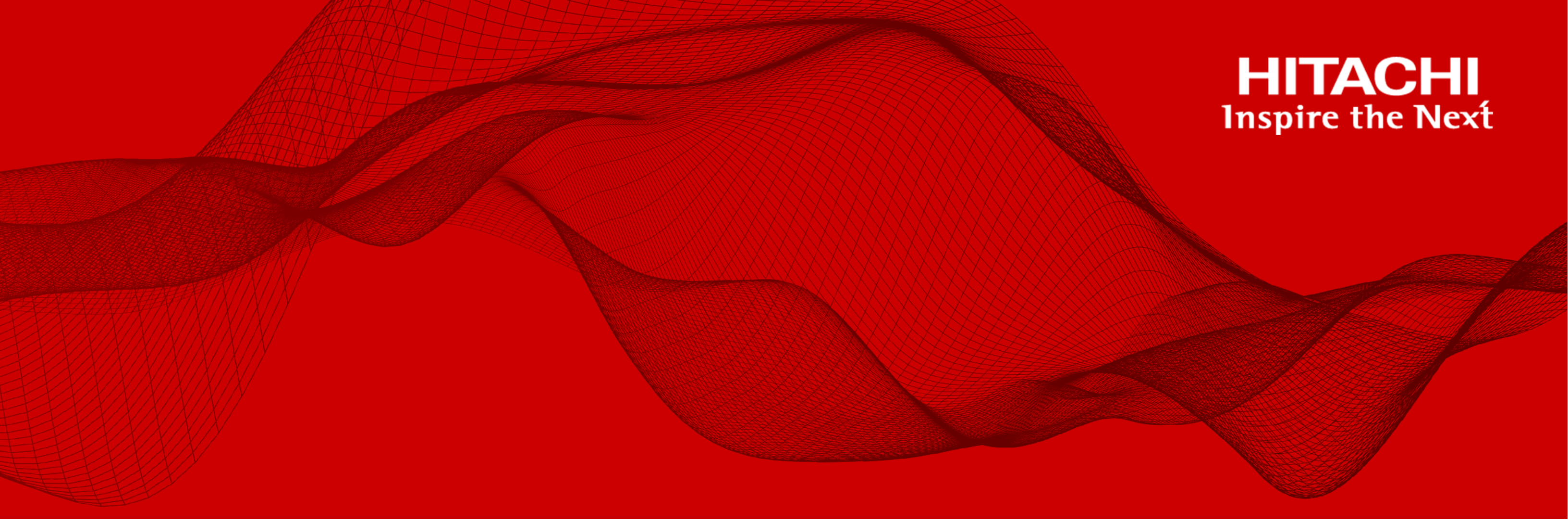


Bravura Identity

Quick Start Guide

Software revision: 12.2.4
Document revision: 30072
Last changed: 2022-03-01

Contents

Part I

INTRODUCTION

About this document 1

1.1 This document

This document is intended as a guide for setting up *Bravura Identity* for testing or demonstration purposes. It includes instructions and examples for the most common cases.

If you have not yet installed *Hitachi ID Bravura Security Fabric* please use the "Installation Quick Start Guide" (installation-quickstart.pdf) for test or demonstration installations, or the *Bravura Security Fabric* Documentation for full deployment.

When planning a major deployment, it is recommended that you read the *Bravura Security Fabric* Documentation .

1.2 Conventions

This document uses the following conventions:

This information . . .	displayed in . . .
Variable text (substituted for your own text)	<*angle brackets*>
Non-text keystrokes – for example, **[Enter]** key on a keyboard.	**[brackets]**
Terms unique to *Hitachi ID Bravura Security Fabric*	*italics*
Button names, text fields, and menu items	**boldface**
Web pages (names)	***italics and boldface***
Literal text, as typed into configuration files, batch files, command prompts, and data entry fields	`monospace font`

Wrapped lines of literal text (indicated by the → character)	`Write this string as a`
	`→single line of text.`

Hypertext links – click the link to jump to a section in this document or a web site	Purple text
External document – click the link to jump to a section in another document. The links only work if the documents are kept in the relative directory path.	Magenta text

1.3 Feedback and help

If you have feedback about this document or wish to report an omission or error, please contact doc-feedback@Hitachi-ID.com.

If you require technical assistance with *Hitachi ID Bravura Identity*, contact support@Hitachi-ID.com.

Implementing User Provisioning 2

To implement user provisioning with *Hitachi ID Bravura Identity*:

1. Set up email notification

   Bravura Identity actively notifies users about events that may require their attention; this is generally done through email. It is recommended that all users have email addresses configured.

   Ensure that the email server and port are correctly configured on the **Manage the system** → **Workflow** → **Email configuration** page.

2. Add target systems

   Add at least one target system that will be an authoritative list of users to be imported into *Bravura Identity*. If supported, ensure that all users have email addresses configured on the target. At least one target system should be able to verify passwords for users.

3. Set up accounts on each managed system to use as templates in *Bravura Identity*

   See the *Bravura Security Fabric* Integration Guide for information about creating accounts on specific systems. Ensure that you note the login ID of each model account.

   This is not necessary if new account requests will be fulfilled by human implementers.

   > **Note:** It is recommended that you do *not* add template accounts to managed groups. Managed group memberships should be handled by including them in roles.

4. Configure account attributes if required

   The term *account attributes* refers to the attributes of accounts on target systems. *Bravura Identity* uses an attribute catalog to determine rules for “handling” each attribute when managing users. You can override the default settings for templates, target systems, or target types.

5. Import users

   Run auto discovery to import a list of users, their accounts and other attributes, from one or more target systems.

6. Configure authentication

   Ensure that the **Authentication priority** list and **Identification priority** list are configured on the **Policies** menu. This is required to allow users to access the main menu.

7. Add profile and request attributes

   Profile and request attributes are used to collect and display information about a user. They can be mapped to account attributes.

8. Add profile and request attribute groups for access control

   Grouping attributes allows you to configure access controls to determine users' read / write privileges. They also determine how profile and request attributes are displayed to users.

9. Add template accounts

   Bravura Identity template accounts are mapped to model accounts on target systems. See the Connector Pack Integration Guide to learn how to set up template accounts for each target type.

   Users set up or request new accounts based on individual templates or named sets of templates referred to as roles.

10. Configure managed groups

    Bravura Identity uses managed groups to manage memberships in groups on target systems.

11. Add roles

    Users assign required resources to a set of users by using roles. Users can also request a role.

12. Configure access rules

    Access rules determine what users can do for themselves or others.

13. Add segregation of duties rules

    Users request exceptions to roles or possible access conflicts.

14. Configure authorization workflow

15. Configure user provisioning options, including:

    - Resource assignment
    - Profile ID assignment
    - Password options
    - Provisioning by human agents, or *implementers*.

16. Configure web features for request input, validation, and authorization

Part II

CONFIGURING IDENTITY MANAGER

Adding a target system 3

Hitachi ID Bravura Identity manages accounts on shared computer systems referred to as *target systems*. In order to list and manage accounts on these systems, you must first define target system parameters and operations using the *Manage the system* (PSA) module.

This section shows you the typical procedure for adding an Microsoft Active Directory target. For this demonstration, this target will be set up so that it becomes the source of *Bravura Identity* profiles. This means that users with accounts in Active Directory will have profiles, including full user name, created for them in *Bravura Identity*.

1. Click **Manage the system** → **Resources** → **Target systems** → **Manually defined** to see the ***Target systems*** page.
2. Click **Add new...** to add a new target system.
3. Enter a unique identifier for the new target system. The target **ID** can contain *only* letters (A-Za-z), digits (0-9), and underscores (_).
4. Select the target system's **Type**; for example, **Active Directory**.
5. Type a **Description** for the target system.
6. Click **Change** next to the **Address** field to enter values for the target system address. For Active Directory, there are three primary methods for specifying the Active Directory target address:

   - `globaldomain.example.com`
   - `\\mydomaincontroller.example.com`
   - `\\mydomaincontroller`

   You can restrict user listing by container or group membership.
7. Select the **Source of profile IDs** checkbox.
8. If you want *Bravura Identity* to generate a list of attributes for each account during auto discovery, select **List attributes**. You *must* select this checkbox if you want *Bravura Identity* to import OrgChart data from the target system.
9. Select the **Allowed in the certification process** checkbox.
10. For this demonstration installation, leave other parameters with default values.
11. Click **Add**.

    The ***Administrator credentials*** page displays so you can add a target system administrator for the target.
12. Type the target system administrator's login ID in the **Administrator ID** field.

13. Type the account password in the **Password** and **Confirm password** fields.
14. Click **Update**.

For more detailed information about target configuration parameters and options, see the *Bravura Security Fabric* Documentation .

Configuring Email notification 4

Hitachi ID Bravura Identity actively notifies users about events that may require their attention; this is generally done through email. Some *Bravura Identity* features, such as *authorization workflow*, require the ability to notify users and rely heavily on this interaction.

For a production deployment, Hitachi ID Systems recommends that all users have an email address defined in *Bravura Identity*. In most cases, *Bravura Identity* determines email addresses by the value of the EMAIL profile attribute, which can be mapped to an account attribute on a given target system; for example, the EMAIL profile attribute is mapped to the mail attribute in an Active Directory target system by default.

Other options for defining email addresses are detailed in Determining users' email addresses.

Configure the following email settings on the **Manage the system** → **Workflow** → **Email configuration** page:

Table 4.1: Email options

Option	Description
MAIL SERVER	The mail server address.
MAIL SERVER PORT	The port number for the mail server. For SMTP mail, this is usually `25`.
RECIPIENT EMAIL	The email address of the *Bravura Identity* administrator who should receive notification of events relating to the running of the server. This value is set during installation.
SENDER EMAIL	The email address that will appear as the sender of emails.

For more detail about email notification settings, see the *Bravura Security Fabric* Documentation .

Importing Users 5

In *Hitachi ID Bravura Identity*, profiles are used to authenticate, audit, and control access for individual users. Some systems do not differentiate between users and accounts; however, in Hitachi ID Systems software, some users – product administrators – do not necessarily have accounts. Note the following terminology:

User *Bravura Identity* user. Users are identified by their profile IDs.

Account An object on a target system that establishes a user's identity on that target system.

Profile A record within *Bravura Identity* describing a user, their associated accounts, and other data such as attributes or access controls.

For more detail about these and other options, see the *Bravura Security Fabric* Documentation .

5.1 Importing users

You add users to *Hitachi ID Bravura Identity* by importing lists of users from one or more systems of record, referred to as target systems. The import process is part of *auto discovery*.

To import users into *Bravura Identity*:

1. Add your source of profile IDs target system to *Bravura Identity*.

   Ensure that you select the **Source of profile IDs** checkbox on the ***Target system information*** page.

2. Execute auto discovery.

   To do this, click **Manage the system** → **Maintenance** → **Auto discovery** → **Execute auto discovery**, then click **Continue**.

   This process may take a while. You can click Refresh 🔄 to reload the page and check progress.

3. Determine whether the import was successful by running a users report.

   From the main menu click **Manage reports** → **Reports** → **Users** → **Accounts**. See the Reports User Guide (`reports.pdf`) for details.

5.1.1 User types and access controls

User groups and rules provides details about the types of *Hitachi ID Bravura Identity* users, and shows you how to control users' permissions and capabilities.

Users' capabilities determine the features and functions that they can access in *Bravura Identity*; for example, only certain users can access the *Manage the system* (PSA) module. Depending on their capabilities, users are categorized as one or more of the following user types:

Regular user A user who has an account on a target system, and can log into *Bravura Identity*.

Generally, you create regular users by creating a source of profiles in *Bravura Identity*.

Requester A user who can request access changes.

In general, all regular users can be requesters; however, a user's ability to submit requests may be limited by his access rules, policy rules, authorization workflow logic, or *Bravura Identity* configuration.

Help desk user A regular user who can log into *Bravura Identity* and act on the behalf of other users. Help desk users are participants in a user class that has been granted user access rules, such as the HELP_DESK_MANAGER or the GLOBAL_HELP_DESK user classes.

Authorizer a user who can review and act on security change requests. Any regular user can be assigned as an authorizer.

Delegation manager A user who can delegate the responsibilities of a user to another user.

You can grant this capability by assigning a user the "Delegate workflow requests" user access rule. This capability can also be delegated.

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

For example, instead of running a connector program, *Bravura Identity* can notify an implementer that an access change request has been approved. The implementer then uses the *Requests* app to accept the task, completes the change using tools available on the target system, then uses the *Requests* app to mark the task as completed.

You can grant this capability by adding any user as an implementer for resource operations on a per-resource basis. If a user is also an inventory manager, then they can also assign inventory items. This capability can be delegated.

Inventory manager A user who can manage inventory items by location and type.

You can grant this capability by adding a user to the list of inventory managers (**Manage the system → Inventory → Inventory managers**), and designating the user as an inventory manager for a specific inventory location and type. If a user is also an implementer, then they can also assign inventory items. This capability can be delegated.

Reviewer A user with the responsibility for certifying users' access rights.

You can grant this capability by selecting the user as a reviewer for a certification campaign.

Product administrator A user who has been granted administrative privileges. These privileges control access to the administrative web modules and the *Bravura Identity* API. Product administrators may or may not have an account on a target system.

There are several types of product administrators.

5.2 Static authorizers

In *Hitachi ID Bravura Identity*, an *authorizer* is a user who can review and act on security change requests. You can assign any user as an authorizer to resources such as target systems or managed groups; however adding authorizers in the workflow menu allows you to set up a shortlist to choose from, and allows you to define their role and rights, and how they are notified.

To add an authorizer:

1. Click **Workflow** → **Authorizers**.
2. Type a profile ID in the **ID** field or click **Search** to select the user that you want to add as an authorizer.
3. Select the authorizer's rights, as needed.
4. Click **Add** at the bottom of the form.
5. If necessary, provide an email address and determine when the authorizer should be notified of requests.

Mapping Attributes: OrgChart Data 6

The term *account attributes* refers to the attributes of user accounts on target systems. There are also special account attributes, called *pseudo-attributes*, that exist only in *Hitachi ID Bravura Identity*. They are used to compose values or set flags on a target system. Each target system type has a different list of account attributes.

Bravura Identity includes a “catalog” of shipped default attributes for each target system type. *Bravura Identity* uses the attribute catalog to determine rules for “handling” each attribute when managing users on a target system. The catalog also determines which attributes’ values should be loaded during auto discovery.

Bravura Identity enables you to override the default rules for handling account attributes. Using the *Manage the system* (PSA) module you can:

- Control how accounts are created, updated, or deleted
- Determine which attributes to load during auto discovery
- Add new attributes
- Map account attributes to profile and request attributes

To illustrate how attribute mapping can be used, this chapter shows you how to map an account attribute to a profile attribute in order to build OrgChart data. This data can be used to escalate workflow requests or configure certification campaigns.

6.1 Mapping attributes for organization chart management

To illustrate how attribute mapping can be used, this section shows you how to map an account attribute to a profile attribute in order to build OrgChart data. This data can be used to escalate workflow requests or configure certification campaigns.

Map an account attribute mapping if you want *Hitachi ID Bravura Identity* to:

- Build the initial OrgChart automatically
- Propagate changes to target systems when the OrgChart is updated

The account attribute that you configure must contain the long ID of the user's primary manager. *Bravura Identity* uses the built-in ORGCHART_MANAGER profile/request attribute to determine each user's primary manager. The attribute can also be used to directly update a user's primary manager. Ensure that your "manager" account attribute is configured to be loaded during auto discovery.

CAUTION: *Bravura Identity* allows exactly one OrgChart. If *Bravura Identity* detects multiple trees in your pre-existing data, it uses the largest tree as the basis for your OrgChart.

If there are multiple trees with the same size, then *Bravura Identity* chooses the tree with the greatest depth. Finally, if there are multiple trees with equal depth, then it chooses the first tree that it encountered.

If you want *Bravura Identity* to propagate OrgChart changes to target systems, ensure that your "manager" account attribute can be set.

CAUTION: After the initial OrgChart has been imported, if *Bravura Identity* is still set up to load the "manager" account attribute, but is not set up to propagate OrgChart changes back to the target system, any changes made to the OrgChart using *Bravura Identity* will be overwritten during the next auto discovery.

To configure an Microsoft Active Directory or LDAP Directory Service account attribute for OrgChart management:

1. Click **Resources** → **Account attributes** → **Target system**, then select ▶ the appropriate target.

   Alternatively, you can configure account attributes at the target type level.
2. Click the **Defaults** tab.
3. Override the default account attribute configuration. To do this, for an:

   - LDAP Directory Service target, select ▶ the `manager` attribute.
   - Active Directory target, select ▶ the `manager` attribute.

   Click **Override**.

4. Ensure that the **Map account attribute to profile/request attribute** option is set to `ORGCHART_MANAGER`.
5. Select the **Load attribute values from target system** checkbox if you want *Bravura Identity* to import OrgChart data from the target system.
6. Set **Action when creating account** to "Set to specified value". This means the value will be set by the ORGCHART_MANAGER profile attribute.
7. Select an appropriate action from the **Action when updating account** drop-down list.

   If you do *not* want *Bravura Identity* to propagate OrgChart changes to the target system, select **Do not set this attribute**.
8. Click **Add**.
9. If *Bravura Identity* prompts you to confirm changes to attribute mappings:

   (a) Click **Yes** (recommended).

   (b) Run auto discovery (**Maintenance** → **Auto discovery** → **Execute auto discovery**).

See Implementing Organization Chart Management for more information about organization chart management.

Defining Template Accounts 7

Hitachi ID Bravura Identity uses *templates* to:

- Automatically create new accounts based on the parameters of pre-existing accounts
- Attach inventory items to user profiles

Before you add templates for account provisioning:

1. Set up model accounts on each managed system to use as templates in *Bravura Identity*.

   For example, add a new user in Microsoft Active Directory. Ensure that the **User logon name** and **User logon name (pre-windows 2000)** fields match, or new accounts created using this template may be created with an incorrect value. You can define additional properties – group memberships, logon hours, a logon script, or home directory – for the template account using **Active Directory Users and Computers**. By default, *Bravura Identity* copies many of these properties (attributes) when creating a new user.

   > **Note:** It is recommended that you do *not* add template accounts to *Bravura Identity* managed groups. Managed group memberships should be handled by including them in roles.

2. Add target systems to *Bravura Identity*.
3. Import accounts from target systems.

The following provides an example for setting up a template for user account provisioning:

1. Click **Manage the system** → **Resources** → **Template accounts**.
2. Click **Add new. . .** .
3. Enter an **ID**, and a **Description** to display to users.
4. Select the **Target system ID**.
5. Search for, or type the login ID of the account you want to use as a model.
6. Click **Add**.
7. Select the **Authorization** tab.

8. Type a value for the:

   - **Minimum number of authorizers** – A value of 0 means requests for the resource are auto-approved.
   - **Number of denials before a change request is terminated** – A resource request is canceled when this number of authorizers deny it, as long as the **Minimum number of authorizers** has not been reached.

9. Click **Select...** at the bottom of the **Authorizers** table.
10. Search for, or enable the checkboxes next to the authorizers that you want to assign.
11. Click **Select** at the bottom of the page.

Managing Groups 8

A managed group is a group of accounts defined on a target system, whose membership is monitored and managed in *Hitachi ID Bravura Identity*. On some target systems this can include groups inside groups. An unmanaged group is simply a group whose membership is not monitored and managed in *Bravura Identity*.

During auto discovery, *Bravura Identity* lists all available groups from supported target systems, then loads the group information into its database. By default, *Bravura Identity* only lists group membership for managed groups. This option can be modified on the ***Target system information*** page.

When a group is managed:

- Users can submit requests to join or leave the group.
- The group can be included in roles, so that when a requester selects a role, the request automatically includes group membership.
- The group can be included in segregation of duties (SoD) rules so that users' membership can be examined when identifying possible access conflicts.
- The group can be included in certification campaigns so that users' memberships can be reviewed.
- The group's membership can be used to segment users into user classes.

8.1 Managing groups automatically

Rather than configuring each group individually, you can:

- Configure *Hitachi ID Bravura Identity* to automatically manage groups during auto discovery.

  See Automatically managing groups via auto discovery for details.
- Use the **managegrp** program to configure managed groups in batches. The program reads entries from a file and configures all the specified groups as moderated managed groups.

  See managegrp in the Bravura Security Fabric *Reference Manual* to learn how to use this program.

8.1.1 Automatically managing groups via auto discovery

If supported by the target system, *Hitachi ID Bravura Identity* connectors can list groups during auto discovery. Group owner information is included if it is available. You can configure *Bravura Identity* so that it automatically manages groups and assigns the owner as the group authorizer.

To do this, configure the **Automatically manage groups** option on the applicable ***Target system information*** page. This option applies to Microsoft Active Directory, Oracle Database, or Domino Server Script target system types. Select one of the following:

- **(Disabled)**: This option is disabled; this is the default setting.
- **Only groups with owners, moderated by owners**: Only manage groups that have an owner. Assign the owner as the group authorizer.
- **All groups, approval required**: Manage all groups on the target system. If a group has an owner, then the owner is assigned as the group authorizer. If a group has no owner, then no authorizer is assigned. Groups without authorizers require manual configuration.
- **All groups, no approval required**: Manage all groups on the target system. No authorizers are required by default.

In addition to adding the group owners as authorizers for the managed group, *Bravura Identity* changes the default values for the managed group as follows:

Option/variable	Value
Automatically add group owners as authorizers	Checked
Minimum number of authorizers	1
Number of denials before a change request is terminated	1
Authorization for joining group	Approval required
Authorization for leaving the group	Approval required

Bravura Identity does *not* change the configuration for groups that are already managed.

8.2 Managing groups manually

You use the ***Managed group information*** page to start or stop managing a group. To manually manage a group in *Hitachi ID Bravura Identity*:

1. Click **Manage the system** → **Resources** → **Groups**.
2. Select ▶ the target system on which the group resides.
3. Select ▶ the group that you want to manage.
4. Set authorization settings; for example set the **Authorization for joining group** to "Approval required".
5. Click **Manage**.
6. Execute auto discovery to load group memberships into the *Bravura Identity* database.

   Click **Manage the system** → **Maintenance** → **Auto discovery**.

8.3 Configuring group-level authorization

If authorization is required:

1. On the ***Managed group information*** page, click the **Authorization** tab.

2. Type a value for the:

   - **Minimum number of authorizers** – A value of 0 means requests for the resource are auto-approved.
   - **Number of denials before a change request is terminated** – A resource request is canceled when this number of authorizers deny it, as long as the **Minimum number of authorizers** has not been reached.

3. Click **Select...** at the bottom of the **Authorizers** table.
4. Search for, or enable the checkboxes next to the authorizers that you want to assign.
5. Click **Select** at the bottom of the page.

For more detail on managed groups, see the *Bravura Security Fabric* Documentation .

Adding Implementers 9

By default, account requests are fulfilled automatically by *Hitachi ID Bravura Identity* connectors. If you configure resource operations, then account requests are diverted to human *implementers* instead. Implementers are notified and invited to fulfill requests.

An implementer can be a regular user, or an authorizer who has the **Is an implementer** right.

Resource operations can be split between connectors and implementers on a per-operation basis. They can be defined for target systems, managed groups, and template accounts.

To set up resource operations for human implementation:

1. Select ▶ the resource you want to configure by clicking **Manage the system** → **Resources**, then:
   - **Target systems**
   - **Managed groups**
   - **Template accounts**
2. Click the **Resource operations** tab.
3. For each connector operation that you want to divert to an implementer, select the **Implementer operation** override action.
4. Click **Update**.
5. Click **Select...** at the bottom of the **Implementers** table.
6. Search for, or select the checkboxes next to the implementers that you want to assign to the resource.
7. Click **Select** at the bottom of the page.

See also:

Implementers can also be assigned by user class or using the IDSYNCH IMPLEMENTER PLUGIN. See Determining implementers for details.

Pre-defining Requests 10

The *Hitachi ID Bravura Identity* self-service request facility provides a high degree of flexibility, allowing users to request access changes that involve operations on technical resources. Requesters may not understand the technical details, but can express the request in business terms. For example, users may understand they need to hire a contractor, schedule employee termination, or move an employee to a new department, but may not understand the technical requirements of adding accounts on a target system, setting an account termination date, or managing group membership.

Bravura Identity allows you to configure pre-defined requests that:

- Define common requests in terms that are familiar to users.
- Reduce the number and complexity of steps required to make a request.

You must be a product administrator with the right to configure workflow setup to be able to configure pre-defined requests.

Pre-defined request status

When creating a pre-defined request you must set its status. For a pre-defined request to be used it must be enabled. An enabled pre-defined request can be deprecated once it is used.

Submitting pre-defined requests during a certification campaign

Reviewers' requests to modify or revoke entitlements during a certification campaign are submitted via pre-defined requests. Administrators can add customized pre-defined requests when initiating certification campaigns.

See Managing the Certification Process for more information on initiating certification campaigns.

Submitting pre-defined requests using report output

Users with the "Manage reports" administrative right can feed the output of a report back to *Bravura Identity*'s workflow engine via a pre-defined request.

After running a report, users can select a pre-defined request to submit, and map report columns to profile and request attributes. The request can be submitted immediately or scheduled along with the report. Segments of the report can be submitted to pre-defined requests with iterative submissions.

See Use case: Using report output to disable orphaned accounts and Use case: Using report output to enable disabled accounts.

10.1 Built-in pre-defined requests

The following is a list of built-in pre-defined requests included in the *Hitachi ID Bravura Identity*:

AUTORES Used by the `autores` utility during automatic resource assignment. See Automatic Assignment.

_CERT_ACCOUNT_GROUP_REMEDIATION_ Default remediation request for revoking account group memberships in certification.

_CERT_ACCOUNT_REMEDIATION_ Default remediation request for revoking accounts in certification.

_CERT_ATTR_REMEDIATION_ Default remediation request for updating profile attributes in certification.

_CERT_CHILD_GROUP_REMEDIATION_ Default remediation request for revoking child group memberships in certification.

_CERT_ROLE_REMEDIATION_ Default remediation request for revoking a role assignment in certification.

_CERT_TRANSFER_REMEDIATION_ Default remediation request for transferring a user profile in certification.

_CERT_USER_REMEDIATION_ Default remediation request for revoking a user profile in certification.

_COMPLETE_ATTRS_ Allows users to supply required profile and request attribute values when enforced enrollment is enabled for this task. See Enforced enrollment for more information about enforced enrollment.

_DISABLE_ACCOUNTS_ Allows help desk users to disable other users' accounts. The requester must be a member of the _GLOBAL_HELP_DESK_ user class and the GLOBAL_HELP_DESK rules must include the "Disable account" privilege.

_ENABLE_ACCOUNTS_ Allows help desk users to enable other users' accounts. The requester must be a member of the _GLOBAL_HELP_DESK_ user class and the GLOBAL_HELP_DESK rules must include the "Enable account" privilege.

_GROUP_ADD_MEMBERS_ Allows group owners to add accounts and child groups as members to multiple groups on target systems, using the *Groups* app.

_GROUP_ADD_OWNERS_ Allows group owners to add owners to multiple groups on target systems, using the *Groups* app.

_GROUP_ADD_PARENTGROUPS_ Allows group owners to add parent groups to multiple groups on target systems, using the *Groups* app.

_GROUP_CREATE_ Allows group owners to create a group on a target system, using the *Groups* app.

_GROUP_DELETE_ Allows group owners to delete a group on a target system, using the *Groups* app.

_GROUP_DELETE_MEMBERS Allows group owners to delete members from multiple groups, using the *Groups* app.

_GROUP_DELETE_OWNERS Allows group owners to delete owners from a multiple groups, using the *Groups* app.

_GROUP_DELETE_PARENTGROUPS Allows group owners to delete parent groups from a multiple groups, using the *Groups* app.

_GROUP_UPDATE_ATTRS Allows group owners to update attributes on one or more groups, using the *Groups* app.

_GROUP_UPDATE_MEMBERS Allows group owners to add or remove members from a group, using the *Groups* app.

_GROUP_UPDATE_OWNERS Allows group owners to add or remove owners from a group, using the *Groups* app.

_GROUP_UPDATE_PARENTGROUPS Allows group owners to add or remove parent groups from a group, using the *Groups* app.

IDTRACK Used by the **`idtrack`** utility when submitting requests. See Automated User Administration.

_RESOLVE_ENFORCEMENT_VIOLATIONS_ This pre-defined request is used for **`rbacenforce`**-generated requests. By default, it is enabled but not accessible to requesters.

_RESOLVE_ROLE_DEFICITS_ Allows users to add missing role entitlements.

_RESOLVE_SOD_VIOLATIONS_ Allows users to resolve segregation of duties (SoD) rules violations.

_UPDATE_ACCOUNTS_ Allows users to request to add or delete accounts from their profile or other users' profiles, when the requester has the "Create account" permission and a template account exists.

_UPDATE_ATTRS_ Allows users to update profile information for themselves or others, when the requester has the "Update profile" permission.

_UPDATE_GROUPS_ Allows users to add or revoke group memberships for themselves or others, when the requester has the "Manage group memberships" permission and groups are managed.

_UPDATE_ROLES_ Allows users to add or remove roles from their profiles or other users' profiles, when the requester has the "Add role" permission and a role exists.

_USER_ADD_GROUPS_ Allows users to join groups using the *Groups* app.

_USER_DELETE_GROUPS_ Allows users to leave groups using the *Groups* app.

10.2 Getting started

Requirements

Before you can create a pre-defined request, you need to set up:

- Attribute groups
- Templates
- Roles
- Network Resources
- Managed groups

Planning

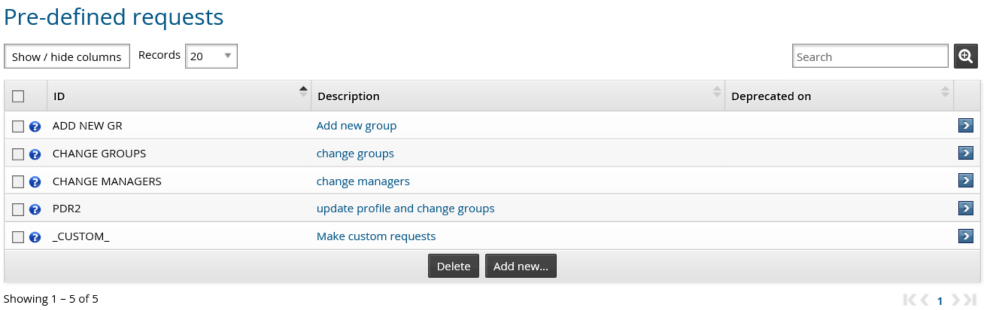
The way you configure the pre-defined request depends on whether they will be submitted from the *View and update profile* (IDR) module, from report output, or from certification. Hitachi ID Systems recommends that you create separate pre-defined requests to be used specifically with reports or with certification, because they have different configuration requirements.

Before creating your pre-defined requests determine:

- Who requires permission to create pre-defined requests?
- For each pre-defined request, who should be able to access and/or edit that request? For example, if it is a request that will be available in reports, the user will also need permission to run reports.
- How will you manage those permissions? For example, will you have a group on Active Directory that is attached to a user class, or will you explicitly attach accounts to a user class?
- Which requests do you want to run from the *View and update profile* (IDR) module? Hitachi ID Systems recommends that you do not make these requests available to reports or certification.
- Which requests do you want to run from reports? Only these pre-defined requests should be made available to reports by enabling the **Accessible from report** option.
- Which requests do you want to run from certification? Only these pre-defined requests should be made available to certification by enabling the **Accessible from certification** option.

Best practices

- Create pre-defined requests which are only used for reports, a separate set to be used for certification, and a separate set to be used from the *View and update profile* (IDR) module.
- Use the principle of least privilege; only provide users with privileges which are essential for them to do their work.
- When using report output to submit requests, do a trial run with a subset of data before using all of the records. See Submitting pre-defined requests using report output in the *Reports User Guide* for details.



Pre-defined requests

□	ID	Description	Deprecated on
□	ADD NEW GR	Add new group	
□	CHANGE GROUPS	change groups	
□	CHANGE MANAGERS	change managers	
□	PDR2	update profile and change groups	
□	_CUSTOM_	Make custom requests	

Showing 1 – 5 of 5

Navigation steps

You use the ***Pre-defined request information*** page to configure general information, and to access additional configuration settings. To configure pre-defined requests:

1. Click **Manage the system** → **Workflow** → **Pre-defined requests**.
2. To define:
   - A new pre-defined request – click **Add new. . .**
   - An existing pre-defined request – search for, or select ▶ the pre-defined request you want to view or modify.

Note: You cannot modify a deprecated pre-defined request. You must restore it first.

WARNING!: Changes to a pre-defined request that has been scheduled to run in a report can cause serious problems. Editing the pre-defined request will change its composition and may invalidate the attribute mappings. There is also the possibility that modifying the pre-defined request could change the report to pre-defined request's intended result.

Bravura Identity will warn you if the request is scheduled to run in a report; however, you can still edit the pre-defined request. Remember to thoroughly test your changes.

10.3 Use cases

This section includes steps through some typical use cases for pre-defined requests:

- Use case: Requesting a group membership
- Use case: Creating a new user, adding a role
- Use case: Request a new desktop
- Use case: Updating a subordinate's scheduled termination
- Use case: Using report output to disable orphaned accounts
- Use case: Using report output to enable disabled accounts

10.3.1 Use case: Requesting a group membership

This use case demonstrates how to add a pre-defined request to allow users to easily request membership to a limited set of groups. It assumes you have set up a target system and managed groups (p18).

1. Click **Manage the system** → **Workflow** → **Pre-defined requests** and add a new request with the following general settings:

   ID `CHANGELOCALGROUP`

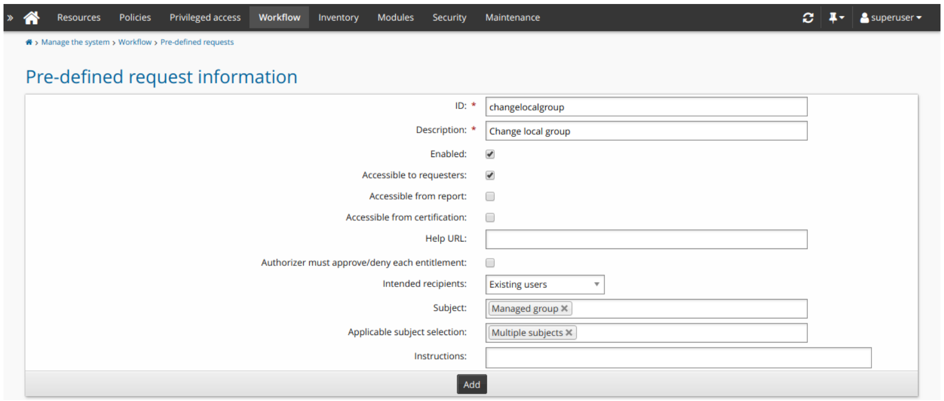
   Description `Change local group`

   Enabled Selected

   Intended recipients Existing users

   Instructions `Select options to join or leave your local group.`

2. Click **Add**.



Pre-defined request information

ID: *	changelocalgroup
Description: *	Change local group
Enabled:	☑
Accessible to requesters:	☑
Accessible from report:	☐
Accessible from certification:	☐
Help URL:	
Authorizer must approve/deny each entitlement:	☐
Intended recipients:	Existing users
Subject:	Managed group ✕
Applicable subject selection:	Multiple subjects ✕
Instructions:	

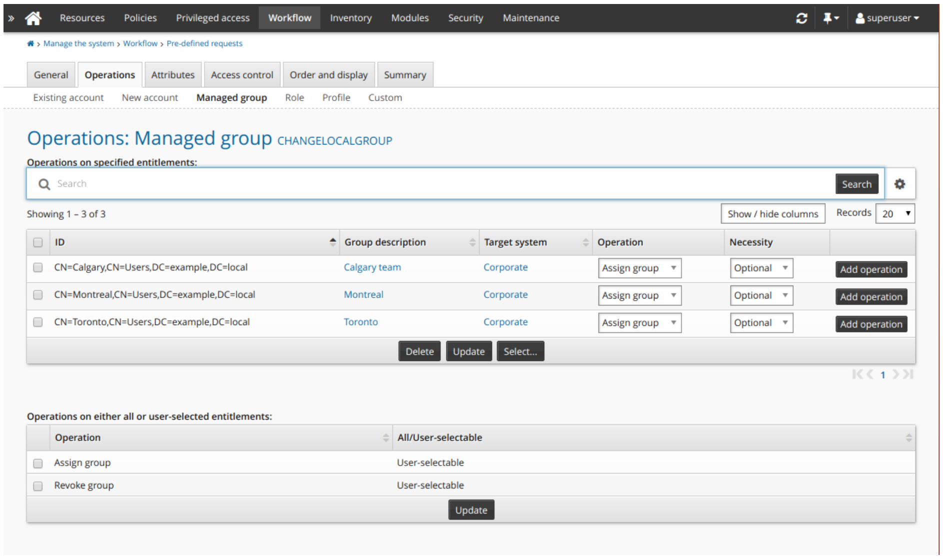
See Creating a pre-defined request for more information on general settings. You can now define operations and other parameters.

Define operations

For this use case, the request is to assign or revoke group memberships:

1. Click the **Operations** tab, then the **Managed group** sub-tab.
2. Click **Select. . .** to select managed groups that you want included in the request.

   Click **Select**.
3. Select "Assign group" from the **Operation** drop-down list, and "Optional" from the **Necessity** drop-down list next to each group.
4. Click **Update**.



Operations: Managed group CHANGELOCALGROUP

Operations on specified entitlements:

Showing 1 – 3 of 3

□	ID	Group description	Target system	Operation	Necessity	
□	CN=Calgary,CN=Users,DC=example,DC=local	Calgary team	Corporate	Assign group	Optional	Add operation
□	CN=Montreal,CN=Users,DC=example,DC=local	Montreal	Corporate	Assign group	Optional	Add operation
□	CN=Toronto,CN=Users,DC=example,DC=local	Toronto	Corporate	Assign group	Optional	Add operation

Operations on either all or user-selected entitlements:

□	Operation	All/User-selectable
□	Assign group	User-selectable
□	Revoke group	User-selectable

See Defining operations for more information on operation settings.

Add access controls to the request

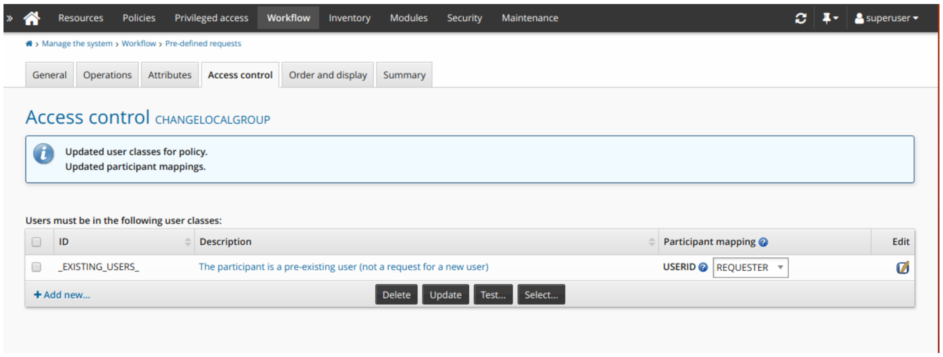
For this case, use the default _EXISTING_USERS_ class to allow existing users to request the new group membership.

To set up access controls:

1. Click the **Access control** tab.
2. Click **Select. . .** .
3. Select the _EXISTING_USERS_ user class and click **Select**.

   Hitachi ID Bravura Identity warns that you need to complete the access control configuration by mapping user class participants to a participant in the policy (requester or recipient).
4. Set the **Participant mapping** to REQUESTER.

5. Click **Update**.



Access control CHANGELOCALGROUP

Updated user classes for policy.
Updated participant mappings.

Users must be in the following user classes:

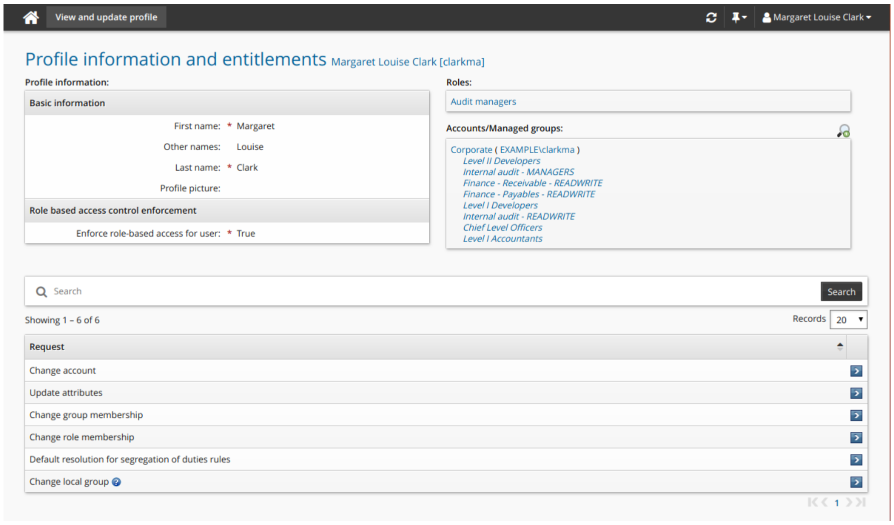
□	ID	Description	Participant mapping	Edit
□	_EXISTING_USERS_	The participant is a pre-existing user (not a request for a new user)	USERID REQUESTER	

See Defining access controls for more information on access control settings.

Submit a request

To submit the pre-defined request, login as an end user:

1. Click **View and update profile**.



Profile information and entitlements Margaret Louise Clark [clarkma]

Profile information:

Basic information

First name: * Margaret
Other names: Louise
Last name: * Clark
Profile picture:

Role based access control enforcement

Enforce role-based access for user: * True

Roles:

Audit managers

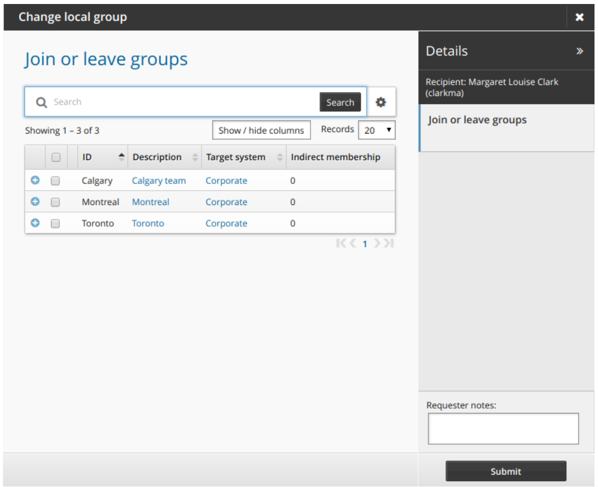
Accounts/Managed groups:

Corporate (EXAMPLE\clarkma)
Level II Developers
Internal audit - MANAGERS
Finance - Receivable - READWRITE
Finance - Payables - READWRITE
Level I Developers
Internal audit - READWRITE
Chief Level Officers
Level I Accountants

Showing 1 – 6 of 6

Request
Change account
Update attributes
Change group membership
Change role membership
Default resolution for segregation of duties rules
Change local group

2. Click **Change local group**.



Showing 1 – 3 of 3

Records 20

	ID	Description	Target system	Indirect membership
□	Calgary	Calgary team	Corporate	0
□	Montreal	Montreal	Corporate	0
□	Toronto	Toronto	Corporate	0

Recipient: Margaret Louise Clark (clarkma)

3. Select groups you want to join, then click **Submit**.

10.3.2 Use case: Creating a new user, adding a role

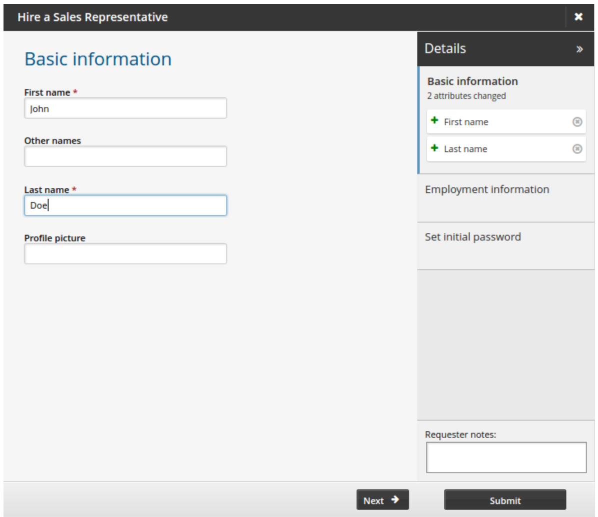
To submit the pre-defined request, login as an end user:

1. From the main menu , click **Create a new user profile** .

   If your administrator has set up pre-defined requests, *Hitachi ID Bravura Identity* displays a menu of request types.

2. Click **Hire a Sales Representative**.

3. Enter basic profile information.



First name *: John

Other names:

Last name *: Doe

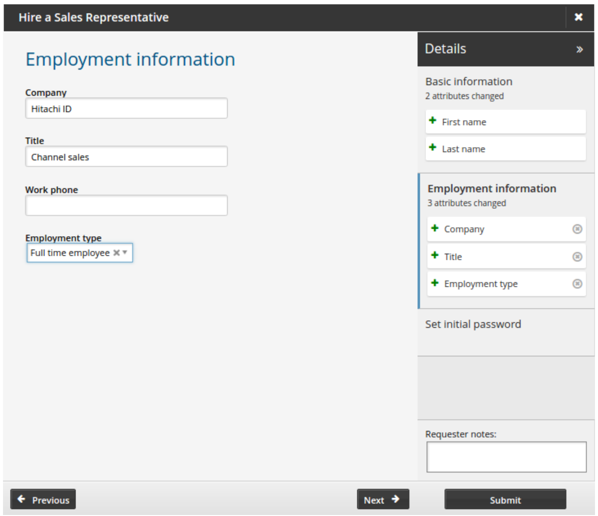
Profile picture:

Basic information
2 attributes changed
+ First name
+ Last name

Click **Next**.

4. Enter employment information.

   This is information defined by the ORG-INFO attribute group.



Hire a Sales Representative

Employment information

Company: Hitachi ID

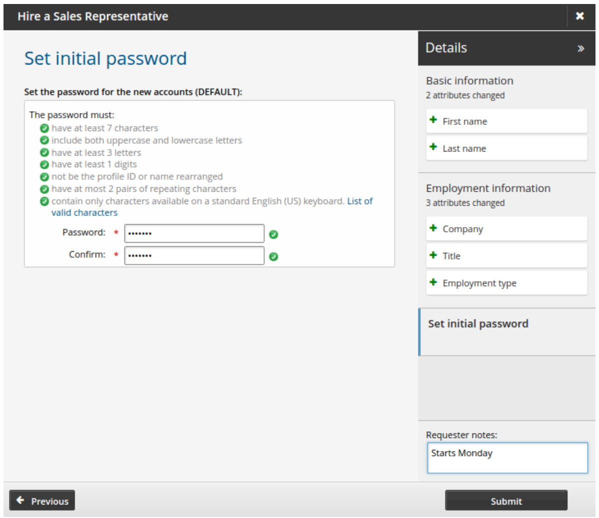
Title: Channel sales

Work phone:

Employment type: Full time employee

   Click **Next**.

5. Set the initial password as required for new accounts.



Hire a Sales Representative

Set initial password

Set the password for the new accounts (DEFAULT):

The password must:

- ✓ have at least 7 characters
- ✓ include both uppercase and lowercase letters
- ✓ have at least 3 letters
- ✓ have at least 1 digits
- ✓ not be the profile ID or name rearranged
- ✓ have at most 2 pairs of repeating characters
- ✓ contain only characters available on a standard English (US) keyboard. List of valid characters

Password: * ••••••• ✓

Confirm: * ••••••• ✓

Requester notes: Starts Monday

6. Click **Submit**.

10.3.3 Use case: Request a new desktop

This use case demonstrates how to define a request users can select to submit a request for a new desktop.

This case assumes:

- You have set a NULL target system for inventory.
- You have configured an inventory template. See Inventory Templates.
- A REQUEST-NOTES profile and request attribute exists.

  See Profile/Request Attributes for details.
- The profile and request attribute is a member of an attribute group called REQUEST_NOTES.

  See Attribute Groups for details.

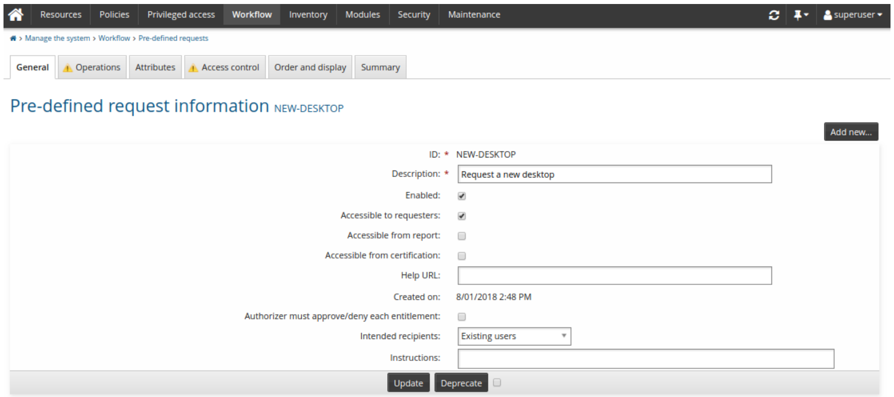
1. Click **Manage the system** → **Workflow** → **Pre-defined requests** and add a new request with the following general settings:

   ID `NEW-DESKTOP`

   Description `Request a new desktop`

   Enabled Selected

   Intended recipients Existing users.



Pre-defined request information NEW-DESKTOP

ID: * NEW-DESKTOP

Description: * Request a new desktop

Enabled: ☑

Accessible to requesters: ☑

Accessible from report: □

Accessible from certification: □

Help URL:

Created on: 8/01/2018 2:48 PM

Authorizer must approve/deny each entitlement: □

Intended recipients: Existing users

Instructions:

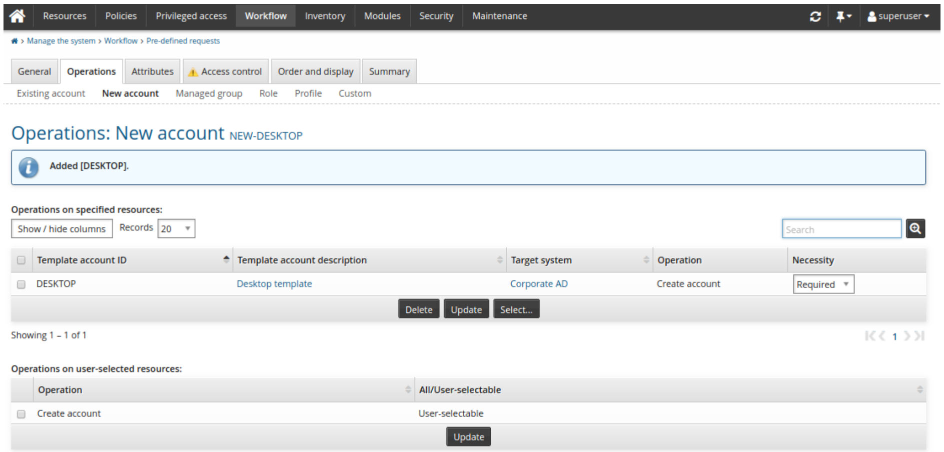
2. Click **Add**.

See Creating a pre-defined request for more information on general settings. You can now define operations and other parameters.

Define operations

For this use case, the request is to add an inventory item to an existing user profile:

1. Click the **Operations** tab, then the **New account** sub-tab.
2. Click **Select...** in the upper table.
3. Select the DESKTOP template and click **Select**.
4. Ensure the **Necessity** is set to "Required".



Operations: New account NEW-DESKTOP

Added [DESKTOP].

Operations on specified resources:

□	Template account ID	Template account description	Target system	Operation	Necessity
□	DESKTOP	Desktop template	Corporate AD	Create account	Required

Showing 1 – 1 of 1

Operations on user-selected resources:

	Operation	All/User-selectable
□	Create account	User-selectable

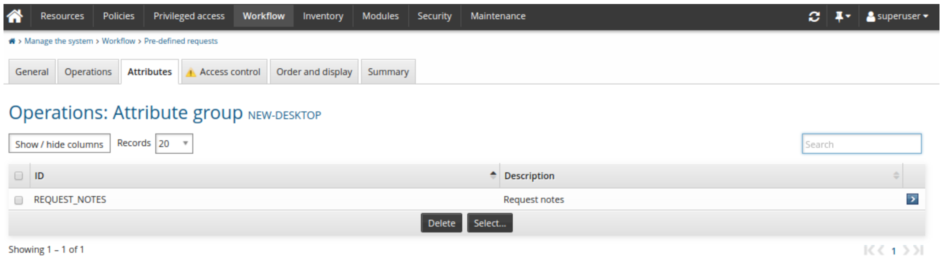
Note: Inventory templates are used to attach inventory items to user profiles rather than create new accounts.

See Defining operations for more information on operation settings.

Select attributes

Select attribute groups to determine what information needs to be updated.

1. Click the **Attributes** tab.
2. Click **Select. . .**
3. Select REQUEST_NOTES.
4. Click **Select**.



Operations: Attribute group NEW-DESKTOP

□	ID	Description
□	REQUEST_NOTES	Request notes

Showing 1 – 1 of 1

See Selecting attributes for requests for more information on attribute settings.

Add access controls to the request

For this case, use the default _EXISTING_USERS_ class to allow existing users to request a new desktop.

To set up access controls:

1. Click the **Access control** tab.
2. Click **Select. . . .**
3. Select the _EXISTING_USERS_ user class and click **Select**.

   Hitachi ID Bravura Identity warns that you need to complete the access control configuration by mapping user class participants to a participant in the policy (requester or recipient).
4. Set the **Participant mapping** to REQUESTER.
5. Click **Update**.

See Defining access controls for more information on access control settings.

Customize the wizard

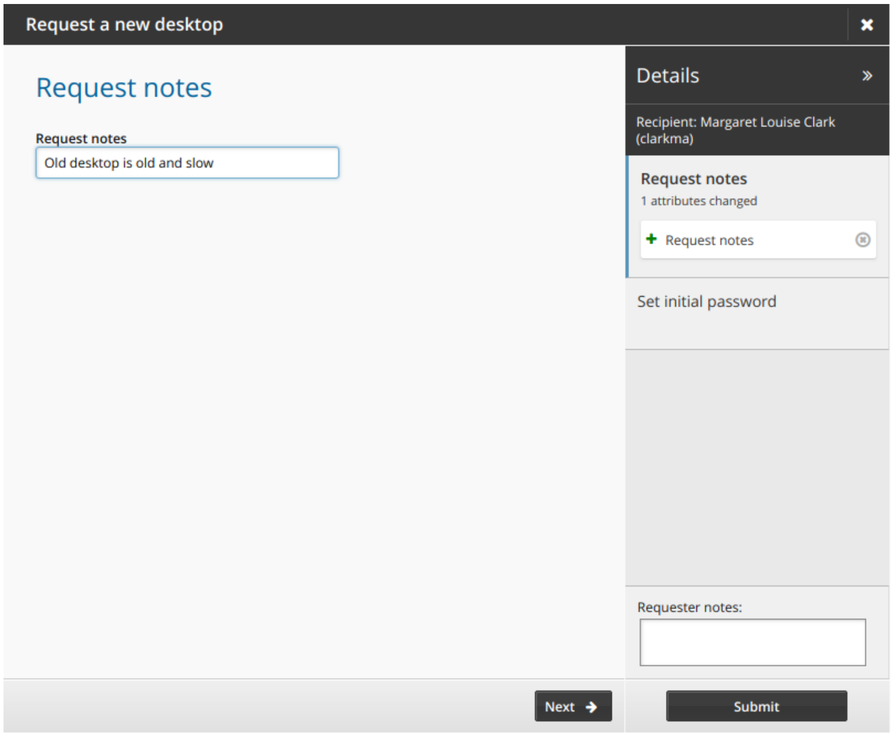
Hitachi ID Bravura Identity automatically adds request wizard pages according to the operations and attributes you add. To customize the wizard:

1. Click the **Order and display** tab.
2. Set the **Attribute group: Request notes** setting to "Show".
3. Click **Update**.

Submit a request

To submit the pre-defined request, login as an end user:

1. Click **View and update profile**.
2. Click **Request a new desktop**.
3. Enter request details.



Request notes: Old desktop is old and slow

Requester notes:

4. Click **Submit**.

The request has been submitted and in this case, the implementer will receive a notification and action the request.

10.3.4 Use case: Updating a subordinate's scheduled termination

This use case demonstrates how to invite a manager to defer a subordinate's scheduled termination. The manager will receive an email two weeks prior to the termination with a link to *Hitachi ID Bravura Identity*. When the manager follows the link and successfully logs in she can use the pre-defined request to update the subordinate's termination date.

This case assumes that an HR system that contains termination details is set up as a target system, and:

- The HR system's scheduled termination date account attribute is mapped to a profile and request attribute called SCHEDULED_TERMINATION_DATE.

  See Mapping Attributes: OrgChart Data for details.
- The profile and request attribute is a member of an attribute group called SCHEDULED_TERMINATION.

  See Attribute Groups for details.

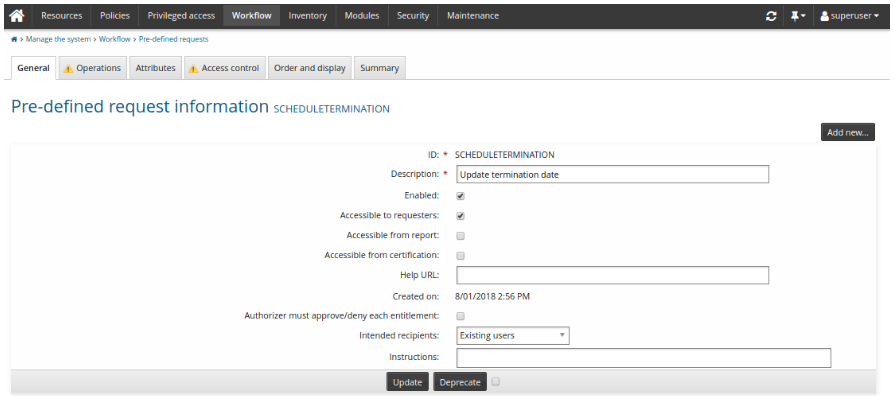
1. Click **Manage the system** → **Workflow** → **Pre-defined requests** and add a new request with the following general settings:

ID `SCHEDULETERMINATION`

Description `Update termination date`

Enabled Selected

Intended recipients Existing users



Pre-defined request information SCHEDULETERMINATION

ID: *	SCHEDULETERMINATION
Description: *	Update termination date
Enabled:	☑
Accessible to requesters:	☑
Accessible from report:	☐
Accessible from certification:	☐
Help URL:	
Created on:	8/01/2018 2:56 PM
Authorizer must approve/deny each entitlement:	☐
Intended recipients:	Existing users
Instructions:	

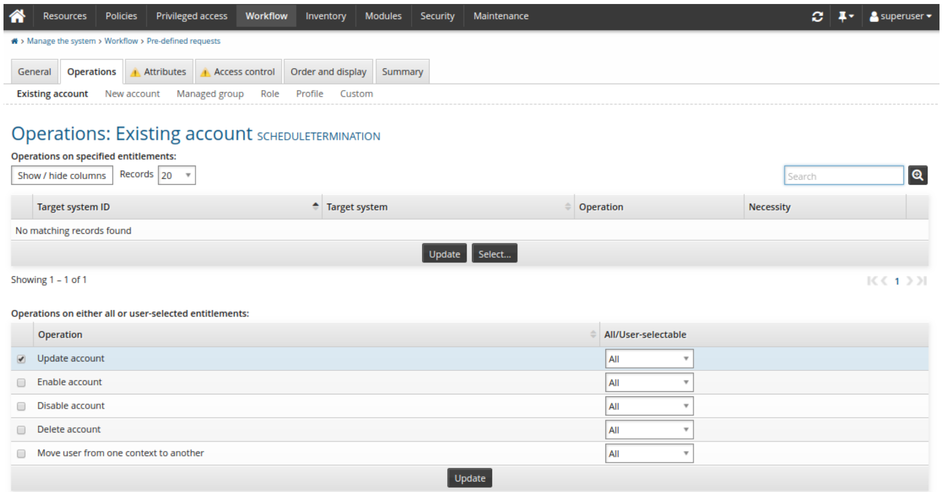
2. Click **Add**.

See Creating a pre-defined request for more information on general settings. You can now define operations and other parameters.

Define operations

For this use case, the request is to update existing accounts:

1. Click the **Operations** tab, then the **Existing account** sub-tab.
2. In the bottom table select **Update account** and select "All" from the **All/User-selectable** drop-down list.
3. Click **Update**.



Operations: Existing account SCHEDULETERMINATION

Operations on specified entitlements:

Target system ID	Target system	Operation	Necessity
No matching records found			

Showing 1 – 1 of 1

Operations on either all or user-selected entitlements:

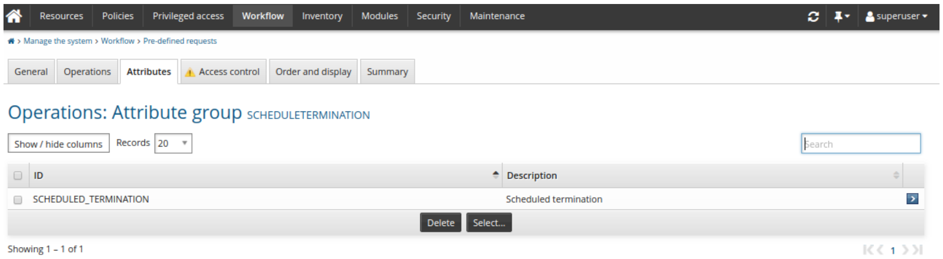
	Operation	All/User-selectable
☑	Update account	All
☐	Enable account	All
☐	Disable account	All
☐	Delete account	All
☐	Move user from one context to another	All

See Defining operations for more information on operation settings.

Select attributes

Select attribute groups to determine what information needs to be updated.

1. Click the **Attributes** tab.
2. Click **Select. . .**
3. Select SCHEDULED_TERMINATION.
4. Click **Select**.



Operations: Attribute group SCHEDULETERMINATION

Records 20

ID	Description
SCHEDULED_TERMINATION	Scheduled termination

Showing 1 – 1 of 1

See Selecting attributes for requests for more information on attribute settings.

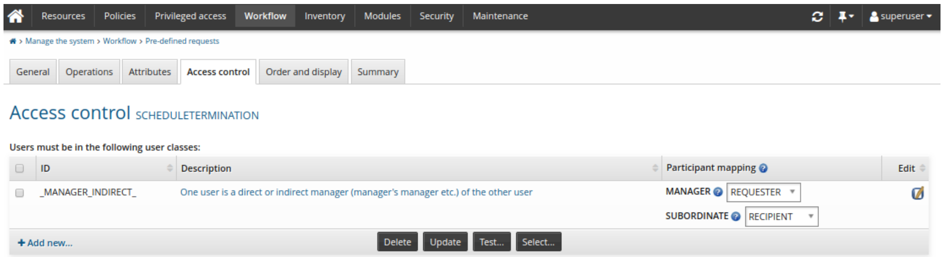
Add access controls to the request

For this case, use the default _MANAGER_INDIRECT_ class to allow a manager to request the update on behalf of a subordinate. We will assume that the Orgchart has been set up, and that managers have permission to update subordinates' information.

To set up access controls:

1. Click the **Access control** tab.
2. Click **Select. . . .**
3. Select the _MANAGER_INDIRECT_ user class and click **Select**.

   Hitachi ID Bravura Identity warns that you need to complete the access control configuration by mapping user class participants to a participant in the policy (requester or recipient).
4. Set the **Participant mapping** for MANAGER to REQUESTER, and set SUBORDINATE to RECIPIENT.
5. Click **Update**.



Access control SCHEDULETERMINATION

Users must be in the following user classes:

□	ID	Description	Participant mapping	Edit
□	_MANAGER_INDIRECT_	One user is a direct or indirect manager (manager's manager etc.) of the other user	MANAGER REQUESTER SUBORDINATE RECIPIENT	

See Defining access controls for more information on access control settings.

Customize the wizard

Hitachi ID Bravura Identity automatically adds request wizard pages according to the operations and attributes you add. In this case, *Bravura Identity* added a page for each of the attribute groups. In this case, you will hide the RBACENFORCE group from requesters, because the default setting is assumed.

To customize the wizard:

1. Click the **Order and display** tab.
2. Set the **Attribute group: Role based access control enforcement** setting to "Hide".
3. Click **Update**.

Configure tracking

1. Set up automated user administration (**`idtrack`**) to track the scheduled termination attribute.
2. During the nightly processing, when a termination is scheduled for two weeks from now, send an email to the manager notifying her of the upcoming termination. Embed a URL linking the user to the *View and update profile* (IDR) module:

   `https://idm-server/default/view-and-update-profile`

   When the manager successfully logs in she will be automatically redirected to the *View and update profile* (IDR) module, where she can select the `Update termination date` pre-defined request to update the termination date.

10.3.5 Use case: Using report output to disable orphaned accounts

This use case demonstrates how to create a pre-defined request and run a report to list orphaned accounts and then submit request to disable those accounts.

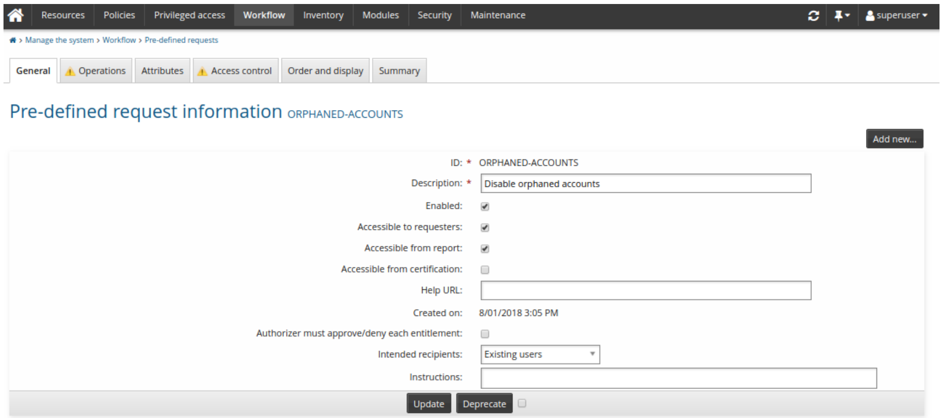
1. Click **Manage the system** → **Workflow** → **Pre-defined requests** and add a new request with the following general settings:

   ID `ORPHANED-ACCOUNTS`

   Description `Disable orphaned accounts`

Enabled Selected
Accessible from report Selected
Intended recipients Existing users

2. Click **Add**.



Pre-defined request information ORPHANED-ACCOUNTS

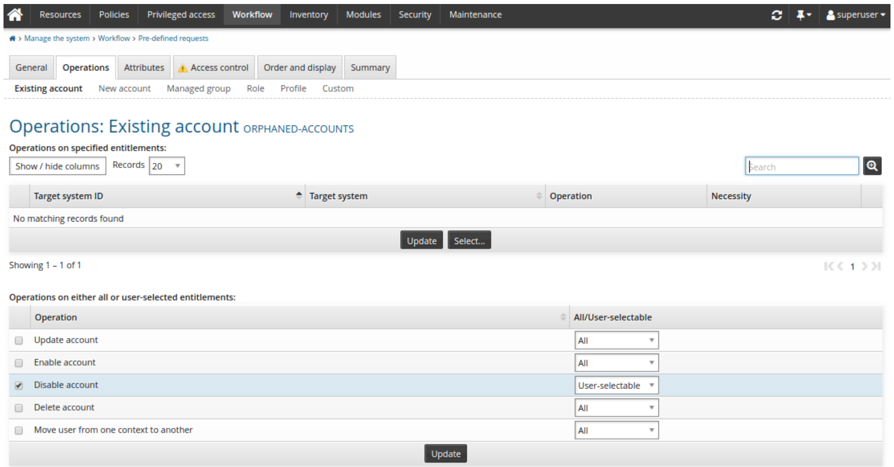
ID: *	ORPHANED-ACCOUNTS
Description: *	Disable orphaned accounts
Enabled:	☑
Accessible to requesters:	☑
Accessible from report:	☑
Accessible from certification:	☐
Help URL:	
Created on:	8/01/2018 3:05 PM
Authorizer must approve/deny each entitlement:	☐
Intended recipients:	Existing users
Instructions:	

See Creating a pre-defined request for more information on general settings. You can now define operations and other parameters.

Define operations

For this use case, the request is to disable existing accounts based on certain conditions:

1. Click the **Operations** tab, then the **Existing account** sub-tab.
2. In the bottom table select **Disable account** and select "User-selectable" from the **All/User-selectable** drop-down list.
3. Click **Update**.



Operations: Existing account ORPHANED-ACCOUNTS

Operations on specified entitlements:

Target system ID	Target system	Operation	Necessity
No matching records found			

Showing 1 – 1 of 1

Operations on either all or user-selected entitlements:

	Operation	All/User-selectable
☐	Update account	All
☐	Enable account	All
☑	Disable account	User-selectable
☐	Delete account	All
☐	Move user from one context to another	All

See Defining operations for more information on operation settings.

Add access controls to the request

For this case, use the default _REPORT_READERS_ user class to allow users who can run reports to submit this pre-defined request. We will assume that users have been added to the user class.

To set up access controls:

1. Click the **Access control** tab.
2. Click **Select. . .** .
3. Select the _REPORT_READERS_ user class and click **Select**.

   Hitachi ID Bravura Identity warns that you need to complete the access control configuration by mapping the user class participant to a participant in the policy (requester or recipient).
4. Set the **Participant mapping** to REQUESTER.

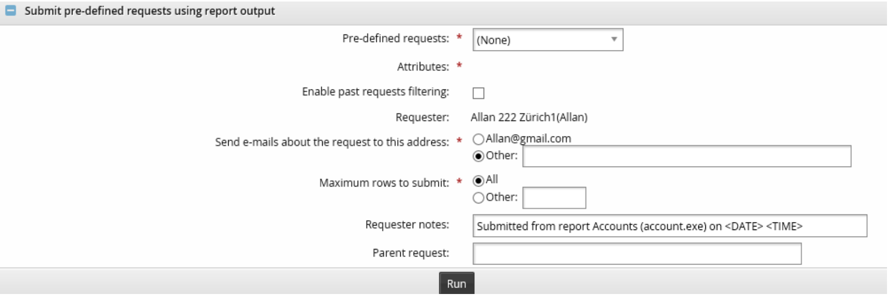
   This allows any user in the user class to act as requester of the request.
5. Click **Update**.

See Defining access controls for more information on access control settings. The pre-defined request is ready to use with report output.

Run the Orphan / Inactive report

To run a report and use the output to submit a request to disable orphan accounts:

1. Log in as a member of _REPORT_READERS_.
2. Click **Manage reports** → **Reports** → **Users** → **Orphan** / **Inactive**.
3. Run the report.
4. Expand **Submit pre-defined requests using report output** at the bottom of the report form.



Submit pre-defined requests using report output

Pre-defined requests: *	(None)
Attributes: *	
Enable past requests filtering:	□
Requester:	Allan 222 Zürich1(Allan)
Send e-mails about the request to this address: *	○ Allan@gmail.com ● Other:
Maximum rows to submit: *	● All ○ Other:
Requester notes:	Submitted from report Accounts (account.exe) on <DATE> <TIME>
Parent request:	

5. Select the ORPHANED-ACCOUNTS pre-defined request.
6. Click on the magnifying glass icon🔍 to configure **Attributes**.

   (a) Map the Recipient ID to a static ID, such as the user running the report.

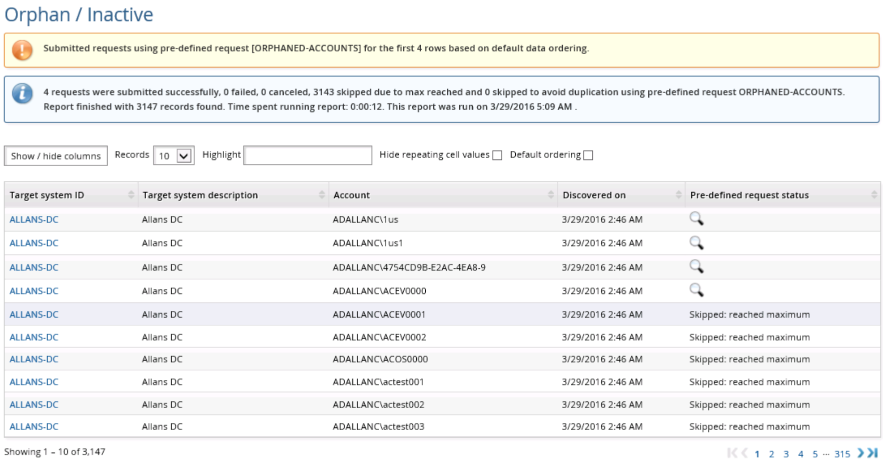
> **Note:** The recipient ID needs to match a *Bravura Identity* profile ID. If the report output has that information, you can map this attribute to that output, otherwise, you will need to enter a static ID.

(b) Map the target ID and account attributes to the respective columns.

(c) Click **Done**.

7. Click **Run for submission**.

   Hitachi ID Bravura Identity displays a summary of the requests submitted.



Orphan / Inactive

Submitted requests using pre-defined request [ORPHANED-ACCOUNTS] for the first 4 rows based on default data ordering.

4 requests were submitted successfully, 0 failed, 0 canceled, 3143 skipped due to max reached and 0 skipped to avoid duplication using pre-defined request ORPHANED-ACCOUNTS. Report finished with 3147 records found. Time spent running report: 0:00:12. This report was run on 3/29/2016 5:09 AM .

Target system ID	Target system description	Account	Discovered on	Pre-defined request status
ALLANS-DC	Allans DC	ADALLANC\1us	3/29/2016 2:46 AM	🔍
ALLANS-DC	Allans DC	ADALLANC\1us1	3/29/2016 2:46 AM	🔍
ALLANS-DC	Allans DC	ADALLANC\4754CD9B-E2AC-4EA8-9	3/29/2016 2:46 AM	🔍
ALLANS-DC	Allans DC	ADALLANC\ACEV0000	3/29/2016 2:46 AM	🔍
ALLANS-DC	Allans DC	ADALLANC\ACEV0001	3/29/2016 2:46 AM	Skipped: reached maximum
ALLANS-DC	Allans DC	ADALLANC\ACEV0002	3/29/2016 2:46 AM	Skipped: reached maximum
ALLANS-DC	Allans DC	ADALLANC\ACOS0000	3/29/2016 2:46 AM	Skipped: reached maximum
ALLANS-DC	Allans DC	ADALLANC\actest001	3/29/2016 2:46 AM	Skipped: reached maximum
ALLANS-DC	Allans DC	ADALLANC\actest002	3/29/2016 2:46 AM	Skipped: reached maximum
ALLANS-DC	Allans DC	ADALLANC\actest003	3/29/2016 2:46 AM	Skipped: reached maximum

Showing 1 – 10 of 3,147

   You can click on the info icon 🔍 in the request status column to view the status of each request, or use the Requests link from the main menu.

See the Reports User Guide for more information on running reports.

10.3.6 Use case: Using report output to enable disabled accounts

This use case demonstrates how to run the account report to list disabled accounts, then use the output to submit a request to enable those accounts.

1. Click **Manage the system** → **Workflow** → **Pre-defined requests** and add a new request with the following general settings:

   ID `ENABLE-ACCOUNTS`

   Description `Enable disabled accounts`

   Enabled Selected

   Accessible from report Selected

   Intended recipients Existing users

2. Click **Add**.

See Creating a pre-defined request for more information on general settings. You can now define operations and other parameters.

Define operations

For this use case, the request is to enable existing disabled accounts:

1. Click the **Operations** tab, then the **Existing account** sub-tab.
2. In the bottom table select **Enable account** and select "User-selectable" from the **All/User-selectable** drop-down list.
3. Click **Update**.

See Defining operations for more information on operation settings.

Add access controls to the request

For this case, use the default _REPORT_READERS_ user class to allow users who can run reports to submit this pre-defined request. We will assume that users have been added to the user class.

To set up access controls:

1. Click the **Access control** tab.
2. Click **Select. . .** .
3. Select the _REPORT_READERS_ user class and click **Select**.

   Hitachi ID Bravura Identity warns that you need to complete the access control configuration by mapping the user class participant to a participant in the policy (requester or recipient).
4. Set the **Participant mapping** to REQUESTER.

   This allows any user in the user class to act as requester of the request.
5. Click **Update**.

See Defining access controls for more information on access control settings.

The pre-defined request is ready to use with report output.

Run the accounts report

To run a report and use the output to submit a request to enable disabled accounts:

1. Log in as a member of _REPORT_READERS_.
2. Click **Manage reports** → **Reports** → **Users** → **Account attributes**.
3. Set account attribute **@accountEnabled** to `false`.
4. Run the report.
5. Expand **Submit pre-defined requests using report output** at the bottom of the report form.
6. Select the ENABLE-ACCOUNTS pre-defined request.

7. Click on the magnifying glass icon 🔍 to configure **Attributes**.

   (a) Map the Recipient ID to a static ID, such as the user running the report.

   > **Note:** The recipient ID needs to match a *Bravura Identity* profile ID. If the report output has that information, you can map this attribute to that output, otherwise, you will need to enter a static ID.

   (b) Map the target ID and account attributes to the respective columns.

   (c) Click **Done**.

8. Click **Run for submission**.

   Hitachi ID Bravura Identity displays a summary of the requests submitted.

   You can click on the info icon 🔍 in the request status column to view the status of each request, or use the Requests link from the main menu.

See the Reports User Guide for more information on running reports.

10.4 Creating a pre-defined request

To create a pre-defined request:

1. Navigate to the ***Pre-defined request information*** page (p25).
2. Type a unique **ID** and **Description**.
3. Determine whether the pre-defined request is **Enabled** for use by end users.
4. Enable **Accessible to requesters** if you want the pre-defined request to be available to requesters outside of certification and reports.
5. Enable **Accessible from report** if you want the pre-defined request to be available in the *Manage reports* (RPT) module.
6. Enable **Accessible from certification** if you want the pre-defined request to be available for certification remediation. Enabling this will reveal the **Remediation type** option, allowing you to select which types of remediation the pre-defined request can be used for.
7. Type a **Help URL** if you want to provide a longer description for users.

   You can compose and post a web page that describes this request further, and enter its URL here. Users can open the URL by clicking the request description text wherever the text appears in the user interface.
8. Enable **Authorizer must approve/deny each entitlement** if you want the assigned authorizers to approve/deny each entitlement.
9. Determine the **Intended recipients**.

   This determines where the request can be accessed (if it is accessible to requesters) and which types of certification remediation this request will be available for (if it is accessible to certification).

   If the request is enabled, and accessible to requesters, and the intended recipients are:

- Existing users, the request is available to users via the **View and update profile** links on the main menu or, if you set the **Subject** field to "Managed groups", the request is available via the **Groups** link on the main menu (see Step 10).
- New users, the request is available to users via the **Create a new user profile** link on the main menu.
- Existing and new users, the request is available via any of the above.
- Existing groups, the request is available to users via the **Groups** link on the main menu.
- New groups,the request is available to users via the **Groups** link on the main menu.
- Non-user-based, the request is available to users via the **Use pre-defined requests for custom operations** link on the main menu.
- Network resources, the request is available to users via the **Request access to network resources** link on the main menu.
- Existing parent groups, the request is available to users via the **Groups** link on the main menu.
- Existing child groups, the request is available to users via the **Groups** link on the main menu.

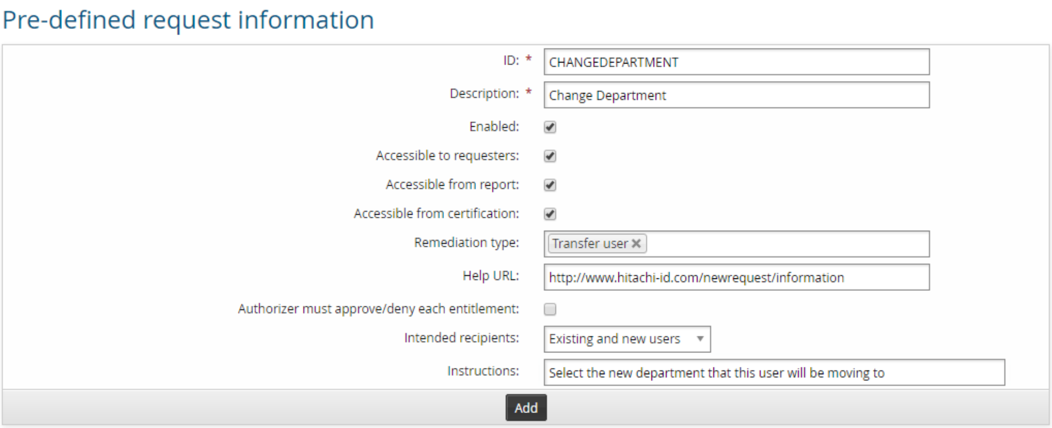
10. If the intended recipients are existing users with **Subject** set to "Managed groups", or if the intended recipients are existing groups, determine the **Applicable subject selection**.

    This controls whether the request is displayed based on how many groups are selected in the *Groups* app. Assuming the user has appropriate access to the request, "Single subject" makes the request available if exactly one group is selected. "Multiple subjects" makes the request available if two or more groups are selected.

11. Enter **Instructions** if you want to provide users with additional information.

    These instructions will be presented to users after they select the pre-defined request.

12. Click **Add**.



Pre-defined request information

ID: *	CHANGEDEPARTMENT
Description: *	Change Department
Enabled:	☑
Accessible to requesters:	☑
Accessible from report:	☑
Accessible from certification:	☑
Remediation type:	Transfer user ✕
Help URL:	http://www.hitachi-id.com/newrequest/information
Authorizer must approve/deny each entitlement:	☐
Intended recipients:	Existing and new users ▾
Instructions:	Select the new department that this user will be moving to

Next:

Define operations (p45) that are part of the pre-defined request.

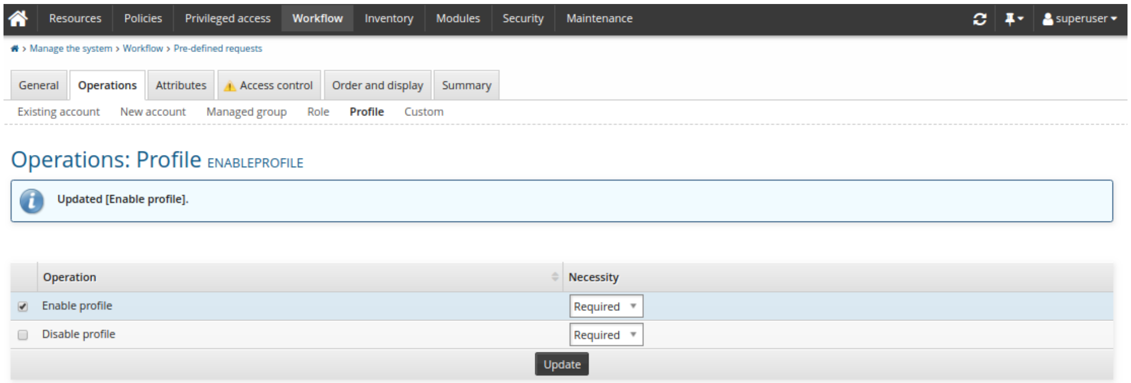
10.5 Defining operations

Select the operations to be performed on resources to define what will happen once a pre-defined request is approved.

> **Note:** If adding a resource will cause the pre-defined request to be in violation of a segregation of duties rule, adding the resource will be disallowed or its default operation will be changed to **Delete**.

To define operations for a pre-defined request:

1. Navigate to the ***Pre-defined request information*** page (p25).
2. Select the **Operations** tab.
3. Select the sub-link for:
   - **Existing account** to add operations for existing accounts.
   - **New account** to add operations to create accounts based on a template accounts.
   - **Managed group** to add operations to join, leave, or edit managed groups.
   - **Role** to add operations to add or remove roles.
   - **Profile** to add operations to enable or disable profiles.
   - **Custom** to add custom operations.
4. Define operations on specified groups, accounts, or roles, if applicable. See Operations on specified entitlements/resources.
5. Define operations on either all, or user-selected groups, accounts, or roles, if applicable. See Operations on either all or user-selected entitlements.
6. For profile operations, determine whether the enable or disable profile operation is required or optional.



Operations: Profile ENABLEPROFILE

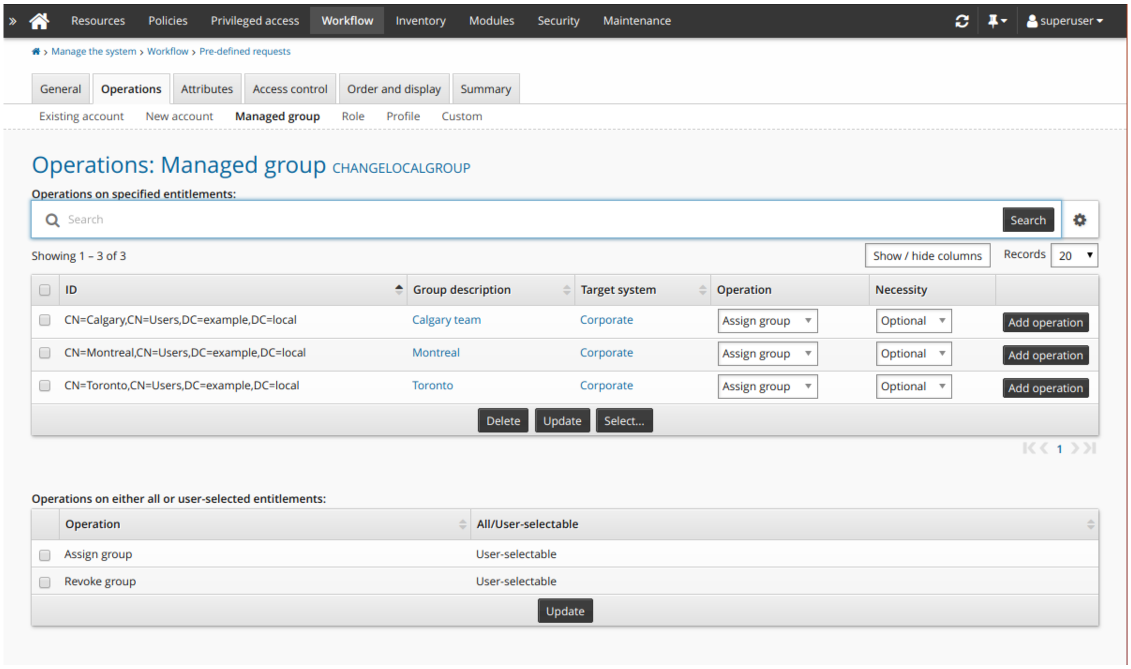
Updated [Enable profile].

	Operation	Necessity
☑	Enable profile	Required
□	Disable profile	Required

10.5.1 Operations on specified entitlements/resources

To define operations on specified groups, accounts, or roles:

1. Click **Select...** in the upper table.
2. Select one or more groups, target systems (for existing accounts), template accounts (for new accounts), or roles. Click **Select**.
3. Select an operation from the drop-down list next to the entitlement, if options are available.
4. Click **Add operation** next to an entitlement or resource to add more operations, if applicable.
5. For operations that add a group membership, account, or role, determine whether the new entitlement or resource is required or optional by selecting appropriate option in the **Necessity** column.
6. Click **Update**.



Operations: Managed group CHANGELOCALGROUP

Operations on specified entitlements:

Showing 1 – 3 of 3

ID	Group description	Target system	Operation	Necessity	
CN=Calgary,CN=Users,DC=example,DC=local	Calgary team	Corporate	Assign group	Optional	Add operation
CN=Montreal,CN=Users,DC=example,DC=local	Montreal	Corporate	Assign group	Optional	Add operation
CN=Toronto,CN=Users,DC=example,DC=local	Toronto	Corporate	Assign group	Optional	Add operation

Operations on either all or user-selected entitlements:

Operation	All/User-selectable
Assign group	User-selectable
Revoke group	User-selectable

It helps to understand how the necessity column will work if you run the pre-defined request from a report, or from the *View and update profile* (IDR) module. The table below shows the impact of the required and optional setting on the pre-defined request:

Necessity	Submitted via report output	Submitted by an end user
Required	Attributes are mapped automatically to the report output.	The operation cannot be removed from a request.
Optional	You will be prompted to map the pre-defined request attributes to the report output.	The operation is optional.

10.5.2 Operations on either all or user-selected entitlements

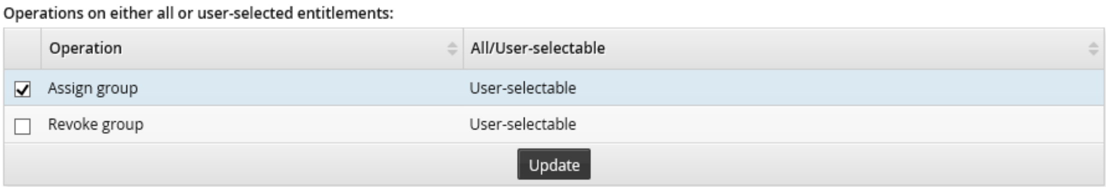
If you select an operation from the checklist in the lower table, and click **Update**, this has one of two effects, depending on whether it applies to 'All' or 'User-selectable' entitlements (not all operations have both):

- **All** means the operation will be performed on all entitlements of one type.

  Note: If 'All' is selected for update accounts, only the accounts with an account attribute mapped to the modified profile attribute will be updated.

- **User-selectable** means the operation will only be performed on entitlements selected by the requester, who can choose from all entitlements of one type.

For example, if you select "Assign group" for managed groups, users will be able to join or leave any managed group on any target system.



Operations on either all or user-selected entitlements:

	Operation	All/User-selectable
☑	Assign group	User-selectable
□	Revoke group	User-selectable

Note: There is no place in the user interface to configure authorizers for enable/disable profile operations. You must use the authorizer criteria modification plugin to add authorizers on the request or set the number of authorizations required. Enable/disable operations in requests are affected by the MIN AUTHORIZERS variable.

Next:

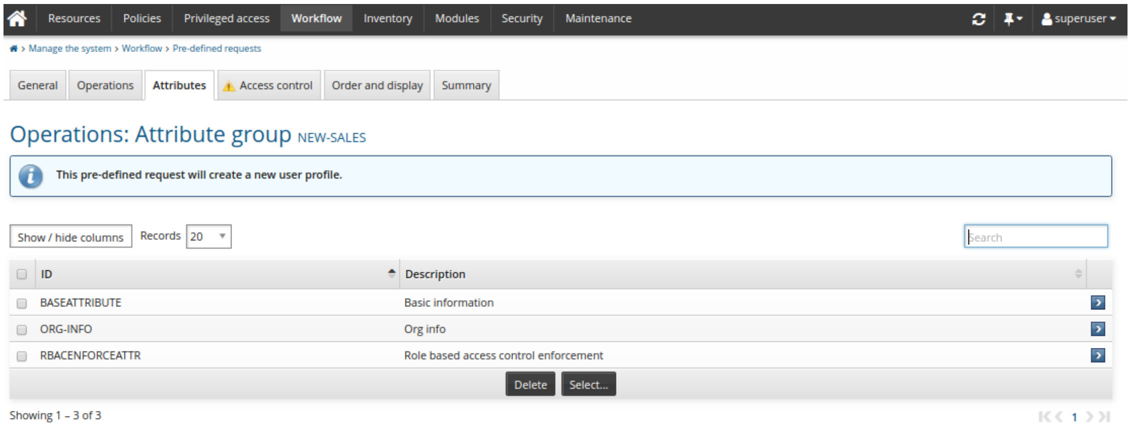
Select attributes (p48) to be displayed on the request form.

10.6 Selecting attributes for requests

Select attribute groups to determine what information needs to be gathered for a request.

To define attributes for a pre-defined request:

1. Navigate to the ***Pre-defined request information*** page (p25).
2. Select the **Attributes** tab.
3. Click **Select...**.
4. Select the attribute groups you want to add to the request and click **Select**.



Operations: Attribute group NEW-SALES

This pre-defined request will create a new user profile.

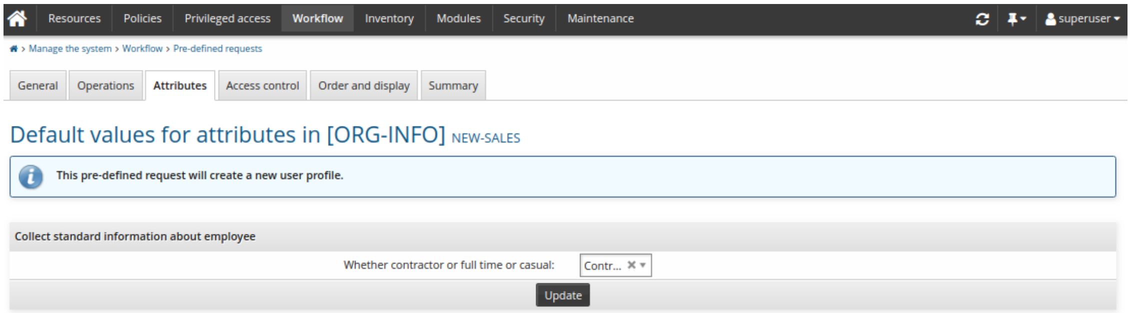
☐	ID	Description
☐	BASEATTRIBUTE	Basic information
☐	ORG-INFO	Org info
☐	RBACENFORCEATTR	Role based access control enforcement

Showing 1 – 3 of 3

10.6.1 Defining default attribute values for requests

To specify default attribute values for a request:

1. On the ***Operations: Attribute group <request>*** page, search for, or select ▶ the relevant attribute group.
2. Enter default values for attributes as required.
3. Click **Update**.



Default values for attributes in [ORG-INFO] NEW-SALES

This pre-defined request will create a new user profile.

Collect standard information about employee

Whether contractor or full time or casual: Contr...

Note: The display of attributes is controlled by attribute group permissions; for example, you can set a default value for an attribute that is neither viewable nor editable to a requester.

Next:

Add Access controls (p49) to the request.

10.7 Defining access controls

You can use user classes to create controls that determine which users have access to a pre-defined request.

To add access controls:

1. Navigate to the ***Pre-defined request information*** page (p25).
2. Select the **Access control** tab.
3. Click **Select...** to select existing classes, or **Add new...** to create a new class.
4. Configure **Participant mapping** for each user class that you add.

   Select and create user classes until you have defined control filters.
5. If your criteria includes multiple user classes, define whether users are required to match **All of the user classes** or **Any of the user classes**.

Note: When the **Intended recipients** is set to anything other than "Existing users" and/or "New users", only single participant user classes will be available, and mapping will not be required.

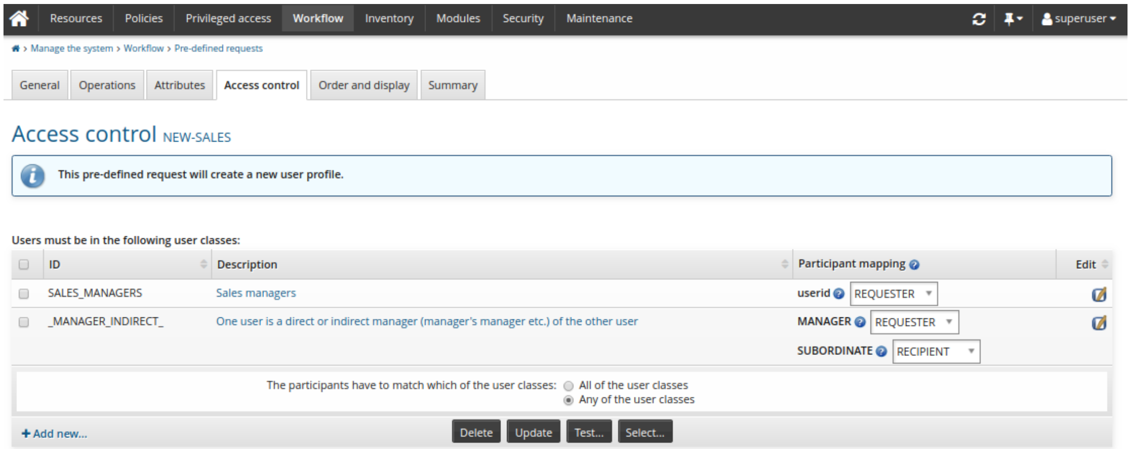
Note: Access controls do not apply to certification remediation. If the certification initiator allows it, all reviewers will be able to submit that pre-defined request for remediation.

Example

To define access control in a way that allows a manager to update the profile of his subordinate:

- Select the default "MANAGER INDIRECT" user class
- Configure the participant mapping as follows:

  MANAGER : REQUESTER
  SUBORDINATE : RECIPIENT



Access control NEW-SALES

This pre-defined request will create a new user profile.

Users must be in the following user classes:

□	ID	Description	Participant mapping	Edit
□	SALES_MANAGERS	Sales managers	userid: REQUESTER	
□	_MANAGER_INDIRECT_	One user is a direct or indirect manager (manager's manager etc.) of the other user	MANAGER: REQUESTER SUBORDINATE: RECIPIENT	

The participants have to match which of the user classes: ○ All of the user classes ● Any of the user classes

Next:

Configure the request wizard (p50).

10.8 Defining the request wizard order and display

When a user makes a request *Hitachi ID Bravura Identity* will present a *wizard*; a series of form pages which lead the user through a series of steps. This allows users to make requests without having to know the complex details of the pre-defined request.

The **Order and display** tab allows you to rearrange the order of the different pages in the pre-defined request that require user input, and you can decide to display them or not.

Pages are added to the wizard as you add operations that require user input; for example adding the "Assign group" operation adds the "Join or leave groups" page. Every attribute group added to the pre-defined request will have its own page on the wizard.

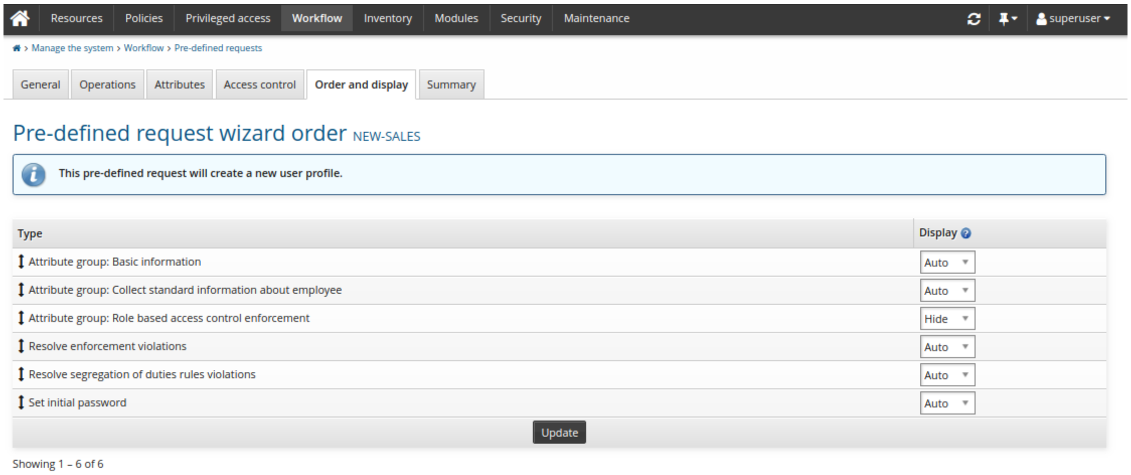
When a pre-defined request is first added, it will have the following pages by default in the given order before any operations, or attribute groups have been added:

- Resolve segregation of duties rules violations

- Set initial password
- Request summary

The **Display** column determines whether a page will be shown to the requester. All default operations are set to "Auto", which means *Bravura Identity* will decide whether to show the page depending on the requested resources so far; for example, users only need to set an initial password if the create account operation is included. Choose "Hide" when the values are provided by a plugin.

WARNING!: Misconfiguring this page can cause the pre-defined request to not function properly. Ensure you thoroughly test your changes.



Pre-defined request wizard order NEW-SALES

This pre-defined request will create a new user profile.

Type	Display
Attribute group: Basic information	Auto
Attribute group: Collect standard information about employee	Auto
Attribute group: Role based access control enforcement	Hide
Resolve enforcement violations	Auto
Resolve segregation of duties rules violations	Auto
Set initial password	Auto

Showing 1 – 6 of 6

Profile/Request Attributes 11

Profile and request attributes can play an important role during *Hitachi ID Bravura Identity* processes. A profile and request attribute can define a user object's parameters and use. In many cases, attributes and attribute values represent different roles and access privileges on target systems. Many organizations determine a user's system status by the value of some attribute. For example, the value of an attribute of `"F"` versus `"T"` may determine whether the user is disabled on a given system or not.

You can also define profile and request attributes to gather extra information about a user. For example, users may enter human resource information such as date of birth, mobile phone provider and number, or social security number.

Profile and request attributes can be defined according to the following types:

String A short alpha-numeric value

Integer An all-numeric value

Boolean A true or false value.

Memo A multi-line alpha-numeric value

Password A value hidden from view. *Bravura Identity* obscures user input with asterisk (*) or other characters.

This type of profile and request attribute can be mapped to character or numerical account attributes only.

Date/time Users select a date/time in one of the three following formats:

- year/month/day (YYYY/MM/DD)
- year/month/day hour:minute (YYYY/MM/DD hh:mm)
- year month day (YYYY <*month*> DD), where <*month*> is spelled out

Note: Attributes of type "Date/time" cannot accept values predating 1970.

User A user profile. A valid profile ID entered into this attribute will be displayed as a clickable user object on read-only pages.

Link An external link to a web page or image; for example a personal web page or photo ID. When the link is read-only, users can click on it to open a window or tab in the browser. Hover your cursor over an image link for a preview of the image.

File Users can attach a file to their profile or request. Various file extensions are supported.

The default maximum file size is 1000KB, which can be set using the **MAX UPLOAD FILE SIZE** system variable in the **Manage the system** → **Workflow** → **Options** menu.

Target system A target system. Users can search for the ID of the target system. A valid discovered system ID entered into this attribute will be displayed as a clickable target system object on read-only pages.

Managed system A managed system, for privileged access management. Users can type, or search for, the ID of the managed system. A valid managed system ID entered into this attribute will be displayed as a clickable managed system object on read-only pages.

Discovered system An unmanaged discovered system. Users can search for the ID of the discovered system. A valid discovered system ID entered into this attribute will be displayed as a clickable discovered system object on read-only pages.

Manageable account A managed or unmanaged account. Users can search for the ID of the manageable account. A valid account ID entered into this attribute will be displayed as a clickable account object on read-only pages.

The following provides an example for adding a profile and request attribute:

1. Click **Manage the system** → **Workflow** → **Profile and request attributes** → **Profile and request attributes**.
2. Click **Add new. . .** .
3. Type an **ID**, and the **Description** that users will see.
4. Select a **Type**.

   Bravura Identity refreshes the page and displays settings according to the type you selected. If JavaScript is not enabled for your browser, you must click **Add** to allow the page to refresh.
5. Set parameters according to attribute type.

   For example:

   - To add a string-type attribute for "Date of birth", configure:

     Description of input values: type `YYYY/MM/DD` as a description to be displayed to users to show them how to enter values for this attribute.

     Format requirement of input values: type `NNNN/NN/NN` to indicate a series of numbers, which must be separated by forward slashes. Using only "N" formatting ensures that alphabetic characters will not be accepted, only numeric.
   - To add a string-type attribute for "Employee type" that requires users to select from set values:

     Minimum required number of values Type `1` to ensure the value is set for all users.

     Maximum allowed number of values Type `1` to ensure that users can belong to only one type.

     Allow this attribute to be sent in emails so that information is included in notifications about requests.

     Plugin used to generate a list of restricted values Leave this field blank to define restricted values manually (see below on the following page).
6. Click **Add**.

Defining restricted values manually

For the "Employee type" example above, *Hitachi ID Bravura Identity* adds a **Restricted values** section to bottom of the page when you click **Add**. To define the values that users must choose from:

1. Click **More** twice to add three sets of values, where the **Actual value** is recorded and the **Displayed value** is shown to users.
2. Define the restricted values; for example:

   Actual value Employee **Displayed value** Employee

   Actual value Contractor **Displayed value** Contractor

   Actual value Temporary **Displayed value** Temporary
3. Click **Update** when you have added all values.

The displayed values will appear in a drop-down list in the **Default values for the attribute**. Setting this parameter will mean that if users do not make a selection, the attribute will automatically be set to this value.

See the *Bravura Security Fabric* Documentation for more information.

Next:

Include the attribute in an attribute group to configure access controls and display properties. See Attribute Groups.

Attribute Groups 12

An *attribute group* is a named collection of *profile and request attributes*. *Hitachi ID Bravura Identity* uses attribute groups to determine:

- Who can see or edit certain attribute values (access controls).
- How attributes are displayed to users.

You assign permissions to *user groups*, called *access controls*, which control their members' read and write access to attribute groups, and therefore the attributes within each group. An individual user's access is determined by his or her membership in one or more user groups.

The following provides an example for creating an attribute group:

1. Click **Manage the system** → **Workflow** → **Attribute groups**.
2. Click **Add new...**.
3. Type a unique **ID** and **Description**.
4. Set rules for validation enforcement:
   - **Enforce validation when creating new accounts** – Enable this if new account requests can only proceed if correctly formatted values are entered for this attribute group.
   - **Validation behavior when updating existing accounts** – Determine whether *Bravura Identity* should always validate values for this attribute group before proceeding with a request, or only if the values have been modified.
5. Click **Add**.
6. Click the **Members** tab.
7. Click **Select** to see a list of all attributes.
8. Search for, or select the checkboxes next to the attributes you want to include.
9. Click **Select**.
10. Click the **Access control** tab.
11. Select **Read** and **Write** checkboxes as required.
12. Click **Update**.
13. Click the **Display criteria** tab.
14. Determine the **Display type**. Select:

- **Main** – to display the group and its attributes on the main request or profile page.
- **Subsidiary** – to display the group’s attributes on a subsidiary page.
- **None** – to hide the group and its attributes from users.

15. Select the operations for which the attributes are displayed.
16. If there is more than one attribute in the group, type a number in the **Relative order value** field next to each attribute to indicate the order in which they are listed. Attributes with lower numbers are listed first.
17. Click **Update**.

Part III

USING IDENTITY MANAGER

Viewing / Updating Profiles 13

Hitachi ID Bravura Identity provides you with a means to manage your own profile and resources, and the profile of other users.

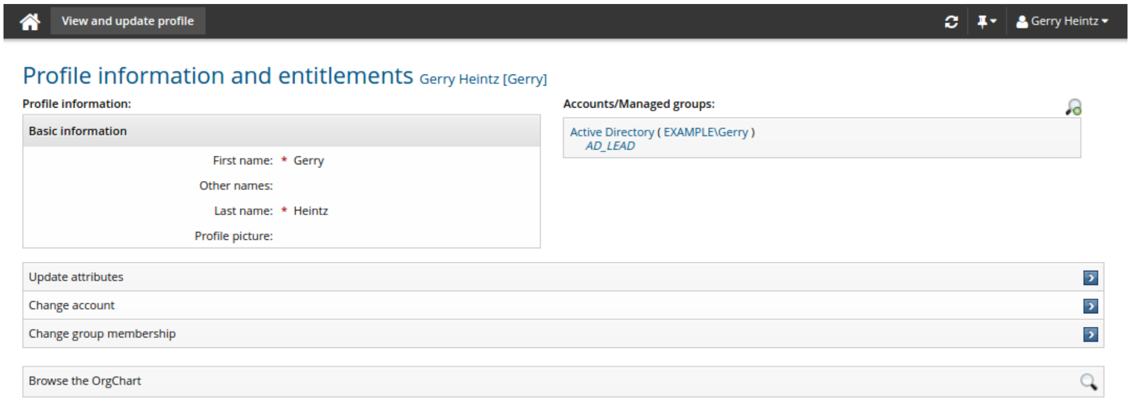
13.1 Getting started

From the main menu , click **View and update profile** under:

- **My profile** to view or update your own profile.
- **Other users** to select another existing user to view or update.

Depending on configuration and your permissions, *Hitachi ID Bravura Identity* displays profile information and a menu of pre-defined requests, which are set up by *Bravura Identity* administrators and use a simplified wizard form.

> **Note:** The operations that you are allowed to carry out on another user's profile are controlled by an operation filter. By default, the only operation that regular users can perform for other users is to request new resources.



View and update profile | Gerry Heintz

Profile information and entitlements Gerry Heintz [Gerry]

Profile information:

Basic information

First name: * Gerry
Other names:
Last name: * Heintz
Profile picture:

Accounts/Managed groups:

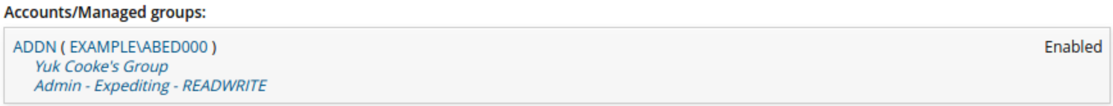
Active Directory (EXAMPLE\Gerry)
AD_LEAD

Update attributes
Change account
Change group membership

Browse the OrgChart

Account status

You can also view account status by clicking the "Account status" icon, provided you have required permissions ("View account"). The status will be displayed next to the account.



Accounts/Managed groups:

ADDN (EXAMPLE\ABED000) Enabled

Yuk Cooke's Group

Admin - Expediting - READWRITE

13.2 Updating profile information

Hitachi ID Bravura Identity uses *profile and request attributes* to help define requested resources and to collect information about you. Attributes are grouped for organizational purposes and to determine who can read or write the information.

Bravura Identity can be configured with other customized groups of attributes listed on the ***View and update profile*** page and other request forms.

You can update profile information provided you have write permissions for profile attributes.

Note the following:

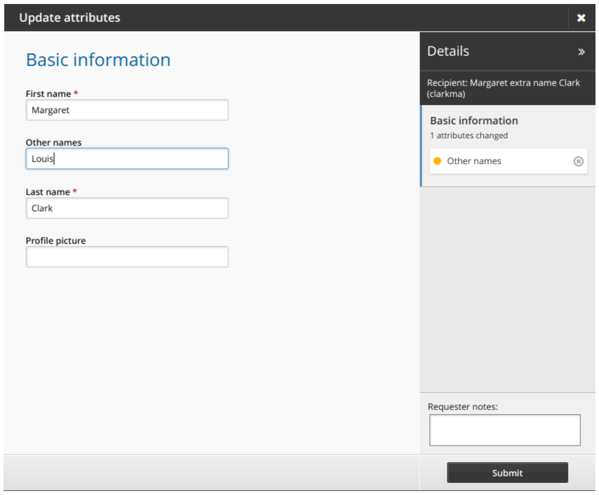
- If an attribute field allows multiple values, you can click the More icon ⊕ or button until the configured maximum number of values has been entered.
- If you do not enter values for all required attributes (marked with a red asterisk), *Bravura Identity* will return an error.
- If a field has been filled with a default value, this value will be included unless you change it. This applies to both required and optional values.
- You may be required to confirm a value by re-typing it in a second text box. For example, some password-type attributes "hide" the value as you type.

13.2.1 Use case: Update attributes

The following procedure describes how to update profile information using the standard **Update attributes** request. Details may vary according to configuration. To update profile information:

1. Navigate to the ***Profile information and entitlements*** page (p58).
2. Click **Update attributes** in the requests section.

   Hitachi ID Bravura Identity displays the request wizard.



Basic information

First name *
Margaret

Other names
Louis

Last name *
Clark

Profile picture

Recipient: Margaret extra name Clark (clarkma)

Basic information
1 attributes changed
● Other names

Requester notes:

3. Make changes as required.

   Click **Next** if available to proceed through attribute group pages.

4. If required, select accounts that you want to update.

   If an account selection page is not present, *Bravura Identity* updates all accounts attached to your profile.

5. Click **Submit**.

   Relevant authorizers are notified to review the request if necessary. See Tracking Requests to learn how to track your request.

13.3 Resolving SoD rule violations

When requesting resources, your request might violate a segregation of duties (SoD) rule, which is a security rule designed to ensure that users do not have too much access to certain restricted entitlements. An error is displayed when a request violates an SoD rule.

You must resolve the violation by:

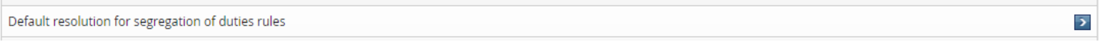
- Requesting an exception to the rule, or
- Removing entitlements from the request

If an exception is approved, the SoD rule will be ignored, and the requested entitlements will be assigned to you.

If an outstanding request conflicts with a new request, you will not be able to submit the request. The outstanding request needs to be completed, canceled or denied before an exception to the SoD rule can be requested.

If a user already had the conflicting entitlements before the SoD rule was created, the violations can be resolved via a user's ***Profile information and entitlements*** page (p58). The standard built-in request is

Default resolution for segregation of duties rules, which navigates to an SoD wizard page where all pre-existing SoD violations are listed.



Default resolution for segregation of duties rules

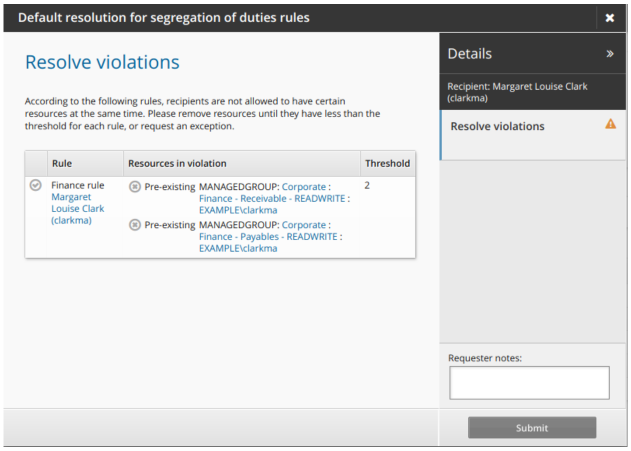
The link may be available from other users' profile pages depending on access controls for the built-in pre-defined request (PDR) _RESOLVE_SOD_VIOLATIONS_.

> **Note:** When a request causes new SoD violations, the SoD wizard page will present before submitting the request. All unresolved SoD violations including existing ones are listed on that page.

13.3.1 Use case: Group membership change causing rule violation

The following procedure describes how to request an exception to a rule where a request for group memberships would cause the recipient to be in violation.

If exceptions are allowed, *Hitachi ID Bravura Identity* adds a wizard page to ***Resolve violations***.



Default resolution for segregation of duties rules

Resolve violations

According to the following rules, recipients are not allowed to have certain resources at the same time. Please remove resources until they have less than the threshold for each rule, or request an exception.

	Rule	Resources in violation	Threshold
✓	Finance rule Margaret Louise Clark (clarkma)	⊗ Pre-existing MANAGEDGROUP: Corporate : Finance - Receivable - READWRITE : EXAMPLE\clarkma ⊗ Pre-existing MANAGEDGROUP: Corporate : Finance - Payables - READWRITE : EXAMPLE\clarkma	2

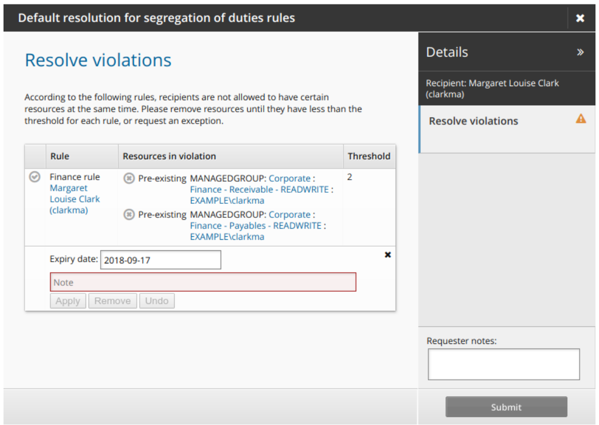
Details

Recipient: Margaret Louise Clark (clarkma)

Resolve violations ⚠

Requester notes:

1. Click the request exception icon ✓ to submit a request to allow the user to keep the conflicting entitlements.



Default resolution for segregation of duties rules

Resolve violations

According to the following rules, recipients are not allowed to have certain resources at the same time. Please remove resources until they have less than the threshold for each rule, or request an exception.

	Rule	Resources in violation	Threshold
○	Finance rule Margaret Louise Clark (clarkma)	Pre-existing MANAGEDGROUP: Corporate : Finance - Receivable - READWRITE : EXAMPLE\clarkma Pre-existing MANAGEDGROUP: Corporate : Finance - Payables - READWRITE : EXAMPLE\clarkma	2

Expiry date: 2018-09-17

Details

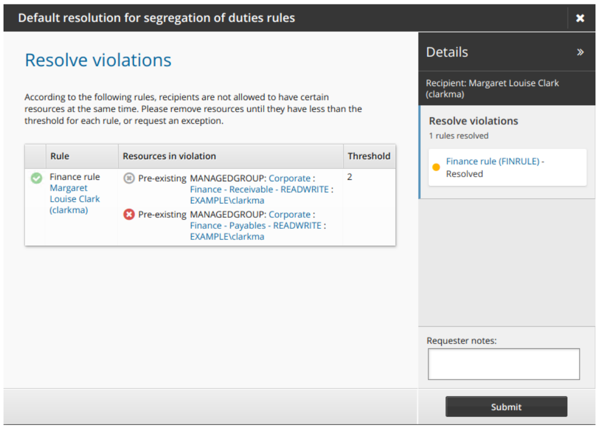
Recipient: Margaret Louise Clark (clarkma)

Resolve violations

Requester notes:

Type a reason for the exception and modify the expiry date if necessary, then click **Apply**.

2. Alternatively, click the revoke icon ⊗ to remove one of the conflicting entitlements.



Default resolution for segregation of duties rules

Resolve violations

According to the following rules, recipients are not allowed to have certain resources at the same time. Please remove resources until they have less than the threshold for each rule, or request an exception.

	Rule	Resources in violation	Threshold
✓	Finance rule Margaret Louise Clark (clarkma)	Pre-existing MANAGEDGROUP: Corporate : Finance - Receivable - READWRITE : EXAMPLE\clarkma ☒ Pre-existing MANAGEDGROUP: Corporate : Finance - Payables - READWRITE : EXAMPLE\clarkma	2

Details

Recipient: Margaret Louise Clark (clarkma)

Resolve violations

1 rules resolved

● Finance rule (FINRULE) - Resolved

Requester notes:

3. Click **Submit**.

   Relevant authorizers are notified to review the request if necessary. See Tracking Requests to learn how to track your request.

Note: When you remove a resource from a user's profile, it is permanently deleted.

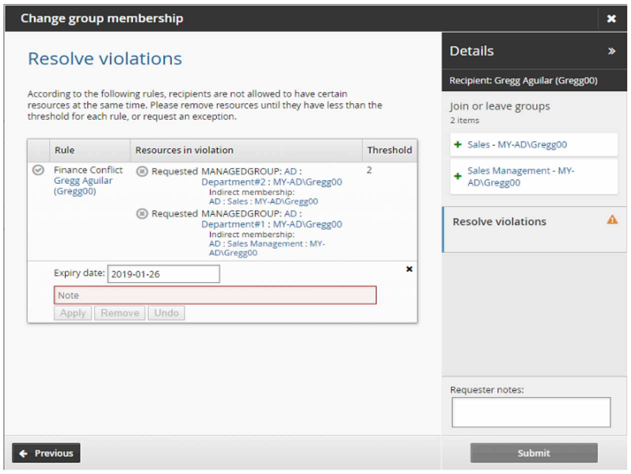
13.3.2 Use case: Indirect group membership change causing rule violation

Some target systems support the concept of a *nested group*. A nested group is a group that is a member of another group. For example, in Active Directory you can add a group as a member of another group. The *nested group* then inherits the rights of the *parent group*.

Hitachi ID Bravura Identity also calls these groups *parent groups* and *child groups*. If an account is a member of a child group, they have what is called *indirect membership* to the parent group.

When requesting resources that have nested groups, your request might violate a SoD rule wapplied to a nested resource.

The main procedure on how to request an exception for a rule remains the same for indirect groups, except that **Indirect membership** details are displayed on the *Bravura Identity* wizard page.



Change group membership

Resolve violations

According to the following rules, recipients are not allowed to have certain resources at the same time. Please remove resources until they have less than the threshold for each rule, or request an exception.

	Rule	Resources in violation	Threshold
	Finance Conflict Gregg Aguilar (Gregg00)	Requested MANAGEDGROUP: AD : Department#2 : MY-AD\Gregg00 Indirect membership: AD : Sales : MY-AD\Gregg00 Requested MANAGEDGROUP: AD : Department#1 : MY-AD\Gregg00 Indirect membership: AD : Sales Management : MY-AD\Gregg00	2

Expiry date: 2019-01-26

Note

Details

Recipient: Gregg Aguilar (Gregg00)

Join or leave groups

2 items

- Sales - MY-AD\Gregg00
- Sales Management - MY-AD\Gregg00

Resolve violations

Requester notes:

Creating a New User 14

This chapter shows you how to create a new user and request resources for them using the self-service workflow feature.

> **Note:** The layout and content of the forms can vary from the way it is described and illustrated here.

There are two basic ways to create a new user:

- A pre-defined request.

  Hitachi ID Bravura Identity administrators can set up pre-defined requests to create new user profiles for different purposes. *Bravura Identity* displays a sequence of form pages depending on the requirements for the new profile.

  See Use case: Create a new user from a pre-defined request.

- Copy entitlements from an existing user.

  This type of request allows you to create a new user profile by copying the desired attributes of an existing user.

  See Copying entitlements from an existing user.

14.1 Use case: Create a new user from a pre-defined request

The following example creates a new profile using a pre-defined request, to hire a new sales representative.

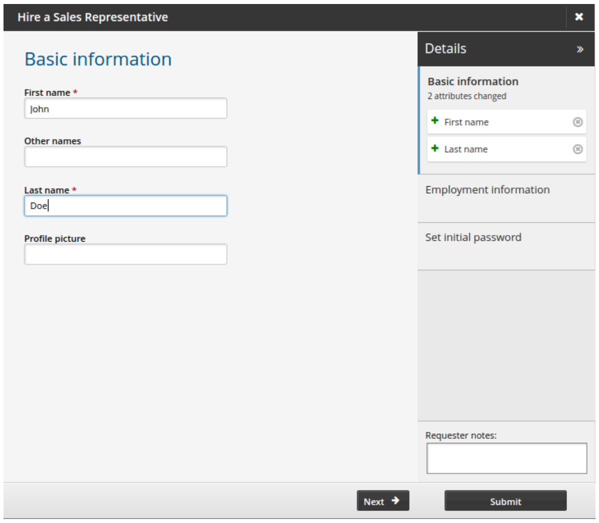
To submit the pre-defined request, login as an end user:

1. From the main menu , click **Create a new user profile** .

   If your administrator has set up pre-defined requests, *Hitachi ID Bravura Identity* displays a menu of request types.

2. Click **Hire a Sales Representative**.

3. Enter basic profile information.

   Hire a Sales Representative

   Basic information

   First name * John

   Other names

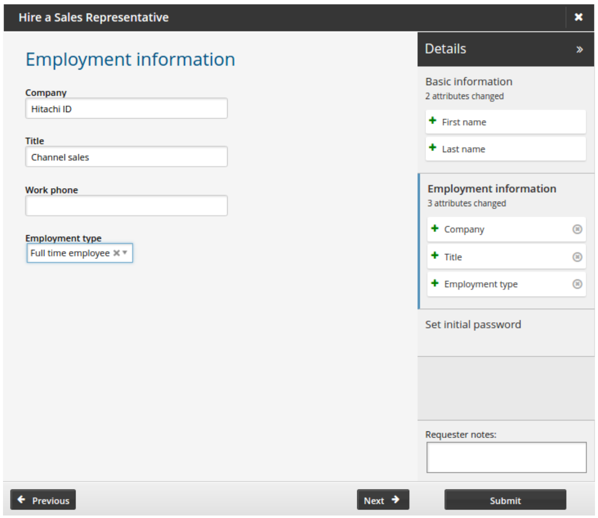
   Last name * Doe

   Profile picture

   Click **Next**.

4. Enter employment information.

   This is information defined by the ORG-INFO attribute group.



Employment information

Company: Hitachi ID

Title: Channel sales

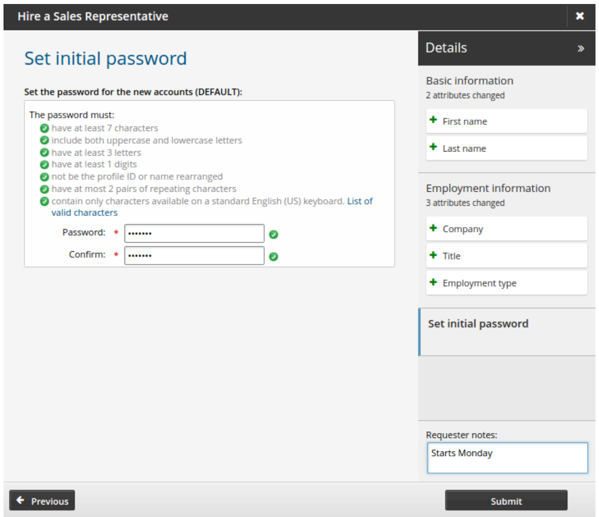
Work phone:

Employment type: Full time employee

Requester notes:

Click **Next**.

5. Set the initial password as required for new accounts.



Set initial password

Set the password for the new accounts (DEFAULT):

The password must:
- ✓ have at least 7 characters
- ✓ include both uppercase and lowercase letters
- ✓ have at least 3 letters
- ✓ have at least 1 digits
- ✓ not be the profile ID or name rearranged
- ✓ have at most 2 pairs of repeating characters
- ✓ contain only characters available on a standard English (US) keyboard. List of valid characters

Password: * ••••••• ✓

Confirm: * ••••••• ✓

Requester notes: Starts Monday

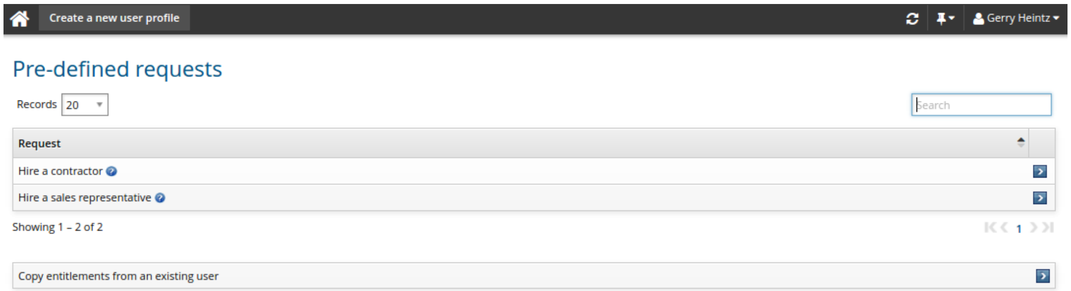
6. Click **Submit**.

14.2 Copying entitlements from an existing user

You can create a new user profile by copying entitlements from an existing user, provided that you meet criteria set by profile comparison rules.

To model a profile after another user:

1. From the main menu , click **Create a new user profile**.



Pre-defined requests

Records 20

Search

Request
Hire a contractor
Hire a sales representative

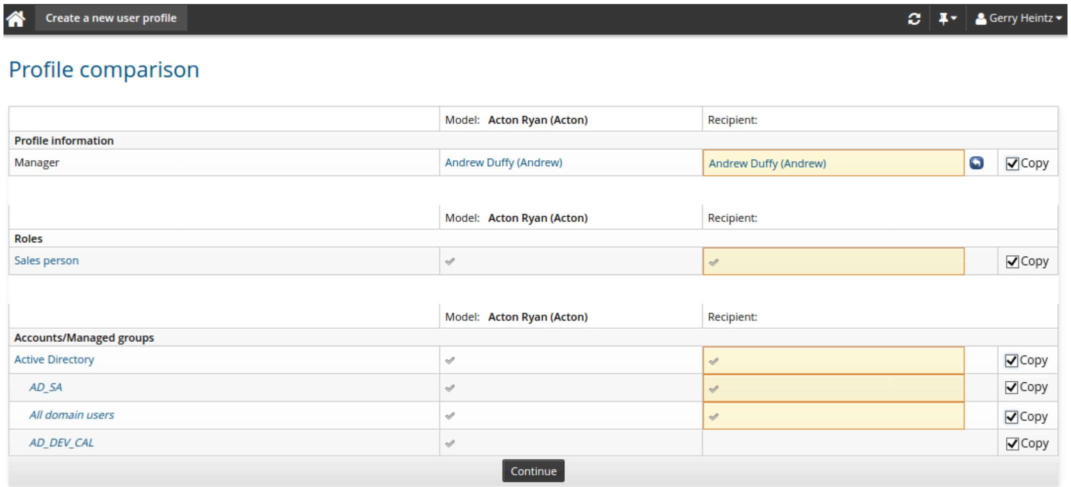
Showing 1 – 2 of 2

Copy entitlements from an existing user

2. Click **Copy entitlements from an existing user**.
3. Select the user you want to use as model user.

   The profile comparison page is displayed along with attributes that are configured to be used on comparison pages.

   Depending on your permissions, you can copy the attributes, roles, accounts and group membership.



Profile comparison

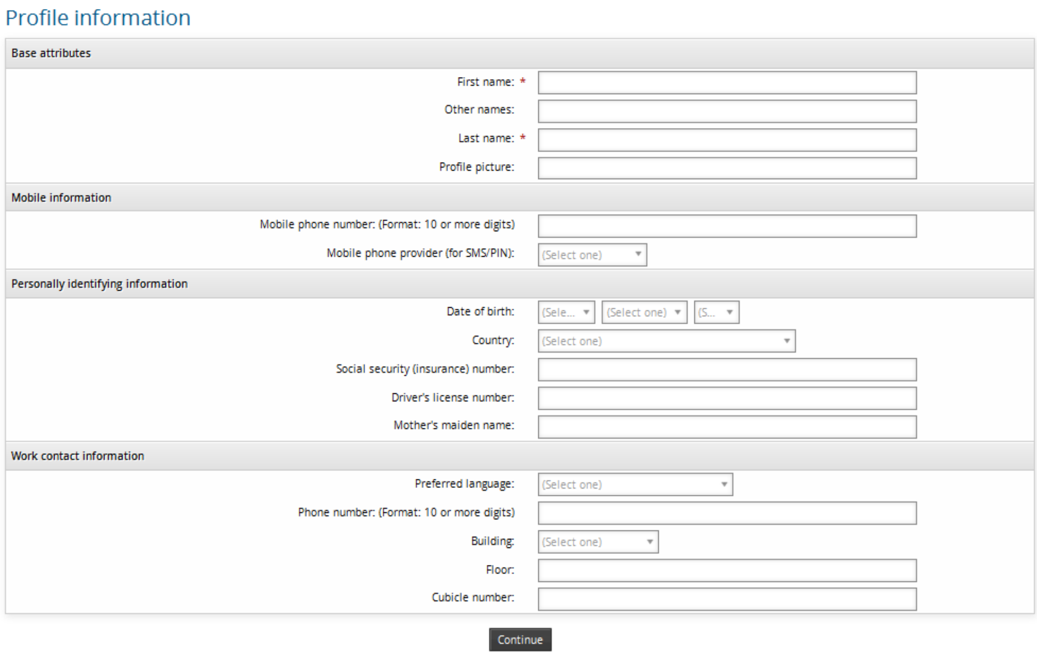
	Model: Acton Ryan (Acton)	Recipient:	
Profile information			
Manager	Andrew Duffy (Andrew)	Andrew Duffy (Andrew)	☑Copy
	Model: Acton Ryan (Acton)	Recipient:	
Roles			
Sales person	✓	✓	☑Copy
	Model: Acton Ryan (Acton)	Recipient:	
Accounts/Managed groups			
Active Directory	✓	✓	☑Copy
AD_SA	✓	✓	☑Copy
All domain users	✓	✓	☑Copy
AD_DEV_CAL	✓		☑Copy

4. Once you have selected which items to copy, click **Continue**.

> **Note:** If you copied attributes or entitlements in the previous step, you do not have to specify them in the following forms.

5. Enter values for attribute fields as required.

   There may be one or more forms for personal information.



Profile information

Base attributes

First name: *

Other names:

Last name: *

Profile picture:

Mobile information

Mobile phone number: (Format: 10 or more digits)

Mobile phone provider (for SMS/PIN): (Select one)

Personally identifying information

Date of birth: (Sele... (Select one) (S...

Country: (Select one)

Social security (insurance) number:

Driver's license number:

Mother's maiden name:

Work contact information

Preferred language: (Select one)

Phone number: (Format: 10 or more digits)

Building: (Select one)

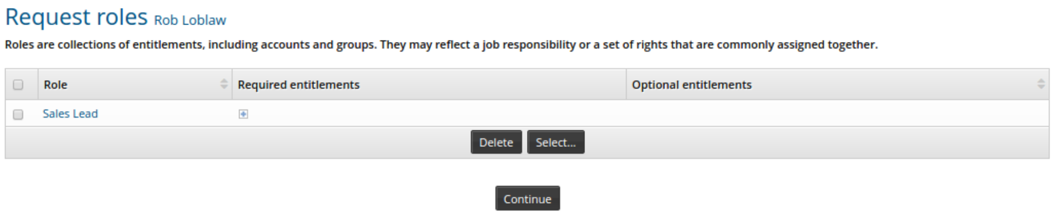
Floor:

Cubicle number:

   Click **Continue**.

6. Optional: Select additional roles.

   Click **Continue**.

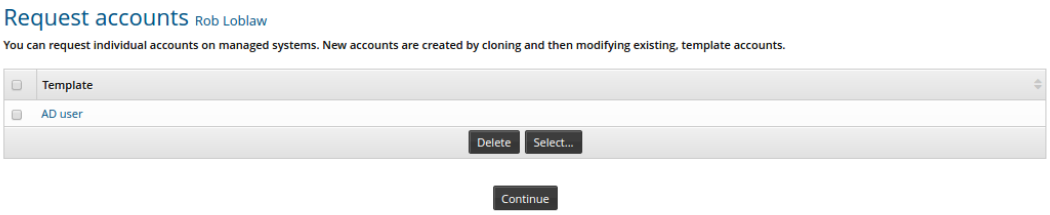


Request roles Rob Loblaw

Roles are collections of entitlements, including accounts and groups. They may reflect a job responsibility or a set of rights that are commonly assigned together.

☐	Role	Required entitlements	Optional entitlements
☐	Sales Lead	⊞	

7. Optional: Select additional template accounts to copy for the new user.



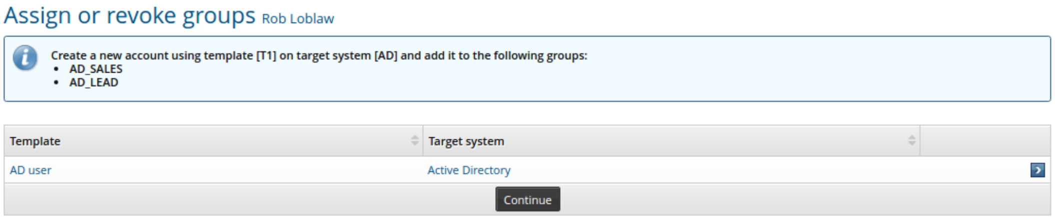
Request accounts Rob Loblaw

You can request individual accounts on managed systems. New accounts are created by cloning and then modifying existing, template accounts.

☐	Template
☐	AD user

   Click **Continue**.

8. Optional: modify the managed groups to join/leave.



Assign or revoke groups Rob Loblaw

Create a new account using template [T1] on target system [AD] and add it to the following groups:
- AD_SALES
- AD_LEAD

Template	Target system	
AD user	Active Directory	▶

   (a) Select ▶ the account for which you want to manage group membership.
   (b) Enable/disable the checkboxes for the groups which you want to change in the request
   (c) Click **Select**.
   (d) Repeat steps 8a to 8c for each account for which you want to manage group membership.
   (e) Click **Continue**.

> **Note:** From this point, *Bravura Identity* displays an error message if you select items that conflict with role enforcement or SoD rules. See Resolving SoD rule violations to learn more.

9. If one or more of the accounts requires a password, type an initial password in the **Password** and **Confirm** fields.

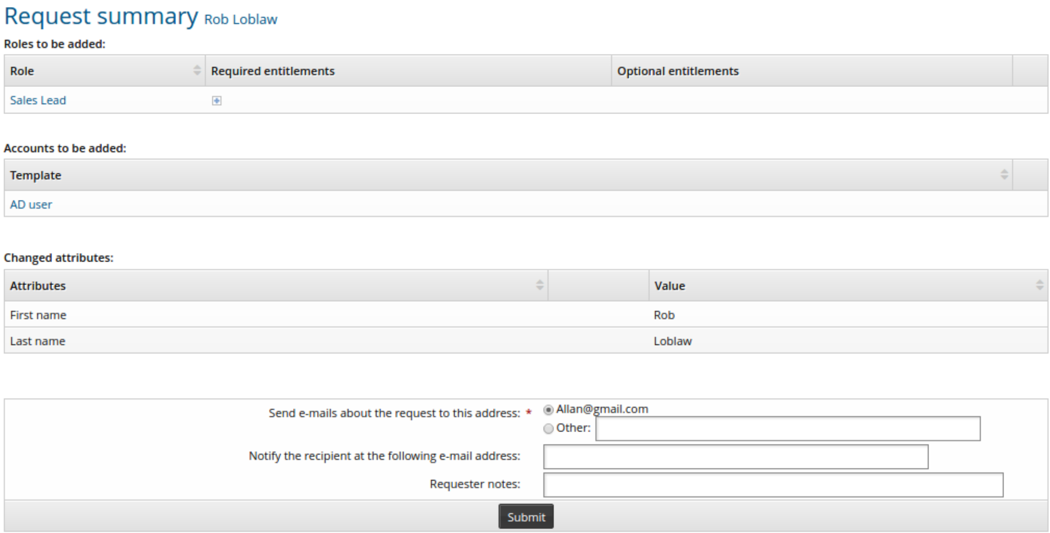
   Bravura Identity provides a list of correctly formatted passwords as suggestions in the drop-down list.

   Click **Continue**.

10. Define request notification information.

    Click **Continue**.

11. Review the request summary.



Request summary Rob Loblaw

Roles to be added:

Role	Required entitlements	Optional entitlements
Sales Lead	⊞	

Accounts to be added:

Template
AD user

Changed attributes:

Attributes	Value
First name	Rob
Last name	Loblaw

Send e-mails about the request to this address: * ● Allan@gmail.com ○ Other:

Notify the recipient at the following e-mail address:

Requester notes:

Click **Submit**.

Tracking Requests 15

This chapter describes how users can view, cancel, or access requests using the *Requests* app.

Terminology

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, abstain or change a request depending on their privileges.

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

Workflow manager A user who can act on individual authorization requests of other users.

Delegation manager An authorizer who can delegate the responsibilities of a user to another user.

Who can view and cancel requests

Requesters and recipients can track the status of their own active requests. Depending on access rules configured by a *Hitachi ID Bravura Identity* administrator, users may be able to view their own archived requests. Help desk users may be able to view all open requests.

By default, requesters can cancel their own requests before they are authorized, and recipients can view and cancel requests that apply to them as long as the requests are not termination requests.

If an update or account creation is scheduled to start in the future, requesters and recipients can also cancel the request. You can also cancel approved updates or account creations that are scheduled to start in the future.

Navigation

When you make a request, you can use the link displayed at the final step to access the *Requests* app, where you can track the status of your request.

Later, you can access the *Requests* app page by clicking the **Requests** option on the main menu.

For general information about using *Hitachi ID Bravura Identity* applications see Using Apps in the Bravura Security Fabric *Self-Service and Help Desk User Guide*

Prerequisites

The *Requests* app is accessible via the **Requests** link to:

- Users with accounts when they have the "Requests" user access rule (all self-service users by default)

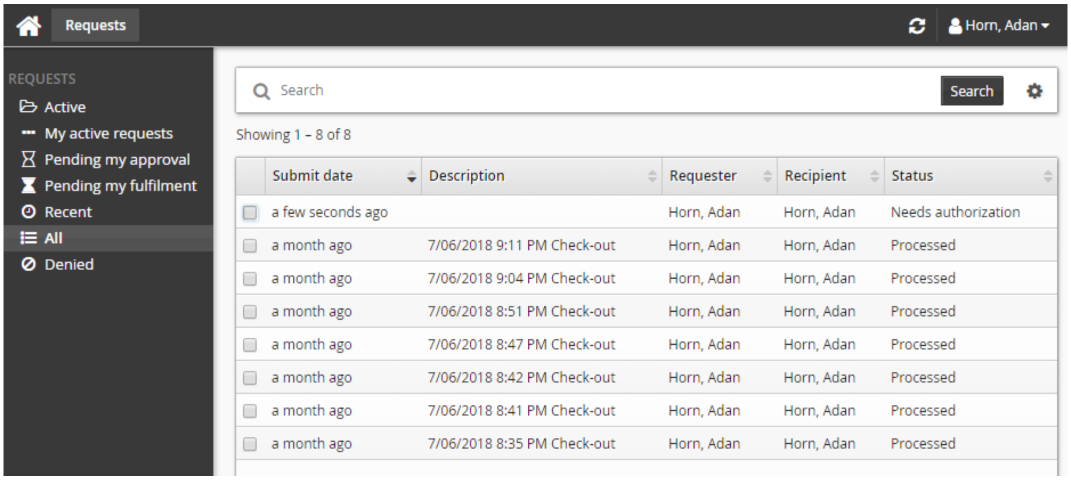
- Product administrators who have the "Manage reports" user access rule. Users with this right can view requests they have submitted via reports.
- Help desk users with the "View workflow requests" user access rule. These users can view other users' authorization requests.
- Workflow managers with the "Manage workflow requests" rule. These users can manage other users' authorization requests.
- Delegation managers with the "Delegate workflow requests" user access rule. These users can delegate other users' authorization requests.

15.1 Tracking and updating requests

To check the status, cancel, or escalate a request:

1. From the main menu , click **Requests**.

   By default, the app shows your active requests in the Results panel.

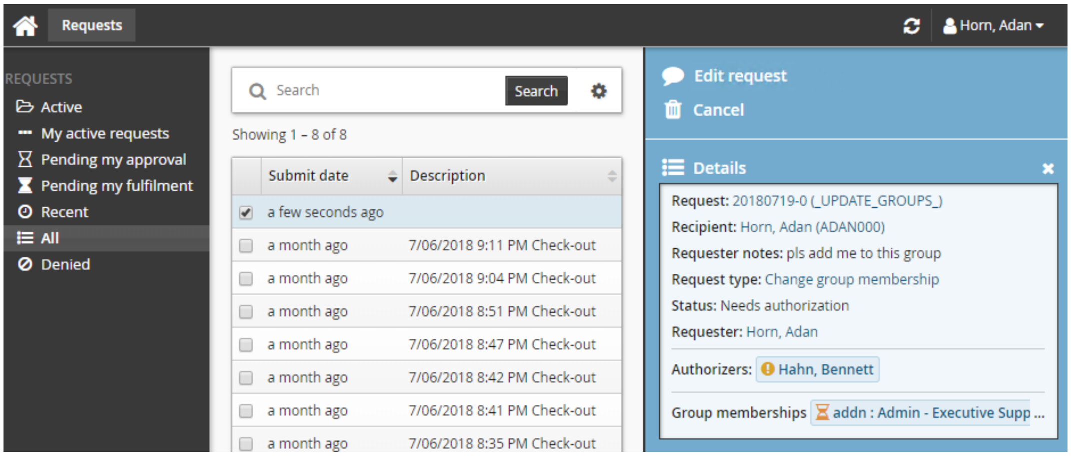


Showing 1 – 8 of 8

	Submit date	Description	Requester	Recipient	Status
☐	a few seconds ago		Horn, Adan	Horn, Adan	Needs authorization
☐	a month ago	7/06/2018 9:11 PM Check-out	Horn, Adan	Horn, Adan	Processed
☐	a month ago	7/06/2018 9:04 PM Check-out	Horn, Adan	Horn, Adan	Processed
☐	a month ago	7/06/2018 8:51 PM Check-out	Horn, Adan	Horn, Adan	Processed
☐	a month ago	7/06/2018 8:47 PM Check-out	Horn, Adan	Horn, Adan	Processed
☐	a month ago	7/06/2018 8:42 PM Check-out	Horn, Adan	Horn, Adan	Processed
☐	a month ago	7/06/2018 8:41 PM Check-out	Horn, Adan	Horn, Adan	Processed
☐	a month ago	7/06/2018 8:35 PM Check-out	Horn, Adan	Horn, Adan	Processed

   You can use the links in the Filter panel to view other requests. For example, click **All** to view all of your requests.

2. Select a request from the Results panel to view the details in the Actions panel.



Showing 1 – 8 of 8

	Submit date	Description
☑	a few seconds ago	
□	a month ago	7/06/2018 9:11 PM Check-out
□	a month ago	7/06/2018 9:04 PM Check-out
□	a month ago	7/06/2018 8:51 PM Check-out
□	a month ago	7/06/2018 8:47 PM Check-out
□	a month ago	7/06/2018 8:42 PM Check-out
□	a month ago	7/06/2018 8:41 PM Check-out
□	a month ago	7/06/2018 8:35 PM Check-out

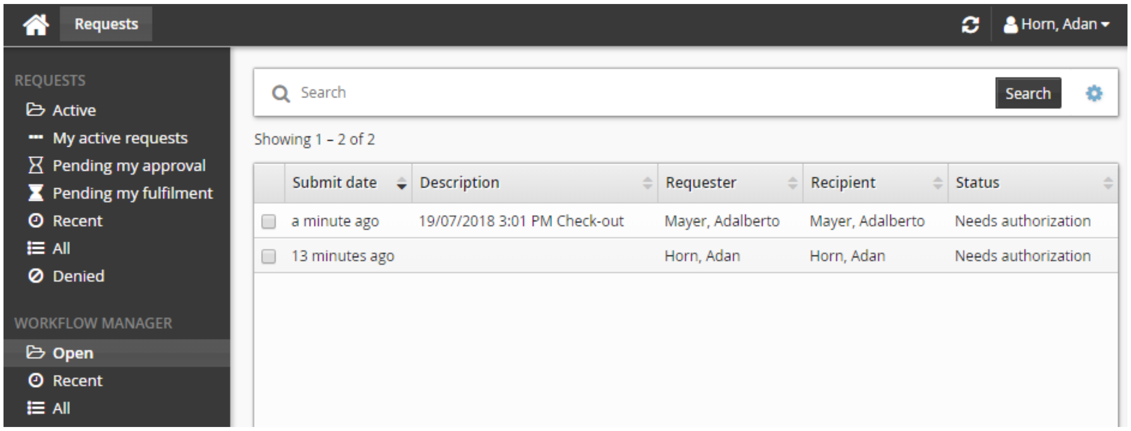
Request: 20180719-0 (_UPDATE_GROUPS_)
Recipient: Horn, Adan (ADAN000)
Requester notes: pls add me to this group
Request type: Change group membership
Status: Needs authorization
Requester: Horn, Adan
Authorizers: Hahn, Bennett
Group memberships addn : Admin - Executive Supp ...

3. In the Actions panel you can:

   - View details, including the status and authorizers for your request.
   - Cancel a request that has not begun processing, by clicking **Cancel**.
   - Click **Escalate now** (if available) to escalate a request to another authorizer if the original authorizer has not responded.
   - Click **Edit request** to edit requests that include attribute changes. See Updating attributes and entitlements for more information.

15.1.1 Tracking other users' requests

If you have the "View workflow requests" privilege, you can view other users' authorization requests under the **OTHER REQUESTS** heading. If you have the "Manage workflow requests" privilege, you can view other users' authorization requests under the **WORKFLOW MANAGER** heading.



Showing 1 – 2 of 2

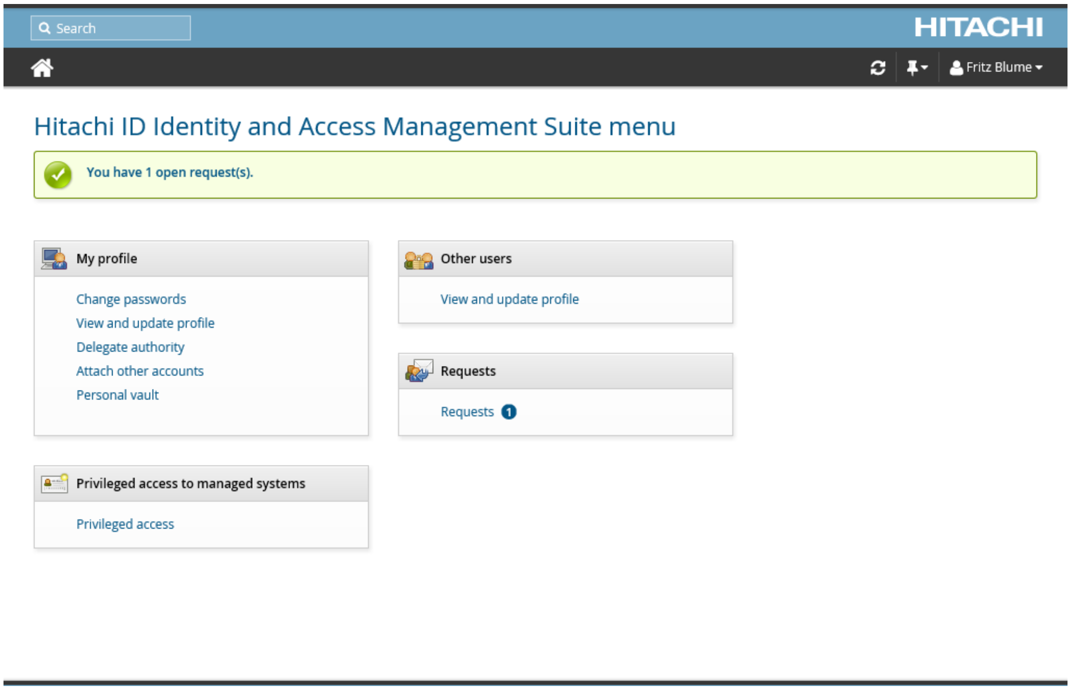
	Submit date	Description	Requester	Recipient	Status
□	a minute ago	19/07/2018 3:01 PM Check-out	Mayer, Adalberto	Mayer, Adalberto	Needs authorization
□	13 minutes ago		Horn, Adan	Horn, Adan	Needs authorization

You must have the "Manage workflow requests" privilege to be able to act on other usrs' authorization requests. See Reviewing requests for more information.

15.2 Example: Tracking and canceling a request

This example demonstrates the typical workflow for a regular user who wants to check the status of a request and then cancel it:

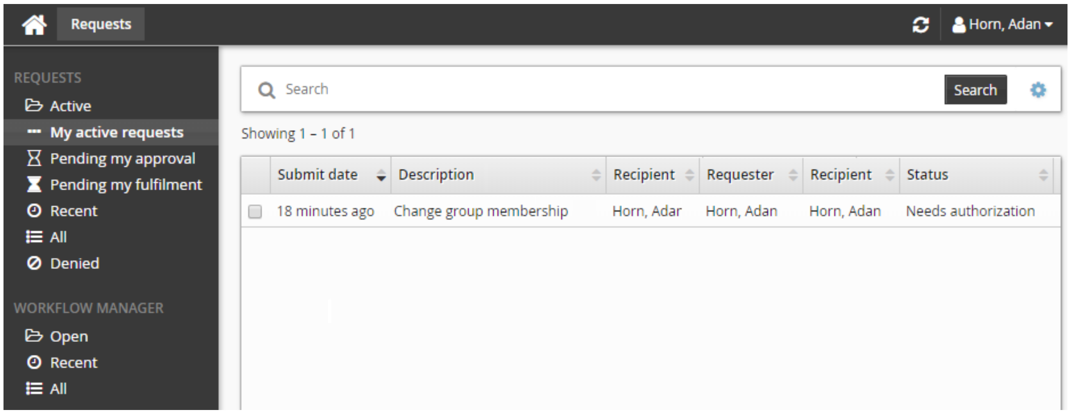
1. Log into the Front-end (PSF) and observe a notification regarding open requests.



Hitachi ID Identity and Access Management Suite menu

You have 1 open request(s).

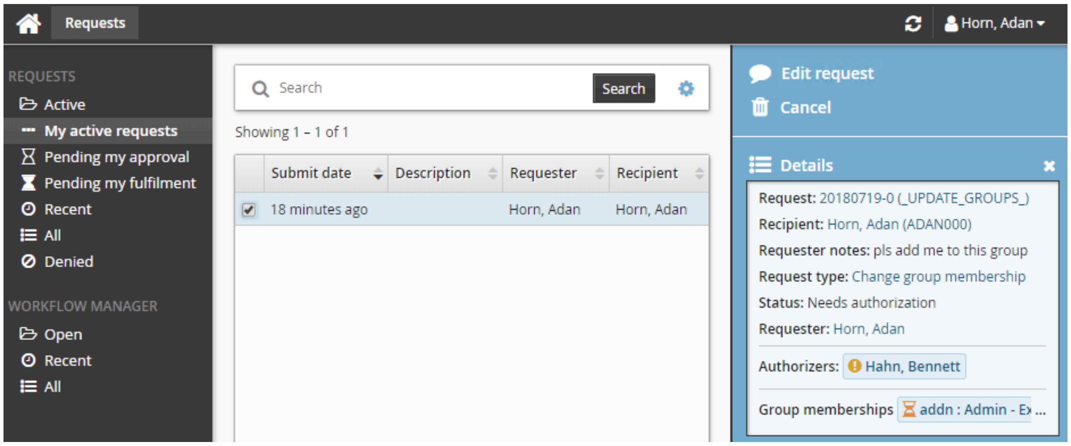
2. Click the notification link, or **Requests**, to see active requests.



Showing 1 – 1 of 1

	Submit date	Description	Recipient	Requester	Recipient	Status
□	18 minutes ago	Change group membership	Horn, Adar	Horn, Adan	Horn, Adan	Needs authorization

3. Select a request from the Results panel to view the details in the Actions panel.



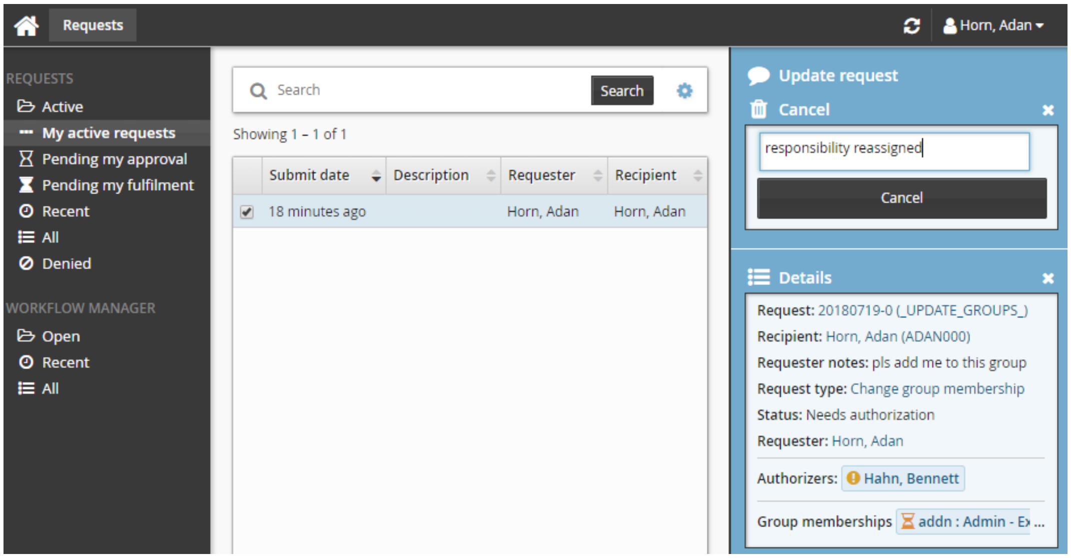
Showing 1 – 1 of 1

	Submit date	Description	Requester	Recipient
☑	18 minutes ago		Horn, Adan	Horn, Adan

Request: 20180719-0 (_UPDATE_GROUPS_)
Recipient: Horn, Adan (ADAN000)
Requester notes: pls add me to this group
Request type: Change group membership
Status: Needs authorization
Requester: Horn, Adan
Authorizers: Hahn, Bennett
Group memberships addn : Admin - Ex ...

In the Actions panel you can see that the request has not been processed yet. This means that you can cancel the request.

4. Click **Cancel**.



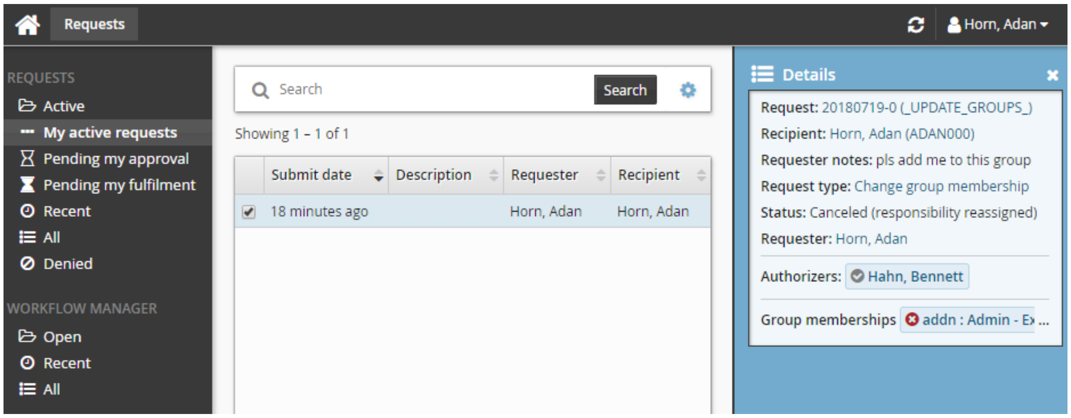
responsibility reassigned

Showing 1 – 1 of 1

	Submit date	Description	Requester	Recipient
☑	18 minutes ago		Horn, Adan	Horn, Adan

Request: 20180719-0 (_UPDATE_GROUPS_)
Recipient: Horn, Adan (ADAN000)
Requester notes: pls add me to this group
Request type: Change group membership
Status: Needs authorization
Requester: Horn, Adan
Authorizers: Hahn, Bennett
Group memberships addn : Admin - Ex ...

5. Enter a reason for the cancellation and click **Cancel**.



Showing 1 – 1 of 1

	Submit date	Description	Requester	Recipient
☑	18 minutes ago		Horn, Adan	Horn, Adan

Request: 20180719-0 (_UPDATE_GROUPS_)
Recipient: Horn, Adan (ADAN000)
Requester notes: pls add me to this group
Request type: Change group membership
Status: Canceled (responsibility reassigned)
Requester: Horn, Adan
Authorizers: Hahn, Bennett
Group memberships addn : Admin - Ex ...

Authorizing Requests 16

When requests are submitted in *Hitachi ID Bravura Identity*, *authorizers* review the requests to approve, deny, or modify them. This chapter shows you how to review and act on requests, using the *Requests* app.

16.1 About authorization

16.1.1 How authorizers are assigned

When a request is issued, *Hitachi ID Bravura Identity* notifies authorizers based on the entitlement, or some business logic via a workflow plugin.

Authorizers are notified of their tasks by email. *Bravura Identity* also displays task links at the top of the main menu to notify the authorizers that they have requests to review.

16.1.2 Delegation and escalation

Hitachi ID Bravura Identity users can act on behalf of other users in one of two ways:

- **Delegation** – A user can request to delegate all their responsibilities or a single request to another user. A *delegation manager* can also delegate a user's responsibilities to a third party.
- **Escalation** – When an authorizer fails to act on a workflow request in a timely manner, the request can be escalated to another user higher in the organization.

  If escalation is *not* configured, the request remains in the pending requests queue until it is approved or denied by one or more authorizers.

When escalation or delegation occurs, the user who takes over will be able to act as the original authorizer, with the same privileges, when dealing with the request.

Delegates are notified of their tasks by email. *Bravura Identity* also displays task links at the top of the main menu to notify the users that they have requests to review as a delegate.

See

- Delegating Responsibility in the *User Guide* to learn how to request or respond to a request for delegation.
- Acting on behalf of another authorizer to learn how to change who you are acting on behalf of, when authorizing requests.

16.1.3 Automatic approval of requests

Hitachi ID Bravura Identity can automatically approve a request if the requester is also an authorizer assigned to the affected resource.

A request will *not* be auto-approved if:

- Authorizers must enter values for required attributes when a request is reviewed.

  Or,

- More than one authorization is required to approve the request.

16.1.4 Managing authorization workflow

Authorizers who are granted the role of *workflow manager* can also cancel any request. This extra option is available to workflow managers on the request authorization pages.

They can also act as implementers, to act or decline manual tasks, and mark the tasks as completed or cannot be completed.

16.2 Reviewing requests

Hitachi ID Bravura Identity notifies available authorizers if a request needs to be reviewed. A link is also displayed when you log in, if you need to review current requests.

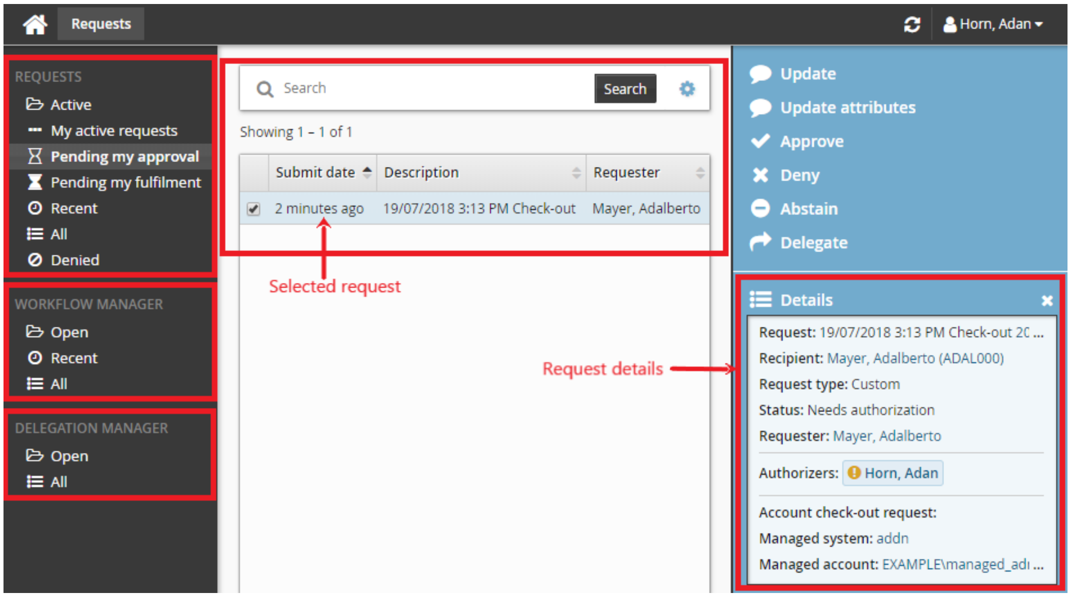
1. Click the task link or **Requests** from the main menu to launch the *Requests* app.

   Depending on your role and the type of operations, from here you can:

   - Use the links under REQUESTS in the Filter panel to display requests where you are assigned as the authorizer.
   - If you are a workflow manager, you can also view requests assigned to other authorizers using the links under the WORKFLOW MANAGER heading in the Filter panel.
   - If you are a delegation manager, you can view requests assigned to other authorizers using the links under the DELEGATION MANAGER heading in the Filter panel.

2. From the Results panel, select the request you want to review. The details will appear in the Actions panel.

   See Searching in an app in the *User Guide* for information about searching in the *Requests* app.



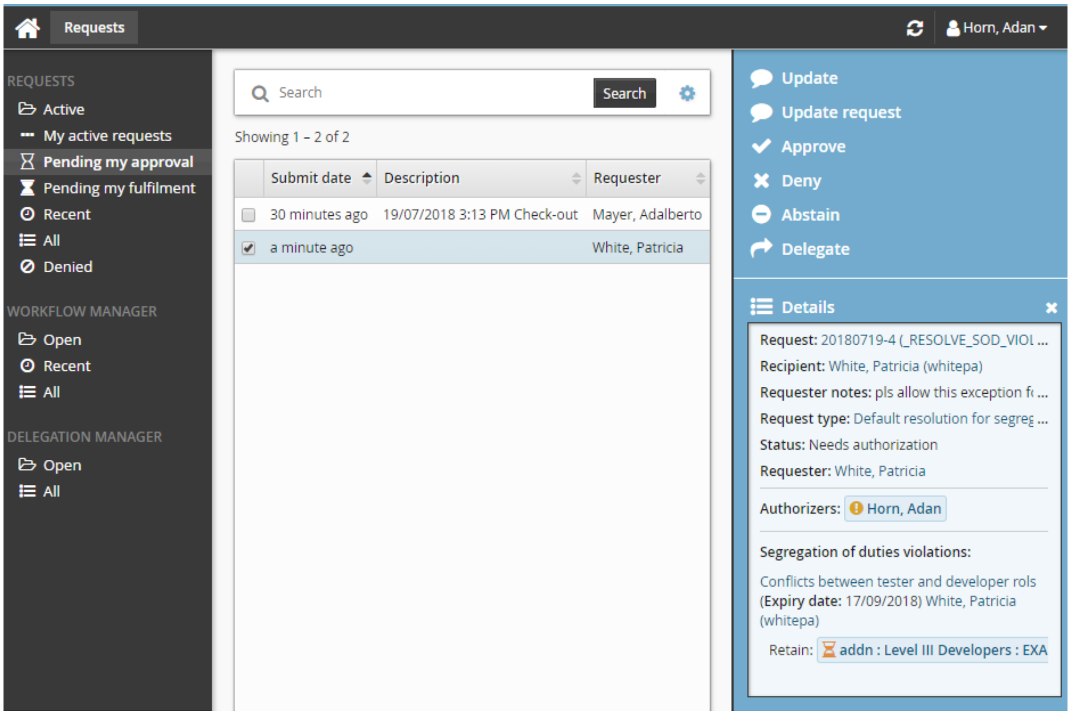
Showing 1 – 1 of 1

	Submit date	Description	Requester
☑	2 minutes ago	19/07/2018 3:13 PM Check-out	Mayer, Adalberto

Request: 19/07/2018 3:13 PM Check-out 2C ...
Recipient: Mayer, Adalberto (ADAL000)
Request type: Custom
Status: Needs authorization
Requester: Mayer, Adalberto
Authorizers: Horn, Adan
Account check-out request:
Managed system: addn
Managed account: EXAMPLE\managed_adı ...

Authorizing requests for exception to SoD rule

Requests may include exceptions to segregation of duties (SoD) rules (p60). In the example below, the rule disallows users from having both the QA tester and Developer roles. The request is that the user retains the Developer role, while requesting an exception to also have the QA tester role.



Showing 1 – 2 of 2

	Submit date	Description	Requester
□	30 minutes ago	19/07/2018 3:13 PM Check-out	Mayer, Adalberto
☑	a minute ago		White, Patricia

Request: 20180719-4 (_RESOLVE_SOD_VIOL ...
Recipient: White, Patricia (whitepa)
Requester notes: pls allow this exception fı ...
Request type: Default resolution for segreg ...
Status: Needs authorization
Requester: White, Patricia
Authorizers: Horn, Adan
Segregation of duties violations:
Conflicts between tester and developer rols (Expiry date: 17/09/2018) White, Patricia (whitepa)
Retain: addn : Level III Developers : EXA

If you click on a resource available in the Retain section, additional details about the group that caused the rule violation are displayed, including *indirect membership* details, if applicable.

Next:

Act on behalf of (p78).

16.3 Acting on behalf of another authorizer

If you are acting as a delegate, or you are workflow or delegation manager, you can change who you are acting on behalf of:

1. Use the links under the WORKFLOW MANAGER or DELEGATION MANAGER to view the requests.
2. Select the request from the Results panel.

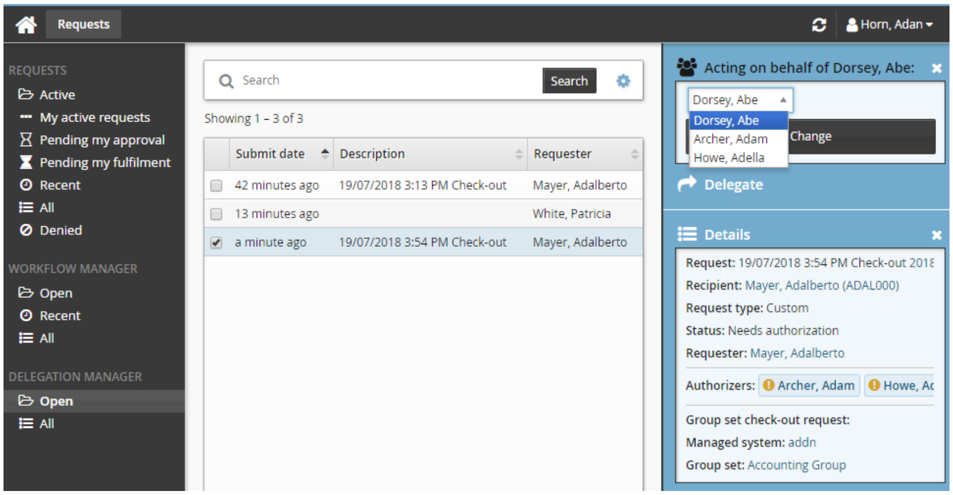
   The Actions panel will display who you are acting on behalf of.

   To change who you are acting on behalf of:

   (a) Click **Acting on behalf of <*user*>**.

   (b) Choose the required user from the drop-down list.

   (c) Click **Change**.



Showing 1 – 3 of 3

	Submit date	Description	Requester
□	42 minutes ago	19/07/2018 3:13 PM Check-out	Mayer, Adalberto
□	13 minutes ago		White, Patricia
☑	a minute ago	19/07/2018 3:54 PM Check-out	Mayer, Adalberto

Request: 19/07/2018 3:54 PM Check-out 2018
Recipient: Mayer, Adalberto (ADAL000)
Request type: Custom
Status: Needs authorization
Requester: Mayer, Adalberto
Authorizers: Archer, Adam Howe, Ac
Group set check-out request:
Managed system: addn
Group set: Accounting Group

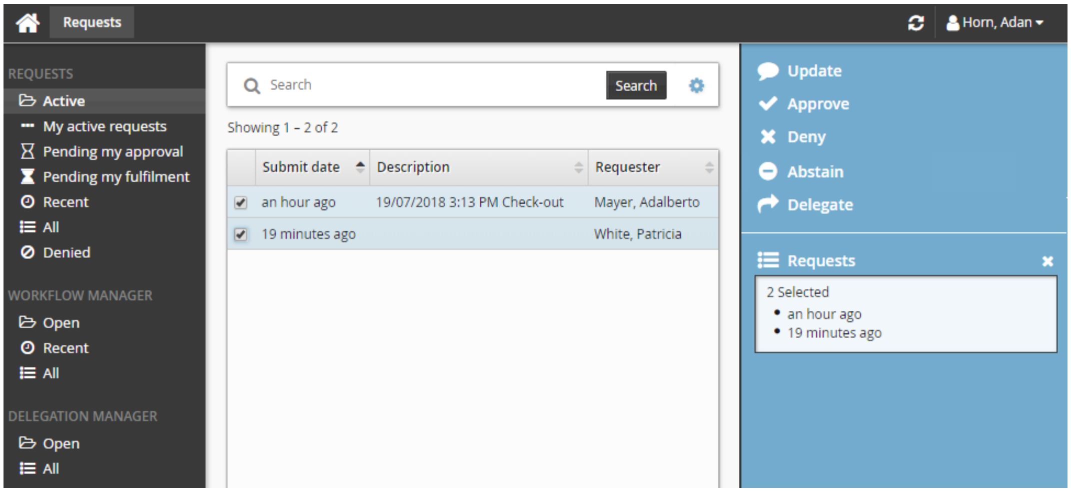
Note: If you are acting on behalf of different users for different requests, those requests must be actioned individually.

Next:

Act on requests (p79).

16.4 Acting on requests

1. After reviewing the requests, select the request you want to act on. You can act on multiple requests at a time by selecting more than one request from the Results panel.



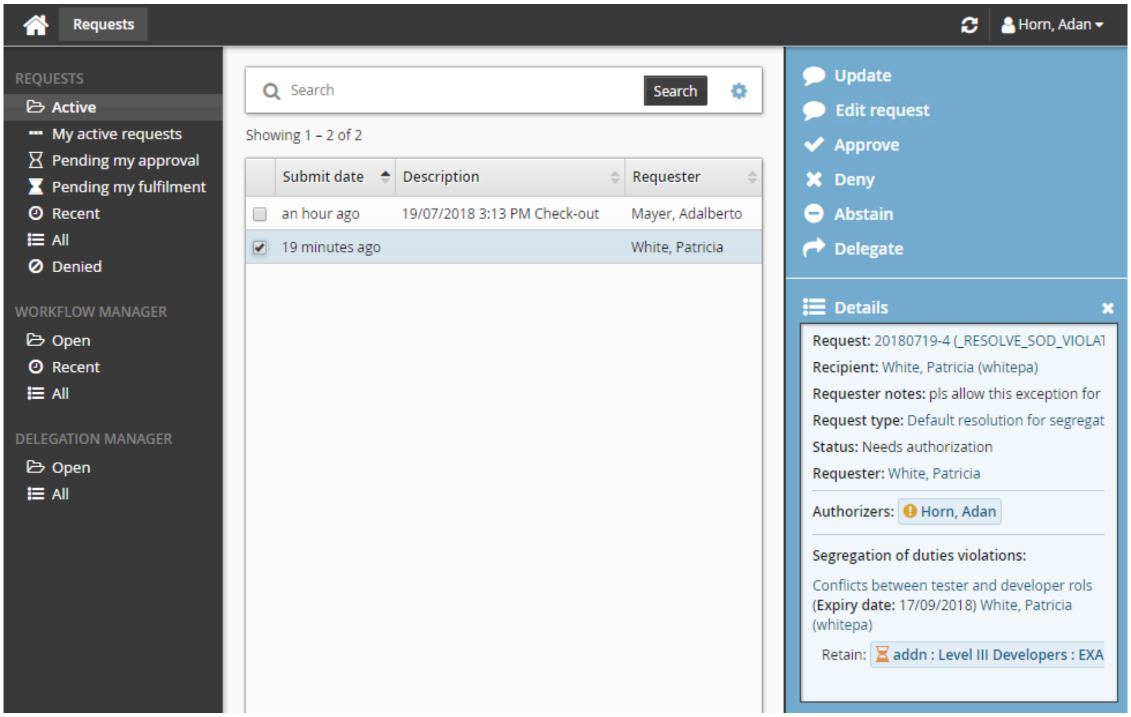
Showing 1 – 2 of 2

	Submit date	Description	Requester
☑	an hour ago	19/07/2018 3:13 PM Check-out	Mayer, Adalberto
☑	19 minutes ago		White, Patricia

2 Selected
- an hour ago
- 19 minutes ago

2. Click the action, from the available options in the Actions panel:

   - Update (notes) (p80)
   - Edit request (attributes and entitlements) (p80)
   - Approve (whole request) (p82)
   - Approvals (individual entitlements) (p83)
   - Deny (p83)
   - Abstain (p83)
   - Implementation tasks (p83)
   - Delegate (not as a workflow manager) (p84)
   - Cancel (workflow managers only) (p84)



Showing 1 – 2 of 2

	Submit date	Description	Requester
□	an hour ago	19/07/2018 3:13 PM Check-out	Mayer, Adalberto
☑	19 minutes ago		White, Patricia

Request: 20180719-4 (_RESOLVE_SOD_VIOLAT

Recipient: White, Patricia (whitepa)

Requester notes: pls allow this exception for

Request type: Default resolution for segregat

Status: Needs authorization

Requester: White, Patricia

Authorizers: Horn, Adan

Segregation of duties violations:

Conflicts between tester and developer rols (**Expiry date:** 17/09/2018) White, Patricia (whitepa)

Retain: addn : Level III Developers : EXA

16.4.1 Updating request notes

As an authorizer you can add a note to the request:

1. Click **Update**.
2. Enter the information you want to add.
3. Click **Update**.

16.4.2 Updating attributes and entitlements

The **Edit request** button is available to users if *both* the following conditions are met:

1. The request includes changes to profile attributes; for example if the request only includes group operations, the button will *not* be displayed.
2. The user has read and write permissions for at least one attribute group included in the request.

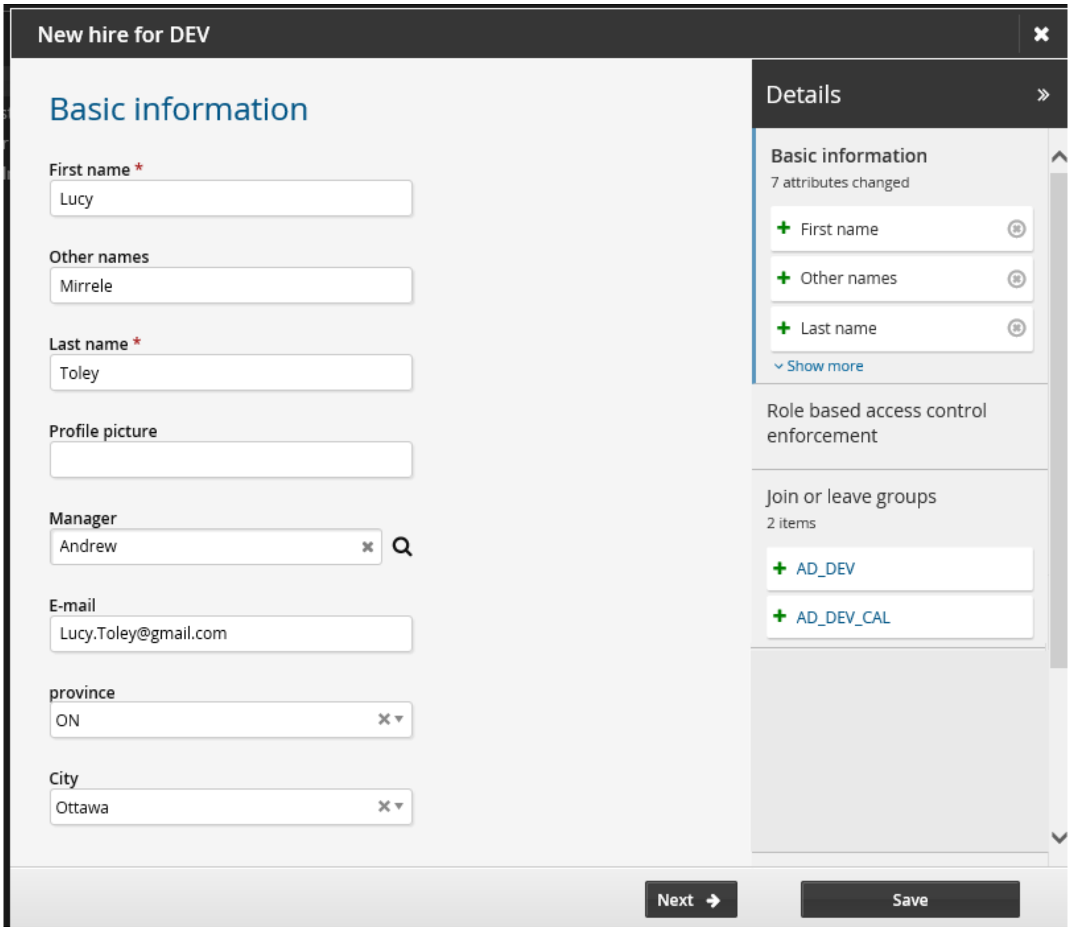
To update information and entitlements requested:

1. Click **Edit request**

   Hitachi ID Bravura Identity displays the request wizard.

You may be required to choose to make the updates as a requester, recipient, authorizer, or implementer. Select your choice and click **Update**.

2. Modify attributes that you want to update in the first attribute group.



New hire for DEV

Basic information

First name * Lucy

Other names Mirrele

Last name * Toley

Profile picture

Manager Andrew

E-mail Lucy.Toley@gmail.com

province ON

City Ottawa

Details

Basic information
7 attributes changed

- First name
- Other names
- Last name

Show more

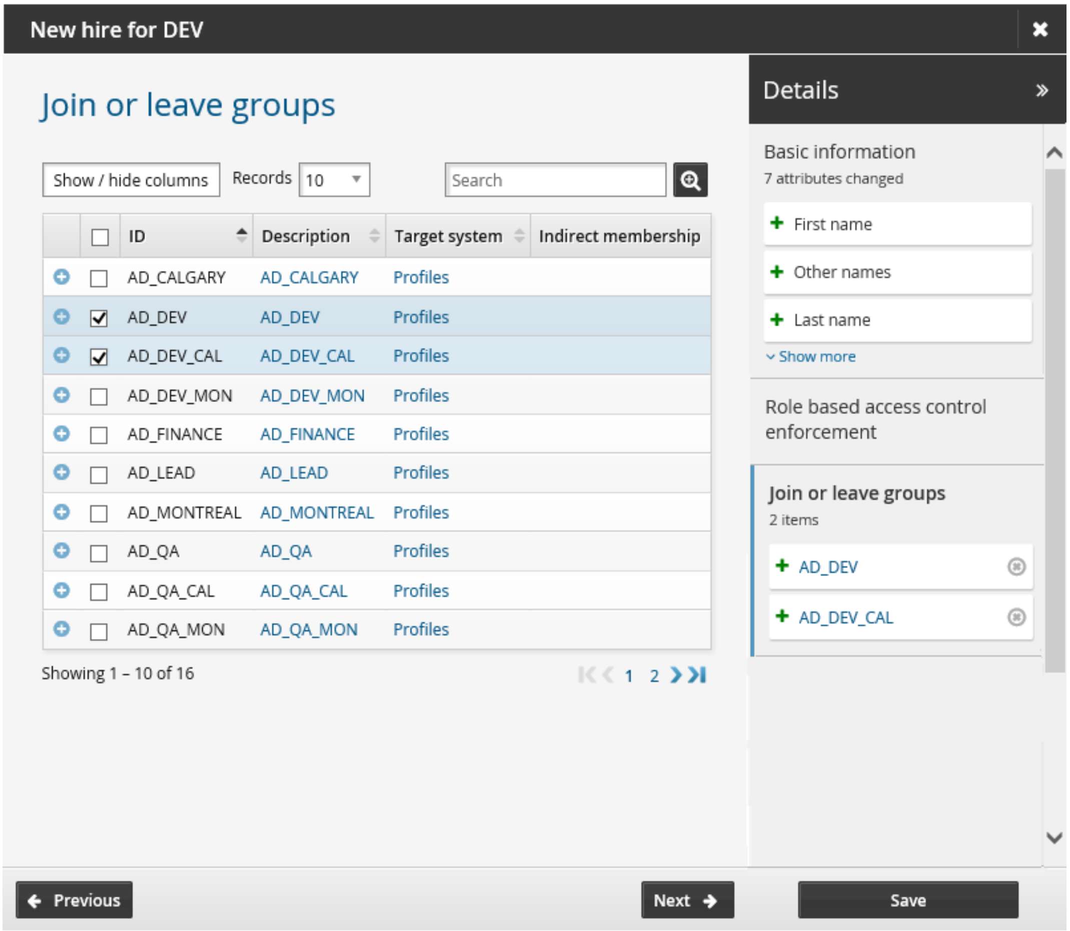
Role based access control enforcement

Join or leave groups
2 items

- AD_DEV
- AD_DEV_CAL

3. Click **Next** to update values in the next attribute group if applicable.

4. Click **Next** to go to the ***Join or leave groups*** wizard if applicable and change groups.



Join or leave groups

	ID	Description	Target system	Indirect membership
□	AD_CALGARY	AD_CALGARY	Profiles	
☑	AD_DEV	AD_DEV	Profiles	
☑	AD_DEV_CAL	AD_DEV_CAL	Profiles	
□	AD_DEV_MON	AD_DEV_MON	Profiles	
□	AD_FINANCE	AD_FINANCE	Profiles	
□	AD_LEAD	AD_LEAD	Profiles	
□	AD_MONTREAL	AD_MONTREAL	Profiles	
□	AD_QA	AD_QA	Profiles	
□	AD_QA_CAL	AD_QA_CAL	Profiles	
□	AD_QA_MON	AD_QA_MON	Profiles	

Showing 1 – 10 of 16 1 2

Basic information
7 attributes changed
+ First name
+ Other names
+ Last name
Show more

Role based access control enforcement

Join or leave groups
2 items
+ AD_DEV
+ AD_DEV_CAL

5. Click **Next** to go to the ***Change role membership*** wizard if applicable and change roles.

6. Click **Save** to save the changes for the request.

   Bravura Identity displays a notification that your update was successfully submitted. Click the **View request** link next to the message to view changes in the request.

16.4.3 Approving a request

Once you have selected the requests you want to approve you can:

1. Click **Approve** to approve the request.

2. If applicable, provide a reason for your actions.

   Hitachi ID Bravura Identity can be configured to require an authorizer to provide a reason when they approve or deny a request.

3. If required, enter your digital signature.

   Bravura Identity can be configured to require an authorizer to use a digital signature to sign-off on the requests.

16.4.4 Acting on individual entitlements

Hitachi ID Bravura Identity can be configured to allow you to act on individual entitlements in a request (by enabling **IDP APPROVE SINGLE RESOURCE** at **Manage the system** → **Workflow** → **Options** → **General**). When enabled, you can select an action for each entitlement.

Select the request you want to action:

1. Click **Approvals**.
2. For each entitlement select one of the following:
   - **Set Later** The individual entitlement request will be left in a pending state until approved, denied or expired.
   - **Approve** The individual entitlement request will be approved.
   - **Deny** The individual entitlement request will be denied.
   - **Abstain** The user is removed from the authorizer list for the individual entitlement.
3. Click **Finish** to commit the changes.

16.4.5 Denying a request

1. Click **Deny** to deny the request.
2. If applicable, provide a reason for your actions.

   Hitachi ID Bravura Identity can be configured to require an authorizer to provide a reason when they approve or deny a request.

16.4.6 Abstaining from a request

You can abstain from approving or denying a request where it would be inappropriate due to a conflict of interest. If the number of authorizers left to review the request falls below the number required to approve it, then it will be automatically denied due to lack of approvals.

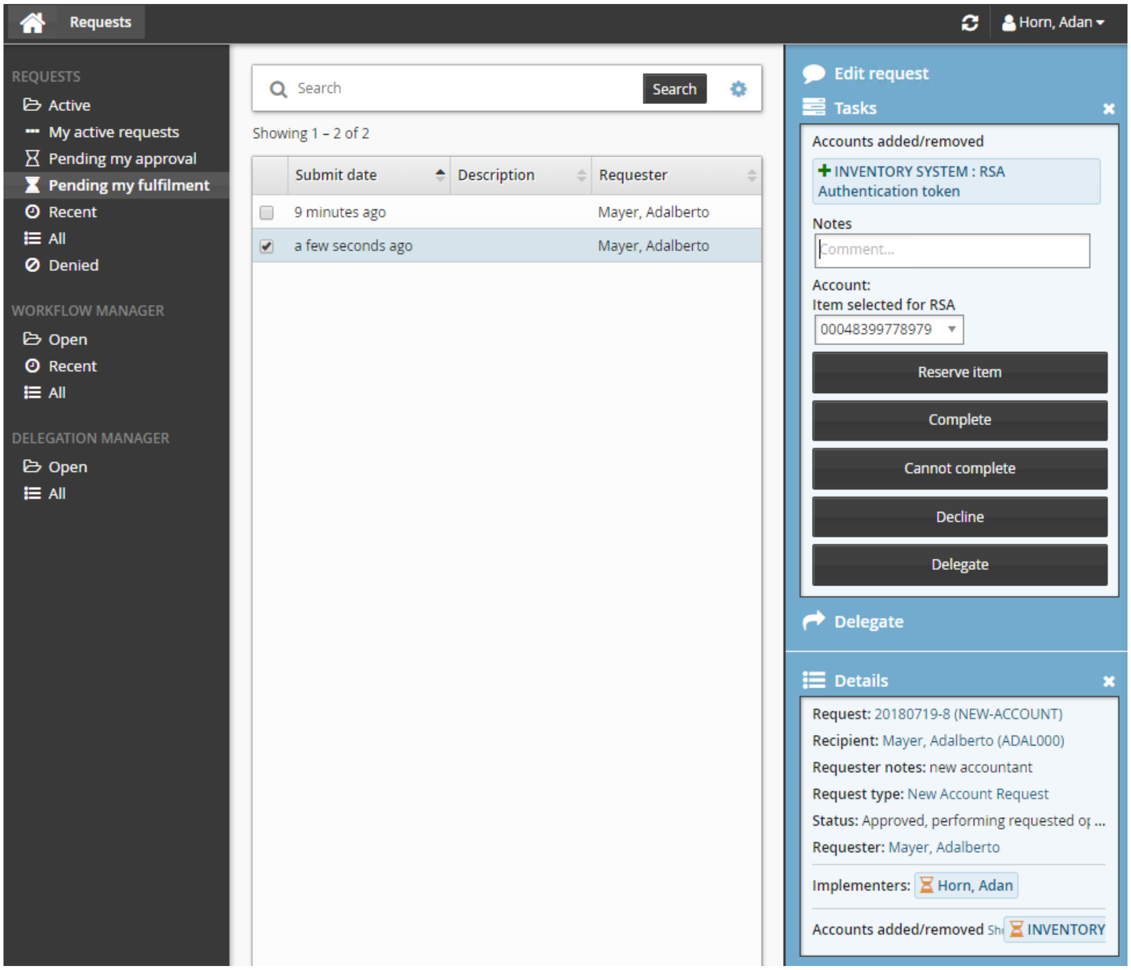
1. Click **Abstain**.
2. Provide a reason for your actions.

16.4.7 Carrying out implementation tasks

If you are an implementer that is also an inventory manager, you can click on **Pending my fulfillment** to choose inventory items for account creation requests. For example, to choose an RSA Authentication Manager 7.1/8.2 token when provisioning a new token for a user.

The inventory item may be selected from the drop down list. Click **Reserve item** to reserve the item for the request to use for the account creation.

Click **Release item** to choose a different inventory item for the request.



Showing 1 – 2 of 2

	Submit date	Description	Requester
□	9 minutes ago		Mayer, Adalberto
☑	a few seconds ago		Mayer, Adalberto

Accounts added/removed

INVENTORY SYSTEM : RSA Authentication token

Notes

Comment...

Account:

Item selected for RSA

00048399778979

Request: 20180719-8 (NEW-ACCOUNT)

Recipient: Mayer, Adalberto (ADAL000)

Requester notes: new accountant

Request type: New Account Request

Status: Approved, performing requested op...

Requester: Mayer, Adalberto

Implementers: Horn, Adan

Accounts added/removed Sh INVENTORY

16.4.8 Delegating requests

If you chose to delegate a request, on the ***Delegation information*** page, set the delegation options.

16.4.9 Canceling requests

If you are a workflow manager, you can click **Cancel** and cancel the request.

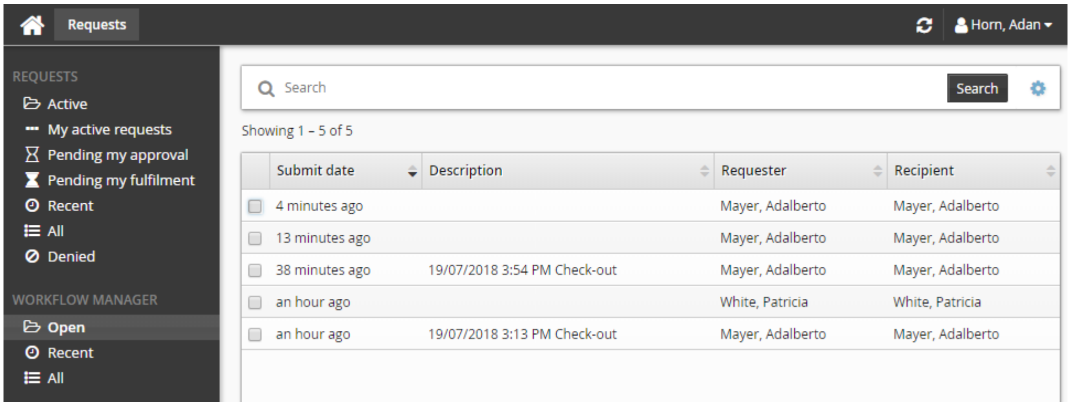
16.5 Example: Acting on behalf of another user

This example demonstrates the typical steps followed when a *workflow manager* reviews several requests and then authorizes a request on behalf of another user.

Reviewing requests as a workflow manager

The *workflow manager* regularly checks requests to ensure none have been sitting for too long waiting for action.

1. Log into the Front-end (`PSF`) as a *WORKFLOW MANAGER*.
2. From the main menu , click **Requests**.
3. Click **Open** underneath WORKFLOW MANAGER from the Filter panel.



Showing 1 – 5 of 5

	Submit date	Description	Requester	Recipient
□	4 minutes ago		Mayer, Adalberto	Mayer, Adalberto
□	13 minutes ago		Mayer, Adalberto	Mayer, Adalberto
□	38 minutes ago	19/07/2018 3:54 PM Check-out	Mayer, Adalberto	Mayer, Adalberto
□	an hour ago		White, Patricia	White, Patricia
□	an hour ago	19/07/2018 3:13 PM Check-out	Mayer, Adalberto	Mayer, Adalberto

4. Select each of the requests, one at a time, from the Results panel and review the details that appear in the Actions panel.

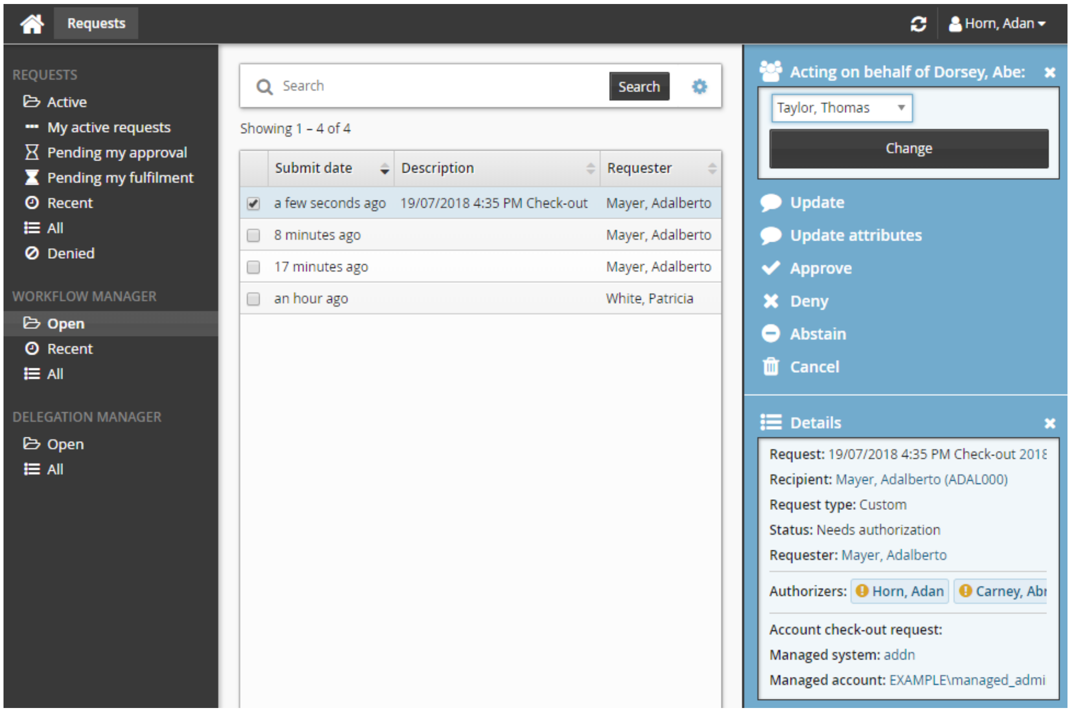
Authorize a request

The *workflow manager* finds one request that has been waiting for authorization for 24 days and knows the authorizer has been away on sick leave so authorizes the request.

1. Select the request from the Results panel.

   Change who you are acting on behalf:

   (a) Click **Acting on behalf of Dorsey,Abe**.
   (b) Choose `Taylor, Thomas` from the drop-down list.
   (c) Click **Change**.



Showing 1 – 4 of 4

	Submit date	Description	Requester
☑	a few seconds ago	19/07/2018 4:35 PM Check-out	Mayer, Adalberto
□	8 minutes ago		Mayer, Adalberto
□	17 minutes ago		Mayer, Adalberto
□	an hour ago		White, Patricia

Acting on behalf of Dorsey, Abe:

Taylor, Thomas

Request: 19/07/2018 4:35 PM Check-out 2018
Recipient: Mayer, Adalberto (ADAL000)
Request type: Custom
Status: Needs authorization
Requester: Mayer, Adalberto
Authorizers: Horn, Adan Carney, Abı
Account check-out request:
Managed system: addn
Managed account: EXAMPLE\managed_admi

2. Click **Approve**

3. Type a note in the available box. For example, enter `user away on sick leave, authorizing on behalf of.`

4. Click **Approve**

   The request has now been authorized.

Index of Variables and Options

Index

Hitachi ID Systems, Inc.
500, 1401 - 1 Street SE, Calgary AB Canada T2G 2J3   Tel: 1.403.233.0740   E-Mail: sales@hitachi-id.com