Citi Mobile® App with Enhanced Security

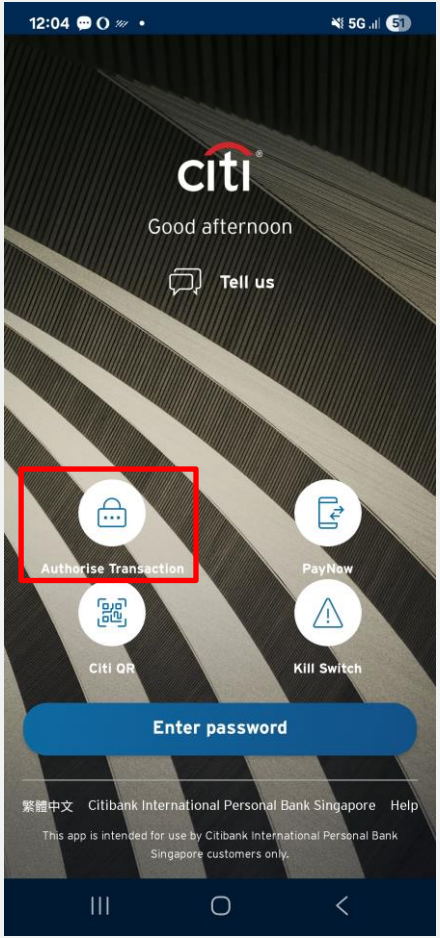
Quick Start Guide
Citi Mobile® App

Enhanced Security on your Citi Mobile® App

We have updated the Citi Mobile® App with enhanced security capabilities to provide you with a more convenient and seamless mobile banking experience.

This feature securely links your Citi Mobile® App to your mobile device, providing a quick and reliable way to verify your identity for transactions.

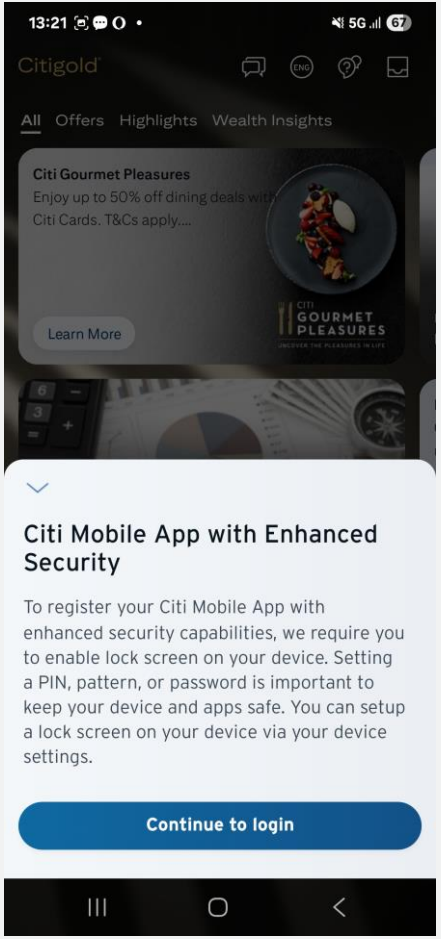
Once you set up this enhanced security, you will see an 'Authorise Transaction' icon directly on your Citi Mobile® App's login screen. Post a 12 hours Cooling Period after enrolment, you will be able to proceed with your transactions seamlessly and securely on this device without having to enter SMS OTP.



Pre-requisite to set up

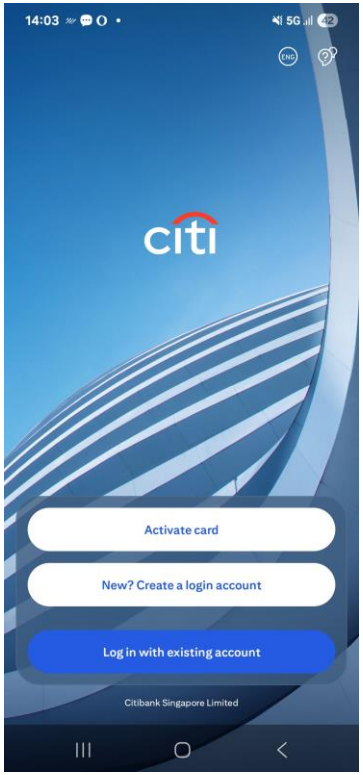
Ensure that the ‘Lock Screen’ function has been setup on your mobile device.

The Lock Screen acts as a safety layer (e.g. PIN, Pattern, Password or Biometrics) to prevent unauthorized access to your device.

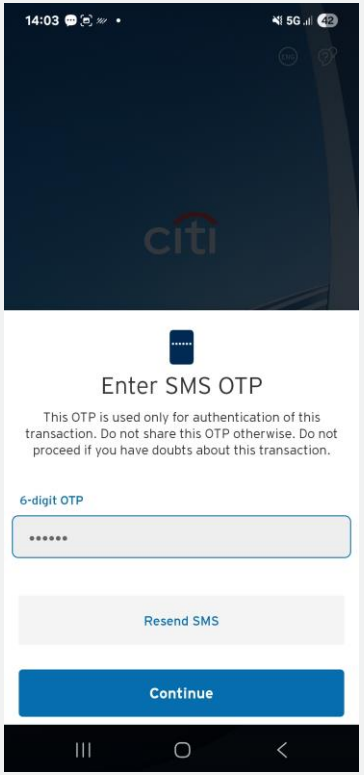


How to setup

1 Log in to the Citi Mobile® App

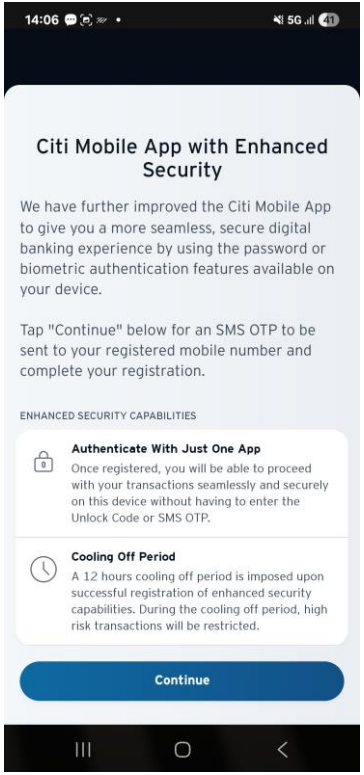


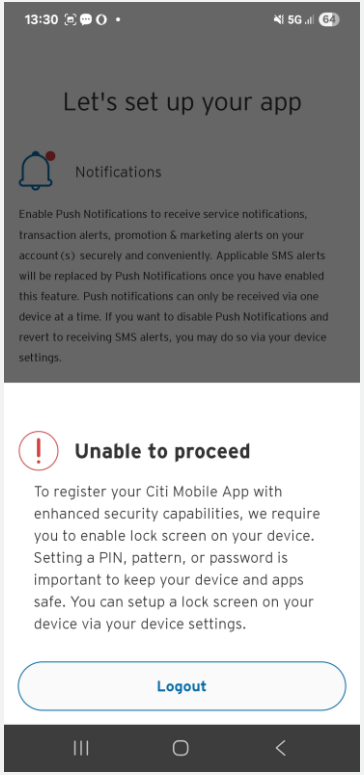
2 Perform SMS OTP authentication



How to setup

3 Click on “Continue” to proceed with enrolment



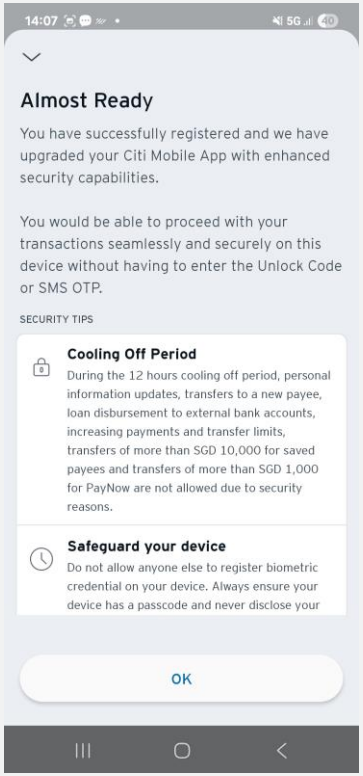


If you have not set up Lock Screen on your device, you will not be able to continue with the setup and will be logged out

How to setup

4 If you have biometric data setup on your device (Face ID for iOS or Fingerprint for Android), you can perform Biometric login enrolment at this point

5 Upon successful enrolment, you will see this screen



Please note that there is a 12 hours Cooling Off Period upon enrolment.

Click “OK” to proceed to your Wealth Dashboard

Your Role and Responsibility

Keep your User ID and Password Confidential
You should never disclose your User ID and Password and you should also ensure that no one is watching you while you enter your User ID and Password or any confidential information. Memorize your User ID and Password and do not record it anywhere. Under no circumstances should you reveal your User ID and Password to anyone even if they purport to be a staff of Citibank.

Do not use a shared computer or device that cannot be trusted for internet banking such as the computer at an Internet café. These devices may be installed with certain software that could capture your personal information prior to your approval.

The One-time PIN(OTP) generated with Online Security Device, Citi Mobile® Token or via an SMS should also not be shared with anyone else.

Mobile Malware
New variants of mobile malware targeting Android smartphones continue to appear in the Asia Pacific region. These malicious apps often target mobile banking apps, and may attempt to steal customer credentials and perform fraudulent transactions.

In some cases, the mobile malware will attempt to circumvent the additional layer of security provided by One Time PINs (OTPs) by intercepting text messages (SMSs) or generating a fake dialogue inside the mobile banking app in order to trick a user.

Citi recommends customers remain alert for malware threats and review our Online Security Tips. Specifically, Citi suggests that all mobile users consider:

- Only installing applications from trusted and official sources
- Installing a reputable mobile anti-virus application
- Keeping mobile device software up-to-date
- Being aware of the heightened risks associated with 'rooted' or 'jailbroken' devices
- Not following any links or instructions provided from unknown or suspicious sources.

If you notice unusual behavior in your online banking session, you should immediately terminate the online banking session and contact 24-Hour CitiPhone Banking at +65 6224 5757.

Beware of Online Threats

Online threats are very common nowadays and it tricks you into surrendering your confidential information. It is important to know its mechanisms and take preventive measures to safeguard yourself.

As an internet banking user, you have a role to play to ensure that you are protected while banking online. Here are some of the ways you could take to safeguard yourself:

Always make sure that you have entered your User ID and Password and other confidential information in the legitimate Citibank International Personal Bank Website by entering Citibank International Personal Bank's Website address http://www.ipb.citibank.com.sg directly onto your Web browser.

To ensure you are on a secure website, check the beginning of the Web address in your browser's address field - it will be "https://" rather than "http://". Secure websites will also contain a padlock icon on the status bar at the top of the browser. Double-click to view details of the security certificate, which is issued to Citibank.

- To verify that the website is authentic, check for the following details:
- The certificate is issued to http://www.ipb.citibank.com.sg
- The certificate is issued by Verisign.
- The certificate has a valid date.

Do not save your online banking login details on the browsers by clearing your browser's cache and history after each session. Click here for steps to clear browsers' cache. Always remember to log out when you have completed your internet banking session.

Always update the bank whenever you have changed your contact details so that you can be contacted in a timely manner should we detect any unusual transactions.

Ensure that your computer has the latest anti-virus software as they help to guard against new viruses. Your computer's operating system and browser software should be updated with the latest security patches. All these will help prevent unauthorized access to your computer.

General Disclaimers

The contents of this document are for general information and illustrative purposes only and are not intended to serve as financial, investment or any other type of advice. This document does not constitute the distribution of any information or the making of any offer or solicitation by anyone in any jurisdiction in which such distribution or offer is not authorized or to any person to whom it is unlawful to distribute such a document or make such an offer or solicitation. Some products and services may not be available in certain jurisdictions. You should consult your professional advisers as to whether you require any governmental or other consent or need to observe any formalities to enable you to utilize or purchase the products and services described in this document. The actual product and service may vary due to enhancements. Citibank Singapore Limited shall not be responsible for any loss or damage of whatsoever nature (including consequential loss or damage) suffered or incurred, directly or indirectly, by the customer or any other person resulting from access to, or use of this document or any information contained in it.

Citibank full disclaimers, terms and conditions apply to individual products and banking services. For more information, please visit www.ipb.citibank.com.sg.

Sign On Now
Explore these capabilities on Citibank Online & Citi Mobile® App

Key Features Available Online

Servicing
Current Balances, Up to 7 years of Statements and 2 years Advices

Investing
FX, Time Deposits, Bonds, Brokerage, Premium Account, Investment Funds

Banking
Telegraphic Transfers, Citibank Global Transfers

Citibank Online
www.ipb.citibank.com.sg

Citi Mobile® App

Available on the App Store

Available on the Google play