

# **Password Policy**

# Contents

**The Password Policy.....3**  
    View the Password Policy.....3  
    Configure the Password Policy..... 3

## The Password Policy


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

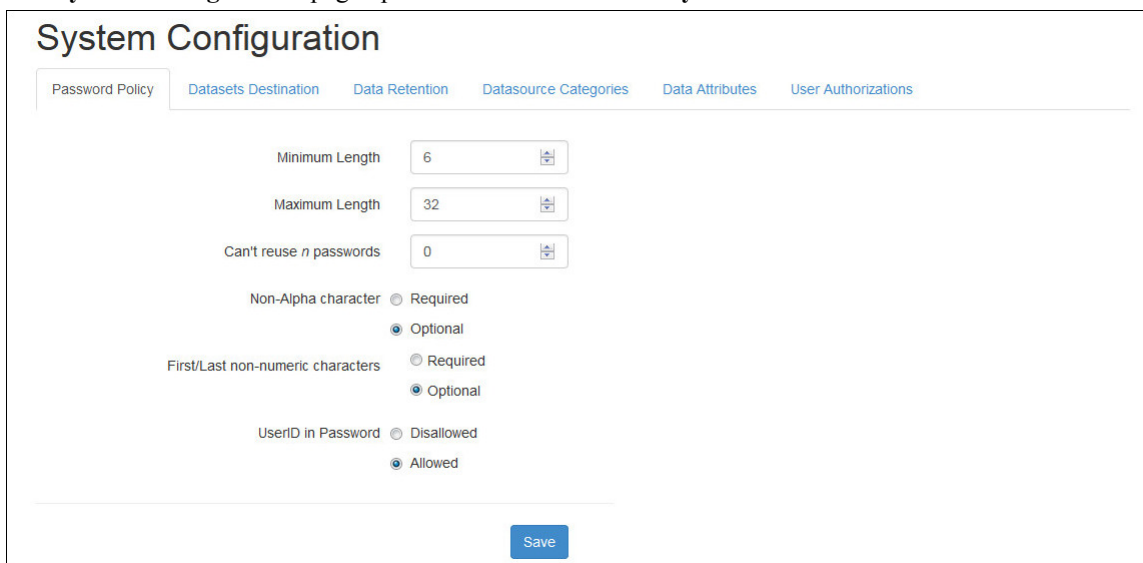
A password policy generally enforces the strength of a password, by requiring passwords to be of a certain length and by stipulating that a password must include a certain mix of letters, numbers, and/or special characters. The password policy may also control how quickly a given password can be reused.

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.




The screenshot shows the 'System Configuration' page with the 'Password Policy' tab selected. The page contains several configuration options for password strength and reuse:

- Minimum Length:** A text input field with the value '6'.
- Maximum Length:** A text input field with the value '32'.
- Can't reuse *n* passwords:** A text input field with the value '0'.
- Non-Alpha character:** Radio buttons for 'Required' and 'Optional'. 'Optional' is selected.
- First/Last non-numeric characters:** Radio buttons for 'Required' and 'Optional'. 'Optional' is selected.
- UserID in Password:** Radio buttons for 'Disallowed' and 'Allowed'. 'Allowed' is selected.

A 'Save' button is located at the bottom right of the configuration area.

## 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.

## System Configuration

Password Policy
Datasets Destination
Data Retention
Datasource Categories
Data Attributes
User Authorizations

Minimum Length

Maximum Length

Can't reuse *n* passwords

Non-Alpha character

☐ Required  
☒ Optional

First/Last non-numeric characters

☐ Required  
☒ Optional

UserID in Password

☐ Disallowed  
☒ Allowed

## 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.

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.

**Option**

**Description**

The default is Allowed.

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