Administrator Quick Start Guide

Contents

Introducing PHEMI Central

To be written

Intro blurb to segue into following overview content.

PHEMI Central Overview

To be written.

This topic will provide a basic introduction to and overview of PHEMI Central. It will include relevant content and diagrams similar to that in the Product Description currently being developed.

Introducing the Management Console

Quick Tour of the Management Console

Before You Configure

Before you start configuring PHEMI Central, the system must be installed and you should have your organization's governance policy clearly defined.

System Installation

PHEMI Central may be shipped as an appliance, deployed on Amazon Web Services (AWS), or deployed on your organization's VMware environment. Regardless of the deployment type, a PHEMI representative will install and set up the base system of cluster nodes with a management node and will install the PHEMI Central software on the cluster.

The representative will create an administrator account for you on PHEMI Central, and will provide you with the user name and password for the account, together with the URL of the PHEMI Central Management Console. At that point, you can log on to the Management Console.

Governance Policies

To protect your data and the privacy of your data, you should have your organization's governance policy in place before configuring PHEMI Central. A governance policy is a coordinated approach to protecting data and assigning privileges to users.

There are three main aspects to a governance policy:

- Data visibility. Data can have different levels of visibility or sensitivity, and your organization may need to protect different data in different ways. You may want some data visible to every user but other data visible only to selected users. In PHEMI Central, these levels are called "data visibilities." *Tell me more about data visibilities*
- User authorizations. Different users may be required to interact with data differently. For example, clinicians might be allowed to access all data, while researchers might be allowed to read only non-identified or de-identified data. *Tell me more about user authorizations*
- Access policies. Your organization's governance policy will state how users with different authorizations can interact with data of different visibility. *Tell me more about access policies*

The data visibilities, user authorizations, and access policies defined in your governance policies will drive how you configure PHEMI Central. If you are uncertain as to the appropriate data visibilities, user authorizations, or access policies to define for your organization, consult with your Information Officer, Privacy Officer, or with someone in a comparable role.

Configuration Workflow

Since some configuration tasks must be completed before others can be performed, use this workflow to configurePHEMI Central.

In these first steps, order matters. You cannot create users until you have defined user authorizations. Likewise, you cannot create access policies without defining both user authorizations and data visibilities.

1. *Log on to the PHEMI Central Management Console*.
2. *Define user authorizations.*
3. *Create users.* Create at least one PHEMI administrator, at least one privacy officern, and at least one data analyst.
4. *Define data visibilities.*

Data categories must be added before you can define data sources. Access policies are optional for data source configuration. If you are using a Data Processing Function (DPF) to create derived data from raw data, you upload the DPF archive as part of data source configuration.

5. *Add data categories.*
6. *Create access policies.*
7. *Define data sources.*

In general, it is the data analyst, not the PHEMI administrator, who builds and executes datasets. However, configuring dataset destinations is part of system configuration.

8. *Configure dataset destinations.*

Logging On to the Management Console

The PHEMI Central Management Console is web-based.

Note: Use either Mozilla Firefox or Google Chrome to access the PHEMI Central Management Console. Microsoft Internet Explorer is not supported.

The URL for the PHEMI Central Management Console is configured during installation and setup of PHEMI Central. Your PHEMI representative will provide you with the URL.

To access the PHEMI Central Management Console:

1. In the address bar of the browser, enter the URL configured for the PHEMI Central Management Console.

   The PHEMI Central login screen appears.

2. Enter your user name and password. Click **Login**.
   The PHEMI Central Management Console launches.The Management Console initially opens on the Data Sources page. Subsequently, the system remembers the last page you viewed and opens on that page.

Define User Authorizations

Define user authorizations on the **System Configuration** page.

Provisional: needs to be updated from demo system.

Note: Once defined, a user authorization may be neither edited nor deleted.

To define 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 **Authorizations** tab.

   The **Authorizations** screen opens.
3. Set the authorization information.

Option	Description

4. Save the authorization information by clicking the **Save** button.

Create a New User

Create a new user on the **Manage Users** page.

To create a new user:

1. Open the **Manage Users** page, by clicking the **Users** icon in the left navigation bar.

   The **Manage Users** page lists all users defined in the system so far.
2. Click the **Create User** button.

   The **Create a New User** window opens.
3. Enter the user information.

Option	Description
Full Name	Mandatory. The user's full name.
User name	Mandatory. The user ID for this user. The **User Name** field autopopulates with the first initial and last name entered for as the user's full name. For example, if the user's full name is Jane Smith, the **User Name** field autopopulates with jsmith. The user ID can be edited after it has been autopopulated. IDs can be up to 16 characters long. Alphabetic and numeric values are permitted, as well as underscore ("_"). Spaces and hyphens are not permitted.
Phone Number	Optional. The user's phone number. You must configure this field if you want the system to send alerts to the user's phone.
Email	Mandatory. The user's email address. If you configure the system to send email alerts to the user, this is the email address that will be used.
Role	Mandatory. The user's system role. Together with the user authorization configured and the visibility set for data, the user role determines what access the user will have to data. Each user has exactly one role.*Tell me about user roles.*
Authorizations	Optional. The types of data the user is authorized to access. Use either the **Shift** key or the **Ctrl** key to make multiple selections. *Tell me about user authorizations.*
Password	Mandatory. The password policy (such as minimum and maximum length, whether a password can be reused, and so on) is set by your administrator in

Option	Description
	system configuration. Passwords must be confirmed by re-entering.

4. Save the user information by clicking the **Save User** button. The system confirms when the user has been successfully saved. Click **Close** to close the screen.

Define Data Visibilities

Define data visibilities on the **System Configuration** page.

Note: Once defined, a data visibility may be neither edited nor deleted.

To define the visibility levels for data stored in PHEMI Central:

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 **Manage Visibilities** tab.

   The **Manage 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 remind you or someone else of the intention of the visibility.

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

Add a Data Category

Use the **Datasource Categories** screen of the **System Configuration** page to add a data category.

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 **Datasource Categories** tab.

   The **Datasource Categories** screen opens.
3. Click the **New Category** button.

   The **Datasource 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.

Create an Access Policy

Create a new access policy on the **Access Policy Builder** page.

Before you can define an access policy you must configure the following:

- User authorities
- Data visibilities
- Environments (access networks)

To create a new access policy, define one or more access rules:

1. Open the **Access Policy Builder** page, by clicking the **Access Policy Builder** icon in the left navigation bar.

   The **Access Policy Builder** page opens.

2. Click the **New Policy** button.

   The form for the new access policy opens, with Rule 1 ready for you to edit.

3. Enter the access rule information.

Option	Description
Subject	Mandatory. The user authorizations allowed to perform the action on the data. User authorizations are configured for the system by the administrator.
Action	Mandatory. The action(s) an authorized user may take on the data. Supported actions are as follows: • Read. The user may view the data. • Export. The user may export the data to a destination, such as a SAP system.
Object	Mandatory. The data visibilities authorized users are allowed to access. Data visibilities are configured by the administrator.

4. Add another rule by clicking the **Add Rule** button. Or, save the access policy by clicking the **Save Access Policy** button. The system confirms when the access policy has been successfully saved.

Define a Data Source

Define a data source on the**Data Sources** page.

Before defining a data source, you must configure the following:

- Data categories
- Data visibilities
- Users

To configure users, you must first configure user authorizations. If you want to apply access policies to the data source, you must first configure the access policies.

To define a new data source:

1. Open the **Data Sources** page, by clicking the **Data Sources** icon. in the left navigation bar.

   The **Data Sources** page opens showing all defined data categories.

2. Click the **New Data Source** button.

   The **New Data Source** screen opens.

3. Describe the source.

Option	Description
Name	Mandatory. A descriptive name for the data source. Numbers, letters, spaces, and special characters are supported. **Note:** Once you save a data source, the name cannot be edited. To change the name, you must delete the data source and reconfigure it with the correct name.
Source Category	Mandatory. The data category of the data source. Choose from the drop-down list of defined data categories. *How do I define a data category?*
Institutional Owner	Mandatory. The individual responsible overall for data stored in PHEMI Central. The user must be a PHEMI Administrator. Choose from the drop-down list of eligible users.
Privacy Officer	Mandatory. The individual responsible for defining the organization's governance policy and for approving access policies. The user must be a Privacy Officer. Choose from the drop-down list of eligible users.
Source Owner	Mandatory. The individual responsible for approving dataset requests involving this data source. The user must be a PHEMI Administrator. Choose from the drop-down list of eligible users.
Document Format	Optional. The kinds of document expected from this data source. Examples are Microsoft Word, Excel, or JSON.
Definition	Optional. A brief description of the kinds of documents expected from this data source.
Notes	Optional. Any additional notes for the data source.
Data Sharing Agreement	Optional. A copy of the agreement allowing data to reside on PHEMI Central. Only one data sharing agreement can be uploaded.

4. Save the data source information by clicking the **Save Data Source** button. The system confirms when the data source has been successfully saved.

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. To the right of the **Choose Destination to Edit** field, click the **New Destination** button.

   The **Destination Details** screen opens.

4. Enter the destination details.

Option	Description
Name	Mandatory. The name of 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.
Host	Mandatory. The IP address of the destination, in dotted decimal format.
Port	Mandatory. The port on the destination to send data to.
Database Name	Mandatory. The name of the destination database.
Schema	Mandatory. The schema being used in the destination database.
User Name	Mandatory. The user name to be used to log on to the database.
Password	Mandatory. The password to be used to log on to the database.
Confirm Password	Mandatory. Re-enter the password to ensure it is correct.

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