

***Bravura Identity* Implementation:**

Detect rehire and reactivate or block

Hitachi ID Bravura Identity has components that set default rules and thresholds for comparing identity attributes in requests to onboard new users with attributes of existing users, in order to compute a likelihood that the proposed new hire is, in fact, a returning user with an existing profile. Threshold values set by this component determine whether a given score merits a warning to the requester or should block an onboarding request, due to the high certainty that it is a returnee.

Terminology

The following terms are introduced in this unit:

External data store enables product administrators to view and update data in the External data store.

Component a collection of scripts and data which provide extra functionality to *Hitachi ID Bravura Identity*.

pre-defined request (PDR)s allow users to request changes that involve operations on technical resources.

This unit contains:

- Requirement
- Solution
- Use case: User flagged as a rehire
- Use case: User flagged as a rehire on a SoR

1 Requirement

Organizations need to differentiate between new employees and employees that are being rehired. Employees that are being rehired should go through a different process that could enable their previous resources or, in certain circumstances some employees maybe flagged to not rehire.

2 Solution

Hitachi ID Bravura Identity is configured to retain identity information for all users, even after deactivation. This means that user profiles are not deleted, but instead, deactivated. Identity attributes normally include name, date of birth and identifiers such as a driver's license number or social security number. Moreover, when a user is deactivated, three termination-related attributes are populated: termination date, reason for deactivation and whether rehiring this user is allowed.

When processing onboarding requests, regardless of whether they originate in a system of record (such as HR) or a request form, *Bravura Identity* applies rules to score how closely the new identity matches any identities already known to the system. These rules work by matching different sets of attributes – for example, first name plus last name plus date of birth. How closely the new user matches an existing profile is used to compute a confidence score. If the confidence score is above one threshold, a warning is generated that the new hire may not actually be new. If the confidence score is above another, higher threshold, then the request is blocked, because there is sufficient certainty that the new user is, in fact, a returning old user.

When an onboarding request using a request form, closely matches an existing profile, the following actions can occur:

- Users of *Bravura Identity* are either instructed to terminate the process, as the old user was flagged as do-not-rehire
- Users are instructed to reactivate the old user profile.

When an onboarding request closely matches an existing profile from a Source of Records, the following actions can occur:

- The request is blocked with rehire not permitted.
- The request is permitted and a subsequent request is submitted for someone to review the potential conflict.

In no case should a new user profile be created for a returning old user.

3 Use case: User flagged as a rehire

This use case uses the `Scenario.im_corp_detect_rehire` scenario component that utilizes request forms in the way of pre-defined request (PDR)s. In this case, a user will be terminated urgently, setting the REHIRE-ALLOWED flag to false. The attempt to rehire will be prevented.

Requirements

This use case assumes that:

- Hitachi ID Bravura Identity and Hitachi ID Connector Pack are installed.
- An Active Directory target is configured and is a source of profiles.
- A HR target is configured as a Source of Records.

Configure the scenario

1. Log in to *Bravura Identity* as `superuser`.
2. Install the `scenario.im_corp_detect_rehire` scenario.


This scenario component sets default rules and thresholds for comparing identity attributes in requests to onboard new users with attributes of existing users, in order to compute a likelihood that the proposed new hire is, in fact, a returning user with an existing profile.
3. Navigate to the **Manage external data store** to verify the following tables are available. The tables are pre-configured, however, may require some customization for your environment:
 - `HID_GLOBAL_CONFIGURATION` to configure rehire parameters.
 - `IM_POLICY_DETECT_REHIRE` to set rehire detection criteria.
4. Click **Manage the system** → **Workflow** → **Pre-defined requests**.
5. The following PDRs have been pre-configured for the termination scenario. You may want customize to your needs; for example, edit the access control or change the operations.

REHIRE Used to enable user accounts after they have been terminated. This pre-defined request is valid if the user is allowed to be rehired.

RESTORE-TERMINATED-USER Used to restore a user that was terminated.
6. Complete an urgent termination of a user using the URGENT-TERM PDR. The REHIRE-ALLOWED flag is automatically set to false.

See `user-termination.pdf` for information on how to complete this task.

Attempt a rehire

1. Log in to *Bravura Identity* as a user.
2. Click **Create a new user profile**.
3. Select  the **Hire a contractor** PDR.

4. Fill out the new user's information with duplicate information that matches the terminated user.
5. Attempt to submit the request.
An error should appear stating that a rehire of an existing user is attempted and will be prevented.

4 Use case: User flagged as a rehire on a SoR

This use case uses the `Scenario.im_corp_detect_automated_rehire` scenario. In this use case a user is flagged as a rehire from a Source of Records.

Requirements

This use case assumes that:

- *Hitachi ID Bravura Identity* and *Hitachi ID Connector Pack* are installed.
- An Active Directory target is configured and is a source of profiles.
- A HR target is configured as a Source of Records.

Configure the scenario

1. Log in to *Bravura Identity* as `superuser`.
2. Install the `Scenario.im_corp_detect_automated_rehire` scenario.
This scenario component will detect rehires being submitted from the source of records and submit follow up requests for an implementer to review the new user being onboarded.
3. Click **Manage external data store** to verify the following tables are available. The tables are pre-configured, however, may require some customization for your environment:
 - `HID_GLOBAL_CONFIGURATION` to configure rehire parameters.
 - `HID_POLICY_REQUEST_CHAIN` to submit a request to review new the hire.
 - `IM_POLICY_AUTHORIZATION` to set authorization on the require detection request.
 - `IM_POLICY_DETECT_REHIRE` to set rehire detection criteria.
 - `IM_POLICY_IMPLEMENTERS` to set implementers to review the potential rehire.
4. The following pre-defined request (PDR)s have been pre-configured for the termination scenario. You may want customize to your needs; for example, edit the access control or change the operations.
REHIRE Used to enable user accounts after they have been terminated. This pre-defined request is valid if the user is allowed to be rehired.
NEW-EMPLOYEE
5. Complete a scheduled termination of a user.
See `user-termination.pdf` for how to complete these steps.

Attempt a rehire

1. Add an account in Source of Records (SoR) target.
2. Execute auto discovery.
A request is submitted and a child request is submitted for review.
3. Log in to *Bravura Identity* as a request implementer.

Note: HR systems are usually set as read only targets and require an implementer to complete tasks as opposed to a connector automatically completing the task.

4. Verify that there are pending requests open to implement.

See also:

- The **components.pdf** document for more information about components.
- The **terminate-user.pdf** document for more information about the termination components.
- The [Bravura Security Fabric Documentation](#) for more information about attributes and PDRs.