OTP (One-Time Password) Email MFA

Introduction

Definition

OTP Email MFA is a Multi-factor authentication plugin that sends a one-time password to a user's email providing an additional layer of security.

Multi-Factor Authentication (MFA) is a security best practice that adds an extra layer of protection on top of a username and password combination. By requiring an additional authentication code from a trusted device, MFA safeguards access to a user’s account even if the password is compromised.

Plugin Information

Plugins Available in the Bundle:

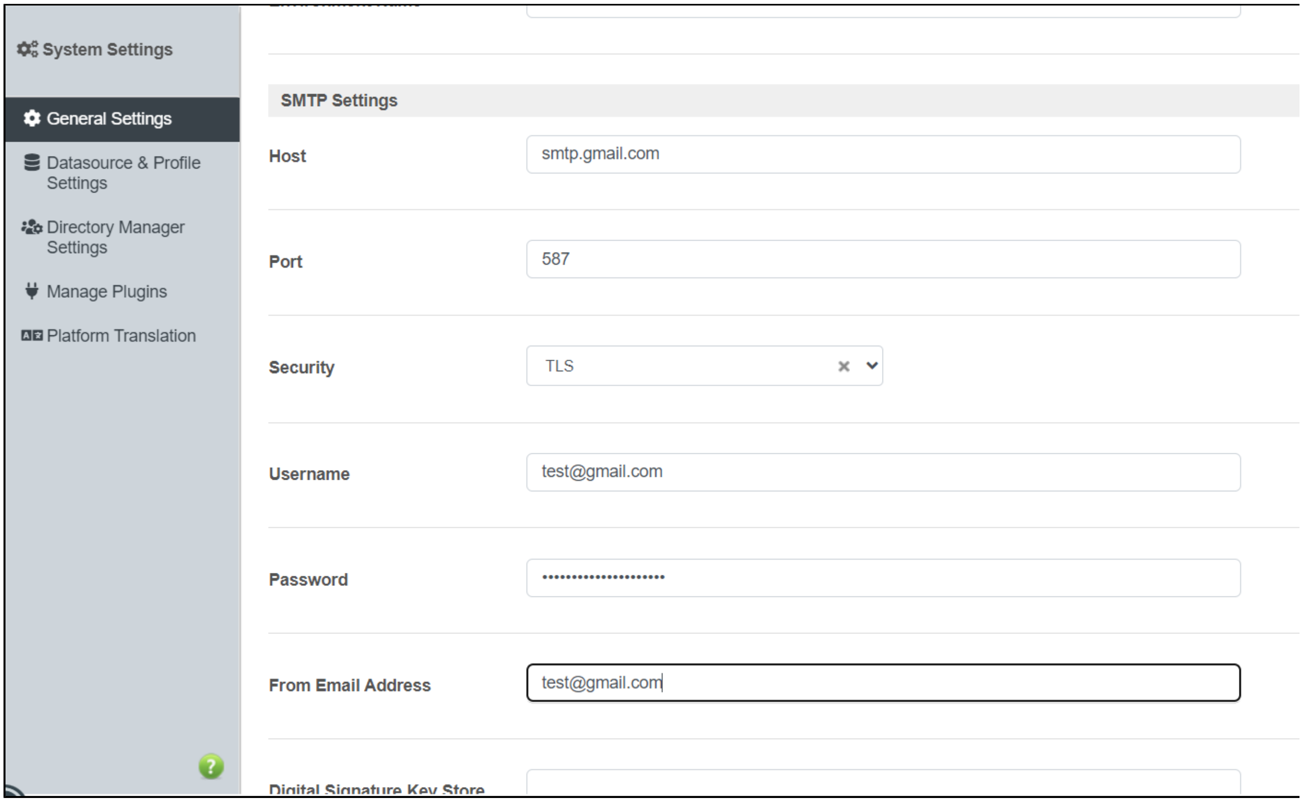
1. OTP Email MFA

This plugin bundle is compatible with Joget DX 8 and Joget DX 7

Get Started

Prerequisites

1. Set up SMTP values in the Joget App for the email tool to be working properly.



SMTP Settings

Host: smtp.gmail.com

Port: 587

Security: TLS

Username: test@gmail.com

Password: ••••••••••••••••••••••

From Email Address: test@gmail.com

Digital Signature Key Store

Figure 1: SMTP Settings

For more details, please refer to **General Settings > SMTP Settings.**

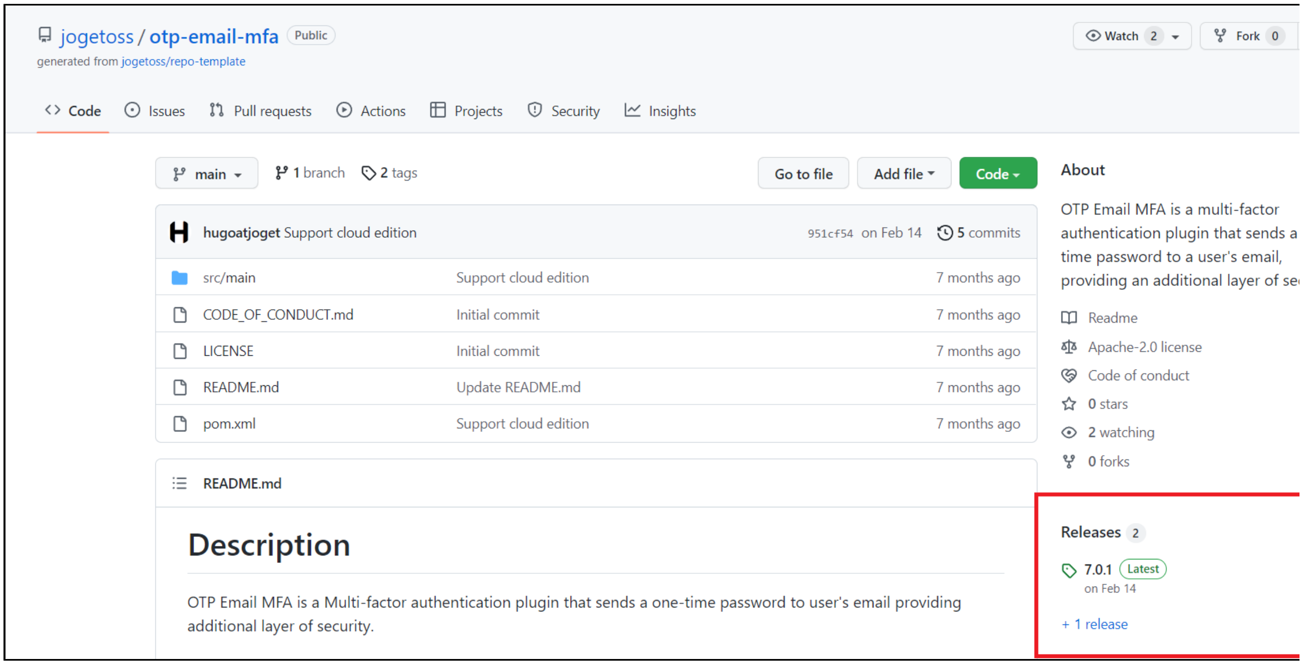
SMTP settings in **General settings** will enable Joget DX to use these SMTP values as **global default values** for all your apps.

Joget apps will ignore this global SMTP settings if the respective apps already have the settings configured, either in the Plugin Default Properties or Email Tool - Configure SMTP Settings page.

Steps to Import this Plugin

1. Go to the website https://github.com/jogetoss/otp-email-mfa.

2. Go to the "**Releases**" page (See Figure 2).



hugoatjoget Support cloud edition 951cf54 on Feb 14 5 commits

src/main	Support cloud edition	7 months ago
CODE_OF_CONDUCT.md	Initial commit	7 months ago
LICENSE	Initial commit	7 months ago
README.md	Update README.md	7 months ago
pom.xml	Support cloud edition	7 months ago

README.md

Description

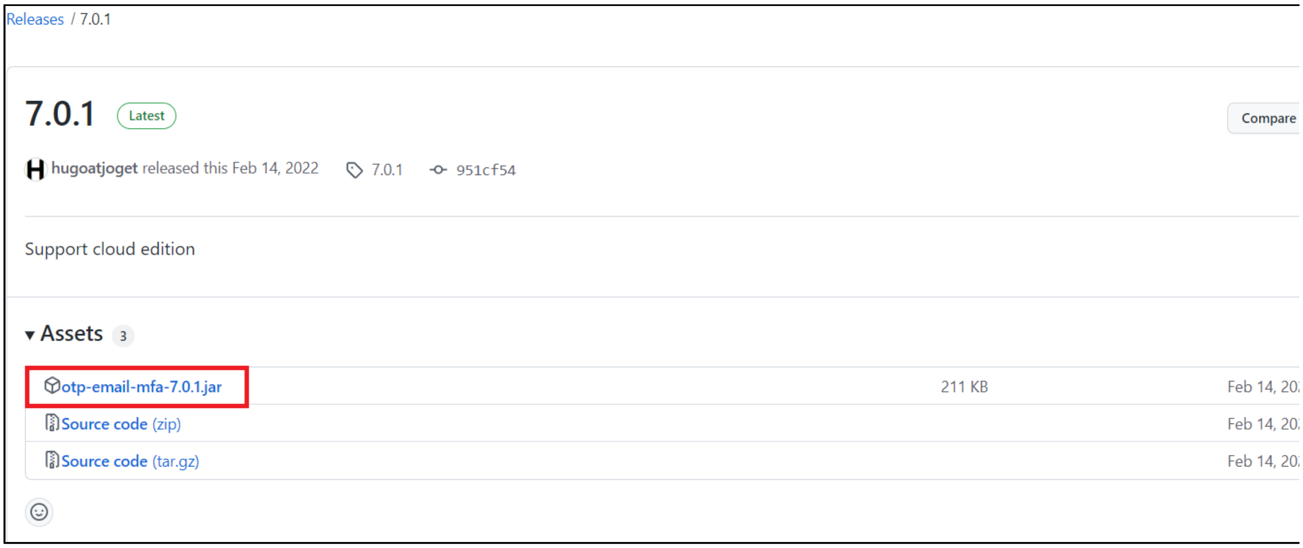
OTP Email MFA is a Multi-factor authentication plugin that sends a one-time password to user's email providing additional layer of security.

About

OTP Email MFA is a multi-factor authentication plugin that sends a time password to a user's email, providing an additional layer of se

Figure 2:Plugin Releases

3. Click on the **.jar** file to initiate the download (See Figure 3).



hugoatjoget released this Feb 14, 2022 7.0.1 951cf54

Support cloud edition

otp-email-mfa-7.0.1.jar	211 KB	Feb 14, 20
Source code (zip)		Feb 14, 20
Source code (tar.gz)		Feb 14, 20

Figure 3: Download .jar file

4. Go to your Joget Workflow localhost or server and log in as **admin.**

5. In Joget Console navigate to "**Admin Bar > Systems Settings > Manage Plugins**" and click the "**Upload Plugins**" button.

6. In "Upload Plugin", select the **plugin .jar** file you just downloaded, then click "**Upload**".

7. You should be able to view the newly installed plugin under the "**Installed Plugins**" tab.

8. Remember to always uninstall the old plugin before uploading a new version.

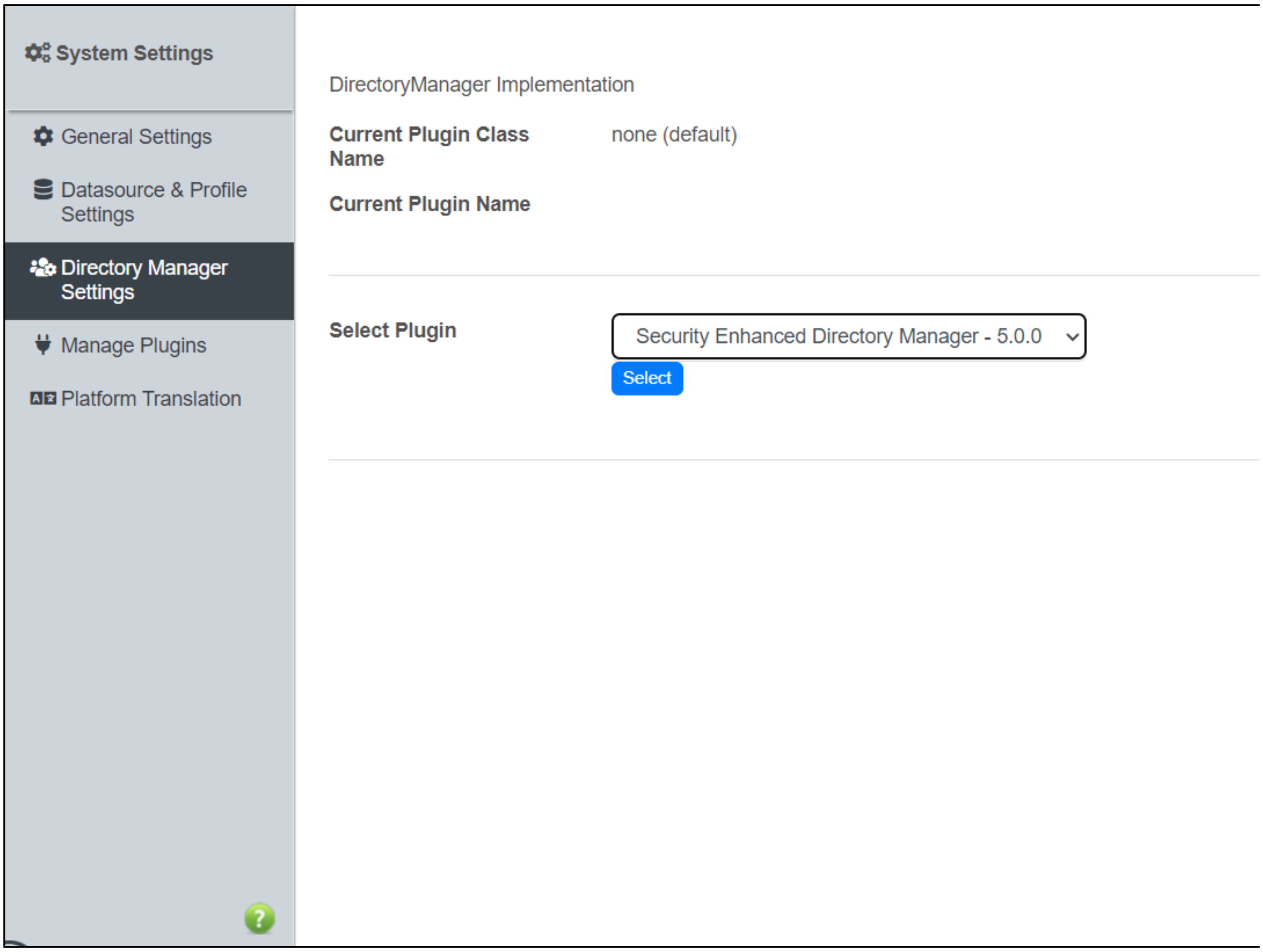
9. The Joget Workflow Knowledge Base has more information on managing and developing plugins.

Steps to Use this Plugin

Steps for Administrators

1. Start the Joget server and open the **App Center**.

2. Log in as admin, click on Settings in the admin bar, and navigate to **Directory Manager Settings.** (See Figure 4)



DirectoryManager Implementation

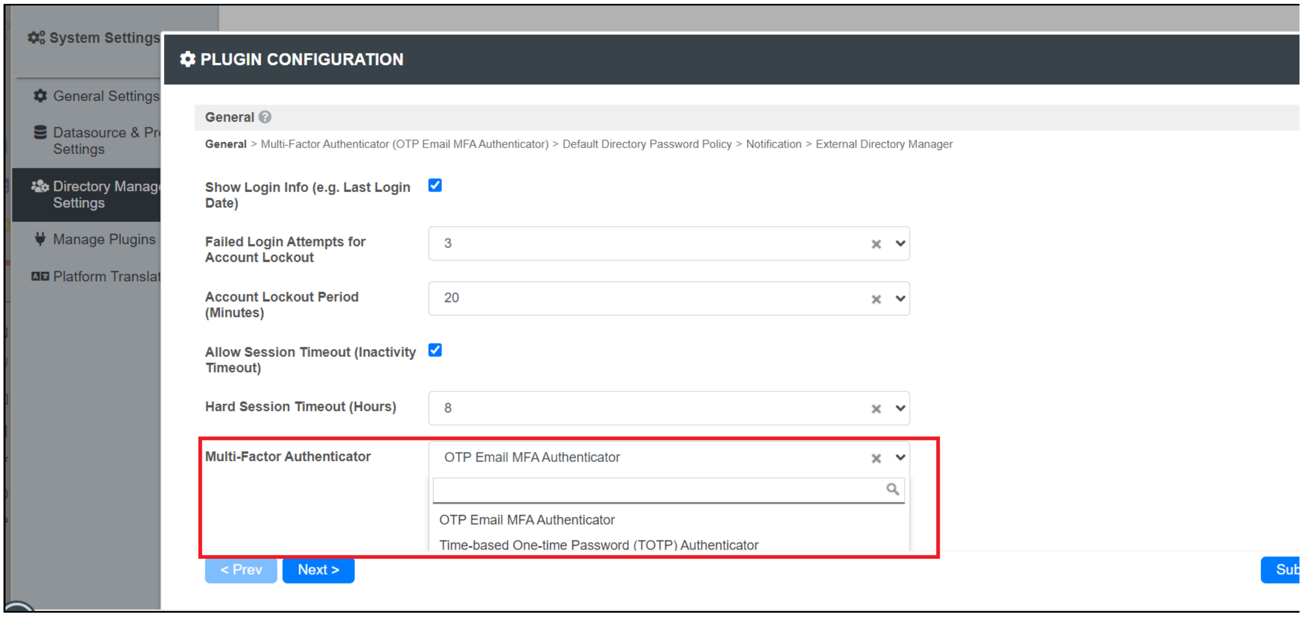
Current Plugin Class Name none (default)

Current Plugin Name

Select Plugin Security Enhanced Directory Manager - 5.0.0

Figure 4 :Directory Manager Settings

3. Choose the Security Enhanced Directory Manager in the **Select Plugin** field and select **OTP Email MFA Authenticator** for the **Multi-Factor Authenticator** property. (See Figure 5)



PLUGIN CONFIGURATION

General

General > Multi-Factor Authenticator (OTP Email MFA Authenticator) > 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): 20

Allow Session Timeout (Inactivity Timeout) ☑

Hard Session Timeout (Hours): 8

Multi-Factor Authenticator: OTP Email MFA Authenticator

OTP Email MFA Authenticator
Time-based One-time Password (TOTP) Authenticator

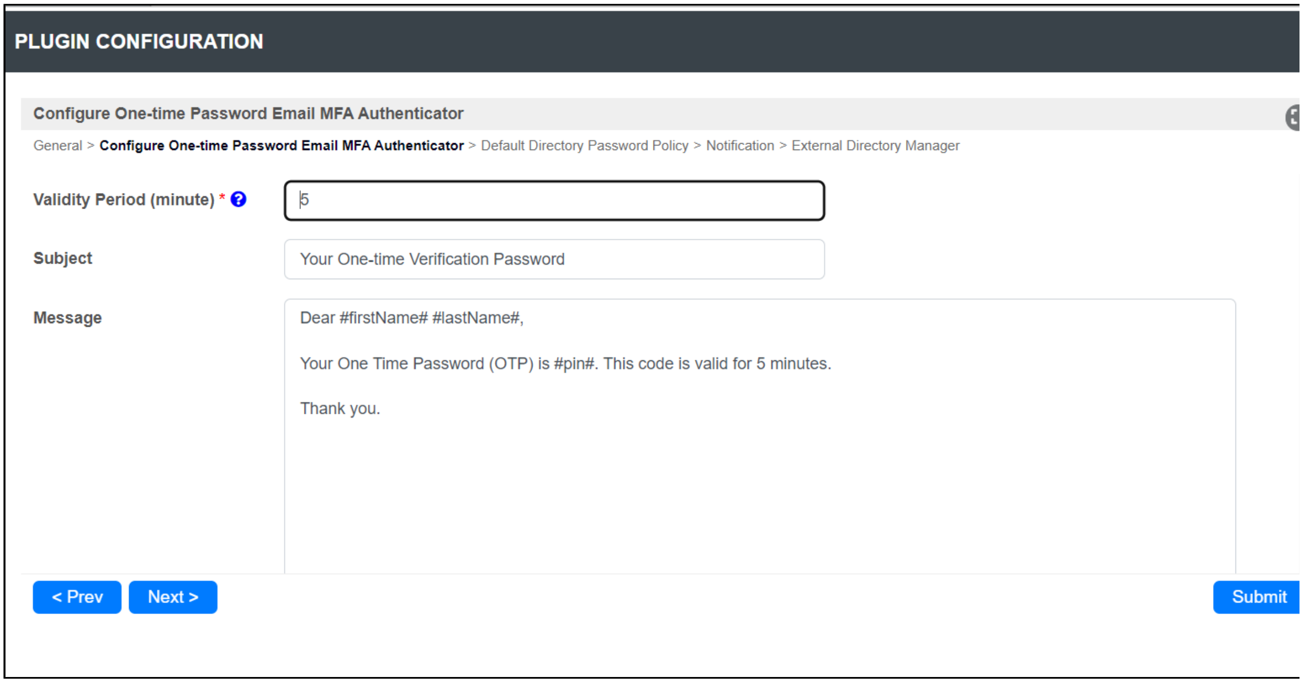
< Prev Next > Sub

Figure 5 : Multi Factor Authenticator

One-Time Password OTP Email MFA Authenticator Properties

Configure One-time Password OTP Email MFA Authenticator

1. This configuration will determine the properties of your **OTP Email MFA Authenticator** and the outcome of your plugin.
In **General > Configure One-time Password Email MFA Authenticator**



PLUGIN CONFIGURATION

Configure One-time Password Email MFA Authenticator

General > **Configure One-time Password Email MFA Authenticator** > Default Directory Password Policy > Notification > External Directory Manager

Validity Period (minute) *: 5

Subject: Your One-time Verification Password

Message:

Dear #firstName# #lastName#,

Your One Time Password (OTP) is #pin#. This code is valid for 5 minutes.

Thank you.

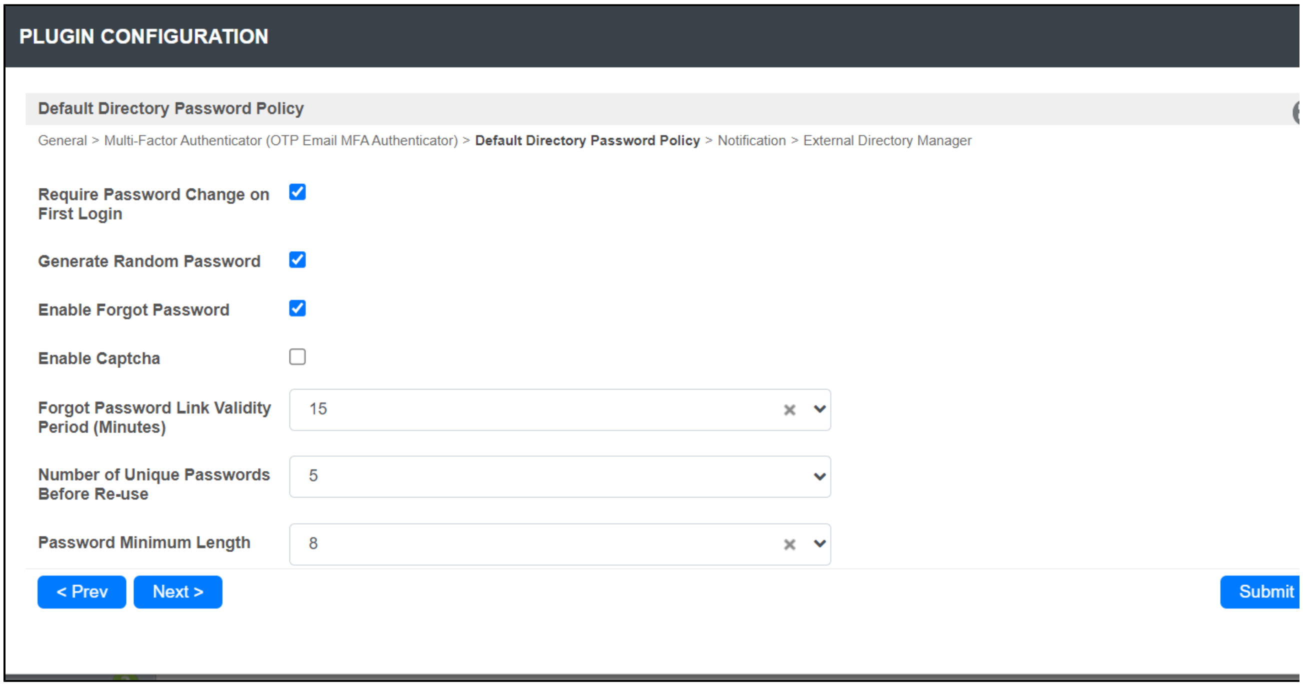
< Prev Next > Submit

Figure 6: Configure OTP Password Email MFA Authenticator

Name	Description

Validity Period (minute)	The expiration time for the One Time Password (OTP) sent to the user's email registered in the profile remains valid in minutes. The default value is 5 minutes.
Subject	The subject of the email with the OTP.
Message	The message is to be displayed in the email.

2. Then, in **General > Configure One-time Password Email MFA Authenticator>Default Directory Password Policy**



PLUGIN CONFIGURATION

Default Directory Password Policy

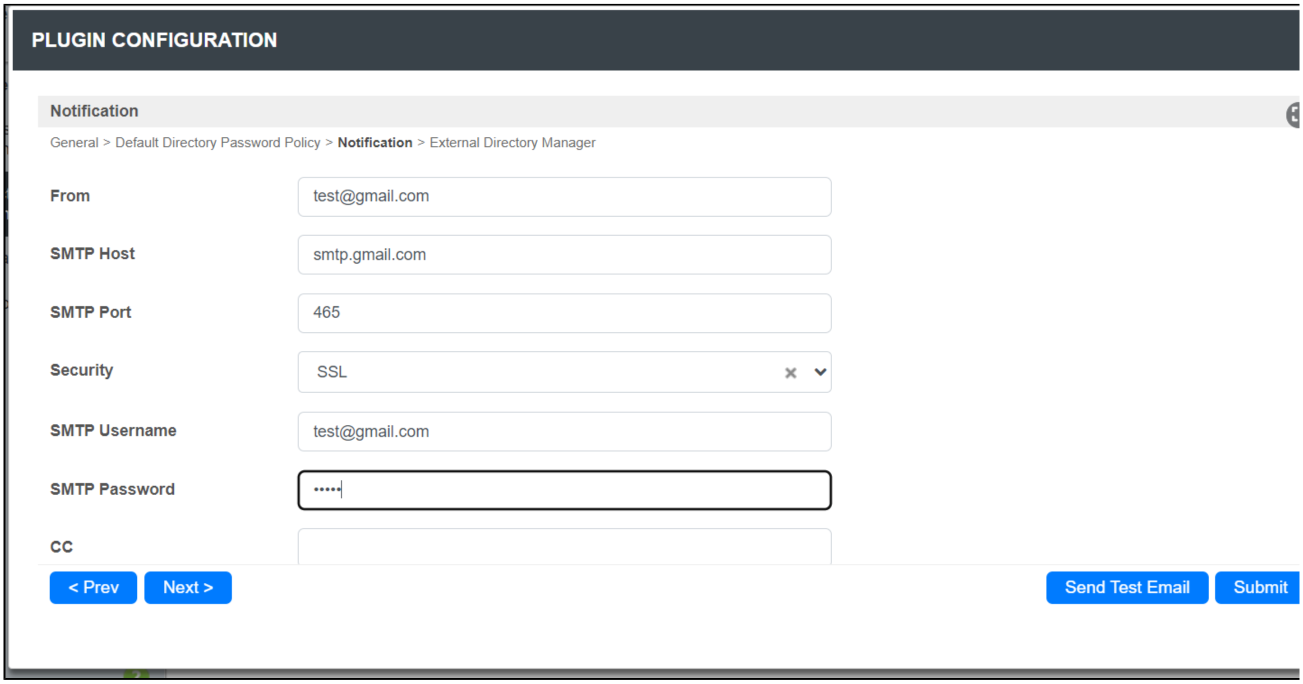
General > Multi-Factor Authenticator (OTP Email MFA Authenticator) > **Default Directory Password Policy** > Notification > External Directory Manager

Require Password Change on First Login	☑
Generate Random Password	☑
Enable Forgot Password	☑
Enable Captcha	☐
Forgot Password Link Validity Period (Minutes)	15
Number of Unique Passwords Before Re-use	5
Password Minimum Length	8

Figure 7 : Default Directory Password Policy

3.In **General > Configure One-time Password Email MFA Authenticator>Default Directory Password Policy>Notification**

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



PLUGIN CONFIGURATION

Notification

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

From	test@gmail.com
SMTP Host	smtp.gmail.com
SMTP Port	465
Security	SSL
SMTP Username	test@gmail.com
SMTP Password	•••••
CC	

Figure 8 : Notification

Important

If you set the values in this Notification tab, this settings will **ignore** the values that you have set from the SMTP Settings > General Settings and send notification based on the configured values here.

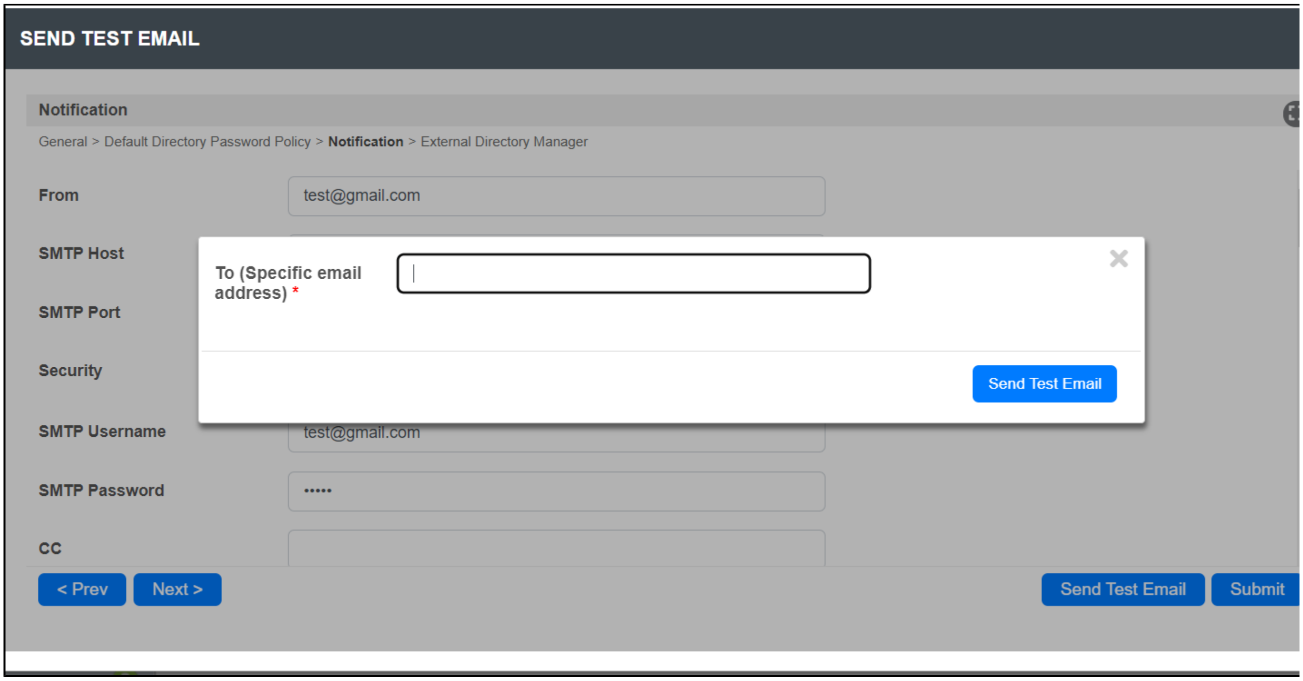
Name	Description
From	Sender email address. **Example** no-reply@your-company-name.com
SMTP Host	Email Server SMTP Host **Example** smtp.gmail.com
SMTP Port	Email Server SMTP Port Typically, port **465** for **SSL** security option and **587** for **TLS**
Security	• None • TLS • SSL Alternatively, you 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.

6. Before submitting the **OTP Email MFA Authenticator,** you may click on **Send Test Email** to verify your Email configuration (See Figure 9)



SEND TEST EMAIL

Notification

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

From: test@gmail.com

SMTP Username: test@gmail.com

SMTP Password: •••••

To (Specific email address) *

Figure 9: Send Test Email

7. Once all configurations have been inspected and tested, you may **submit** the **OTP Email MFA Authenticator to Enable it.** Once enabled, users will be able to enable MFA **individually** in their **User profile.**

8. **Optionally**, you may also activate **all users** to use **OTP Email MFA Authenticator** by **default** by adding their username as entries into the dir_user_meta table.

Here's an SQL query where you can do so :

```
insert into dir_user_meta (username, meta_key, meta_value)
    select username,'OTP_EMAIL','enabled'
    from dir_user t1
    where not exists(
        select id
        from dir_user_meta t2
        where t2.username = t1.id
    );
```

9. This query will add all the existing users in the dir_user table into the **dir_user_meta** table with the following values :

username : <username>

meta_key : OTP_EMAIL

meta_value : enabled

The "where not exist" clause is to check and skip for existing users already having otp enabled.

Joget authentication will automatically check if the user exists in this table and prompt them with the "please enter OTP" message.

Steps for Users

1. Users can activate **OTP Email MFA Authenticator** in their respective user profiles by clicking the "**Activate**" button. (See Figure 10)

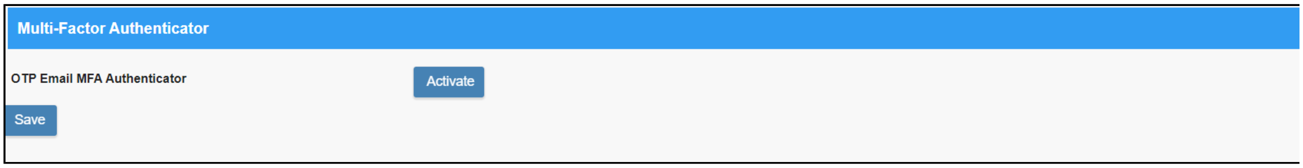
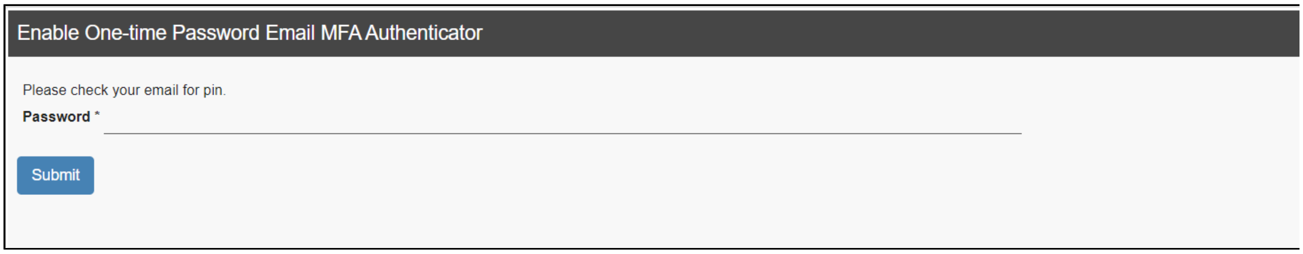


Figure 10: Activate button

2. Before activating **OTP Email MFA Authenticator,** users should make sure that a valid and working email has been registered in their profile under the **User Details** section as the email containing the **OTP** will be sent to this registered email.

3. A popup dialog will appear showing a **Password** field to submit the email OTP sent to the user. If the code is valid, **OTP Email MFA** will be activated (See Figure 11).


Enable One-time Password Email MFA Authenticator

Please check your email for pin.

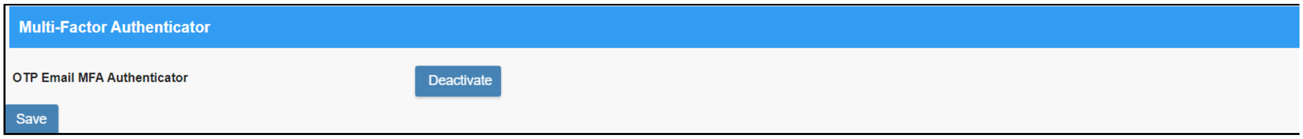
Figure 11: Password field to submit the email OTP sent to the user

4. The users should always remember to save their user profile after activating MFA.

5. On subsequent logins, the users will be prompted for an OTP password which will always be sent to the user's email.

Deactivating Multi-Factor Authentication

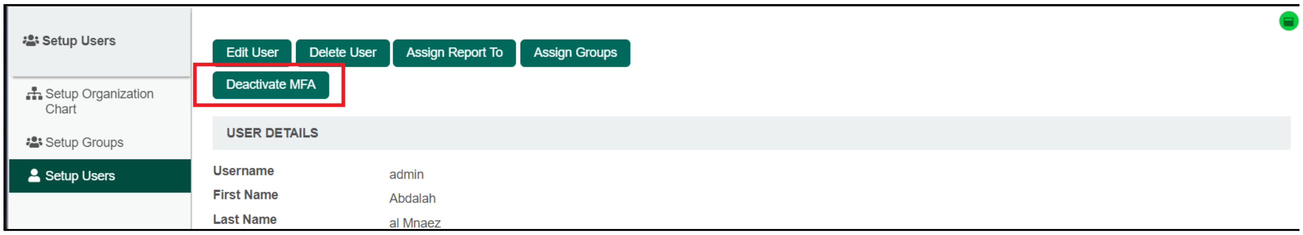
1. As a user, you can disable **OTP Email MFA Authenticator** by clicking on the **Deactivate** button in your user profile. (See Figure 12)



OTP Email MFA Authenticator

Figure 12: Deactivate

2. Administrators can also disable MFA for a specific user by selecting the Setup Users under **Users** in the admin bar and clicking on the **Deactivate MFA** button. (See Figure 13)



USER DETAILS

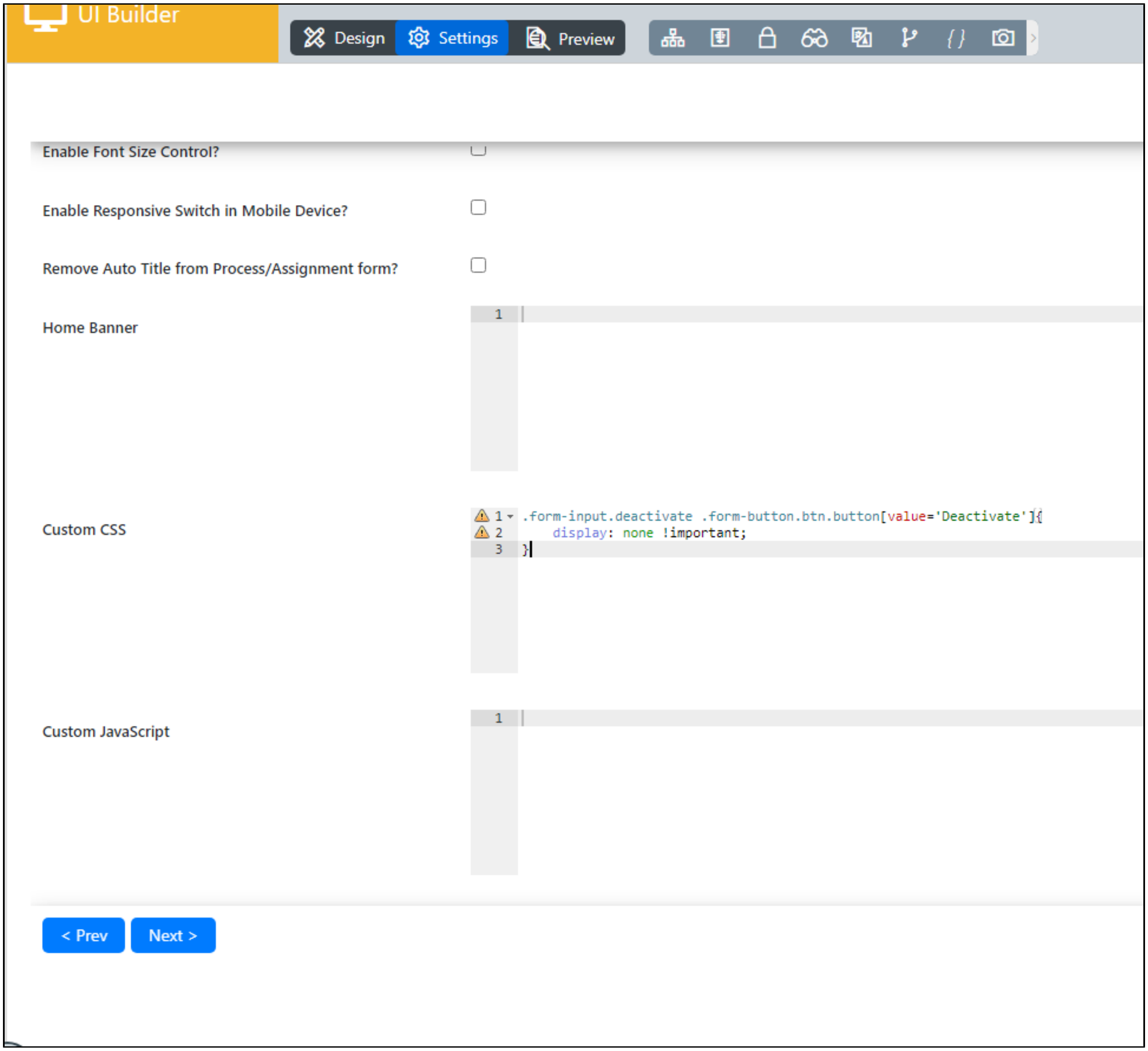
Username	admin
First Name	Abdalah
Last Name	al Mnaez

Figure 13 :Deactivate MFA button

Disable the Deactivate MFA button for all users in their profile section

1. Administrator can hide/(disable) the **Deactivate MFA** button from all users profile section to prevent users from individually disabling the MFA.
2. To achieve this, you can add this css to the application UI that you want to hide the button from at **UI Builder > Settings > Configure [theme name] > Custom CSS**

```
.form-input.deactivate .form-button.btn.button[value='Deactivate']{
  display: none !important;
}
```



Enable Font Size Control? □

Enable Responsive Switch in Mobile Device? □

Remove Auto Title from Process/Assignment form? □

Home Banner

Custom CSS

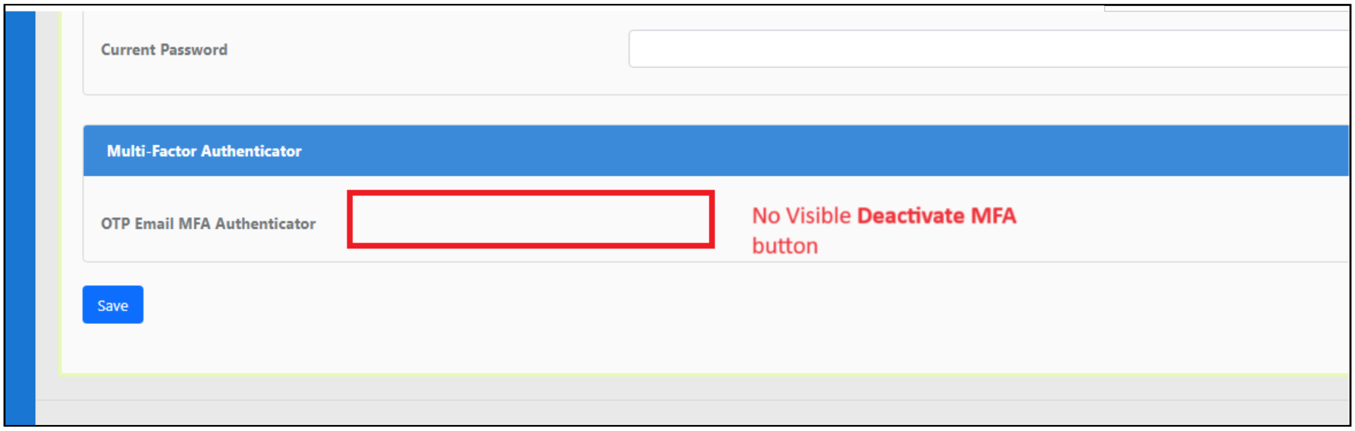
```
.form-input.deactivate .form-button.btn.button[value='Deactivate']{
    display: none !important;
}
```

Custom JavaScript

Figure 13 : Apply Custom CSS in UI Builder > Settings > Configure [theme name] > Custom CSS

3.Expected outcome on the implementation of the CSS code:

The **Deactivate MFA** button is hidden/disabled for the user to access nor view it.



No Visible **Deactivate MFA** button

Figure 14 : Expected outcome > Deactivate MFA button is not visible

Related Documentation

General Settings

Security Enhanced Directory Manager