System Configuration

Contents

System Configuration

The System Configuration page includes functions the PHEMI Administrator uses to set up and maintain PHEMI Central.

What is the workflow for initial configuration?

The Password Policy

A password policy is one way your organization can secure your information systems.

A password policy generally enforces the strength of a password, by requiring passwords to be of a certain length and by stipulating that a password must include a certain mix of letters, numbers, and/or special characters. The password policy may also control how quickly a given password can be reused.

The password policy is generally decided on by the privacy officer, or someone in a similar role. The privacy policy is implemented in PHEMI Central by the PHEMI Administrator, as part of system configuration.

View the Password Policy

View the configured password policy on the **Password Policy** screen of the **System Configuration** page.

Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.

The **System Configuration** page opens on the **Password Policy** screen.

Configure the Password Policy

Set the password policy on the **Password Policy** screen of the **System Configuration** page.

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.
   The **System Configuration** page opens on the **Password Policy** screen.

2. Set the password policy information.

Option	Description
Minimum Length	Mandatory. The minimum length for the password. The range is 6 to 15. The default is 6.
Maximum Length	Mandatory. The maximum length for the password. The maximum starts at the value set for **Minimum Length** (that is, maximum and minimum value can be the same) and ranges to 32 characters. The default is 32.
Can't reuse *n* passwords	Optional. Specifies the number of times in a row a password can be used. For example, if this value is set to 1, the user cannot reuse the same password twice; at least one more password must intervene before reusing the original password. The range is 0 to 12. The default is 0, which means that the same password can be repeated indefinitely.
Non-Alpha Character	Optional. Specifies whether the password must include with a non-alphabetical character. Non-alphabetical characters are numbers or special characters. Spaces are not supported. Supported values are as follows: • Required: Passwords must include at least one non-alphabetical character. • Optional: Passwords can consist of only alphabetic characters.

Option	Description
	The default is Optional.
First/Last non-numeric characters	Optional. Specifies whether the password must begin and end with a non-numeric character. Non-numeric characters include alphabetical characters and special characters. Spaces are not supported. Supported values are as follows: • Required: Passwords must begin and end with a non-numeric character. • Optional: Passwords may begin and end with alphabetic or special characters. The default is Optional.
User ID in Password	Optional. Specifies whether the string representing the user's ID may appear in the password. Supported values are as follows: • Disallowed: The user ID may not appear in the password. • Allowed: The user ID may appear in the password. The default is Allowed.

3. Save the password policy by clicking the **Save** button.

User Authorizations

User authorizations are configurable attributes you can assign to PHEMI Central users. Authorizations are defined in PHEMI Central by the PHEMI Administrator, who sets them in accordance with the organization's governance policies.

User authorizations are used together with data visibilities to create access policies. The access policy matches the authorization against the data visibility to determine what action, if any, a user may take with respect to accessing the data.

Some examples of possible user authorizations are as follows:

- C_LEVEL: The user is a C-Level individual (for example, CEO, COO, CIO, or CTO) with a privileged level of access. Individuals with C_LEVEL authorization, for example, might be permitted to read data with CONFIDENTIAL visibility.
- DOCTOR: A user with DOCTOR authorization might, for example, be permitted to read any information, including personally identifiable information or personal health information.
- ANALYST: A user with ANALYST authorization might be restricted to accessing only the de-identified or nonidentified data.

A user can be assigned multiple authorizations. User authorizations are set by the PHEMI Administrator during system configuration.

All users are assigned the predefined PUBLIC authorization by default. The PUBLIC authorization can subsequently be removed by the PHEMI Administrator.

Note: Once defined, a user authorization setting may be neither edited nor deleted. The description may be subsequently edited.

View Defined User Authorizations

View defined user authorizations on the **User Authorizations** screen of the **System Configuration** page.

To view defined user authorizations:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.
   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **User Authorizations** tab.

   The **User Authorizations** screen opens, showing you each authorization that has been defined, along with a brief description.

Define User Authorizations

Define user authorizations on the **User Authorizations** screen of the **System Configuration** page.

The user authorizations you define should reflect your organization's governance policies. Consult your privacy officer, or a person in a similar role, to understand what user authorizations your organization recognizes.

How do I define a governance policy?

Note: Once defined, a user authorization label may be neither edited nor deleted. The description may be subsequently edited.

To define a user authorization:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.

   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **User Authorizations** tab.

   The **User Authorizations** screen opens.

3. Cick the **Create Authorization** button.

   The **Create Authorization** screen opens.

4. Specify the authorization information.

Option	Description
Name	The authorization label to be applied to users.
Description	A brief description for the authorization label.

5. Save the authorization information by clicking the **Create** button.

Modify Authorization Description

Modify user authorizations on the **User Authorizations** screen of the **System Configuration** page.

Although you can't delete a user authorization or edit the authorization label, you can edit the description after the authorization has been created.

To edit a user authorization description:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.

   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **User Authorizations** tab.

   The **User Authorizations** screen opens.

3. Location the description for the authorization you want to edit. Click the **Modify** button.

   The

4. Save the change by clicking the **Modify** button.

Dataset Destinations

Datasets can be exported to consuming applications and tools.

Tell me about datasets.

Datasets can be consumed by querying them through the PHEMI RESTful API or by configuring a dataset export target as a "destination" in the Management and Governance Console.

Dataset destinations are configured by the PHEMI Administrator. The destination is characterized in terms of the connection type, the network parameters, the destination database and schema names, and the user credentials for logging on to the destination.

View Dataset Destinations

View dataset destinations on the **Dataset Destinations** screen of the **System Configuration** page.

To view defined dataset destinations:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.

   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **Dataset Destinations** tab.

   The **Dataset Destinations** screen opens.

3. At the right of the **Choose Destination to Edit** field, click the drop-down arrow to see configured dataset destinations.

Create a Dataset Destination

Define a new dataset destination on the **Dataset Destinations** screen of the **System Configuration** page.

To create a new dataset destination:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.

   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **Dataset Destinations** tab.

   The **Dataset Destinations** screen opens.

3. Click the **New Destination** button to the right of the **Choose Destination to Edit** field.

   The **Destination Details** screen opens.

4. Enter the destination details.

Option	Description
Name	Mandatory. Provide a name for the destination.
Type	Mandatory. The destination type. Supported values are as follows: • MySQL. The destination is a MySQL database. • HANA. The destination is a SAP HANA database.

Option	Description
	Both MySQL and HANA destination types use a Jave Database Connectivity (JDBC) connection.
Host	Mandatory. The IP address of the destination, in dotted decimal format.
Port	Mandatory. The destination TCP port.
Database Name	Mandatory. The name of the destination database.
Schema	Mandatory. The name of the schema being used in the destination database.
User Name	Mandatory. The user name for logging on to the destination.
Password	Mandatory. The password for logging on to the destination.
Confirm Password	Mandatory. Re-enter the password to ensure it is correct.

5. Click the **Save Destination** button to save the new destination.

View Dataset Destination Information

View information about a dataset destination on the **Dataset Destinations** screen of the **System Configuration** page.

To view information for a dataset destination:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.

   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **Dataset Destinations** tab.

   The **Dataset Destinations** screen opens.

3. Click the drop-down arrow at the right of the **Choose Destination to Edit** field to see configured dataset destinations. Select the destination you want to view.

4. The **Destination Details** screen opens, showing information for the selected dataset.

Modify Dataset Destination Information

Modify information for a dataset destination on the **Dataset Destinations** screen of the **System Configuration** page.

To modify information for a dataset destination:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.

   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **Dataset Destinations** tab.

   The **Dataset Destinations** screen opens.

3. Click the drop-down arrow at the right of the **Choose Destination to Edit** field to see configured dataset destinations. Select the destination you want to modify.

4. The **Destination Details** screen opens, showing information for the selected dataset. *What do these fields mean?*

5. Click the **Edit Destination** button. The fields on the **Destination Details** screen become editable, and the **Delete Destination** buttons and **Save Destination** buttons appear.

6. Make your changes. If you need to change the destination password information, click the **Modify Connection Password** button.

   The **Set Password** pane opens underneath the other destination information.

7. Complete your changes, then click the **Save Destination** button to save the changed information.

Delete a Dataset Destination

Delete a dataset destination on the **Dataset Destinations** screen of the **System Configuration** page.

To delete a dataset destination:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.

   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **Dataset Destinations** tab.

   The **Dataset Destinations** screen opens.

3. Click the drop-down arrow at the right of the **Choose Destination to Edit** field to see configured dataset destinations. Select the destination you want to delete.

4. The **Destination Details** screen opens, showing information for the selected dataset.

5. Click the **Edit Destination** button. The fields on the **Destination Details** screen become editable, and the **Delete Destination** buttons and **Save Destination** buttons appear.

6. Click the **Delete Destination** button. The system asks you to confirm permanent deletion. Click **Delete**.

Data Retention Behavior

Each data collection has a data policy that specifies, among other things, how long data items should be retained in the system. When the item's "time to live" expires,
Content-Reference to:../_Variables/PHEMI_Central/con_Product-Vars.xml#product-name
deletes the item from the data store. The data retention behavior, which is set in system configuration, specifies when
Content-Reference to:../_Variables/PHEMI_Central/con_Product-Vars.xml#product-name
checks the data store to see what data, if any, is expired and should be deleted from the data store.

You can configure
Content-Reference to:../_Variables/PHEMI_Central/con_Product-Vars.xml#product-name
to check on a schedule, or you can manually initiate checking.

View the Data Retention Schedule

View the schedule for data retention behavior on the **Data Retention** screen of the **System Configuration** page.

To see the configured data retention schedule:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.

   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **Data Retention** tab.
   The **Data Retention** page opens, showing the schedule for automatic checking.

Set the Data Retention Schedule

Set the schedule for data retention on the **Data Retention** screen of the **System Configuration** page.

To set how often the system checks for expired data:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.
   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **Data Retention** tab.
   The **Data Retention** page opens.

3. In the **Frequency** field, choose between **hourly**, **daily**, or **weekly**, or specify the number of minutes between checks.
4. Click **Save** to save the changes.

Manually Check Data Retention

Trigger data retention checking at any time on the **Data Retention** screen of the **System Configuration** page.

To manually initiate checking for expired data:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.
   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **Data Retention** tab.
   The **Data Retention** page opens.

3. In the **Data Collections** field, select all the data collections you want to check.
4. Click **Enforce Retention Now**. PHEMI Central checks the selected data collections for expired data.

Data Categories

High-level data categories help you classify the data that will be stored in PHEMI Central.

Each data category can include multiple collections, data systems (such as different databases), or data collections. For example, an organization might have a category BILLING, which could include data from several different billing systems in the organization. Another might have a category ECG, which might contain electrocardiograms from different data sources.

View Data Categories

View the names of defined data categories on the **Data Categories** screen of the **System Configuration** page.

To view data category names:

Open the **Data Collections** screen, by clicking the **Data Collections** icon in the left navigation bar.

The **Data Collections** page opens showing the defined data categories.

If you are a PHEMI Administrator, you can also view data category names from the **System Configuration** > **Data Categories** screen.

Open the **System Configuration** screen, by clicking the **System Configuration** icon. Then click the **Data Categories** tab to open the **Data Categories** screen. At the right side of the **Choose Category to Edit** field, click the drop-down list to see the list of defined data categories.

Add a Data Category

Add a data category on the **Data Categories** screen of the **System Configuration** page.

Datasource categories are configured by the PHEMI Administrator. To add a data category:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.
   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **Data Categories** tab.
   The **Data Categories** screen opens.

3. Click the **New Category** button.

   The **Data Categories** screen expands to show the **Category Details** area.

4. Enter a name for the category.
5. Save the data category by clicking the **Save Category** button.

Edit a Data Category Name

Modify a data category name on the **Data Categories** screen of the **System Configuration** page.

To edit a data category name:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.
   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **Data Categories** tab.
   The **Data Categories** screen opens.

3. At the right side of the **Choose Category to Edit** field, click the drop-down list and select the category you want to edit.

   The **Category Details** screen opens.

4. Make your edits to the category name.
5. Save the changes by clicking the **Save Category** button.

Delete a Data Category

Delete a data category on the **Data Categories** screen of the **System Configuration** page.

To delete a data category:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.
   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **Data Categories** tab.
   The **Data Categories** screen opens.

3. At the right side of the **Choose Category to Edit** field, click the drop-down list and select the category you want to delete.

   The **Category Details** screen opens.

4. Click the **Delete Category** button.
5. The system asks you to confirm permanent deletion of the category. Click **Delete**.

Data Visibilities

Data visibilities identify the privacy requirements for data.

All raw data and derived data stored in PHEMI Central can be tagged with labels that provide information about the data's sensitivity. This sensitivity is described in terms of the visibility the data should have to different system users. The visibility tags you define for your data should reflect the sensitivity of the data as identified by your organization.

The visibility of data in your organization should be set out in your organization's governance policy. Working from the governance policy, the PHEMI Administrator and is configured as part of system configuration.

You can define data visibilities to suit your organization's needs. Possible examples are CONFIDENTIAL to identify data that is sensitive and requires a user to a certain level of access or certification to access, PII to identify Personally Identifiable Information, PHI to identify personal health information, or SECRET to identify especially sensitive material.

Note: Once defined, a data visibility may be neither edited nor deleted. The description for the visibility can be modified subsequently.

The data visibilities specified for a data collection are referred to in access policies and matched against user authorizations to determine what actions, if any, a given user is allowed to perform on the data. The access policy can then be applied to a data collection or dataset during system configuration. *Tell me about user authorizations. Tell me about access policies.*

In addition, any data visibility defined in the system can be used by a Data Processing Function (DPF) to tag any derived data fields. These derived data elements can be assigned different privacy levels from the data collection and from one another. For example, the Social Security Number extracted from a health record can be tagged CONFIDENTIAL if that data visibility has been defined in the system. This mechanism provides field-level privacy protection.

View Configured Data Visibilities

View configured data visibilities on the **Data Visibilities** screen of the **System Configuration** page.

To view the data visibilities that have been configured in the system:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.

   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **Data Visibilities** tab.

   The **Data Visibilities** screen opens, listing all the data visibilities configured for the system.

Define Data Visibilities

Define a data visibility on the **Data Visibilities** screen of the **System Configuration** page.

Note: Once defined, a data visibility may be neither edited nor deleted. The description may be modified subsequently.

To define data visibilities:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.
   The **System Configuration** page opens on the **Password Policy** screen.

2. Click the **Data Visibilities** tab.
   The **Data Visibilities** screen opens.

3. Click the **Create Visibility** button. The **Create Visibility** screen opens.
4. Enter the visibility information.

Option	Description
Name	Enter a name for the data visibility; for example, "CONFIDENTIAL," "SECRET" or "PII".
Description	Enter a brief description to describe the intention of the visibility.

5. Save the visibility information by clicking the **Create Visibility** button.