

Frequently Asked Questions on Second Factor Authentication (2FA)

In this 2FA FAQ section, we will cover the following:

- [General FAQs](#)
- [Installation of Google Authenticator](#)
- [Use of Google Authenticator](#)
- [Setup of 2FA \(Initial Registration\)](#)
- [Reset of 2FA \(Re-register for new phones\)](#)
- Issues during the Setup of 2FA (Initial Registration)
 - [Option 1 - Phone Time not synchronized](#)
 - [Option 1a – Android Phones](#)
 - [Option 1b – iPhones](#)
 - [Option 2 – Google Authenticator Time not synchronized for Android Phones](#)

General FAQs

1) What is Second Factor Authentication (2FA)?

2FA can be based on any two of the factors

- (i) What you know (e.g. PIN);
- (ii) What you have (e.g. One-Time-Pin (OTP) token);
- (iii) Who you are (e.g. Biometrics).

A common form of 2FA involves you entering your password as the first factor, together with a One-Time-Pin (OTP) generated by token to log in to an online system (in this case PSA Digital).

2) Why is 2FA needed?

The primary objective of 2FA to secure the authentication process and to protect your online PSA account against unauthorised access. When implemented, 2FA offers much greater protection against hacking than single-factor password authentication and helps to safeguard your account from unauthorised access even when the passwords have been compromised. Online fraud and mischief are becoming increasingly sophisticated and as they evolve, online security itself must advance to combat these threats. The usage of 2FA will mean a greater peace of mind for you when using PSA Digital.

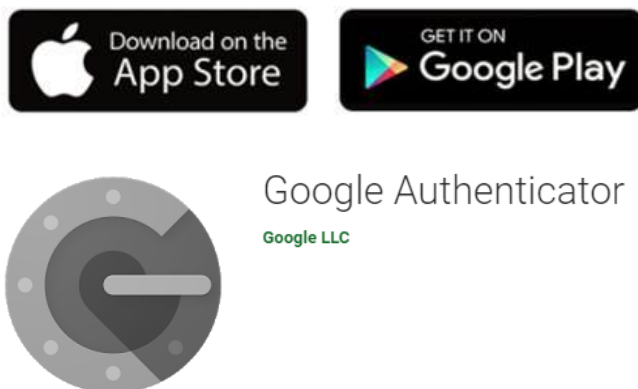
3) When is the use of the 2FA required?

2FA is required for each login to PSA Digital, in addition to your usual login credentials which is the PSA User ID and Password.

General FAQs

4) How will I receive a One-Time-Pin (OTP) for 2FA?

You will receive the 2FA One-Time-Pin (OTP) via the **Google Authenticator** application. This app can be downloaded onto your mobile phone via your phone's app store:



5) What do I need for 2FA?

You will only need a mobile phone with a camera function to scan the QR code (with the Google Authenticator app installed). Not forgetting your PSA User ID and password to login. Also, ensure that your Office Email address is updated in PSA under User Admin.

6) What is a QR code?

A QR code (Quick Response code) is a type of 2D bar code that is used to provide easy access to information through a (smart) mobile phone. In this process, known as mobile tagging, the mobile phone's owner points the phone at a QR code and opens a barcode reader app which works in conjunction with the phone's camera.

7) If I forget to bring my mobile phone to work, will I be able to login to PSA Digital?

You will not be able to login to PSA Digital if you do not bring your mobile phone to the office.

Installation of Google Authenticator

1) How do I install the Google Authenticator application?

- (i) Open the App Store or Google Play application in your mobile phone;
 - (ii) Search for **Google Authenticator**;
 - (iii) Install the application in your mobile phone.
- (Note: This installation is a pre-requisite before you do the 2FA setup)

2) Do I need data to install the Google Authenticator application?

Yes, your mobile phone needs access to data either using your mobile phone's data plan or Wi-Fi only for the installation of the Google Authenticator application.

3) Does the Google Authenticator application need data to run?

No, the One-Time-Pin (OTP) will be randomly generated from Google Authenticator application even when your mobile phone's data plan is off or Wi-Fi is unavailable.

Use of Google Authenticator

1) How fast does the 2FA One-Time-Pin (OTP) change/refresh?

Each OTP will be displayed by 30 seconds. Just before the OTP expires, you will see the colour of the OTP change from blue to red. If the OTP is red, wait for OTP to change/refresh.

PSA (Username(User ID))

723 408



2) Does every staff who needs access to PSA Digital download the Google Authenticator application?

Yes, every staff (who accesses PSA Digital) must download Google Authenticator into their individual mobile phone's. Only one mobile device can be registered to a PSA Digital User ID at any one time.

3) Can staff share the same mobile phone?

No. Each staff must have their own mobile phone.

4) What if I am travelling and need to access PSA from overseas?

You can still access PSA Digital from overseas with the mobile phone that you have downloaded and setup the Google Authenticator application.

5) What if I have overseas colleagues who need access to PSA Digital?

Your overseas colleagues will also need to download the Google Authenticator application into their own overseas phones.

6) Can my PSA Digital User ID be shared among colleagues?

No, each staff within your company must have their own unique PSA Digital User ID & Password. Sharing of User IDs among staff leads to risks related to accountability and ease of compromise of your PSA Digital account.

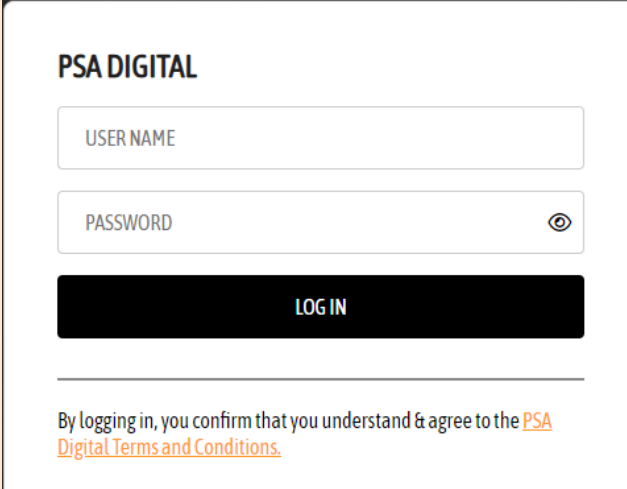
Setup of 2FA (Initial Registration)

1) How do I setup 2FA?

The simple registration steps are as follows:

Step 1

Login to PSA Digital with your Username & Password.



PSA DIGITAL

USER NAME

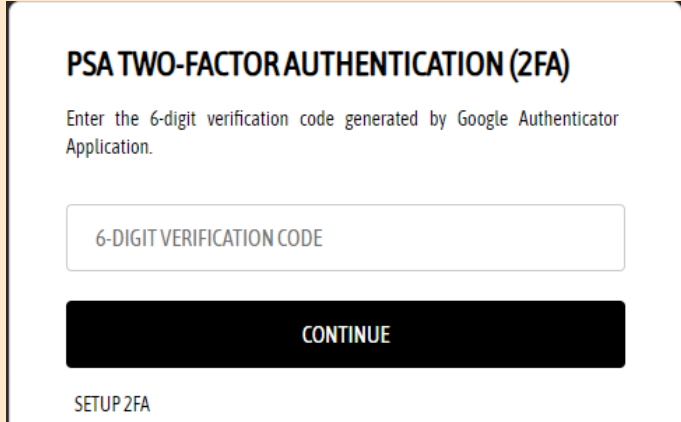
PASSWORD

LOG IN

By logging in, you confirm that you understand & agree to the [PSA Digital Terms and Conditions](#).

Step 2

Click Setup.



PSA TWO-FACTOR AUTHENTICATION (2FA)

Enter the 6-digit verification code generated by Google Authenticator Application.

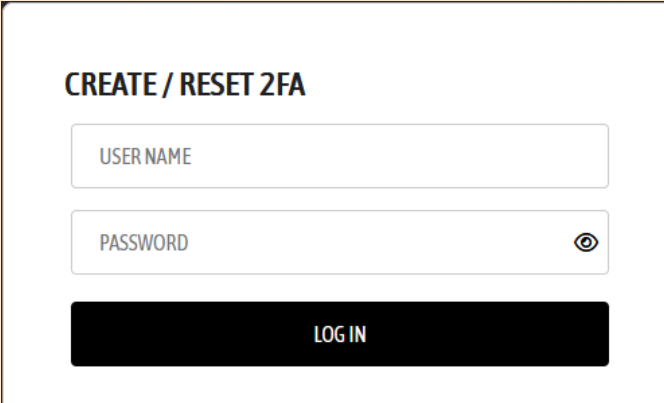
6-DIGIT VERIFICATION CODE

CONTINUE

SETUP 2FA

Step 3

Login with your PSA Digital your Username & Password.



CREATE / RESET 2FA

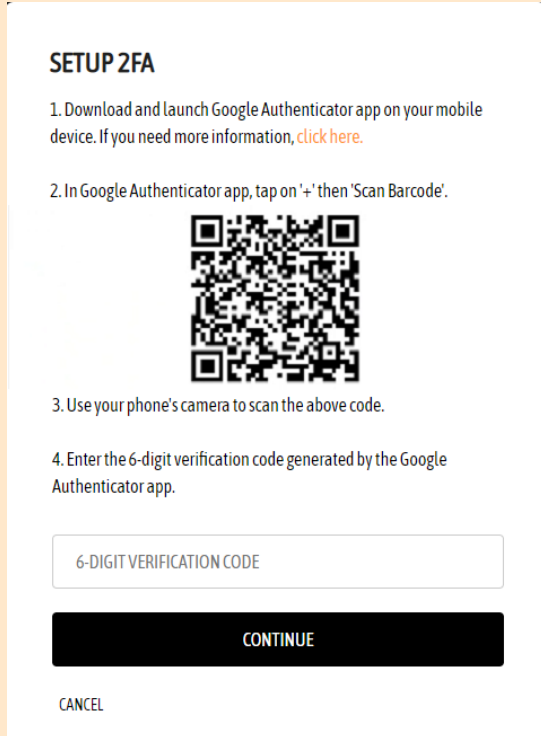
USER NAME

PASSWORD

LOG IN

Step 4


Launch your Google Authenticator app & scan the QR code.



SETUP 2FA

1. Download and launch Google Authenticator app on your mobile device. If you need more information, [click here](#).

2. In Google Authenticator app, tap on '+' then 'Scan Barcode'.



3. Use your phone's camera to scan the above code.

4. Enter the 6-digit verification code generated by the Google Authenticator app.

6-DIGIT VERIFICATION CODE

CONTINUE

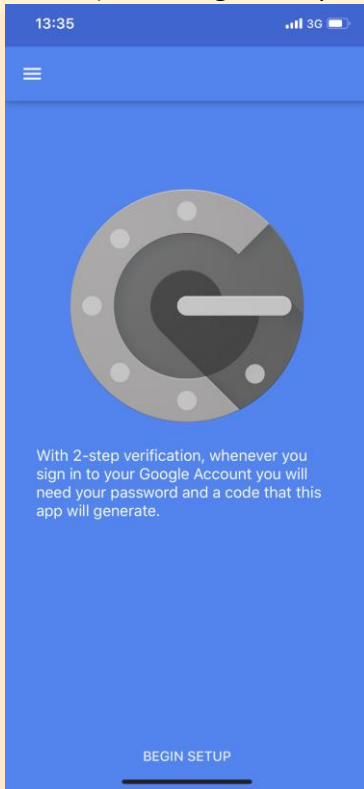
CANCEL

(setup continued on the next page)

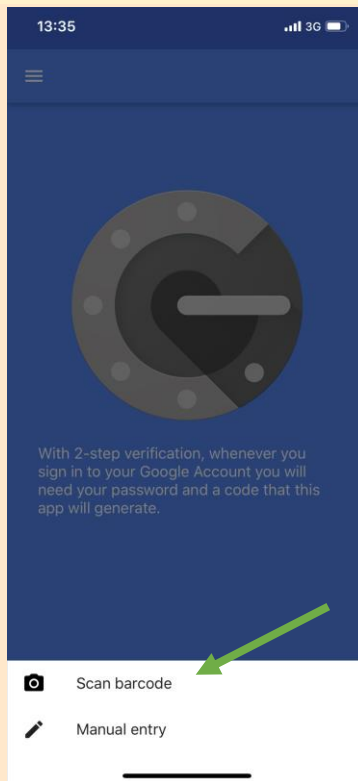
Setup of 2FA (Initial Registration)

Step 5 – Screens from your own Phone (screens may vary across mobile phone)

a) Click Begin Setup



b) Click Scan Barcode



c) Apps opens the camera



Step 6 – Screen from your own Phone

Enter this 6-digit verification code into PSA Digital.




Step 7

Enter the 6-digit code & click Continue.

SETUP 2FA

- Download and launch Google Authenticator app on your mobile device. If you need more information, [click here](#).
- In Google Authenticator app, tap on '+' then 'Scan Barcode'.



- Use your phone's camera to scan the above code.
- Enter the 6-digit verification code generated by the Google Authenticator app.

6-DIGIT VERIFICATION CODE

CONTINUE

CANCEL

(setup continued on the next page)

Setup of 2FA (Initial Registration)

Step 8

Click Ok.

You will be re-directed to the PSA Digital login page.

SETUP 2FA

Your 2FA has been setup successfully. Please re-login to continue.

LOG IN

Step 9

Login to PSA Digital with your Username & Password.

PSA DIGITAL

USER NAME

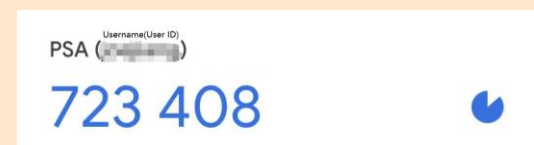
PASSWORD

LOG IN

By logging in, you confirm that you understand & agree to the [PSA Digital Terms and Conditions](#).

Step 10

Open Google Authenticator and key in the 6-digit code.
Click Continue.



PSA TWO-FACTOR AUTHENTICATION (2FA)

Enter the 6-digit verification code generated by Google Authenticator Application.

6-DIGIT VERIFICATION CODE

CONTINUE

RESET 2FA

Warning: Clicking "Continue" means that you understand & agree to the <Product> Terms and Conditions & accept that your use of the <Product> & Licensed Materials & execution of all transactions on <Product> are governed thereby. If you do not agree to these terms, do not login. Any unauthorised user is subject to criminal prosecution under the Computer Misuse and Cybersecurity Act (Cap. 50A).

Step 11

You should be able to see the menu of the system that you initially login to via PSA Digital.

Setup of 2FA (Initial Registration)

2) What happens if I choose to skip the Google Authenticator 2FA setup?

You will not be allowed to login to PSA Digital without 2FA.

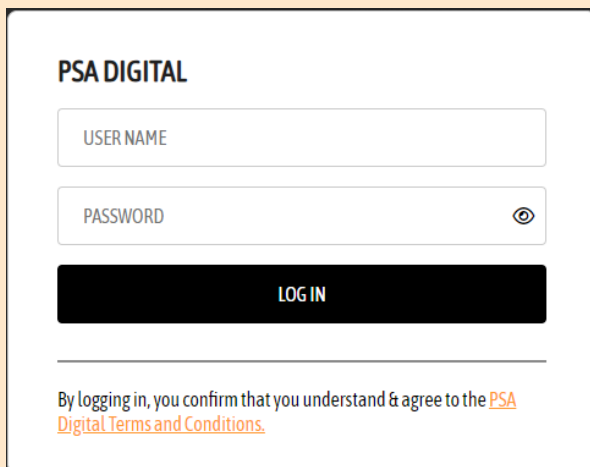
Reset 2FA (Re-Register)

1) I have a new mobile phone or I have lost my mobile phone and bought a new one. What should I do?

If you do not have a back-up image of your previous mobile phone on your new mobile phone, you will need to reset your 2FA. The simple reset steps for 2FA are as follows:

Step 1

Login to PSA Digital with your Username & Password.



PSA DIGITAL

USER NAME

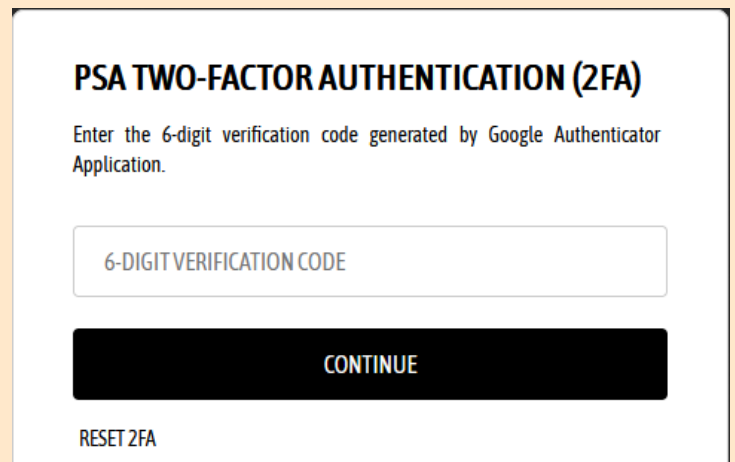
PASSWORD

LOG IN

By logging in, you confirm that you understand & agree to the [PSA Digital Terms and Conditions](#).

Step 2

Click 'Reset'.



PSA TWO-FACTOR AUTHENTICATION (2FA)

Enter the 6-digit verification code generated by Google Authenticator Application.

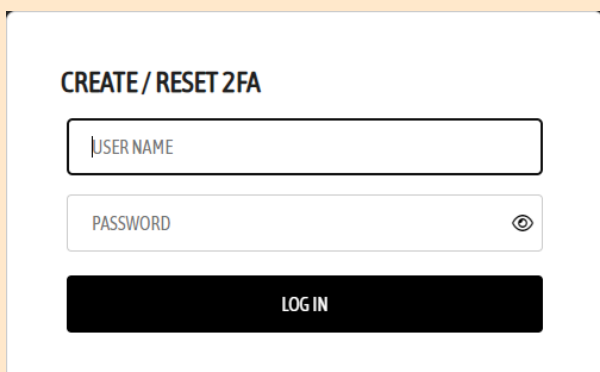
6-DIGIT VERIFICATION CODE

CONTINUE

RESET 2FA

Step 3

Login with your PSA Digital your Username & Password.



CREATE / RESET 2FA

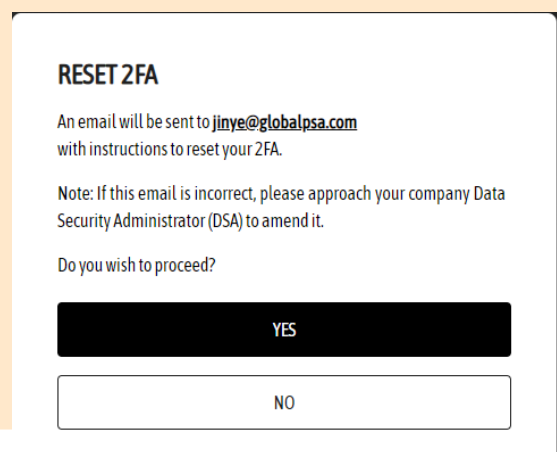
USER NAME

PASSWORD

LOG IN

Step 4

If your email is correct, click Yes.
(If incorrect, approach your company DSA to update it)



RESET 2FA

An email will be sent to jinye@globalpsa.com with instructions to reset your 2FA.

Note: If this email is incorrect, please approach your company Data Security Administrator (DSA) to amend it.

Do you wish to proceed?

YES

NO

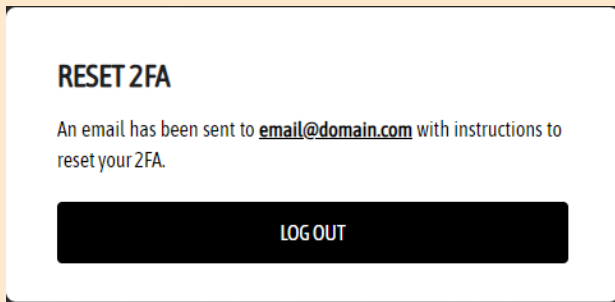
(reset continued on the next page)

Reset 2FA (Re-Register)

Step 5

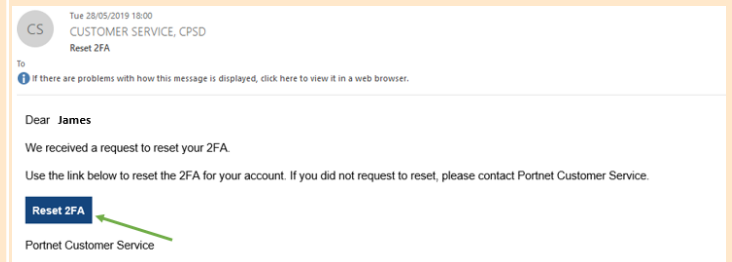
Click Logout.

Note: If the email is incorrect, approach your DSA to update it in User Admin (PSA).



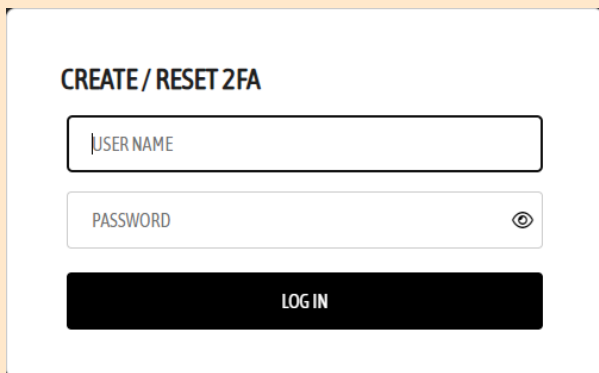
Step 6

Open your email, look for the email titled 'Reset 2FA' and click on 'Reset 2FA'.



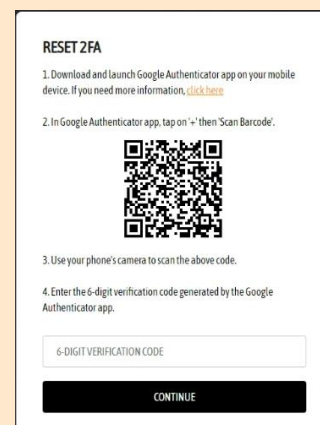
Step 7

Login with your PSA Digital your Username & Password.



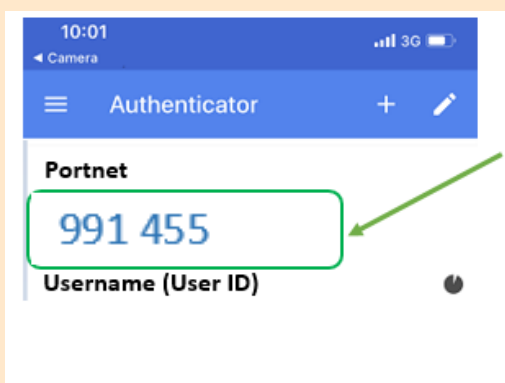
Step 8

Launch your Google Authenticator app & scan the QR code (similar to first time setup). and click on 'CONTINUE'.



Step 9

Enter this 6-digit verification code into PSA Digital.



Step 10

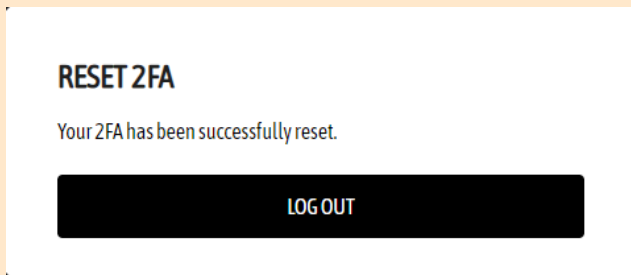
Enter the 6-digit code & click Continue.



Reset 2FA (Re-Register)

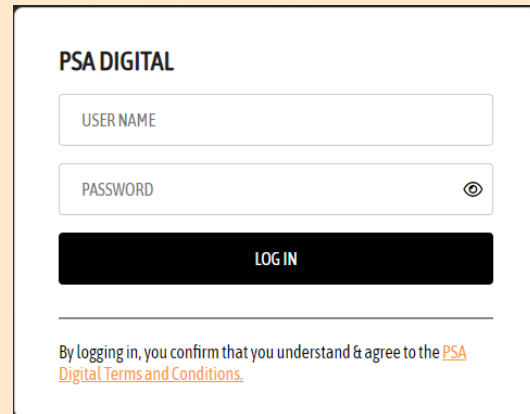
Step 11

Click Ok.
You will be re-directed to the PSA Digital login page.



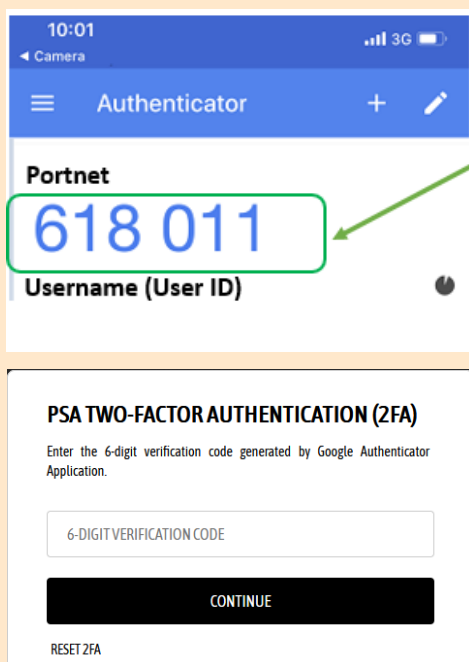
Step 12

Login to PSA Digital with your Username & Password.



Step 13

Open Google Authenticator and key in the 6-digit code.
Click Continue.



Step 14

You should be able to see the menu of the system that you initially login to via PSA Digital.

2) I am using the same mobile phone but the number has changed, is there anything I need to do?

If your mobile phone is the same, there is no need to do anything. The same Google Authenticator can still be used to generate the OTP and login to PSA Digital.

Issues during the Setup of 2FA (Initial Registration)

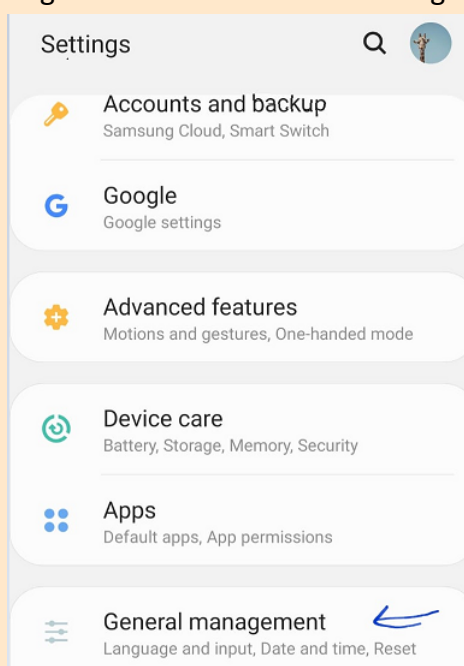
1) I cannot set up 2FA. I see a message saying 'Your 2FA setup has failed. Please try again'.

The setup may fail if your phone's time setting is not synchronised to the standard time.

Option 1a – Android Phones

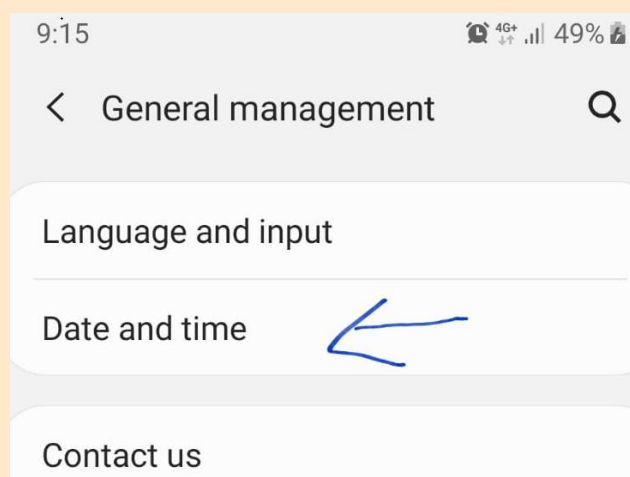
Step 1 – from your phone

Go to Settings and Click on 'General Management'.



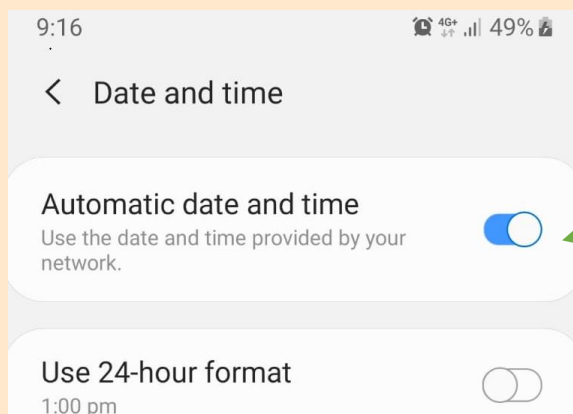
Step 2 – from your phone

Click on 'Date and time'.



Step 3 – from your phone

Turn on 'Automatic date and time'.



Step 4 – Proceed to setup 2FA

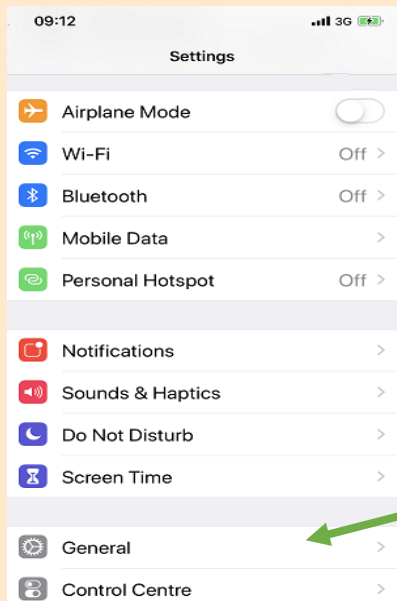
Continue with the [setup of 2FA](#) .

Issues during the Setup of 2FA (Initial Registration)

Option 1b - iPhones

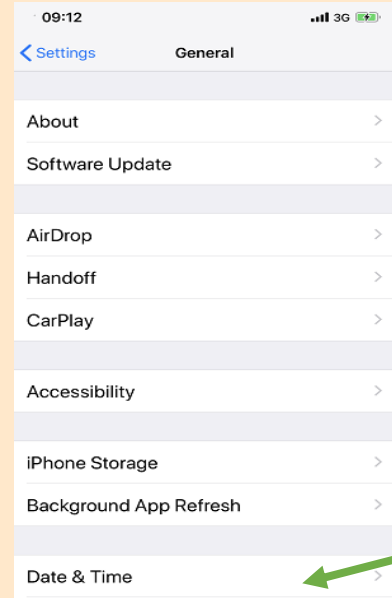
Step 1 – from your phone

Go to Settings and Click on 'General'.



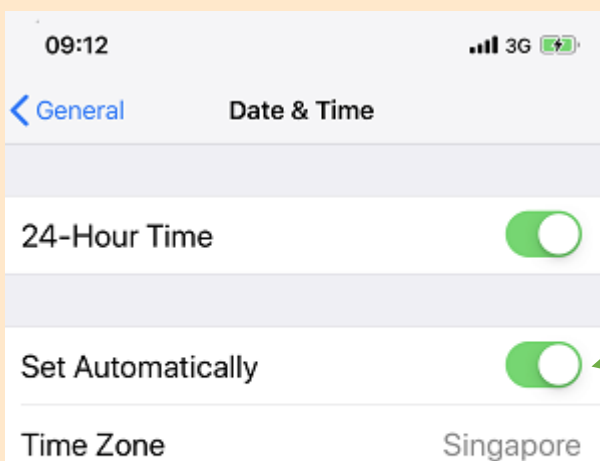
Step 2 – from your phone

Click on 'Date and time'.



Step 3 – from your phone

Turn on 'Set Automatically'.



Step 4 – Proceed to setup 2FA

Continue with the [setup of 2FA](#).

Issues during the Setup of 2FA (Initial Registration)

If the setup still fails after setting your Phone's Date & Time to "Automatic Date & Time" setting, try Option 2.

Option 2 - Android Phones (only)

Step 1 – from your phone

Go to Google Authenticator.



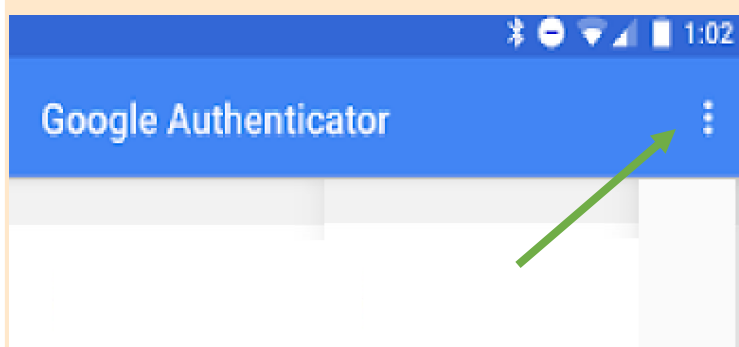
Step 2 – from your phone

Press and hold (the colour will change to blue as shown below). Delete this set-up.



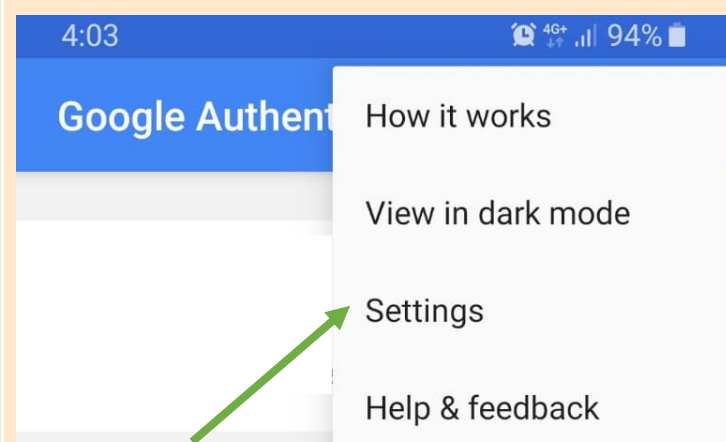
Step 3 – from your phone

Click on the dots (right hand corner).



Step 4 – from your phone

Click on Settings.

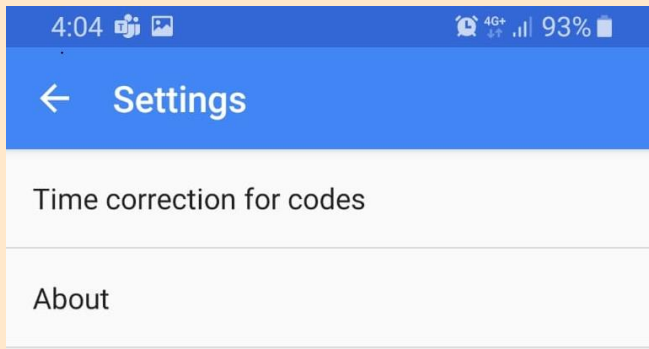


(continued on the next page)

Issues during the Setup of 2FA (Initial Registration)

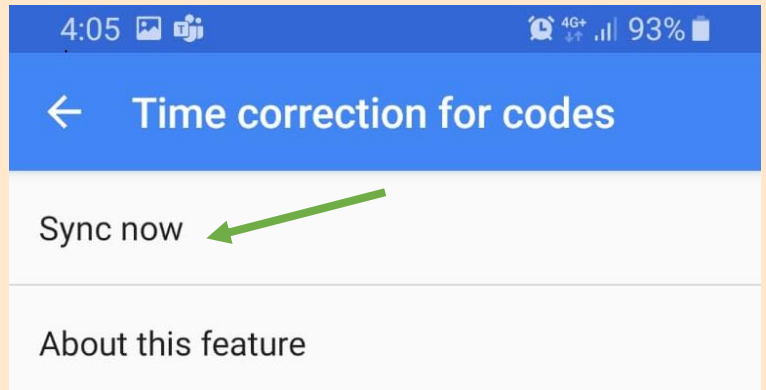
Step 5 – from your phone

Click on 'Time correction for codes'.



Step 6 – from your phone

Click on 'Sync now'.



Step 7 – Proceed to setup 2FA

Continue with the [setup of 2FA](#).

End