Password Policy

Contents

Password Policies

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. In PHEMI Central, the privacy policy is configured by the PHEMI Administrator as part of system configuration.
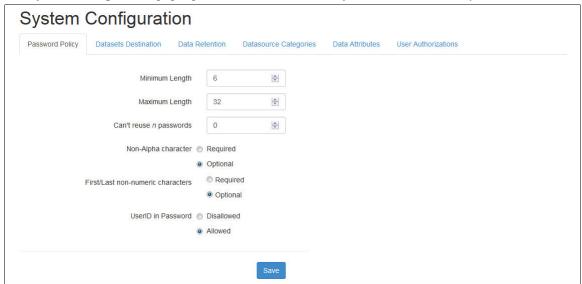
View the Password Policy

Use the **Password Policy** screen of the **System Configuration** page to see the configured password policy.

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. *What do these fields mean?*
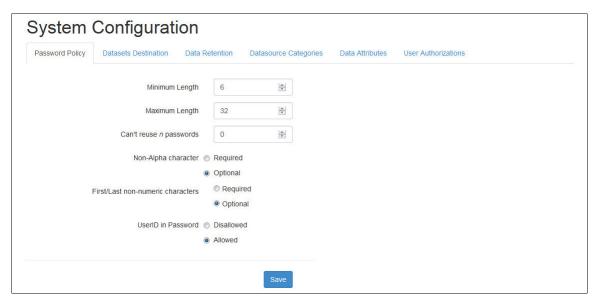

Configure the Password Policy

Use the **Password Policy** screen of the **System Configuration** page to configure your organization's password policy.

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. 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.