

***Bravura Security Fabric* Implementation:**

Map attributes - admin

Hitachi ID Bravura Security Fabric includes a “catalog” of shipped attribute presets for each target system type. The catalog includes each attribute’s native name, and default requirements, configured actions, and profile and request attribute mappings.

Bravura Security Fabric uses the attribute catalog to determine rules for “handling” each attribute when managing accounts on a target system. The catalog also determines which attributes’ values should be loaded during auto discovery.

Terminology

The following terms are introduced in this unit:

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 *Hitachi ID 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 *Hitachi ID Bravura Security Fabric* GUI.

Attribute groups An attribute group is a named collection of profile and request attributes. *Hitachi ID Bravura Security Fabric* uses attribute groups to determine:

- Who can see or edit certain attribute values.
- How attributes are displayed to users.

You need to assign permissions, or access controls, to give end users read and write access to attribute groups, and therefore the attributes within each group. You can be selective, using highly configurable rules, about which users have access. In order for a profile attribute to be seen or updated by users – that is, to show up on a self-service request page – it must belong to an attribute group.

This document contains:

- Requirement
- Solution
- Use case: Creating profile and request attributes
- Use case: Mapping account attributes to profile and request attributes
- Use case: Grouping profile and request attributes

- Use case: Defining restricted values manually
- Use case: Setting attribute validation rules
- Use case: Modifying attribute priority

1 Requirement

Organizations require the data stored in target systems such as an email address, or phone number to become part of the users' profiles in *Hitachi ID Bravura Security Fabric*.

2 Solution

Profile and request attributes allow any number of account attributes to be mapped to a single value in users' profile data. Several attributes are mapped by default; for example, the Microsoft Active Directorymail and Lotus Domino Server InternetAddress account attributes are mapped to the EMAIL profile and request attribute. Attributes that are mapped to profile and request attributes are listed by default when the target system's List attributes setting is enabled.

In order to map an account attribute to a profile and request attribute, the attributes' requirements (number of values, attribute type, encoding) must be compatible.

Information can be collected by:

- The auto discovery process, which loads *account attribute* information – from target systems that support attribute listing – into mapped profile and request attributes.
- A plugin that automatically collects and/or generates or looks up information, such as an employee ID, from a database.
- Users who update profile information using the web interface.

2.1 Mapping profile and request attributes

You can map profile and request attributes to account attributes to load users' information from a target system. You can also configure attributes so that users' accounts are updated when their profile information is updated.

The type and number of values of the profile and request attribute must be compatible with the account attribute. For example, you cannot map a required account attribute to an optional profile and request attribute, or a single-valued account attribute to a multi-valued profile and request attribute.

2.2 Grouping attributes

Attributes must be included in an attribute group in order to be used. You can organize attributes into groups to:

- Assign read and write privileges to users in different stages of authorization workflow.
- Assign read and write privileges to creators of managed system policies, when *Bravura Privilege* features are used.
- Determine whether attributes are displayed for specific operations, such as view profile.
- Determine how attributes are displayed to users on the request form.

3 Use case: Creating profile and request attributes

In this use case you will create a profile and request attribute to gather information from users.

This use case assumes:

- *Hitachi ID Bravura Security Fabric* and *Hitachi ID Connector Pack* are installed.

Add a profile and request attribute

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Workflow** → **Profile and request attributes** → **Profile and request attributes**.
3. Click **Add new...**
4. Enter the following information:

ID `VEHICLE-DESCRIPTION`

Description `Vehicle description`

Type `String`

Leave other settings as default.
5. Click **Add**.
6. Click **Profile and request attributes** in the top navigation path.
Locate the new attribute in the list.

4 Use case: Mapping account attributes to profile and request attributes

In the event you need to track a particular attribute loaded from a target system account you can link a profile or request attribute within *Hitachi ID Bravura Security Fabric* to the account attribute through mapping. We will create a new profile attribute to map our Active Directory carLicense account attribute to.

When using *Bravura Security Fabric* there are often many ways to achieve the same outcome. To demonstrate an alternative way to create a profile attribute, you will create the new VEHICLE-LICENSE profile attribute during the process of mapping the carLicense account attribute.

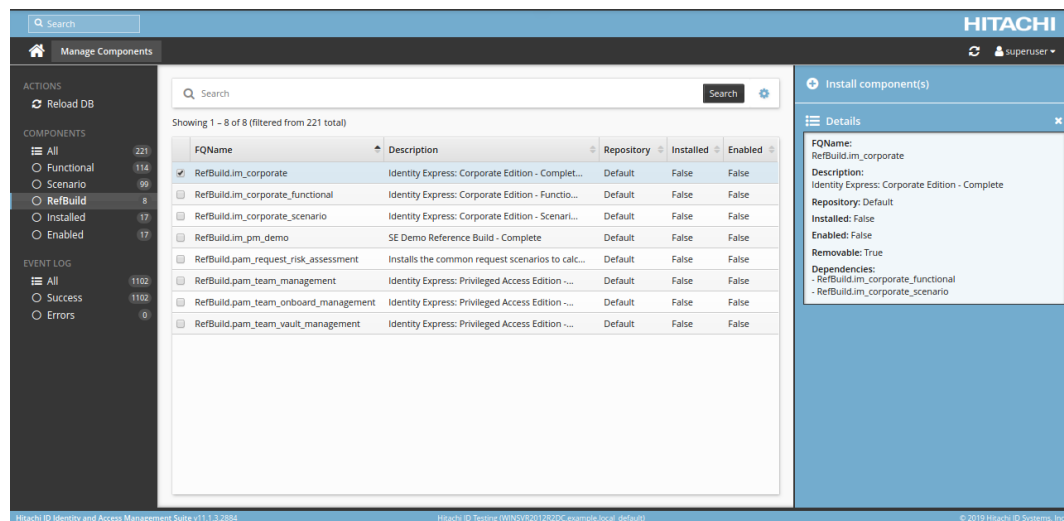
This use case assumes:

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

Install Bravura Pattern: Workforce Edition

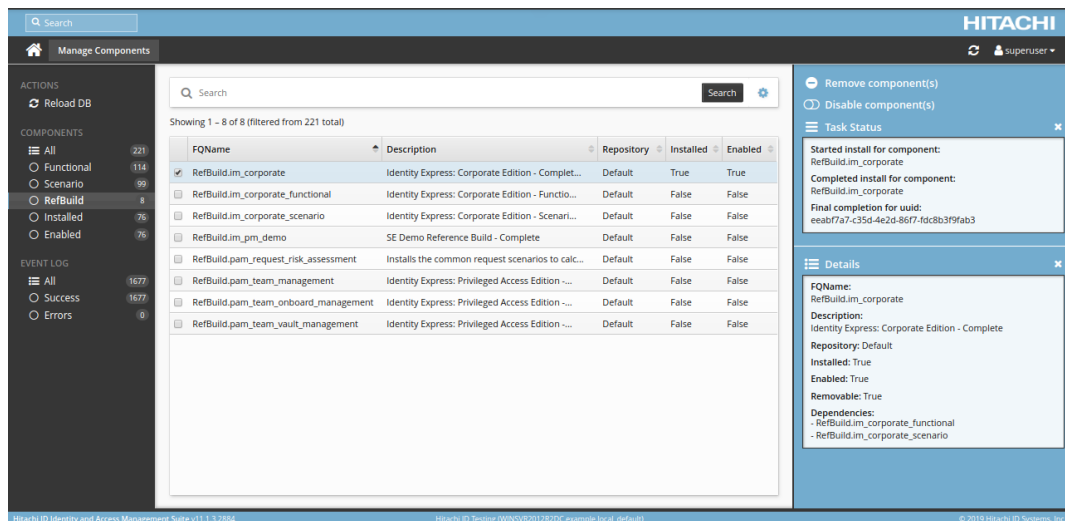
To install the *Hitachi ID Bravura Pattern: Workforce Edition* components:

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage Components** → **RefBuild**.
3. Select the checkbox for **Refbuild.im_corporate**.



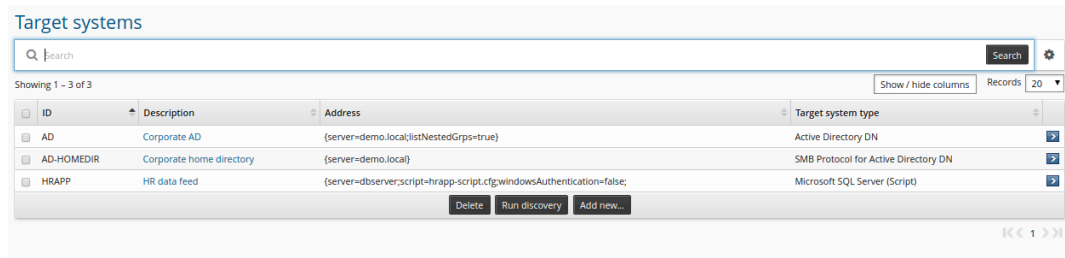
4. Click **Install component(s)** from the Actions panel on the right.

The component management program installs the components along with any dependencies. This may take some time depending on configuration requirements and dependencies. You should see "Completed install for component" messages for each selected component in the **Details** section of the Actions panel.



When you install a component, the component management program creates the database tables and configurations that are necessary for the plugin points to function. Additional post-install configuration may still be required for some use cases to run properly.

- Take a look at some of the new configuration parameters that the reference implementation components add to the manually defined target systems by navigating to **Manage the system** → **Resources** → **Target systems** → **Manually defined**.



As we continue through the training you will see how we utilize the configurations installed by the reference implementation to enhance the functionality of *Hitachi ID Bravura Security Fabric*.

Map the carLicense account attribute to a new profile attribute

- Click **Resources** → **Account attributes** → **Target system**, then select the Active Directory target system.
- Click the **Defaults** tab.

[Manage the system](#) > [Resources](#) > [Account attributes](#) > [Target system](#)

Target system level overrides Target system type level overrides **Defaults**

Account attributes ^{AD}

Show / hide columns Records 20

Account attribute ID	Action when creating account	Action when updating account	
accountExpires	Copy from template	None	
accountNameHistory	Copy from template	None	
aCSPolicyName	Copy from template	None	
adminCount	Copy from template	None	
adminDescription	Copy from template	None	
adminDisplayName	Copy from template	None	

This page lists all the default actions for account attributes that the Active Directory connector extracts from the target.


- for and select the carLicense attribute.
- Click **Override**.
- Set **Action when creating account** to "Set to specified value".
- Set **Action when updating account** to "Set to specified value".
- Set the **Minimum number of values** to 0.
- Click the search icon in the **Map account attribute to profile/request attribute** field.
- Click **Add new...** at the bottom left of the **Profile and request attributes** table.
Hitachi ID Bravura Security Fabric displays the **Profile and request attribute information** form in a pop-up page.
- Create another attribute with the following information:

ID VEHICLE-LICENSE
Description Vehicle license
Type String

 Leave the other settings as default.
- Click **Add**.
Bravura Security Fabric warns about access control, which we will fix later.
- Close the pop-up window to return to the profile attribute selection page.
- Refresh the page so that VEHICLE-LICENSE is included in the list.
- Search for and select VEHICLE-LICENSE and click **Select**.
- Select the **Load attribute values from target system** checkbox to allow *Bravura Security Fabric* to import carLicense account attribute values from the target system.
The **Populate mapped profile attribute with values from target system** is automatically selected.
- Click **Add**.
- Click **Yes** to retrieve a full attribute list during the next auto discovery.


Run auto discovery

You need to run auto discovery to apply the override on the account attribute action and to populate VEHICLE-LICENSE profile attribute:

1. In the *Manage the system* (PSA) module, click **Maintenance** → **Auto discovery**.
2. Click **Execute auto discovery**.
The **Execute auto discovery** page is displayed.
3. Click **Continue**.
4. Click Refresh  until the page displays `Auto discovery is not running`.

Confirm the attributes have been mapped

You can now run a report to confirm the attributes are mapped and loaded correctly:

1. Click Home .
2. Click **Manage reports** → **Reports**.
3. Click **Users** → **Profiles**.
4. Select the following from **User attributes to display**:
 - Vehicle license
 - First name
 - Last name
5. Click **Run**.

You should now see the Vehicle license profile attribute for each user, but it will be blank since our Active Directory users do not have values for the carLicense account attribute.

Manage reports > Reports

Profiles

User profiles, including accounts, group memberships and identity attributes.

Report finished with 854 records found. Time spent running report: 0:00:02. This report was run on 8/13/2019 11:03 PM.

Show / hide columns Records: 10 Highlight Hide repeating cell values ☒ Default ordering ☐

User ID	User name	Profile status	First name	Last name	Vehicle license
_API_USER	Shipped user of the API	Unlocked, Enabled			
_API_USER_GUACAMOLE	Shipped user of the API for Guacamole	Unlocked, Enabled			
_API_USER_TPM	Shipped user of the API for Telephone Password Manager	Unlocked, Disabled			
_LOA_API_USER	_LOA_API_USER	Unlocked, Enabled			
_TEMP_RES_AUTHORIZER	Authorizer for temporary entitlement	Unlocked, Enabled			
_TEMP_RES_REQUESTER	Requester for temporary entitlement	Unlocked, Enabled			
ABBIEL	Abbie Lester	Unlocked, Enabled	Abbie	Lester	
ABBYN	Abby Norton	Unlocked, Enabled	Abby	Norton	
ABDULO	Abdul Ochoa	Unlocked, Enabled	Abdul	Ochoa	
ABRAHB	Abraham Bruce	Unlocked, Enabled	Abraham	Bruce	

Showing 1 – 10 of 854

You have now mapped an account attribute to a profile and request attribute, and used the configuration to populate user profile data.

5 Use case: Grouping profile and request attributes

This use will show you how to include attributes in an attribute group to allow them to be seen and updated by users.

This use case assumes:

- *Hitachi ID Bravura Security Fabric* and *Hitachi ID Connector Pack* are installed.
- An Active Directory target system is added as a source of profiles.
- Complete [Use case: Creating profile and request attributes](#).
- Complete [Use case: Mapping account attributes to profile and request attributes](#).

Create a vehicle attribute group

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Workflow** → **Attribute groups**.
3. Click **Add new...**
4. Type the following information:

ID VEHICLE-INFO

Description Vehicle information

If you want to provide additional information for end users, enter text in the **Notes (above attributes)** or **Notes (below attributes)** fields.

Leave other values as default.

The validation rules will be discussed in a later unit.

5. Click **Add**.

Manage the system > Workflow > Attribute groups

General Access control Members Display criteria

Attribute group definition VEHICLE-INFO

Add new...

ID: * VEHICLE-INFO

Description: * Vehicle information

Enforce validation when creating new accounts: ☒

Validation behavior when updating existing accounts: Always enforce

Notes (above attributes):

Notes (below attributes):

Update Delete

6. Click the **Members** tab.

7. Click **Select...** to see a list of all attributes.

8. Select the checkboxes next to:

- VEHICLE-DESCRIPTION
- VEHICLE-LICENSE

General Access control Members Display criteria

Members: Profile attribute VEHICLE-INFORMATION

Added [VEHICLE-DESCRIPTION].
Added [VEHICLE-LICENSE].

ID	Description
VEHICLE-DESCRIPTION	Vehicle description
VEHICLE-LICENSE	Vehicle license

Delete Update Select...

Showing 1 - 2 of 2

9. Click **Select**.

10. Use the drag-and-drop arrows next to the attribute ID to move VEHICLE-LICENSE above VEHICLE-DESCRIPTION.

This determines the order in which the attributes are listed when displayed to users.

11. Click **Update** to save the changes.

12. Click the **Access control** tab.

13. Assign permissions to allow it to be updated by a user requesting an update or a new account. You probably wouldn't want all recipients to be able to change these values however. For this example:

- Select **Read** and **Write** permissions for ALLREQUESTERS, ALLAUTHORIZERS, and ALLIMPLE-
MENTERS.
- Select **Read** permissions for ALLRECIPIENTS.

Access control VEHICLE-INFO

Q Search Search ⚙

Showing 1 - 19 of 19 Show / hide columns Records 20 ▾


ID	Description	Allow read	Allow write
PII	Read-write PII	<input type="checkbox"/>	<input type="checkbox"/>
REHIRE_DETECTION_SEARCH	Search permissions for Rehire detection	<input type="checkbox"/>	<input type="checkbox"/>
VIEW-PII	View own PII	<input type="checkbox"/>	<input type="checkbox"/>
REPORTS_TO	Orgchart Manager Information	<input type="checkbox"/>	<input type="checkbox"/>
TERM_SEARCH	Search permissions for Terminations	<input type="checkbox"/>	<input type="checkbox"/>
ALLREQUESTERS	All requesters	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TERM	Terminations	<input type="checkbox"/>	<input type="checkbox"/>
ALLRECIPIENTS	All recipients	<input checked="" type="checkbox"/>	<input type="checkbox"/>
UPDATE-OWN-CONTACT	Update own contact info.	<input type="checkbox"/>	<input type="checkbox"/>
UPDATE-ORG-INFO	Change org information	<input type="checkbox"/>	<input type="checkbox"/>
ALLSELF	Self	<input type="checkbox"/>	<input type="checkbox"/>
DEFERRED-TERM	Deferred termination	<input type="checkbox"/>	<input type="checkbox"/>
VIEW-HOME-CONTACT	View user's home contact info	<input type="checkbox"/>	<input type="checkbox"/>
ALLREVIEWERS	All reviewers	<input type="checkbox"/>	<input type="checkbox"/>
_EXPLICIT_API_USERS_	Read-write access for explicit api users	<input type="checkbox"/>	<input type="checkbox"/>
NEW_USER	Fill in blanks for a new user	<input type="checkbox"/>	<input type="checkbox"/>
ALLAUTHORIZERS	All authorizers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
LOA_SEARCH	Search permissions for LOA	<input type="checkbox"/>	<input type="checkbox"/>
ALLIMPLEMENTS	All implementers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Update

Click **Update**.

14. Click the **Display criteria** tab.

15. Set the **Display type** to "Main" to display these attributes on users' main profile page.

The "Subsidiary" option means that user must click an icon  to display the values on a separate page.

16. Select the operations for which the attributes will be displayed. For this lab select:

View profile

Update profile

Create user profile

General Access control Members **Display criteria**

Display criteria VEHICLE-INFO

Display type: Main ▾

Display for custom requests containing the following operations:
This list of operations does not apply to pre-defined requests.

Update profile X Create user profile X View profile X

Update

17. Click **Update**.

Create an employee attribute group

1. Click **Manage the system** → **Workflow** → **Attribute groups**.

2. Click **Add new...**

3. Type the following information:

ID EMPLOYEE-INFO

Description Employee information

Leave other values as default.

4. Click **Add**.

5. Click the **Members** tab.

6. Click **Select...** to see a list of all attributes.

7. Select the checkboxes next to:

- EMPLOYEE-NUMBER
- EMPLOYEE-TYPE

General Access control **Members** Display criteria

Members: Profile attribute EMPLOYEE-INFO

i Added [EMPLOYEE-NUMBER].
Added [EMPLOYEE-TYPE].

<input type="checkbox"/>	ID	Description
<input checked="" type="checkbox"/>	↓ EMPLOYEE-TYPE	Type of user (employee, contractor, etc)
<input checked="" type="checkbox"/>	↓ EMPLOYEE-NUMBER	Employee number

Delete Update Select...

Showing 1 – 2 of 2

8. Click **Select**.

9. Click the **Access control** tab.

- Select **Read** and **Write** permissions for ALLREQUESTERS, ALLAUTHORIZERS, and ALLIMPLEMENTERS.
- Select **Read** permissions for ALLRECIPIENTS.

Access control EMPLOYEE-INFO

Search

Showing 1 - 19 of 19


Show / hide columns Records 20

ID	Description	Allow read	Allow write
PII	Read-write PII	<input type="checkbox"/>	<input type="checkbox"/>
REHIRE_DETECTION_SEARCH	Search permissions for Rehire detection	<input type="checkbox"/>	<input type="checkbox"/>
VIEW-PII	View own PII	<input type="checkbox"/>	<input type="checkbox"/>
REPORTS_TO	Orgchart Manager Information	<input type="checkbox"/>	<input type="checkbox"/>
TERM_SEARCH	Search permissions for Terminations	<input type="checkbox"/>	<input type="checkbox"/>
ALLREQUESTERS	All requesters	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TERM	Terminations	<input type="checkbox"/>	<input type="checkbox"/>
ALLRECIPIENTS	All recipients	<input checked="" type="checkbox"/>	<input type="checkbox"/>
UPDATE-OWN-CONTACT	Update own contact info.	<input type="checkbox"/>	<input type="checkbox"/>
UPDATE-ORG-INFO	Change org information	<input type="checkbox"/>	<input type="checkbox"/>
ALLSELF	Self	<input type="checkbox"/>	<input type="checkbox"/>
DEFERRED-TERM	Deferred termination	<input type="checkbox"/>	<input type="checkbox"/>
VIEW-HOME-CONTACT	View user's home contact info	<input type="checkbox"/>	<input type="checkbox"/>
ALLREVIEWERS	All reviewers	<input type="checkbox"/>	<input type="checkbox"/>
_EXPLICIT_API_USERS_	Read-write access for explicit api users	<input type="checkbox"/>	<input type="checkbox"/>
NEW USER	Fill in blanks for a new user	<input type="checkbox"/>	<input type="checkbox"/>
ALLAUTHORIZERS	All authorizers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
LOA_SEARCH	Search permissions for LOA	<input type="checkbox"/>	<input type="checkbox"/>
ALLIMPLEMENTERS	All implementers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Click **Update**.

10. Click the **Display criteria** tab.

11. Set the **Display type** to "Main" to display these attributes on users' main profile pages.

The "Subsidiary" option means that user must click an icon  to display the values on a separate page.

12. Select the operations for which the attributes will be displayed. For this lab select:

View profile

Update profile

Create user profile

General Access control Members **Display criteria**

Display criteria EMPLOYEE-INFO

Display type: Main

Display for custom requests containing the following operations:
This list of operations does not apply to pre-defined requests.

Update profile ✕ Create user profile ✕ View profile ✕

Update

13. Click **Update**.

Login as a regular user

To test this attribute group you will sign in as a regular user to see that the attributes are displayed when viewing or updating the user profile. Later, you will create a new user profile and add values to these attributes.

To log in and enroll as a regular user:

1. Log into the Front-end (PSF) as `<user>`.

2. Enter the password `<password>`.

3. In the **My profile** section, click **View and update profile**

You should see the **Vehicle information** and **Employee information** displayed on the **Profile information and entitlements** page.

Profile information and entitlements Jordon Hancock [JORDOH]

Profile information:

Basic information	
First name:	* Jordon
Other names:	C
Last name:	* Hancock
Profile picture:	Profile picture

Employee Information	
Employee number:	C1000011
Type of user (employee, contractor, etc):	Contractor

Vehicle information	
Vehicle description:	
Vehicle license:	

6 Use case: Defining restricted values manually


The *Hitachi ID Bravura Pattern* onboarding scenario components defines an EMPLOYEE-TYPE profile attribute that is mapped to the Active Directory employeeType account attribute. This type of attribute is populated by a set of restricted values. This use case will guide you through adding an additional restricted value to this attribute.

This use case assumes:

- *Hitachi ID Bravura Security Fabric* and *Hitachi ID Connector Pack* are installed.
- An Active Directory target system is added as a source of profiles.
- Complete [Use case: Creating profile and request attributes](#).
- Complete [Install Hitachi ID Bravura Pattern: Workforce Edition](#).

Define additional restricted values

To manually define restricted values:

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Workflow** → **Profile and request attributes** → **Profile and request attributes**.
3. Select  EMPLOYEE-TYPE.
Hitachi ID Bravura Security Fabric loads the **Profile and request attribute information** page.
4. Click the **Restricted values** tab.
5. Type the following values in the empty fields at the bottom of the table:
Actual value S
Displayed value Student
6. Click **More**.
7. Type:
Actual value P
Displayed value Part time
8. Click **Update**.

General
Restricted values
Test
Priority
Attribute groups

Restricted values EMPLOYEE-TYPE

Sort by: Actual value ▼

Delete	Actual value	Displayed value
<input type="checkbox"/>	C	Contractor
<input type="checkbox"/>	E	Employee
<input type="checkbox"/>	O	Other
<input type="checkbox"/>	P	Part time
<input type="checkbox"/>	S	Student
<input type="checkbox"/>	T	Temporary
<input type="checkbox"/>	V	Vendor
	<input type="text"/>	<input type="text"/> More
Update		

The **Actual value** is recorded in the database and written out to target systems, The **Displayed value** is shown to users in the *Bravura Security Fabric* interface.

CAUTION: If actual values contain the sequence `!!!`, *Bravura Security Fabric* will treat them as macros and expand them according to the skin being used. The actual values applied in this case will be different from what is defined in the attribute configuration. This will lead to the values being rejected, due to restricted list mismatch. The `!!!` sequence must therefore be avoided in actual values. If localization is required, specify the macro tag in the displayed value instead.

Default values

Attributes can be set up with default values for new resources and new profiles.

In the **General** tab, the **Default values** field is a drop-down list, allowing you to select one of the restricted values as the default. For this lab we will leave the Default values blank.

The screenshot shows a configuration form with the following fields and options:

- Restricted values are case-sensitive:** ☒
- Plug-in used to generate a list of restricted values:**
- Parent attribute:**
- Default values:** A dropdown menu with the following options: (Select one), Contractor, Employee, Other, Part time, Student, Temporary, Vendor.
- Inherit validation enforcement from attribute group:** ☐
- Update** button

7 Use case: Setting attribute validation rules


The EMPLOYEE-NUMBER profile attribute that we added to the [EMPLOYEE-INFO attribute group \(p11\)](#) is mapped to the Active Directory employeeNumber account attribute. In this use case you will define a validation rule for this attribute so that when new users are created their employee number must follow a particular format.

This use case assumes:

- *Hitachi ID Bravura Security Fabric* and *Hitachi ID Connector Pack* are installed.
- An Active Directory target system is added as a source of profiles.
- Complete [Use case: Grouping profile and request attributes](#).

To define a validation rule:

1. Log in to *Bravura Security Fabric* as `superuser`.

2. Click **Manage the system** → **Workflow** → **Profile and request attributes** → **Profile and request attributes**.
3. Select  EMPLOYEE-NUMBER.
Bravura Security Fabric loads the **Profile and request attribute information** page.
4. In the **Description of input values** type `One character followed by seven numbers only (example E1234567)`.
This is the description displayed to users to show them how to enter a value.
5. In the **Format requirement of input values** field, type `ANNNNNNN`.
6. Click **Update**.

Users will now be required to enter employee number values in the correct format.

Test the validity rules

You can test an attribute's validity once you have configured it.

To test, click the **Test** tab, enter an attribute value to validate, then click the **Test** button. You should see that a value like 1234 will fail, whereas entering a value that follows the format, such as E7654321 will pass.

The value entered is validated against the **Format requirement of input values** setting, the **Regular expression used for validation of input values** setting, the **Plugin used to generate a list of restricted values**, and any manually entered restricted values.

8 Use case: Modifying attribute priority

When you install *Hitachi ID Bravura Pattern: Workforce Edition*, the onboarding scenario component mapped `employeeNumber` to the EMPLOYEE-NUMBER profile attribute. However, that is not the only account attribute mapped to the EMPLOYEE-NUMBER. In cases where multiple account attributes have values and are all mapped to a single profile attribute, the attribute priority will determine which value is used. You will configure the EMPLOYEE-NUMBER profile attribute so that the `employeeNumber` from *Active Directory* takes priority.

This use case assumes:

- *Hitachi ID Bravura Security Fabric* and *Hitachi ID Connector Pack* are installed.
- *Bravura Pattern: Workforce Edition* is installed.
- An Active Directory target system is added as a source of profiles.

To define attribute priority:

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Workflow** → **Profile and request attributes** → **Profile and request attributes**.

3. Select  EMPLOYEE-NUMBER.

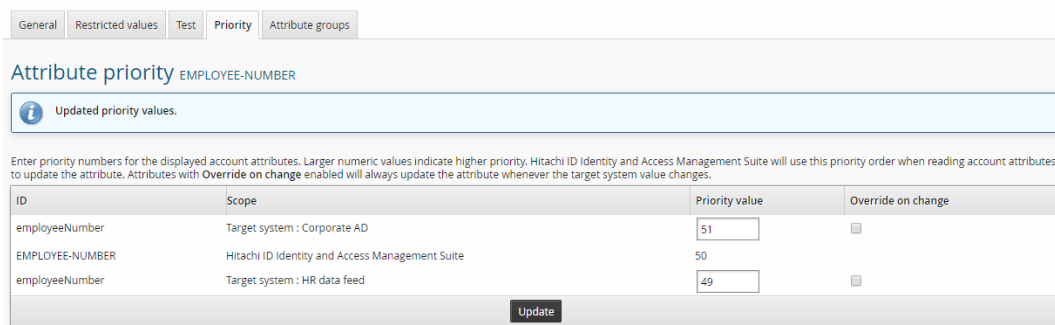
Bravura Security Fabric loads the **Profile and request attribute information** page.

4. Click the **Priority** tab.

Note that all priority values are set at 50, which means that *Bravura Security Fabric* will default to setting priority by alphabetical order of the attribute ID.

5. Set the **Priority value** of the Corporate AD employeeNumber to 51 and set the **Priority value** of the HR data feed employeeNumber to 49.

6. Click **Update**.



General Restricted values Test **Priority** Attribute groups

Attribute priority EMPLOYEE-NUMBER

Updated priority values.

Enter priority numbers for the displayed account attributes. Larger numeric values indicate higher priority. Hitachi ID Identity and Access Management Suite will use this priority order when reading account attributes to update the attribute. Attributes with **Override on change** enabled will always update the attribute whenever the target system value changes.

ID	Scope	Priority value	Override on change
employeeNumber	Target system : Corporate AD	51	<input type="checkbox"/>
EMPLOYEE-NUMBER	Hitachi ID Identity and Access Management Suite	50	<input type="checkbox"/>
employeeNumber	Target system : HR data feed	49	<input type="checkbox"/>

Update

The employeeNumber attribute from the Corporate AD target now has a higher priority and its value will be used first even if the other account attributes have values.

See also:

- For more detailed information about attributes see the [Bravura Security Fabric Documentation](#).
- The Connector Pack Integration Guide provides details on handling account attributes for each target system type.