization, the target system's authorization is displayed.
- If you chose to not inherit authorization, then the page shows authorization explicitly setup; no authorization from the target system should display.

**Note:** If you chose "Do not inherit any configuration" you cannot statically assign the authorizer assigned at the target level.

- If you chose to add to inherited authorization, then it should display authorization from both.

**Note:** When you choose to add to inherited authorization, the minimum number of required authorizers will pick up the bigger minimum number of authorizers configured.

## 4 Configuring phased authorization

You can configure *Hitachi ID Bravura Security Fabric* at the resource level to send authorization requests in multiple separate phases. These phases allow authorization from distinct groups independent of each other and can be configured either sequentially or in parallel. The required number of approvals must be met before the request is processed.

### 4.1 Initial considerations

Answer the following questions to determine the best solution:

- Are there more than one stakeholder required to approve resources?  
For example; does someone in Human Resources need to approve a resource as well as someone in the Finance department?
- Is there a time requirement for the authorizations to be completed?  
Phased authorization can be sequential or parallel. In phased authorization the next phase cannot be started until the previous phase has been completed. With parallel authorization all authorizations start at the same time thus shortening the authorization process.

See [Use case: Phased authorization](#) for a demonstration of this use case.

## 5 Selecting authorizers using a plugin

When a user submits a request, *Hitachi ID Bravura Security Fabric* can use a plugin to dynamically assign authorizers in addition to, or instead of, those assigned to a workflow object or resource.

*Bravura Security Fabric* allows for flexibility as the authorization process progresses. You can implement a sequential approval process that allows authorizers or other criteria to be added or removed at each step, or for responses to be overruled.

For example, an organization may have "weighted authorizers" where a request could move to the next stage if enough high-ranked authorizers approved it, overriding the minimum required authorizers.

Higher-ranked authorizers could also overrule the response of lower-ranked authorizers. The weighting would be determined by business logic, such as organization chart data, and built into the plugin.

The plugin is run after each authorization step, accepting all information about the:

- Current authorizers
- Requester/Recipient
- Requested resources and attributes

The plugin can override and update:

- Request approval criteria (minimum authorizers)
- Authorizers assigned to the request
- Authorization response (approved, denied) for each authorizer
- The number of authorization phases (add, remove)
- The authorizers within each phase (add, remove)

## 6 Use case: Configuring static authorization

Any regular user with a valid profile can be assigned as a static authorizer. Static authorizers can be mapped directly to resources or policies.

The types of requests that static authorizers can review, and the actions they can take, depend on the privileges granted to them by user access rules.

### Requirements



This use case assumes that:

- There is an Active Directory target system set up as a source of profiles.
- The Active Directory target system is configured so that groups with owners are automatically managed by *Hitachi ID Bravura Security Fabric*, to be moderated by owners. This means that *Bravura Security Fabric* assigns the owners of those groups as the authorizers.

### Configure static authorizers for groups

You can assign static authorizers to a resource in the configuration settings for the resource.

In this use case you will add an extra static authorizers for a group:

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Resources** → **Groups**.
3. Select  the AD target system to view its listed groups.
4. Select  any group and take note of its settings.
5. Ensure the entries for the following settings are selected:

**Authorization for joining group** `Approval required`

**Authorization for leaving group** `Approval required`

6. Click the **Authorization** tab.
7. Set the **Minimum number of authorizers** to 1 if it is not set to 1 already.  
This means that any one of the authorizers you map to this target may approve the request.

8. Set the **Number of denials before a change request is terminated** to 1 if it is not set to 1 already.  
This means that a change to an existing account is canceled if one of the authorizers deny the request.
9. In the **Authorizers** table, click **Select...**

**Note:** You will notice that the group manager has already been added as an authorizer because he is the owner of the selected group.

10. for and select HARRYJ.
11. Click **Select**.

The group now has two authorizers listed, either one of which could approve or deny a request to join the group.

## 7 Use case: Configuring dynamic authorization

In this use case, you will set up authorizers for the target systems, so that when a user requests a change to an existing account, the recipient's direct or indirect manager can authorize the request. An indirect manager could be the manager's manager, and so on up the chain of command.


### Requirements

This use case assumes:

- *Hitachi ID Bravura Pattern: Workforce Edition* is installed.
- There is an Active Directory target system set up as a source of profiles.
- User E000000001 manages user E000000002, who manages E000000001.

### Assign dynamic authorizers to resources

To set up authorizers for existing accounts:

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Resources** → **Target systems** → **Manually defined**.
3. Select  the AD target.
4. Click the **Authorization** tab.
5. Change the **Minimum number of authorizers** to 1.
6. Change the **Number of denials before a change request is terminated** to 1.
7. Click **Update** for the updated section.
8. In the user classes table at the bottom of the form, click **Select...**



9. Select the checkbox for `_MANAGER_INDIRECT_`, and click **Select**.

*Hitachi ID Bravura Security Fabric* displays an error because you have not mapped the participants in the user class yet.

10. Under **Participant mapping** for MANAGER, select AUTHORIZER.
11. Under **Participant mapping** for SUBORDINATE, select REQUESTER.

General
Credentials
Authorization
Resource operations
Role enforcement
Discovery options
Test connection
Logs

### Authorization AD

Users who will be invited to approve changes to existing accounts on this target system.

Minimum number of authorizers: \* 1
Number of denials before a request is terminated.: \* 1  
(0=ignore denials, only count approvals)

Update

Authorizers:

| ID                | Name |
|-------------------|------|
| No data available |      |

Select...

Users must be in the following user classes:

| <input type="checkbox"/> | ID                              | Description   | Participant mapping   | Edit |
|--------------------------|---------------------------------|---|---|------|
| <input type="checkbox"/> | <code>_MANAGER_INDIRECT_</code> | One user is a direct or indirect manager (manager's manager etc.) of the other user | MANAGER <small>?</small> AUTHORIZER <small>?</small><br>SUBORDINATE <small>?</small> REQUESTER <small>?</small> |      |

+ Add new...
Delete
Update
Test...
Select...

12. Click **Update**.

### Test the user class participant mapping

To test if a change request will have enough authorizers:

1. Click **Test...** in the user class table.
2. In the table **List matching users**, select AUTHORIZER in the drop down.
3. In the **REQUESTER** field, type `E000000003`.
4. Click **List**.

Test users: AD

Test users:

RECIPIENT:

REQUESTER:

AUTHORIZER:

Test

List matching users:

List: AUTHORIZER

where the following participants are

RECIPIENT:

REQUESTER:

List

Users that can act as AUTHORIZER for REQUESTER [E000000003]: Records to display: 20 Page 1 / 1

| ID         | Name            |
|------------|-----------------|
| E000000002 | Nicholas Little |
| E000000001 | Dustin Townsend |

Hitachi ID Bravura Security Fabric should list E000000002 and E000000001 as managers in the chain of command above E000000003.

**Note:** On the *Target system information* page, you can enable the setting to **Default authorization for child resources, including templates and managed groups, will be inherited from the target system**. This would mean the authorizers you mapped above, to review requests to change existing accounts, would be mapped to all groups on the target system.

You have now set up dynamic authorization for change requests related to existing accounts.

### Submit a request to change attributes

1. Log into the Front-end (PSF) as E000000003.
2. Click **View and update profile** in the **My profile** section.
3. Select **Update attributes** near the bottom of the page.  
The request wizard opens.
4. Fill in the following information:
 

**First name** Kathy

**Last name** Robinson
5. Click **Submit**.
6. Review the request details and you should see that the request is pending approval from E000000002 and E000000001.

### Approve the attribute request

1. Log into Front-end (PSF) as E0000000002.
2. Click **There are 1 request(s) awaiting your approval**.  
The *Requests* app opens.
3. Select the request from the Results panel.  
The details of the request will appear in the Actions panel.
4. Click **Approve**.
5. Click the **Approve** button to confirm the request.
6. Navigate back to E0000000003's home page.
7. Click **View and update profile** in the **My profile** section.  
The **First name** and **Last name** will now be populated with our changes.

## 8 Use case: Phased authorization

This use case shows you how to configure *Hitachi ID Bravura Security Fabric* to use phased authorization on specific resources.

**Note:** Phased authorization can only be configured on resources on a per resource basis.

### Requirements

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.

### Configure phased authorization


To enable parallel authorization:

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Workflow** → **Options** → **General**
3. Set the **WF PHASED AUTH** setting to Enabled.

## Enable phased authorization on a resource

Configure a resource to use phased authorization in *Hitachi ID Bravura Security Fabric*.

To configure parallel authorization:

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Resources** → **Target systems** → **Manually defined**.
3. Select  a target system to configure or create a new target system.
4. Click on the **Authorization** tab.
5. Add a new authorization phase or modify an existing phase.  
You can also set the authorization type for the entire resource. Selecting **Phased** will cause each phase to be sequential and **Parallel** will cause the phases to be processed in parallel.
6. Select a phase.
7. Select authorizers.
  - Under **Authorizers** you can select several static authorizers for this resource.
  - Under **Users must be in the following user classes** you can select a user class to dynamically assign authorizers.

**Note:** All users in the user class will be assigned to request for authorization.

## See also:

- The [Bravura Security Fabric Documentation](#) for more information about authorization workflow.
- The *Bravura Security Fabric Reference Manual* for more information about Workflow Manager Service (idwfm) and Transaction Monitor Service (idtm).