Bravura Privilege Implementation: Team Management for Privileged Access

Team management in *Hitachi ID Bravura Pattern: Privileged Access Edition* delegates onboarding of systems and accounts and definition of access control rules to business stake-holders.

This document contains:

Terminology

Team A container for users and resources, that often represent a real business unit in an organization. Teams are used to define who manages and gets access to those resources managed by *Hitachi ID Bravura Privilege*.

Team groups Groups of individual users or managed groups with assigned team privileges.

1 About team management

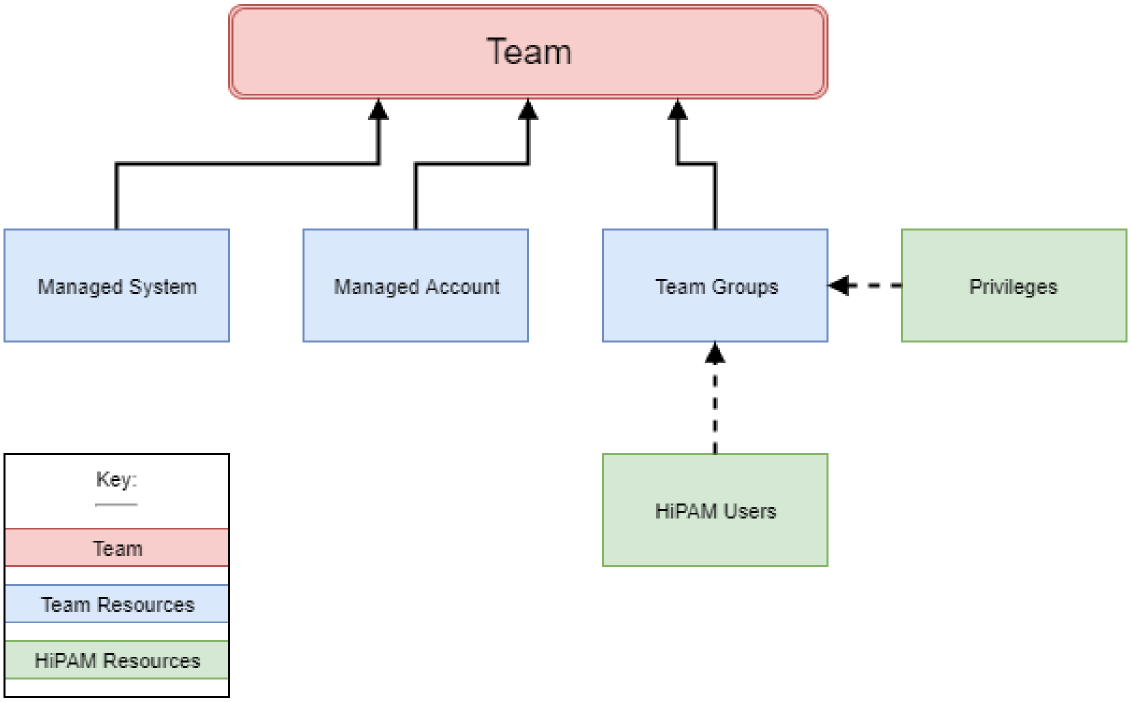
Team management is constructed around a number of concepts:

- A *team* may represent a group of people, an application or an organizational unit.
- Teams contain:
  - *Managed systems* with which *Hitachi ID Bravura Privilege* is integrated.
  - *Managed accounts* that appear on managed systems and whose passwords *Bravura Privilege* may set.
  - *Team groups* used to assign privileges to *Bravura Privilege* users.
- Team groups contain:
  - *Privileges*, such as trustee, approver, requester. See Privileges and appropriate users for more.
  - Individual *Bravura Privilege* users.
  - *Managed groups* – collections of users that appear on integrated systems, such as AD or LDAP.
- *Team vaults* are only used to store and retrieve passwords – not to set or randomize them – where there is no communication with target systems. Team vaults contain:

© 2021 Hitachi ID Systems, Inc. All rights reserved.

  - *System vaults* – representations of systems in the environment, but without a connector or technical integration.
  - *Vault accounts* – representations of accounts on system vaults, along with stored (but not actively managed) passwords.

- *Proxy zone* – a set of *Bravura Privilege* proxy servers responsible for running connectors that communicate with a set of systems, typically in the same location or on the same network segment. *Bravura Privilege* may also connect to managed systems directly; that is, a connector runs locally on the *Bravura Privilege* application server and uses an appropriate API and network protocol to sign into the system in question.



1.1 Team administrators

Team administrators are users that are responsible for creating and deleting teams. When creating a team a team administrator assigns team trustees to the teams. Team administrators and team trustees can both manage team group memberships, but once the trustees are assigned, a team administrator will require permission from the team trustee to make changes. It is best practice not to allow team administrators to also be team trustees.

The team administrator role is generally given to a user within the company that is aware of how the business is structured. The user may be a technical person that also functions as a product administrator for *Hitachi ID Bravura Privilege* or they may be more involved in the business operations of the company.

Users must be a member of the PAM_TRUSTEE_ADMINS user class to be team administrator and create and delete teams.

© 2021 Hitachi ID Systems, Inc. All rights reserved.

1.2 Team trustees

Team trustees use *Hitachi ID Bravura Privilege* to manage their assigned teams by controlling team group membership and privileges. They are also responsible for onboarding and offboarding systems and accounts to their teams.

Users who are assigned as team trustees are automatically added to the PAM_PRIV_TEAM user class to gain access to the appropriate PDRs.

CAUTION: Do not add groups to the PAM_PRIV_TRUSTEES user class.

1.3 Privileges and appropriate users

Within the team structure, team groups are created to assign privileges to. Team group members can be assigned the following privileges:

Account trustee a user who can onboard, offboard, and update privileged accounts.

Approver A user who can allow or disallow access requests.

Approvers are also referred to as *authorizers* in the core *Hitachi ID Bravura Privilege* configuration and documentation.

Approvers are often the owners of the managed account or an appropriate manager of the requester.

Auto_Approved A usr who can check-out access to systems and accounts without making an access request. These users must also have permission to request access.

Users that check out an account on a regular basis should be given the auto-approval privilege to avoid holding up their work and to avoid approver fatigue.

Credential_Manager A user who can override or randomize the stored password on a checked-out account. These users must also have the requesters privilege.

Credential manager privilege is often given to the owners of the managed account.

LC trustees a user who can create and update vaulted credentials.

OTP Trustees a user who can create and use OTP accounts.

Requester A user who can make access requests.

Requesters that require approvers are generally users that do not require access to the managed account on a regular basis, but should still have access to the account in the event of an emergency or a circumstance that arises on occasion.

Subscriber trustee a user who can make subscriber validation requests.

System trustee a user who can onboard, offboard, and update privileged systems.

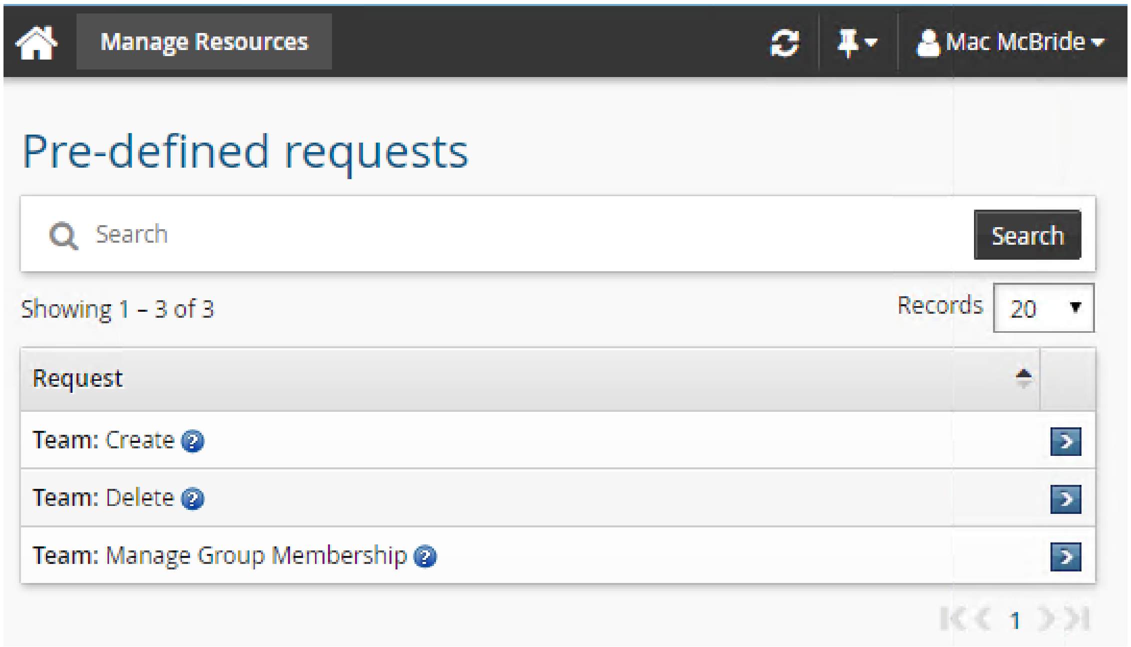
Team trustee a user who can make team management requests.

Vault trustee a user who can create, archive, and update vault systems and accounts.

© 2021 Hitachi ID Systems, Inc. All rights reserved.

1.4 Creating and deleting teams

Team administrators can access pre-defined requests, via the **Manage Resources** option in the **Request** section on the home page, that can create, delete and alter group memberships of teams.



Pre-defined requests

Showing 1 – 3 of 3

Records 20

Request
Team: Create
Team: Delete
Team: Manage Group Membership

The **Team: Create** PDR is for creating teams, the **Team: Delete** PDR is for removing teams and the **Team: Manage Group Membership** PDR allows administrators to add users to team groups in order to grant them privileges. Trustees of a group will be asked for their approval of any group memberships that the team administrator requests.

© 2021 Hitachi ID Systems, Inc. All rights reserved.

2 Use case: Creating a team

This use case demonstrates how to define team administrators, how a team administrator creates a team, and how a trustee manages team group members.

Requirements

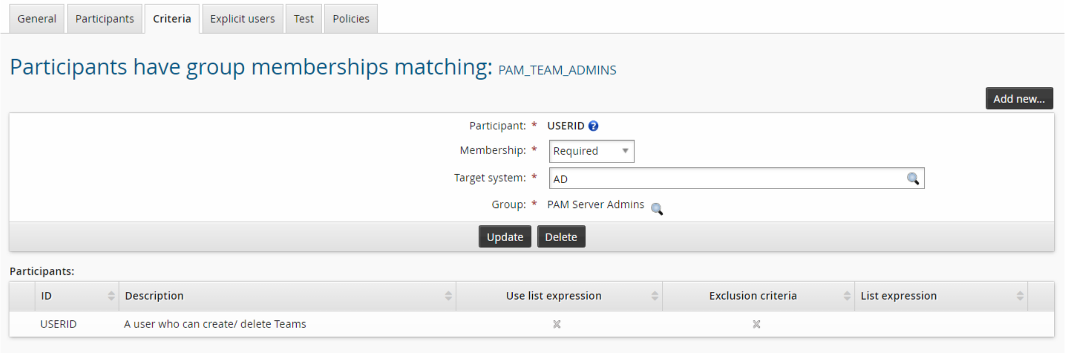
This use case requires:

- *Hitachi ID Bravura Privilege* and *Hitachi ID Connector Pack* installed
- *Hitachi ID Bravura Pattern: Privileged Access Edition* installed
- Active Directory source of profiles

> **Note:** RefBuild.pam_team_management and Scenario.pam_personal_admin_management are installed when *Bravura Pattern: Privileged Access Edition* is installed.

Add team administrators

1. Log in to *Bravura Privilege* as `superuser`.
2. Click **Manage the system** → **Policies** → **User classes**.
3. Select ▶ **PAM_TEAM_ADMINS**.
4. Click the **Criteria** tab.
   Hitachi ID Bravura Privilege displays the user class criteria page.
5. Click **Add new...** in the **Participants have group memberships matching:** section.
   Bravura Privilege displays the add criteria page.
6. Choose "Required" from the **Membership** drop-down list to include users who belong to the specified group in the user class.
7. for, and select ▶, the AD target system.
8. for the `PAM Server Admins` managed group, and select ▶ that group.
9. Click **Add**.



Participants have group memberships matching: PAM_TEAM_ADMINS

Participant: * USERID

Membership: * Required

Target system: * AD

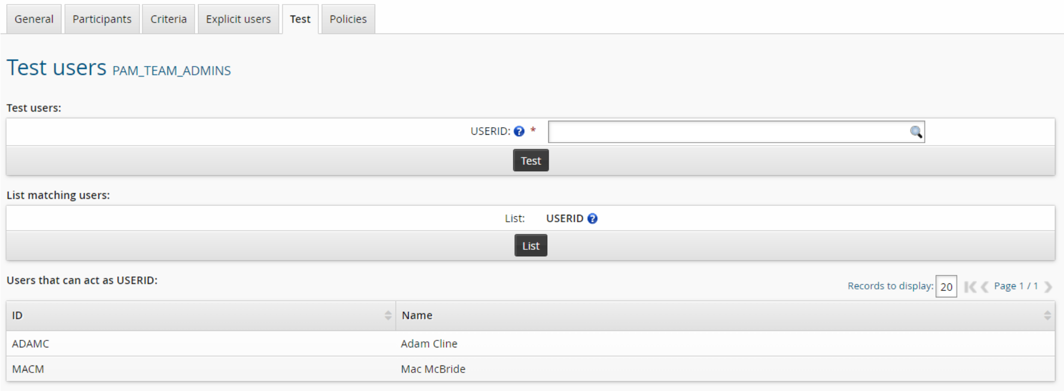
Group: * PAM Server Admins

Participants:

ID	Description	Use list expression	Exclusion criteria	List expression
USERID	A user who can create/ delete Teams	✗	✗	

10. Click the **Test** tab and click **List** to list all users who match the criteria.

    The result should display users similar to the image below:

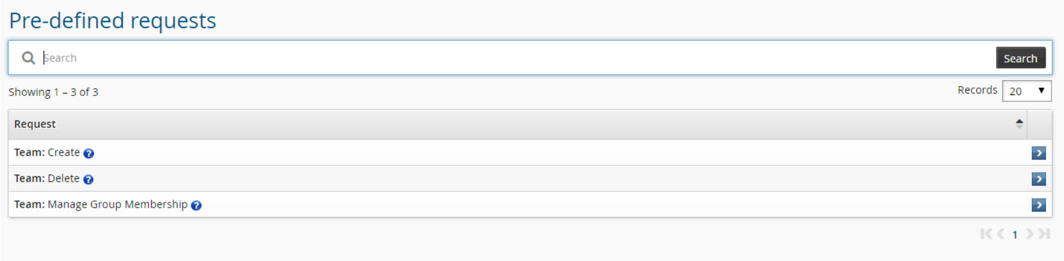


ID	Name
ADAMC	Adam Cline
MACM	Mac McBride

11. Click the **General** tab and click **Recalculate** to update the user class membership cache.

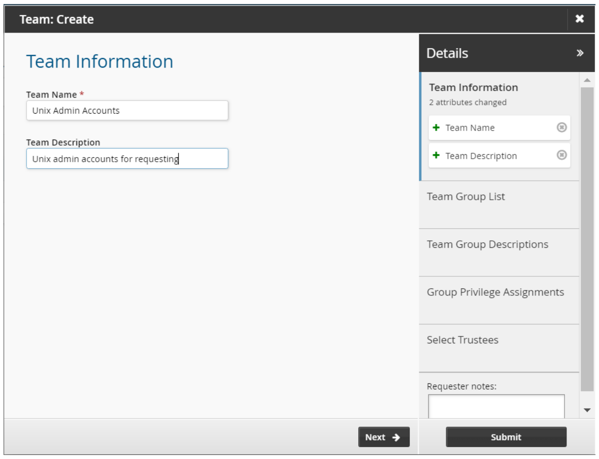
Create a team

1. Log in to *Bravura Privilege* as a team administrator.
2. In the **Requests** section of the main menu, click **Manage Resources**.



Request
Team: Create
Team: Delete
Team: Manage Group Membership

3. Click **Team: Create**.



Team Information

Team Name *: Unix Admin Accounts

Team Description: Unix admin accounts for requesting

4. Enter the following:

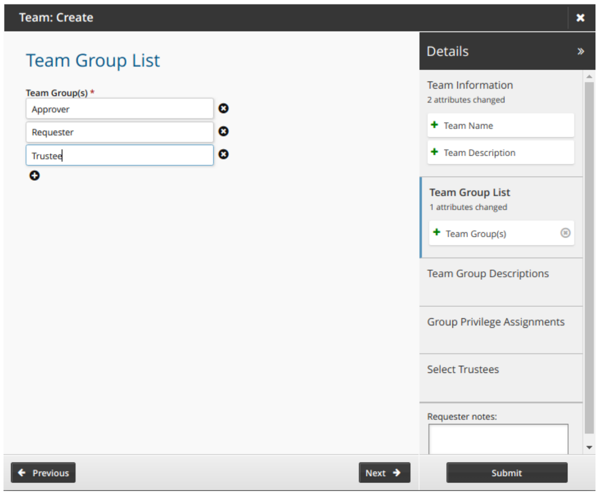
   Team Name Unix Admin Accounts
   Team Description Unix admin accounts for requesting

   Click **Next**

5. Create the following groups:

   - Approver
   - Requester
   - Trustee

   Use the "More" icon ⊕ to add more team name fields to the list.



Team: Create

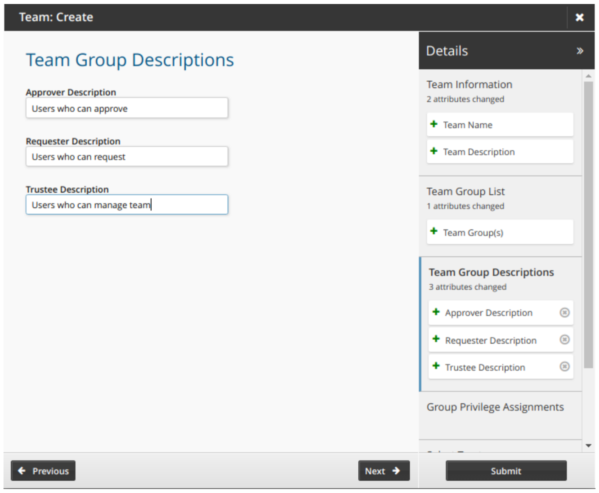
Team Group List

Team Group(s) *: Approver / Requester / Trustee

   Click **Next**

6. Enter the following team group descriptions.

   Approver Users who can approve
   Requester Users who can request
   Trustee Users who can manage team



Team: Create

Team Group Descriptions

Approver Description: Users who can approve

Requester Description: Users who can request

Trustee Description: Users who can manage team

Click **Next**.

7. Assign privileges to the team groups as follows:

   Approver Approvers, Auto_approved, Credential_Manager, Requesters

   Requester Requesters

   Trustee Team Trustees

   Note that it is important that users who have the Auto_approved privilege also have the Requesters privilege.

   Click **Next**.

8. Search for and select a user as the initial team trustee for the new team.

   Team trustees can manage team resources and members. There must be at least one team trustee to create a team.

9. Click **Submit**.

   Hitachi ID Bravura Privilege notifies authorizers to review the request if required.

10. Click the **View request** link at the top of the page to view the status of the request.

    You will see that the request has been processed. The team has been fully configured.

Add group memberships

To manage team group membership as a team trustee:

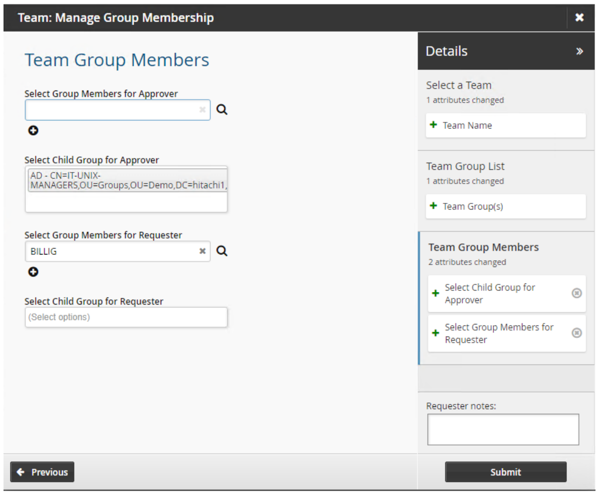
1. Log in to *Bravura Privilege* as the team trustee for the "Unix Admin Accounts" team.
2. In the **Requests** section of the main menu, click **Manage Resources**.

   Note the requests that are available to this user.
3. Click **Team: Manage Group Membership**.
4. Select the "Unix Admin Accounts" team.

   Click **Next**.
5. On the **Team Group List** page, select "Approver" and "Requester".

   Click **Next**.
6. In the **Select Child Group for Approver** field, select the "IT-UNIX-MANAGERS" group.
7. In the **Select Group Members for Requester** field, select the user.

© 2021 Hitachi ID Systems, Inc. All rights reserved.



Team: Manage Group Membership

Team Group Members

Select Group Members for Approver

Select Child Group for Approver: AD - CN=IT-UNIX-MANAGERS,OU=Groups,OU=Demo,DC=hitachi1,

Select Group Members for Requester: BILLIG

Select Child Group for Requester: (Select options)

Details

Select a Team
1 attributes changed
+ Team Name

Team Group List
1 attributes changed
+ Team Group(s)

Team Group Members
2 attributes changed
+ Select Child Group for Approver
+ Select Group Members for Requester

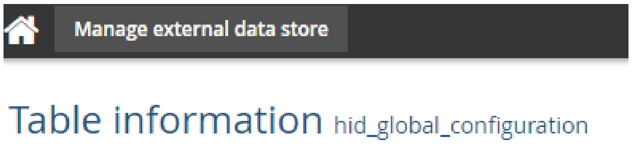
Requester notes:

8. Click **Submit**.

3 Configuring global team groups and privileges

Normally when you create a team, you are prompted to create custom team groups to assign privileges to. To standardize your teams and save time you can set up a global configuration for your teams so when new ones are created you start off with the appropriate groups available with the correctly assigned privileges. It is then up to the administrator who created the team to just add the appropriate users to each team group. These global groups are still customizable to allow non-standard team setups.

You configure global team groups and privileges in the hid_global_configuration table in the *Manage external data store* (DBE) module.

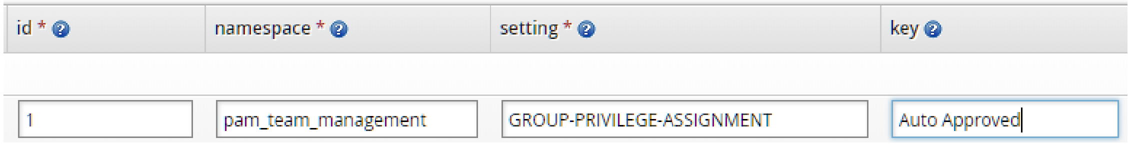


Manage external data store

Table information hid_global_configuration

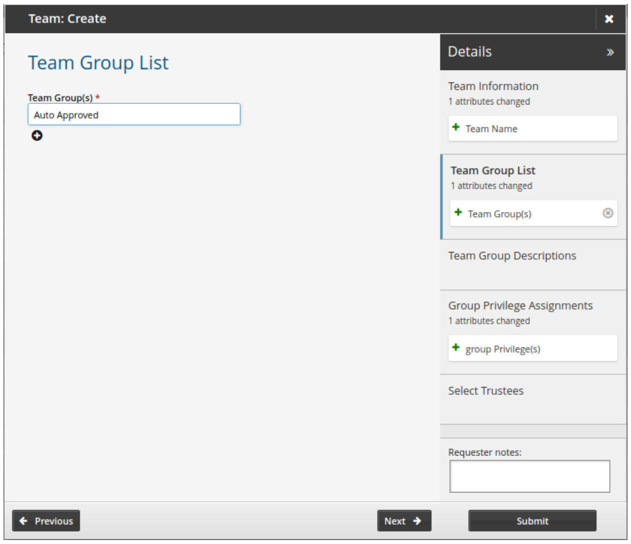
3.1 Configuring global team groups

To create a team group that will automatically be configured for team administrators when they create a new team, add a new entry to the hid_global_configuration table. Each entry must use the new group name as the key and each group can have one or more rows.



id *	namespace *	setting *	key
1	pam_team_management	GROUP-PRIVILEGE-ASSIGNMENT	Auto Approved

Each different key under the "GROUP-PRIVILEGE-ASSIGNMENT" setting will assign a new group to the default groups for a team. Below is the default group that would be configured for the "Team: Create" request:

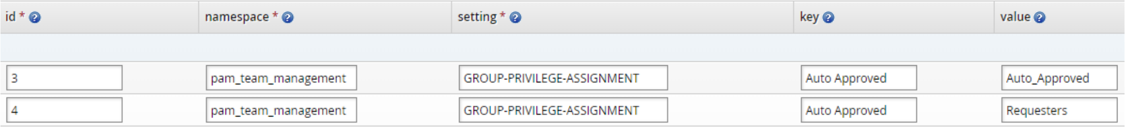

Team: Create

Team Group List

Team Group(s) *
Auto Approved

3.2 Configuring global privileges

To pre-assign a privilege to a group, assign a value to a default group in the hid_global_configuration table. Create a new row for each privilege that needs to be assigned to a group. The screenshot below shows an example of the same group getting Auto_Approve and Requester privileges:



id *	namespace *	setting *	key	value
3	pam_team_management	GROUP-PRIVILEGE-ASSIGNMENT	Auto Approved	Auto_Approved
4	pam_team_management	GROUP-PRIVILEGE-ASSIGNMENT	Auto Approved	Requesters

4 Use case: Creating global team groups and privileges

To make creating new teams more efficient, you can define rules in the hid_global_configuration external data store (**extdb**) table that will configure standard team groups with attached privileges that get automatically created whenever a user triggers the Team:Create pre-defined request.

This use case demonstrates how to make the entries required in the hid_global_configuration external data store (**extdb**) table and create a new team for the Windows administrator accounts using the new standardized configuration.

Requirements

This use case requires:

- *Hitachi ID Bravura Privilege* and *Hitachi ID Connector Pack* installed
- *Hitachi ID Bravura Pattern: Privileged Access Edition* installed
- Active Directory source of profiles

Create global team groups and privileges

1. Log in to *Bravura Privilege* as `superuser`.
2. Click **Manage external data store** → **hid_global_configuration**.
3. Add the following rules to the table:
   - Rules to add a global team group called **Approver** with the approvers, auto-approved, credential_manager and requesters privileges:

     id: 100
     namespace: pam_team_management
     setting: GROUP-PRIVILEGE-ASSIGNMENT
     key: Approver
     value: Approvers
     description: Add Approver group with approvers privilege to new teams.

     id: 101
     namespace: pam_team_management
     setting: GROUP-PRIVILEGE-ASSIGNMENT
     key: Approver
     value: Auto_Approved
     description: Add Approver group with auto-approval privilege to new teams.

     id: 102
     namespace: pam_team_management
     setting: GROUP-PRIVILEGE-ASSIGNMENT
     key: Approver
     value: Credential_Manager
     description: Add Approver group with credential manager privilege to new teams.

  id: 103
  namespace: pam_team_management
  setting: GROUP-PRIVILEGE-ASSIGNMENT
  key: Approver
  value: Requesters
  description: Add Approver group with requesters privilege to new teams.

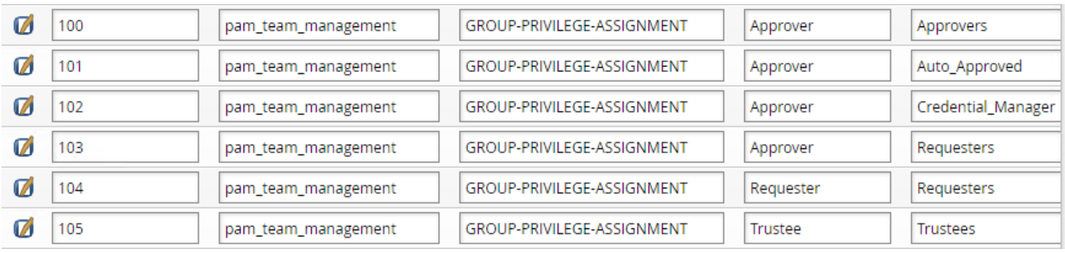
- Rule to add a global team group called **Requester** with the requesters privilege:

  id: 104
  namespace: pam_team_management
  setting: GROUP-PRIVILEGE-ASSIGNMENT
  key: Requester
  value: Requesters
  description: Add Requester group with requesters privilege to new teams.

- Rule to add a global team group called **Trustee** with the trustees privilege:

  id: 105
  namespace: pam_team_management
  setting: GROUP-PRIVILEGE-ASSIGNMENT
  key: Trustee
  value: Trustees
  description: Add Trustee group with trustees privilege to new teams.

4. Click **Update** at the bottom of the table once all your entries are added.



100	pam_team_management	GROUP-PRIVILEGE-ASSIGNMENT	Approver	Approvers
101	pam_team_management	GROUP-PRIVILEGE-ASSIGNMENT	Approver	Auto_Approved
102	pam_team_management	GROUP-PRIVILEGE-ASSIGNMENT	Approver	Credential_Manager
103	pam_team_management	GROUP-PRIVILEGE-ASSIGNMENT	Approver	Requesters
104	pam_team_management	GROUP-PRIVILEGE-ASSIGNMENT	Requester	Requesters
105	pam_team_management	GROUP-PRIVILEGE-ASSIGNMENT	Trustee	Trustees

Create teams using global group rules

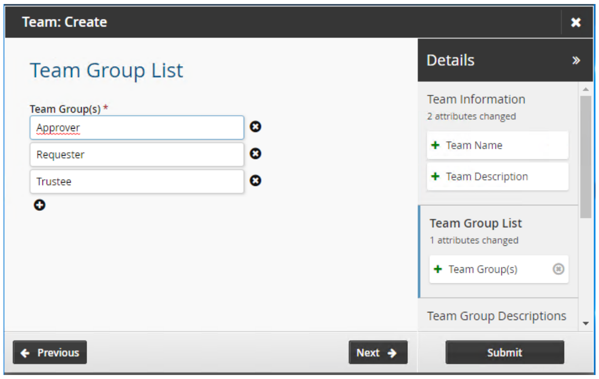
1. Log in to *Bravura Privilege* as a team administrator.

2. In the **Requests** section of the main menu, click **Manage Resources**.

3. Click **Team: Create**.

4. Define values for the team name, description, and members.

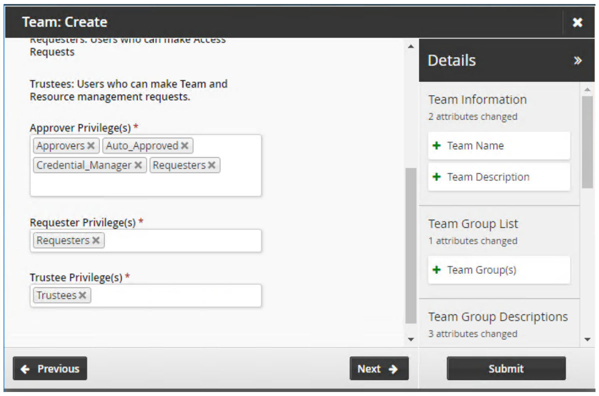
   Click **Next** and proceed to add the information for the team. Group information and the privileges for each group are added automatically.


Team: Create

Team Group List

Team Group(s) *
Approver
Requester
Trustee

Details
Team Information
2 attributes changed
Team Name
Team Description
Team Group List
1 attributes changed
Team Group(s)
Team Group Descriptions


Team: Create

Requesters: Users who can make Access Requests

Trustees: Users who can make Team and Resource management requests.

Approver Privilege(s) *
Approvers ✖ Auto_Approved ✖ Credential_Manager ✖ Requesters ✖

Requester Privilege(s) *
Requesters ✖

Trustee Privilege(s) *
Trustees ✖

Details
Team Information
2 attributes changed
Team Name
Team Description
Team Group List
1 attributes changed
Team Group(s)
Team Group Descriptions
3 attributes changed

5. Click **Submit**.

   Hitachi ID Bravura Privilege notifies authorizers to review the request if required.

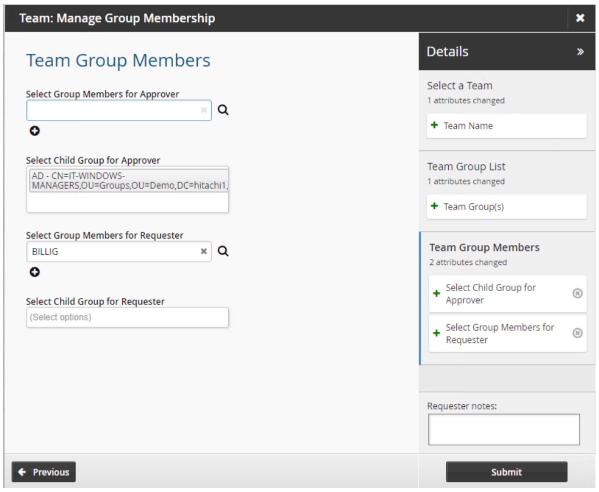
Add group memberships

1. Open another browser tab and login as trustee for the "Windows Admin Accounts" team.
2. Click **Manage Resources** → **Team: Manage Group Membership**.
3. Select the "Windows Admin Accounts" team.

   Click **Next**.
4. On the **Team Group List** page, select "Approver" and "Requester".

   Click **Next**.
5. In the **Select Child Group for Approver** field, select the "IT-WINDOWS-MANAGERS" group.
6. In the **Select Group Members for Requester** field, select the "billig" user.

© 2021 Hitachi ID Systems, Inc. All rights reserved.



Team Group Members

Select Group Members for Approver:

Select Child Group for Approver: AD - CN=IT-WINDOWS-MANAGERS,OU=Groups,OU=Demo,DC=hitachi1,

Select Group Members for Requester: BILLIG

Select Child Group for Requester: (Select options)

Select a Team
1 attributes changed
+ Team Name

Team Group List
1 attributes changed
+ Team Group(s)

Team Group Members
2 attributes changed
+ Select Child Group for Approver
+ Select Group Members for Requester

Requester notes:

7. Click **Submit**.