Bravura Privilege Implementation: Personal Privileged Access

This document shows you how to configure and use the personal privileged access feature.

Terminology

The following terms are used in this document:

Personal administrative account An account with elevated privileges that is owned by a single user.

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

Help desk trustee any user that is a member of the help desk trustee user class, and so can submit a request to assign an owner at account onboard or update.

1 Objective

Technical staff in many companies have their normal employee account as well as an administrator account that contains elevated privileges. These accounts are checked out at the start of almost everyday in order to connect to various systems to complete their tasks. It is tedious to request, check out, and disclose over and over again for something so critical to their day-to-day duties.

Organizations require administrators to streamline their workflow by automatically checking out personal administrator accounts that they have ownership of at login when launching the *Privileged access* app.

2 Solution

The personal privileged access feature automates the request process, allowing specific account access to be assigned to a single owner. The act of signing into *Hitachi ID Bravura Privilege* triggers an automatic check-out of all the owner's personal privileged access accounts.

2.1 Initial considerations

Determine which accounts should be personal administrator accounts and who should own them by considering the following:

- How often is this account accessed?
- Is the same person always accessing this account?

If an account is accessed frequently, such as part of daily tasks, and is always accessed by the same person, it is a good candidate to make it a personal admin account and assign it single ownership.

3 Use case: Onboard an account and assign a single owner

This use case shows you how to configure *Hitachi ID Bravura Privilege* to onboard an account and assign an owner.

Requirements

This use case assumes that:

- *Hitachi ID Bravura Privilege* and *Hitachi ID Connector Pack* are installed.
- An Active Directory target has been configured and is a source of profiles.
- *Hitachi ID Bravura Pattern: Privileged Access Edition* is installed.
- Scenario.pam_personal_admin_management is installed.
- Teams have been configured with account trustees.
- Systems have been discovered and onboarded.

> **Note:** RefBuild.pam_team_management is installed when *Bravura Pattern: Privileged Access Edition* is installed.

> **Note:** Systems onboarded before this component is installed will need to be manually added to the "Personal administrator access" MSP.

Onboard an account and assign owner as an account trustee

1. Log in to *Bravura Privilege* as an account trustee.
2. In the **Requests** section of the main menu, click **Manage Resources**.
3. Click the **Account: Onboard** pre-defined request (PDR).
4. Select a managed account.
5. Click **Next**.
6. Select **Personal administrator access** policy.
7. Configure other settings as appropriate.
8. Click **Next**.
9. Select a privileged access owner.
10. Click **Next**.
11. Configure session monitoring options as appropriate.
12. Click **Submit**.

> **Note:** Help desk trustees can also submit requests, but task will not be implemented until an account trustee approves the request.

4 Use case: Transfer ownership from a team to a single owner

This use case shows you how to configure *Hitachi ID Bravura Privilege* to transfer an account from a team and assign an owner.

Requirements

This use case assumes that:

- *Hitachi ID Bravura Privilege* and *Hitachi ID Connector Pack* are installed.
- An Active Directory target has been configured and is a source of profiles.
- *Hitachi ID Bravura Pattern: Privileged Access Edition* is installed.
- Scenario.pam_personal_admin_management is installed.
- Teams have been configured with account trustees.
- Systems have been discovered and onboarded.
- There is at least one account managed by a team.

Transfer owner of an account from a team to a single owner

1. Log in to *Bravura Privilege* as an account trustee.
2. In the **Requests** section of the main menu, click **Manage Resources**.
3. Click the **Account: Update** pre-defined request (PDR).
4. Select a managed account.
5. Click **Next**.
6. Select the **Personal administrator access** policy.
7. Configure other settings as appropriate.
8. Click **Next**.
9. Select a privileged access owner.
10. Click **Next**.
11. Configure session monitoring options as appropriate.
12. Click **Submit**.

5 Use case: Check out personal admin access

This use case shows you how to assess the personal admin account as the owner.

Requirements

This use case assumes that:

- *Hitachi ID Bravura Privilege* and *Hitachi ID Connector Pack* are installed.
- An Active Directory target has been configured and is a source of profiles.
- *Hitachi ID Bravura Pattern: Privileged Access Edition* is installed.
- Scenario.pam_personal_admin_management is installed.
- Teams have been configured with account trustees.
- Systems have been discovered and onboarded.
- At least one personal admin account exists.

Check out personal admin account access

1. Log in to *Bravura Privilege* as an account trustee.
2. In the **Requests** section of the main menu, click **Privileged access**.
3. Search and select personal admin accounts.
   Verify personal admin accounts are checked out.

See also:

- *Bravura Security Fabric* Documentation for more information about team management and onboarding systems and accounts
- The **`manage-teams.pdf`** task document for more information about team management.