Bravura Security Fabric Implementation: Auto Discovery - Accounts

Hitachi ID Bravura Security Fabric discovers information about users from one or more systems of record, referred to as *target systems*, during auto discovery.

Terminology

The following terminology is used in this document:

Target system A computer system or application that has users or accounts to be managed or referenced by *Hitachi ID Bravura Security Fabric*. Example target systems include an Active Directory domain, a Microsoft SQL Server instance, a Unix server.

User Generally refers to *Bravura Security Fabric* user. Users are identified by their profile IDs.

Account Generally refers to an object that establishes a user's identity or ability to connect to a target system. Accounts are identified by their login IDs on target systems.

Profile A record within *Bravura Security Fabric* describing a user. This may include a full name, personal details, information about the user's accounts (login IDs and attributes), access controls, authentication data, and more.

In *Bravura Security Fabric*, 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.

Managed group A group of accounts defined on a target system, whose membership is monitored and managed in *Bravura Security Fabric*. 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 Security Fabric*.

Attributes Attributes can refer to:

Account attributes the attributes of user accounts on target systems; for example, most target systems store the "first name" and "last name" of the users on that system. In Active Directory, the attribute that stores the first name is `givenName`, and the attribute that stores the last name is `sn`. When you add a target system, there is an option to list account attributes, if supported by the target system.

Profile and request attributes the attributes associated with *Bravura Security Fabric* users and processes. They can provide information about a user, or a request, or both. Values for these attributes can be loaded automatically from associated account attributes, provided by a plugin, or entered by users in a form on the *Bravura Security Fabric* GUI.

Group attributes the attributes of groups on target systems; for example, the group description in Active Directory. When you add a target system, there is an option to list group attributes. Group attributes can be mapped to resource attributes.

Resource attributes the attributes defined in *Bravura Security Fabric* and associated with resource objects such as target systems and managed groups.

Resource entitlement attributes the attributes that define the relationship between two resources.

Group entitlement attributes define the relationship between a user and their group membership; for example, the membership expiry date is a group entitlement attribute for the relationship between a user and their group membership.

Role entitlement attributes define the relationship between a user and their role assignment; for example, an expiry date for a student's registration in a math course at university is a role entitlement attribute for the relationship between the student and their role as a math student.

Auto discovery The process by which *Bravura Security Fabric* lists users, accounts, and other objects on connected target systems and loads the information into its database. The listing and loading is carried out by the **psupdate** program, which is scheduled to run nightly by default.

You can also run **psupdate** manually.

This document contains:

1 Requirement

Automatic discovery of accounts, identity attributes, groups and group memberships, with data being extracted periodically from AD domain.

2 Solution

Hitachi ID Bravura Security Fabric discovers information about users from one or more systems of record, referred to as *target systems*, during auto discovery. During the auto discovery process, *Bravura Security Fabric* also performs several important maintenance tasks. Auto discovery is initiated and controlled by the **`psupdate`** program. This program calls a series of other programs that perform the actual work for most of these tasks.

Connector programs connect to target systems and extract information about users (accounts) and other objects from those systems. Each connector is designed to target a specific type of system.

Connector programs write the extracted information to SQLite database files in the `\`<*instance*>`\`psconfig`\` directory. In *Bravura Security Fabric* these files are referred to as *list files*. A SQLite database list file is saved for each target system.

This document shows you how to import user information and associate it with *Bravura Security Fabric* profile IDs.

3 User profiles

When you make an Active Directory server a source of profile IDs. Each account that *Hitachi ID Bravura Security Fabric* listed on that target system is imported into the *Bravura Security Fabric* database and assigned a profile ID based on their Active Directory short ID.

Bravura Security Fabric associates the following information with a user's profile ID:

- Owned accounts
- Group memberships
- Profile attributes
- Access controls
- Last login time
- Password change method
- Password history
- Language
- Profile status (enabled, locked, disabled)
- OrgChart data
- Security question data
- Inventory items

Most of this information is gathered during auto discovery. Other information can be imported in batches or collected in workflow requests by product administrators, help desk users, or end users themselves.

3.1 Profile IDs

Your source of profile IDs should contain a login ID for all, or most, of the *Hitachi ID Bravura Security Fabric* users in your organization. If possible, designate a system that uses the most common or standardized naming convention.

By default, *Bravura Security Fabric* uses the short ID (sAMAccountName for Active Directory) from a source of profiles system. You can specify a different account attribute to use as profile ID; for example a UPN or employeeID attribute.

Bravura Security Fabric preserves the case of what is imported or entered, although the usage of profile IDs is case insensitive; for example a search for `user1` will yield `User1`.

3.2 Owned accounts

Hitachi ID Bravura Security Fabric extracts a list of login IDs from each target system, every 24 hours by default. This process is fail-safe; where account lists extracted from a target system fail to return sufficient data, they are discarded and the previously-harvested account list is retained.

Some target systems are designated as sources of user profiles. Every user ID that appears in one of the source of profiles systems is assigned a user profile in *Bravura Security Fabric*, if one did not already exist. Existing user profiles that no longer appear on any of these authoritative systems are automatically deactivated.

Login IDs on systems that are identified as having a consistent naming scheme are automatically attached to *Bravura Security Fabric* user profiles.

Login IDs on systems that are identified as using non-standard login IDs are stored in inventory, but may not be automatically attached to user profiles, unless there is some other, consistent and reliable attribute that can be used to match local login IDs to global user profiles.

Users enrol to complete profiles

A set of rules can be used to decide whether any given user must enroll to complete their profile. Users may be invited to enroll in order to provide personal information, such as a mailing address, to set up security questions, to attach non-standard login IDs to their profiles or to enroll a mobile device.

Users who are flagged as in need of enrollment are notified – either by email or by automatically opening a web browser during their network login script. A deployment management facility is used to ensure that an individual user is not invited too frequently and that the number of users asked to enroll on any given day is limited. The former limit eliminates nuisance to users, while the latter reduces load on the mail delivery system and limits the potential call volume that confused users might cause by calling the help desk.

To enroll, users either click on a URL in a registration-request email or use a web browser window opened during their network login sequence. Users authenticate with a current network or directory login ID and password and are walked through the registration process (fill in the blanks) one screen at a time.

By default, user profile data is stored in the *Hitachi ID Bravura Security Fabric* database, which is replicated among *Bravura Security Fabric* servers. The schema for this database is well documented and available to Hitachi ID Systems customers.

User profile data can also be reflected into an external directory, most often an LDAP directory, where other applications can consume it.

In most organizations, users are assigned consistent login IDs on different systems and applications. Where this is the case, accounts are automatically mapped to user profiles using the login ID.

Where accounts have non-standard login IDs:

1. If account attributes suitable for ID mapping are both reliable and widely populated, link accounts to

user profiles by matching employee numbers or other unambiguous IDs.

2. Do not map accounts to profiles using user names, because multiple people may have the same name, because different administrators may have setup accounts for the same user with variations of the same name and because people sometimes change their name, but such changes may not be reflected on all systems and applications.

3. On systems or applications where there is not well-populated or reliable mapping data, invite users to attach accounts to their own profiles using the self-service mechanism provided in *Hitachi ID Bravura Pass*.

4. Do not ask support staff to map accounts to user profiles as an alternative to self-service enrollment. When a user attaches an account to their profile they are required to provide the current password, which verifies that they own that account.

   Although technically possible, when a support staff member completes the mapping there is no method to confirm the support staff member has mapped the correct account to the profile. This could result in someone having access to an account they do not own, due to human error.

   If the account cannot be mapped automatically, requesting users to attach their own accounts is the most secure method of ensuring the correct account is attached to the correct profile.

3.2.1 Automatically attaching accounts to profiles

Standard IDs are login IDs (short IDs) that belong to a single user and match the user's profile ID. If some or all of your target systems use standard IDs, you can configure *Bravura Security Fabric* to automatically attach accounts on these systems to a profile ID. You do this by selecting the **Automatically attach accounts** checkbox (this is the default).

You can specify an **Account attribute to automatically attach accounts to user profiles** , rather than use the short ID. If the target system is a:

- Source of profile IDs, this is the attribute value that other systems can match against when attaching accounts; for example, a mail attribute or employee ID
- Non-source, this is the attribute that matches the format of the profile ID; for example, where login IDs on your source of profile IDs target system are in the format jsmith@example.com, which matches the value of InternetAddress on a Lotus Domino target system.

Make sure the chosen attribute is loaded from the target system and that it is populated for all accounts; the accounts for which this attribute is blank or doesn't exist won't be attached to any profile. If the attribute has the same value for more than one account, all of those accounts will be attached to a single profile

3.2.2 Self-service profile building

The *Hitachi ID Bravura Security Fabric* user interface includes the *Attach other accounts* (PSL) module which builds on auto discovery to allow users to attach their own non-standard login IDs to their profile.

To block access to this feature, turn off the **PSL ENABLED** setting.

4 Use case: Adding Active Directory as a source of profiles

Hitachi ID Bravura Security Fabric lists accounts on shared computer systems referred to as *target systems*. This use case shows you how to manually define an Microsoft Active Directory target system so that it becomes the source of *Bravura Security Fabric* profiles. This means that users with accounts in Active Directory will have profiles, including full user name, created for them in *Bravura Security Fabric*.

> **Note:** When you install *Bravura Pattern*, common target systems are automatically defined. The settings need to be adjusted to suit your environment and requirements.

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 the following information, for example:

   ID `AD`

   Type `Active Directory DN`

   Description `Corporate AD`

   Managed group/Network resource target system type
   `SMB Protocol for Active Directory DN`

   The target **ID** can contain *only* letters (A-Za-z), digits (0-9), and underscores (_).
4. Click **Change** to the right of the **Address** field and enter values such as:

   Domain or domain controller `example.corp`

   OUs to list users from: List
   `*,ou=Demo,dc=example,dc=corp`

   OUs to list groups from: List
   `*,ou=Demo,dc=hitachi1,dc=corp`

   List nested groups deselect

   Name format `DN`

   For Active Directory, there are three primary methods for specifying the Active Directory target address:

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

   See the Active Directory Integration Guide (**`active-directory.pdf`**) for details about Active Directory address parameters.
5. Click **Continue** to return to the ***Target system information*** page.
6. Ensure **Source of profile IDs**, **List accounts**, **List account attributes**, **List groups**, and **List group attributes** are selected.

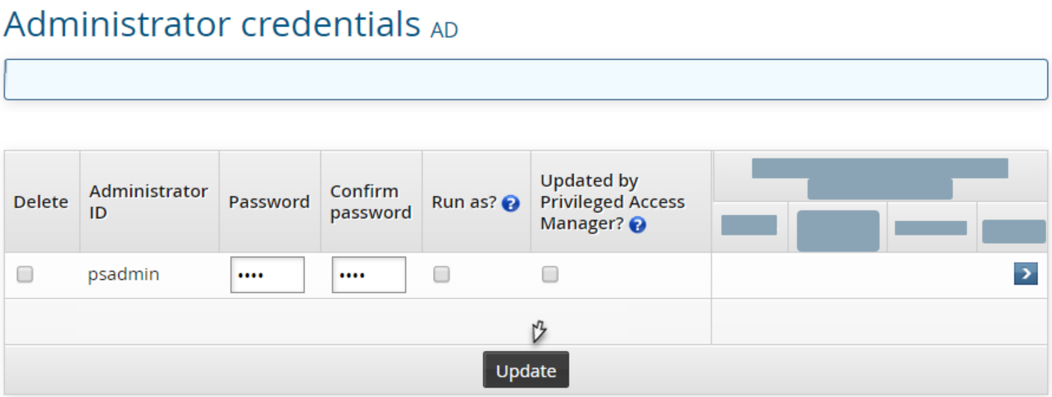
7. Select **Create profile IDs from enabled accounts only**.
8. For this use case, leave other parameters with default values.
9. Click **Add**.

Add target system administrator credentials

Next you need to add the administrator credentials that *Hitachi ID Bravura Security Fabric* will use to connect with the target system and perform operations. In a production environment, *Bravura Security Fabric* connects to an Active Directory target using a domain administrator account or delegated ID so that it can manage passwords and accounts.

To add the credentials:

1. Click on the **Credentials** tab
2. Type the target system administrator's login ID in the **Administrator ID** field.
3. Type the account password in the **Password** and **Confirm password** fields.
4. Deselect **Updated by Privileged Access Manager?**.
5. Click **OK** to confirm the action.
6. Click **Update**.



Administrator credentials AD

Delete	Administrator ID	Password	Confirm password	Run as?	Updated by Privileged Access Manager?	[redacted]
□	psadmin	••••	••••	□	□	›

Test the connection

To test that your target system is configured correctly:

1. Click the **Test connection** tab.
2. Click **Test credentials**.

   Results should show "Success"; if not, verify that the address, target type and administrator credentials are entered correctly.

   For the next test, *Bravura Security Fabric* performs a list operation to enumerate user accounts on the target system. The results of the list operation are for testing purposes only and, unlike during auto discovery, will not be loaded into the database.

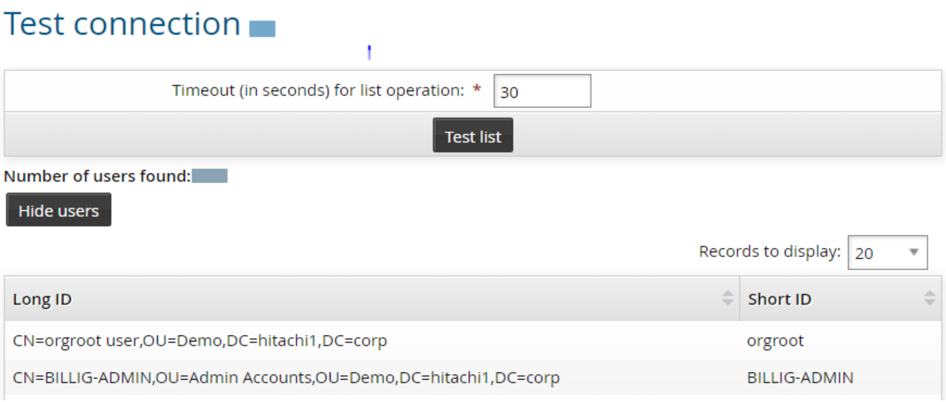
> **WARNING!:** Listing can be a costly operation on the target system. This may take a long time on some systems.

3. Click **Test list**.

   While the list operation is running, you can click the Refresh 🔄 button in the *Bravura Security Fabric* navigation bar to update the page status. When the operation completes, the "Number of users found" should match the number of enabled accounts on the target system.

4. Click **Show users**.

   Hitachi ID Bravura Security Fabric displays the results of the generated user list.



Test connection [redacted]

Timeout (in seconds) for list operation: * 30

Number of users found: [redacted]

Records to display: 20

Long ID	Short ID
CN=orgroot user,OU=Demo,DC=hitachi1,DC=corp	orgroot
CN=BILLIG-ADMIN,OU=Admin Accounts,OU=Demo,DC=hitachi1,DC=corp	BILLIG-ADMIN

Run auto discovery

Once a target has been added and is flagged as a source of profile IDs, you need to run **`psupdate`** to list accounts and create user profiles:

1. Click on the **General** tab.

2. On the ***Target system information*** page, click **Run discovery** at the bottom of the page.

   Alternatively, on the ***Target systems*** list page, select the target system and click **Run discovery**.

3. Confirm that you want to start the update.

   Depending on the number and type of target systems, this process may take several minutes to complete.

4. Click Home 🏠.

5. Click **Manage reports** → **Reports** → **Users** → **Accounts**.

6. Click **Run** at the bottom of the report form.

   If auto discovery was successful you should see a number of accounts listed as auto-associated.

Use case: Testing and troubleshooting auto discovery includes use cases for testing auto discovery via the web UI and from the command line.

5 Use case: Testing and troubleshooting auto discovery

If you executed auto discovery as described in the target systems lab, you have already seen one way of checking whether the users were successfully listed; by viewing the **Accounts** report. In this lab we will look at two other ways of configuring and testing user listing:

- Running auto discovery from the web interface
- Running auto discovery from the command line

5.1 Running auto discovery from the web interface

To test that your target is listing users correctly, you can run auto discovery from the *Manage the system* (PSA) module and confirm that users have been listed by looking at the generated file:

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Resources** → **Target systems** → **Manually defined**.
3. Select ▶ the Corporate AD target to update that target.
4. Deselect **List accounts**.
5. Click **Update**.
6. Navigate to the \<*instance*>\psconfig\ directory.
7. Delete all files named **`AD.*`**.
8. From the *Manage the system* (PSA) module, click **Maintenance** → **Auto discovery** → **Execute auto discovery**.
9. Click **Continue**.
10. Click **Maintenance** → **Auto discovery** → **Last log**, and refresh the page until the log shows "done psupdate".
11. Check the \<*instance*>\psconfig\ directory.

    There should be a file that named **`AD.db`** in \<*instance*>\psconfig\, but it will be 0KB and empty because the old ones were deleted and user listing was turned off for the Active Directory target.
12. Click **Manage the system** → **Resources** → **Target systems** → **Manually defined**.
13. Select ▶ the Corporate AD target.
14. Select **List accounts**, **List account attributes**, **List groups**, **List group attributes** and **Create profile IDs from enabled accounts only**.
15. Click **Update**.
16. Execute auto discovery: **Maintenance** → **Auto discovery** → **Execute auto discovery** → **Continue**.

17. Once the process is complete, check the \\<*instance*>\\psconfig\\ directory.

    The **AD.db** file in \\<*instance*>\\psconfig\\ should have a much larger file size now because you turned on user listing for the Active Directory target again.

18. Confirm the auto discovery successfully listed users by opening the file:

    ```
    C:\Program Files\Hitachi ID\IDM Suite\<instance>\psconfig\AD.db
    ```

    If auto discovery is successful, this file lists users with accounts on the Active Directory target system. A file is added for each target system on which listing is enabled.

19. Confirm that auto discovery listed users successfully from your target systems by searching the idmsuite.log for the line in which the agent listed items from your target. Open:

    ```
    C:\Program Files\Hitachi ID\IDM Suite\Logs\<instance>\idmsuite.log
    ```

    You should see lines in the psupdate section for each agent indicating list succeeded. The lines will look something like this:

    ```
    2021-01-22 01:34:18.542.5089 - [psupdate4936_6408] agtaddn.exe [1352,5096]
    Info: [listobj] for Object [GRP] succeeded
    2021-01-22 01:34:18.815.7331 - [psupdate4936_6408] agtaddn.exe [1352,1756]
    Perf: PerfConnector. Address:
    {[server=hitachi1.corp;listOUs=["*,ou=Demo,dc=hitachi1,dc=corp";];listGroupOUs=["*,ou=
    | AdminID: {psadmin} | Duration: {775} | Event: {connector-operation} |
    Message: {} | Operation: {listobj} | Result: {0} | SysID: {} | TargetID:
    {AD}
    2021-01-22 01:34:18.815.7387 - [psupdate4936_6408] agtaddn.exe [1352,1756]
    Info: [listobj] for Object [ACCT] succeeded
    ```

> **Note:** There is also a "Run discovery" button in the **Manage the system** → **Resources** → **Target systems** → **Manually defined** section for running auto-discovery against individual targets.

5.2 Running auto discovery from the command line

An alternative way to test auto discovery is to run the **psupdate** program from the <*instance*>\\util directory. You can use arguments with this command to specify part of the auto discovery process. In this lab, you will use the -list argument to just list users on a single target:

1. Delete all files named **AD.*** from the \\<*instance*>\\psconfig\\ directory.

2. From a Windows Administrator Command Prompt, navigate to:

   ```
   C:\Program Files\Hitachi ID\IDM Suite\<instance>\util\
   ```

3. Type:

   ```
   psupdate -list -target AD
   ```

4. Check the \\<*instance*>\\psconfig\\ directory.

   There should now be an updated file named **AD.db** in \\<*instance*>\\psconfig\\ because you executed **psupdate** with the `list` option to create list files.

See also:

- Auto Discovery in the Bravura Security Fabric *Documentation* describes the process in detail.
- psupdate in the Bravura Security Fabric *Reference Manual* describes all arguments for the **`psupdate`** command.

6 ID filters

Hitachi ID Bravura Security Fabric uses *ID filters* to determine which users (profile IDs) and accounts (long IDs) are imported to *Bravura Security Fabric* from a target system. During the auto discovery process the importing of accounts is controlled by the **Use ID filters to include only certain users and accounts** checkbox, located on the ***Target system information*** page.

When the **Use ID filters to include only certain users and accounts** option is:

- Selected – the ID filter acts as an inclusion list; *Bravura Security Fabric* imports *only* those IDs that have been explicitly included.

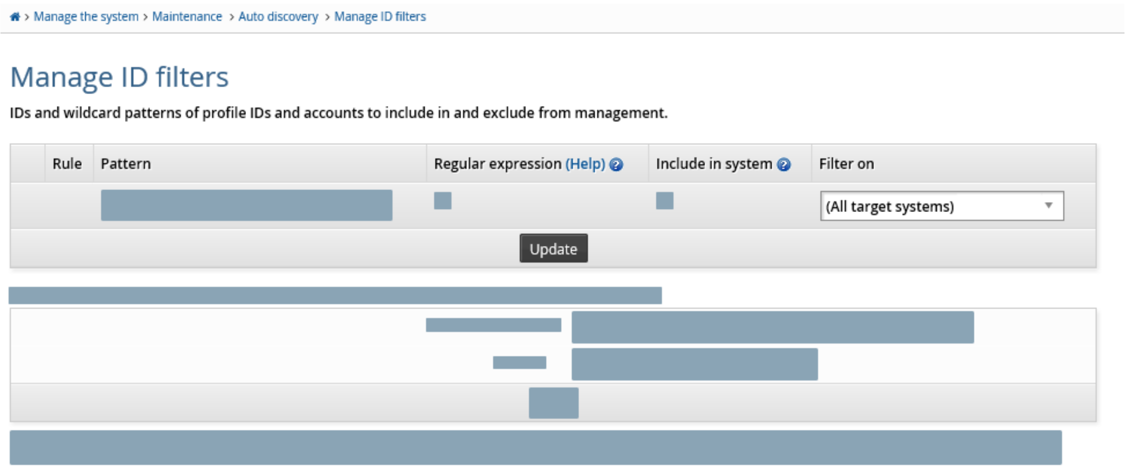
  An ID is “included” if it matches a **Pattern** on the ***Manage ID filters*** page and the corresponding **Include in system** checkbox is selected.
- Not selected – the ID filter acts as an exclusion list; *Bravura Security Fabric* imports all IDs *except* those that have been explicitly excluded.

  An ID is “excluded” if it matches a **Pattern** on the ***Manage ID filters*** page and the corresponding **Include in system** checkbox is not selected.

Use the ***Manage ID filters*** page to identify individual IDs, or groups of IDs, that you want or don’t want managed by *Bravura Security Fabric*. You can also use the ***Manage ID filters*** page to identify those IDs you want to be included or exclude as a source of profile IDs.

For example, configure *Bravura Security Fabric* to filter IDs if:

- You do not want anyone to access profiles for certain administrative accounts.
- The total number of profile IDs exceeds the number of users you are licensed for.
- You want to prevent users from attaching accounts that are used for specific purposes on a system. For example, you may want to prevent users from attaching an `nt_guest` account on a Windows NT system.
- You want to prevent *Hitachi ID Bravura Identity* from creating users and accounts with certain IDs.



> Manage the system > Maintenance > Auto discovery > Manage ID filters

Manage ID filters

IDs and wildcard patterns of profile IDs and accounts to include in and exclude from management.

Rule	Pattern	Regular expression (Help)	Include in system	Filter on
				(All target systems)

Update

Note: Filters on "(All target systems)" includes "(Profile ID)". This means the filter will match all account IDs as well as *Bravura Security Fabric* Profile IDs.

7 Use case: Including and excluding accounts

This lab shows you how to filter certain users accounts on your Active Directory target so they are not imported into the *Hitachi ID Bravura Security Fabric* database.

Create a filter

To create a filter to exclude accounts:

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Maintenance** → **Auto discovery** → **Manage ID filters**.

   Hitachi ID Bravura Security Fabric displays the ***Manage ID filters*** page.
3. Set the following:

   Pattern `.*admin`

   Regular expression selected

   Filter on `Corporate AD (AD)`

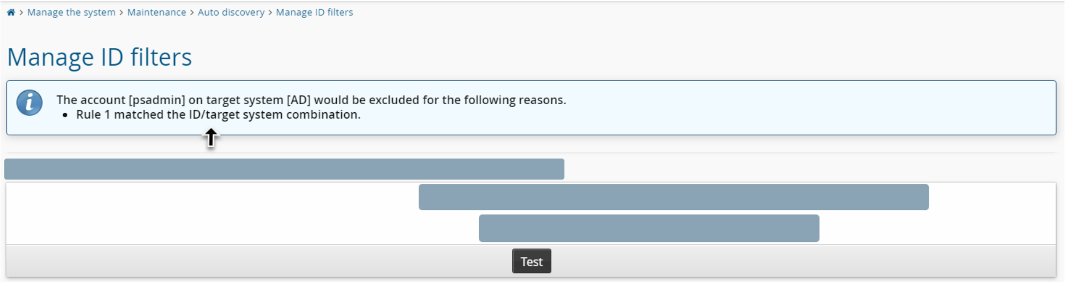
   Note: *Bravura Security Fabric* preserves the case of account IDs; however, all profile IDs are treated as case-insensitive.
4. Click **Update**.

   You have created a filter that excludes `AD` user accounts that include `.*admin`.

Test the filter

1. Type `psadmin` in the **Profile ID/Account** field.
2. Select `Corporate AD (AD)` from the **Test on** drop-down list.
3. Click **Test**.

   Hitachi ID Bravura Security Fabric displays the results at the top of the page. It should tell you that `psadmin` account will be excluded.


Manage the system › Maintenance › Auto discovery › Manage ID filters
Manage ID filters
Test

The account [psadmin] on target system [AD] would be excluded for the following reasons.

- Rule 1 matched the ID/target system combination.

Summary

The auto discovery process imports information about users and groups, and performs several important maintenance tasks. The process itself requires little maintenance, but can be enhanced to provide automated access control and provisioning functions.