



# **Corporate Cyberbanking Quick Start Guide**

The Bank of East Asia, Limited

(01/2018)

Welcome! Thank you for choosing Corporate Cyberbanking (“CCB”). You are just a few steps away from enjoying a whole new level of convenience and cost effectiveness.

Please be sure to review the Terms and Conditions and security tips prior to using CCB.

This document is produced by The Bank of East Asia, Limited (“BEA”). It is intended to serve as a general guideline for use of our Corporate Cyberbanking services. While every effort has been made to ensure accuracy, BEA makes no representation or warranty, express, implied, or statutory, with respect to, and assumes no responsibility for, the accuracy, completeness, sufficiency, or usefulness of the information contained herein.

## Contents

How to Access CCB .....	4
Overview .....	4
User Types .....	4
PIN.....	6
PIN Activation (applicable to administrator and default user only) .....	7
First Time Login .....	8
Internet Banking .....	8
Mobile Banking.....	9
Phone Banking .....	10
User Creation.....	11
User Access Rights .....	12
Sign-and-Send .....	12
Important Notes for Security in relation to Cyberbanking.....	13
Frequently Asked Questions .....	17
Administrators .....	17
Normal Users and Signers .....	18
Service Overview.....	19
Internet Banking .....	19
Mobile Banking.....	20
Phone Banking .....	21
Service Hours .....	22
Daily Withdrawal Limits.....	26
Internet Banking .....	26
Internet Banking with Digital Certificate .....	26
Phone Banking .....	26
Daily Deposit Limits .....	27
Service Hotlines.....	27

## How to Access CCB

You can access CCB through the following channels, giving you greater freedom to manage your company's finances whenever and wherever you want:

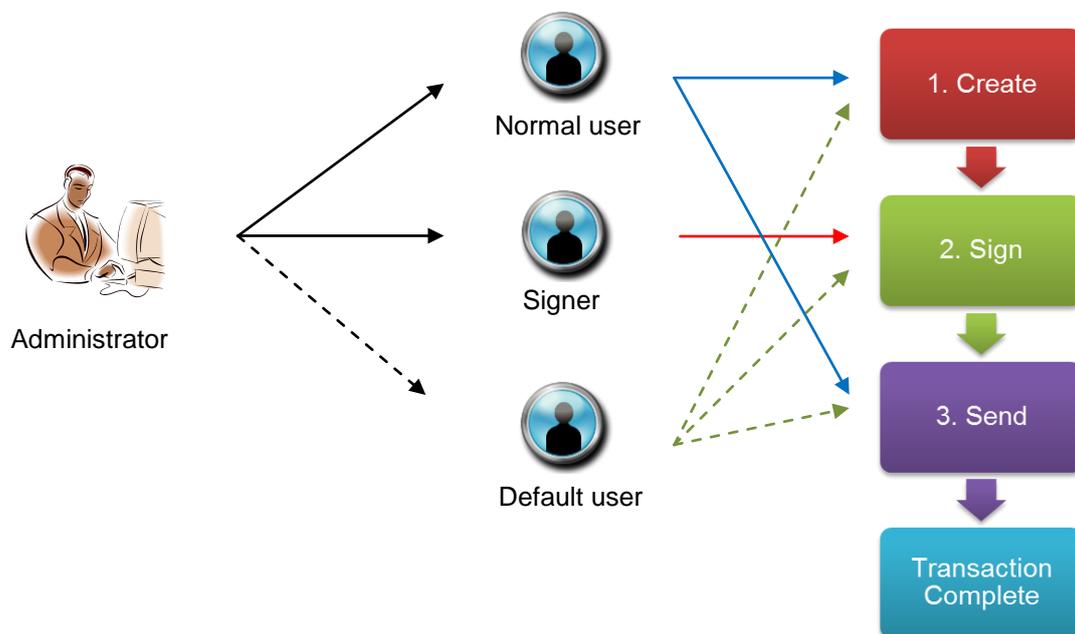
- **Internet:** Visit the BEA website at [www.hkbea.com](http://www.hkbea.com) and select "Hong Kong – Corporate Cyberbanking" from the login menu
- **Mobile:** Register your mobile phone number via the CCB internet service to activate this service
- **Phone:** Dial (852) 2211 1838 from any touch-tone phone

## Overview

### User Types

You can assign different duties to different users in line with your existing operations.

1. The **administrator** creates users and defines access rights in CCB
2. Each **user** has an individual profile
3. **Perform transactions** according to their profiles



Explanation of Different User Types

<b>User Type</b>	<b>Role</b>	<b>Details</b>	<b>Default User ID for Login</b>
Administrator	Human resources: assigning users and account settings  *Cannot directly access account-related functions	- Create and delete users - Manage user profiles - Manage service options  *Each CCB account allows for 2 administrators	SYSADM1/ SYSADM2
Normal User	Clerk: preparing transactions for officer/manager approval	- Create and send transactions - Other functions according to the access rights granted by the administrator	Assigned by the administrator
Signer	Officer/Manager: authorising transactions	- Sign transactions - Other functions according to the access rights granted by the administrator	Assigned by the administrator
Default User	SME business owner: performing all steps as a single user	- Create, sign, and send transactions - "Sign-and-Send" feature enabled  *Pre-defined user with access to all functions, created by the system upon your request during account opening	USER1/ USER2

## **PIN**

There are three types of PIN used in CCB:

- Login PIN: every user will have an internet login PIN to access the internet service
- Signer PIN: users with signing rights will have an additional PIN that must be entered to authorise transactions
- Phone PIN: each CCB account will also have a phone PIN to access phone banking services

<b>User Type</b>	<b>Login PIN</b>	<b>Signer PIN</b>	<b>Phone PIN</b>
Administrator	PIN mailer provided by BEA	N/A	PIN mailer provided by BEA (each CCB account has one phone PIN only)
Default User	PIN mailer provided by BEA	PIN mailer provided by BEA ("User ID/Class" A01/A02 according to the linked Signer ID)	
Normal User	Assigned by the administrator	N/A	
Signer	Assigned by the administrator	PIN mailer provided by BEA	

## ***PIN Activation (applicable to administrator and default user only)***

Follow these steps to activate all PINs provided by BEA:

1. Make a copy of the PIN acknowledgement letter for your records
2. Return the letter to your account opening branch to activate the associated PINs
3. After activation, enter the PIN printed on the PIN mailer with the corresponding reference no. indicated on the PIN acknowledgement letter

**A** 企業電子網絡銀行服務賬戶號碼  
Corporate Cyberbanking A/C No. 015-000-00-00000-1

敬啓者  
Dear Customer,

企業電子網絡銀行服務新密碼簽收函  
**Corporate Cyberbanking New PIN(s) Acknowledgement Letter**

多謝 貴公司選用企業電子網絡銀行服務。以下是密碼之有關資料而密碼另函奉上。為保障 貴公司利益，請於收到密碼後核對有關資料，簽署此函並將正本送回 貴公司之開戶分行以便開放密碼供 貴公司使用。

At your request, the related information of the new PIN(s) is displayed below and your new PIN(s) will be issued to you separately. For your own protection, please check the information upon receipt of your PIN(s), and acknowledge receipt by signing this letter and returning the original to your A/C opening branch for activation of your PIN(s).

<b>C</b> 參考編號 Reference No.	類別 User Type	<b>B</b> 號碼 / 級別 User I.D. / Class
001312	SYSADM	SYSADMIN
001313	DEFAULT USER	USER1
001314	SIGNER	A01
001315	PHONE PIN	Phone Banking

**Corporate Cyberbanking "CCB" Account Login**

Account No.: 015 **A**

User ID: **B**

PIN: **C**  the onscreen keypad

Save your CCB account no. on this computer.

**Log in**

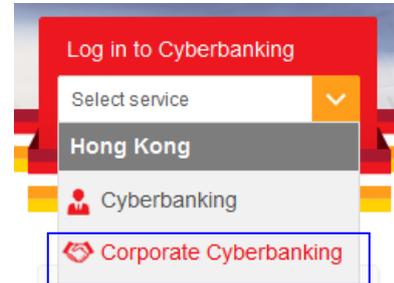
[First-time Login Demo](#)

Q W E R T Y U I O P 3 8 1  
A S D F G H J K L 5 7 6  
Z X C V B N M 2 0 9  
Backspace Clear 4

## First Time Login

### Internet Banking

1. Visit the BEA website at [www.hkbea.com](http://www.hkbea.com) and select “Hong Kong – Corporate Cyberbanking” from the login menu



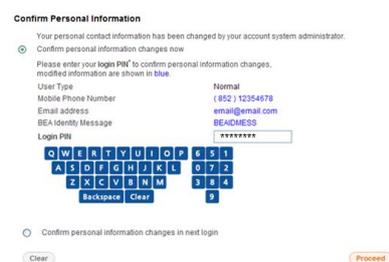
2. Enter your login details

If you use a Digital Certificate to log in, enter your USB token password

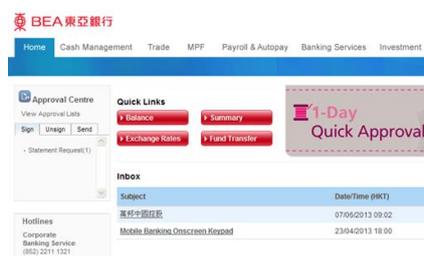


3. Confirm your personal information by entering your login PIN

For default users and signers, confirm by entering your signer PIN



4. Login is successful



\*Click “First-time Login Demo” under “Log in” on the CCB login page for an online demonstration.

## Mobile Banking

### Administrator

#### Designate mobile banking users

Log in to the CCB internet service and select “Service Maintenance” then “Mobile Banking” to register for the service and designate users

Setup	Mobile Banking	Mobile Login	User ID	User Name	Phone Number
<input type="checkbox"/>	Available	Enable	A02	A02	12345678
<input type="checkbox"/>	Not Available	Enable	B01	B01	12345678

### Designated users

#### Confirm personal information

1. Log in to the CCB internet service and create your mobile PIN
2. Activate mobile banking by confirming via the SMS link

Confirm Personal Information

Your personal contact information has been changed by your account system administrator.

Confirm personal information changes now

Please enter your **signer PIN** to confirm personal information changes, modified information are shown in blue.

User Type: Signer  
Mobile Phone Number: (852) 12345678  
Mobile Services Provider: SmartTone-locabank  
Email address: user001@locabank.com  
BEA Identity Message: TestSMS A02  
New Mobile Banking PIN: [input field]

Re-confirm New Mobile Banking PIN: [input field]

Signer PIN: [numeric keypad]

Confirm personal information changes in next login

Proceed

#### Complete mobile banking setup

3. Select “Settings”, “Change Mobile Banking Setup”, then “Mobile Banking Quick Setup” to set up accounts and mobile templates

Settings

1. **Mobile Banking Quick Setup**
2. Change Mobile Banking Login PIN
3. Resend Mobile Banking Login Link
4. Maintain Mobile Banking Account Name
5. Sign Mobile Template
6. Unsign Mobile Template

#### Start using the service

4. Access the service using a handset that supports internet access

BEA 東亞銀行

繁體

Corporate Cyberbanking  
Mobile Banking

PIN: [input field]

[2] [3] [7] [5] [9]  
[0] [4] [6] [8] [1]  
[Backspace] [Logon]

Enter your PIN using the onscreen keypad.

### ***Phone Banking***

1. Dial (852) 2211 1838 on any touch-tone telephone
2. Select language: 1 for Cantonese, 2 for Putonghua, or 3 for English
3. Enter your CCB account number and phone banking PIN then follow the voice prompts to select the required service

## User Creation

1. Log in as an administrator, select “User Maintenance” from the main menu, then click “New”



2. Enter the user’s personal information and login details. Then, select the Function Access Profile (“FAP”) and Data Access Profile (“DAP”)

Assign the signing class to users with signing rights

\*You have to enter the user’s mobile phone number and email address

The "New User" form includes the following fields and options:

- User ID: [input field]
- User Name: [input field]
- Type:  Normal  Signer
- FAP: [input field]
- DAP: [input field]
- Sign-and-Send:  Enable  Disable
- Mobile Phone No.\*: [input field] Country Code (ISO 3166) [input field] Phone Number [input field]
- BEA Language\*:  English  Chinese
- BEA Identity Message\*: [input field]
- Email Address: [input field]
- Internet Login:  Enable  Disable
- Setup Initial PIN: [input field]
- Confirm Initial PIN: [input field]

3. User is created. The following information should be passed to the user:
  - CCB account no.
  - User ID
  - Initial login PIN
  - BEA identity message
  - PIN mailer corresponding to the signing class assigned (for users with signing rights only)



\*You can view an online demo after logging in to CCB.

## ***User Access Rights***

The administrator must assign a Function Access Profile (“FAP”) and Data Access Profile (“DAP”) to each user, for granting access rights to functions. FAP and DAP templates are available for your reference.

Alternatively, the administrator can customise the FAP and DAP by selecting “User Maintenance”, “Function Access Profile (FAP)” or “Data Access Profile (DAP)”, then “New”. Then, the administrator can assign users with specific access levels using the customised FAP and DAP:

### Sample Customised FAP

<b>Functions</b>	<b>Account Enquiry</b>	<b>Fund Transfer</b>	<b>Bill Payment</b>	<b>Payroll &amp; Autopay</b>
User A	✓	✓	x	x
User B	x	✓	x	x
User C	x	x	✓	✓

### Sample Customised DAP

<b>Accounts</b>	<b>Account 1</b>	<b>Account 2</b>	<b>Account 3</b>	<b>Account 4</b>
User A	Full Control	Full Control	No Access	No Access
User B	Enquiry only	No Access	No Access	Enquiry only
User C	Full Control	Full Control	Enquiry only	Enquiry only

## ***Sign-and-Send***

Sign-and-Send allows you to perform transactions more efficiently by combining the “Sign” and “Send” actions in one simple step. In order to use this service, enable “Sign-and-Send” in the user profile, and ensure you meet the following requirements:

### 1. CCB Account Requirements

Your CCB account must allow the approval of bank transactions by one signer.

### 2. User Settings

The user must be assigned with the full function FAP “DEFFAP1”, or a customised FAP which authorises both “Sign” and “Send” actions.

### Important Notice:

Please remember to update or delete user IDs when staff members come or go. If a new staff member with signing rights requires access to CCB, a new signer PIN should be requested at a BEA branch, because each user has a unique profile and user IDs should not be shared between individuals.

## Important Notes for Security in relation to Cyberbanking

These important notes apply to both personal and corporate Cyberbanking services (together referred to as "Cyberbanking"). Please read and adopt the following security precautions before using Cyberbanking:

- (1) Keep your Cyberbanking account number, ATM card number, private key, Digital Certificate password, and Personal Identification Number ("PIN") for all Cyberbanking and ATM channels confidential at all times. Ensure that you (and, where relevant, any Authorised Person) do not disclose or share this information with anyone - including any joint account holder or any financial management software or programs - under any circumstances, and do not transmit this information via email or any instant messaging software/programs. Never assign the same PIN or password for any other service (such as your internet connection, or login for another website).
- (2) Notify The Bank of East Asia, Limited ("BEA") immediately of any actual or possible unauthorised use of your Cyberbanking account number, PIN, or Digital Certificate, and send confirmation in writing to BEA without delay.
- (3) Under no circumstances will BEA use an email, SMS, instant message, phone call, or any other method to ask for your personal information, such as your password, One-time Password ("OTP"), HKID number, date of birth, account/credit card number, credit card expiry date, telephone number, or Cyberbanking account number/user ID. Do not disclose this information to anyone, including but not limited to any person who claims to be an employee or representative of BEA, under any circumstances.
- (4) Contact BEA for confirmation immediately whenever a website or app claiming to originate from BEA looks suspicious to you.
- (5) Do not use apps, programs, or software from untrustworthy sources.
- (6) Only log in to Cyberbanking through [www.hkbea.com](http://www.hkbea.com). Do not click on URLs or hyperlinks embedded in any email, SMS, instant message, QR code, search engine, or any untrusted source to access Cyberbanking. Do not use/install any software or program to access Cyberbanking.

You should access the BEA website by typing [www.hkbea.com](http://www.hkbea.com) into the web browser directly or by bookmarking the genuine website for subsequent access.

- (7) Disable your browser's "AutoComplete" function. On some browsers, this function remembers the data you have input previously. Refer to your browser's "Help" function if necessary.
- (8) Make sure that all other browsers are closed before logging in to Cyberbanking.
- (9) Every time you log in to Cyberbanking, please verify your last login date and time on the homepage. After logging in to the Cyberbanking mobile phone service, check that the "BEA Identity Message" is authentic.
- (10) If any suspicious screens pop up, or any unusual login screen request appears asking you to provide additional personal information, or if your device's network/traffic is unusually slow, you should log out of your internet or mobile phone service/account immediately and scan your device, including but not limited to computers and mobile or tablet devices (together referred to as your "device"), with the most up-to-date version of your virus protection software.
- (11) After you finish a session, make sure to log out of Cyberbanking and the BEA App, and clear your browser cache.
- (12) Check your bank balance and transaction history regularly. Notify BEA immediately if you discover any problems (such as a lost ATM card) or any suspicious transactions and/or unauthorised transactions.

- (13) Never leave your device unattended while using Cyberbanking or let any other person use your Cyberbanking service. Set a passcode for your device that is difficult to guess and activate the auto-lock function. Limit the number of people who can use your device.
- (14) Do not use a public computer or public Wi-Fi to access the Cyberbanking. Choose encrypted networks and remove any unnecessary Wi-Fi connection settings when using Wi-Fi to log in to the Cyberbanking internet service or mobile phone service. Please disable any wireless network functions (e.g. Wi-Fi, Bluetooth, near-field communication (NFC)), or payment apps whenever such functions are unnecessary.
- (15) Take precautions against hackers, viruses, spyware, and any other malicious software when sending and receiving emails, opening email attachments, visiting and disclosing personal/financial information to unknown websites, and downloading files or programmes from websites. Do not browse suspicious websites or click on the hyperlinks and attachments in suspicious emails or messages received through WhatsApp, Line, WeChat, and other e-communities.
- (16) Use proper firewalls, anti-virus software and anti-spyware software, and promptly install the most up-to-date versions to scan your device from time to time to strengthen their security.
- (17) Upgrade your browser and applications to support Transport Layer Security (TLS) encryption or a higher encryption standard, and make sure that the browser option for storing or retaining usernames, PINs, and Digital Certificate passwords is unselected.
- (18) Remove shared files and printers from your computer, especially when accessing the internet via a cable modem, broadband connection, wireless network, or similar setup.
- (19) Change your PIN immediately by selecting a new PIN the first time you use the service, and then destroy all documents that your former PIN is printed on.
- (20) Use a combination of numbers (0 to 9) and letters (A to Z) for your Cyberbanking PIN. Do not use your identity card number, telephone number, date of birth, driving license number, or any commonplace number sequence (such as 987654 or 123456) when choosing your PIN or ATM card/Digital Certificate password. Do not use the same number or alphabet more than twice.
- (21) Memorise your PIN and Digital Certificate password. Do not write them down.
- (22) Keep your PIN and Digital Certificate password separate from your Cyberbanking account number, user ID, and Digital Certificate. Keep your ATM card safe, and do not keep your ATM card and password together.
- (23) Change your PIN and ATM card/Digital Certificate password regularly.
- (24) Check your surroundings before performing any banking transactions, and make sure that no one sees your PIN or Digital Certificate password. Cover the keypad when you enter your PIN on any device, such as a personal computer, mobile device, or other self-service terminal. Check that the protective keypad cover is intact before using any ATM in Hong Kong. If in doubt, please notify BEA immediately.
- (25) Check the authenticity of the BEA website by checking the URL and the Bank's name in its Digital Certificate. A security icon that looks like a lock or key will appear when authentication and encryption is expected. Check the identity of authentication code when you access BEA App.
- (26) Change your PIN immediately if you suspect that you have been deceived by a fraudulent website or email, or through a public Wi-Fi, public computer, third party's device, or any other means (for example, if you fail to log in to a service website after inputting your correct PIN, whether or not any alert messages appear).
- (27) Notify BEA of any change to the information provided to the Certification Authority as soon as such change occurs. BEA shall not in any event be held liable for any loss or damage suffered resulting from or in connection with your failure to do so.
- (28) Do not use your Digital Certificate after it has been cancelled or revoked or has otherwise

become invalid.

- (29) Set a password to protect your Digital Certificate immediately.
- (30) When you receive an SMS with an OTP, verify the accuracy of the transaction details prior to entering the OTP. When you receive our SMS message and/or notification message, verify the accuracy of the transaction details in a timely manner and inform BEA immediately of any suspicious situations. No SMS containing an OTP will be forwarded to any other mobile phone number, even if you have subscribed to an SMS-forwarding service provided by your telecommunications provider in Hong Kong.
- (31) Make sure your Digital Certificate and its private key is non-duplicable and stored in a secure format. Remove the device storing the Digital Certificate from your computer after use.
- (32) Keep your Digital Certificate, ATM Card, bank statements, cheque books, other important documents, and any security device for accessing Cyberbanking in a safe place. If you want to discard any documents that contain your personal information, destroy them first.
- (33) Check the website's privacy policy statement and statement on security safeguards before providing personal data to the website.
- (34) Should you notice any suspicious devices at any ATM (such as micro-skimmers, pin-hole cameras, or fake key pads) or any suspicious activities around you when performing an ATM transaction, cancel your transaction immediately and inform BEA.
- (35) Please count the banknotes instantly after withdrawing cash at an ATM to ensure the accuracy of transaction. You should not take away any banknotes at the cash dispenser or ATM card at the card insertion slot left behind by someone else, and should let the banknotes or ATM card return to the ATM automatically.
- (36) If you intend to withdraw cash at overseas ATMs, you should activate the overseas ATM cash withdrawal function in advance and set a prudent overseas ATM cash withdrawal limit and an activation period. You may also check with BEA in advance whether your ATM card can be used to withdraw cash at your intended overseas destination.
- (37) Use the version of operating system, BEA App, and browser recommended by BEA to access the Cyberbanking. Do not jailbreak or root your mobile device.
- (38) If your device is capable of biometric authentication (e.g. fingerprint recognition), do not let any other person register his/her biometrics on it.
- (39) Avoid installing sideloading apps and/or apps downloaded from third-party sources.
- (40) Keep the operating system and apps installed on your device up to date with the latest security patches.
- (41) Check the storage, battery, and mobile data usage of apps in your device from time to time to see if there are any suspicious apps. Uninstall any suspicious app when necessary.
- (42) Carefully read installation and/or permission requests from websites, apps, and other software and programs. Be wary of any unusual or unnecessary request.
- (43) Consider using the latest versions of security software/programs to scan your device from time to time to strengthen its security.
- (44) Your mobile phone number, email address, and correspondence address must be up to date at all times in order to successfully receive notifications from BEA. Please update your information at any BEA branch immediately following any changes.
- (45) Protect yourself from email scams - verify the sender's identity before you take any action, to avoid being deceived.
- (46) Review and follow the security tips issued by BEA on a regular basis.

For more information on how to ensure your safety when using internet banking, please visit the website of:

The Hong Kong Association of Banks  
The Hong Kong Monetary Authority

## Frequently Asked Questions

### ***Administrators***

**1. I forgot my login PIN. How can I request a new one?**

Please visit any BEA branch to request a new PIN.

**2. How do I reset a user's login PIN?**

Select "User Maintenance" and "User List", then select the user whose password you need to reset. On the bottom right of the user details, click "Reset PIN" to reset the PIN.

**3. I have already reset the user's login PIN, but they still cannot log in successfully. What is the problem?**

Select "User Maintenance" and "User List", then select the user who cannot log in, and ensure that "Internet Login" is set to "Enable". If it needs to be updated, click "Edit" and update accordingly.

**4. How do I reset a user's Signer PIN?**

Please visit any BEA branch to request a new PIN. After returning the PIN acknowledgement letter to BEA, the user can use the new PIN immediately.

**5. Can I make enquiries or perform transactions?**

No, administrators cannot make enquiries or perform transactions. You must log in as a user/signer to access your company's bank accounts.

**6. Where can I obtain more information on CCB functions?**

Please log in to CCB and click "Demo" in the Quick Links area.

**Quick Links**



## ***Normal Users and Signers***

### **1. How do I find out my login details?**

The administrator will provide the following information for you to log in to CCB:

- CCB account no.
- User ID
- Initial login PIN
- PIN mailer which contains the signer PIN (for users with signing rights only)

### **2. I forgot my login PIN. How can I get a new one?**

Ask the administrator to reset your login PIN for you. For security reasons, you will be forced to change the PIN the next time you log in.

### **3. I am a signer and forgot my signer PIN. How can I get a new one?**

Inform the administrator and he/she will go to the branch and request a new signer PIN for you.

### **4. Can I change my PIN?**

On the top right hand side of the screen, near the display of your user ID and previous log in information, click on "Settings". There are links for you to change your PINs.

### **5. My colleague has access to functions and accounts that I do not. Is something wrong with my user account?**

CCB supports segregation of duties, and each user is assigned a unique profile. Please contact the administrator if you have questions on the accessibility of your user ID.

### **6. Where can I obtain more information on CCB functions?**

Log in to CCB and click the "Play" button in the Tools panel on the right hand side.



## Service Overview

### *Internet Banking*

Service Type	Function(s)
Account enquiry	<ul style="list-style-type: none"> <li>- Account balance</li> <li>- Account summary</li> <li>- Today's activity</li> <li>- Account history</li> <li>- Bill position</li> <li>- Credit limit</li> </ul>
Fund transfer	<ul style="list-style-type: none"> <li>- Fund transfer to BEA HK account</li> <li>- Fund transfer to BEA China account</li> </ul>
Remittance	<ul style="list-style-type: none"> <li>- Telegraphic transfer</li> <li>- HKD/USD/CNY CHATS</li> <li>- Electronic clearing (HKD)</li> </ul>
Bill payment	<ul style="list-style-type: none"> <li>- Bill payment</li> <li>- E-bill payment</li> </ul>
Time deposit	<ul style="list-style-type: none"> <li>- Deposit enquiry</li> <li>- Placement</li> <li>- Uplift</li> <li>- Renewal (single or multiple)</li> <li>- Cancel renewal instruction</li> </ul>
Liquidity management	<ul style="list-style-type: none"> <li>- Balance sweeping</li> <li>- Zero balancing</li> </ul>
Payroll and autopay	<ul style="list-style-type: none"> <li>- Payroll</li> <li>- Autopay</li> <li>- Collection</li> <li>- Upload MAS/ISS file</li> </ul>
Mandatory Provident Fund ("MPF")	<ul style="list-style-type: none"> <li>- Online remittance statement</li> <li>- Upload MPF file</li> <li>- Contribution enquiry</li> <li>- Latest constituent fund price</li> <li>- Monthly investment summary</li> <li>- Quarterly MPF newsletter</li> </ul>
Trade services	<ul style="list-style-type: none"> <li>- Letter of credit application</li> <li>- Letter of credit amendment</li> </ul>
Cheque	<ul style="list-style-type: none"> <li>- Cheque status enquiry</li> <li>- Cheque book request</li> <li>- Stop cheque</li> <li>- Cheque image request</li> </ul>
e-Cheque	<ul style="list-style-type: none"> <li>- e-Cheque book request</li> <li>- e-Cheque issuance</li> <li>- e-Cheque presentment</li> <li>- e-Cheque issuance/presentment enquiry</li> <li>- Stop e-Cheque</li> </ul>

Statement/Advice	<ul style="list-style-type: none"> <li>- Request statement</li> <li>- View e-statement</li> <li>- View e-advice</li> </ul>
------------------	--

Service Type	Function(s)
Download	<ul style="list-style-type: none"> <li>- Download account/merchant transaction records</li> <li>- Download forms</li> <li>- Download new release of MAS</li> </ul>
Rate enquiry	<ul style="list-style-type: none"> <li>- HKD deposit rate</li> <li>- Foreign currency ("FCY") deposit rate</li> <li>- FCY note exchange rate</li> <li>- FCY telegraphic transfer exchange rate</li> <li>- Gold price</li> <li>- Prime rate</li> <li>- Interbank offer rate</li> </ul>

To activate a service, please visit any BEA branch.

### **Mobile Banking**

Service Type	Function(s)
Account enquiry	<ul style="list-style-type: none"> <li>- Account balance</li> <li>- Today's activity</li> <li>- Account history</li> </ul>
Fund transfer	<ul style="list-style-type: none"> <li>- HKD fund transfer to associated and pre-designated accounts</li> </ul>



## Service Hours

Service	Service Hours <sup>1</sup>
Account enquiry <sup>2</sup> - Current Account - Multi-currencies Statement Savings Account - Hong Kong Dollar Savings Account - Foreign Currency Savings Account - Time Deposit Account (Deposit enquiry)	24 hours
Rate enquiry - Exchange rate - Deposit rate - Gold price - Prime rate - Interbank offer rate	24 hours
Change PIN	24 hours
Fund transfer - Current Account (HKD) - Multi-currencies Statement Savings Account (HKD) - Hong Kong Dollar Savings Account	24 hours
Fund transfer - Current Account (CNY) - Multi-currencies Statement Savings Account (CNY)	Mon - Fri: 9:00 a.m. - 5:00 p.m. Sat : 9:00 a.m. - 1:00 p.m.
Fund transfer <sup>3</sup> - Current Account (USD) - Foreign Currency Savings Account - Multi-currencies Statement Savings Account (Foreign Currencies)	Mon - Fri: 9:00 a.m. - 7:00 p.m. Sat : 9:00 a.m. - 1:00 p.m.
Fund transfer to BEA China account <sup>4</sup>	Mon - Fri: 9:00 a.m. - 3:00 p.m.
Bill payment <sup>5</sup>	24 hours
E-bill payment <sup>6</sup>	24 hours
Time deposit - Deposit enquiry - HKD placement and uplift - FCY placement and uplift - Add or edit maturity instruction	24 hours Mon - Sat: 9:00 a.m. - 7:00 p.m. Mon - Fri: 9:00 a.m. - 7:00 p.m. Mon - Sat: 9:00 a.m. - 7:00 p.m.
Telegraphic transfer (HKD and foreign currencies)	Mon - Fri: 9:00 a.m. - 5:00 p.m.
Telegraphic transfer (CNY)	Mon - Fri: 9:00 a.m. - 2:00 p.m.
HKD/USD/RMB CHATS	Mon - Fri: 9:45 a.m. - 4:00 p.m.
Electronic clearing	24 hours
Trade services - Letters of credit	24 hours
MPF remittance statement	24 hours

<b>Service</b>	<b>Service Hours<sup>1</sup></b>
Payroll and autopay - HKD - CNY - Collection (HKD only)	Mon - Sat: 9:00 a.m. - 7:00 p.m. Mon - Fri: 9:00 a.m. - 7:00 p.m. Mon - Sat: 9:00 a.m. - 6:00 p.m.
Bill position enquiry Credit limit utilisation enquiry	Mon - Fri: 9:00 a.m. - 6:00 p.m. Sat: 9:00 a.m. - 3:00 p.m.
Statement request - HKD Current, Statement Savings	24 hours
Statement request - USD Current - CNY Current	Mon - Fri: 9:00 a.m. - 6:00 p.m. Sat: 9:00 a.m. - 1:00 p.m.
Cheque status enquiry	Mon - Sat: 9:00 a.m. - 11:00 p.m.
Cheque book request - HKD Current	24 hours
Cheque book request - USD Current - CNY Current	Mon - Fri: 9:00 a.m. - 7:00 p.m. Sat: 9:00 a.m. - 1:00 p.m.
Stop cheque/e-Cheque order	Mon - Fri: 9:00 a.m. - 7:00 p.m. Sat: 9:00 a.m. - 1:00 p.m.
e-Cheque book request - HKD Current - USD Current - CNY Current	24 hours
e-Cheque issuance	24 hours
e-Cheque presentment	24 hours
e-Cheque issuance/presentment enquiry	24 hours
Merchant services - Account transaction download	24 hours
Linked deposit account enquiry	24 hours
Linked deposit rate enquiry - Currency linked deposits - Equity linked deposits - Single/Basket equity linked deposits - with callable and optional kick-in features	Mon – Fri: 9:15 a.m. – 7:00 p.m. Mon – Fri: 9:30 a.m. – 7:00 p.m. Mon – Fri: 10:30 a.m. – 4:00 p.m.
Linked deposit order placement - Currency linked deposits - Equity linked deposits - Single/Basket equity linked deposits - with callable and optional kick-in features	Mon – Fri: 9:15 a.m. – 5:30 p.m. Mon – Fri: 9:30 a.m. – 12:00 noon 1:00 p.m. – 3:30 p.m. Mon – Fri: 10:30 a.m. – 3:30 p.m.

1. All hours expressed in the timetable are based on Hong Kong Time (HKT). The same applies to all expressions of time in all screens, such as account balance screens.
2. For newly-added related accounts, the updated balance enquiry will be effective on the next business day.

3. Fund transfers in the same foreign currency are available 24 hours.
4. Fund transfers to BEA China accounts are only available on working days in both China and Hong Kong.

5. Bill payment processing schedule:

<b>Transaction made</b>	<b>Transaction will be processed</b>
- before 4:00 p.m. from Monday to Thursday	the same day
- after 4:00 p.m. from Monday to Thursday - on Saturday - on Sunday - on a public holiday - when a Typhoon No.8 or higher signal or Black Rainstorm warning is hoisted	the next working day
after 4:00 p.m. on Friday	the first working day of the following week

6. E-bill payment processing schedule:

<b>Transaction made</b>	<b>Transaction will be processed</b>
- before 7:00 p.m. from Monday to Thursday	the next working day*
- after 7:00 p.m. on Thursday - on Friday - before 7:00 p.m. on Saturday	the first working day of the following week
- after 7:00 p.m. from Monday to Wednesday - after 7:00 p.m. on Saturday - on Sunday - on a public holiday	the second working day

\*If a Typhoon No.8 Signal or Black Rainstorm warning is hoisted and remains in force at 9:00 a.m. the next day, the transaction will not be processed until the following working day.

## Daily Withdrawal Limits

### *Internet Banking*

Transaction Type	Withdrawal Limit (per account per day)
To related and associated accounts	HK\$20,000,000 or its equivalent
To pre-designated third party accounts (BEA and other banks)/bill payments <sup>#</sup>	HK\$5,000,000 or its equivalent
To non-designated third party accounts (BEA and other banks)	HK\$1,000,000 or its equivalent
Payroll & Autopay (BEA and other banks)	HK\$3,000,000 or its equivalent

### *Internet Banking with Digital Certificate*

Transaction Type	Withdrawal Limit (per account per day)
To related and associated accounts	No limit*
To pre-designated third party accounts (BEA and other banks)/bill payments <sup>#</sup>	No limit*
To non-designated third party accounts (BEA and other banks)	HK\$2,000,000 or its equivalent
Payroll & Autopay (BEA and other banks)	No limit*

<sup>#</sup>Includes bill payments and high-risk merchant payments. "High-risk" includes payments to all types of merchant except the following: Government or Statutory Organisation, Public Utility, Education (Primary or Secondary School), and Education (Post-secondary or Specialised Institution). The Bank shall have the right to revise the types of merchant that fall under the high-risk merchant category from time to time at its own discretion.

\*There is no daily transaction limit for fund transfers to related accounts, associated accounts, pre-designated third party accounts, or those made via the Payroll and Autopay services using a Digital Certificate. However, you are advised to set an accumulated daily limit for the above-mentioned transaction types for security reasons.

### *Phone Banking*

Transaction Type	Withdrawal Limit (per account per day)
To related accounts	HK\$1,000,000 or its equivalent
To pre-designated third party BEA accounts	HK\$500,000 or its equivalent

## Daily Deposit Limits

Daily deposit limits for non-designated BEA accounts receiving fund transfers through CCB are as follows:

Transaction Type	Deposit Limit for Non-designated BEA Account (per account per day)
From CCB accounts	HK\$1,000,000 or its equivalent
From CCB accounts with a Digital Certificate	HK\$1,000,000 or its equivalent

## Service Hotlines

Hotlines	Service Hours
Corporate Cyberbanking Enquiry Hotline (852) 2211 1321	Mon - Fri: 9:00 a.m. - 9:00 p.m. Sat: 9:00 a.m. - 5:00 p.m.
Lost PIN Reporting Hotline (during office hours) (852) 2211 1345  During non-office hours, please dial (852) 2211 1862	Mon - Fri: 9:00 a.m. - 9:00 p.m. Sat: 9:00 a.m. - 5:00 p.m.
MPF Enquiry Hotline (852) 2211 1777	Mon - Fri: 9:00 a.m. - 7:00 p.m. Sat: 9:00 a.m. - 1:00 p.m.