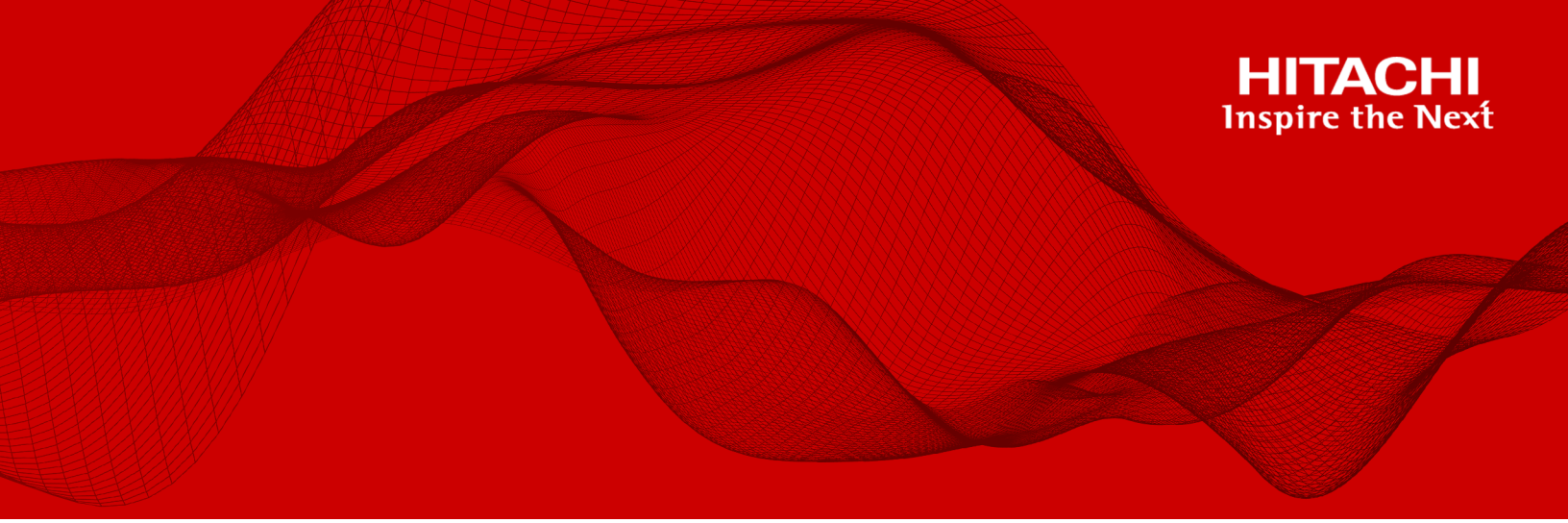


Bravura Group

Quick Start Guide

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

Contents

Part I

INTRODUCTION

Implementing Network Resource Management 1

Network resource management allows users to request access to network resources for themselves or others without the need to understand the underlying security infrastructure. In *Hitachi ID Bravura Security Fabric*, network resource management is provided by *Hitachi ID Bravura Group*.

Bravura Group manages different types of resources using connectors and programs shipped with *Hitachi ID Connector Pack* in the agent directory:

- The **`nrsmb`** program binds *Bravura Group* to a specific resource whose access is mediated by membership in a group on a Legacy Active Directory target system. These resources include shares, folders, printers, and mail distribution lists.
- The **`nrcifs`** program binds *Bravura Group* to a specific resource whose access is mediated by membership in a group on an Active Directory DN target system. These resources include shares, folders, printers, and mail distribution lists.
- The **`nrshrpt`** program binds *Bravura Group* to a specific resource managed by a SharePoint Resource target system. Microsoft Office SharePoint Server resources include sites and documents.

In general, the process for gaining access to a Windows shared folder is as follows:

1. A Network Administrator creates a shared folder on the target system.
2. A Network Administrator grants permissions, using groups, to control access to the shared folder.
3. A target system is configured to manage network resources.
4. A user (requester) logs into the *Bravura Group* web application and selects the network resources link.

   Bravura Group displays a search page.
5. The user selects the share that he wants to view.

   The **`nrsmb`** or **`nrcifs`** program gathers initial information about the share and displays a tree view of the folders in the selected share.
6. The user browses for and selects a folder where access is desired.

   The **`nrsmb`** or **`nrcifs`** program gathers additional information about the share and displays a list of groups that have privileges on the share as well as the groups' owners and read / write privileges.
7. The user selects a group to join and submits the request.

   Bravura Group enters the request into the authorization workflow.

8. The Workflow Manager Service (idwfm) routes the request to the selected group owner for authorization.
9. After authorization is complete the Transaction Monitor Service (idtm) runs a connector program that adds the user to the selected group on the target system.

When users are granted membership in a group they are granted access to all the resources that the group has permission to access. Likewise, taking away users' access to a particular resource results in the users losing their membership in the group that was providing the access, and losing access to all the resources the group has permission to access.

1.1 Setting up network resource management

In order to implement *network resource management* using *Hitachi ID Bravura Group*:

1. Prepare the resource on the external target system.
2. Set up email notification.

   Bravura Group 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.
3. Add target systems as source of profiles.

   Add at least one target system that will be an authoritative list of users to be imported into *Bravura Group*. 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.
4. Import users.

   Run auto discovery to import a list of users, their accounts and other attributes, from one or more target systems.
5. 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.
6. Add the target system that mediates access to the resource.

   Set the **Managed group**/**Network resource target system type** option to the appropriate value.
7. Add the network resource to *Bravura Group*.
8. Manage groups.

   You can manually select which managed groups you want managed, or allow *Bravura Group* to select them for you.
9. Configure additional features and settings.

1.2 Preparing resources on target systems

All shared resources to which users are going to request access must be correctly configured on the target system. *Hitachi ID Bravura Group*'s ability to successfully control access to the resources depends heavily on how the resources are configured on the target system.

Some thought must be given to planning how many groups need to be created and what resources they will have permission to access, so that adding/removing a user's membership in a group provides them with the exact access to network resources that they need. To provide access to resources on a resource by resource basis, you need to create a group for each resource.

In general, you must do the following:

1. Create groups with appropriate permissions to control access to the resources that are going to be managed by *Bravura Group*.
2. Ensure that each group has an owner (recommended).

   Bravura Group can use group owners as authorizers for requests to join the group. See Groups for more information.
3. Ensure that all resources to be managed have the correct groups assigned to them.

See the Connector Pack Integration Guide for details on setting up target systems for network resource management.

1.2.1 Setting up target systems for network resource management

This section describes configuration requirements for target systems that support network resource management in *Hitachi ID Bravura Group*.

1.2.2 Configuration notes for Legacy Active Directory

For a resource whose access is mediated by membership in Microsoft Active Directory groups, ensure that the target system is configured as follows:

Setting	Value
Target type	**Legacy Active Directory**
Manage group/Network resource target system type	**SMB Protocol for Legacy Active Directory**
Target address	For a share / folder, this is the domain where the share is published. You set the path to individual shares when you add resources. For a printer, this is the print server or domain where printers are published. For a mail distribution list, this is the domain where distribution groups are stored.

1.2.3 Configuration notes for Active Directory DN

For a resource whose access is mediated by membership in Active Directory DN groups, ensure that the target system is configured as follows:

Setting	Value
Target type	**Active Directory DN**
Manage group/Network resource target system type	**SMB Protocol for Active Directory DN**
Target address	For a share / folder, this is the domain where the share is published. You set the path to individual shares when you add resources. For a printer, this is the print server or domain where printers are published. For a mail distribution list, this is the domain where distribution groups are stored.

1.2.4 Configuration notes for SharePoint

For a resource whose access is mediated by membership in SharePoint resources, ensure that the target system is configured as follows:

Setting	Value
Target type	**SharePoint Server**
Manage group/Network resource target system type	**SharePoint Resource**

Target address	Main URL of the site, followed by a colon, then the port number, a slash, and the site name. For example: `http://sharepoint1:2427/site1/site2/`

See the Connector Pack Integration Guide for further details on setting up target systems for network resource management.

1.3 Configuration examples and use cases

1.3.1 Use Case 1: Requesting access to the Sales folder

This use case demonstrates the process a user would follow to request access to the Sales folder.

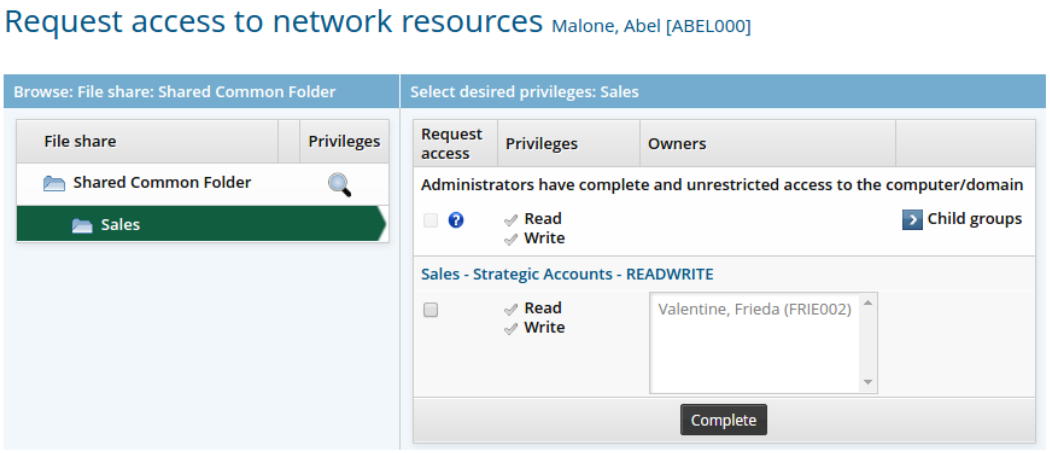
The user could request access to the appropriate group that would provide him access to the folder, however, in most instances, a user would not know which group that would be. An alternative is to set up network resources and allow the user to request access to the shared folder. *Hitachi ID Bravura Group* will do the work in the background to enable the access.

Before a user can request access to the Sales folder, the following is required:

- The Sales folder is shared on a Microsoft Windows file server.
- Groups have been used on the share to apply security, and those groups are managed by *Bravura Group*.
- An Active Directory DN target has been added, and is configured to manage network resources.
- Authorization has been set on the groups.
- The share is added to *Bravura Group* as a network resource.

To request access to the Sales folder:

1. From the main menu, click **Request access to network resources** in the **My profile** section.
2. Click **Shares**/**Folders**.
3. Select the Shared Common Folder.
4. Click the icon next to the **Sales** folder.
   The privileges appear on the right hand side.



5. Select **Sales-Strategic Accounts - READWRITE** and click **Complete**.

   Bravura Group enters the request into the authorization workflow.

The Workflow Manager Service (idwfm) routes the request to the selected group owner for authorization. After authorization is complete the Transaction Monitor Service (idtm) runs a connector program that adds the user to the selected group on the target system and the user will have access to the Sales folder.

1.3.2 Use Case 2: Requesting access to documents in SharePoint

This use case demonstrates the process a user would follow to request access to a document library in SharePoint.

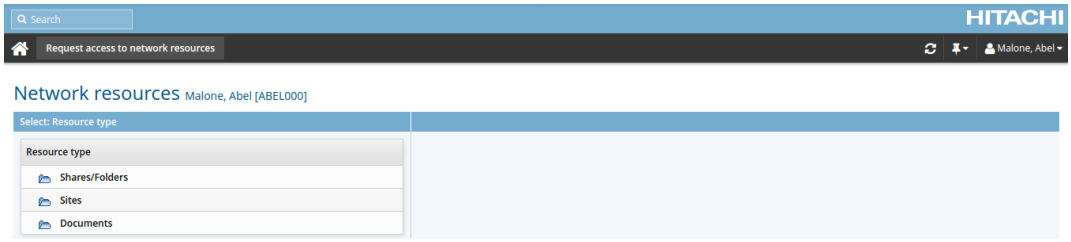
Before a user can be granted access to a document library in SharePoint, the following is required:

- A document library has been created in Windows SharePoint.
- At least one document exists in the document library.
- Users have at least *read* privileges to the SharePoint site. In this use case, the "domain users" Active Directory group has been added to the SharePoint Visitors group.
- The Visitors, Members, and Owners SharePoint groups all have owners.
- A SharePoint target has been added to *Hitachi ID Bravura Group*, and is configured to manage SharePoint network resources.
- The document library is added to *Bravura Group* as a network resource.

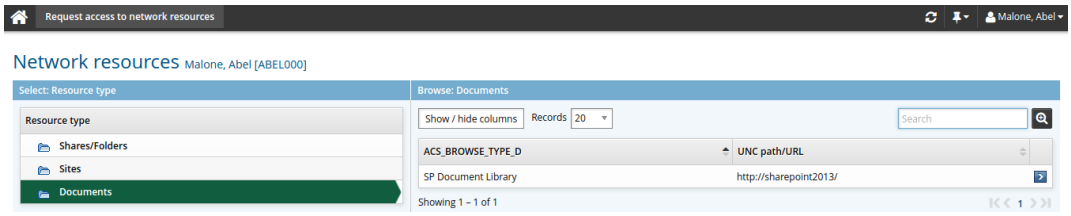
To request access to the document library:

1. From the main menu, click **Request access to network resources** in the **My profile** section.

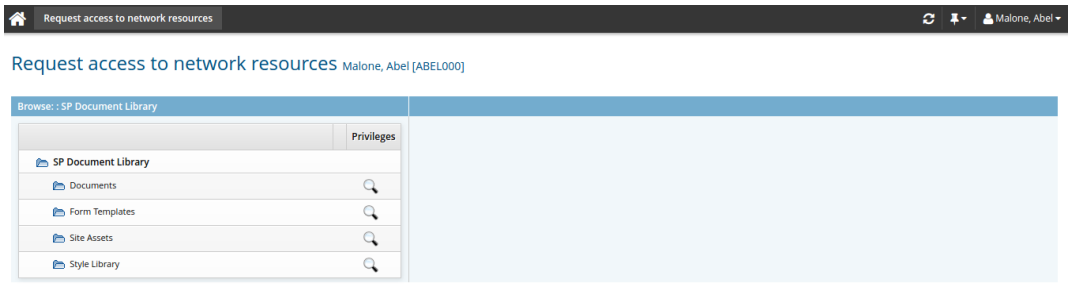
   The ***Request access to network resources*** page appears.



2. Click **Documents**.
   Bravura Group displays available document libraries on the right hand side.

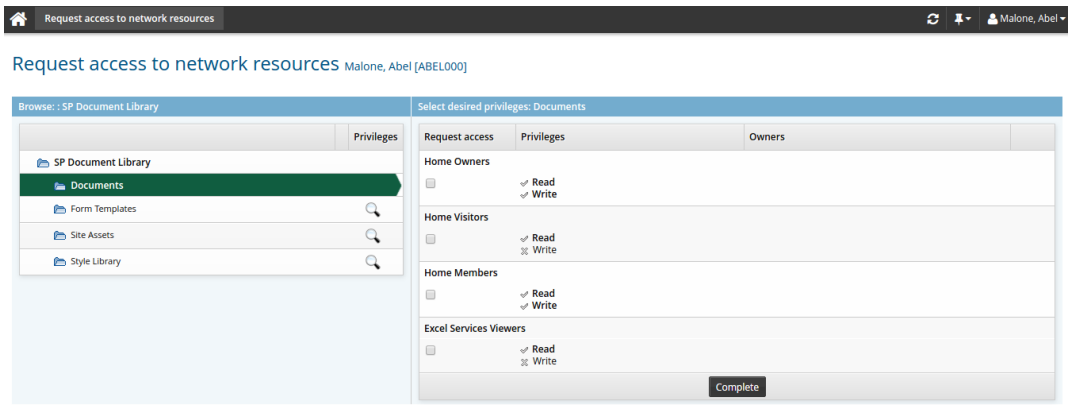


3. Select SP Document Library.
   Bravura Group displays available resources in the document library.



   You can click the icon next to the various folders to view privileges.

4. Click the icon next to **Documents**.
   The privileges are displayed on the right hand side.



5. Select the **Home Members** group and click **Complete**.
   Bravura Group enters the request into the authorization workflow.

The Workflow Manager Service routes the request to the selected group owner for authorization. After authorization is complete the Transaction Monitor Service runs a connector program that adds the user to the selected group on the target system and the user will have access to the Sales folder.

Part II

CONFIGURING GROUP MANAGER

Adding a Target System 2

Hitachi ID Bravura Group manages resources and 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 Group* profiles. This means that users with accounts in Active Directory will have profiles, including full user name, created for them in *Bravura Group*.

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 a:
   - Share / folder – this is the host name of the domain where the share is published. You set the path to individual shares when you add resources.
   - Printer – this is the host name of the print server or domain where printers are published.
   - Mail distribution list – this is the host name of the domain where distribution groups are stored.
7. Set the **Managed group/Network resource target type** to **SMB Protocol**.
8. Select the **Source of profile IDs** checkbox.
9. If you want to list users' email addresses from Active Directory for use by *Bravura Group*, select the **List attributes** checkbox.
10. If you want *Bravura Group* to generate a list of attributes for each account during auto discovery, select **List attributes**.
11. For this demonstration installation, leave other parameters with default values.
12. Click **Add**.

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

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

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

Importing Users 3

You add users to *Hitachi ID Bravura Group* 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 Group*:

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

   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.

Adding Network Resources 4

To add a network resource that can be managed by *Hitachi ID Bravura Group*:

1. Click **Manage the system** → **Resources** → **Network resources**
2. Set the network resource options as described in Table 4.1.
3. Click **Add**.

Table 4.1: Network resource options

Option	Description
ID	A unique identifier for the resource.
Description	The resource name that is displayed to users.
Type	The resource type. The options displayed depend on network resource management plugin settings on the ***Target system information*** page. • SMB Protocol (**`nrsmb`**): – **Shares/Folders** – **Printers** – **Mail distribution lists** • SMB Protocol for Active Directory DN (**`nrcifs`**): – **Shares/Folders** – **Printers** – **Mail distribution lists** • SharePoint Resource (**`nrshrpt`**): – **Sites** – **Documents**
UNC path/URL	(Shares/Folders only) The path to the network share that you want to manage; for example, `\\<server name>\<share name>`. Alternately, you can use <*IP Address*> instead of <*server name*>. (Sites or Documents only) The URL to the Microsoft Office SharePoint Server server that you want to manage; for example, `http://sharepoint1:2427/sitename`.

. . . continued on next page

Table 4.1: Network resource options (Continued)

Option	Description
Target system of the resource	The target system that mediates access to the resource. This is the target you configured in step 6 on page 3.
Users can only see sub-resources if they have rights to the resource	(Shares/Folders or Sites only) Click this checkbox if you want to limit users who can view subfolders to those who belong to a group that can view the parent folder. For resources automatically created by the *Shell Extension*, this is controlled by the **IDR NETWORK RESOURCE VALIDATE** setting. See View and update profile (IDR).

Once resources are set up, resources are available to users via the **Request access to network resources** link in the self-service menu.

See also:

- The **`nrsmb`**, **`nrcifs`** and **`nrshrpt`** programs are shipped with *Hitachi ID Connector Pack*. You can add custom target types and programs using the **`loadplatform`** program. See loadplatform in the Bravura Security Fabric *Reference Manual* for details.
- You can use the **`listadresources`** and **`loadnetres`** programs to quickly load published resources on an Microsoft Active Directory target system into the *Hitachi ID Bravura Group* database. See listadresources in the *Reference Manual* for details.
- You use the ***Network resource filters*** page to add filter rules.

Managing Groups 5

This chapter shows you how to manage target system groups in *Bravura Group*. Groups can be used to apply access controls and policies.

This chapter includes:

5.1 About managed groups

A managed group is a group of accounts defined on a target system, whose membership is monitored and managed in *Hitachi ID Bravura Group*. 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 Group*.

During auto discovery, *Bravura Group* lists all available groups from supported target systems, then loads the group information into its database. By default, *Bravura Group* 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.
- Group owners can manage membership and ownership.
- The group's membership can be used to segment users into user classes.

See also:

- Network resource group filtering in the *Reference Manual* to learn how to filter groups available to users for network resources.
- Displaying group IDs to learn how to display long or short group IDs.
- User classes to learn how to use a group's membership to define user classes.

5.1.1 Membership types

Generally, groups managed by *Hitachi ID Bravura Group* can be:

- Open – no approval is required to change their membership
- Moderated – Changes to membership must be approved by an authorizer
- Closed – No membership changes are allowed via *Bravura Group*

The way that users join a managed group is controlled by the group's **Authorization for joining group** setting (p21). The way that users leave a managed group is controlled by the **Authorization for leaving group** setting (p21). These options can be set at the target system level when the target system's **Automatically manage groups** option is set to "Only groups with owners, moderated by owners" or "All groups, approval required".

Membership of managed groups can be defined as:

No approval required	Group owners can manage access, and users can submit requests to join the group. These requests do *not* require authorization from the managed group's authorizers.
Approval required	Group owners can manage access, and users can submit requests to join the group. These requests require authorization from the group's authorizers.
Open to members of another group without approval	Does not apply to *Bravura Group*.
No changes to group membership allowed	Users can view the group, but they *cannot* submit requests to join the group. Group owners cannot manage access for groups that do *not* allow membership changes.

Users can only submit requests to join **Approval required** or **No approval required** type groups if the recipient has an account on the group's target system. It is possible to set differing permissions for adding and removing users from groups. For example, a user may need authorization to join a group, and be removed without requiring authorization.

WARNING!: A managed group's type affects how access requests are handled for that group. Requests made to groups where approval is *not* required are auto-approved.

Requests made to groups that require approval without a minimum authorizers requirement are handled like requests to groups that do *not* require approval, and are also auto-approved. Care should be taken in setting a managed group's type and configuration options, so that the proper access restrictions are put in place.

5.2 Getting started

Requirements

- You require the **Manage resources** administrative privilege in order to access the **Manage the system** → **Resources** → **Groups** menu.
- Before you can manage a group, you must run auto discovery to generate a list of available groups from target systems.

  See Adding a Target System for more information about target systems, and Auto Discovery for more information about auto discovery.

Note: Any group whose long group ID contains more than 200 characters is ignored, is not loaded during auto discovery and cannot be managed. If this happens, an error message is written to the log file.

Proceed to:

- Managing groups automatically to learn how to automatically load and manage groups.
- Managing groups manually to learn how to manually manage groups using the *Manage the system* (PSA) module.

5.3 Managing groups automatically

Rather than configuring each group individually, you can:

- Allow *Hitachi ID Bravura Group* to automatically manage groups that are attached to network resources.

  See Automatically managing groups attached to network resources for details.

- Configure *Bravura Group* 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 *Reference Manual* to learn how to use this program.

5.3.1 Automatically managing groups attached to network resources

Hitachi ID Bravura Group allows users to browse and request access to network resources even before the groups attached to the resource have been enabled for management. When a user chooses an action for resource – for example, a requester selects a group to join, or an owner clicks the owners icon – *Bravura Group* checks the status of the group. If the group is *not* already managed, *Bravura Group* automatically configures and enables it for group management.

In addition to adding the group owners as authorizers for the group, *Bravura Group* 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
Authorization for joining group	Approval required
Authorization for leaving group	Approval required

5.3.2 Automatically managing groups via auto discovery

If supported by the target system, *Hitachi ID Bravura Group* connectors can list groups during auto discovery. Group owner information is included if it is available. You can configure *Bravura Group* 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 Group* 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 Group does *not* change the configuration for groups that are already managed.

5.4 Managing groups manually

You use the ***Managed group information*** page to to start or stop managing a group, and to configure other options for a group. To access this page for a given group:

1. Click **Manage the system** → **Resources** → **Groups**.
   Hitachi ID Bravura Group displays a list of existing target systems.
2. Select the target system on which the group resides.
   Bravura Group displays a list of available groups for the target system, indicating which groups are currently managed.
3. Select the group that you want to configure.
4. Set required authorization settings:
   - **Minimum number of authorizers**
   - **Number of denials before a change request is terminated**
   - **Authorization for joining group**

- **Authorization for leaving group**

See Configuring group-level authorization for details.

5. Click **Manage**.
6. Run auto discovery to load group membership into the *Bravura Group* database.
   Click **Manage the system** → **Maintenance** → **Auto discovery**.

Next:

- Manually configure managed group options (p21)
- Configure group-level authorization (p22)
- Define group membership by user class (p23)

5.5 Updating group options

Table 5.3: Group options

Option	Description
Overridden description	The description to display to users. If you leave this field blank, *Hitachi ID Bravura Group* uses the **Group description** loaded from the target system.
Help URL	In case a longer description would help users, you can compose and post a web page that describes this group further, and enter its URL here. Users can open the URL by clicking the group description text wherever the text appears in the user interface.
Track changes	Select this checkbox to capture changes to this managed group. Changes include joining or leaving the group. See Tracking changes to group membership for details.
Detect out-of-band additions and automatically generate a workflow request	If enabled, then additions of users or groups that were done without using *Bravura Group* are detected, and requests are automatically generated to undo or redo the change via the Workflow Manager Service (idwfm). The **Track changes** setting must also be enabled. See Tracking changes to group membership for details. See also Automated workflow request options for information about options related to automated group requests.

. . . continued on next page

Table 5.3: Group options (Continued)

Option	Description
Detect out-of-band deletions and automatically generate a workflow request	If enabled, then deletions of users or groups that were done without using *Bravura Group* are detected, and requests are automatically generated to undo or redo the change via the Workflow Manager Service. The **Track changes** setting must also be enabled. See Tracking changes to group membership for details. See also Automated workflow request options for information about options related to automated group requests.
Automatically add group owners as authorizers	Select this checkbox to automatically add group owners as authorizers for the group. If the group owner is a group, its group members must be listed before they can be added as authorizers. See Managing groups automatically for more information.
Authorization for joining group	(Required) Determines how users can be added to the group. See Membership types for more information about join types.
Authorization for leaving group	(Required) Determines how users can be removed from the group. See Membership types for more information about leave types.
Minimum number of authorizers	(Required) The number of authorizers who must approve requests related to this group. See Determining number of required approvals for details.
Number of denials before a change request is terminated	(Required) A resource request is canceled when this number of authorizers deny it. See Determining number of required approvals for details.

5.6 Configuring group-level authorization

Read this section to learn how to:

- Set the number of approvals or denials required for requests involving the group (p23).
- Manually assign *static authorizers* for the group (p23).
- Automatically add group owners as static authorizers for the group (p24).

When requesting access to network resources using *Hitachi ID Bravura Group*, users can only submit requests for groups that have at least one authorizer or group owner assigned.

Users must be loaded into the *Bravura Group* database before you can define them as authorizers.

You must assign enough authorizers to meet the minimum number of authorizers requirement. If you do not do this, requests involving the resource are automatically denied unless authorizers are assigned by a workflow plugin.

5.6.1 Determining number of required approvals

To set authorization thresholds for a managed group:

1. Navigate to the ***Managed group information*** page (p20).
2. Click the **Authorization** tab.
   Select a phase if phased authorization is enabled.
3. 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.
4. Click **Update**.

5.6.2 Manually assigning static authorizers

To assign static authorizers to a managed group:

1. Navigate to the ***Managed group information*** page (p20).
2. Click the **Authorization** tab.
   Select a phase if phased authorization is enabled.
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.

5.6.3 Assigning authorizers by user class

To assign authorizers to a managed group based on user class:

1. Navigate to the ***Managed group information*** page (p20).
2. Click the **Authorization** tab.
   Select a phase if phased authorization is enabled.
   The **Users must be in the following user classes** table allows you to define membership criteria.

3. To define membership criteria:
   - Select existing user classes: Click **Select...** and enable the checkboxes for the user classes you want to add, then click **Select**.
   - Create new user classes: Click **Add new...**.
4. Configure **Participant mapping** for each user class that you add.
   Select and create user classes until you have defined membership.
5. If your membership criteria includes multiple user classes, define whether users are required to match **All of the user classes** or **Any of the user classes**.

Removing users from membership

To remove users from membership, you can:

- Edit user classes to change the participants.
- Delete user classes from the membership criteria.
  1. Navigate to the membership criteria page where user classes are listed.
  2. Enable the checkbox next to the user classes you want to delete.
  3. Click **Delete**.

5.6.4 Using group owners as authorizers

Rather than assigning authorizers manually, you can configure *Hitachi ID Bravura Group* to automatically add group owners as authorizers. *Bravura Group* determines group owners using:

- The **`idtrack`** utility. This program can detect:
  - The group owner
    Group owners can be either a single user or a group. If a group owner is a group, and the group owner is assigned as an authorizer, then all its members and its child group's members will be added as group authorizers.
  - The users added to and removed from the group
  - Which accounts were added and deleted
  - Which groups have been added and deleted

  See idtrack in the *Reference Manual* for details.
- The network resource management plugin. This plugin determines group owners by examining the group's configuration on the target system.
- The group owners selection plugin. This plugin is used in addition to the resource management plugin. It can:

  - Replace the assigned owners.
  - Add additional owners.
  - Set owners for resources that have no owners assigned.

Before you begin:

- Ensure that the **Minimum number of authorizers** (p23) is greater than 0.
- Ensure that all potential group owners have email addresses.
- Set the **Managed group/Network resource target type** for the target system on which the group resides.

  This setting determines the network resource management plugin to run. See Target system options for details.

To configure *Bravura Group* to automatically add group owners as authorizers:

1. Navigate to the ***Managed group information*** page (p20).
2. Enable the **Automatically add group owners as authorizers** checkbox.
3. Set other parameters as required (p21).
4. Click **Manage** if the group is not already managed; otherwise, click **Update**.

Generally, *Bravura Group* determines the owners of a particular group by examining the group's configuration on the target system. This is done in real time using a network resource plugin such as **`nrsmb`** or **`nrcifs`**.

You can also write a group owner selection plugin to do the following:

- Replace the assigned owners returned by **`nrsmb`** or **`nrcifs`**.
- Add additional owners for the user to select.
- Set owners for resources that have no owners assigned.

Any owner returned by the plugin will have the same requirements of an authorizer. If the owner is new, *Bravura Group* adds the owner as a *static authorizers* and maps him to the managed group object.

Note: Group owners are not necessarily the users who will authorize requests for a group. The **IDSYNCH AUTH CRITERIA MOD PLUGIN** may be configured to alter the list of authorizers at the time that the Workflow Manager Service processes a request.

To use a group owner selection plugin:

1. Click **Workflow** → **Options** → **Plugins**.

2. Type the name of the plugin program or PSLANG script in the **IDACCESS OWNERS PLUGIN** field.
3. Click **Update**.

See Group owner selection in the *Reference Manual* to learn how to write your own plugin.

5.7 Tracking changes to group membership

You can configure *Hitachi ID Bravura Group* to track changes to group membership in managed groups on Microsoft Active Directory and LDAP Directory Service target systems.

When the **Track changes** option is configured for a group, *Bravura Group* compares the new group membership information, extracted from the target system during auto discovery, with data in the *Bravura Group* database, and creates a diff set. *Bravura Group* can configured to propagate changes on target systems or submit requests via *Bravura Group*'s workflow system.

You can configure the default for this setting with **AUTO TRACK MGROUP** in the **Resources** → **Options** menu. If the setting is enabled, new groups that are managed will use this setting unless overridden.

You can also set this option on the target system information page so that all groups on the target system are tracked.

The tracked changes are viewable in reports as part of each user's profile history.

5.7.1 Handling out-of-band changes

Out-of-band changes happen when a user or a group is added to or deleted from a managed group outside of *Hitachi ID Bravura Group*. Tracking changes to group membership allows *Bravura Group* to monitor managed groups for out-of-band additions or deletions, then automatically submit a request undo or redo the change via the workflow system.

> **Note:** When out-of-band settings are first configured, users or groups who are already managed group members are not detected as out-of-band additions.

To act on out-of-band changes to group membership in a managed group:

1. Navigate to the ***Managed group information*** page (p20) for the group.
2. Enable the **Track changes** checkbox.
3. From the drop-down list, select an action to:
   - **Detect out-of-band additions and automatically generate a workflow request**
   - **Detect out-of-band deletions and automatically generate a workflow request**

The default behavior is to take no action. *Bravura Group* can either submit a request to undo the change, or undo the change then submit a request to redo the change via the *Bravura Group* workflow system.

4. Set **Authorization for joining group** and **Authorization for leaving group** as appropriate.

   These settings determine whether a change request be authorized.

5. Click **Update**.
6. Configure group-level authorization (p22).
7. Click **Manage the system** → **Workflow** → **Options** → **Automation**.
8. Type a profile ID for the **OOB REQ GROUPJOIN REQUESTER** and **OOB REQ GROUPLEAVE REQUESTER** .

   This will be the ID of the requester on all automatically-submitted requests to add or remove users or groups from managed groups.

9. Optional: Configure event actions for out-of-band changes to managed groups. See Automated workflow events that launch interface programs for details.
10. Run auto discovery.

When auto discovery is finished, configuration is complete. Now if any out-of-band changes are made to group membership, then they will be detected the next time auto discovery is run. When an out-of-band addition to the group is detected:

- A request is generated for the out-of-band user or group or join or leave the group. This request is sent to the group authorizer.
- An email is sent to the recipient (out-of-band user).
- An email is sent to the group authorizer.

The content of these email messages can be customized using the following tags:

- EM_WORKFLOW_REQ_INITIAL_AUTHORIZER_NEEDAUTHOOB_CONTENT_PRIMARY – This is the email body that is sent to the group authorizer when a request is generated to add or remove the out-of-band user or group.
- EM_WORKFLOW_REQ_INITIAL_RECIPIENT_OOB_ADD_NOTICE
- EM_WORKFLOW_REQ_INITIAL_RECIPIENT_OOB_ADDBACK_NOTICE
- EM_WORKFLOW_REQ_INITIAL_RECIPIENT_OOB_DEL_NOTICE
- EM_WORKFLOW_REQ_INITIAL_RECIPIENT_OOB_DELBACK_NOTICE
- EM_WORKFLOW_REQ_INITIAL_RECIPIENT_OOB_NESTED_GROUP_ADD_NOTICE
- EM_WORKFLOW_REQ_INITIAL_RECIPIENT_OOB_NESTED_GROUP_ADDBACK_NOTICE
- EM_WORKFLOW_REQ_INITIAL_RECIPIENT_OOB_NESTED_GROUP_DEL_NOTICE
- EM_WORKFLOW_REQ_INITIAL_RECIPIENT_OOB_NESTED_GROUP_DELBACK_NOTICE

See also:

- See Customizing workflow email using the *Manage the system* (PSA) module for details on email customization.
- See Automated workflow events that launch interface programs for details on available event actions for out-of-band changes to managed groups.

5.8 Managing invalid groups

If a group that is managed by *Hitachi ID Bravura Group* is deleted from the target system, then the group is listed as invalid the next time auto discovery runs. *Bravura Group* remembers the group until it is restored, or until *Bravura Group* automatically stops managing the group. If a group is restored, then the group members are also restored.

> **Note:** Depending on the target system, adding a new group with the same name may not necessarily restore the group.

Once a group is listed as invalid, *Bravura Group* automatically stops managing the group after 30 days by default. When *Bravura Group* automatically stops managing a group, it is removed from all roles, segregation of duties (SoD) rules, and pre-defined requests.

You can control the amount of time that a group can be listed as invalid by changing the value of the **KEEP INVALID MANAGED GROUP DAYS** system variable.

Bravura Group administrators are notified when:

- A managed group becomes invalid
- A managed group is restored
- *Bravura Group* automatically stops managing a group

The invalid status of a managed group is visible to product administrators and to requesters. Requesters are still able to create requests for invalid managed groups, but the requests cannot be completed until the group is restored.

5.8.1 Managed group options for invalid groups

The following managed group options can be accessed from **Manage the system** → **Resources** → **Options**:

Table 5.4: Managed group options

Option	Description
KEEP INVALID MANAGED GROUP DAYS	Specify the number of days that must pass once a managed group becomes invalid before *Hitachi ID Bravura Group* automatically stops managing the group. The default value is 30. If undefined, then data is kept indefinitely.

The following managed group events apply to all modules and can be accessed from **Manage the system** → **Resources** → **Options**:

Table 5.5: Managed group events that launch interface programs

Option	Description
KEEP INVALID MGROUP INVALIDATED	A managed group disappears from the target system.
KEEP INVALID MGROUP RESTORED	A managed group is restored on the target system.
KEEP INVALID MGROUP UNMANAGED	*Bravura Group* automatically stops managing a managed group.

See Event Actions (Exit Traps) for more information about event configuration.

5.9 Deleting unknown objects

Group members and group owners are considered unknown when:

- They are not in the same OU as that of the managed group, or;
- They are of a type other than account or group; that is, contact or computer object.

Hitachi ID Bravura Group detects unknown object types during auto discovery. You can view them using the ***Membership*** report. Click **Manage reports** → **Reports** → **Reports** → **Roles and Groups** → **Membership**. In the **Membership type** field, select "Unknown object".

Unknown objects can be deleted via the *Bravura Group* API and the Workflow Manager Service (idwfm) using:

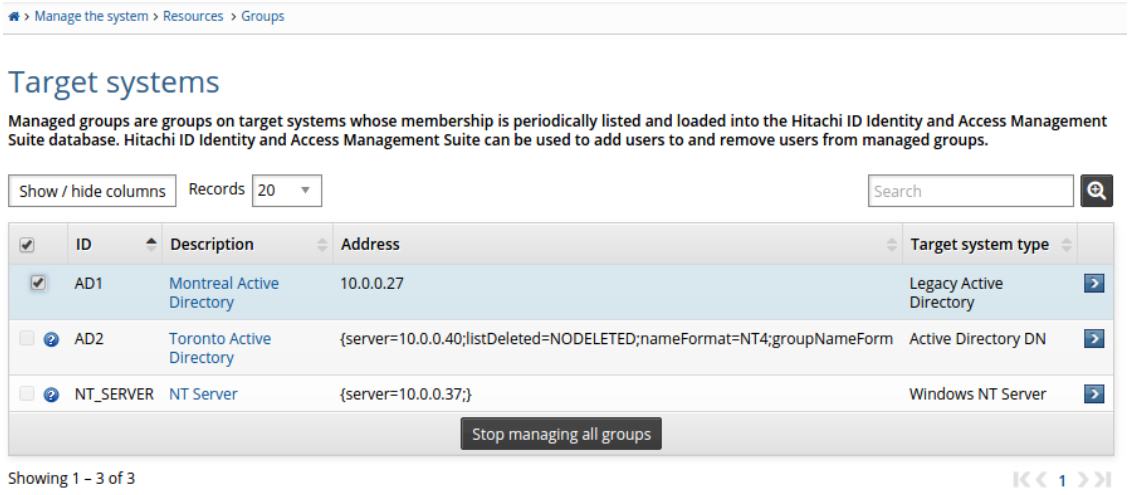
- Pre-defined requests _GROUP_DELETE_MEMBERS_ and _GROUP_DELETE_OWNERS_
- Workflow operation codes GRBD and GOOD

See the *Bravura Security Fabric* Remote API manual for more information about using the API.

5.10 Stopping management of all groups on a target system

You can use the ***Target systems*** page to stop managing all groups, in a single click, from all the selected targets:

1. Click **Manage the system** → **Resources** → **Groups**.
   Hitachi ID Bravura Group displays a list of existing target systems.
2. Select the checkboxes for the target systems on which you want to stop managing groups.
3. Click **Stop managing all groups**.



Note: In cases where the managed groups are being used elsewhere (roles, templates, and so on) *Bravura Group* displays an error message reporting the number of groups that has failed to be unmanaged.

Part III

USING GROUP MANAGER

Viewing / Updating Groups 6

The *Groups* app allows users to request changes to group membership, or to create or update groups if they have assigned privileges.

Users can request to join or leave groups. Group owners can also:

- Delete groups
- Update group attributes
- Update owners
- Update membership (accounts, child groups, parent groups)

See also:

- Users with appropriate permission can use the *Groups* app to create groups on target systems. See Creating Groups.

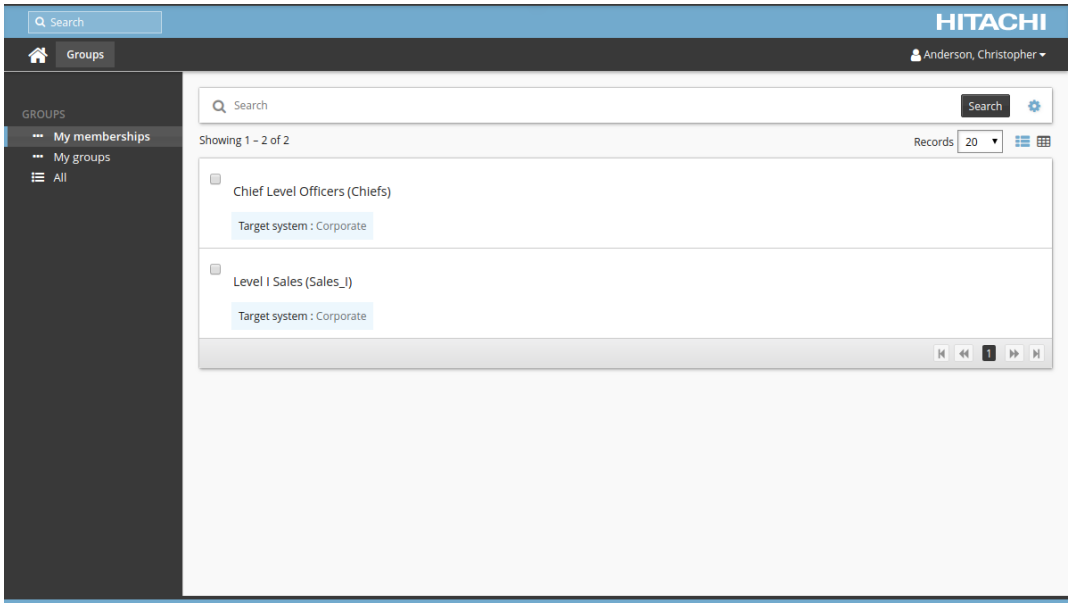
6.1 Getting started: Viewing groups

You can access the *Groups* app via the self-service menu. You may also receive email notification containing a link to view a particular group.

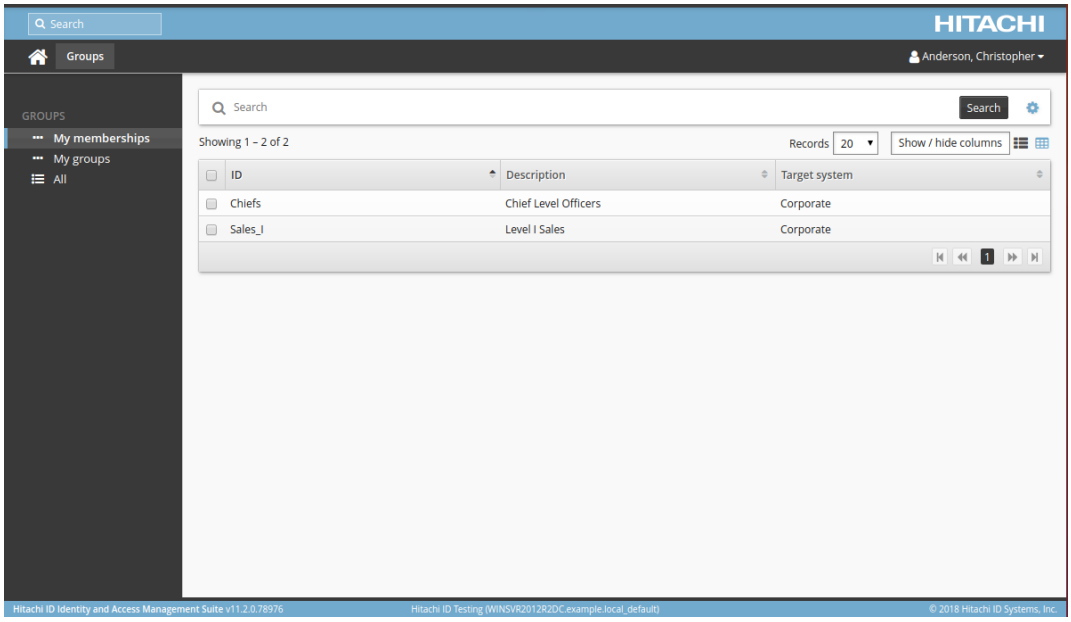
To access the *Groups* app from the self-service main menu:

1. Click **Groups**.

   Your group memberships are shown in *Card view* by default:



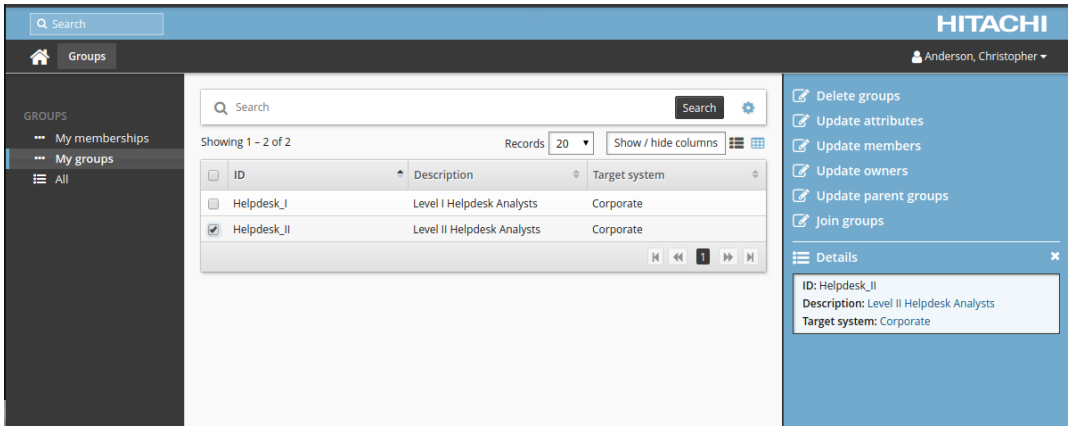
Click the icon in the top left corner of the middle panel to switch to *Table view*:



Click **My groups** in the Filter panel to view groups that you own.

Click **All** in the Filter panel to view all groups managed by *Hitachi ID Bravura Group*.

2. Select one or more groups from the Results panel, then select an action from the Actions panel. The actions available depend on the groups selected and the permissions of the user.

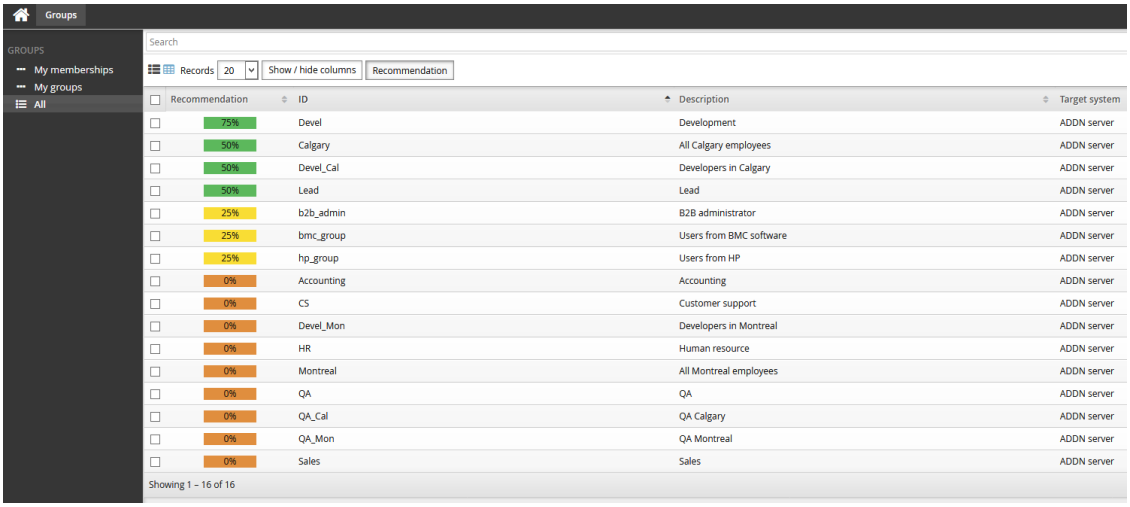


6.1.1 Group recommendations

Product administrators can configure the *Groups* app so that users see recommendations of group memberships to add or delete, based on consistency among the user's peer group.

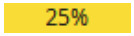
A *peer group* is a group of users with some attribute in common; for example, users working at the same location or department, or having the same manager.

When configured, users show or hide the recommendations by clicking the **Recommendations** button in the middle panel. Recommendations are visually represented by a color bar with a number stating the percentage of peers who are members. This can help the user to decide whether to add or delete membership.

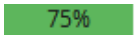


In the above screenshot:

0% Membership is not recommended. None of the user's peers are members.



Membership is recommended. 25% of the user's peers are members.



Membership is strongly recommended. 75% of the user's peers are members.

6.2 Changing your group memberships

Self-service users can use the *Groups* app to request to join or leave groups managed by *Hitachi ID Bravura Group*.

6.2.1 Use case: Join groups

The following procedure describes how to use the standard **Join groups** request.

To add yourself to a group:

1. Navigate to the *Groups* app (p32).
2. Click **All** in the Filter panel.
3. Select a group from the Results panel.
4. Click **Join groups**.
   Hitachi ID Bravura Group displays a confirmation dialog box.
5. Click **OK** to confirm the action.
   Relevant authorizers are notified to review the request if necessary.

6.3 Updating group attributes

Group owners can use the *Groups* app to update the group description and other attributes configured by product administrators.

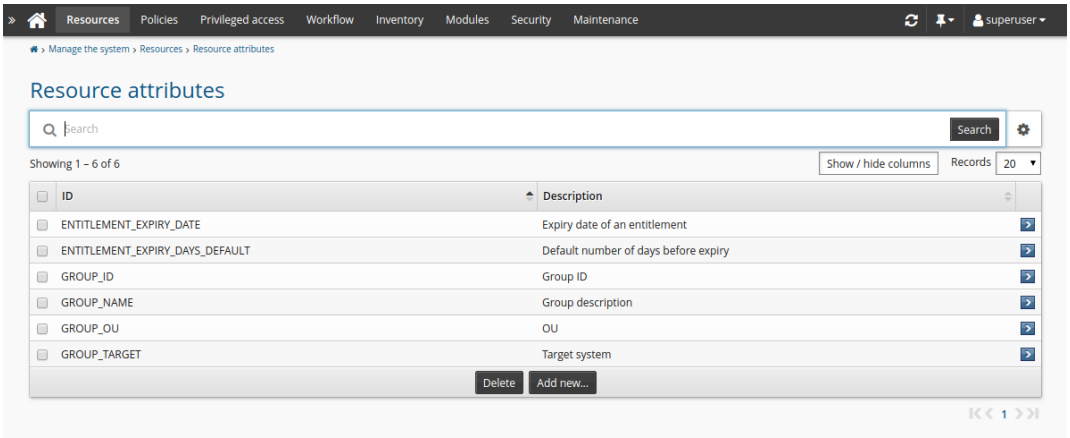
6.3.1 Use case: Adding and updating group attributes

In this use case, a product administrator adds a group attribute that can be updated by group owners using the standard **Update attributes** request.

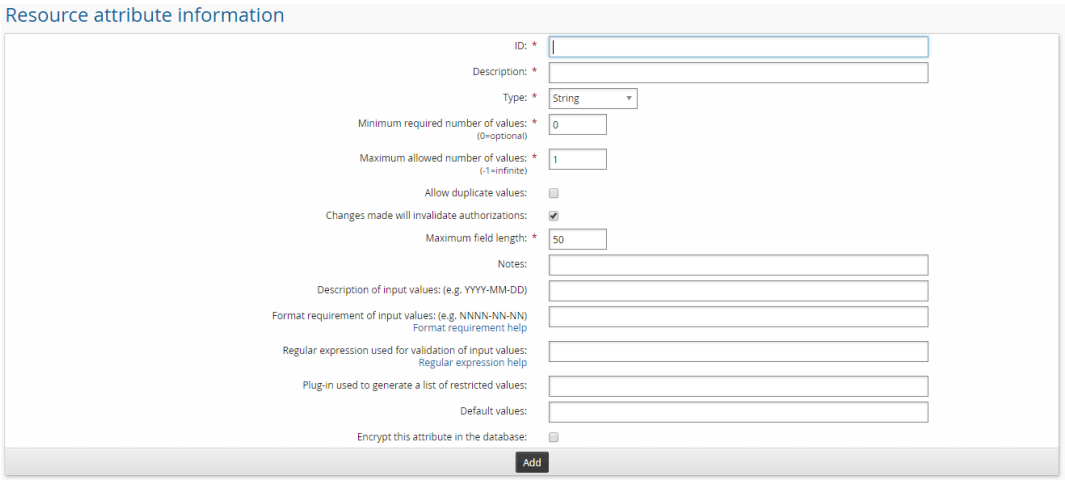
Add a group attribute

To add a group attribute:

1. As a product administrator, click **Manage the system** → **Resources** → **Resource attributes**.



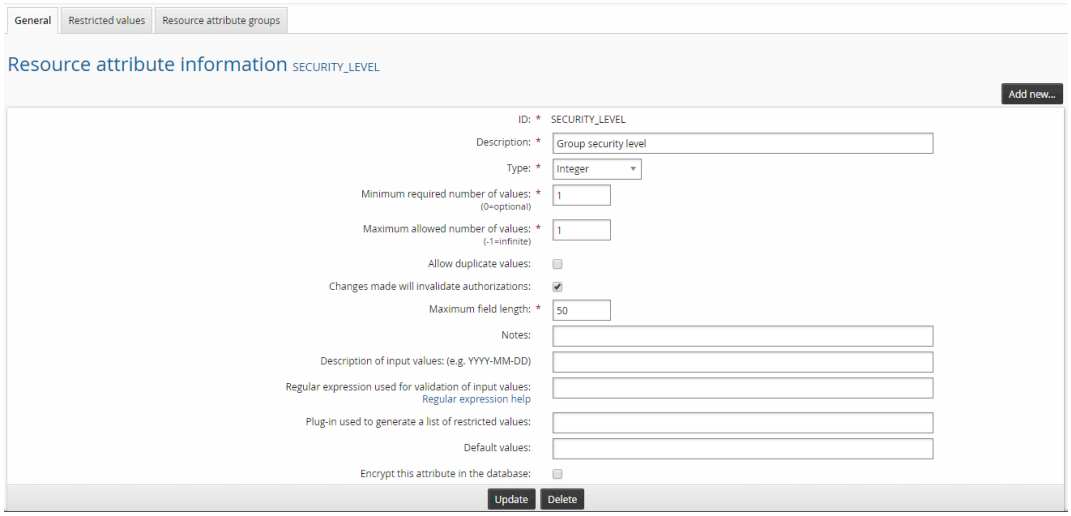
2. Click **Add new...**



3. Enter values as follows:

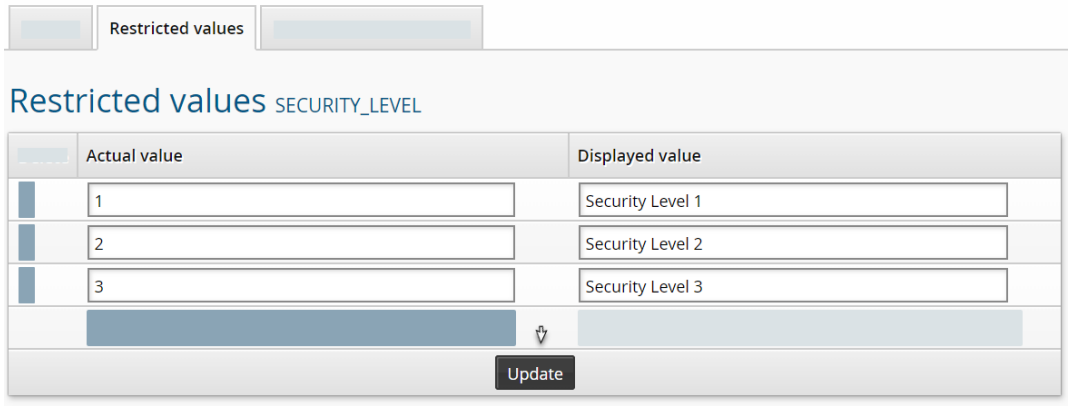
   ID: SECURITY_LEVEL
   Description: Group security level
   Type: Integer
   Minimum required number of values: 1
   Maximum allowed number of values: 1

4. Click **Add**.



5. Add three restricted values:

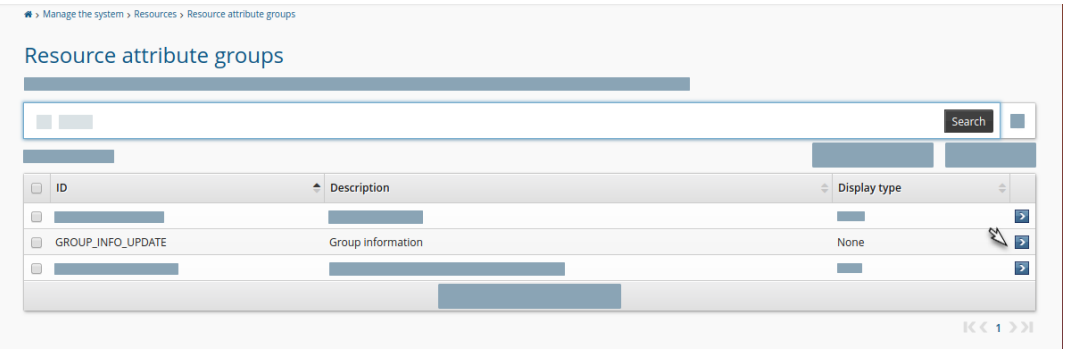
   (a) Click the **Restricted values** tab.
   (b) Type `1` in the **Actual value** and **Displayed value** fields, then click **More**.
   (c) Type `2` in the new **Actual value** and **Displayed value** fields, then click **More** again.
   (d) Type `3` in the new **Actual value** and **Displayed value** fields.
   (e) Click **Update**.



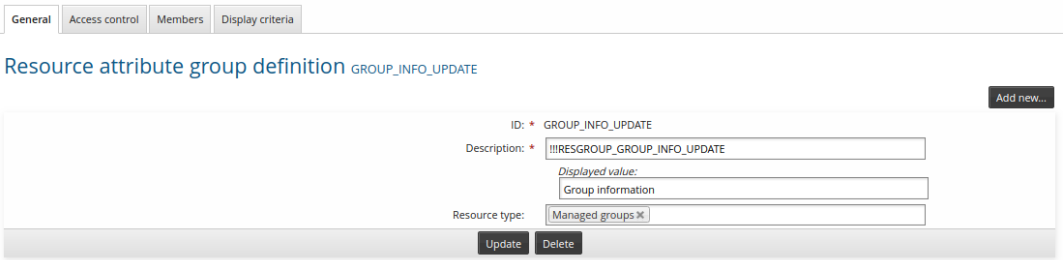
Set attribute access controls

To set access controls for the new attribute, add it to an attribute group:

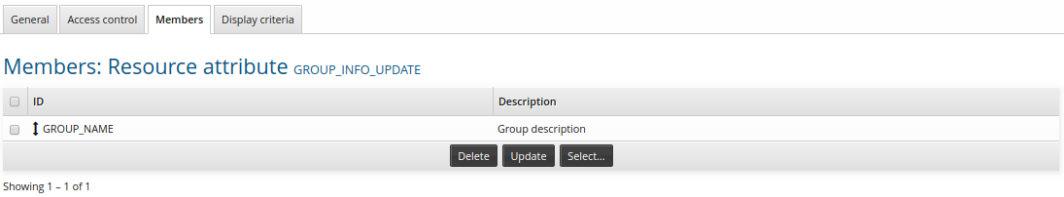
1. As a product administrator, click **Manage the system** → **Resources** → **Resource attribute groups**.



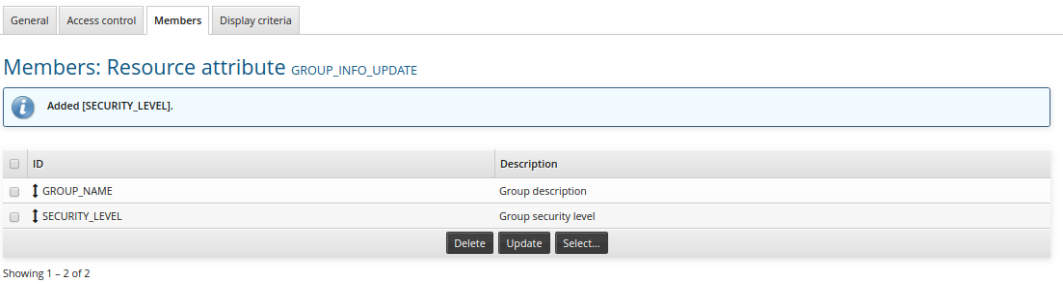
2. Select **GROUP_INFO_UPDATE**.
   Group resource attributes that are members of this group can be updated by group owners.



3. Click the **Members** tab.



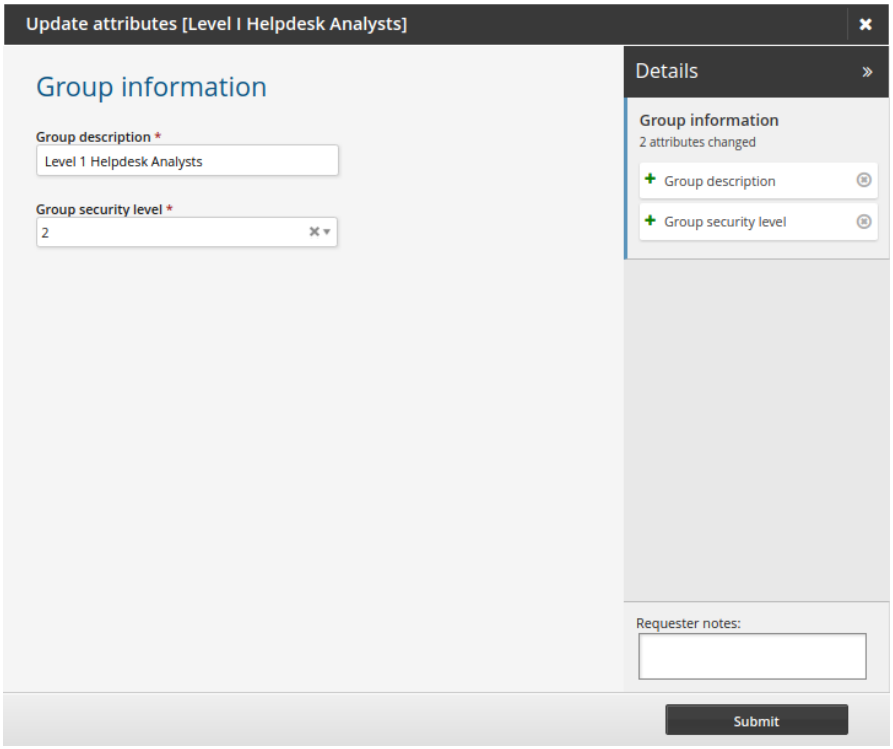
4. Click **Select...**
5. Select the checkbox for the **SECURITY_LEVEL** attribute you added above, then click **Select**.



Update group attributes

To update group attributes as a group owner:

1. Navigate to the *Groups* app (p32).
2. Click **My groups** in the Filter panel.
3. Select a group from the Results panel.
4. Click **Update attributes**.



5. Select a **Group security level**.
6. Click **Submit**.
   Relevant authorizers are notified to review the request if necessary.

6.4 Deleting groups

Group owners can use the *Groups* app to delete groups that they own.

To delete a group:

1. Navigate to the *Groups* app (p32).
2. Click **My groups** in the Filter panel.
3. Select a group from the Results panel.
4. Click **Delete group**.
   Hitachi ID Bravura Group displays a confirmation dialog box.
5. Click **OK** to confirm the action.
   Relevant authorizers are notified to review the request if necessary.

6.5 Updating group members

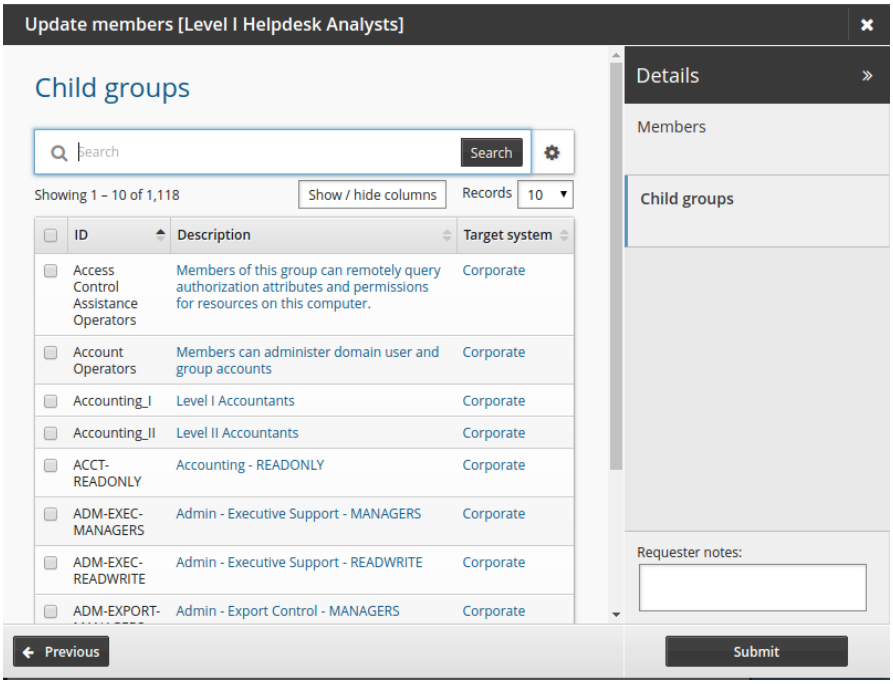
Group owners can use the *Groups* app to update group members; this includes adding or removing users and child groups.

Owners can select multiple groups then add or delete multiple accounts or groups as members. Note that when multiple groups are selected, there are separate requests for adding or deleting members.

6.5.1 Use case: Adding a child group

The following procedure describes how a group owner can add a child group to another group using the standard **Update members** request. To include a group as a member of another group:

1. As a group owner, navigate to the *Groups* app (p32).
2. Click **My groups** in the Filter panel.
3. Select a group from the Results panel.
4. Click **Update members**.
5. From the details panel, click **Child groups**.

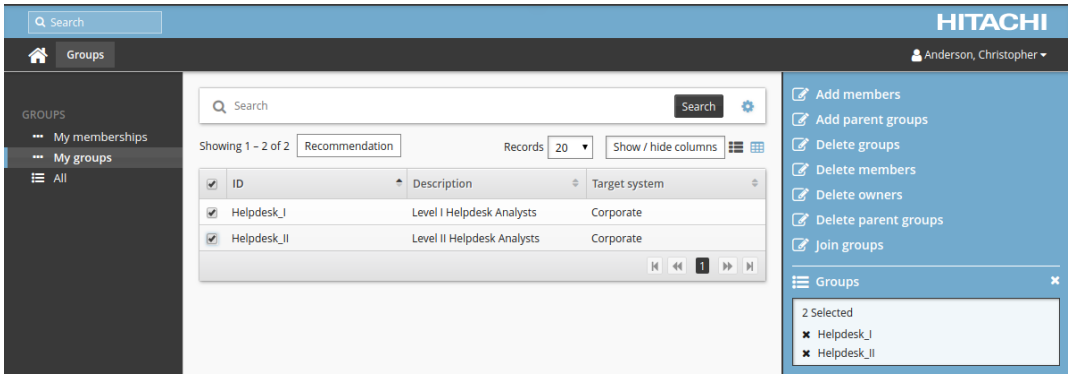


6. Search for and select a child group.
7. Click **Submit**.
   Relevant authorizers are notified to review the request if necessary.

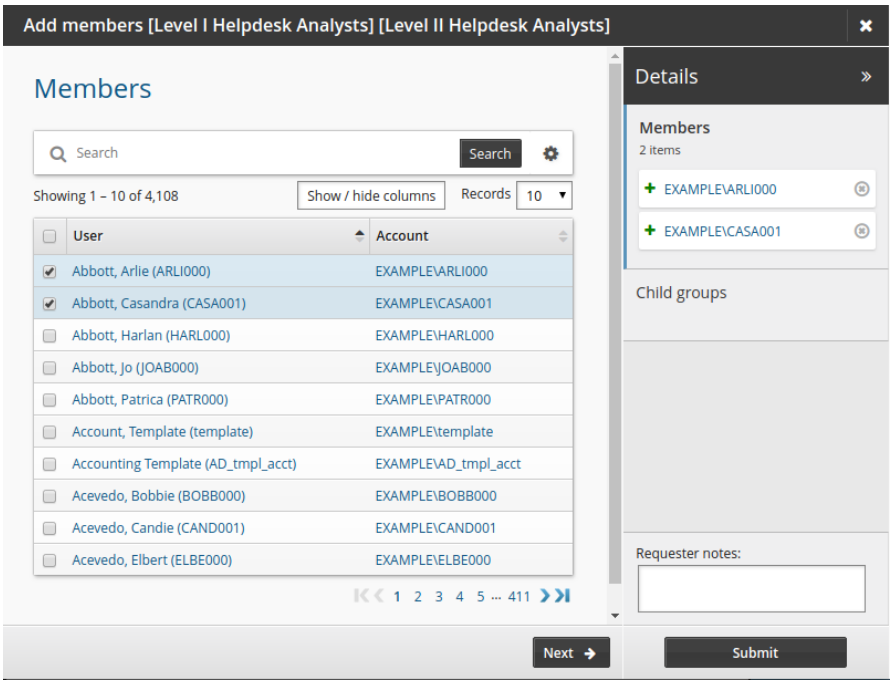
6.5.2 Use case: Adding members to multiple groups

The following procedure describes how a group owner can add account members to multiple groups using the standard **Add members** request. To include accounts as members of other groups:

1. As a group owner, navigate to the *Groups* app (p32).
2. Click **My groups** in the Filter panel.
3. Select multiple groups from the Results panel.



4. Click **Add members**.



5. Select checkboxes for members you want to add.
6. Click **Submit**.

   Relevant authorizers are notified to review the request if necessary.

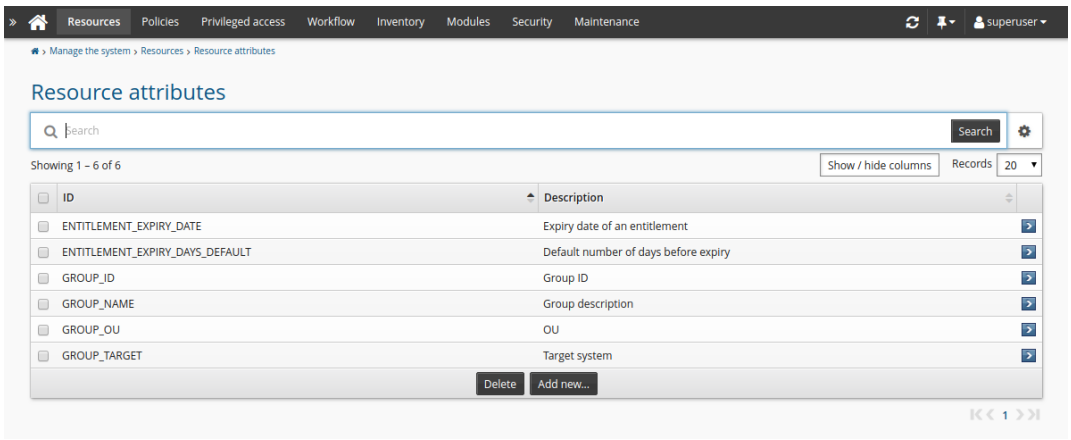
6.5.3 Use case: Update group members and attributes

In this use case, a product administrator adds a group attribute that can determine when membership of a group expires, and modifies the **Update members** request so that users can join a group and update a group attribute at the same time.

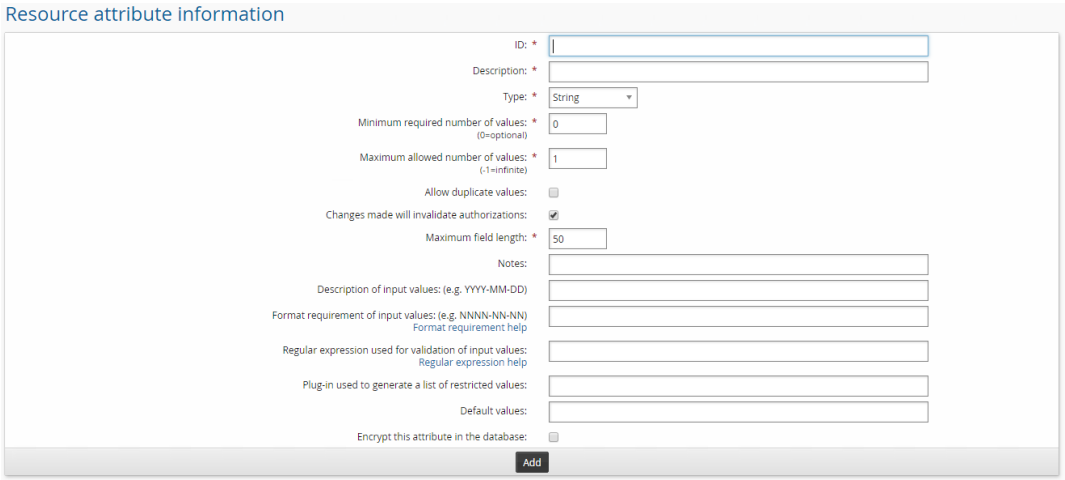
Add a group attribute

To add a group attribute:

1. As a product administrator, click **Manage the system** → **Resources** → **Resource attributes**.



2. Click **Add new...**



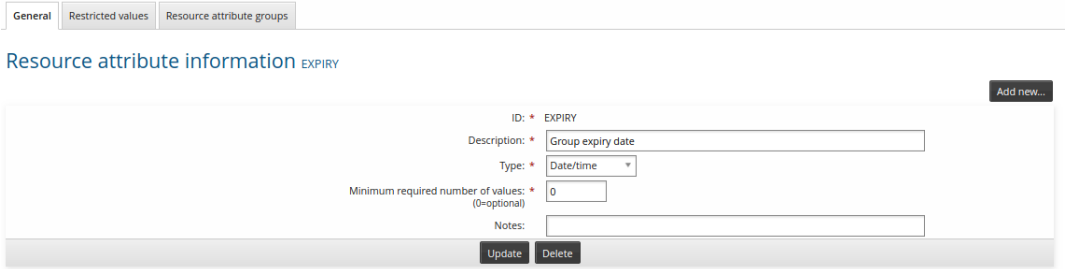
3. Enter values as follows:

   ID: EXPIRY

   Description: Group expiry date

   Type: Date/time

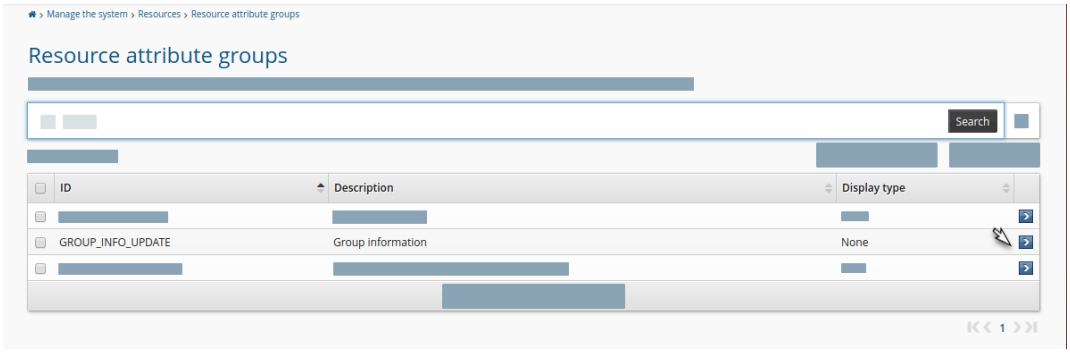
4. Click **Add**.



Set attribute access controls

To set access controls for the new attribute, add it to an attribute group. In this case, create a new group:

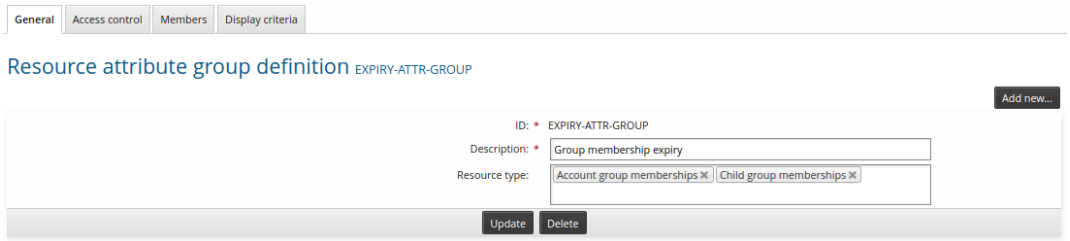
1. As a product administrator, click **Manage the system** → **Resources** → **Resource attribute groups**.



2. Click **Add new...**
3. Enter the following values:

   ID EXPIRY-ATTR-GROUP
   Description Membership attribute group
   Resource type Account group memberships, Child group memberships

4. Click **Add**.

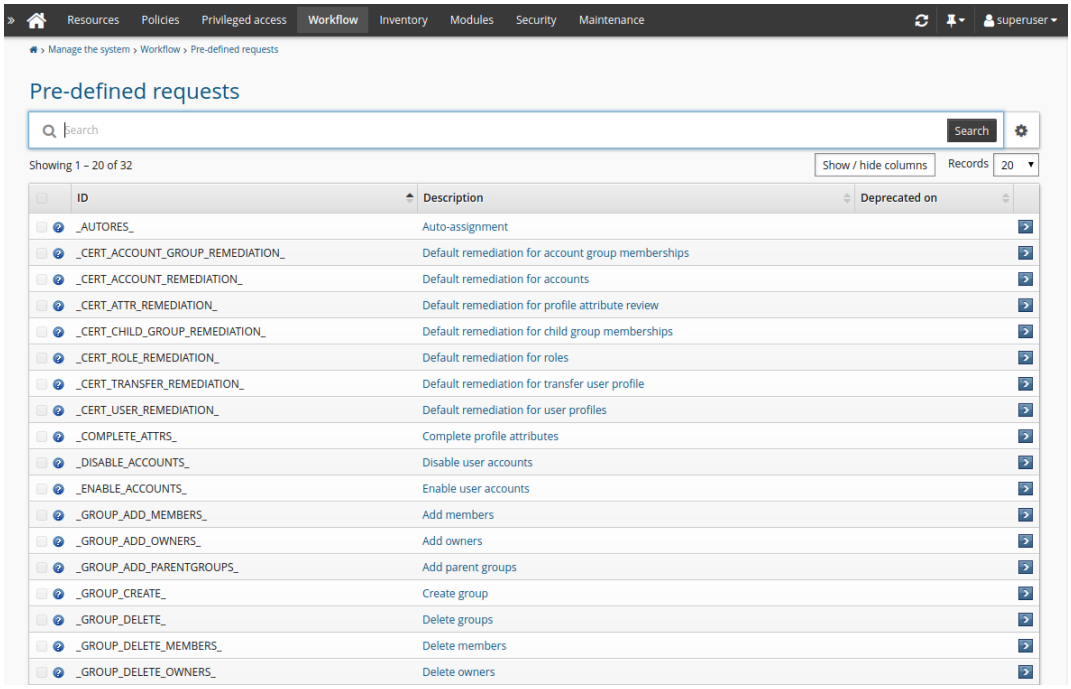


5. Click the **Access control** tab.
6. Click the **Allow read** and **Allow write** checkboxes for ALLUSERS then click **Update**.
7. Click the **Members** tab.
8. Click **Select...**
9. Click the checkbox for **EXPIRY** then click **Select**.

Add the attribute group to the 'Update members' request

To add the new attribute group to the **Update members** pre-defined request:

1. As a product administrator, click **Manage the system** → **Workflow** → **Pre-defined requests**.



2. Select **_GROUP_UPDATE_MEMBERS_**.

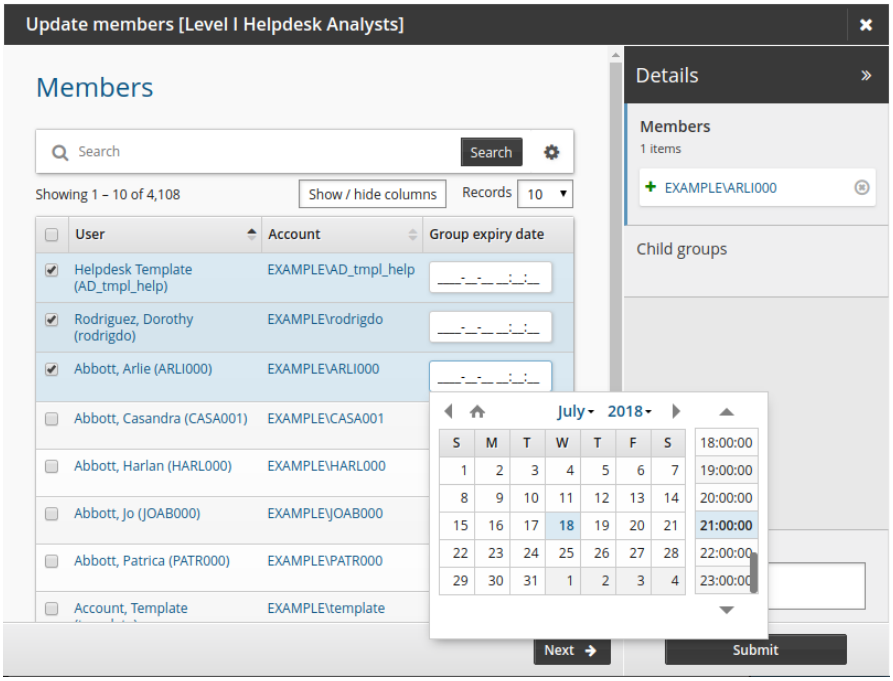
   By default, this group allows "Assign group", "Revoke group", "Add child group", and "Delete child group" operations.

3. Click the **Attributes** tab.
4. Click **Select...**
5. Click the checkbox for **EXPIRY-ATTR-GROUP** then click **Select**.

Update a group's membership

To request an update to a group's membership:

1. As a group owner, navigate to the *Groups* app (p32).
2. Click **My groups** in the Filter panel.
3. Select a group from the Results panel.
4. Click **Update members**.
5. Select a user account.



6. Select a **Group expiry date**.
7. Click **Submit**.

   Relevant authorizers are notified to review the request if necessary.

6.6 Changing group owners

Group owners can add or delete group owners, depending on the group's properties. *Hitachi ID Bravura Group* blocks requests to add multiple owners to a group if the target system only supports single-owner groups. When changing the owner of a single-owner group, you must delete the original owner at the same time as adding a new owner.

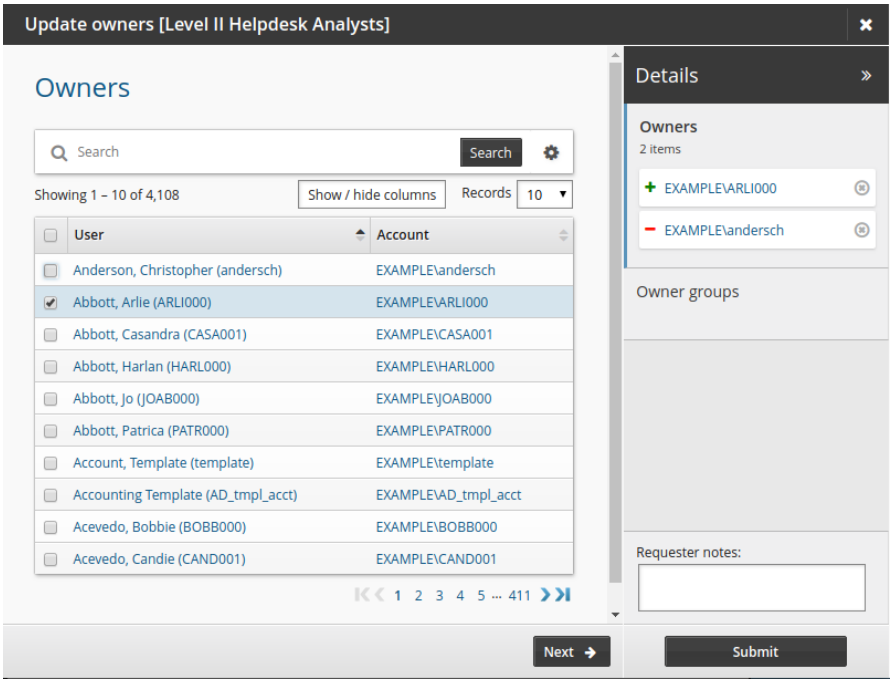
CAUTION: Ensure that you do not delete all owners of a group without adding a new owner. The *Groups* app does not allow non-owner users to add owners to groups. Depending on target system settings, groups without owners may no longer be managed by *Bravura Group*.

6.6.1 Use case: Changing an Active Directory group's owner

In this use case, the group owner removes himself and adds a new group owner using the **Update owners** request.

To change owners:

1. As a group owner, navigate to the *Groups* app (p32).
2. Click **My groups** in the Filter panel.
3. Select a group from the Results panel.
4. Click **Update owners**.
5. Deselect the checkbox of the original owner.
6. Select the checkbox of the user to be added as owner.



7. Click **Submit**.
   Relevant authorizers are notified to review the request if necessary.

6.7 Changing parent groups

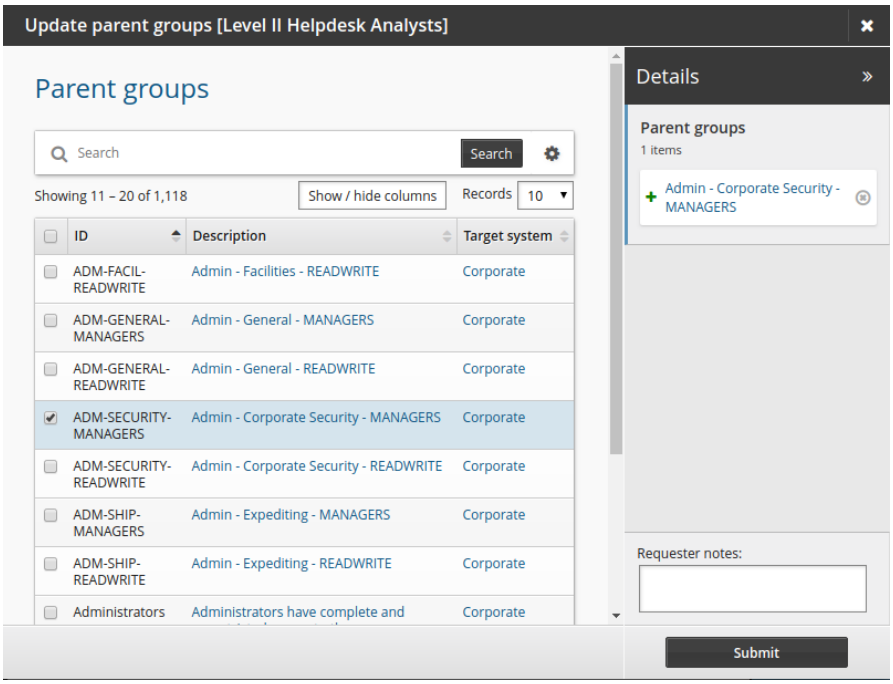
Group owners can use the *Groups* app to add or delete parent groups for a group; in effect, the owner requests group membership changes on behalf of a group.

Owners can select multiple groups then add or delete multiple groups as parent groups. Note that when multiple groups are selected, there are separate requests for adding or deleting parent groups.

6.7.1 Use case: Adding a parent group

This case describes how a user can add a parent group using the standard **Update parent groups** request. To add a parent group to a group:

1. As a group owner, navigate to the *Groups* app (p32).
2. Click **My groups** in the Filter panel.
3. Select a group from the Results panel.
4. Click **Update parent groups**.
5. Search for and select a group that you want to add as parent.



6. Click **Submit**.

   Relevant authorizers are notified to review the request if necessary.

Creating Groups 7

Users with appropriate permission can use the *Groups* app to create groups on target systems.

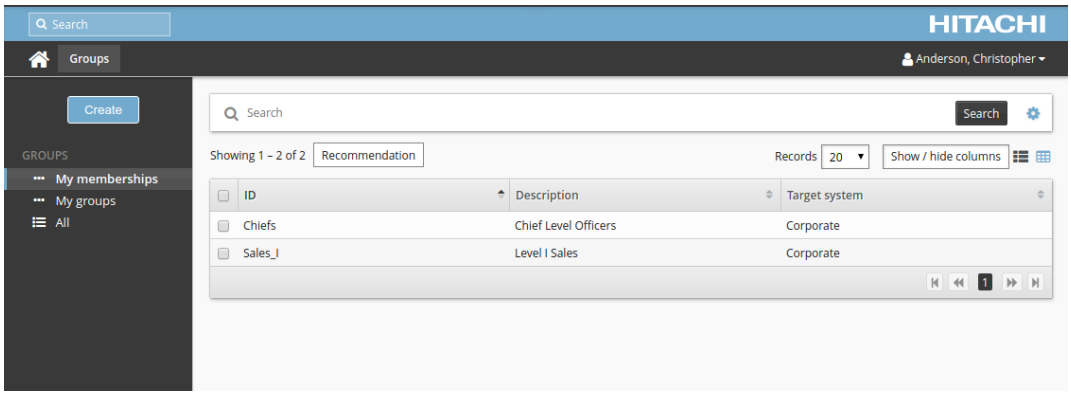
Requirements

Users who belong to the _GROUP_CREATE_USERS_ user class can use the *Groups* app to create groups.

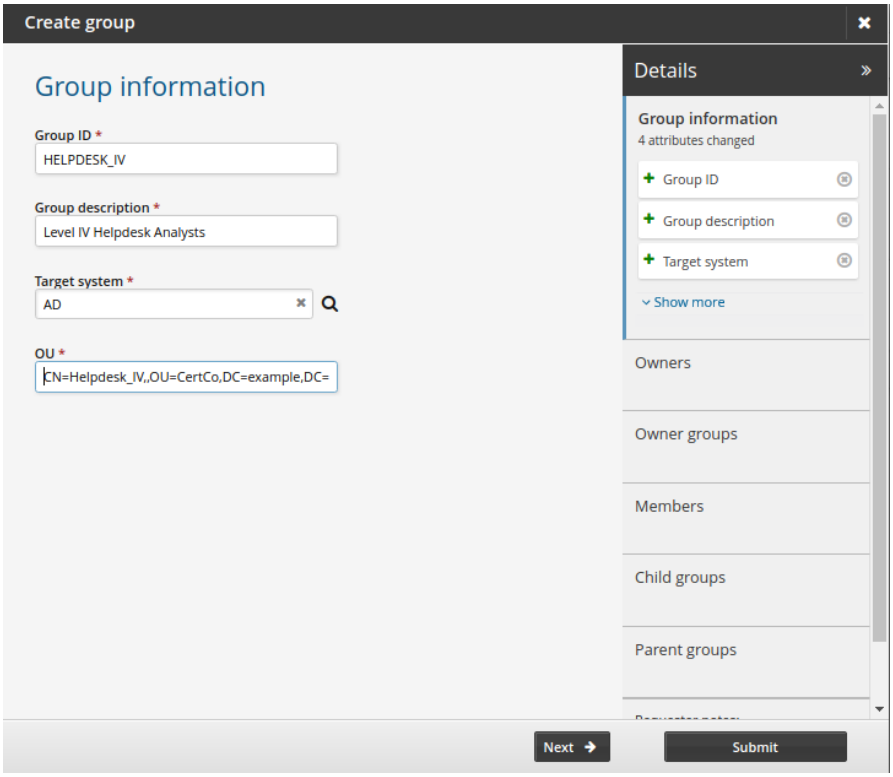
7.1 Use case: Create group

The following procedure describes how to create a group using the standard **Create group** request. To create a group:

1. From the self-service main menu, click **Groups**.



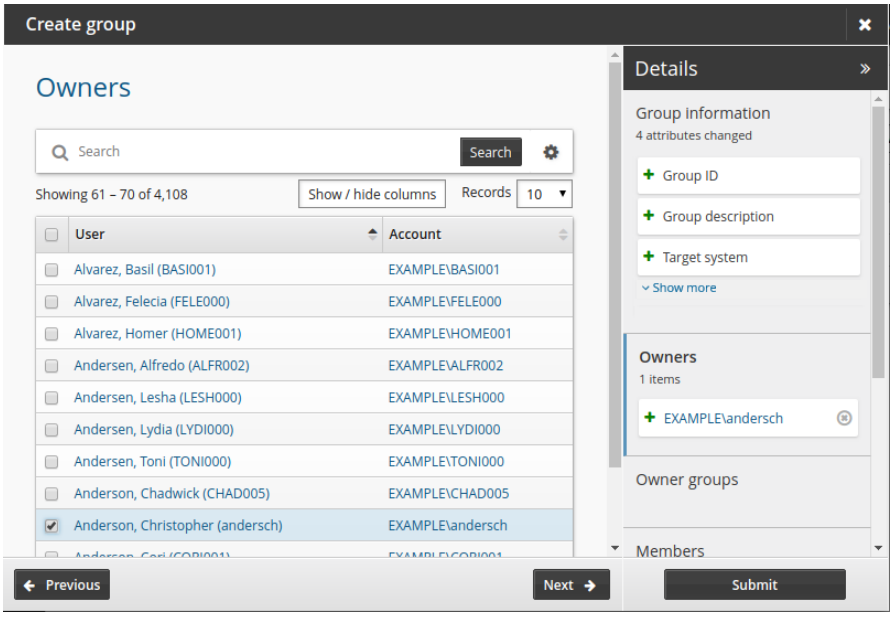
2. Click **Create** at the top of the Filter panel.
3. Define group information.



Note: In wizards, the number of entries displayed in the sidebar is limited to three. Click **Show more** to expand the list.

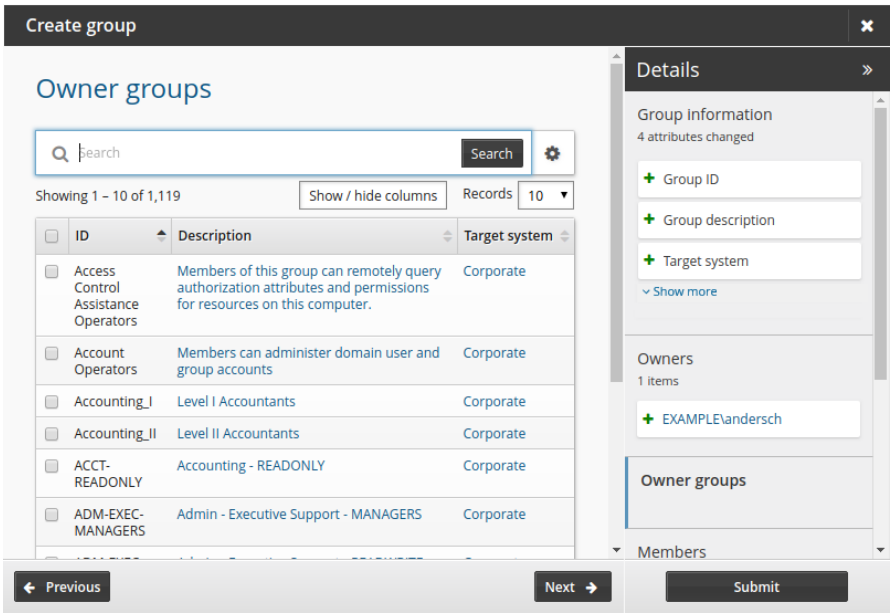
Click **Next**.

4. Define owner accounts if applicable.



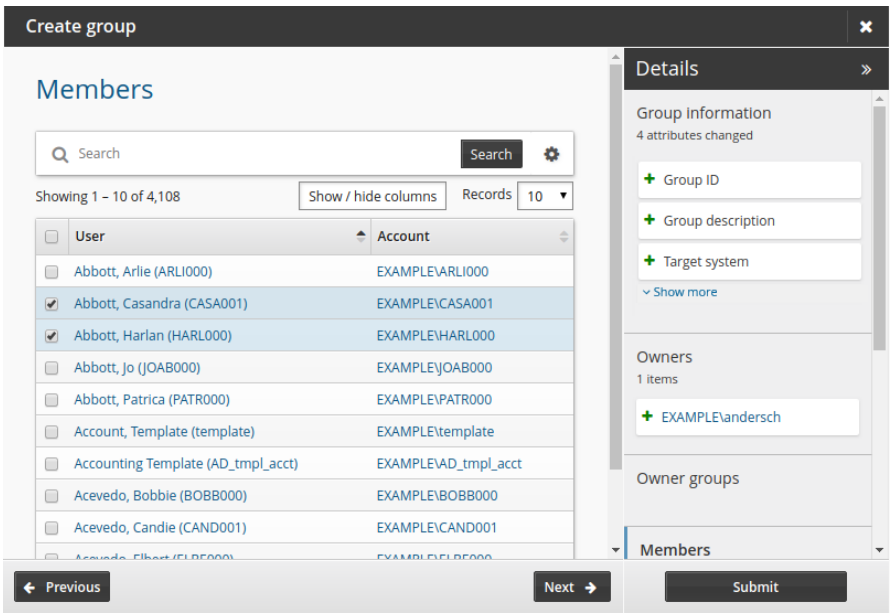
Click **Next**.

5. Define owner groups if applicable.



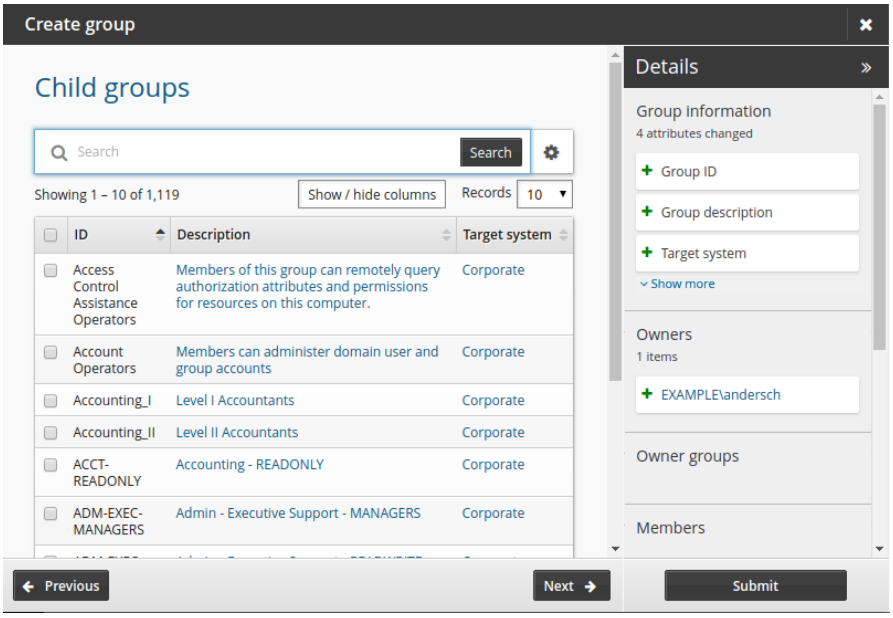
Click **Next**.

6. Define member accounts.



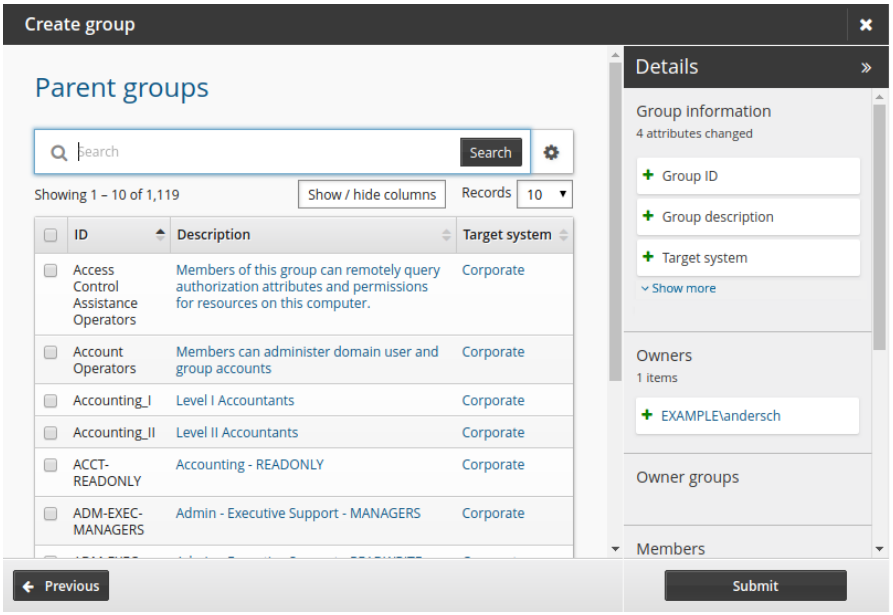
Click **Next**.

7. Define child groups.



Click **Next**.

8. Define parent groups.



9. Click **Submit**.

Requesting Access to Network Resources

8

In most IT systems, access to network resources is controlled by membership in security groups. *Hitachi ID Bravura Group*™ provides two methods that enable users to request access to network resources without the need to understand the underlying security infrastructure.

You can either log into Front-end (PSF) and use a simple web interface, or, if the Hitachi ID Systems Shell Extension is installed, you can request access by right-clicking, or double clicking on the network resource directly from your desktop.

As a user, you can request access to:

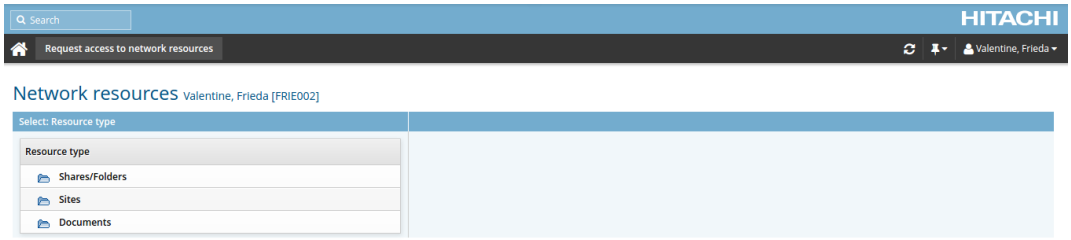
- A folder in Microsoft Active Directory.
- A printer.
- A Microsoft Office SharePoint Server resource, site, or document.

8.1 Requesting access using the *Bravura Group* interface

To request access to a network resource:

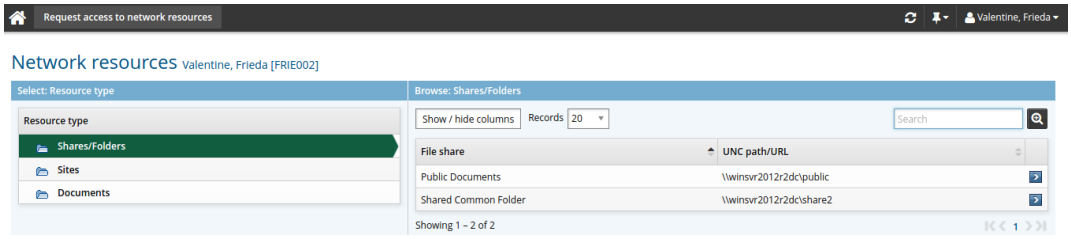
1. Log into the main menu .
2. Click **Request access to network resources** in the:
   - **My profile** section to request access for yourself.
   - **Other users** section to request access for another user.
     Hitachi ID Bravura Group displays the ***Select a user*** search page. Select the user that you want to request access for.

   Bravura Group displays a table that allows you to browse network resources. Available resource types are listed in the **Select: Resource Type** (left) column:



3. Select the appropriate resource type.

   Bravura Group displays individual resources in the **Browse: *<Selected Type>*** (right) column:



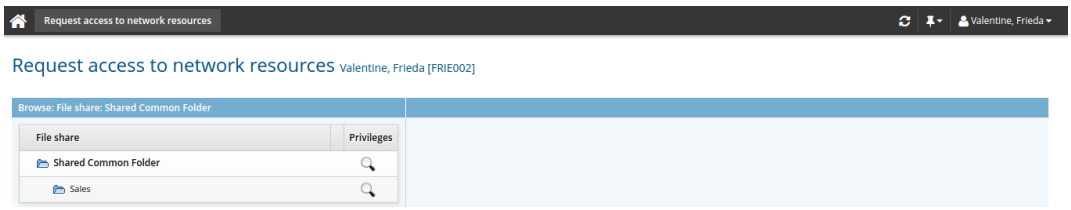
   Alternatively, you can search for the resource.

4. Select the resource you want to browse.

   If you or the selected user has multiple accounts on the target system managing the resource, you are prompted to select which account you are requesting access permissions for. If the selected resource is a:

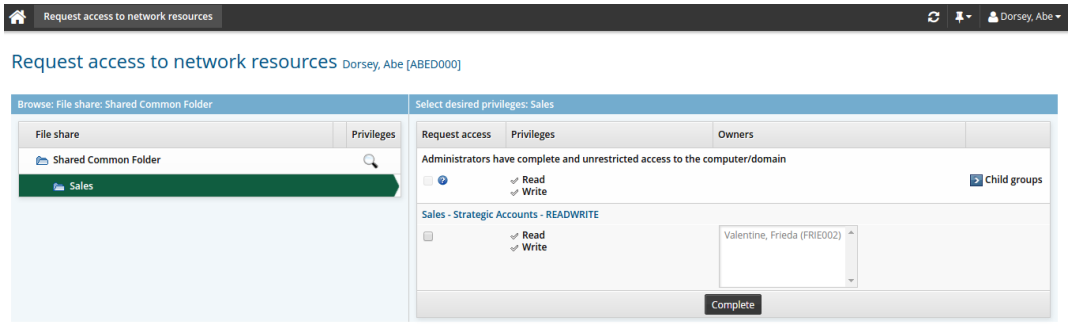
Resource type	***Bravura Group* displays . . .**
Share/folder	A tree-view of the folder including any sub-folders.
Mail distribution list	A tree-view of the directory.
Printer	A list of printer names written in the format: *<server name>-<printer name>*.
Sites	A tree-view of Microsoft Office SharePoint Server site including any sub-sites.
Documents	A tree-view of SharePoint documents including any sub-documents.

   Click the or icon to expand or collapse folders or directory containers. Depending on how *Bravura Group* is configured, you may not be able to browse subfolders of a resource unless you are already a member of a group with read access.



5. Click the privileges icon next to the resource you want to view.

   Bravura Group displays a request form in the **Select desired privileges for: <*Resource name*>** (right) column:



   If applicable, this column contains:

   - A list of groups with privileges on the resource
   - A **Request access** checkbox for each group that you can request access to.
     You cannot request access for yourself if you are already an owner or a member of the group. You cannot request access for somebody else if he or she is already an owner or a member of the group.
   - The read / write **Privileges** assigned to each group
   - The **Owners** for each group
   - A **Sub-groups** icon for groups that have member groups
     If you want to view or request access to a member group, click **Sub-groups** next to the parent group (if applicable). To return to the parent group, you can click return at the top of the page.
   - A display owners icon and a members icon for groups where you are a group owner
     These icons are *not* available when requesting resources for another user. See Managing Access to Network Resources for more information about performing operations as a group owner.

6. Select the checkboxes for the groups that you want to request access to.
7. Click **Complete**.

   Bravura Group enters the request into the authorization workflow.

8.1.1 Example: Requesting access to the Sales folder

This use case demonstrates the process a user would follow to request access to the Sales folder.

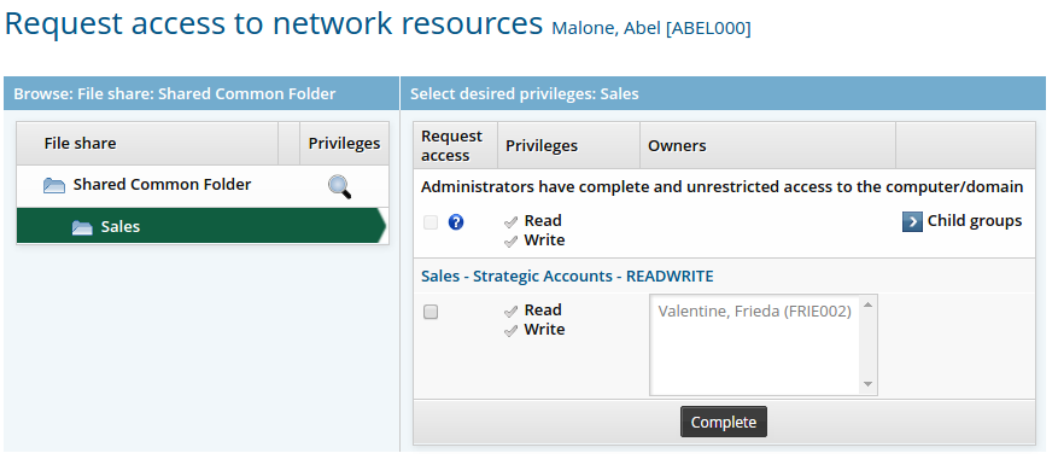
The user could request access to the appropriate group that would provide him access to the folder, however, in most instances, a user would not know which group that would be. An alternative is to set up network resources and allow the user to request access to the shared folder. *Hitachi ID Bravura Group* will do the work in the background to enable the access.

Before a user can request access to the Sales folder, the following is required:

- The Sales folder is shared on a Microsoft Windows file server.
- Groups have been used on the share to apply security, and those groups are managed by *Bravura Group*.
- An Active Directory DN target has been added, and is configured to manage network resources.
- Authorization has been set on the groups.
- The share is added to *Bravura Group* as a network resource.

To request access to the Sales folder:

1. From the main menu, click **Request access to network resources** in the **My profile** section.
2. Click **Shares/Folders**.
3. Select the Shared Common Folder.
4. Click the icon next to the **Sales** folder.
   The privileges appear on the right hand side.



5. Select **Sales-Strategic Accounts - READWRITE** and click **Complete**.
   Bravura Group enters the request into the authorization workflow.

The Workflow Manager Service (idwfm) routes the request to the selected group owner for authorization. After authorization is complete the Transaction Monitor Service (idtm) runs a connector program that adds the user to the selected group on the target system and the user will have access to the Sales folder.

8.1.2 Example: Requesting access to documents in SharePoint

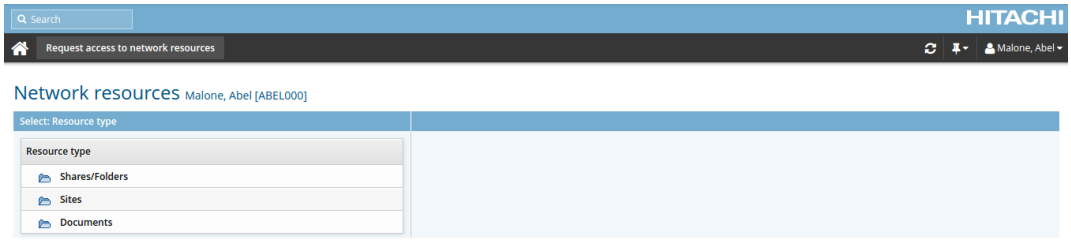
This use case demonstrates the process a user would follow to request access to a document library in SharePoint.

Before a user can be granted access to a document library in SharePoint, the following is required:

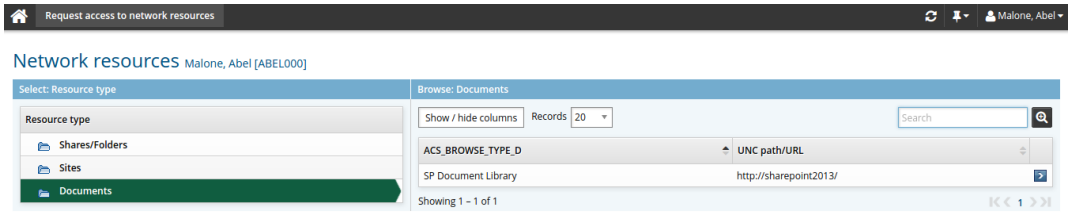
- A document library has been created in Windows SharePoint.
- At least one document exists in the document library.
- Users have at least *read* privileges to the SharePoint site. In this use case, the "domain users" Active Directory group has been added to the SharePoint Visitors group.
- The Visitors, Members, and Owners SharePoint groups all have owners.
- A SharePoint target has been added to *Hitachi ID Bravura Group*, and is configured to manage SharePoint network resources.
- The document library is added to *Bravura Group* as a network resource.

To request access to the document library:

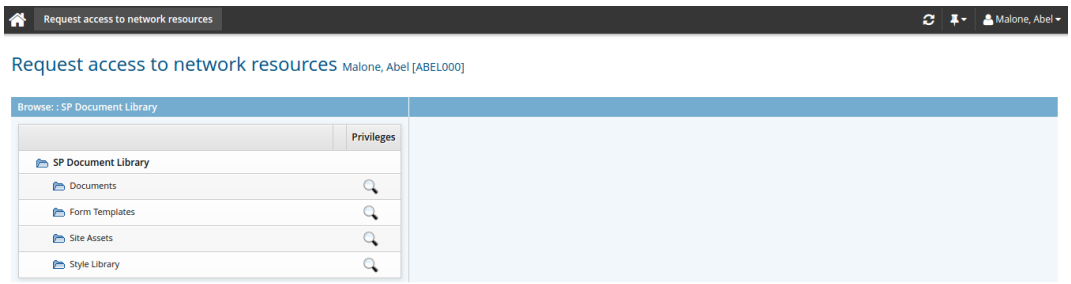
1. From the main menu, click **Request access to network resources** in the **My profile** section.
   The ***Request access to network resources*** page appears.



2. Click **Documents**.
   Bravura Group displays available document libraries on the right hand side.

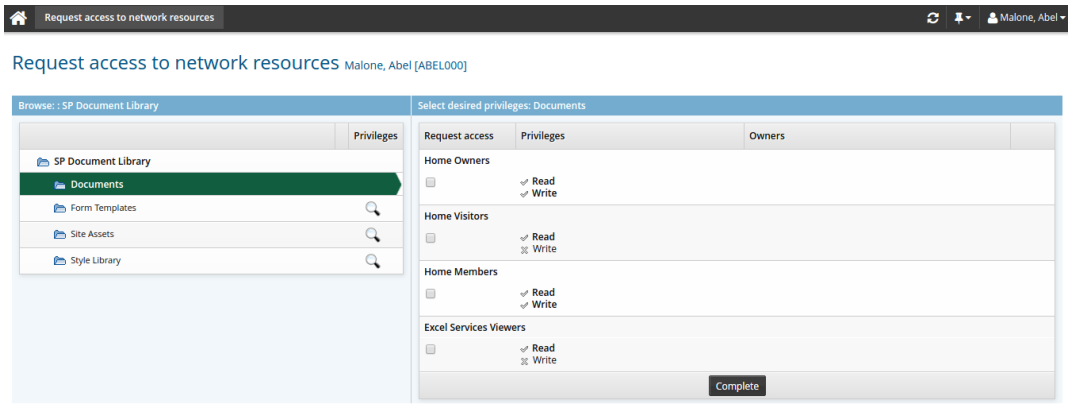


3. Select SP Document Library.
   Bravura Group displays available resources in the document library.



You can click the icon next to the various folders to view privileges.

4. Click the icon next to **Documents**.
   The privileges are displayed on the right hand side.



5. Select the **Home Members** group and click **Complete**.
   Bravura Group enters the request into the authorization workflow.

The Workflow Manager Service routes the request to the selected group owner for authorization. After authorization is complete the Transaction Monitor Service runs a connector program that adds the user to the selected group on the target system and the user will have access to the Sales folder.

8.1.3 Example: Requesting access to a printer

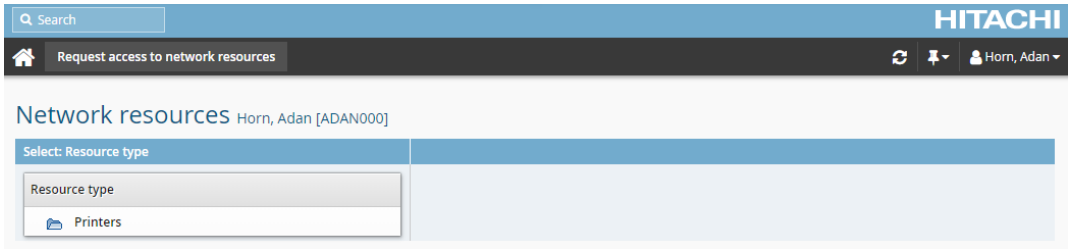
This use case demonstrates the process a user would follow to request access to a shared network printer.

Before a user can be granted access to a printer, the following is required:

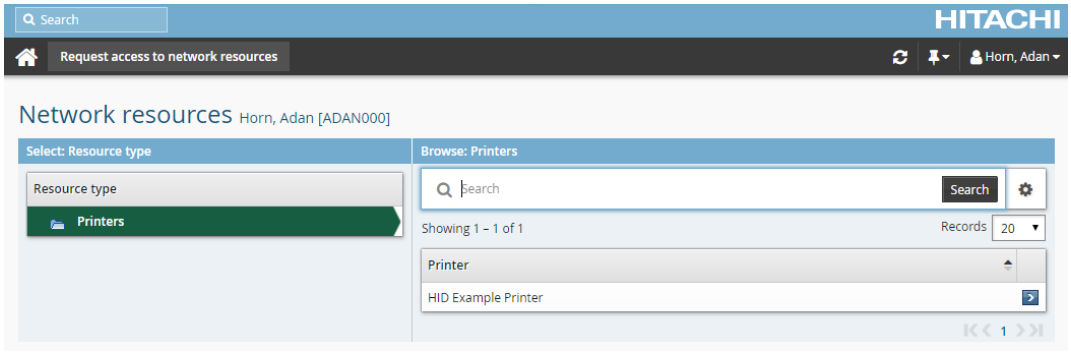
- A network printer has been shared and listed in Active Directory.
- A printer is added to *Hitachi ID Bravura Group* as a network resource.
- Security has been set up on the printer using Active Directory groups.
- The Active Directory groups used for security have owners.
- The **Run as** checkbox has been selected for the administrator credentials for the Active Directory target system.

To request access to the document printer:

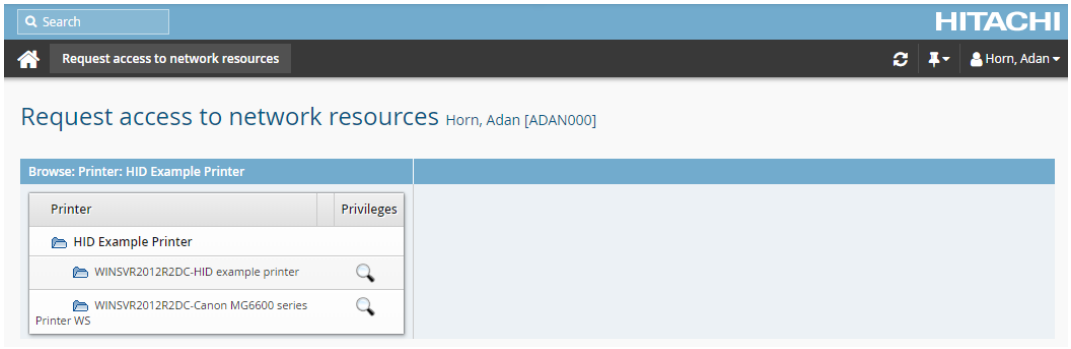
1. From the main menu, click **Request access to network resources** in the **My profile** section.
   The ***Request access to network resources*** page appears.



2. Click **Printers**.
   Bravura Group displays available printers on the right hand side.

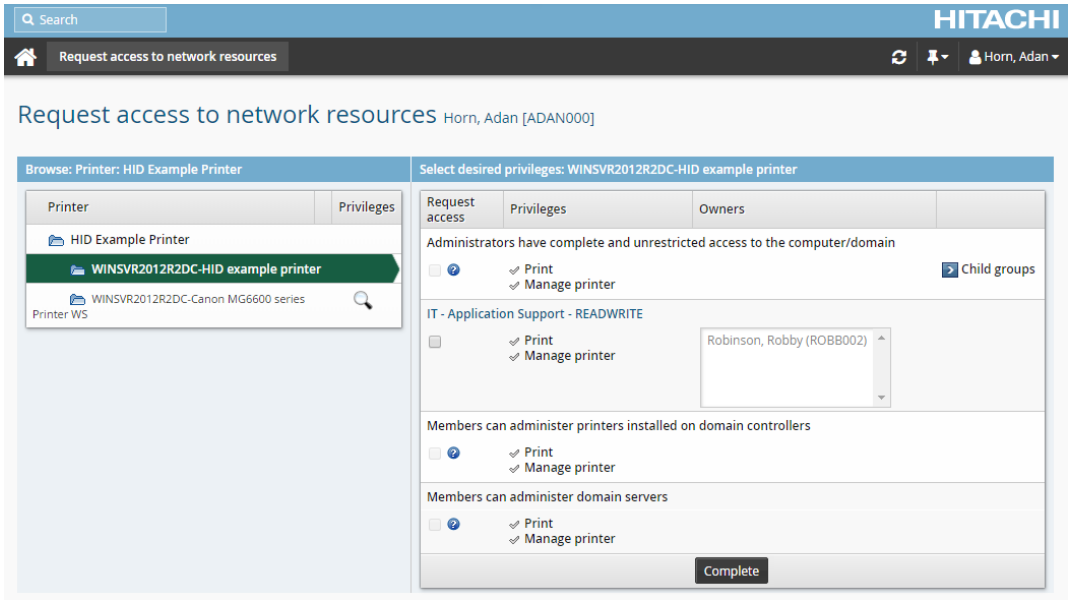


3. Select HID Example Printer.
   Bravura Group displays available printers on the network.



   You can click the icon next to the various printers to view privileges.

4. Click the icon next to **HID example printer**.
   The privileges are displayed on the right hand side.



5. Select the **IT-Application Support** group and click **Continue**.

   Bravura Group enters the request into the authorization workflow.

The Workflow Manager Service routes the request to the selected group owner for authorization. After authorization is complete the Transaction Monitor Service runs a connector program that adds the user to the selected group on the target system and the user will have access to the printer.

Managing Access to Network Resources

9

As a group owner you can add and remove users from the groups that manage the network resources, effectively controlling access to those network resources. You can also control ownership to those groups, allowing other users to manage the network resources too.

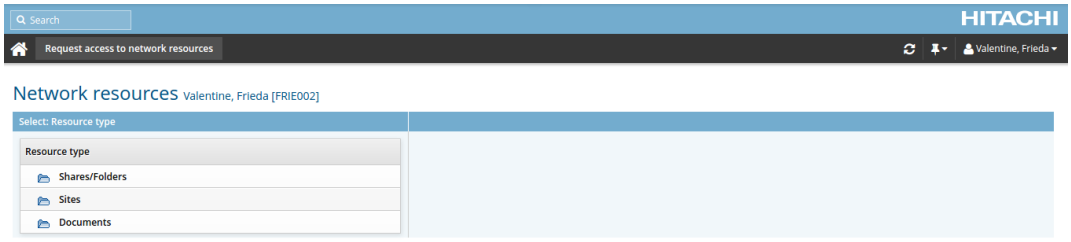
This chapter shows you how users, who are designated as *group owners*, use *Hitachi ID Bravura Group* to:

9.1 Browse network resources

To browse network resources:

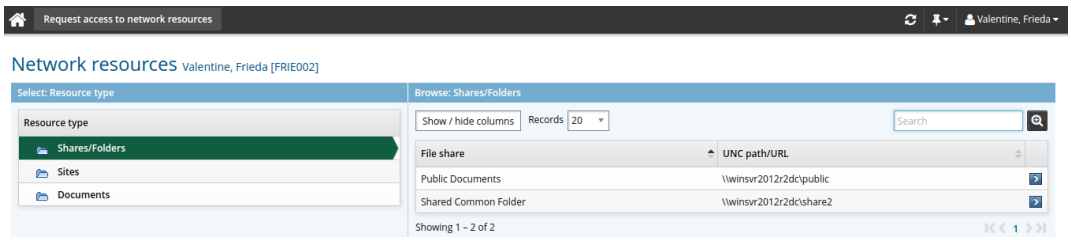
1. Log into the main menu .
2. Click **Request access to network resources** in the **My profile** section.

   Hitachi ID Bravura Group displays a table that allows you to browse network resources. Available resource types are listed in the **Select: Resource Type** (left) column:



3. Select the appropriate resource type.

   Bravura Group displays individual resources in the **Browse: <*Selected Type*>** (right) column:



Alternatively, you can search for the resource.

4. Select the resource you want to browse.

   If you have multiple accounts on the target system managing the resource, you are prompted to select which account to use.

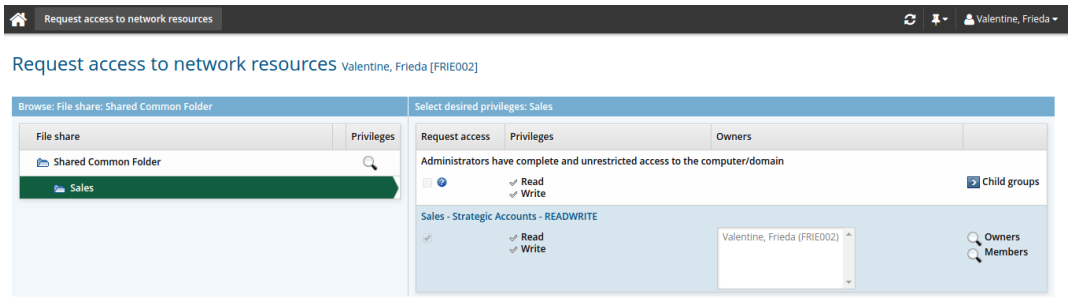
   If the selected resource is a:

Resource type	***Bravura Group* displays . . .**
Share/folder	A tree-view of the folder including any subfolders.
Printer	A list of printer names written in the format: *<server name>-<printer name>*.
Sites	A tree-view of Microsoft Office SharePoint Server site including any sub-sites.
Documents	A tree-view of SharePoint documents including any sub-documents.

   Click the or icon to expand or collapse folders or directory containers. Depending on how *Bravura Group* is configured, you may not be able to browse subfolders of a resource unless you are already a member of a group with read access.

5. Click the privileges icon next to the folder, or container that you want to view.

   Bravura Group displays information about the resource in the **Select desired privileges for: *<Resource name>*** (right) column:



   If applicable, this column contains:

   - A list of groups with privileges on the resource
   - A **Request access** checkbox for each group that you can request access to.

The checkbox is grayed-out if you are already an owner or a member of the group.

- The read / write **Privileges** assigned to each group
- The **Authorizers** for each group
- A **Sub-groups** icon for groups that have member groups
  If you want to view or request access to a member group, select sub-groups next to the parent group (if applicable). To return to the parent group, you can click the return icon at the top of the page.
- A display owners icon and a members icon for groups where you are a group owner

6. Click the display icon next to:
   - **Members** to add or remove members of a group. Proceed to Managing group members.
   - **Owners** to add, remove, or transfer ownership of a group. Proceed to Managing owners.

9.2 Managing group members

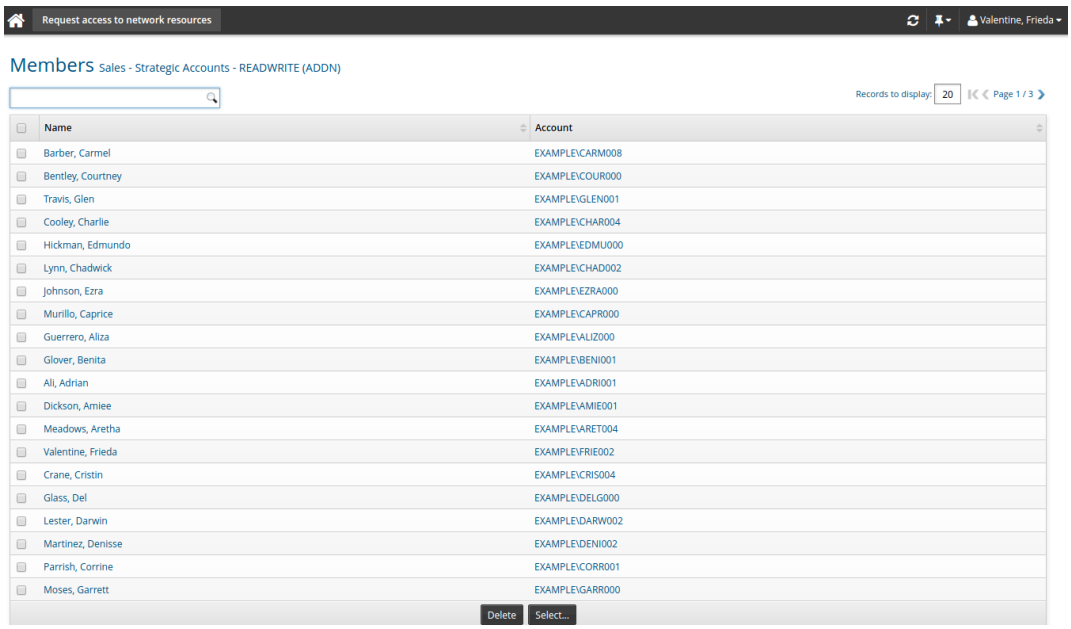
When you add a user to a group you also grant the user privileges to the selected resource. Likewise, when you remove a user from a group you revoke the user's privileges.

Changes to group membership are entered in to a workflow. If *pass-thru* authorization is enabled, and if no other authorizations are required, your request is automatically approved.

9.2.1 Adding group members

To add members to a group:

1. Browse network resources and navigate to the ***Members*** page (p61)
   Hitachi ID Bravura Group displays a list of users with accounts on the target system associated with the resource.



2. Click **Select...** to display a list of potential members.
3. Select the checkboxes next to the users you want to add to the group, then click **Select**.
4. Complete the details for the request:
   (a) Select an email address for notification,
   (b) Type any notes you have for the authorizers who will review the request.
   (c) If required, modify additional attributes for the request.
5. Click **Submit**.

9.2.2 Removing group members

To remove members from a group:

1. Browse network resources and navigate to the ***Members*** page (p61)
   Hitachi ID Bravura Group displays a list of users with accounts on the target system associated with the resource.
2. Select the checkboxes next to the accounts you want to remove from the group.
3. Click **Delete**.
4. Complete the details for the request:
   (a) Select an email address for notification,
   (b) Type any notes you have for the authorizers who will review the request.
   (c) If required, modify additional attributes for the request.

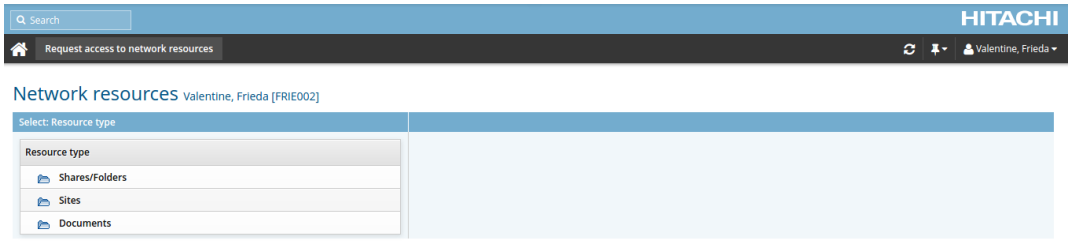
Click **Continue**.

5. Review the request summary.
6. Click **Submit**.

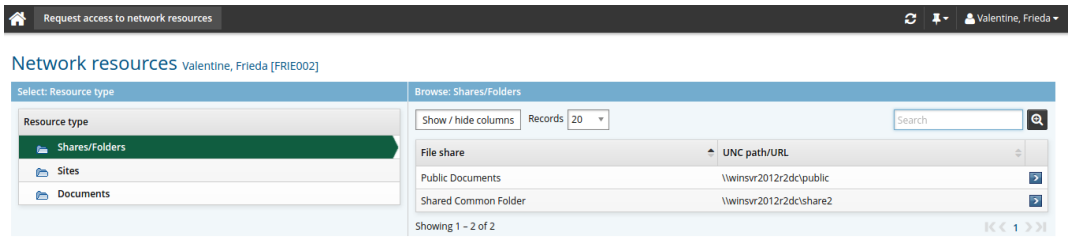
9.2.3 Example: Provide a user access to the Sales folder

To provide a user permission to the Sales folder:

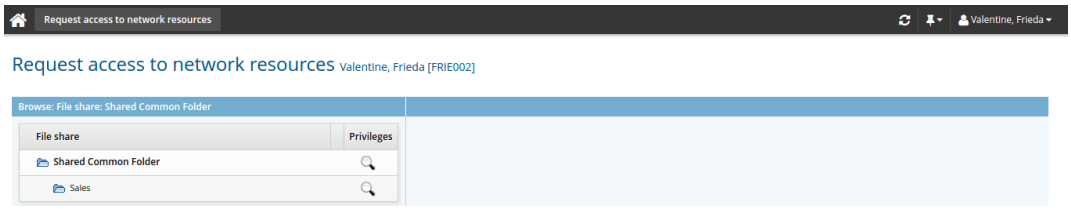
1. Log into the main menu .
2. Click **Request access to network resources** in the **My profile** section.



3. Select the **Shares/Folder** resource.

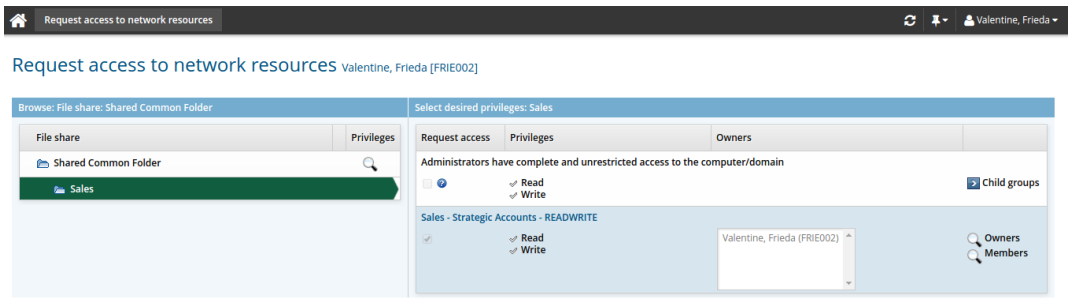


4. Select the **Shared Common Folder**.

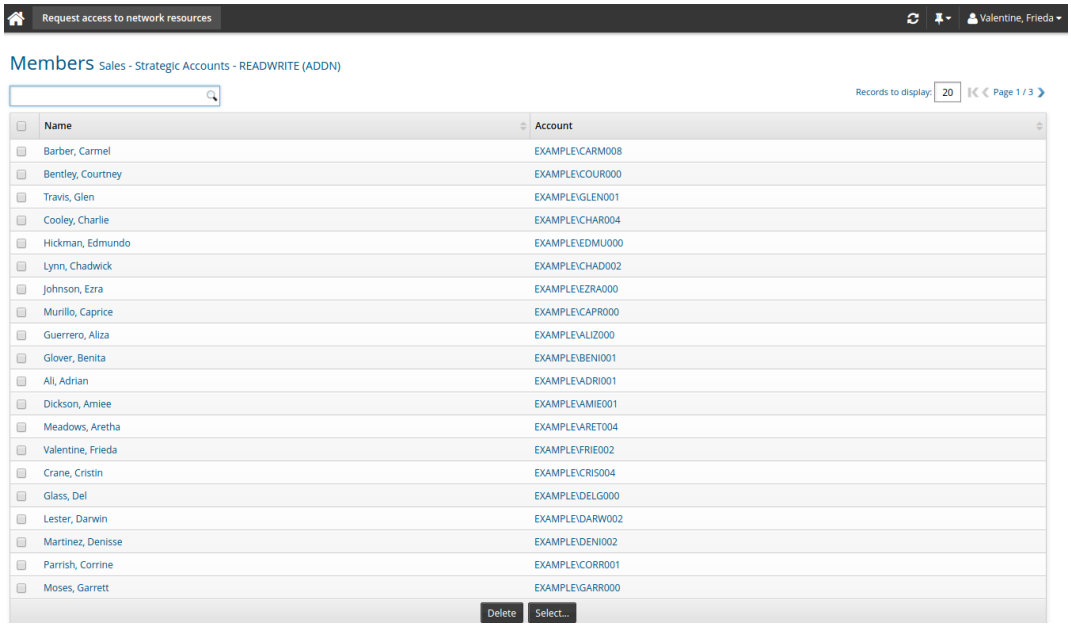


5. Click the privileges icon next to the Sales folder.

   Hitachi ID Bravura Group displays information about the resource in the **Select desired privileges for:Sales** (right) column:



6. Click the display icon next to **Members**.
   Bravura Group displays a list of users with accounts on the target system associated with the resource.



7. Click **Select...**.
8. Select the checkboxes next to the users you want to add to the group, then click **Select**.
9. Complete the details for the request:
   (a) Select an email address for notification,
   (b) Type any notes you have for the authorizers who will review the request.
   (c) If required, modify additional attributes for the request.
10. Click **Submit**.

9.3 Managing owners

Depending on how *Hitachi ID Bravura Group* is configured and whether a resource supports multiple owners, you can add, delete, or change group owners.

9.3.1 Adding group owners

> **Note:** You can only add group owners if your resource supports multiple owners.

To add group owners:

1. Browse network resources and navigate to the ***Owners*** page (p61)
2. Click **Add new...** to see a list of accounts.
   Hitachi ID Bravura Group automatically narrows down the list of accounts to those on the target system associated with the resource.
3. Select the checkboxes next to the accounts you want to add as group owners, then click **Add**.
4. Complete the details for the request:
   (a) Select an email address for notification.
   (b) Type any notes you have for the authorizers who will review the request.
   (c) If required, modify additional attributes for the request.
5. Click **Submit**.

9.3.2 Deleting group owners

To remove group owners:

> **Note:** You can only delete group owners if your resource supports multiple owners and if *Bravura Group* is configured to allow owners to delete other owners. Resources must have at least one owner.

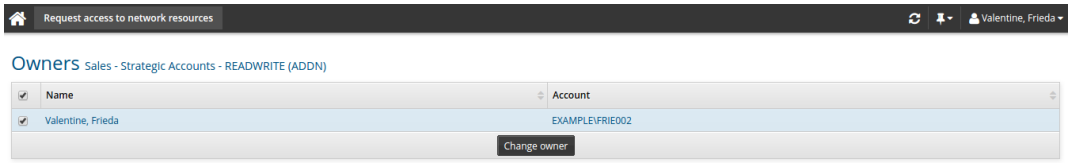
1. Browse network resources and navigate to the ***Owners*** page (p61)
2. Select the checkboxes next to the owners you want to remove, then click **Delete**.
3. Complete the details for the request:
   (a) Select an email address for notification.
   (b) Type any notes you have for the authorizers who will review the request.
   (c) If required, modify additional attributes for the request.
4. Click **Submit**.

9.3.3 Changing group ownership

Changing group ownership removes accounts from the owners list and adds others in a single operation. It also automatically makes the new group owner an authorizer for the group.

To change group ownership, from one or more owners to others:

1. Browse network resources and navigate to the ***Owners*** page (p61)



2. Click **Change owner**.

   Hitachi ID Bravura Group displays the list of users who can become owners.

3. If the resource supports multiple owners, select the checkboxes next to users you want to add as owners, then click **Add**.

   If the resource does not support multiple owners, select the user you want to add as the owner.

4. Complete the details for the request:

   (a) Select an email address for notification.

   (b) Type any notes you have for the authorizers who will review the request.

   (c) If required, modify additional attributes for the request.

5. Click **Submit**.

Index of Variables and Options

Index

U

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