

# Password Creation

- [Configuring the password Rules](#)
- [Creating initial Password](#)
- [Managing Password changes](#)

## Configuring the password Rules

Joget allows you to define the password rules in the security plugin. These rules can be modified or set in the following location

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

Check the rules and minimum length of the password

**Plugin Configuration**

**Default Directory Password Policy**

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

Forgot Password Link Validity Period (Minutes)

Number of Unique Passwords Before Re-use

**Password Minimum Length**

**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)

Number of days to show notification before password expiry

Click on Submit to save the settings

## Creating initial Password

Create User allows administrators to create a password for a user or generate a random password. The randomness comes from a combination of pseudo-random numbers and alphabets. These numbers and alphabets are taken from the password policy rules set using the process described above

Checking the generate random password will allow the admin user to generate a random password for user and un checking the same would allow an admin to create a password for the user .

### Create New User ✕

Status Active ▼

---

**Employee Detail**

Employee Code

Job Title

Organization  ▼

Department  ▼

Grade  ▼

Start Date

End Date

---

**Admin Setting**

Generate Random Password

No Password Expiration

## Managing Password changes

In case a user forgets a password or if an admin wants to force a change in password, Joget allows you to do this

1. Admin can check "Reset Password" to send the new password to the user via Email.
2. Admin can also force user to change his password. Check "Force Password Change" to do that.
3. Admin also has an option to check "No password Expiration" in case he/she doesn't want their user's password to expire.

### Edit User

Status: Active

**Employee Detail**

Employee Code:

Job Title:

Organization:

Department:

Grade:

Start Date: 2013-10-24

End Date: 2013-10-22

**Admin Setting**

Force Password Change

Reset Password

No Password Expiration

Save Cancel

End Date: 2013-10-22

Forcing a password change would require a user to change his password in the next login. The image below shows the screen that appears in case of forced password change. The user will have to enter the older password and the new password to complete the enforcement.

### Change Password

**Login**

Username: vishu

Password:

**New Password**

New Password:

Confirm New Password:

Password length must be larger or equals to 8  
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.  
Cannot reuse previous 5 passwords.

Submit