

***Bravura Privilege* Implementation:**

Onboard Systems

This document contains:

- [About Managed Systems](#)
- [Modes: push, local service and vault-only systems](#)
- [Use case: Creating a push-mode managed system](#)
- [Self-service system management](#)
- [Use case: Onboarding managed systems](#)

Terminology

The following terminology is used in this document:

Managed systems A workstation or server which is a member of a *Hitachi ID Bravura Privilege* managed system policy. *Bravura Privilege* periodically randomizes administrator passwords on a managed system and automatically stores the ID and password in the *Bravura Privilege* database.

Managed system policy A container for configuration information for managed systems. Policies define user access, which accounts and groups to manage, password randomization and creation, session monitoring and recording, methods and rules.

Local service mode The Local Service is a service installed on each IT resource that will be managed by *Bravura Privilege*. It performs local password resets and communicates with the *Bravura Privilege* server.

Privileged Access Manager Service (idarch) The Privileged Access Manager Service (*idarch*) is a service installed on the *Bravura Privilege* server. It performs remote password resets on IT resources. It can be used where there is a requirement for zero software footprint on local resources, or for systems other than Windows and Unix. It also handles password check-out / check-in functionality.

Vault-only systems A workstation for which administrator IDs and passwords are stored manually on the *Bravura Privilege* database. Unlike managed workstations, there is no service installed on a vault-only workstation and passwords are not randomized.

1 About Managed Systems

IT assets often have multiple sensitive passwords such as administrator passwords, service passwords, application passwords. These passwords commonly do not have expiry enabled. Changing these passwords can be time-consuming because of the large number of IT assets, users who need to know the passwords, and configuration interfaces, scripts, or programs that may contain hard coded passwords.

Hitachi ID Bravura Privilege secures administrative passwords on servers and workstations by periodically randomizing them, while maintaining the ability of IT staff to retrieve current credentials for devices into which they must log in. In the context of *Bravura Privilege*, these systems are referred to as *managed systems*.

You can make any target system a managed system by selecting the **Automatically create a Privileged Access Manager managed system** setting on the **Target system information** page.

The Privileged Access Manager Service (idarch) uses parameters of the target system to determine which connector program to run and what credentials to use when it resets passwords for a managed system.

2 Modes: push, local service and vault-only systems

Hitachi ID Bravura Privilege randomizes passwords using either *push mode* or *local service mode*. In *vault-only* mode, *Bravura Privilege* only stores information. This section explains the differences between the modes, and how to determine which mode to use.

2.1 Push mode

In push mode, *Hitachi ID Bravura Privilege* performs remote password resets using the Privileged Access Manager Service (idarch).

Changes at the *Bravura Privilege* server typically trigger immediate actions on managed systems; whereas, in local service mode, actions are triggered when the workstation connects to the server at the end of the next polling interval.

A system can be managed in push mode when it is manually added as a target system, or when it is discovered on a domain. Accounts can also be managed manually or during auto-discovery.

Choose push mode if you:

- Do not want a software footprint on your servers or workstations
- Require “real time” integration
- Want to manage passwords on systems other than Windows
- Have systems in a DMZ that cannot connect to your *Bravura Privilege* server

2.2 Local service mode

In local service mode, you install the Privileged Access Manager Local Workstation Service (hipamlws) on the system you want to manage. Local service mode works as follows:

1. After installation on the system to be managed, the Local Workstation Service waits a finite random amount of time.
This prevents large numbers of Local Workstation Services, installed during a mass deployment, from contacting the *Hitachi ID Bravura Privilege* server simultaneously.
2. The Local Workstation Service then connects to the PAMLWS module on the *Bravura Privilege* server over HTTP or HTTPS (recommended) and registers itself with *Bravura Privilege*. This initiates the discovery process, during which the system is listed as a discovered object, and evaluated against import rules. This process is repeated until the system passes an import rule and is managed, or is disabled.
3. Once a system is discovered and managed, the *Bravura Privilege* server periodically checks on what needs to be done, based on workflow requests and password expirations, and sets the necessary flags for it.
4. The Local Workstation Service periodically connects to, or polls, the PAMLWS module over HTTP or HTTPS to check on any tasks, such as listing users and attributes, changing a password, or adding and removing users from groups.
5. The Local Workstation Service performs the assigned task, if any, and sends the required data back to the PAMLWS module at the next poll. This may either be the list of users, groups and attributes, or success and failures on other tasks. It will wait a configured amount of time before connecting to the *Bravura Privilege* server again.

Local service mode is only available for Windows systems; however, a plugin architecture supports applications running on Windows.

Choose local service mode if you have:

- Many Windows machines that are not permanently connected to the domain (laptops, workstations etc.)
- Systems that aren't always on or are periodically unavailable.

Note: When users request privileged access on local service mode systems, group and account operations may take longer than on push mode systems, since *Bravura Privilege* is required to wait for communication from the local workstation.

2.3 Vault-only systems

Vault-only policies can be used to manually store information about managed systems. For these policies, there is no communication between the *Hitachi ID Bravura Privilege* server and the managed system. *Bravura Privilege* does *not* automatically randomize passwords for these managed systems. Users can be granted permission, via access controls, to randomize or override the stored passwords.

3 Use case: Creating a push-mode managed system

In order to manage credentials for a managed system, you must first add it to the *Hitachi ID Bravura Privilege* database.


This use case demonstrates how to turn a Linux target system into a managed system, and install components to manage and access accounts on the system.

Requirements

This use case requires:

- *Hitachi ID Bravura Privilege* and *Hitachi ID Connector Pack* installed
- Linux target system manually added

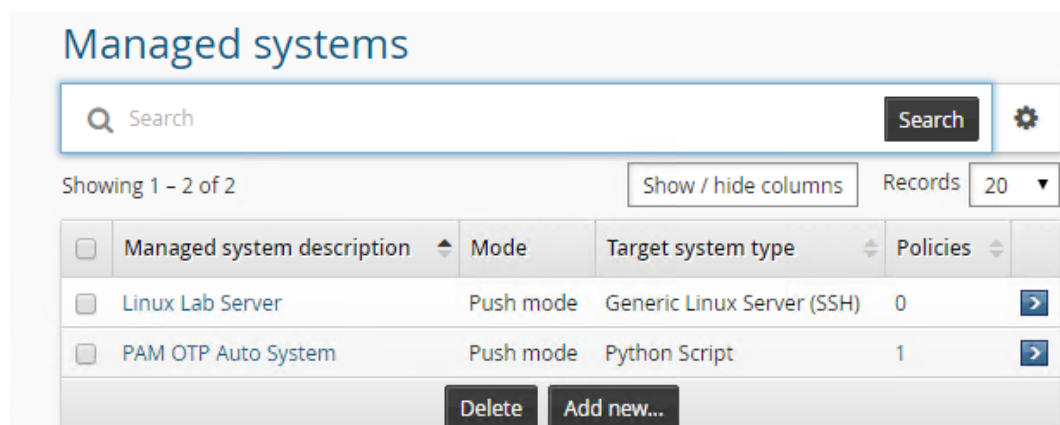
Create a managed system

- Log in to *Bravura Privilege* as `superuser`.
- Click **Manage the system** → **Resources** → **Target systems** → **Manually defined**
- Select  the LINUX target system.
- Select **Automatically create a Privileged Access Manager managed system**.
This allows you to manage privileged accounts on this system.
- Scroll to the bottom of the page and click **Update**.
- Run auto-discovery again to add the target as a managed system.
 - Click **Run discovery** at the bottom of the page.
 - Confirm you want to start the update.

View the managed systems

To view the managed systems in *Hitachi ID Bravura Privilege*:

1. Click to **Manage the system** → **Privileged access** → **Managed systems**.
2. Verify that the LINUX target system is listed as a managed system.



4 Self-service system management

The previous use case demonstrated how product administrators add managed systems manually via the *Manage the system* (PSA) module. After the initial set up of *Hitachi ID Bravura Privilege* it will become more common practice for team trustees to onboard new systems that have not been managed yet. Pre-defined requests (PDRs) give the trustees the ability to add managed systems and accounts easily.

The *Bravura Privilege* self-service request facility provides a high degree of flexibility, allowing users to request changes that involve operations on technical resources.

Installing *Hitachi ID Bravura Pattern: Privileged Access Edition* configures several pre-defined request to simplify team and resource management. The following sections focus on requests that allow team trustees to onboard, update, archive and offboard systems managed by *Bravura Privilege*.

Using the **System: Onboard** request, trustees onboard a system by specifying the system's type, address, proxy zone and either new or existing credentials with which *Bravura Privilege* will connect to the system (both operationally and as evidence that the requester already has access to the system in question).

Before using the managed system onboarding request, you must install one of the optional scenario components that support the following types of systems:

- Linux: CentOS/RHEL/SuSE.
- Database: Oracle.
- Windows server.
- Solaris
- AIX

Components can be readily developed to integrate with other types of systems and applications.

Trustees can use the **System: Update** request to move a managed system to a different team.

Using the **System: Archive** request, a trustee offboards a managed system by moving its credential and check-out history data to an archival policy. It is strongly advised to use the **System: Archive** PDR to

offboard a system 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 *Bravura Privilege*.

4.1 Onboarding a system

Users assigned as team trustees can use the **System: Onboard** request to onboard a system.

The screenshot shows the 'System: Onboard' form. The main area contains the following fields:

- System Instance ID ***: odb1
- System Port**: 1521
- System Team ***: Databases

The right sidebar contains the following sections:

- System Type Info**: 1 attributes changed. Includes a '+ System Type' button.
- System onboarding details**: 4 attributes changed. Includes buttons for '+ System Instance ID', '+ System Port', '+ System Team', and '+ Zone'.
- System onboarding credentials**: (Empty section)
- Requester notes:** (Text input field)

At the bottom of the form are three buttons: 'Previous', 'Next', and 'Submit'.

Once the request has been approved, trustees can manage accounts on this system. Systems are onboarded in real time; there is no need to wait for auto discovery to load the system into the database.

4.2 Migrating a system to another team

Users assigned as team trustees can use the **System: Update** request to migrate a system to another team.

4.3 Offboarding a system

The offboarding process usually involves disabling a system while data is archived, then deleting it. Users assigned as team trustees can use the **System: Archive** request to disable or delete a system.

WARNING!: When you delete a system, all historical password data associated with accounts on the system will be deleted. To ensure that data is kept, disable it instead.

Note: You cannot delete a system that still has managed accounts associated with it.

See also:

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

5 Use case: Onboarding managed systems

This use case demonstrates how to install an optional scenario component to support Windows system onboarding. Acting as a trustee, the user will onboard a system for their team.

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

Install the Windows onboarding and disclosure components

1. Log in to *Bravura Privilege* as `superuser`.
2. Click **Manage Components** → **Scenario**.
3. Select the checkbox for `Scenario.pam_system_type_winnt` and `Scenario.pam_disclosure_rdp_local_account`.
4. Click **Install component(s)** from the Actions panel on the right.

The component management program installs the components along with any dependencies. You should see "Completed install for component" messages for the selected components in the **Details** section of the Actions panel.

Onboard a Windows system

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. Click **System: Onboard**.
4. In the **System Type** field, select "Windows Server".
Click **Next**.
5. Enter the **System FQDN** and **System Team**.

The screenshot shows a web interface titled "System: Onboard". The main area is "System onboarding details" with two input fields: "System FQDN *" containing "wkstn1.hitachi1.corp" and "System Team *" with a dropdown menu showing "Windows Admin Accounts". To the right is a "Details" sidebar with "System Type Info" (1 attribute changed) showing a "+ System Type" button, and "System onboarding details" (3 attributes changed) showing "+ System FQDN", "+ System Team", and "+ Zone" buttons. At the bottom are "Previous", "Next", and "Submit" buttons.

Click **Next**.

6. Add the credentials for the Windows server.
7. Click **Submit**.
8. Click the **View request** link at the top of the page to view the status of the request.
9. In the Actions panel on the right, click the **Request:** ID to review the details of the request. Next to **Display details:** check the box for **Operations** to ensure the onboarding operation is listed as successful.

Request details

Request summary:

Request: 20190411-1	Requester: Cordelia Hodge (CORDEH)
Status: Processed Auto approved	
Request type System: Onboard	
Requester notes: <input type="text"/>	
Display details: <input checked="" type="checkbox"/> Operations <input type="checkbox"/> Authorizers <input type="checkbox"/> Authorization notes	

Add discovered system to inventory:

System	Operation	Status	Results
	Add discovered system to inventory	Approved	Success

Onboard a managed system:

Requested attributes:

Attribute	Requested value	Requester
System FQDN	wkstn1.hitachi1.corp	Cordelia Hodge (CORDEH)
System Team	Windows Admin Accounts	Cordelia Hodge (CORDEH)
Zone		Cordelia Hodge (CORDEH)
System Admin ID	Administrator	Cordelia Hodge (CORDEH)
System Admin Password	****	Cordelia Hodge (CORDEH)
System Type	WINNT	Cordelia Hodge (CORDEH)

Verify the managed systems

To view the managed systems in *Hitachi ID Bravura Privilege*:

1. Log in to *Bravura Privilege* as `superuser`.
2. Click **Manage the system** → **Privileged access** → **Managed systems**.
3. Verify that your Windows target system is listed as a managed system.

Managed systems

Search ⚙️

Showing 1 - 3 of 3 Show / hide columns Records 20 ▾

<input type="checkbox"/>	Managed system description	Mode	Target system type	Policies	
<input type="checkbox"/>	Linux Lab Server	Push mode	Generic Linux Server (SSH)	0	➤
<input type="checkbox"/>	PAM OTP Auto System	Push mode	Python Script	1	➤
<input type="checkbox"/>	WINNT: wkstn1.hitachi1.corp	Push mode	Windows NT Server	1	➤
Delete Add new...					