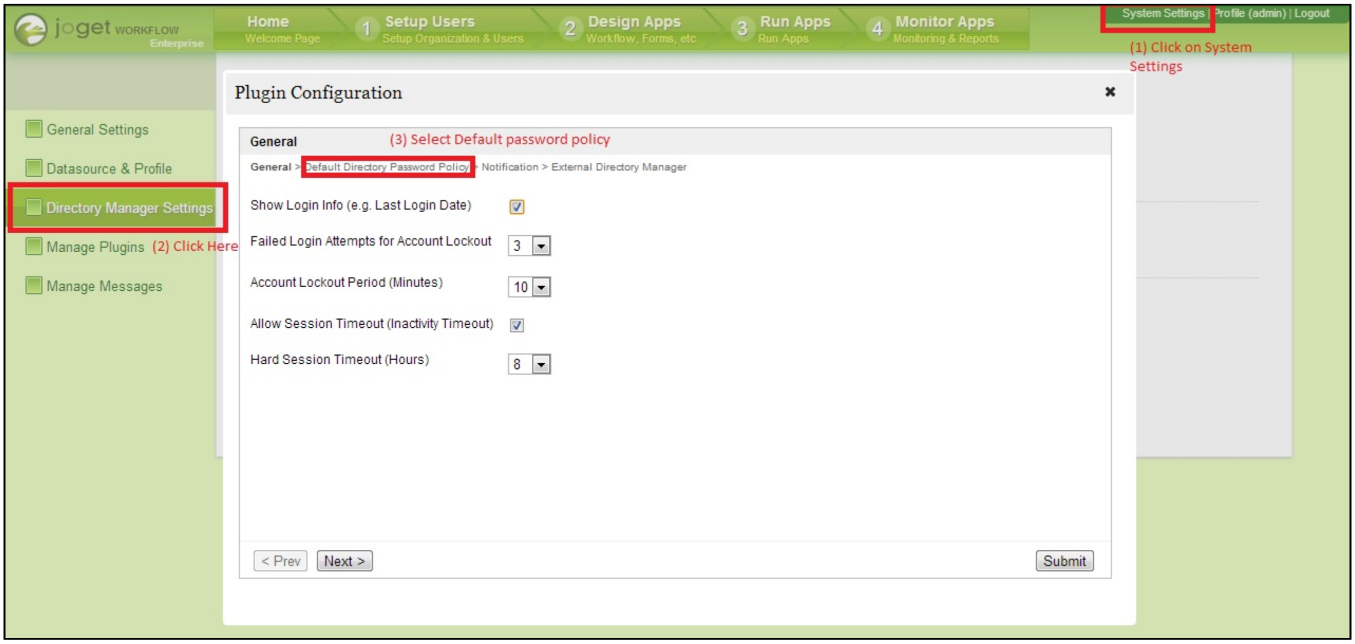
Password Reuse Policy

Enforcing Password history

Enforcing password history will define how frequently the passwords can be used from the history base. These settings can be administered using the **Security Enhanced Directory Manager** plugin

Here are the steps

Go to **System Settings>Directory Manager Settings>Configure Plugin(Security Enhanced Directory Manager)>Default Directory Password Policy**



joget WORKFLOW Enterprise
Home Welcome Page
1 Setup Users Setup Organization & Users
2 Design Apps Workflow, Forms, etc
3 Run Apps Run Apps
4 Monitor Apps Monitoring & Reports
System Settings
Profile (admin) | Logout
General Settings
Datasource & Profile
Directory Manager Settings
Manage Plugins
Manage Messages
< Prev
Next >
Submit

(1) Click on System Settings

(2) Click Here

(3) Select Default password policy

Plugin Configuration

General

General > Default Directory Password Policy > Notification > External Directory Manager

Show Login Info (e.g. Last Login Date) ☑

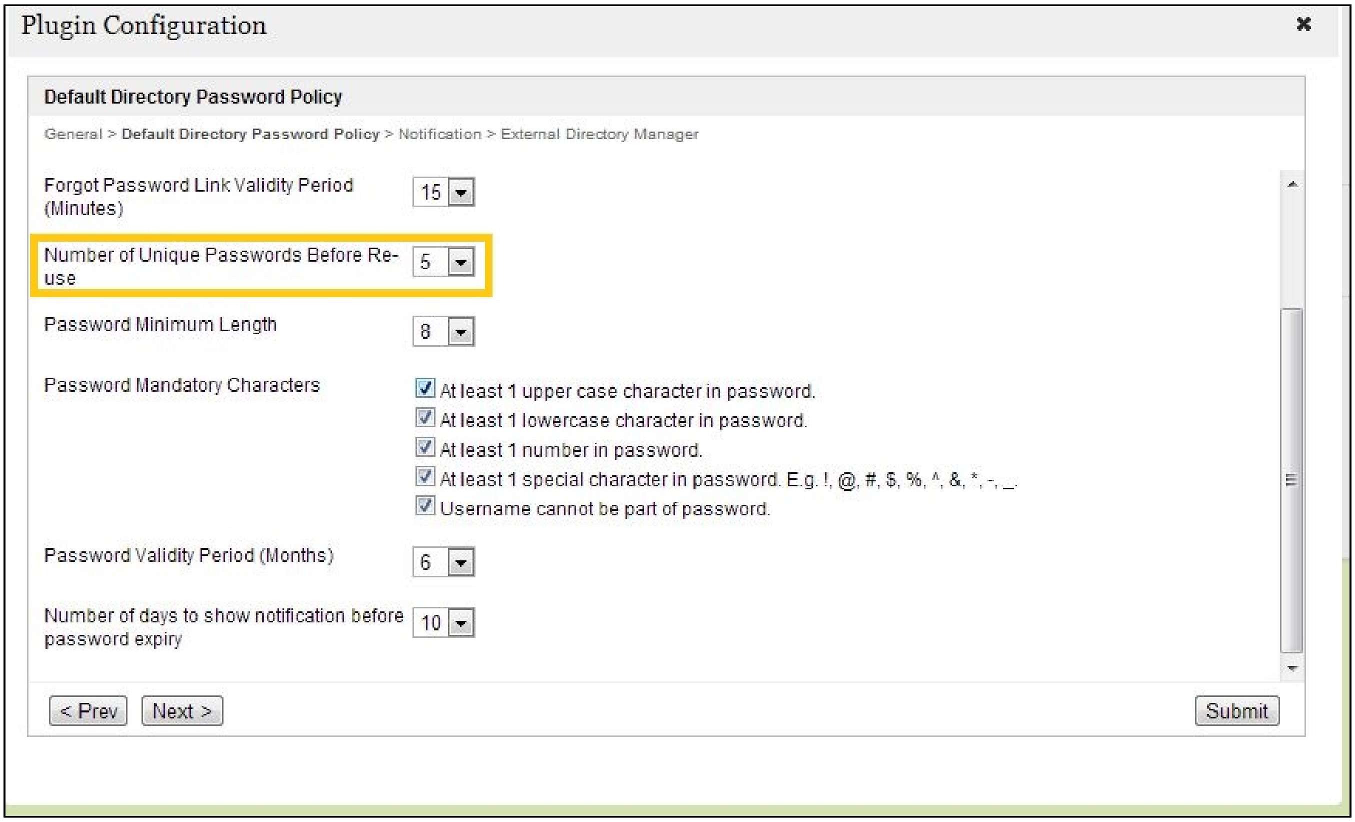
Failed Login Attempts for Account Lockout 3

Account Lockout Period (Minutes) 10

Allow Session Timeout (Inactivity Timeout) ☑

Hard Session Timeout (Hours) 8

The default is set to 5 for "Number of Unique Passwords Before Re-use". A select box allows an admin to select other options or remove this setting from the system.



Plugin Configuration

Default Directory Password Policy

General > **Default Directory Password Policy** > Notification > External Directory Manager

Forgot Password Link Validity Period (Minutes) 15

Number of Unique Passwords Before Re-use 5

Password Minimum Length 8

Password Mandatory Characters

☑ At least 1 upper case character in password.
☑ At least 1 lowercase character in password.
☑ At least 1 number in password.
☑ At least 1 special character in password. E.g. !, @, #, $, %, ^, &, *, -, _.
☑ Username cannot be part of password.

Password Validity Period (Months) 6

Number of days to show notification before password expiry 10