

***Bravura Security Fabric* Implementation:**

Security questions and basic authentication

Hitachi ID Bravura Security Fabric provides administrators the flexibility to configure security questions to be used by end-users as a means to authenticate to systems.

This document contains:

- Requirement
- Solution
- Use case: Configure question sets
- Use Case: Configure question sets so that help desk users can ask questions
- Use Case: How end users complete their profile
- Use Case: How help desk users use question sets when helping a users

1 Requirement

Organizations require an alternate, or sometimes, an additional layer added to the authentication process. They also require an easy to use process to assist users if they forget their passwords.

2 Solution

Hitachi ID Bravura Security Fabric Front-end (PSF) supports multiple, highly configurable methods of authentication. By default, when you add your first target system, *Bravura Security Fabric* automatically configures itself to identify imported users by their ID on the target system, and to authenticate them using the password for their associated account on that target system. No additional configuration is required.

The second default authentication method uses security questions, where users type answers to personal questions.

You can disable security question authentication by changing the **PSQ ENABLED** setting in the **Modules** → **Update security questions (PSQ)** menu.

It is common for enterprises to build more complex authentication chains. If security questions are used, they are usually part of a multi-factor authentication chain, rather than relied on as a single authentication alternative.

There are many more configuration options for identification and authentication. This document demonstrates the basic default methods.

When question sets are configured, the basic, default authentication chain works this way:

1. Users visit the Front-end (PSF) login page.
2. Users enter their login ID for a trusted system, or their profile ID.
By default, users must identify themselves with their login ID from the first target system that you add as a source of profile IDs.
Product administrators such as superuser, who do not have accounts on integrated systems, must always enter their profile IDs.
3. With an out-of-the-box installation, users who have a completed security questions profile are given the option to authenticate either with a password or by answering a subset of their security questions.
4. Users who choose to authenticate via security questions are directed to the main menu if they provide correct answers to the required number of questions.

**BEST
PRACTICE**

When security questions are used:

- Prompt users to answer a random subset (e.g., 2/5) of pre-defined questions first and a random subset of self-defined questions second (e.g., 1/2). This hides self-defined questions from attackers, who must first correctly answer standard questions.
- Once a random subset of questions is chosen for a given user, continue to prompt for the same questions until there is a successful authentication. Do not allow attackers to "shop" for questions that they happen to know answers for.
- Use approximate string matching on answers, since users often type the same answers with different capitalization, punctuation, spaces or spelling.
- Questions should be chosen for each set except the one where users make up their own questions.
- Questions should have clear, memorable, non-changing answers that are not well known to people other than the user in question.

3 Use case: Configure question sets

This use case shows you how to configure the out-of-the-box question sets so that users have a number of user-defined and pre-defined questions.


Requirements

This use case assumes that:


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

Configure the user-defined question set

To configure the user-defined question set:

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Policies** → **Question sets**.
3. Click **User-defined questions**.
Hitachi ID Bravura Security Fabric lists the default user-defined question sets.
4. Select  **DEFAULT_USERQSET** to have a look at this default question set.
End users must create at least two questions and answers for this set. They will be asked two questions from this set during security question authentication.
5. Leave the **Minimum number of answered questions per user** at 2.
6. Change the **Number of questions to ask during authentication** to 1.
7. Click **Update**.
8. Return to the **Manage the system** → **Policies** → **Question sets** menu.

Configure pre-defined questions

1. Click **Pre-defined questions**.
Hitachi ID Bravura Security Fabric lists the default pre-defined question set.
2. Select  **DEFAULT_PREDEFQSET** to have a look at this question set.
End users must provide answers to at least 4 of the questions for this set, and the answers must be unique (cannot use the same value twice). The questions are listed in the bottom table on the configuration page. They will be asked two questions from this set during security question authentication.
You can select any of the questions to change its requirements, or add new questions.
3. Change the **Minimum number of answered questions per user** to 2.
4. Change the **Number of questions to ask during authentication** to 1.
5. Click **Update**.

4 Use Case: Configure question sets so that help desk users can ask questions

This use case demonstrates how to create a new question set that can be used by help desk users to help users.

Requirements

This use case assumes that:

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

Add a new question set to be used by help desk users

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Policies** → **Question sets**.
3. Click **Pre-defined questions**.
4. Click **Add new...**
5. Set the following:

ID `QD_HD`

Description `Help desk questions`

Enabled Select this checkbox

Users allowed to edit answers Select this checkbox

Minimum number of answered questions per user `2`

Help-desk permissions Select "Allowed to view security questions"

Number of questions to ask during authentication `2`

Page number for question set to be displayed in `1`

Note: Note that the **Ask users to answer questions from this set** checkbox should be left unselected. This means that end users will not have to answer questions from this set when they authenticate themselves – it will only be used when they call the help desk.

6. Click **Add**.
7. To define questions, click **Add new...** under **Question definition information** at the bottom of the question set page.
8. Enter the following:

Question `What department are you in?`

Minimum length of answer `2`

Maximum length of answer `25`

9. Click **Add**.
10. Click **Add new...** in the top right to add another question.
11. Enter the following:

Question What is your employee ID number?

Minimum length of answer 5

Maximum length of answer 5

Format of answer NNNNN

12. Click **Add**.
13. Click **Add new...** in the top right to add another question.
14. Enter the following:
 - **Question** What is your help desk PIN?
 - **Minimum length of answer** 4
 - **Maximum length of answer** 15

15. Click **Add**.
16. Click **Add new...** in the top right to add another question.
17. Enter the following:
 - **Question** How do you get to work most days?
 - **Minimum length of answer** 2
 - **Maximum length of answer** 25
18. Click **Add**.

Set up the help desk questions for use

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Policies** → **Authentication chains** → **Help desk authentication**.
3. Click **Disable** under **HELPDESK_LOGIN**.
This allows you to edit the authentication chain.
4. Under the **Modules** section, click **Add new...**
5. In the **Module configuration** section, select the "Security questions" module from the drop-down list, and click **Update**.
6. In the **Number of questions to ask during authentication** section, select "1" from the **From QD_HD** list.
Ensure that "(None)" is selected for the other lists.
7. Click **Update**.
8. Select the `scorepna.pss` module and click **Delete**.
9. Click **Enable**.

The QD_HD question set is now enabled for use in the *Help users* (IDA) module.

5 Use Case: How end users complete their profile

Security question authentication is only available to users after they complete their security question profiles. The default method for populating users' security questions and answers is to invite users to provide the information. *Bravura Security Fabric* can force users to do this by automatically directing them to the *Update security questions* (PSQ) module if their security question profile is incomplete. This facility can also be used for other enrollment tasks, such as claiming alternate IDs, filling in additional user information, or agreeing to an acceptable use policy.

The **PSF FORCE ENROLLMENT** setting in the **Modules** → **Front-end (PSF)** menu controls which tasks users must complete before they do anything else in *Hitachi ID Bravura Security Fabric*.

This use case will demonstrate what it looks like for a regular user when they complete their security question profile for the first time.

Requirements

This use case assumes that:

- *Hitachi ID Bravura Security Fabric* and *Hitachi ID Connector Pack* installed.
- An Active Directory target system is added as a source of profiles.
- Completed [Use case: Configure question sets](#).
- Completed [Use Case: Configure question sets so that help desk users can ask questions](#).

Completing the enrollment process

1. Log into the Front-end (PSF) as an end user.
2. Enter the password `Examplepassword`.
3. Complete the security questions profile.

You will notice that now the user is prompted to fill six questions. Two from the user-defined question set, two from the pre-defined question set and two from the new help desk question set created in [Use Case: Configure question sets so that help desk users can ask questions](#).

Note: By default, the security questions are case insensitive.

The guided enrollment process cannot be skipped, ensuring users have completed the above steps before gaining access to the product.

4. Log out.
5. Go to the Front-end (PSF) again and enter the ID for the same user.
This time you are given a choice of how to authenticate (password or security questions).
6. Choose **Answer security questions**.
7. Answer the questions.

Notice how instead of being requested to answer six security questions, you are only prompted to answer one question from the user-defined question set and one from the pre-defined question set.

8. Log out.

6 Use Case: How help desk users use question sets when helping a users

Hitachi ID Bravura Security Fabric allows authorized help desk staff to reset passwords on behalf of a user. This use case will show how a help desk user can authenticate a user using their security questions and then, reset that user's password.

By default, help desk users would authenticate a user by asking security questions from the user's standard questions.

In [Use Case: Configure question sets so that help desk users can ask questions](#) we set up a custom question set to be used only by help desk users. In this use case we will use those custom questions.

Requirements

This use case assumes that:

- *Hitachi ID Bravura Security Fabric* and *Hitachi ID Connector Pack* installed.
- An Active Directory target system is added as a source of profiles.
- Completed [Use Case: How end users complete their profile](#).
- Help desk user has "view security questions" and "view answers to security questions" privileges.

Reset a password

1. Log into the Front-end (PSF) as `ZorroOne`, password `ExamplePassword`.
2. Click **Help users**.
3. Search or browse to select the end user.
Hitachi ID Bravura Security Fabric presents you with a security question from the QD_HD set.
4. Answer the questions, and click **Continue**.
5. Click the **Security questions** tab.
Notice that you can see the user's answers to the security questions from the QD_HD set.
6. Click the **Change passwords** tab.
7. Type a new password for the caller in the **New password** and **Confirm** fields.
Ensure that the password satisfies all the strength rules displayed on this page. The maximum allowable length for a password is 127 characters.
8. Click **Change and expire passwords** to expire the password after the initial login and allow the user to choose their own password.