

# ***Bravura Privilege* Implementation:**

## **Onboard accounts**

This document contains:

- Self-service account management
- Use case: Onboarding managed accounts
- Use case: Randomizing passwords for managed accounts

## **1 Self-service account management**

Once systems are added in *Hitachi ID Bravura Privilege*, team trustees can onboard new accounts from the managed systems through the use of pre-defined requests (PDRs). Adding managed accounts using this method will attach them to the appropriate team, disclosure and session monitoring policies, and authorization rules.

This document focuses on requests that allow team trustees to user self-service requests to onboard, update, and offboard accounts managed on *Bravura Privilege*.

### **1.1 Onboarding an account**

Using the **Account: Onboard** request, trustees onboard an account by specifying the managed system the account belongs to, the managed system policy it should be managed by, the team it needs to be assigned to, how the password should be disclosed to requesters, if the sessions need to be monitored for this account and whether the account password can be overridden. Credentials existing on the managed system will be used to manage the password of the newly onboarded account.

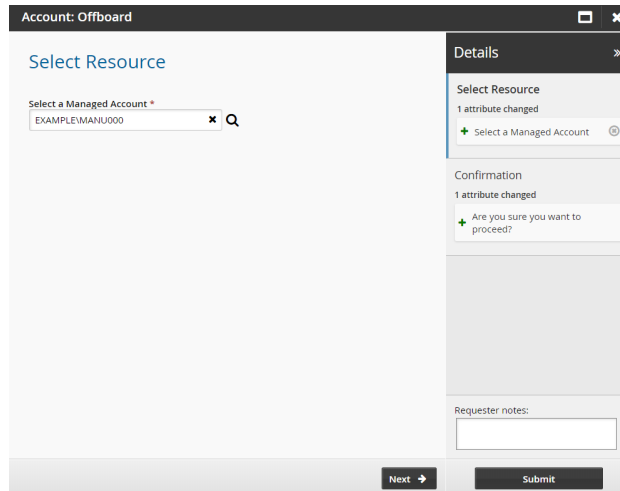
## 1.2 Updating an account

Trustees can use the **Account: Update** request to move a managed account to a different team or change the disclosure, session monitoring and password override permissions.

## 1.3 Offboarding an account

Using the **Account: Offboard** request, a trustee offboards a managed account by moving its credential and check-out history data to an archival policy. It is strongly advised to use the **Account: Offboard** PDR to offboard an account since if it is done manually through a product administrator there will be additional rules left in policy tables that need to be located and removed. Failure to remove all the appropriate the policy table rules within extdb will result in functionality errors in *Hitachi ID Bravura Privilege*.

**Note:** When you offboard an account, all historical password data associated with the account is still available. Historical data is only deleted if the managed system is also offboarded.



**See also:**

See the [Bravura Security Fabric Documentation](#) for more information about configuring and using account management requests.



## 2 Use case: Onboarding managed accounts

### Requirements

This use case requires:

- *Hitachi ID Bravura Privilege* and *Hitachi ID Connector Pack* installed
- *Hitachi ID Bravura Pattern: Privileged Access Edition* installed
- Team groups and privileges set up
- Managed systems onboarded

### Manage Windows account

1. Log in to *Bravura Privilege* as the trustee for the Windows Account Admins Team.
2. In the **Requests** section of the main menu, click **Manage Resources**.
3. Select  **Account: Onboard**.
4. In the **Select a Managed Account** field, select  "Administrator".

Manageable accounts		
<div> <input type="text" value="Search"/> <input type="button" value="Search"/> </div>		
<div> Showing 1 - 10 of 27 <div>Show / hide columns</div> <div>Records 10</div> </div>		
Managed system description	Account	Managed system policy ID
WINNT: wkstn1.hitachi1.corp	Administrator	
WINNT: wkstn1.hitachi1.corp	DefaultAccount	
WINNT: wkstn1.hitachi1.corp	Guest	
Linux Lab Server	adm	
Linux Lab Server	bin	

Click **Next**.

- Enter the following information:

**Account Team:** Windows Admin Accounts

**Managed System Policy ID:** standard policy

**Single Sign On** selected

**View and Copy Password** selected

Click **Next**.

- Leave **Session Monitoring Options** blank.

Click **Next**.

- Click **Submit**.

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

### 3 Use case: Randomizing passwords for managed accounts

#### Requirements

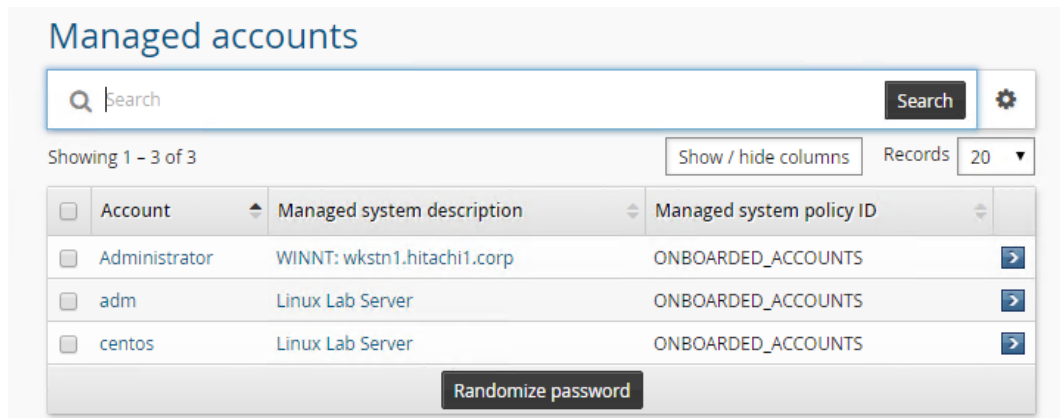
This use case requires:

- *Hitachi ID Bravura Privilege* and *Hitachi ID Connector Pack* installed
- *Hitachi ID Bravura Pattern: Privileged Access Edition* installed
- Team groups and privileges set up
- Managed systems onboarded
- Managed accounts onboarded

#### Randomize passwords

To randomize the passwords for managed accounts in *Hitachi ID Bravura Privilege*:

1. Log in to *Bravura Privilege* as `superuser`.
2. Click **Manage the system** → **Privileged access** → **Managed accounts**.



3. Check the boxes for all of the managed accounts and click **Randomize password**. Confirm the action when prompted.
4. Click **Check results here** to make sure all accounts have been successfully randomized.

Managed system policy	Managed system	Account	Randomization results	Orchestration results
standard policy	Linux Lab Server	adm	Success	Not applicable
standard policy	Linux Lab Server	centos	Success	Not applicable
standard policy	WINNT: wkstn1.hitachi1.corp	Administrator	Success	Not applicable