

# ***Bravura Identity* Implementation:**

## **User termination**

### **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: Scheduled termination of a contractor or employee
- Use case: Urgent termination (not not rehire)

## **1 Requirement**

Organizations need a way to manage the offboarding of users from *Hitachi ID Bravura Identity*. This can include scheduled or urgent termination.

## 2 Solution

An urgent termination request disables an account and profile immediately. In addition, any attributes indicating the cause for termination and that the user should never be rehired are set.

Subsequent archive and cleanup processes are handled the same way as with scheduled termination.

User access deactivation can be scheduled in *Hitachi ID Bravura Identity*. In practice, scheduled access deactivation is a multi-step process that begins a number of days before the scheduled termination date and continues long after access is disabled.

Scheduled termination is completed in four phases:

1. Before and on the day of scheduled termination, notify the appropriate managers and/or HR that a user is set to be terminated.
2. Deactivate access on the scheduled date. This means disabling all login accounts and the user's IAM profile. The user's description is also updated to indicate the disabled status.
3. Some time later (X days):
  - (a) Remove entitlements associated with each user account.
  - (b) Possibly move the user to a different directory container (for example, disabled users OU).
  - (c) Possibly attach additional group memberships (for example, disabled users group).
  - (d) Reassign the user's subordinates to the user's manager.
  - (e) Detach the user from his old manager.
  - (f) Call a batch file (specific to the *Bravura Identity* system implementation) to archive the user's home directory and mail folders.
4. Some time later still (Y days), delete the user's accounts, but retain the IAM profile, to support future rehire detection.

### 3 Use case: Scheduled termination of a contractor or employee

This use case uses the **Scenario.im\_corp\_automated\_termination** scenario which automates the termination process based on data retrieved from a Source of Records (SoR). In this case, a user's termination date is scheduled using the organizations HR system. *Hitachi ID Bravura Identity* will email the user's manager advising of the upcoming termination 30, 15 and 10 days beforehand. On the scheduled day the user's accounts will be disabled. 90 days after termination the user's accounts will be archived.

#### Requirements

This use case assumes that:

- *Hitachi ID Bravura Identity* and *Hitachi ID Connector Pack* are installed.
- Email notifications have been configured.
- 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\_automated\_termination** scenario. This scenario component provides termination logic for automated scheduled terminations.
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 settings for automated terminations. For example; The SoR target ID, the attribute used to determine which users should be terminated and the pre-defined request (PDR)s used for the termination process.
  - `HID_POLICY_ATTRVAL_CALCULATION` to set the computed attribute values.
  - `HID_POLICY_ATTRVAL_DEFAULT` to set relative default attribute values for the PDRs.
  - `IM_POLICY_AUTHORIZATION` to set authorizations for each PDR.
  - `IM_TERMINATION` to set the termination behavior. For example; time periods for warnings, the subject line of the warnings and who the email is sent to.
4. The following PDRs have been pre-configured for the termination scenario. However, you may want customize to your needs. For example; edit the access control or change the operations.
  - `SCHEDULE-NOTIFY`
  - `SCHEDULE-TERM`
  - `ARCHIVE-USER`
  - `CLEANUP-DELETE-USER`

### Schedule a termination

1. Set the scheduled termination date for a user on the Source of Records.  
This process will be different for each organization based on the HR target you use.
2. Execute auto discovery.
3. Depending on the termination date specified one of the following will occur:
  - A termination warning will be submitted the recipient's manager 10,15,30 days prior to termination.
  - The user will be disabled and when the terminated user attempts to login it will fail with a notice that the account is disabled.
4. Execute auto discovery following the archive days (defaulted to 90).
5. Users in a terminated state for the length of the archive days will have an archive request submitted to perform archive tasks.
6. Execute auto discovery following the clean-up days (defaulted to 180).
7. Users in an archived state for the length of the clean-up days will have a clean-up request submitted to perform clean-up tasks.

## 4 Use case: Urgent termination (not not rehire)

This use case uses the **Scenario.im\_corp\_manual\_termination** scenario which utilizes the URGENT-TERM pre-defined request (PDR) to trigger the termination process as opposed to the termination being triggered from a SoR.

When this PDR is used the attribute **REHIRE-ALLOWED** is automatically set to false to avoid the user being reactivated at a later date.

### Requirements

This use case assumes that:


- Hitachi ID Bravura Identity and Hitachi ID Connector Pack are installed.
- Email notifications have been configured.
- 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\_manual\_termination** scenario. This scenario component provides termination logic for both scheduled and urgent terminations.

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_POLICY_ATTRVAL_CALCULATION` to set the computed attribute values.
  - `HID_POLICY_ATTRVAL_DEFAULT` to set relative default attribute values.
  - `HID_POLICY_ATTRVAL_VALIDATION` to set input validations.
  - `IM_POLICY_AUTHORIZATION` to set authorizations for the URGENT-TERM PDR.
4. If required, update the operations to be performed on each target as part of the URGENT-TERM PDR. The PDR has been pre-configured for the urgent termination scenario. You may want customize to your needs; for example, edit the access control or change the operations.

### Complete an urgent termination request

1. Log in to *Bravura Identity* as a manager of the user to be terminated.
2. Click **View and update profile**.
3. Search for and select the user to terminate.
4. Select  the **Urgent termination (do not rehire)** PDR.
5. Submit the request.
6. Log in to *Bravura Identity* as an authorizer assigned to the request.
7. Click the **You have <N> access change requests to review** notification.
8. Select the request to approve.
9. Click **Approve**.
10. If the HR system is set to read only, a request will be sent to an implementer to disable the user's account on the HR system.

The majority of targets will use the connector to perform the disable function, not requiring human intervention.
11. Attempt to log into *Hitachi ID Bravura Identity* as the terminated user. The login attempt should fail and indicate that the user has been disabled.
12. Attempt to log in using an account belonging to the terminated user on a target system.

The user should not be able to log into the target.

### See also:

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