Bravura Security Fabric Implementation: Change passwords - help desk

Hitachi ID Bravura Security Fabric provides help desk users with the ability to assist users with login issues.

This document contains:

1 Requirement

Organizations require an easy to use process to assist users if they forget their passwords.

2 Solution

Help desk users can perform many tasks on behalf of users, such as enabling/disabling profiles, unlocking accounts, updating security questions, managing tokens, viewing/deleting mobile devices and changing passwords.

This document focuses on how help desk users can use the *Hitachi ID Bravura Security Fabric* web interface to assist users who forget their passwords by changing the passwords and simultaneously clearing any password lockout flags.

3 Use Case: Changing user passwords with a single policy

In the simplest scenario, passwords for all of a user's accounts are automatically synchronized when you change his password using the *Bravura Security Fabric* web interface. Depending on your organization's password policy, you may be able to choose which passwords you want to synchronize, or may be required to set different passwords for each account.

Requirements

This use case assumes that:

- *Hitachi ID Bravura Security Fabric* and *Hitachi ID Connector Pack* are installed.
- An Active Directory target system is added as a source of profiles.
- Help desk users have been assigned permissions to allow them to act on behalf of other users.
- Security questions have been set up so that help desk users can authenticate end users before helping them.
- The end user has completed their profile.

To change an end-user's password:

1. From the main menu , click **Help users**.
2. Select ▶ the user you want to manage.
3. Authenticate the user by answering their security questions, and click **Continue**.

   Depending on configuration, help desk users belonging to a user access rule that has the **Bypass security questions** operation enabled might be able to **Skip authentication** and go straight to the ***Help users*** menu for the end-user.
4. Click **Change passwords**.
5. Type a new password for the caller in the **New password** and **Confirm** fields.

   Ensure that the password satisfies all the strength rules displayed on this page. The maximum allowable length for a password is 127 characters.
6. Click **Change and expire** if the target system has the functionality to expire the password after the initial login and allow the user to choose their own password.

   or

   Click **Change passwords**.

   Bravura Security Fabric processes the change request, then displays a message and notifies the end user when successful. If the changes were not successful, depending on configuration, you may try again later or allow *Bravura Security Fabric* to queue the changes.

4 Use Case: Changing user passwords with multiple policies

Users may have accounts belonging to more than one group, and *Hitachi ID Bravura Security Fabric* can be set up to apply different password strength and synchronization rules to different groups of accounts.

Requirements

This use case assumes that:

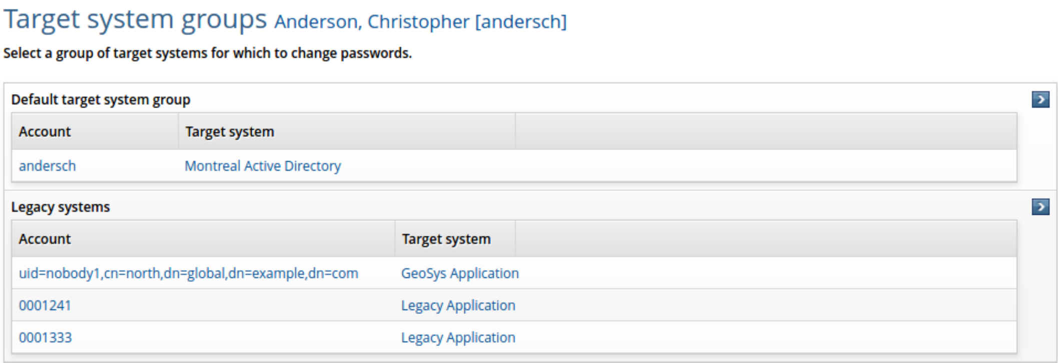
- *Hitachi ID Bravura Security Fabric* and *Hitachi ID Connector Pack* are installed.
- An Active Directory target system is added as a source of profiles.
- Help desk users have been assigned permissions to allow them to act on behalf of other users.
- Security questions have been set up so that help desk users can authenticate end users before helping them.
- The end user has completed their profile.

To change an end-user's password on a group of accounts:

1. From the main menu , click **Help users**.
2. Select ▶ the user you want to manage.
3. Authenticate the user by answering their security questions, and click **Continue**.

   Depending on configuration, help desk users belonging to a user access rule that has the **Bypass security questions** operation enabled might be able to **Skip authentication** and go straight to the ***Help users*** menu for the end-user.
4. Click **Change passwords**.

   Bravura Security Fabric displays one or more groups of accounts on which you can change the user's password. You can change passwords on only one group at a time.



Target system groups Anderson, Christopher [andersch]

Select a group of target systems for which to change passwords.

Default target system group ▶

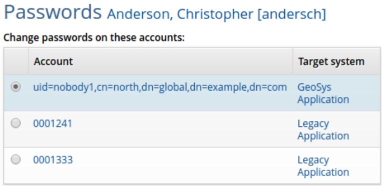
Account	Target system
andersch	Montreal Active Directory

Legacy systems ▶

Account	Target system
uid=nobody1,cn=north,dn=global,dn=example,dn=com	GeoSys Application
0001241	Legacy Application
0001333	Legacy Application

5. Select ❯ the group on which you want to change passwords. The ***Change passwords*** page loads for the selected group.

   If the user is required to have different passwords within a group of accounts, you select one of those accounts by clicking a radio button.

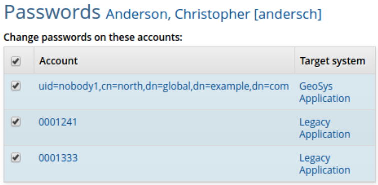
   

   Passwords Anderson, Christopher [andersch]

   Change passwords on these accounts:

	Account	Target system
●	uid=nobody1,cn=north,dn=global,dn=example,dn=com	GeoSys Application
○	0001241	Legacy Application
○	0001333	Legacy Application

   If the user is able to choose more than one account on which to synchronize the password, you select the target systems by enabling the checkboxes. All target systems are selected by default. Click **Clear all** to clear the checkboxes.

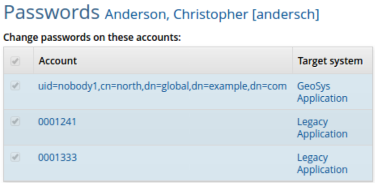
   

   Passwords Anderson, Christopher [andersch]

   Change passwords on these accounts:

☑	Account	Target system
☑	uid=nobody1,cn=north,dn=global,dn=example,dn=com	GeoSys Application
☑	0001241	Legacy Application
☑	0001333	Legacy Application

   If passwords must be synchronized within a group of accounts, all checkboxes are automatically selected.

   Passwords Anderson, Christopher [andersch]

   Change passwords on these accounts:

☑	Account	Target system
☑	uid=nobody1,cn=north,dn=global,dn=example,dn=com	GeoSys Application
☑	0001241	Legacy Application
☑	0001333	Legacy Application

6. Type a new password for the caller in the **New password** and **Confirm** fields.

   Ensure that the password satisfies all the strength rules displayed on this page. The maximum allowable length for a password is 127 characters.

7. Click **Change and expire** if the target system has the functionality to expire the password after the initial login and allow the user to choose their own password.

   or

   Click **Change passwords**.

   Bravura Security Fabric processes the change request, then displays a message and notifies the end user when successful. If the changes were not successful, depending on configuration, you may try again later or allow *Bravura Security Fabric* to queue the changes.

5 Use Case: Unlocking accounts for users

If a user is locked out of an account on a target system because of too many failed login attempts, you can unlock their accounts by using the *Hitachi ID Bravura Pass* web interface. Before you can do this, you must enable the *Unlock accounts* (PSK) module.

> **Note:** This feature may not be available on all systems.
>
> You *cannot* reactivate accounts that were disabled by an administrator.

Requirements

This use case assumes that:

- *Hitachi ID Bravura Security Fabric* and *Hitachi ID Connector Pack* are installed.
- An Active Directory target system is added as a source of profiles.
- Help desk users have been assigned permissions to allow them to act on behalf of other users.
- Security questions have been set up so that help desk users can authenticate end users before helping them.
- The end user has completed their profile.

To unlock accounts for a user using the *Help users* (IDA) module:

1. From the main menu , click **Help users**.
2. Select ▶ the user you want to manage.
3. Authenticate the user by answering their security questions, and click **Continue**.

   Depending on configuration, help desk users belonging to a user access rule that has the **Bypass security questions** operation enabled might be able to **Skip authentication** and go straight to the ***Help users*** menu for the end-user.
4. Click **Unlock accounts**.
5. Enable the checkboxes next to the accounts you want to unlock and click **Unlock**.

   Hitachi ID Bravura Pass displays the ***Account unlock results*** page.

See also:

- See the *Bravura Security Fabric* Self-Service and Help Desk User Guide (**`end-users.pdf`**) for detailed information on help desk tasks.