Bravura Pass Implementation: Password Expiry Notification

The *Hitachi ID Bravura Pass* notification system can notify users about pending password expiry and ensure they change their passwords before they expire.

This document contains:

1 Requirement

Emails should be sent to users warning that their password expiry date is imminent, including an invitation to use *Hitachi ID Bravura Pass* to change their password immediately. Users then comply via web form, complete with descriptive password complexity rules and interactive feedback about password change results, rather than Ctrl-Alt-Delete interface.

2 Solution: 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.

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.

BEST PRACTICE

Configure *Bravura Pass* to monitor upcoming password expiry on all systems. At a minimum, send email reminders to users asking them to change their soon-to-expire password. Include a link to the *Bravura Pass* URL in these emails.

Password expiry emails should be sent to users 10, 5, 3, 2 and 1 days before the next password expires.

3 Use case: Detecting soon-to-expire passwords

This use case shows you how to configure *Hitachi ID Bravura Pass* to detect password expiry on an Active Directory target system.

> **Note:** If both target password expiry and *Bravura Pass* password history are in effect, the earliest expiry time is used.

Requirements

This use case assumes that:

- *Hitachi ID Bravura Pass* and *Hitachi ID Connector Pack* installed.
- An Active Directory target system is added as a source of profiles.

Use target system policy to record expiry

To use the target system policy:

1. Log in to *Bravura Pass* as `superuser`.
2. Click **Manage the system** → **Resources** → **Target systems** → **Manually defined**.
3. Select the Active Directory target system.
4. Ensure that the **Check password expiry** box is selected.

For each target system with the **Check password expiry** setting enabled, *Bravura Pass* records the password expiration date/time, and the last password change, during auto discovery.

Set *Bravura Pass* password policy to use history rules

Configure password expiry policy based on the last time users changed their password using *Bravura Pass*.

A particularly useful strength rule, **not be an old password** prevents or warns users against reusing old passwords. This ensures that if a user's password was divulged in the past, it will not constitute a threat in the future.

To set rules for password history:

1. Log in to *Bravura Pass* as `superuser`.
2. Click **Manage the system** → **Policies** → **Password policies**.
3. Select the **DEFAULT** policy.
4. Click the **Password policy** tab again for the default password policy.
5. Set **not be an old password** to "Required".

6. Set **password must be changed every N days** to "Enabled" and type `42`.
   This value match the default Active Directory password expiry setting (see the note below).
7. Set **allow reuse of old passwords after N days** to "Enabled" and type `420`.
   This value matches the default Active Directory setting.
8. Click **Update**.

WARNING!: The number of days for **allow old passwords after N days** *must* be greater than the number of days for **password must be changed every N days**.

The recommended setting is that N = 6 x maximum age; for example, **password must be changed every N days** set to 30 days, and **allow old passwords after N days** set to 180 days.

If configured incorrectly, users are able to reset and “change” their password using their existing password.

Bravura Pass can list users with soon-to-expire passwords based on both target system password expiry and *Bravura Pass* password policies. If both target password expiry and *Bravura Pass* password history are in effect, the earliest expiry time is used.

Note: By default Active Directory expires passwords every 42 days, and does not allow users to use the last 10 passwords. This means users will not be able to reuse a password until the 11th reset minimum, assuming they only change their password when it expires. The setting **password must be changed every N days** only prompts users to change their passwords when they login to *Bravura Pass*. For use cases where *Bravura Pass* is only accessed when users lock themselves out or forget their password, this setting is not practical. This might be the case, for example, when password synchronization is configured to be triggered from Active Directory (transparent synchronization).

4 Use case: Configuring batch notification for password expiry

This use case shows you how to set up a warning-level password expiry notification.

Requirements

This use case assumes that:

- *Hitachi ID Bravura Pass* and *Hitachi ID Connector Pack* is installed.
- An Active Directory target system is added as a source of profiles.
- Password expiry detection is configured as in Use case: Detecting soon-to-expire passwords.

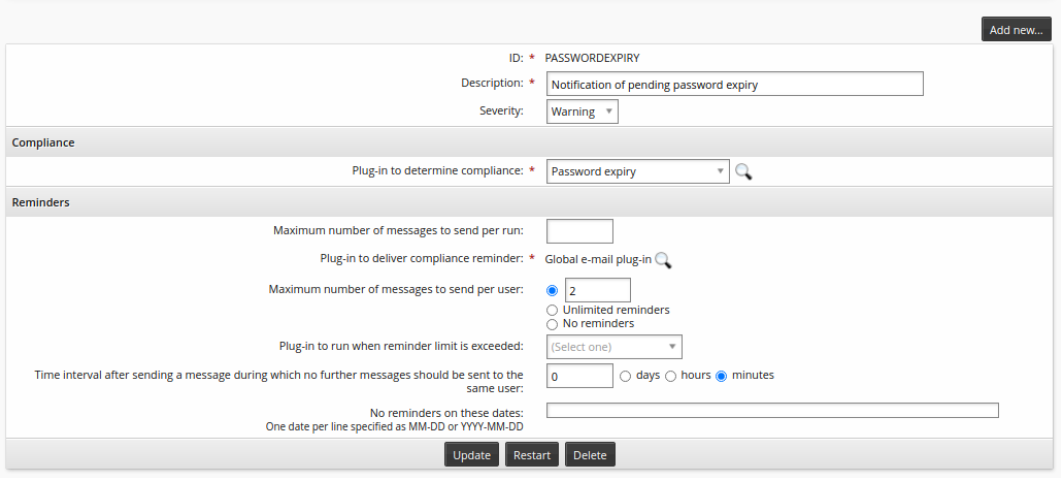
Set up a batch notification

To set up a warning-level password expiry notification:

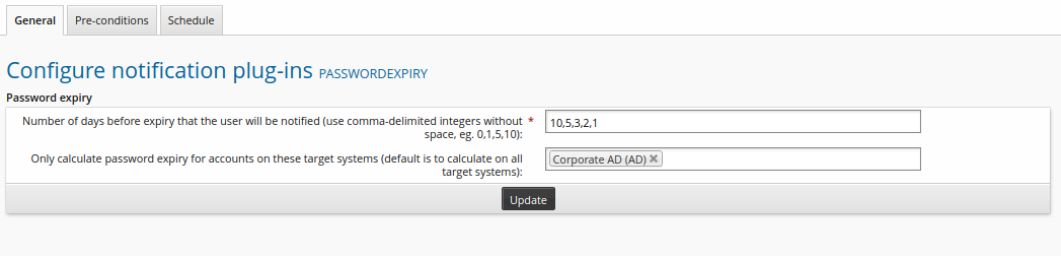
1. Log in to *Bravura Pass* as `superuser`.
2. Click **Manage the system** → **Policies** → **User notifications** → **Batch notifications** .
3. Click **Add new . . . .**
4. Type:
   - **ID** `PASSWORDEXPIRY`
   - **Description** `Notification of pending password expiry`

   The notification ID can only contain ASCII characters.
5. Set the notification **Severity** to "Warning".
6. Set the **Plugin to run to determine compliance** to "Password expiry".
7. Select the radio button for **Maximum number of messages to send per user** and type `2` in the adjacent field.
8. Click **Add**.

   Bravura Pass warns you that the compliance plugin requires configuration.



9. Click the configure icon next to the **Plugin to determine compliance** field.
10. Configure parameters for password expiry:
    - Set the required **Number of days before expiry that the user will be notified** to `10,5,3,2,1`.
    - In the **Only calculate password expiry for accounts on these target systems** field, select the Active Directory system you set up to check password expiry in Use case: Detecting soon-to-expire passwords.
11. Click **Update**.



12. Navigate to the ***Batch notification information*** page for the PASSWORDEXPIRY notification. You can click the **General** tab or use the breadcrumb links.
13. Configure the plugin responsible for delivering reminders.
    (a) Click the configure icon next to the **Plugin to run to deliver compliance reminder** field.
    (b) Enter the following:

    Mail subject `Your password will expire in%DAYS% days.`

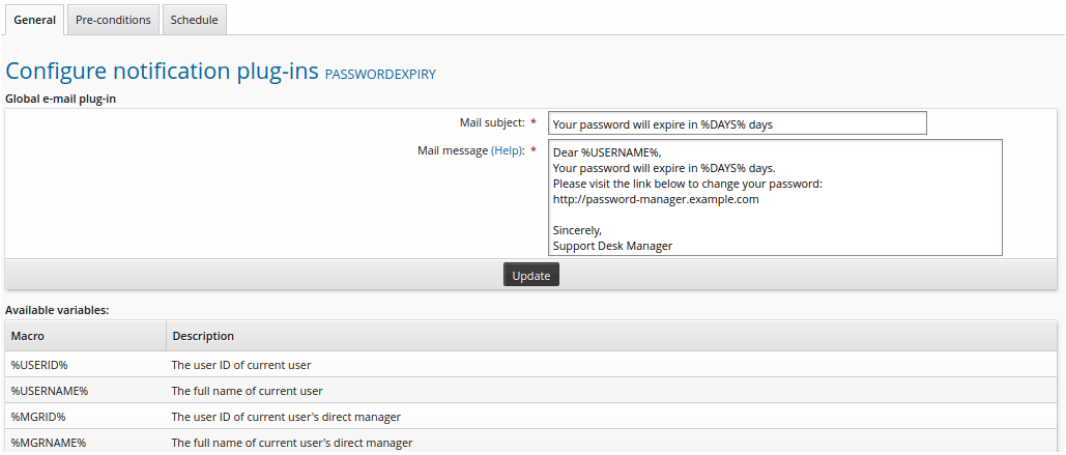
    Mail message

    ```
    Dear %USERNAME%,
    Your password will expire in %DAYS% days.

    Please visit the link below to change your password.
    ```

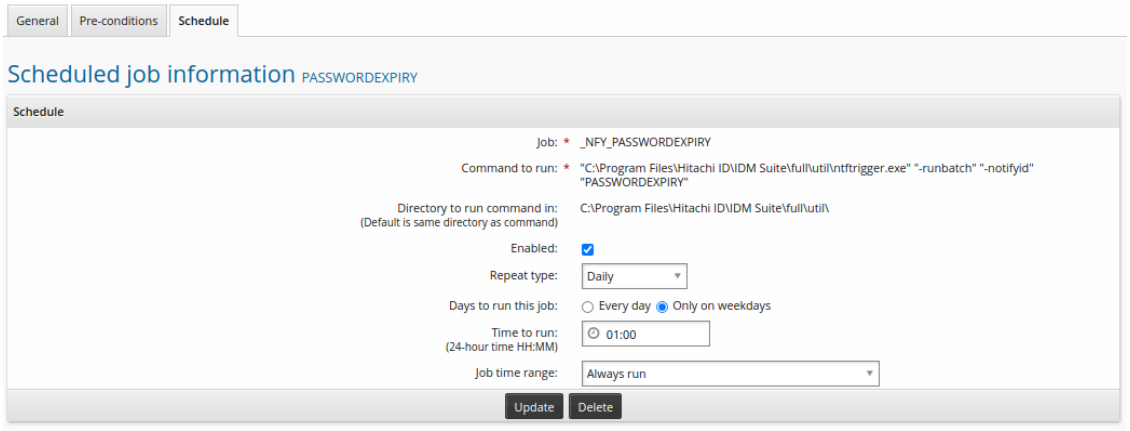


```
http://password-manager.example.com

Sincerely,
Support Desk Manager
```

(c) Click **Update**.



14. Navigate to the ***Batch notification information*** page for the PASSWORDEXPIRY notification. You can click the **General** tab or use the breadcrumb links.
15. Schedule the notification:
    (a) Click the **Schedule** tab.
    (b) Next to **Days to run this job**, select "Only on weekdays".
    (c) Enter `13:00` in the **Time to run** field.
    (d) Click **Add**.



You have now configured *Hitachi ID Bravura Pass* to notify users that their password will expire on Active Directory in 10, 5, 3, 2 and 1 days.