Bravura Identity Implementation: Configure Leave of Absence

The *Hitachi ID Bravura Identity* leave of absence component allows users to request a leave of absence. During the requested period of time the users accounts are temporarily disabled.

This document contains:

1 Requirement

An organization wants to limit or disable employees' access to systems while an employee is on a leave of absence.

2 Solution

An employee will submit a request for a leave of absence and when approved by the appropriate authorizers *Hitachi ID Bravura Identity* will monitor for the start of the leave date. When this date has been reached *Bravura Identity* will submit a workflow request to disable the users accounts. *Bravura Identity* will then monitor the return from leave date. When this date has been reached *Bravura Identity* will enable the user's accounts allowing the user to resume working.

Component

The **`Scenario.im_corp_loa`** component installs policy settings to control corporate leave of absence policies. It does this by implementing a number of pre-defined requests (PDRs) to process leaving and returning users. This includes updating the user's leave of absence status, as well as disabling their accounts when they leave and enabling them when they return.

3 Use case: Leave of Absence - Offboarding and Onboarding

A leave of absence can be applied to staff who will be on extended leave, such as sabbaticals, study, parental, and medical leave. A manager will request a leave of absence on behalf of a user and set start and return dates. A scheduled task will run to trigger the leave of absence and disable the user's accounts.

Since leaves of absence are intended to be reversible, accounts are not deleted and group memberships are not revoked – the only actions are to disable and later re-enable accounts and user profiles.

Requirements

This use case assumes that:

- *Hitachi ID Bravura Identity* and *Hitachi ID Connector Pack* are installed.
- An Active Directory target system has been added as a source of profiles

Deploy Leave of Absence

To deploy the leave-of-absence component.

1. Install `Scenario.im_corp_loa`.
2. Click **Manage external data store** to verify the following tables are available and configured for the environment:
   - HID_GLOBAL_CONFIGURATION to set targets that are a source of profile ID
   - HID_POLICY_ATTRVAL_DEFAULT to set relative default values
   - HID_POLICY_ATTRVAL_VALIDATION to set input validation
   - IM_LEAVE_OF_ABSENCE to set leave of absence configurations
   - IM_POLICY_AUTHORIZATION to set authorizations for the requests
3. Configure the membership of the LOA-AUTHORIZERS user class.
4. Configure the following pre-defined requests:
   - LOA-EFFECTIVE
   - LOA-REQUEST
   - LOA-RETURN
   - LOA-RETURNED

As a manager, request a leave of absence using the pre-defined leave of absence request

To test this feature, request a leave of absence:

1. Log into *Hitachi ID Bravura Identity* as a manager.
2. Click **View and update profile** under **Other users**.

3. Select the user to request a leave of absence for.
4. Click **Leave of absence**.
5. Fill out and submit the request.
6. If required, log into *Bravura Identity* as an authorizer and approve the request.
7. Allow the start date to pass so that LOA-EFFECTIVE can trigger the event.
8. Verify that the user has been modified as follows:
    - The user's status should be set to on leave.
    - The user's profile and account should be disabled.

See also:

- The *Bravura Security Fabric* Documentation for more information about configuring pre-defined requests and user classes.