Bravura Identity Implementation: Deactivate users - Admin

Hitachi ID Bravura Identity can deactivate and clean a user's access when they leave an organization.

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 allows users to request changes that involve operations on technical resources.

This unit contains:

1 Requirement

Over a life cycle of a user they will need to be removed from the system. A user may be required to be deactivated because their contract has concluded or there is a need to urgently deactivate them. Depending on the need, the users will go through a termination process that will progress over several stages including, warning their manager, disabling and archiving their accounts and finally deleting and cleaning their access and information.

2 Solution

Hitachi ID Bravura Identity includes scenario components to manage the offboarding of users from the system. This can include scheduled termination or urgent termination.

Bravura Identity can detect when a user's scheduled termination date is approaching. The termination date will either be set by the manager or via a human resources system. *Bravura Identity* will inform the user's manager via email that they have a subordinate that will be terminated soon. This will give the manager an opportunity to review and potentially extend their access.

When the user's termination date has been reached *Bravura Identity* will disable the user's access. The manager has the option to restore the user at this point if they so desire. After a period of time the user's access will be archived. This process can include moving accounts into a different organizational unit or group and moving home directories.

After another period of time the user's access will be cleaned up by deleting accounts and the user's personal information may be deleted from Bravura Identity. Some information will remain in *Bravura Identity* Identity to detect whether or not the user can be rehired.

BEST PRACTICE	Configure *Bravura Identity* to monitor upcoming terminations. At a minimum, send email reminders to managers telling them their soon to be terminated subordinates and a url link to extend the user's access period. Warning emails should be sent to managers 30, 15 and 10 days before the access is terminated. The archive and cleaning phases should be set to a minimum of 90 and 180 days respectively.

2.1 Initial considerations

Answer the following questions to determine the best solution:

- Are there employees that have a set termination date like contractors? Setting a user's termination date may allow greater flexibility for contractor termination or renewal processes.
- Is there a need to urgently terminate a user and remove their access? A situation may arise where a user's access needs to be removed immediately.
- Where is the scheduled termination information coming from? The user's manager or a human resources system may have this information which is propagated into *Hitachi ID Bravura Identity*.
- What process or periods of time for each stage do you want users' access to go through? The periods of time between notifications of termination and final clean up can be configured.
- Does the user's personal information need to be deleted during the final stage? Depending on your locale this may be required to be compliant with legislation.

3 Use Case: Deactivating users manually

This use case shows you how to install the scenario component that implements use cases for both scheduled and urgent termination of users. When installed, this component configures a number of pre-defined request (PDR)s as well as a dedicated policy table for granular control over each step of a scheduled termination request via the UI using a PDR.

Use this component when:

- You have contractors who should be terminated at a scheduled termination date.
- You may have a business need to defer these termination dates, so you need advance warning of upcoming terminations.
- You have to trigger an urgent termination of a user.
- You may have a business need to restore a terminated user whose accounts are in disabled status, so you need to configure archive and cleanup policy as part of termination.

Requirements

This use case assumes that:

- You have installed *Hitachi ID Bravura Pattern: Workforce Edition*.
- You have configured the AD target system.
- You have configured the HRAPP target system.

3.1 Install termination components

1. Log in to *Bravura Identity* as `superuser`..
2. Install Scenario.im_corp_manual_termination.
3. Navigate to the **Manage external data store** to verify the following tables are available and configured for the environment:
   - im_policy_authorization sets the authorization policies for termination pre-defined requests for both scheduled and urgent termination requests.
   - im_termination contains configuration details for each step of a scheduled termination process.
   - hid_policy_attrval_default sets the rules involving profile and request attributes calculation and validation, required for the workflow engine and scheduled tasks to successfully process termination requests.
4. Click **Manage the system** → **Workflow** → **Pre-defined requests**.
5. Configure the following pre-defined requests as needed:

   SCHEDULE-NOTIFY Used to set notification attributes for scheduled termination during the notification stage of the termination.

   SCHEDULE-TERM Used to disabled user accounts and set termination attributes.

   ARCHIVE-USER Used to archive user accounts and home directories.

   CLEANUP-DELETE-USER Used to delete user accounts and personal information.

   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.

   URGENT-TERM Used to terminate a user immediately. The user will not be allowed to be rehired after this request is issued.

   RESTORE-TERMINATED-USER Used to restore a user that was terminated.

3.2 Set Bravura Identity termination policy

Configure termination policy based on the business logic required using *Hitachi ID Bravura Identity*..

1. Log in to *Bravura Identity* as `superuser`..
2. Click **Manage external data store** → **im_termination table**.
3. Modify settiings to suit your needs. While the default settings are sufficient for majority of cases the following can be changed:

   pdrid The pre-defined request id to be submitted.

   reason The reason to be appended to the pre-defined request.

   days Applies to *archive* and *warning*.
   - For *archive* and *clean*, this defines the number of days after termination to archive or delete the user.
   - For *warning*, this defines the number of days before leave of absence to send a notification.

to Applies to *disable* and *warning*. List of email addresses to send notifications to.

to_fallback Applies to *disable* and *warning*. A fallback email address to send notifications to (if the 'to' condition described above yields no valid email addresses). This can be a comma separated list of email addresses.

subject Applies to *disable* and *warning*. Email subject tag.

body Applies to *disable* and *warning*. Email body tag.

manager_propagate Applies to *archive*. If 'true', update the ORGCHART_MANAGER attribute for the archived user's subordinates to the archived user's managers.

detach_grp Applies to *archive*. If set, remove the archived user from the specified groups. Group must be in the form TARGETID:GROUPFQN. Can be set multiple times.

attach_grp Applies to *archive*. If set, add the archived user from the specified groups. Group must be in the form TARGETID:GROUPFQN. Can be set multiple times.

requester The requester userid. If set, will be used instead of the default _API_USER. If specified multiple times, the first valid requester will be used.

delete_data Whether sensitive user data should be deleted as part of user termination.

deletion_attrs A comma separated list of personal user attributes which should be deleted as part of termination.

4. Click **Manage external data store** → **im_policy_authorization table**. The default settings are sufficient for the majority of cases you can change the authorization flow as desired by the business logic.

5. Test your configuration as follows:

   (a) Log into *Bravura Identity* as a manager.

   (b) Navigate to **View and update profile** menu option for the user to be terminated.

   (c) Submit the **Scheduled or deferred termination** PDR with the scheduled termination date far enough in the future.

   (d) Confirm that the user's manager is warned by email about the approaching termination date of user once per warning period as per the policy.

   (e) Confirm that after the termination date elapses, the user is terminated, their profile is disabled and their accounts are disabled, archived and cleaned up according to policy.

4 Use Case: Termination of a user account originating from a System of Record.

This use case shows you how to configure *Hitachi ID Bravura Identity* to deactivate an account using information from a System of Record; for example, a termination date set on the account in Activate Directory.

Use this component when:

- You want one or more source of record targets to be monitored for deleted records and generate a termination request while avoiding duplication.
- You have contractors who should be terminated at a scheduled termination date.
- You may have a business need to defer these termination dates, so you need advance warning of upcoming terminations.
- You may have a business need to restore a terminated user whose accounts are in disabled status, so you need to configure archive and cleanup policy as part of termination.

Requirements

This use case assumes that:

- You have installed *Hitachi ID Bravura Pattern: Workforce Edition*.
- You have configured the AD target system.
- You have configured the HRAPP target system.

4.1 To configure automated termination

1. Log in to *Bravura Identity* as `superuser`..
2. Install Scenario.im_corp_automated_termination if it is not installed already.
3. Click **Manage external data store** to verify the following tables are available and configured for the environment:
   - im_policy_authorization sets the authorization policies for termination pre-defined requests for both scheduled and urgent termination requests.
   - im_termination contains configuration details for each step of a scheduled termination process.
   - hid_policy_attrval_default sets the rules involving profile and request attributes calculation and validation, required for the workflow engine and scheduled tasks to successfully process termination requests.
   - hid_global_configuration adds TERMINATE_* and TERMINATION_* settings under the AUTOMATION namespace, to identify parameters such as the Target ID for the SoR, the pre-defined request to be used for the automated termination requests or the criterion used to trigger the termination process.

4. Click **hid_global_configuration table**.
5. The AUTOMATION settings are:

   TERMINATE_SOR_TARGET Sets the Source of Record for accounts. This will be a target system that contains the scheduled termination date.

   TERMINATE_SOR_ROOT Sets the target root account.

   TERMINATE_REQUEST_REASON Sets the request reason for the automated termination.

   TERMINATE_PDR Sets the pre-defined request that the automated termination will use.

   TERMINATION_TYPE Sets the condition to use to determine if a user is terminated.

   TERMINATION_ATTR Sets the attribute used to determine whether a user should be terminated (only used when TERMINATION_TYPE = attribute).

   TERMINATION_ATTR_VAL Sets the value to be used to determine whether a user should be terminated (only used when TERMINATION_TYPE = attribute).

6. Test your configuration as follows:
   (a) Remove an account on source of records(SoR) target HRAPP.
   (b) Execute auto-discovery.
   (c) Confirm that termination request is created and profile/accounts are disabled from the *Hitachi ID Bravura Identity*.

See also:

- The **`Components.pdf`** for more information about components.