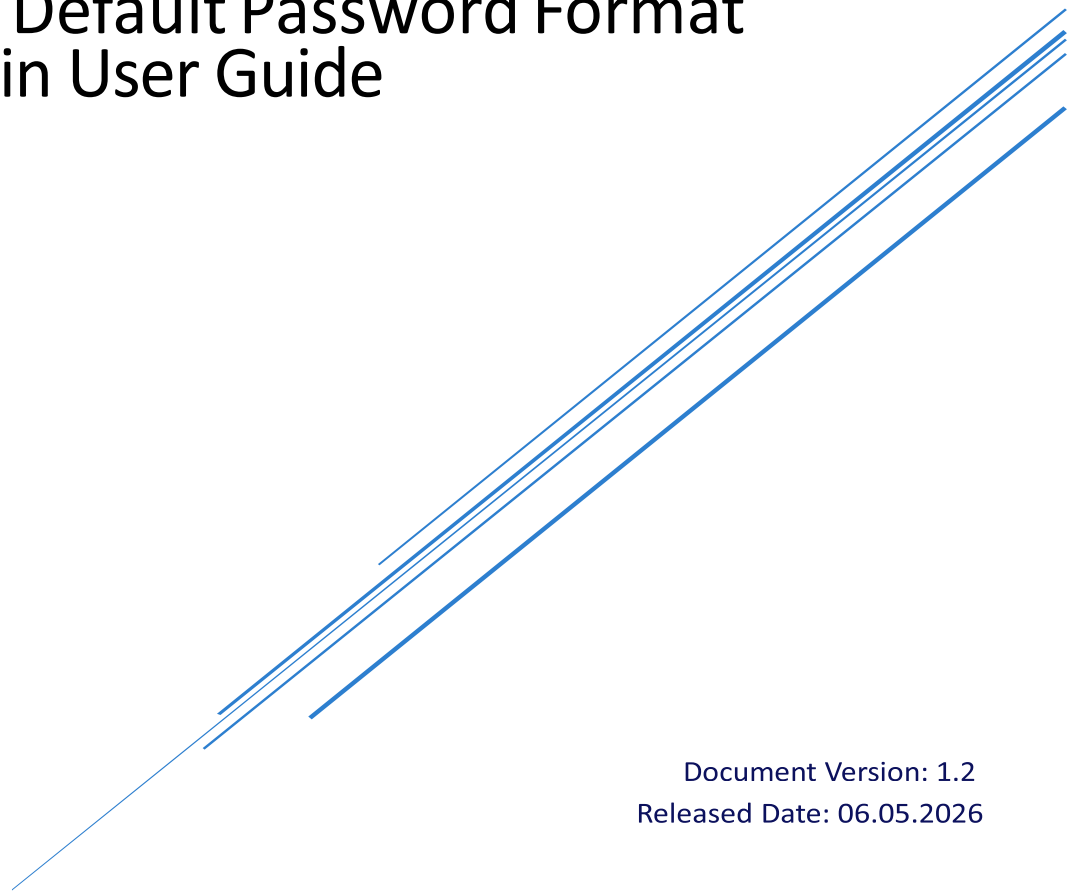
TIMES SOFTWARE

New Default Password Format Admin User Guide



Document Version: 1.2
Released Date: 06.05.2026

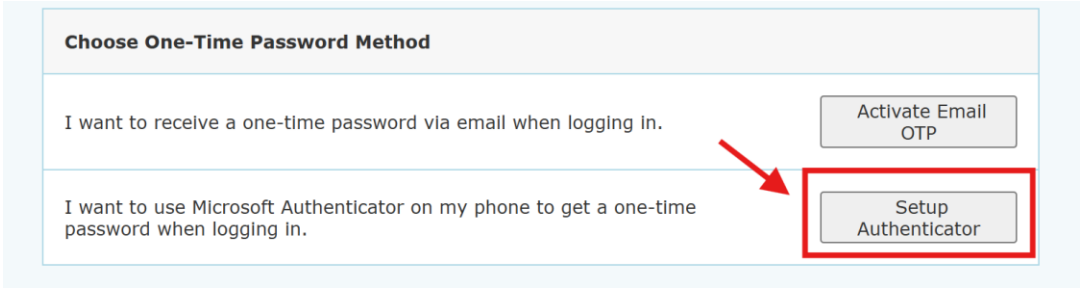
TIMES SOFTWARE

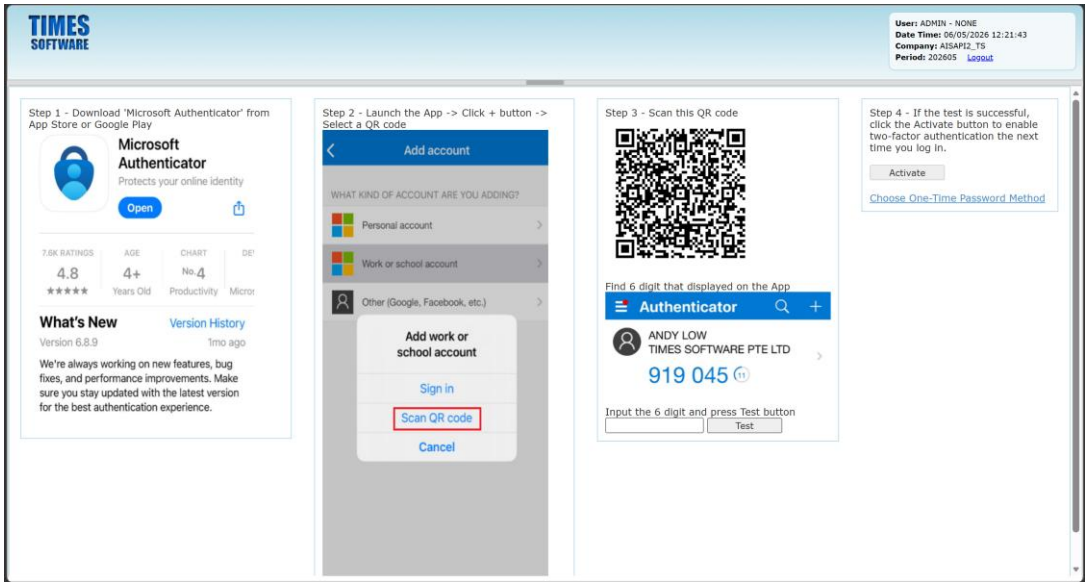
TABLE OF CONTENTS

1) MFA Setup for Admin

1.1) MFA – Microsoft Authenticator

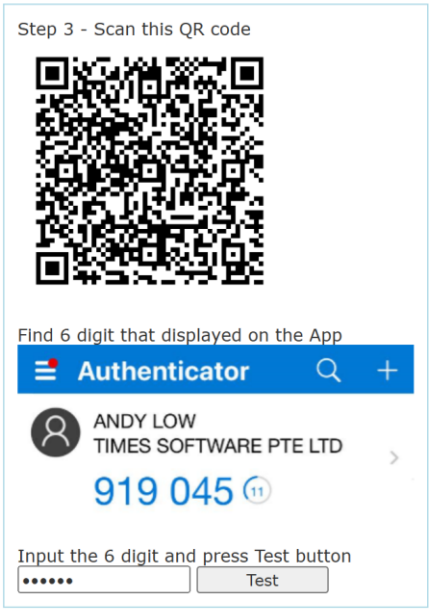
1. Upon logging in to the portal, the user will be prompted to choose an OTP method, select “Setup Authenticator”

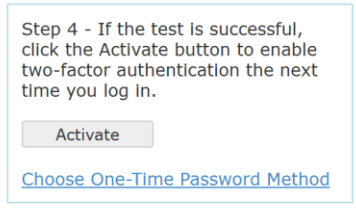


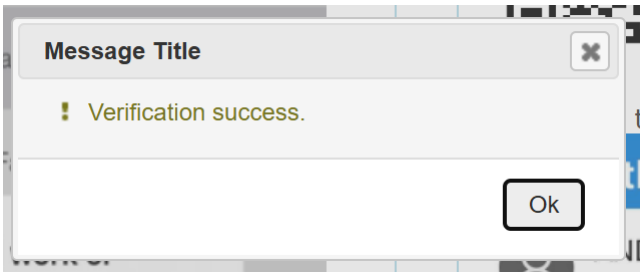


Follow the steps provided (Step 1 -> 4) to download Microsoft authenticator on the user’s mobile device. Then refer to ‘Step 3 – Scan QR Code’ to setup the authenticator.

2. The Microsoft Authenticator will display a 6-digit code. Please enter the code in the field above, then click the 'Test' button to continue.
3. Upon successful setup, the system will prompt 'Verification success'.



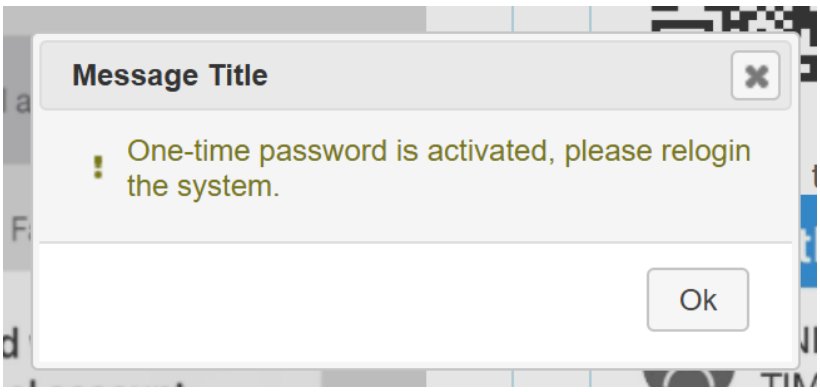




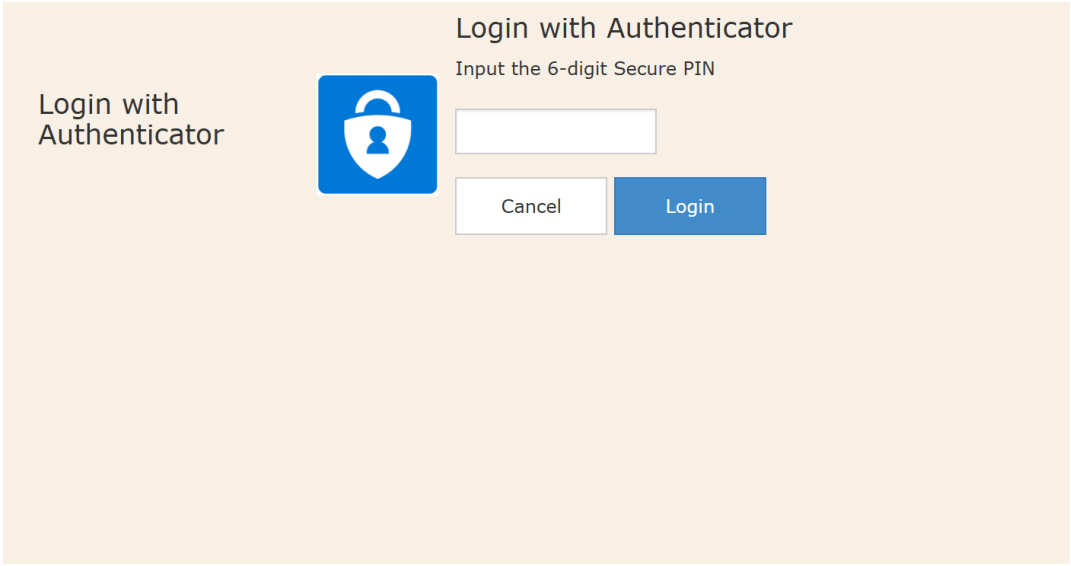
4. Click the [Activate] button to enable two-factor authentication.

**** The activate button will only be enabled after Step 3 has been successfully verified.**

5. After successfully activating the Microsoft Authenticator, the system will display the following message and then automatically log out:

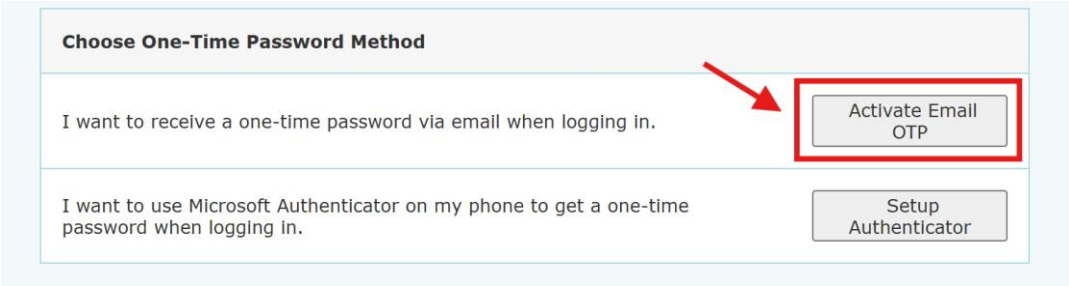


6. Upon successfully re-logging into the system, the user will be prompted to enter the 6-digit code generated by Microsoft Authenticator:

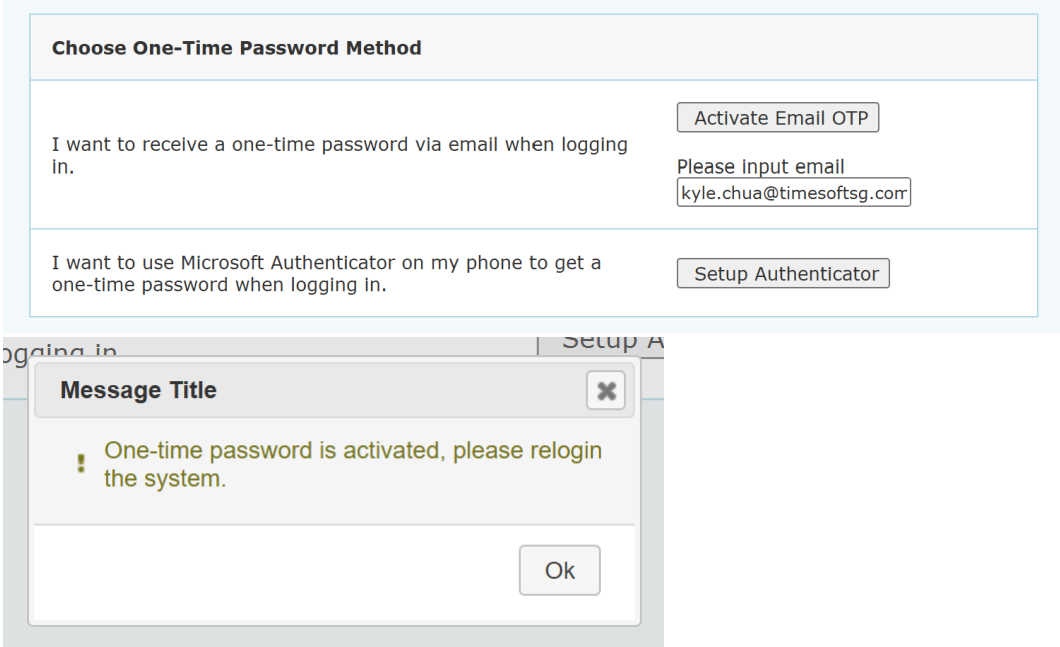


1.2) MFA - Email

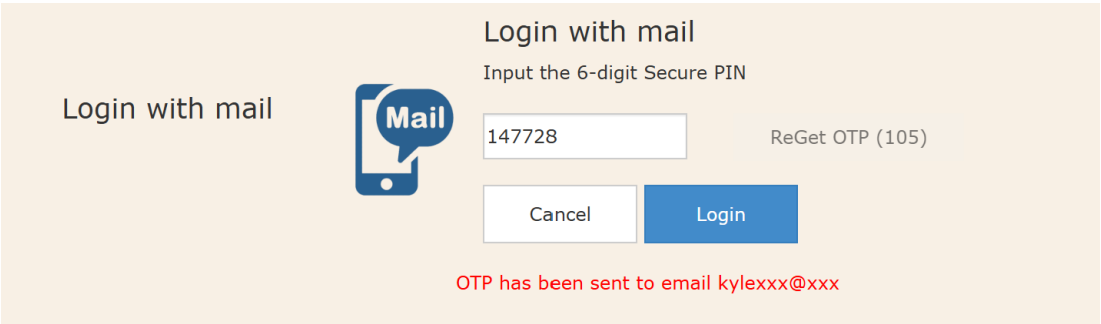
1. Upon logging in, the system will prompt the user to choose an OTP method. Select “Activated Email OTP”



2. The user will be prompted by the system to enter the admin’s email

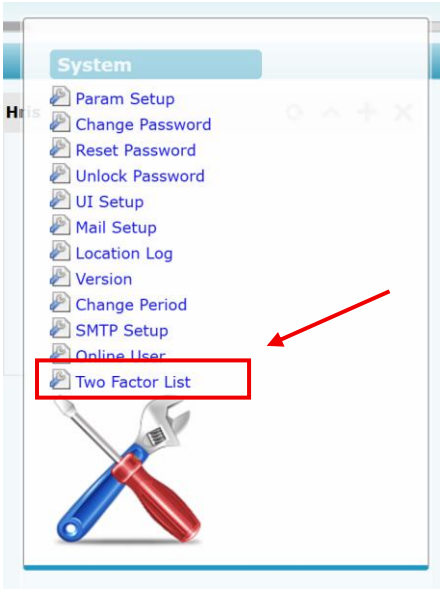


3. Upon success re-login to the system, OTP will be triggered to admin’s email address. The user then enters the OTP and clicks [Login].

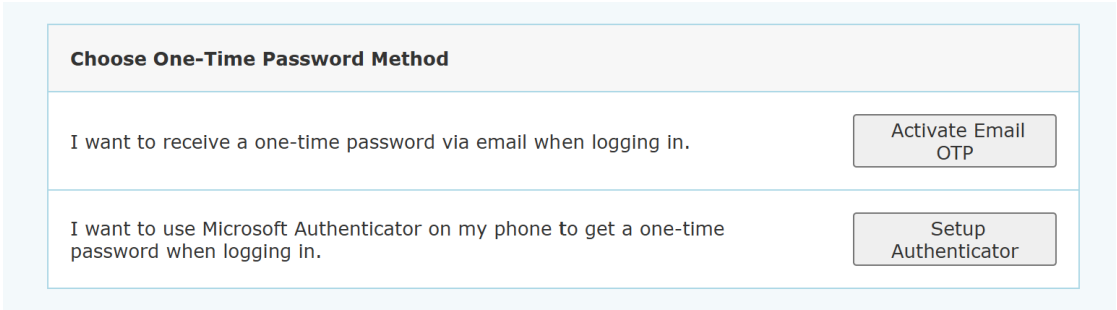


1.3) Change MFA Method

To change the MFA (Multi-Factor Authentication) method, select 'Two Factor List':

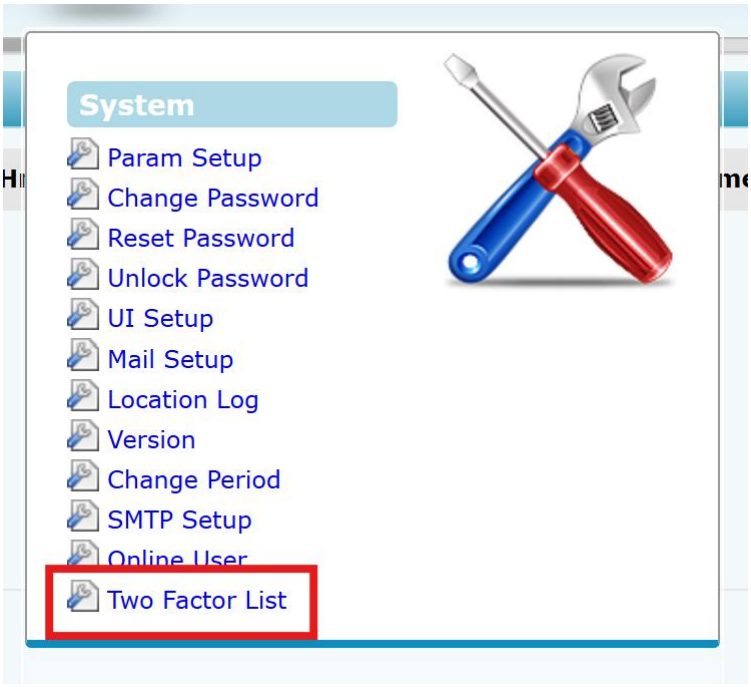


The user will be redirected to the One-Time Password method selection page. Refer to the previous section for the steps to activate Email OTP.



1.4) Admin access to reset MFA Authentication

If an employee is unable to access the MS Authenticator, or if the employee misplaces their mobile phone, the admin will need to reset the MS Authenticator for them.

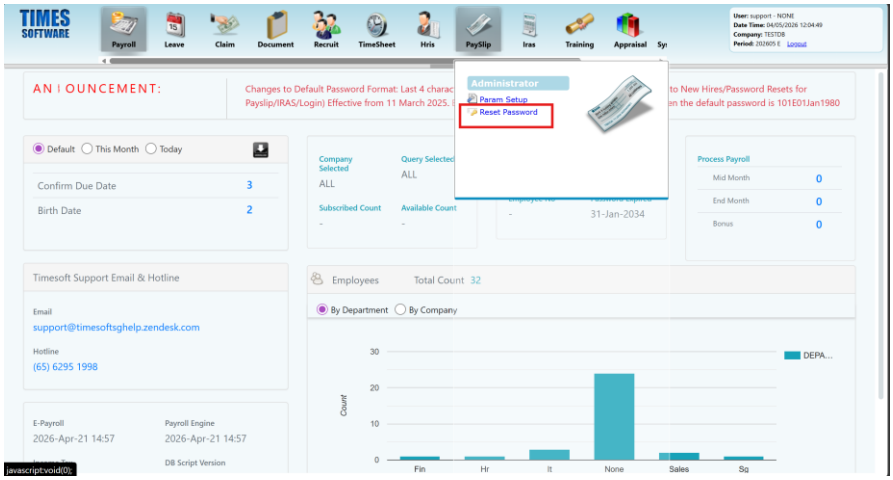


Click on the icon to delete the selected employee's Multi-Factor Authentication(MFA) method. After clicking the icon, the selected employee will be required to choose their MFA method when they login.

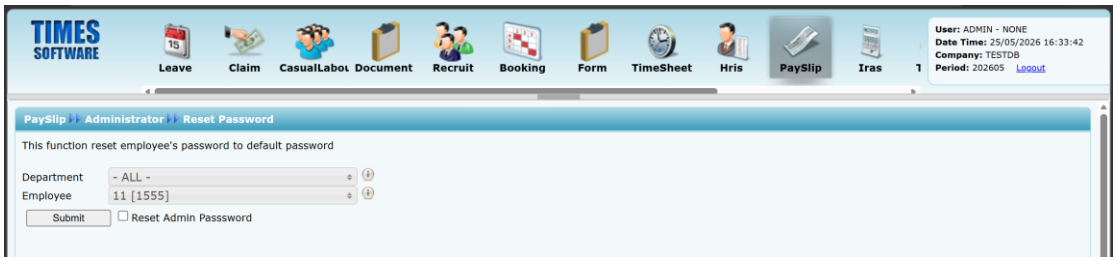
2) E-Password

2.1) Reset Payslip Password (E-Password) (Payslip Module)

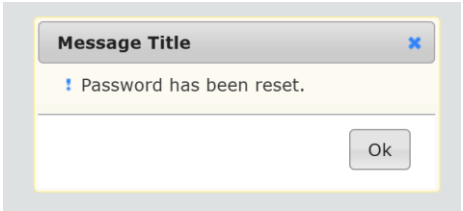
Admin can reset the employee E-Password via the menu at the payslip module.

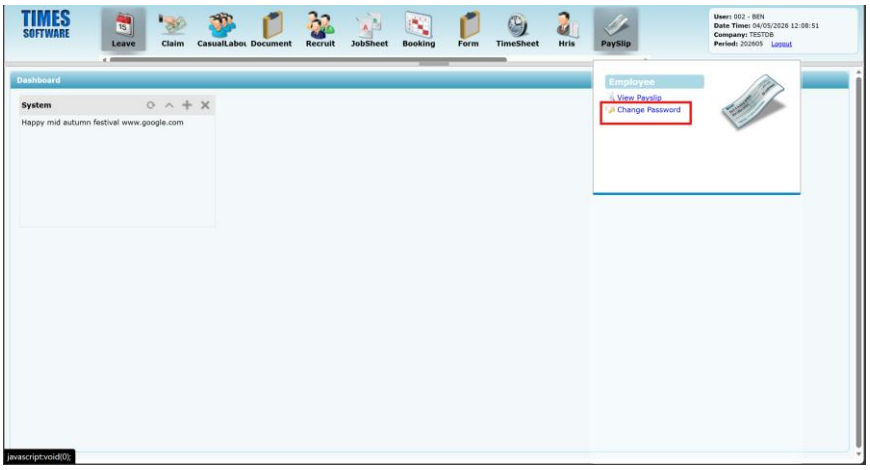


After user clicks on payslip > reset password, user will be redirected to the reset password page shown below:



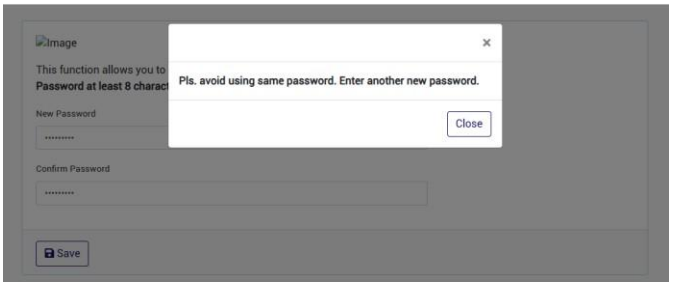
The admin can choose the employee to reset their E-Password. After the admin chooses the employee, they will tick the check box at the bottom part and click the Submit button. After they successfully submit the form, the system will prompt out the message box shown below:



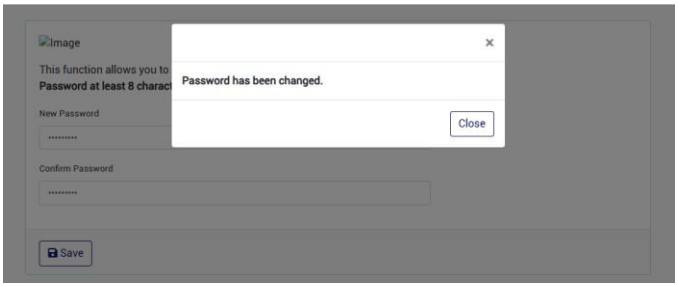


Note: Once the employee has their E-Password reset, they will be prompted to create a new password when they try to view their E-payslip

If the user uses the **same password as their login password**, the following notification will be shown.

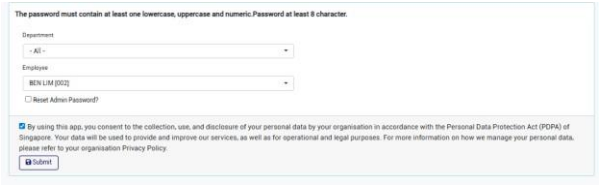


If the new password is successfully created, the following notification will be shown below



2.2) Admin Reset Employee Password

Admin can navigate to Reset Password page to reset the password of a selected employee to the default value.



After the admin resets the selected employee's password, the employee can follow the same steps as **New User First-Time Login** to create a new password.