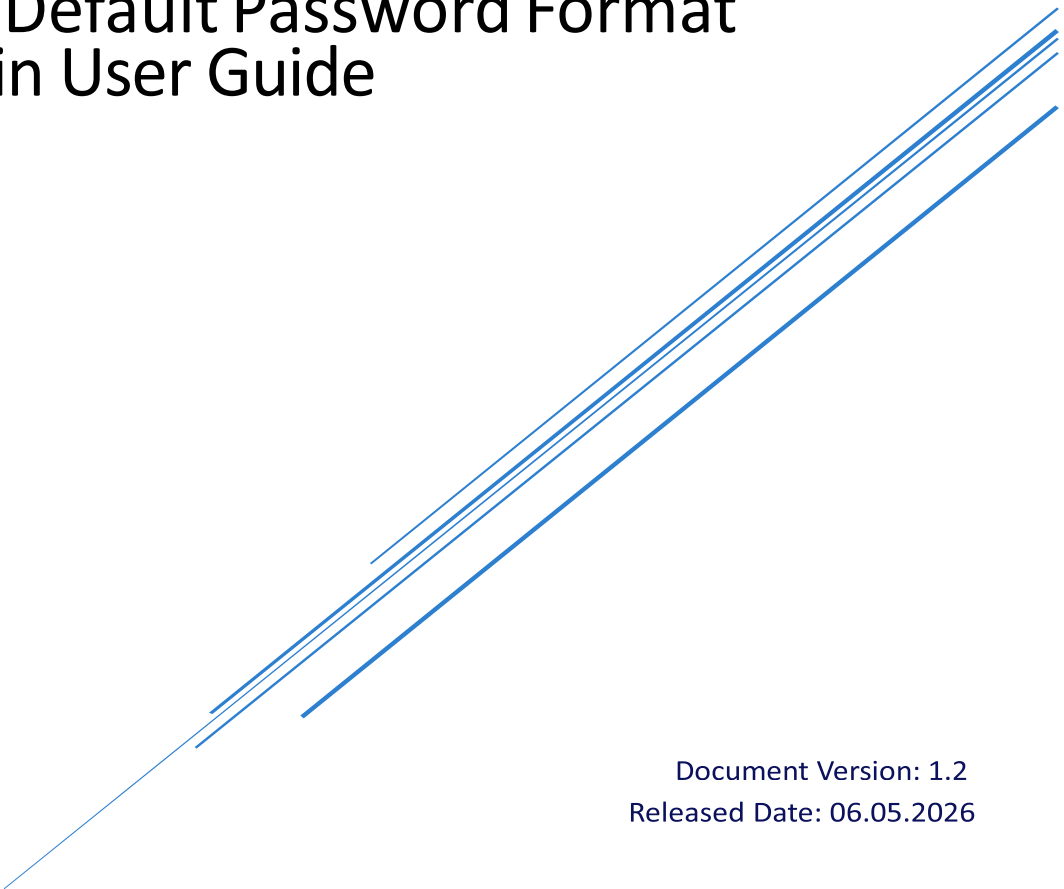




# New Default Password Format Admin User Guide



Document Version: 1.2  
Released Date: 06.05.2026



## TABLE OF CONTENTS

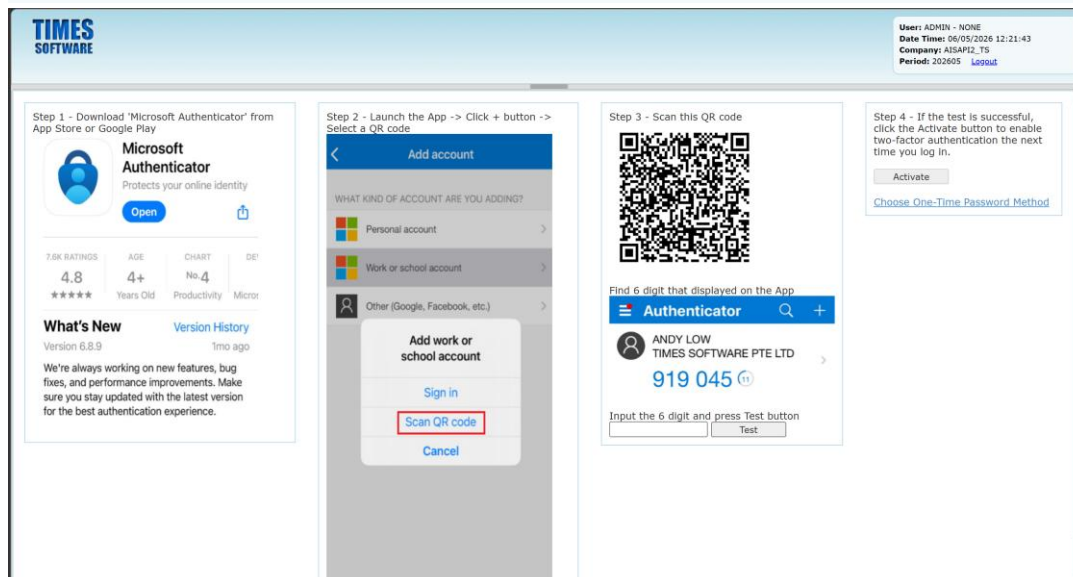
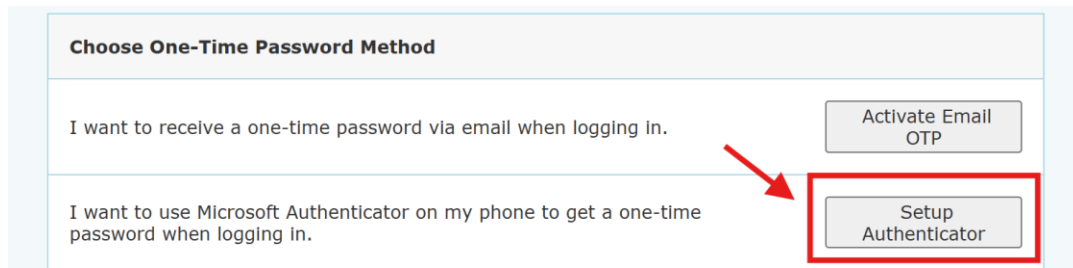
---

<b>1) MFA Setup for Admin .....</b>	<b>3</b>
1.1) MFA – Microsoft Authenticator.....	3
1.2) MFA - Email .....	6
1.3) Change MFA Method.....	7
1.4) Admin access to reset MFA Authentication .....	7
<b>2) E-Password .....</b>	<b>9</b>
2.1) Reset Payslip Password (E-Password) (Payslip Module).....	9
2.2) Admin Reset Employee Password .....	11

# 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”



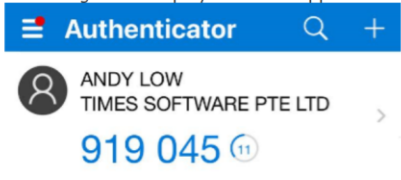
Follow the steps provided (Step 1 -> 4) to download Microsoft authenticator on the user’s mobile device. Then refer to ‘Step 3 – Scan QR Code’ to setup the authenticator.

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

Step 3 - Scan this QR code



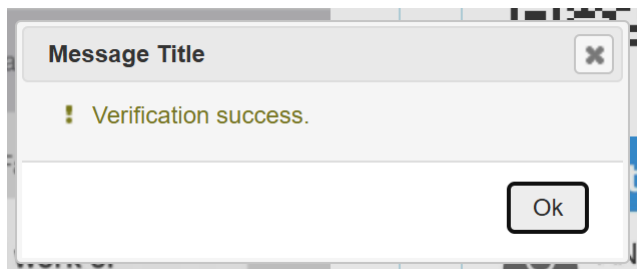
Find 6 digit that displayed on the App



Input the 6 digit and press Test button

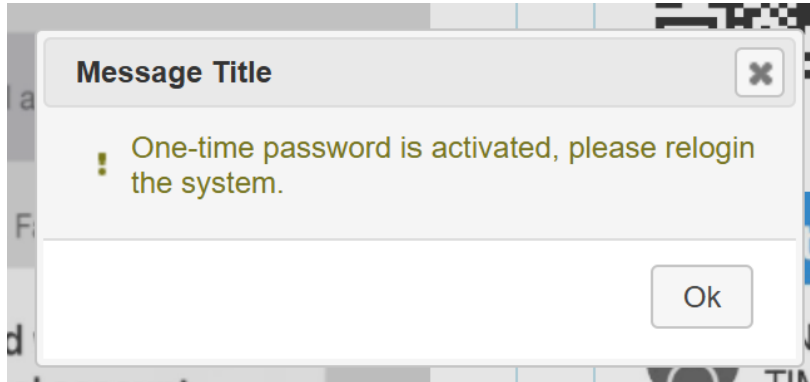
Step 4 - If the test is successful, click the Activate button to enable two-factor authentication the next time you log in.

[Choose One-Time Password Method](#)

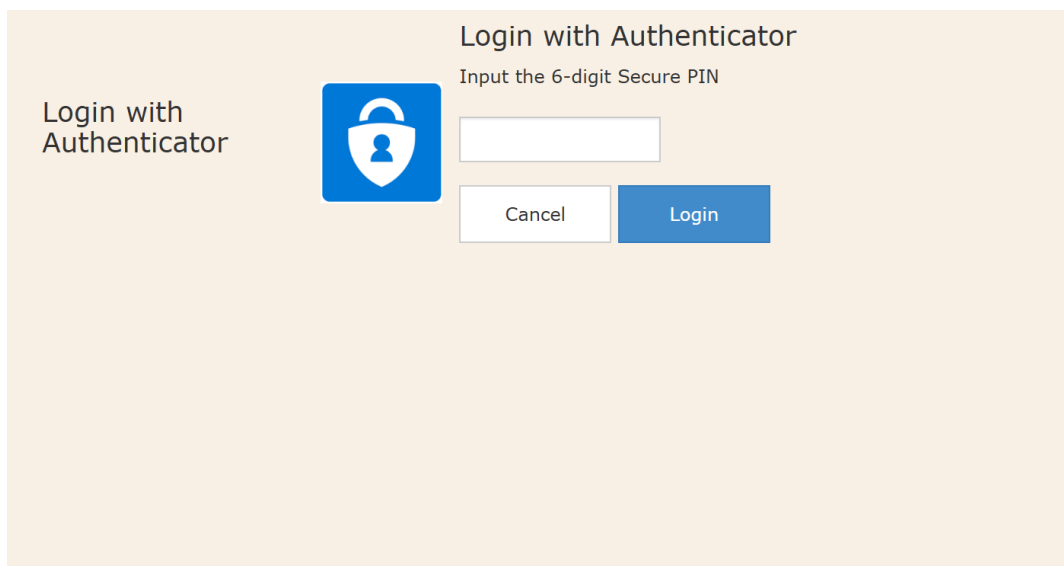


- Click the [Activate] button to enable two-factor authentication.  
**\*\* The activate button will only be enabled after Step 3 has been successfully verified.**

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”

**Choose One-Time Password Method**

I want to receive a one-time password via email when logging in. Activate Email OTP

I want to use Microsoft Authenticator on my phone to get a one-time password when logging in. Setup Authenticator

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

**Choose One-Time Password Method**

I want to receive a one-time password via email when logging in. Activate Email OTP

Please input email

I want to use Microsoft Authenticator on my phone to get a one-time password when logging in. Setup Authenticator

**Message Title**

One-time password is activated, please relogin the system.

Ok

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].

**Login with mail**

Input the 6-digit Secure PIN

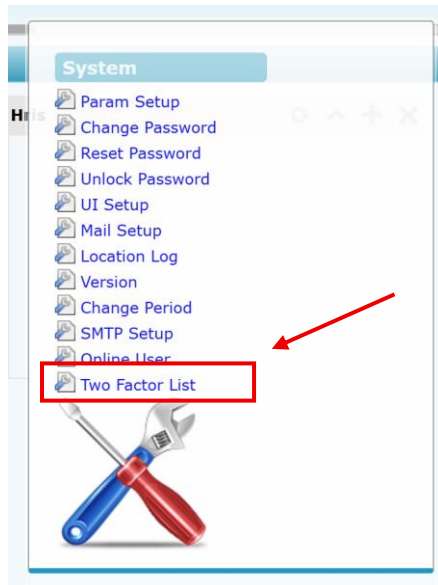
ReGet OTP (105)

Cancel Login

OTP has been sent to email kylexxx@xxx

### 1.3) Change MFA Method

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

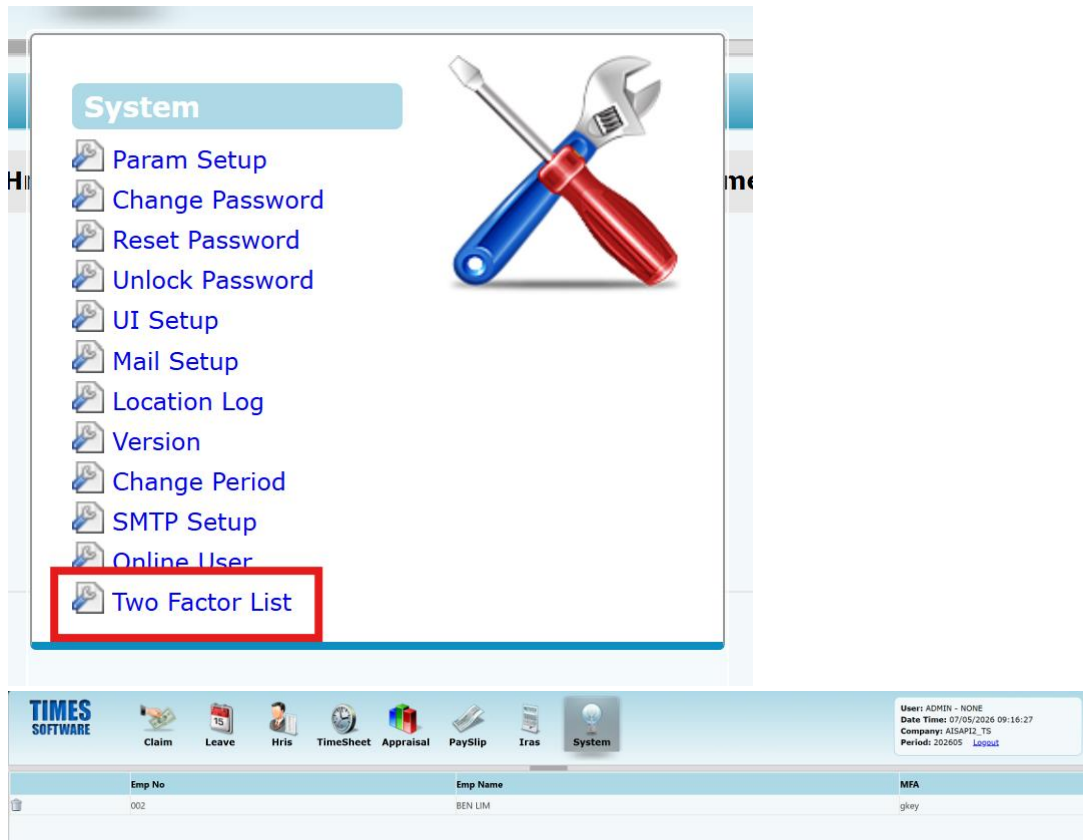


The user will be redirected to the One-Time Password method selection page. Refer to the previous section for the steps to activate Email OTP.

Choose One-Time Password Method	
I want to receive a one-time password via email when logging in.	Activate Email OTP
I want to use Microsoft Authenticator on my phone to get a one-time password when logging in.	Setup Authenticator



### 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.



The screenshot displays the 'System' menu in the Times Software Admin User Guide. The menu items are: Param Setup, Change Password, Reset Password, Unlock Password, UI Setup, Mail Setup, Location Log, Version, Change Period, SMTP Setup, Online User, and Two Factor List. The 'Two Factor List' item is highlighted with a red box. To the right of the menu is an image of a blue and red adjustable wrench and a silver screwdriver. Below the menu is a navigation bar with icons for Claim, Leave, Hris, TimeSheet, Appraisal, PaySlip, Iras, and System. The System icon is selected. In the top right corner, the user information is displayed: User: ADMIN - NONE, Date Time: 07/05/2026 09:16:27, Company: A15AP12\_TS, Period: 202605, and a Logout link. Below the navigation bar is a table with columns for Emp No, Emp Name, and MFA.

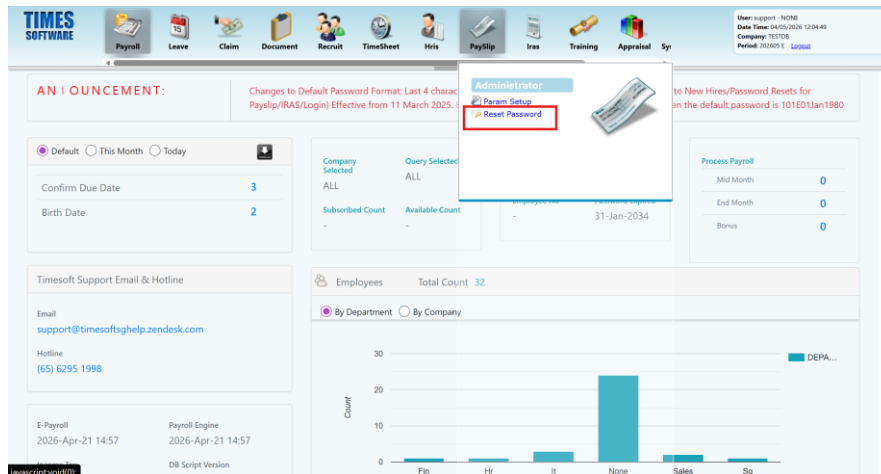
Emp No	Emp Name	MFA
002	BEN LIM	gkey

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.

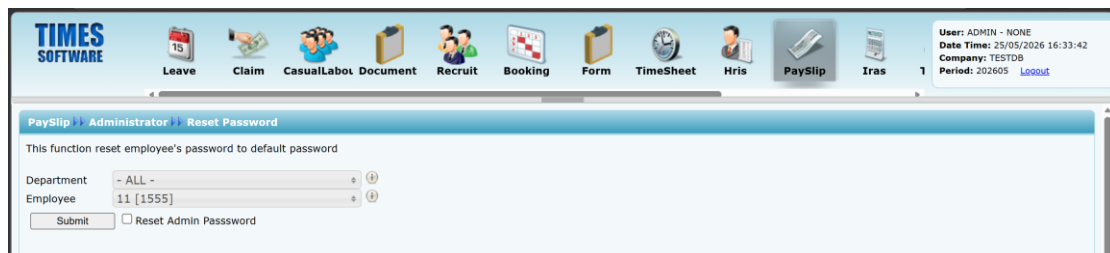
## 2) E-Password

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

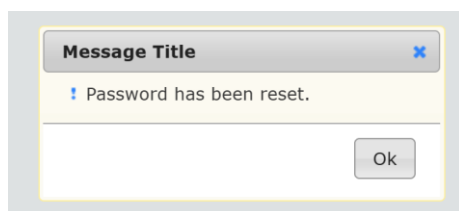
Admin can reset the employee E-Password via the menu at the payslip module.

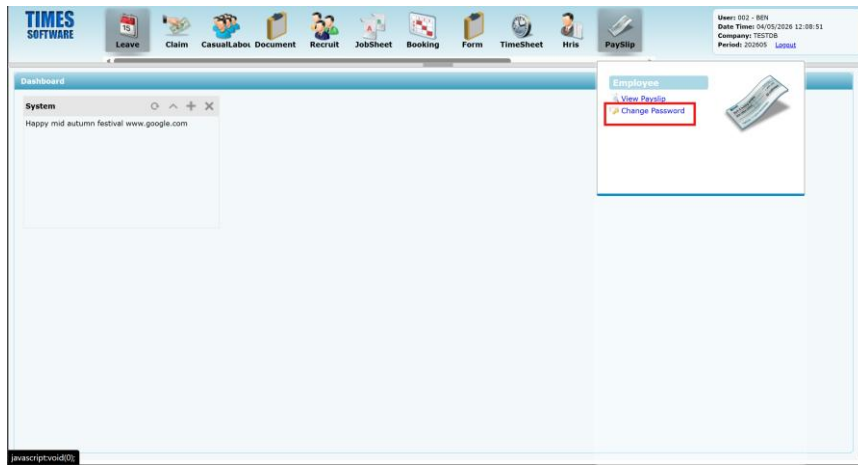


After user clicks on payslip > reset password, user will be redirected to the reset password page shown below:



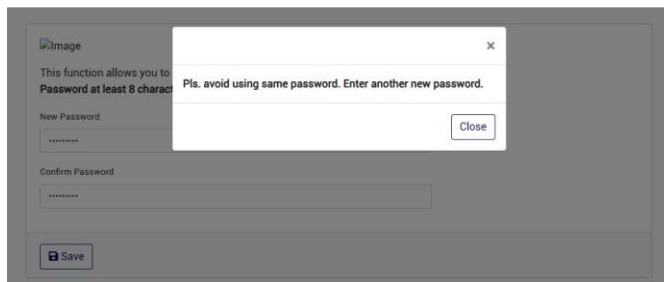
The admin can choose the employee to reset their E-Password. After the admin chooses the employee, they will tick the check box at the bottom part and click the Submit button. After they successfully submit the form, the system will prompt out the message box shown below:



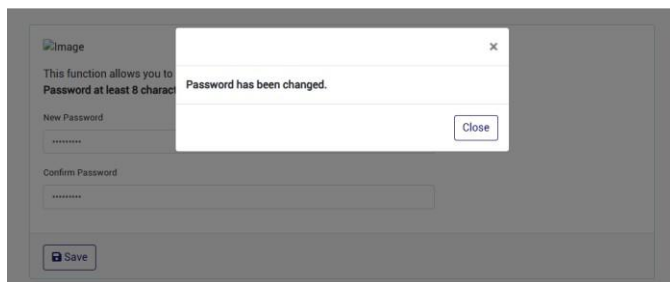


**Note:** Once the employee has their E-Password reset, they will be prompted to create a new password when they try to view their E-payslip

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

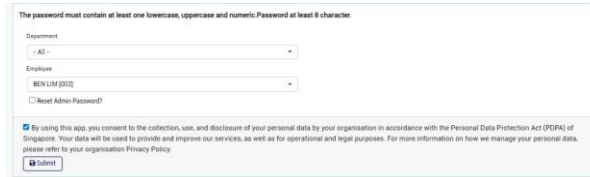


If the new password is successfully created, the following notification will be shown below



## 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.



The screenshot shows a web form for resetting an employee's password. At the top, a note states: "The password must contain at least one lowercase, uppercase and numeric Password at least 8 character:". Below this, there are two dropdown menus: "Department" with "- All -" selected, and "Employee" with "BEN LIM (002)" selected. A checkbox labeled "Reset Admin Password?" is present and unchecked. At the bottom, there is a consent statement: "By using this app, you consent to the collection, use, and disclosure of your personal data by your organisation in accordance with the Personal Data Protection Act (PDPA) of Singapore. Your data will be used to provide and improve our services, as well as for operational and legal purposes. For more information on how we manage your personal data, please refer to your organisation Privacy Policy." Below the consent statement is a "Submit" button.

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.