HITACHI
Inspire the Next

Bravura Pass

Quick Start Guide

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

Contents

Part I

INTRODUCTION

About this document 1

1.1 This document

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

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

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

1.2 Conventions

This document uses the following conventions:

This information . . .	displayed in . . .
Variable text (substituted for your own text)	<*angle brackets*>
Non-text keystrokes – for example, **[Enter]** key on a keyboard.	**[brackets]**
Terms unique to *Hitachi ID Bravura Security Fabric*	*italics*
Button names, text fields, and menu items	**boldface**
Web pages (names)	***italics and boldface***
Literal text, as typed into configuration files, batch files, command prompts, and data entry fields	`monospace font`
Wrapped lines of literal text (indicated by the → character)	`Write this string as a →single line of text.`
Hypertext links – click the link to jump to a section in this document or a web site	Purple text
External document – click the link to jump to a section in another document. The links only work if the documents are kept in the relative directory path.	Magenta text

1.3 Feedback and help

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

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

About Bravura Pass 2

Hitachi ID Bravura Pass is an integrated solution for managing credentials across systems and applications. It simplifies the management of passwords, tokens, smart cards, security questions and biometrics. *Bravura Pass* lowers IT support cost and improves the security of login processes.

Bravura Pass includes password synchronization, self-service password and PIN reset, strong authentication, federated access, enrollment of security questions and biometrics and self-service unlock of encrypted drives.

You can configure *Bravura Pass* to allow users to change forgotten passwords, synchronize some or all of their passwords, or unlock accounts.

The following sections describe the core features.

2.1 Self-service password changes

Users who have forgotten a password or triggered an intruder lockout can sign in to *Hitachi ID Bravura Pass* using other types of credentials to reset their password or clear the lockout. Non-password authentication options include security questions, voice biometrics, smart cards, hardware tokens and random PINs sent to a user's mobile phone using SMS.

Access to self-service is available from a PC web browser, from the Windows login screen, using a telephone or using a mobile device web browser.

2.2 Password policy

2.2.1 Password policy enforcement

Bravura Pass can enforce a uniform global policy in addition to the various password policies enforced natively on each target system. It can also apply multiple alternative password policies to groups of systems.

The built-in password policy engine includes over 50 standard rules, plus a regular expression engine and plugin system that allows organizations to define new rules and rule sets. Open-ended password history and dictionary checks are included.

2.2.2 Expiry notification / early warning

Bravura Pass automatically reminds users to change their passwords regularly. This facility pre-empts native password expiration on target systems and encourages users to synchronize their passwords with a friendly, web-based user interface.

Users are prompted to change passwords either by receiving email with an embedded URL to the *Bravura Pass* server, or by responding to a web browser window that is opened during their network login script.

2.3 Web-based password management

This section describes *Hitachi ID Bravura Pass*'s web-based password management features in more detail.

2.3.1 Password synchronization

Password synchronization is defined as any process or technology that helps users to maintain a single password, subject to a single security policy, and changing on a single schedule, across multiple systems.

End users can synchronize some or all of their passwords by using the *Hitachi ID Bravura Pass* web interface to make routine password changes. Administrative users, known as help desk users, can use the web interface to synchronize passwords on behalf of callers.

The configured password policy for the relevant systems is clearly displayed to users and enforced immediately. This ensures that the password is accepted by the native password security mechanism on all target systems. *Bravura Pass* validates the password against the global password policy. If the password is accepted, *Bravura Pass* synchronizes the passwords on the select systems.

Password change and synchronization with a web browser is more informative and educational than transparent password synchronization but requires users to change their behavior. A user awareness program is often required to encourage use of this feature.

2.3.2 Self-service password changes

Users who have forgotten a password or triggered an intruder lockout can log into *Hitachi ID Bravura Pass* with another form of authentication to perform self-service password changes. Supported authentication factors include answering security questions, using a hardware token, using a biometric sample, and using smart cards.

If a user wants to perform a routine password change (for example, due to upcoming expiry or to synchronize their passwords) they can access the *Bravura Pass* using their existing password, or any of the above authentication factors.

Once authenticated, users can change or un-expire their passwords without calling the help desk. *Bravura Pass* can automatically create tickets on a call tracking system for the event.

2.3.3 Self-service encrypted hard drive recovery

Organizations deploy full disk encryption (FDE) software to protect against data leakage in the event that a corporate workstation is lost or stolen. With FDE, users are generally required to authenticate with a password to unlock the hard disk. This password is often synchronized with the user's primary Windows password.

If a user forgets their hard disk encryption unlock password, the user will be unable to start the operating system. This is a serious service disruption for the user and can contribute to significant support costs for the IT help desk.

Instead of needing to contact the help desk, a user who has lost access to an encrypted system can log into *Hitachi ID Bravura Pass* and access the *Unlock encrypted systems/accounts* (HDD) module, which will provide them with instructions on how to acquire a challenge code for the system, if required. The relevant connector will use this challenge code to generate a response code that can be used to unlock the encrypted device.

For more information, see Unlock encrypted hard disk.

2.3.4 Assisted password changes

When a user calls the help desk, authorized support analysts can sign into the *Hitachi ID Bravura Pass* web user interface, look up a caller's profile, authenticate the caller by keying in their answers to a set of personal questions, and then change one or more of their passwords. A closed ticket can be automatically written to the call tracking system to record the help request.

Support staff do not require any privileges to systems on which *Bravura Pass* allows them to change passwords.

2.3.5 Self-service and assisted account unlock

Users who have locked an account due to too many failed login attempts can use the *Hitachi ID Bravura Pass* web interface to unlock their account. Help desk users can also use the web interface to unlock users.

Users access the *Unlock accounts* (PSK) module after logging into *Bravura Pass* with a known password or with another form of authentication. Once authenticated, users can unlock their account without calling the Help desk. If configured, *Bravura Pass* can automatically create tickets on a call tracking system for the event.

> **Note:** *Bravura Pass* does not allow users to reactivate accounts that were disabled by an administrator.

To implement the self-service and assisted unlock feature, you must enable the *Unlock accounts* (PSK) module.

2.4 Setting up web-based password management

To implement web-based password management with *Hitachi ID Bravura Pass*:

1. Set up email notification

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

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

2. Add at least one target system as a source of profile IDs

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

3. Import users

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

4. 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.

5. Configure target systems for password management. In particular, you can set the following options:

   - **Check password expiry**

     For Novell Directory Services (NDS), Microsoft Windows server, Microsoft Active Directory, and Microsoft SQL Server target systems, *Bravura Pass* can extract a list of users whose passwords will expire soon, or have already expired.

The list can be used by the *Bravura Pass* notification system to warn users of pending expiry.

- **Program to generate a list of target systems**

  For Active Directory, Unix, or GroupWise systems composed of Multiple servers, you can use a *sub-host plugin* to enforce or speed up synchronization.

- **Allow users to change passwords**

  This setting allows the connector (or agent) to change passwords on the system.

- **Accounts must be included in all password changes**

  This prevents users from de-selecting accounts on the target system when changing passwords using the web interface.

  This applies only when the target system belongs to a target system group where web password change restrictions are set to **Any number of accounts can be selected for a password change** or **All accounts are selected for password change**.

- **Allow users to unlock accounts**

  This setting allows users to unlock accounts using either the *Unlock accounts* (PSK) module or *Help users* (IDA) module.

- Display module settings

  Determine whether to include accounts from a target system on the *Change passwords* (PSS) module, *Unlock accounts* (PSK) module, or *Help users* (IDA) module web interface.

6. Configure password strength rules

   You may also need to determine whether a single password policy will apply to all target systems and all users.

7. Configure target system groups to apply password policy and web synchronization restrictions

   You can set target system group options to determine whether passwords must be synchronized, can be unique, or must be unique across target systems.

8. Configure user access controls

   You must set up product administrators and configure their administrative privileges before users can access administrative features. You can also fine tune access controls for regular users.

9. Configure user notification as required.

   You can use the notification system to warn users of pending password expiry, enforce deployment compliance, or other requirements.

10. Configure modules as required

    The *Change passwords* (PSS) module is enabled by default. The *User notifications* (PSN) module and *Unlock accounts* (PSK) module must be enabled for these features to be activated.

2.5 RSA SecurID token management

Hitachi ID Bravura Pass allows users who have RSA SecurID Authenticators (tokens) to manage their tokens from a web browser using the *Manage tokens* (PSP) module, or a telephone using an integrated IVR system. Specifically, you can configure *Bravura Pass* to allow users to do any of the following:

- Enable or disable their tokens
- Clear their PIN
- Set a new PIN
- Request emergency access codes
- Clear their previously-requested emergency access codes
- Re-synchronize their token clock with the RSA Authentication Server

This facility is separate from password management. You cannot synchronize SecurID PINs with passwords unless alpha-numeric PINs are allowed, which is not true in most organizations. If alpha-numeric PINs are enabled on your RSA Authentication Manager Server, then you can synchronize PINs with passwords using *Bravura Pass*.

- If you have an RSA Authentication Manager 7.1/8.2 system installed on your network, the Hitachi ID Systems connector uses the Java API to update and retrieve information from the RSA Authentication Manager 7.1/8.2 server.

  See the Authentication (Tokens / MFA) Integration Guide (**`authentication-tokens-mfa.pdf`**) for more information about integrating with this system.

To set up token management using *Bravura Pass*, you must:

1. Prepare the RSA Authentication Manager 7.1/8.2 server for integration and add it as a target on *Bravura Pass*.

   See the Connector Pack Integration Guide for details.

2. Run auto discovery to load data from the RSA Authentication Manager 7.1/8.2 server.

3. Enable and configure the *Manage tokens* (PSP) module to allow users to manage their own tokens.

   See Manage tokens (PSP).

4. Optionally, configure the *Help users* (IDA) module to allow help desk users to manage tokens on users' behalf.

   See Help users (IDA).

2.6 Transparent password synchronization

Hitachi ID Bravura Pass can extend the native password management on selected types of systems with *transparent password synchronization*. When this is implemented on a *trigger system*:

- Native password changes on the trigger system are subjected to the *Bravura Pass* password policy, and may be rejected on that basis.
- Successful password changes trigger automatic password synchronization for other accounts, on other systems, that belong to the same user.

Transparent password synchronization can be triggered from native password changes on any of the following systems:

- Windows 2012R2/2016/2019 servers and Active Directory domains (password filter DLL on servers and/or DCs).
- z/OS mainframes with RAC/F, ACF2 or TopSecret security products (security exit in the LPAR with the security products).
- OS/400, iSeries servers.
- Unix/Linux servers (passwd program wrapper binary or privileged access management (PAM)).
- Sun/Oracle and IBM LDAP servers (attribute change filter on the directory server).

Each of these triggers contacts the *Bravura Pass* server twice per password change, over an encrypted TCP/IP socket (shared key handshake, 256-bit AES encryption):

- First connection: validate password quality, possibly reject the user's choice of a new password and block the triggering password change due to policy violation
- Second connection: initiate transparent password synchronization

To implement transparent password synchronization, special software is installed on the trigger system to monitor password changes and verify the strength of new password choices with *Bravura Pass* before permitting changes. This software communicates with the Password Manager service (idpm) on the *Bravura Pass* server, using an encrypted TCP socket connection.

> **Note:** Although RSA Authentication Manager 7.1/8.2 servers are not capable of being triggers, transparent synchronization can reset PINs, as long as alpha-numeric PINs are allowed on the RSA Authentication Manager 7.1/8.2 server.

Transparent password synchronization involves the following components:

Components	Purpose

Password Manager service (idpm)	This service works in conjunction with trigger programs and libraries on various systems. Over a secure, encrypted TCP connection, the service evaluates a new password selected by a user, determines whether it should be accepted, and if so, synchronizes the password to a new value on all systems where the user has a login account.
Hitachi ID Password Change Notification Module	This local agent intercepts native password changes on Microsoft Active Directory domain controllers and Windows servers, and triggers transparent password synchronization.
Hitachi ID password replacement program (pspasswd) and the Hitachi ID Systems pluggable authentication module	This program intercepts native password changes on Unix servers and triggers transparent password synchronization.
LDAP password filter plugin (psldap) or OID-LDAP password filter plugin (psldap.so)	This local agent intercepts native password changes on LDAP Directory Service servers and triggers transparent password synchronization.
Hitachi ID OS/400 exit program (pspwdexit)	This exit program intercepts password changes on IBM OS/400 and propagates them to the *Bravura Pass* server for policy validation and to initiate transparent synchronization.

Note: Software components for Windows-based and OS/400 trigger systems are shipped with *Bravura Security Fabric* and installed in the \<*instance*>\addon\transparent-synch\ directory. Software for Unix-based trigger systems is shipped with *Connector Pack*. The location depends on whether you install a global or instance-specific connector pack. The OS/390 trigger software is shipped with *Mainframe Connector*. See the *Mainframe Connector* Installation Guide for more information.

Optionally, you can enable the *Enable password synchronization* (PSR) module to educate users and enforce registration for transparent password synchronization.

WARNING!: If using load balancers, do not configure any SSL options for transparent synchronization traffic. SSL options should only be configured on load balancers for WebUI traffic, not transparent synchronization. Transparent synchronization is encrypted using a proprietary encryption algorithm. Contact support@Hitachi-ID.com for more details.

2.6.1 Interceptor compatibility

Below is a compatibility matrix that should be taken into consideration when upgrading *Hitachi ID Bravura Pass* services (**idpm**/**pushpass**) or interceptors. **Y** denotes that the versions are compatible and **N** denotes that the versions are not compatible.

Table 2.2: *Bravura Pass* interceptor compatibility

Interceptor version	Service version						
	10.0.x	10.1.x	11.0.x	11.1.x	12.0.x	12.1.x	12.2.x
6.4.9	Y	Y	Y	Y	Y	Y	Y
7.3.1	Y	Y	Y	Y	Y	Y	Y
8.2.8	Y	Y	Y	Y	Y	Y	Y
9.0.x	Y	Y	Y	Y	Y	Y	Y
10.0.x	Y	Y	Y	Y	Y	Y	Y
10.1.x	Y	Y	Y	Y	Y	Y	Y
11.0.x	Y	Y	Y	Y	Y	Y	Y
11.1.x	Y	Y	Y	Y	Y	Y	Y
12.0.x	Y	Y	Y	Y	Y	Y	Y
12.1.x	Y	Y	Y	Y	Y	Y	Y
12.2.x	Y	Y	Y	Y	Y	Y	Y
CP 3.0.x (unix)	Y	N	N	Y	Y	Y	Y
CP 3.1.x (unix)	Y	N	N	Y	Y	Y	Y
CP 3.2.x (unix)	Y	Y	Y	Y	Y	Y	Y
CP 3.3.x (unix)	Y	Y	Y	Y	Y	Y	Y
CP 4.0.x (unix)	Y	Y	Y	Y	Y	Y	Y
CP 4.1.x (unix)	Y	Y	Y	Y	Y	Y	Y

Also review the access control list for the **Comma-delimited list of IP addresses with CIDR bitmask that are allowed to send socket requests** setting for the Password Manager service. Password synchronization interceptors that need to access `idpm` must be defined in this field.

For more information about Password Manager service see Password Manager Service (idpm).

2.6.2 Use cases

2.6.2.1 Use case: Users continue to change their Active Directory password from their desktop

Some organizations require users to change their Active Directory passwords on a regular basis. Often users do this from the login prompt on their desktop. Transparent password synchronization can be set up as follows to allow users to continue changing their passwords using the same, familiar method:

1. Install and configure *Hitachi ID Bravura Pass*.
2. Install the Password Change Notification Module on one Active Directory domain controller.

From now on, when a user changes their password using the familiar method, the Password Change Notification Module will intercept the password change. The Password Change Notification Module will then trigger automatic password synchronization for other accounts, on other systems, that belong to the same user.

2.6.2.2 Use case: Users continue to change their password using the regular password program on Unix/Linux

Some organizations require users to change their Unix passwords on a regular basis. Often users do this using the regular password program on Unix. Transparent password synchronization can be set up as follows to allow users to continue changing their passwords using the same, familiar method:

1. Install and configure *Hitachi ID Bravura Pass*.
2. Replace the native password program (/usr/bin/passwd) with **`pspasswd`** to intercept password changes made using the standard password command (passwd).

From now on, when a user changes their password using the familiar method, the password replacement program (pspasswd) will intercept the password change on Unix. The password replacement program will then trigger automatic password synchronization for other accounts, on other systems, that belong to the same user.

See the Transparent Password Synchronization Configuration Guide (**`transparent-sync.pdf`**) to learn how to implement transparent synchronization.

2.7 Self Service Anywhere

Hitachi ID Bravura Pass includes key features to assist mobile users:

1. Email notification to users about upcoming password expiry, since the notice displayed at the Windows login prompt is not shown to users away from the office.
2. Support for resetting forgotten encryption keys for users whose PCs are protected with full disk encryption.
3. Support for resetting forgotten passwords or PINs from the login prompt, even if the user is away from the office and is not physically attached to the Internet.

These features are collectively referred to as *Self Service, Anywhere (SSA)*. Using these features, users can resolve problems with their passwords, smart cards, tokens or full disk encryption software both at the office and mobile, from any endpoint device.

2.7.1 Password expiry warning for mobile users

Problem Mobile users are not notified by Windows when their passwords are about to expire. Users who infrequently connect their laptop to the office network, instead checking email with a solution such as Outlook Web Access, suffer regular password expiry and require frequent password resets.

Solution *Hitachi ID Bravura Pass* sends users emails warning of imminent password expiry. Users change passwords using a web browser. Password Manager Local Reset Extension refreshes the password on their laptop.

The solution involves the following components:

Components	Purpose
Notification Service (psntfsvc)	updates the database with information about notification events and compliance rules, and runs plugins that: • Check if a user is in compliance for a particular event • Send reminders to non-compliant users, either by web or email • Take action if the reminder limit for a user is exceeded • Generate a list of non-compliant users for batch notification
User notifications (PSN) module	Can be used to notify users of pending password expiry via a web page.
Change passwords (PSS) module	Enables users to change passwords for one or more of their accounts.
Password Manager service (idpm)	Can be used to queue password changes if they fail on a target system.
Local Reset Extension	Resets passwords and clears cached credentials on users' local workstations.
`cgilocalr.exe`	The program that supplies HTML to the password status page of the *Change passwords* (PSS) module for the S STATUS EXT plugin point.
`cgilocalr.cfg`	The configuration file for **`cgilocalr.exe`**.

To set up self-service password reset for mobile users:

1. Set up web-based password management features, including expiry notification, as described in the

Bravura Security Fabric Documentation .

2. Enable the Local Reset Extension, as described in Resetting cached credentials in the *Self-Service Anywhere Implementation Guide (**self-service-anywhere.pdf**)*.

2.7.2 Reset forgotten, cached passwords while away from the office

Problem Laptop users sometimes change their password before leaving the office and may forget the new password when they need to use it while not attached to the corporate network. Without a technical solution, the IT help desk cannot resolve these users' problem until they return to the office. User laptops are rendered inoperable until they return to the office.

Solution A *Hitachi ID Bravura Pass* client software component allows users who forgot their primary, cached Windows password and cannot sign into their PC to connect to the Internet over a WiFi hotspot or using an AirCard. Locked-out users can also establish a temporary Internet connection using their home Internet connection or a hotel Ethernet service. Once the user's laptop is on the Internet, *Bravura Pass* establishes a temporary VPN connection and launches a kiosk-mode (full screen, locked down) web browser. The user steps through a self-service password reset process and *Bravura Pass* uses an ActiveX component to reset the locally cached password to the same new value as was set on the network back at the office.

The solution involves the following components:

Components	Purpose
Change passwords (PSS) module	Enables users to change passwords for one or more of their accounts.
Password Manager service	Can be used to queue password changes if they fail on a target system.
Login Assistant	client software that works with a specially constructed and locked-down account, defined on a Windows workstation (7 or higher). It is typically used to allow users, who forgot or otherwise disabled their login password, access to a self-service password reset facility.
Local Reset Extension	Resets passwords and clears cached credentials on users' local workstations.
cgilocalr.exe	The program that supplies HTML to the password status page of the *Change passwords* (PSS) module for the S STATUS EXT plugin point.
cgilocalr.cfg	The configuration file for **cgilocalr.exe**.

To set up local self-service password reset for mobile users:

1. Set up web-based password management features as described in the *Bravura Security Fabric* Documentation .
2. Enable the Local Reset Extension, as described in Resetting cached credentials in the *Self-Service Anywhere Implementation Guide*.
3. Enable the *Login Assistant*, as described in self-service-anywhere.pdf.

2.7.3 Unlock encrypted hard disk

Problem Organizations deploy full disk encryption (FDE) software to protect against data leakage in the event that a corporate laptop is lost or stolen. Users with FDE on their PCs normally have to type a password to unlock their hard disk, before they can boot up an operating system. This password is normally synchronized with the user's primary Windows password, so that the user only has to remember and type a single password at login.

If a user forgets his hard disk encryption unlock password, the user will be unable to start his operating system or use his computer. This is a serious service disruption for the user and can contribute to significant support costs for the IT help desk.

IVR solution Most FDE packages include a key recovery process at the PC boot prompt. This normally involves a challenge/response process between the FDE software, the user, an IT support analyst and a key recovery server. *Hitachi ID Bravura Pass* can front-end this process using an integrated telephony option, so that users can perform key recovery 24x7, from any location, using their telephone and without talking to a human help desk technician.

Web solution Users with access to the *Bravura Pass* web interface can also recover an encrypted system through the *Unlock encrypted systems/accounts* (HDD) module, which will provide them with instructions on how to acquire a challenge code for the system, if required. The relevant connector will use this challenge code to generate a response code that can be used to unlock the encrypted device.

The components used in the solution depend on the type of FDE software, and other requirements of your organization. *Hitachi ID Connector Pack* ships with connectors for systems including Check Point, McAfee EndPoint Encryption, and PGP Whole Disk Encryption (WDE).

- The Check Point connector works with *Phone Password Manager* or a custom application to communicate between Check Point and *Bravura Pass* servers.
- The PGP WDE connector works with *Phone Password Manager* and an ActiveX control, **`nplocalr`**, to updated locally protected resources.

For more information see:

- Integrating with Interactive Voice Response Systems to learn how to interface with interactive voice response (IVR) systems.

- Configuring the Local Reset Extension plug-in to learn how to enable the **nplocalr** Local Reset Extension.
- The *Phone Password Manager* Configuration Guide for details on installing and configuring *Phone Password Manager*.
- Unlocking encrypted systems via the Bravura Pass web interface for information about configuring the *Unlock encrypted systems/accounts* (HDD) module.
- The Connector Pack Integration Guide for information about integrating with hard drive encryption systems.

2.7.4 Smart card PIN reset

Problem Organizations deploy smart cards to strengthen their authentication processes. Users typically sign into their PC by inserting their smart card into a reader and typing a PIN. If users forget their PIN or leave their smart card at home, they cannot sign into their PC. PIN reset is a complex support process since the new PIN has to be physically installed on the user's smart card. This means that IT support may trigger a physical visit to the help desk.

Solution *Hitachi ID Bravura Pass* allows users to access a self-service web portal from anywhere, including from the locked out login screen of their laptop, even away from the office (even using WiFi, as described earlier). Once a user signs into the self-service portal, *Bravura Pass* can download an ActiveX component to the user's web browser, to communicate with the smart card and reset the forgotten PIN. *Bravura Pass* can also be used to assign a user a temporary login password (often a very long and random one) to be used in the event that a user left his smart card at home.

The solution involves the following components:

Components	Purpose
Change passwords (PSS) module	Enables users to change passwords for one or more of their accounts.
Password Manager service	Can be used to queue password changes if they fail on a target system.
scpinplugin	The **scpinplugin** works with the ActiveX control **HISCPINToolAX.ocx** to reset smart card PINs. PIN strength checking can be done by checking the combinations of rules specified in a configuration file and the *Bravura Pass* password policy.

To set up local self-service smart card PIN reset:

1. Set up web-based password management features as described in the *Bravura Security Fabric* Doc-

umentation .

2. Configure the smart card PIN reset plugin as described in CGI / HTML in the Bravura Security Fabric *Reference Manual*.

2.7.5 Low cost multi-factor authentication using mobile phones

Hitachi ID Bravura Pass supports low-cost, multi-factor authentication into its own request portal, using a smart phone as a secondary authentication factor.

This solution is implemented using two technologies included with *Bravura Pass*:

1. Managed enrollment, which automatically invites users to:
   (a) provide their mobile phone number; and/or
   (b) provide their personal email address; and/or
   (c) install the *Hitachi ID Bravura One* app on their phone.
2. Having enrolled,
   (a) If the user connects from outside the private/secure corporate network, start with a CAPTCHA.
   (b) Next, prompt for the user's login ID.
   (c) Fingerprint the user's browser – if the indicated user has signed on successfully from the same browser before, this fact can act as an unobtrusive authentication factor.
   (d) If the user connects from a browser or location not seen before, prompt for another factor, which may be any of the following:
      i. If the user has been activated to use a third party MFA technology, such as a one time password token (e.g., RSA SecurID) or a third party app (e.g., Duo Security, Okta Verify), use that.
      ii. If the user had previously installed *Mobile Access* on their phone, either use push notification to display a PIN on their phone or display a cryptographic challenge in the login screen as a QR code, which the user scans with the app.
      iii. If the user had previously enrolled their mobile phone number, send a PIN to the user's phone, via SMS and prompt the user to enter it.[1]
      iv. If the user had previously enrolled their personal email address, send a PIN to that address, on the assumption that the user has email access on their phone.
   (e) Users may be prompted to select one of several MFA options or one of several alternatives for the same option (e.g., send a PIN via SMS to one of multiple mobile numbers or email addresses).
   (f) Finally, depending on whether the user remembers his password, prompt the user to enter it or answer a series of security questions. Using a second, "knowledge" factor reduces the risk of compromised authentication due to lost or stolen phones or hardware tokens.

[1] Note: an SMS broker is required to do this, which may cost as much as a few cents per message.

See the Hitachi ID Bravura One Configuration Guide for detailed information about installing and configuring Hitachi ID Bravura One.

See the Self-Service Anywhere Implementation Guide to learn how to implement these features.

Part II

CONFIGURING PASSWORD MANAGER

Adding a target system 3

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

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

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

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

   You can restrict user listing by container or group membership.
7. Select the **Source of profile IDs** checkbox.
8. If you want *Bravura Pass* to generate a list of attributes for each account during auto discovery, select **List attributes**.
9. For this demonstration installation, leave other parameters with default values.
10. Click **Add**.

    The ***Administrator credentials*** page displays so you can add a target system administrator for the target.
11. Type the target system administrator's login ID in the **Administrator ID** field.
12. Type the account password in the **Password** and **Confirm password** fields.

13. Click **Update**.

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

Authentication 4

This chapter explains the requirements for configuring authentication to *Hitachi ID Bravura Pass*. For information about more security options, authentication methods including security questions, and authentication chains, see the *Bravura Security Fabric* Documentation .

4.1 How users log in

Users log in using the Front-end (PSF). In general, the Front-end (PSF) authentication process works as follows:

1. A user visits the Front-end (PSF) login page by following a link from your corporate intranet, or typing the URL in a browser:

   `http[s]://<host name>`

   if the index page for this instance is set up as the default web page, or

   `http[s]://<host name>/<virtual directory>/`

   to access the login page for an instance that is not set up as the default web page.

2. Depending on how the *identification priority list* is configured, the Front-end (PSF) displays a list of trusted systems for the user to select from.

3. The user enters an ID.

   This is a login ID for a trusted system, profile ID, email address, or other attribute. See Identifying users for more information.

   Console-only users do not have accounts, and therefore must always enter their profile IDs.

4. The Front-end (PSF) determines the authentication methods that are available to the user. If more than one method is available, the Front-end (PSF) displays a pre-configured list for the user to select from.

5. The user authenticates to *Bravura Pass* using the selected method.

6. Depending on how the module is configured, the Front-end (PSF) ensures that the user has a complete profile, then presents the user with a list of available options.

7. The user clicks a link on the main menu to access functionality provided by another *Bravura Pass* module.

4.2 Configuration requirements

The *Bravura Pass* Front-end (PSF) supports multiple, configurable methods of authentication.

4.2.1 Basic configuration

By default, when you add your first target system, *Bravura Pass* automatically configures itself to identify imported users by their ID on the target system, and to authenticate them using the password for their associated account on the target system. No additional configuration is required.

Bravura Pass can also be set up to use security questions, where users type answers to personal questions; however, this option is only available to users after they complete their security question profiles.

4.2.2 Modified configuration

If you want to modify default behavior, proceed to Login and authentication in the *Bravura Security Fabric* Documentation to learn how to:

- Identify users on different systems
- Configure options for password authentication
- Configure options for security question authentication
- Learn how to enable authentication methods via Front-end (PSF) configuration

To learn how to modify the default password policy, or add additional policies, see Password Policy.

To learn how to modify default question sets, or add additional question sets, Question Sets.

4.2.3 Advanced configuration

Bravura Pass's plugin architecture allows you to add external authentication methods. See Configuring external question sets and authentication plugins for details.

Authentication chains offer more flexible authentication options. See Authentication Chains: Configuration for details.

Configuring Email Notification

5

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

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

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

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

Table 5.1: Email options

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

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

Importing and Managing Users

6

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

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

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

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

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

6.1 Importing users

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

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

   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.

6.1.1 User types and access controls

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

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

Regular user A user who has an account on a target system, and can log into *Bravura Pass*.
Generally, you create regular users by creating a source of profiles in *Bravura Pass*.

Requester A user who can request access changes.
In general, all regular users can be requesters; however, a user's ability to submit requests may be limited by his access rules, policy rules, or *Bravura Pass* configuration.

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

Delegation manager A user who can delegate the responsibilities of a user to another user.
You can grant this capability by assigning a user the "Delegate workflow requests" user access rule. This capability can also be delegated.

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

6.2 Product administrators

This section demonstrates how to set up an existing *Bravura Pass* user as an product administrator with required access controls:

1. Click **Manage the system** → **Security** → **Access to product features** → **Individual administrators**
2. Click **Add new . . . .**
3. In the **ID** field, search for, or type the profile ID of an existing user.
4. Select **The user has the following selected access controls** then select appropriate rights from the list.
5. Click **Add** at the bottom of the form.

See Product administrators in the *Bravura Security Fabric* Documentation for more detail on product administrators.

6.3 User access rules

This section shows you how to define *user access rules* to control access to user profiles for self-service users and help desk users. User access rules define which *privileges* a group of users can have, and user classes define membership criteria for each user access rule. See User classes for more information about user classes.

Use the ***Access to user profiles*** page to configure user access rules. To navigate to this page:

1. Click **Manage the system** → **Security** → **Access to user profiles**.
2. Click a category:
   - **Global help desk rules** (p28) – these rules control what help desk users can do for all other users.
   - **Self-service rules** (p29) – these rules control what regular users can do for themselves.
   - **Delegated administration rules** (p29) – these rules have two participants, and control what one participant (requester) can do for the other participant (recipient).
3. Search for or select an existing user access rule, or click **Add new...**

The main types of user profile access rules are:

- Global help desk rules (p28)
- Self-service rules (p29)
- Delegated administration rules (p29)

Global help desk rules

- Specify what help desk users can do for all other users.
- Apply to users in a single-participant user class - that is, individual users are included based on an attribute or group membership.

The standard global help desk rules are:

ALLREQUESTERS Defines privileges that apply by default to all regular users.

API_REQUEST Defines privileges for API users.

API_TPM_REQUEST Defines privileges for API users of Phone Password Manager.

GLOBAL_HELP_DESK Defines privileges for basic, front-line help desk users.

HELP_DESK_MANAGER Defines privileges for all help-desk managers.

Note: The **Unlock accounts**, **Manage tokens** and **Generate voice print enrollment PIN** privileges all require configuration. If not yet configured, "(Disabled)" is displayed next to their name.

The **Update security questions**, **View security questions**, and **Bypass security questions** privileges have "(Disabled)" displayed next to their name, when the *Update security questions* (PSQ) module is disabled.

Self-service rules

- Specify what self-service users can do for themselves.
- Apply to users in a single-participant user class - that is, individual users are included based on an attribute or group membership.

The default self-service rule is:

ALL_SELF_REQUEST All self-service users who make requests for themselves.

Note: The **Unlock accounts**, **Manage tokens** and **Generate voice print enrollment PIN** privileges all require configuration. If not yet configured, "(Disabled)" is displayed next to their name.

The **Update security questions** privilege has "(Disabled)" displayed next to it when the *Update security questions* (PSQ) module is disabled. If this privilege is not selected, users are not required to update their security questions when logging in, and the link is not displayed on the main menu.

Delegated administration rules

- Allow the same privileges as the global help desk rules.
- Include users based on a *relational user class* – that is, there are multiple participants which are defined as either requester or recipient. An example of this is a manager-subordinate relationship.
- Specify what the requester can do for the recipient.
- Have no default rules defined.

See Access to user profiles in the *Bravura Security Fabric* Documentation for details.

Next:

- Configure user classes to apply the rules to certain users.

6.4 User classes

In *Hitachi ID Bravura Pass*, a *user class* is a way to segment users. A user class defines the criteria for segmenting users.

User classes are used throughout *Bravura Pass*, to help configure product administrators, user access rules, plugins, membership, and relationships between users.

User class criteria

There are three types of criteria that you can use to determine segmentation:

Attribute criteria – defined by profile and request attributes

Membership criteria – defined by group membership

PSLANG criteria – defined by PSLANG expressions

For this document, we will demonstrate how to configure the GLOBAL_HELP_DESK class to include front-line help desk users based on group membership. This section shows you how to:

1. Manage a group on which to test class membership.
2. Add the group membership as user class criteria.
3. Add explicit users to the class.

6.4.1 Managing a group

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

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

When a group is managed:

- The group's membership can be used to segment users into user classes.

If supported by the target system, *Bravura Pass* connectors can list groups during auto discovery. Group owner information is included if it is available. You can configure *Bravura Pass* so that it automatically manages groups.

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.
- **All groups, approval required**: Manage all groups on the target system.
- **All groups, no approval required**: Manage all groups on the target system.

  The approval settings only apply to *Bravura Identity*, *Bravura Privilege*, and *Bravura Group*.

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

1. Click **Manage the system** → **Resources** → **Groups**.
2. Select the target system on which the group resides.
3. Select the group that you want to manage.
4. Click **Manage**.
5. Execute auto discovery to load group memberships into the *Bravura Pass* database.

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

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

6.4.2 Defining user class criteria

Criteria allow you to test users in order to define which users belong to a user class. There are three types of user class criteria that you can use to determine segmentation:

Attribute criteria – defined by profile and request attributes, and only apply to personal user classes.

Membership criteria – defined by group membership, and only apply to personal user classes.

PSLANG criteria – defined by PSLANG expressions, and apply to both types of user classes.

To use membership criteria based on the group you selected in Managing a group:

1. Click **Manage the system** → **Policies** → **User classes**.
2. Select the GLOBAL_HELP_DESK user class.
3. Select the **Criteria** tab.
4. Click **Add new...** in the group membership section.
5. Choose the appropriate value from the **Membership** drop-down list. Select:

- **Required** – to include users who belong to the specified group in the user class.
- **Disallowed** – to include users who do *not* belong to the specified group in the user class.

6. Search for, or type the ID of the **Target system** to which the group belongs.
7. Search for the ID of the managed **Group**.
8. Click **Add**.
9. Test the user class.
   (a) Click the **Test** tab.
   (b) Search for, or type the User ID of the user to evaluate
   (c) Click **Test**.
10. If required, repeat the above procedure to add additional criteria to the user class.

6.4.3 Selecting explicit users

Personal user classes, which have only one participant, allow you to specify explicit users. Explicit users are included in the user class regardless of the user class criteria.

To add explicit users to the class:

1. Click **Manage the system** → **Policies** → **User classes**.
2. Select the GLOBAL_HELP_DESK user class.
3. Select the **Explicit users** tab.
4. Click **Select...**.
5. Enabled the checkboxes for the users you want to select as explicit users.
   Alternatively, you can search for a user.
6. Click **Add**.

For more detailed information on user classes, see User classes in the *Bravura Security Fabric* Documentation .

Setting up User Notification 7

The *Hitachi ID Bravura Pass* user notification system allows you to:

- Streamline *Bravura Pass* deployment and ensure continued security compliance
- Notify users of pending password expiry
- Notify users of other events
- Force users to comply with registration or other requirements

There are two kinds of notification events:

Batch notifications are evaluated at certain times of day, or as requested by *Bravura Pass* administrator. They are evaluated for all users, and those that meet the selection criteria are usually sent notification via email.

Web notifications are triggered when a single user does something, such as log into a workstation or into *Bravura Pass*.

The action or event causes a connection with the Notification Service (psntfsvc), which evaluates which notifications apply to the user, and whether any action needs to be taken. For example, a user logging into his workstation may have a reminder for a pending password expiry. The service could then cause a browser to open for the user to log in and then show an informational page for the notification.

Web notifications can be configured to force the user to take action before allowing them to proceed. In the example above, the service might log the user off if he closes his web browser without changing his password.

7.1 User notification system components

The *Hitachi ID Bravura Pass* user notification system consists of three main components:

Notification Service (psntfsvc) updates the database with information about notification events and compliance rules, and runs plugins that:

- Check if a user is in compliance for a particular event
- Send reminders to non-compliant users, either by web or email
- Take action if the reminder limit for a user is exceeded
- Generate a list of non-compliant users for batch notification

Notification Client (psntfclient) is required only if users will receive notification via their web browser. The client is installed on a network share and is responsible for contacting the Notification Service to determine if users have any pending notifications. If they do, the **`psntfclient`** program opens a browser on the user's workstation for the user to first log in and then to display the notification message in *Bravura Pass*. If any of those notifications are force-level, the **`psntfclient`** opens the browser in kiosk mode, preventing the user from accessing navigation or other functionality until the user becomes compliant.

***User notifications* (PSN) module** acts as the gateway between the Notification Client and the Notification Service, and enables users to receive, acknowledge, and act on notifications from their web browser.

7.1.1 Installing the notification Client (psntfclient)

Client software is required only if users will be notified via their web browser. For Windows clients, Hitachi ID Systems provides **`ntfclient.msi`**, or **`ntfclient-x64.msi`** for 64-bit systems. For Unix/MacOSX clients, you can write a Perl script based on **`ntfclient.pl`**, located in the samples directory.

To manually install the Notification Client for Windows, copy the **`ntfclient.msi`** or **`nftclient-x64.msi`** installer from the <*instance*>\addon\ directory to a scratch directory (C:\temp) on the local workstation or to a publicly accessible share. Launch the installer and follow the prompts. For more detail, see Notification Client (psntfclient) in the *Bravura Security Fabric* Documentation .

> **Note:** The installer simply copies the **`psntfclient`** program to the file system. It does not configure the client to launch. It is recommended that you install the client on network share, and set up a GPO (Group Policy Object) to launch the client with a command such as `psntfclient.exe -userid %USERNAME%`.

See also:

- Installing add-on software for general requirements for using a client MSI installer, and instructions for automatic installation using a group policy.
- Add-on Installers in the *Reference Manual* for more information about setting MSI properties in a transform file or from the command line.

- psntfclient in the *Reference Manual* for more information about the client, including command line usage.

7.2 Adding password expiry detection

Hitachi ID Bravura Pass can detect when users' passwords are about to expire on some target systems. It can also keep track of when their passwords will expire based on the last time the passwords were changed and *Bravura Pass* password policies. Based on these criteria, *Bravura Pass* can determine that it is time for users to change their passwords. If both the target system **Check password expiry** and *Bravura Pass* password policy rule for **password must be changed every N days** are in effect, the earliest expiry time is used. *Bravura Pass* informs users of the upcoming expiry, and asks them to change all of their passwords using *Bravura Pass*, rather than changing individual passwords on the target systems as they expire. *Bravura Pass* notifies users either by email batch notifications, or by web notifications where the user's browser opens to an instructional notification page during network login.

7.2.1 Initial considerations

To determine the best solution for expiry notification, answer the following questions:

1. **Where is the expiry information coming from?**

   You can gather a list of soon-to-expire users from:

   - One or more target systems

     In most environments, password aging is already implemented on one or more target systems. Using target systems as the source means that users' existing scheduled password expiry dates should not be affected.

   - The *Hitachi ID Bravura Pass* database

     The *Bravura Pass* password policy rule for **password must be changed every N days** is enabled to expire passwords.

   - Both target systems and *Bravura Pass* database

     For example, configure the *Bravura Pass* password policy to expire passwords every 80 days and – if required – adjust the password policy on integrated systems to expire passwords every 90 days. This way, *Bravura Pass* passwords will expire first and users will never see the expiry warnings from individual systems and applications.

     Alternately, if feasible, set *Bravura Pass* password expiry to 90 days and modify expiry on all integrated systems to 100 days. This allows a typical organization to retain a 90 day expiry period overall, but involves a bit more change control on existing systems.

2. **How do you want to notify users?**

   You can configure *Bravura Pass* to:

   - Automatically open a browser at the *Bravura Pass* web site when a user first logs into their workstation.

- Send a batch email notification to all users whose passwords are about to expire.
- Take some other action.

> **Note:** If password expiry is enabled on users' primary login account – for example, Active Directory – it is recommended that you do *not* configure *Bravura Pass* to notify users whose password has already expired. This could lead to a situation where a user logs in and receives an expiry notification from the operating system, then changes his password using the operating system's native method. Once logged in, the user would receive a *Bravura Pass* notification to change a password he's already changed. It is also recommended that transparent password synchronization is implemented in this case.

7.3 Configuring web notifications

Once you have installed the Notification Client (psntfclient), you can set up web notifications.

7.3.1 Configuration example: Acceptable use policy

You can use the web notification module to force all users to view, then accept or decline an agreement, such as an acceptable use policy. The following example shows you how to set up a force-level policy agreement:

1. Click **Manage the system** → **Policies** → **User notifications** → **Web notifications** .
2. Click **Add new . . .** .
3. Type the notification **ID** and **Description**. The notification ID can only contain ASCII characters.
4. Set the notification **Severity** to **Forced**.

   If the web browser is closed without the required action taken, the user is forced to log out of the workstation.
5. Set the **Plugin to run to determine compliance** to **Query USERSTAT tag** .
6. Click **Add**.

   Hitachi ID Bravura Pass warns you that the compliance plugin requires configuration.
7. Click the configure icon next to the compliance plugin field.
8. Configure parameters for agreement compliance:

   (a) Direct users to external URL with the value `PSNAUP`.

   This is required for a policy compliance plugin and directs users to a page where they view and accept or decline agreement.

(b) Type a **Message to display to a non-compliant user** .

(c) In the **Acceptable use policy** section, click **Enabled**.

Bravura Pass displays policy configuration settings. Required settings are pre-configured with m4 tags that are defined in \<*instance*>\design\src\z\psn.m4. The tags are mapped to macros defined in \<*instance*>\design\src\common\<*lang*>-<*locale*>-language.kvg.

m4 tag	macro	en-us-language.kvg definition
!!!N_AUP_MESSAGE	_PSN_AUP_TITLE	Acceptable use policy
!!!N_AUP_BUTTON_ACCEPT	BUTTON_ACCEPT	Accept
!!!N_AUP_BUTTON_DECLINE	BUTTON_DECLINE	Decline

(d) Modify policy configuration settings to suit your policy.

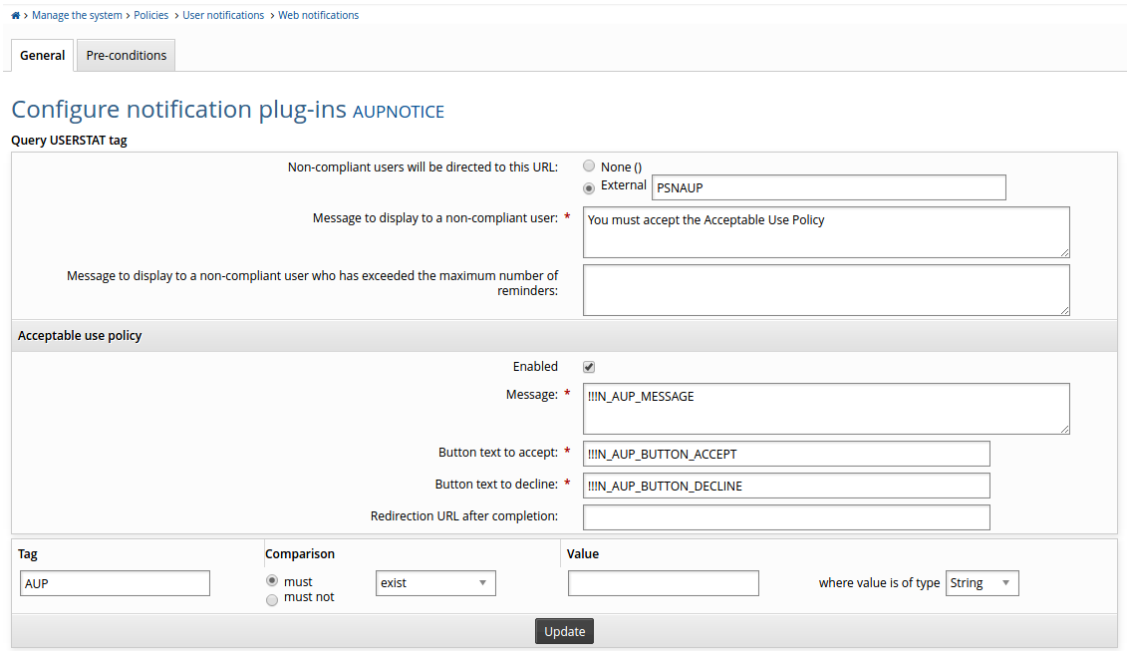
For example, you may want to add a lengthier message in multiple languages. You could add a custom macro `AUP_MESSAGE` and include it under the `!!!N_AUP_MESSAGE` tag in psntfsvc.m4, then define the macro in custom language kvg files. See Adding macros to messages to learn how to add custom tags and macros.

(e) Set the **Tag** that you want to evaluate to determine non-compliant users.

For example, set the tag name to `AUP` (if the tag does not exist, the plugin creates it) and set it to "must exist" and leave the value field blank. This will flag users who do not have the tag or the tag is blank.

9. Click **Update**.

When a user clicks **Accept**, the **AUP DONE** event action is triggered. When a user clicks **Decline**, the **AUP NOT DONE** event action is triggered. You can configure these event actions in the **Manage the system** → **Modules** → **User notifications (PSN)** menu. See Event Actions (Exit Traps) for more information.



7.3.2 Configuration example: Forced-level password expiry notification

The following example shows you how to set up a force-level password expiry notification:

1. Click **Manage the system** → **Policies** → **User notifications** → **Web notifications** .
2. Click **Add new . . . .**
3. Type the notification **ID** and **Description**. The notification ID can only contain ASCII characters.
4. Set the notification **Severity** to **Forced**.

   If the web browser is closed without the required action taken, the user is forced to log out of the workstation.
5. Set the **Plugin to run to determine compliance** to **Password expiry** .
6. Click **Add**.

   Hitachi ID Bravura Pass warns you that the compliance plugin requires configuration.
7. Click the configure icon next to the compliance plugin field.
8. Configure parameters for password expiry.

   For example, select **Internal link** to direct users to the Change passwords (PSS), and set the required **Number of days before expiry that the user will be notified** and **Message to display to a non-compliant user** .
9. Click **Update**.

For detail on configuring this and other types of web notifications, see Configuring web notifications in the *Bravura Security Fabric* Documentation .

7.3.3 Testing web notifications

To test web notifications, type on the command line, in the util directory:

```
ntftrigger.exe -getusernotification -notifyid WEBNOTE -user brownwi
```

See ntftrigger in the *Reference Manual* for more information about **`ntftrigger`**.

7.4 Configuring batch notifications

No additional software installation is required for batch notification.

7.4.1 Configuration example: Warning users to register security questions

The following example shows you how to set up a batch notification to disable users' profiles if they ignore two warnings to register their security questions:

1. Click **Manage the system** → **Policies** → **User notifications** → **Batch notifications** .
2. Click **Add new . . . .**
3. Type the notification **ID** and **Description**. The notification ID can only contain ASCII characters.
4. Set the notification **Severity** to **Warning**.
5. Set the **Plugin to run to determine compliance** to **Security questions registration** .
6. Select the radio button for **Maximum number of messages to send per user** and type 2 in the adjacent field.
7. Set the **Plugin to run when reminder limit is exceeded** to **Disable profile**.
8. Click **Add**.
9. Configure plugin options.

   For this example, only the plugin responsible for delivering the reminders requires configuration.

   (a) Click the configure icon 🔍 next to the **Plugin to run to deliver compliance reminder** field.

   (b) Enter the required subject and message details. These plugins also use settings defined in the **Manage the system** → **Workflow** → **Email configuration** menu.

   (c) Click **Update**.

10. Schedule the notification:

    (a) Click the **Schedule** tab.

    (b) Configure scheduling options.

    See Batch notification scheduled job settings for detail.

    (c) Click **Add**.

For detail on configuring this and other types of batch notifications, see Configuring web notifications in the *Bravura Security Fabric* Documentation .

7.4.2 Testing batch notifications

To test batch notifications, on the ***Batch notification information*** page for a notification, click the **Schedule** tab, then select **Run now**.

Alternatively, type on the command line, in the util directory:

```
ntftrigger.exe -runbatch -notifyid <notification ID> -increment P
```

See ntftrigger in the *Reference Manual* for more information about **`ntftrigger`**.

Part III

USING PASSWORD MANAGER

Updating Your Security Questions

8

When you log into *Hitachi ID Bravura Pass* you must verify your identity, either by using a secure password or by answering questions that you set up in your *security question profile*.

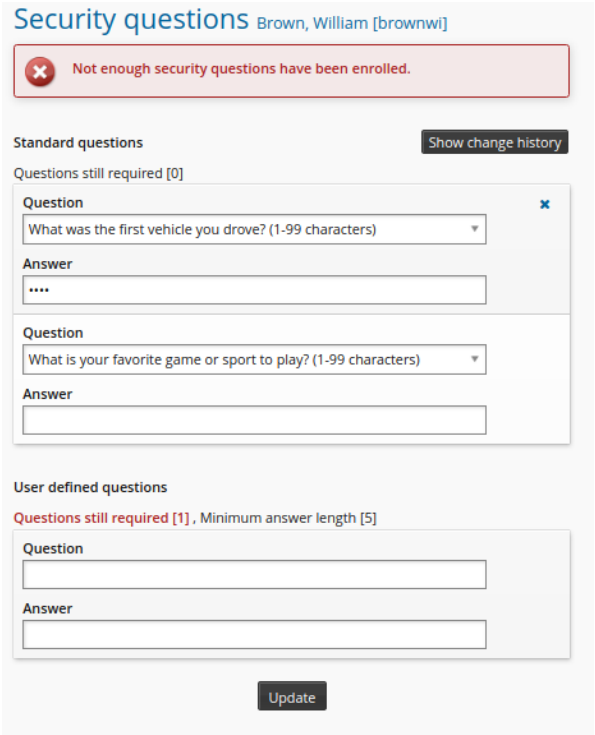
This authentication method can also be used when someone in a help-desk organization is assisting you, and needs to verify your identity before proceeding.

This section shows you how to define and maintain your own security question profile. When you access *Bravura Pass* for the first time, you must authenticate using your network password or other method.

To update your security question profile:

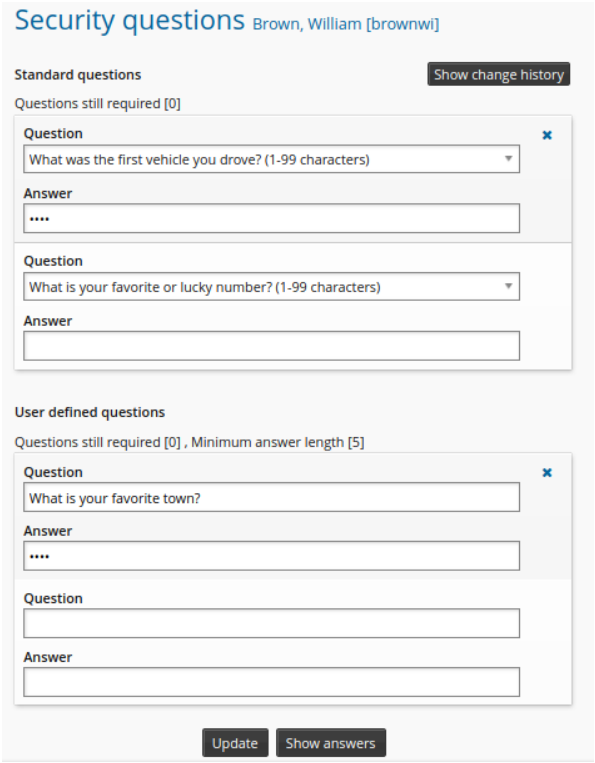
1. From the main menu , click **Update security questions**.

   Bravura Pass displays a message to tell you whether you have enough questions defined and how many question and answer pairs you need to define for each set.



   If answers were previously supplied, they are obscured. If your profile is complete and you have the

required permission, you can click **Show answers** to view answers in plain text.



If an answer was changed by someone else, a caution icon is displayed under the answer.

To view details of when each question was last changed, and who changed them, click **Show change history**. To hide these details, click **Hide change history**.

2. Enter new question and answer pairs, or edit questions or answers in the security question sets displayed on the screen,

   You may be required to select pre-defined questions from a drop-down list, or type in your own questions in the fields containing `*new*`.

   Following is a list of *suggested* questions:

   - First school attended
   - Favorite board game
   - Favorite song
   - Favorite dessert
   - Favorite book character
   - Furthest place travelled
   - Color of first car

- Birth city
- High school mascot
- Childhood street name
- Favorite actor/actress/celebrity is
- Favorite band
- Name of first girlfriend/boyfriend

3. Click **Update**.

Changing Your Passwords 9

You can change passwords on all the systems where you have a login account using the *Hitachi ID Bravura Pass* web interface.

If you need to change a password that you have forgotten, you can access the web interface using another authentication method. This can be another password on a trusted system, security questions, a hardware token (for example, SecurID, SafeWord), or some other means.

Bravura Pass also allows you to synchronize passwords for a group of login accounts, so that you have fewer passwords to remember. The number of passwords you need depends on your organization's password security policy. *Bravura Pass* can be set up so that you have only one password for all accounts. Alternatively, you may be required to have different passwords on some systems; for example, you may have access to a group of applications that require stricter password security than other accounts.

9.1 Use case 1: Synchronizing your passwords with a single policy

In the simplest scenario, your passwords for all the accounts you own are automatically synchronized when you change your password using the *Hitachi ID Bravura Pass* web interface.

To change or synchronize your passwords using the *Bravura Pass* web interface:

1. From the main menu , click **Change passwords**.
2. Type the new password in the **New password** and **Confirm** fields.

   Password strength rules and suggested passwords are shown below the password fields. The maximum allowable length for a password is 127 characters.
3. Click **Change passwords**.
4. If the changes were successful, close your browser.

   It is recommended that you log out of your workstation, then log in again.

   If the changes were not successful, try again later.

Unlocking Your Accounts 10

If you are locked out of an account because of too many failed login attempts, you can unlock your own accounts by using the *Hitachi ID Bravura Pass* web interface, rather than by calling the help desk.

You access the web interface using another authentication method. This can be another password on a trusted system, security questions, a hardware token (for example, SecurID, SafeWord), or some other means. See Logging into *Bravura Pass* in the Bravura Security Fabric *Self-Service and Help Desk User Guide* for more information.

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

To unlock your own accounts using the *Bravura Pass* web interface:

1. From the main menu , click **Unlock accounts**.
2. Enable the checkboxes next to the accounts you want to unlock and click **Unlock**.
3. Close your web browser if the changes were successful, or click **Unlock accounts** to try again.
4. It is recommended that you log out of your workstation, then login again.

Managing Your SecurID Tokens

11

If you have an RSA SecurID Authenticator (token), *Hitachi ID Bravura Pass* can be set up so that you can manage your token, and set and clear your PIN.

11.1 Getting started

To manage your tokens and PIN:

1. From the main menu , click **Manage tokens**.
2. If you have more than one token, select  the token you want to manage.

   Bravura Pass displays the management page for the token you selected. Now you can:

   - Enable or disable your token (p48)
   - Request or clear emergency access codes (p48)
   - Set or clear a PIN (p49)
   - Resynchronize your token (p50)

11.2 Enabling and disabling tokens

From the token management page (p47) you can select the:

- **Enable token** option to activate a new token
- **Disable token** option to deactivate a lost or stolen token

> **Note:** If a user's token is marked as being both disabled and the token has been entered into emergency access mode (marked as being lost), the token will become invalid and users will no longer be able to access their token from the *Manage tokens* (PSP) module. Only product administrators will be able to access the token to either re-enable it or to take the token out of emergency access mode to mark it as no longer being lost.

11.3 Getting emergency access codes for temporary use

Use emergency access codes if you need access to a system protected by SecurID but don't have your token with you. You may specify your own fixed password, have a fixed password be randomly generated, or have *Bravura Pass* generate several more secure one-time passwords for you.

11.3.1 Requesting a fixed password

To request a fixed password:

1. Navigate to the token management page (p47).
2. In the **Put token into Emergency Access Mode** section:
   (a) Type the number of hours for which the code will be valid in the **Number of hours before Emergency Access Mode expires** field.
   (b) Enable **Use a fixed password**, and type your password in the adjacent text field.
   This password must conform to the password rules set by the RSA Authentication Manager server.
   Enter -1 in order to have a fixed password be randomly generated.
3. Select the **Put token into Emergency Access Mode** option.
   Bravura Pass confirms entry into emergency access mode.
4. Make note of the emergency access password you created.

11.3.2 Requesting one-time passwords

To request one-time passwords:

1. Navigate to the token management page (p47).
2. In the **Put token into Emergency Access Mode** section:
   (a) Type the number of hours for which the codes will be valid in the **Number of hours before Emergency Access Mode expires** field.
   (b) Enable **Use one-time passwords**.
   (c) Type a value in the **Number of passwords to generate** field. Each code may only be used once.
3. Select the **Put token into Emergency Access Mode** option.
   Bravura Pass confirms entry into emergency access mode.
4. Make note of the emergency access codes you were given.

> **Note:** Each emergency access code can be used only once.

11.3.3 Clearing emergency access mode

To clear the emergency access mode, if you found your token, select the **Take token out of Emergency Access Mode** on the token management page.

11.4 Setting and clearing a PIN

To set a new PIN for your token, especially if you forgot your current PIN:

1. Navigate to the token management page (p47).
2. In the **Set token PIN** section, type a new **PIN** that will satisfy the requirements of the Token Policy on the RSA Authentication Manager 7.1/8.2 server or leave the **PIN** field empty if you want *Bravura Pass* to select a random PIN for you.
3. Select the **Set token PIN** option.
4. Take note of the new PIN displayed on the screen.

To clear a pin, select the **Clear token PIN** option on the token management page.

11.5 Resynchronizing a token with the RSA Authentication Manager

To resynchronize your token with the RSA Authentication Manager:

1. Navigate to the token management page (p47).
2. Type the code displayed on your token in the **Code displaying on token now** field.
3. Select the **Resynchronize token** option.
4. Wait for the display on your token to change. Type the new code displayed on your token in the **New code displaying on token** field.
5. Select the **Resynchronize token** option.

   Bravura Pass confirms that the resynchronization is successful.

File Locations A

There are three main directories that are created when you install *Bravura Pass* instance:

- <*Program Files path*>\Hitachi ID\IDM Suite\<*instance*>\
- <*Program Files path*>\Hitachi ID\IDM Suite\Logs\<*instance*>\
- <*Program Files path*>\Hitachi ID\IDM Suite\Locks\

When you install *Hitachi ID Connector Pack*, files are placed in different locations depending on the type of *Connector Pack*.

For an instance-specific connector pack, the installer, **`connector-pack-x64.msi`**, installs agent connectors in:

<*Program Files path*>\Hitachi ID\IDM Suite\<*instance*>\agent\.

For a global connector pack, the installer, **`connector-pack-x64.msi`**, installs connectors and supporting files in:

- <*Program Files path*>\Hitachi ID\Connector Packs\global\agent\.

See “File Locations” in the *Bravura Security Fabric* Documentation for more detail.

Index

W

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