Security Enhanced Directory Manager

Introduction

The **Security Enhanced Directory Manager** features enhanced security and control on user management.

Once you have configured SEDM you will gain access to these features :

- Password policy
- Account Timeout & Lockout
- Account Recovery via email
- End user have option to enable MFA, if SEDM configured to enable such MFA plugin

- SEDM acts as middle layer before talking to Directory Manager
    - Defaults to referring to Joget users
    - Can be configured to also communicate with LDAP / Sync LDAP / other DM (Directory Manager) plugins and many more.

Once SEDM is configured, stronger password encryption for local accounts will take over. (Security Enhanced Directory Manager uses the **SHA 256 encryption** to store the password._

Be careful when **disabling** SEDM plugin, as this will cause all local passwords to be invalid. See here for **Disabling Plugin**

Enabling Plugin

Simply go to **System Settings -> Directory Manager Settings** to enable and configure.

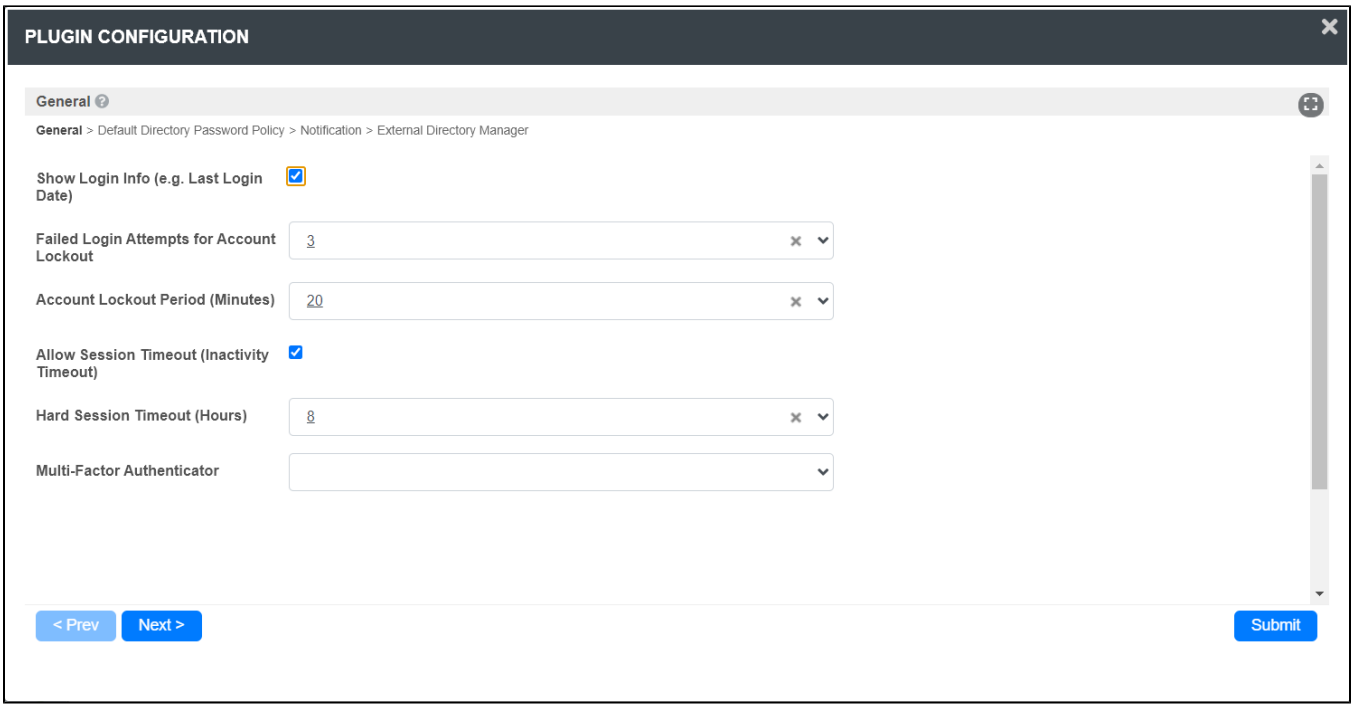

Figure 1: Security Enhanced Directory Manager Properties

Name	Description / Sample Value
Show Login Info	Enable this feature will display the info such as : Last Login Date
Failed Login Attempts for Account Lockout	Set on attempt limit for the user to input the correct password before being locked-out due to incorrect password.
Account Lockout Period (Minutes)	Set a period of time (Minutes) to disabling locked-out user from login.
Allow Session Timeout (Inactivity Timeout)	Enable this feature for automatically logging out inactive user and prompt the user to log in again.
Hard Session Timeout (Hours)	Set a period of time (Hours) for inactivity session for user to be locked out
Multi-Factor Authenticator	Default Multi-Factor Authenticator (MFA) that can be selected is : Time-based One-time Password (TOTP). You may opt to have more MFA by downloading the OTP (One-Time Password) Email MFA plugin

Disabling Plugin

Disabling Plugin

Once the plugin is enabled, users' password would be stored using a new encryption method. Disabling the plugin would cause all the users not to be able to login anymore as the default encryption method is effectively changed.

Security Enhanced Directory Manager uses the **SHA 256 encryption** to store the password.

For example, the old standard encrypted hash for "User@123" is "448ddd517d3abb70045aea6929f02367" using MD5.
When you change the Joget directory manager to use SEDM, the new password becomes something like "@@@@whateverhashencryption@@@@".

If you then later remove/disable the SEDM plugin, the **password is unchanged at SHA 256 encryption**. Because the SEDM is not in play anymore, Joget is unable to authenticate the username because it is expecting the password to be the old MD5 encryption.

Do note that passwords once changed to the new SHA 256 Encryption cannot be changed back to MD5.

If you decide you don't want to use SEDM and then delete the plugin setting, **you will need to use your database backups to restore the table "dir_user" to revert back to the original passwords (using MD5 and before SEDM was implemented).**

You can also run the following query to update the "dir_user" table back to the old password - An example of the SQL query is as follows:

```
UPDATE dir_user SET password = '5f4dcc3b5aa765d61d8327deb882cf99' WHERE id = 'username'
```

The "5f4dcc3b5aa765d61d8327deb882cf99" value is the word "password" using the old encryption.

Troubleshoot

Should you forgotten all the details during any Security Enhanced Directory Manager configuration and you have **Locked yourself out,** please use this workaround :

To disable your Security Enhanced Directory Manager (SEDM) , get into the database

1) Remove the password column value in **dir_user**

- Replace the password column value with new value based on md5 hash.

2) In **wf_setup** >delete any directory manager records

- Remove the 2 rows that starts with "directoryManager".

Then, Joget Workflow will fallback to default directory manager again.

Notification

If you leave the Notification tab below empty, Joget will read the default SMTP configuration values from the General Settings > SMTP Settings page.

Important

Setting up the **Notification** tab in this Enhanced Security Directory Manager is **important and highly recommended**. Do not skip the setup and remember to test sending email out to make sure that the email server settings is correct.

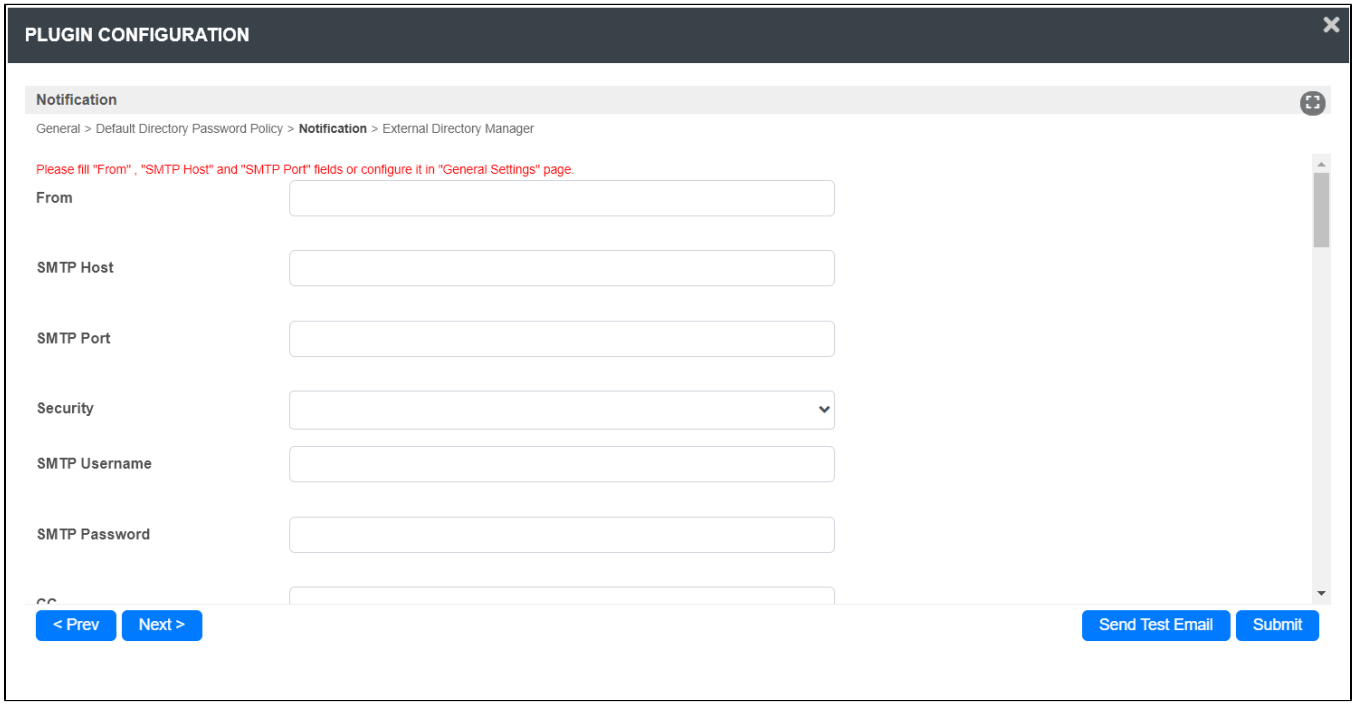

Figure 2: Notification tab

Name	Description
From	Sender email address. **Example** no-reply@your-company-name.com
SMTP Host	Email Server SMTP Host **Example** smtp.gmail.com
SMTP Port	Email Server SMTP Port Typically, port **465** for **SSL** security option and **587** for **TLS**
Security	• None • TLS • SSL Alternatively, you can click on the "hash" symbol to allow the input of hash variables.

SMTP Username	Email Server Account Username On Google email account, use your full email address.
SMTP Password	Email Server Account Password Password submitted will be encrypted for security reason.
CC	Fully qualified address is expected. Multiple values can be accepted by separating them with semicolons. **CC**: lets you send a copy of a message to someone who's interested, but is not the primary recipient.
HTML Content?	Check if "Message" is intended to be a HTML content.
User Creation (Subject)	Email Subject.
User Creation (Message)	Email Message.

Quick Test

Hit on the "Send Test Email" button to quickly validate and test the email settings.

Email notification will be sent out on these important events:

- User Creation: email is sent when the admin creates a new user in "Setup User".
- Password Reset: email is sent when the admin resets the user's password by checking the "Force Password Change" checkbox in "Setup Users > Edit User > Admin Setting".
- Forgot Password: email is sent when the user clicks the forget password link on the login page.
- Account Lockout: email is sent when the wrong password exceeds the limit set in "Failed Login Attempts for Account Lockout".

Related Documentation

General Settings

Time-based One-time Password (TOTP)

OTP (One-Time Password) Email MFA