Corporate Internet Banking/ Corporate Mobile Banking / Bank-Enterprise Direct Link Service Guide (English version)

NCB 南洋商業銀行

Table of Contents

1. Corporate Internet Banking 3

1.1. Introduction 3

1.2. Account Activation and Corporate Internet Banking Login 21

1.3. Security Device 25

1.4. Operator Management 49

1.5. Process Management 51

1.6. Electronic Notification Settings 62

1.7.Service Management 64

1.8. Security Information 67

2. Corporate Mobile Banking 68

2.1. Corporate Mobile Banking Service Overview 68

2.2. Mobile Security Device 72

2.3. How to Conduct Transactions Using Corporate Mobile Banking 78

2.4. Logging into Corporate Mobile Banking 79

2.5. Security Information 81

3. Bank-Enterprise Direct Link Services 84

3.1. Brief Introduction to the Bank-Enterprise Direct Link Service 84

3.2. Security Information 86

4. Technical Support and Queries 87

5.Important matters 87

1. Corporate Internet Banking

1.1. Introduction

1.1.1. Application Methods

Please visit any of our branches and our designated staff will follow up your application. The addresses of branches are listed under "Contact Us" > "Branch Network" > "Branch Address" at our Bank's website www.ncb.com.hk. To enquire application procedures and details, please call NCB Customer Service Hotline at (852) 2622 2633.

1.1.2. System Requirements

Software configuration:

- Microsoft Windows 7 or above; The language used in the system must be the same as that used in the "Corporate Internet Banking"
- For recommended browsers, please refer to our Bank's "Security Information".
- Screen resolution of 1024 x 768 or above.

1.1.3. Service Overview

Functional Module	**Primary Function**	**Secondary Function**
Account Enquiry	Account Information Enquiry	Demand Deposit Account
		Time Deposit

		Account
		Loan Contract
		Business Integrated Financial Account
	Batch Enquiry	
	Statement Enquiry	Electronic Account Statement
		Electronic Consolidated Statement
		Electronic Bills Statement
	E-Notice	
	Account Alias	
Intra Transfer	Creation	
	Batch Voucher Creation	
	Authorisation	
	Batch Authorisation	
	Transaction Enquiry	

	Template	Creation
		Modification
	Drafts	
	Voucher Modification	
	Batch Transaction Inquiry	
	Batch Voucher Modification	
	Pre-set Instruction Modification	
	Regular Transaction Maintenance	
Transfer/Remittance	Creation	Transfer to NCB
		Remittance to Local Bank
		Remittance to Overseas
		FPS
	Batch Voucher	Transfer to NCB
		Remittance to Local

Creation	Bank
	Remittance to Overseas
Authorisation	
Batch Authorisation	
Transaction Inquiry	
Batch Transaction Inquiry	
Template	Creation
	Modification
Drafts	
Voucher Modification	
Batch Voucher Modification	
Pre-set Instruction Modification	
Regular Transaction Maintenance	

	Manage Registered Third Party Accounts	Creation
		Authorisation
		Enquiry
Autopay	Autopay-out	Make Autopay-out Document
		Review Autopay-out
		Recall Documents
		Modify/Delete Documents
		Changing of Document Reviewer
		Amount Limit Query
	Payroll Deduction	Make Autopay-in Document
		Autopay-in Authorisation
		Recall Documents
		Modify/Delete Documents
		Changing of

		Document Reviewer
		Amount Limit Query
		Make Autopay-in Document
	Transaction Inquiry	Autopay-out Transaction Inquiry
		Autopay-in Transaction Inquiry
	Batch Payment Cancellation	
	Customer Information	
Currency Exchange	Exchange Rate Inquiry	
	Creation	
	Authorisation	
	Result Enquiry	
	Voucher Modification	
International Business	Import Credit	Issue
		Amend
		Workflow

	Deal Search
	Information Maintenance
Export Credit	Transfer LC Issue
	Transfer LC Amend
	Workflow
	Deal Search
	Information Maintenance
Issue Guarantee/Standby LC	Issue
	Amend
	Workflow
	Deal Search
	Information Maintenance
Receive Guarantee/Standby LC	Deal Search
Import Collection	Deal Search
Export Collection	DP/DA Collection
	Workflow

		Deal Search
		Information Maintenance
Time Deposit	REWARD-PLUS Time Deposit	Deposit Interest Rate Inquiry
		REWARD-PLUS Set Up
		Set Up Authorisation
		Voucher Modification
		Transaction Flow Inquiry Trade Melt Monthly Statement
	Time Deposit	Time Deposit Rate Enquiry
		Time Deposit Placement
		Placement Authorisation
		Maturity Instruction Amendment

		Maturity Instruction Amendment Authorisation
		Transaction Inquiry
		Voucher Modification
Featured Service	Cheque Book Request	
	Faster Payment System	FPS Registration and Management
		FPS Account Enquiry
	Direct Debit Authorisation	Manage
		Enquiry
		Authorise
		Batch Authorise
		Authorisation Status
	e-Statement/e-Advice Management	
	Stop Payment of Cheques	
	Deposit e-Cheque/Cashier'	

	Order	
Management	Operator Management	Operator Maintenance
		Permissions Assign
	Procedure Management	Default Procedure
		Customized Procedure
		Setting
		Limit Enquiry
	E-Alert	User Management
		E-Alert Management
	Login Name Setting	
	Corporate Mobile Banking Management	
	Dual Master Authorisation	
Customer Service	Log Enquiry	
	Change Password	
	Security Device	Synchronize Security Device

		Activate Security Device
		Report Security Device as Lost
Payment	Bill Payment	
	Pay New Bill	
	Authorisation	
	Pre-set Instruction Modification	
	Transaction Enquiry	
	Merchant Reconciliation File Download	
MPF	MPF Contribution File Upload	
	MPF Contribution File Authorisation	
	Pay Contributions	
	Contributions Authorisation	

	MPF Login	
Funds	Redemption	
	Transaction Records	
	Portfolio Enquiry	
	Fund Information	
Securities	HK Securities Trading	
	A Shares Securities Trading	
	Update/ Delete Order	
	Transaction Record	
	Position Enquiry	
	Monthly Savings Plan Enquiry	
	Corporate Action Enquiry	
	Stock Deposit Enquiry	
	eIPO Enquiry	Allotment Result
		Application Enquiry

	Quote Service Plan	Quote Service Plan Register
		Quote Service Plan Fee Enquiry
	Price Alert	Price Alert Register
		Price Alert Setting
	Schedule of Charges and Others Stock Information	 HK Securities A shares Securities Warrant & CBBC Information Streaming

1.1.4. Account Enquiry

- Account Information Enquiry-Clients may enquire your demand deposit accounts, time deposit accounts, loan contract accounts, asset and liability overviews, and business integrated financial account.
- Batch Enquiry- Clients may enquire account details in batches. When five or more accounts are chosen for detailed enquiry, the enquiry will be conducted and downloaded in a batch manner.
- Statement Enquiry- Clients may enquire statements, comprehensive monthly statements, and trade finance monthly statements.

- Electronic Notifications- Clients may access their electronic notifications.
- Account Alias- Clients may set and enquire their account aliases. Corporate clients can establish aliases for bank accounts linked to the corporate online banking, facilitating easier inquiries.

1.1.5. Corporate Internal Transfers

- Enterprises can realise transfers between registered accounts of "Corporate Internet Banking".
- Support 24/7 transactions.
- Support forward dated and standing transactions.
- Support single and batch transactions.

1.1.6 Transfer/Remittance

- Transfer to NCB

You can transfer funds directly to other individuals' NCB accounts.

- Transfer to Other Local Bank Accounts

You can transfer funds in HKD, USD, EUR and CNY to other banks' accounts via the Real-Time Gross Settlement System of Hong Kong Interbank Clearing Limited by Express Transfer (RTGS/CHATS). The beneficiary bank can receive the funds immediately under normal circumstances.

- Transfer to Global Accounts

Through SWIFT and Faster Payment System (FPS), you can transfer funds in different currencies to different banks around the globe.

- FPS Transfers

Through FPS, you can transfer funds in HKD and CNY to other local banks' accounts. You can get your funds transferred to the account at the receiving bank instantly under normal circumstances.. Additionally, it supports mobile phone numbers, email addresses, or FPS identifier as account identifiers.

1.1.7 Proxy Payment and Payroll Deduction

- NCB Corporate Internet Bankingarranges for customers to deposit specified amounts into designated accounts at specific dates in batches, simplifying bulk payments, reducing administrative costs, and avoiding additional expenses due to delayed payments.
- The collection service assists customers in electronically collecting a large number of receivables, supporting deductions from specified bank accounts at NCB or other banks on specified dates.

1.1.8. Currency Exchange

Offer cross-currency exchange services for HKD, CNY, and more than 10 different foreign currencies.

1.1.9. Time Deposits

- Choose suitable time deposit services.
- Support reviewing of finalized time deposits.
- Amend maturity instructions for opened but yet-to-mature time deposits.
- The drawer can retract unreviewed documents, or modify or delete

documents with unsuccessful reviews.

1.1.10. International Business

NCB provides trade financing services for cross-border trading enterprises:

- Import Services- Opening letters of credit, import collections, issuing guarantees/standby credits.
- Export Services-Letter of credit notifications, letter of credit transfers, export collections.

1.1.11. Specialized Services

Chequebook Issuance: The requested chequebook and crossed chequebook will be posted by ordinary mail while the bearer chequebook will be posted by registered mail. The fees of registered mail will be debited directly from your current account.

Direct Debit Authorization: Clients can set up one-time direct debit instructions to authorise payments from a designated account to specified payees (merchant or institution).

E-Statements:

- Clients can view, print, and download monthly consolidated e-Statements for the past 24 months (accumulating up to 7 years), with other monthly e-Statements and daily e-Statements/e-Advice retained for up to 13 months and 90 days, respectively.
- Handles the application for various e-Statements.
- Clients can modify e-Statement settings, such as language and email

alerts.

You can submit request for re-issuance of paper statement.

Faster Payment System (FPS):

- This service allows third parties to transfer funds to you using the mobile phone number or email address recorded in the bank without knowing your bank account number. The transfer can come from the bank or other local banks providing similar services.
- Upon successful registration for the faster payment service, you can also use QR codes for general payment and receipt services.

1.1.12. Client Service

(1) Contact Us. Clients can create inquiries and receive replies, accessing contact phone numbers and addresses for our branches.

(2) Password Modification. You can change the operator password (including supervising and regular operators). Password rules: passwords cannot contain operator codes; must be 6 to 12 characters long, a combination of upper and lower case letters, and numbers; cannot be the same as the previous password; cannot include three or more consecutive identical digits or letters.

(3) Security Device (Token). Operators can synchronize and activate the Security Device, see 1.4.4 and 1.4.5 for details.

1.1.13. Bill Payment

- Bill Payment Service enables you to settle your bills online in HKD, CNY

and USD. You can select the merchants on the list and make the payment at once or pre-set a payment instruction..

- Bills successfully paid are automatically registered for future payments under the registered bill section.

1.1.14. Mandatory Provident Fund (MPF)

Clients can preset default instructions for MPF contributions.

1.1.15. Funds

- You can enquire the balance of your Funds under custody and in the name of bank nominees held under designated investment account.
- You can enquire the same-day or the past year's transaction record and transaction status for funds subscribed via our branches, Corporate Internet Banking or Corporate Mobile Banking.
- You can view comprehensive market information, including fund prices, asset allocations, fund performances, offering documents, etc.

1.1.16. Securities

- Securities Trading

1. Conduct securities trading, amend or cancel trading orders and enquire the status of your trading orders.

2. Corporate Mobile Banking accept corporate action instructions for relevant services, including Right Subscription, Open Offer, Share Offer, Preferential Subscription, Dividend Option and Offer (subject to the terms and conditions of the corporate actions).

1. You can deposit stock via Corporate Mobile Banking.
2. Real-Time Stock Quote and Stock Price Alert Service.

- Monthly Stock Saving Plan

1. You can choose more than ten kinds of stocks as long-term investments under same plan via Corporate Mobile Banking.
2. You can shell the fractional shares under within monthly stock saving plan with market price via Corporate Mobile Banking, Corporate Internet Banking and Mobile Investment Line.
3. Exempt custodian fee and collecting fees for shareholders' equity(stock dividend).

- Subscription for new stock services

1. You can subscribe for new stock with yellow sheet via Corporate Mobile Banking.
2. If using yellow sheet to subscribe, the rationed shares will be deposited in security account and it will be available for sale until the new shares listed.

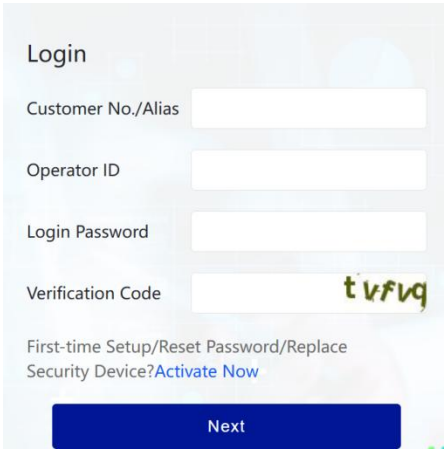
1.2. Account Activation and Corporate Internet Banking Login

1.2.1. Account Activation

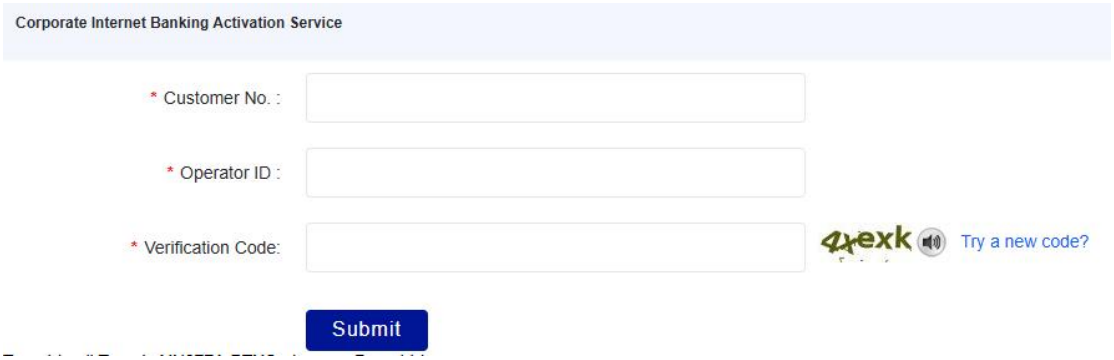
After clients apply for an operator account at the branch, or reset their login

password, or change the Security Device, the operator account status remains as "pending activation". Operators need to successfully activate the account on the Corporate Internet Bankingplatform before accessing Corporate Internet Bankingor Mobile Banking.

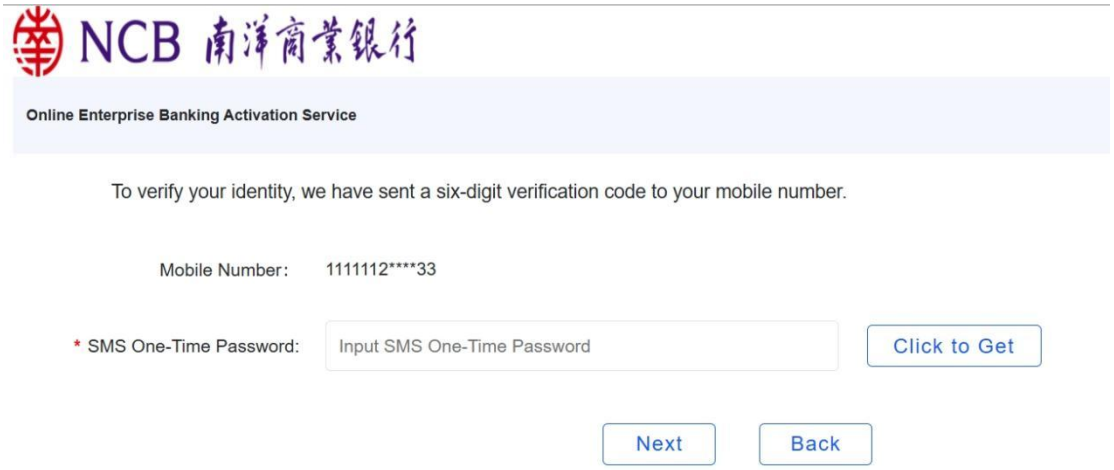
Step 1 - On the login page of Corporate Online Banking, select "Activate Now".



Step 2 - Input your "Client Number", "Operator ID" and "Additional Code", and click "Submit".



Step 3 - Input the SMS verification code received on your bank-registered mobile number, and click "Next".



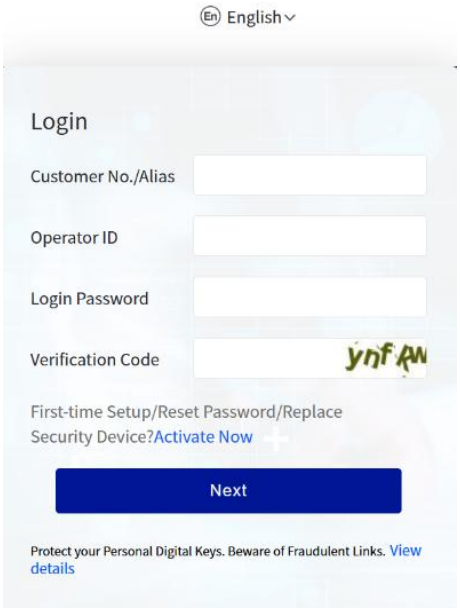
Step 4 - Obtain the "Transaction Confirmation Code" from the security device or mobile security device, enter the "Transaction Confirmation Code" and "Login Password" (the initial password is printed in the password letter/already modified login password), then click "Next" to complete the activation of the operator account.

1.2.2. Logging into Corporate Online Banking

You can access Corporate Internet Banking through NCB website www.ncb.com.hk.

Step 1 - Visit our bank's website www.ncb.com.hk, then select "Login > HK Corporate Online Banking".

Step 2 - Please enter your 「Customer No./Alias」、「Operator ID」、「Login Password」、「Verification Code」 to complete the login process.



If two-factor authentication was activated upon the enterprise's account setup, all enterprise operators logging into the online banking system will additionally need to verify the "Transaction Confirmation Code" obtained from security device or mobile security device.

1.3. Security Device

Our Bank has adopted the "Security Device" as the two-factor authentication tool to enhance customer protection. All online transactions conducted through "Corporate Internet Banking" should be verified by a one-time password generated by the "Security Device". Online transactions can be categorised into two transaction types: "General Transaction" and "Designated Transaction". The verification methods provided by the "Security Device" for these two transaction types are different. To use the "Security Device", customers should apply the "Security Device" and it can be used until customers complete the activation according to the 1.2.1 account activation process.

1.3.1. Application Method

Authorised personnel from the enterprise can visit any of our branches to apply for a Security Device for supervising or regular operators. After identity authentication by the handling staff, the Security Device will be mailed to the client.

1.3.2. Synchronizing the Security Device

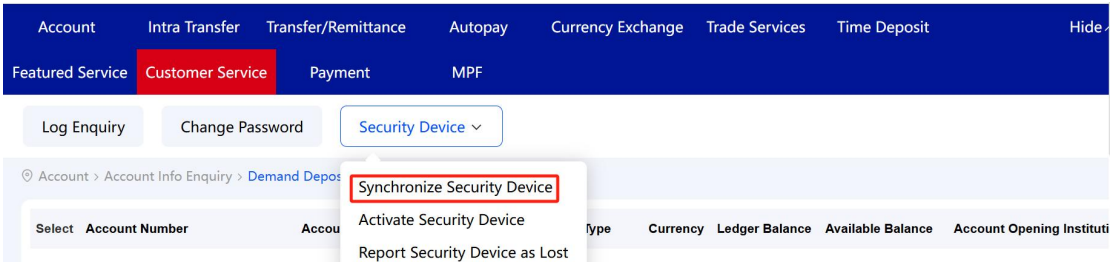
Each Security Device has an embedded clock. Prolonged inactivity, low battery, or environmental factors might cause a significant deviation between the embedded clock and the Security Device server time, resulting in the device's inability to authenticate transactions.

You can correct the clock deviation by "Synchronizing the Security Device"

via Corporate Internet Banking.

Step 1 - Log in to Corporate Internet Banking and select "Client Service > Security Device > Synchronize Security Device".

Step 2 - Obtain the "Security Token" twice consecutively from the "Security Device" and input it twice to complete the synchronization.



1.3.3. Reset Status of Security Device

Five consecutive incorrect entries of the security token or transaction confirmation code will lock the Security Device. The operation from enterprise can reset the Security Device status through below mentioned methods.

Method 1: Master operator can reset the security status via Corporate Internet Banking through "Service Management" > "Operator Management" > "Operator Maintenance"

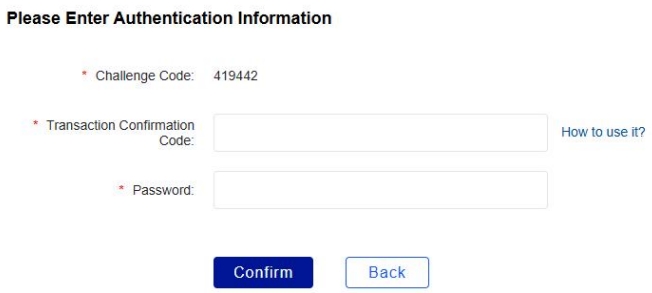
Method 2: Customers can visit any of branches to apply for resetting security device status, the handling person can help customers reset the security device status and unlock it after authentication.

1.3.4. Re-Activation of the Security Device

When a client initiates the mobile security device through Corporate Mobile Banking, the system will automatically deactivate the Security Device (if any). If the client wishes to re-activate the Security Device, they can do so through Corporate Online Banking.

Step 1 - Log in to Corporate Internet Banking and select "Client Service > Security Device > Activate Security Device".

Step 2 - Enter the challenge code prompted on the Security Device page to obtain the "Transaction Confirmation Code". Finally, input the "Transaction Confirmation Code" and "Login Password" into Corporate Online Banking. After submission, the Security Device can be re-activated.



When clients re-activate the Security Device through Corporate Online Banking, the system will automatically deactivate the mobile security device (if any).

1.3.5 Reporting loss of Security Code Device

If losing the security code device, customers can report the loss of it via Corporate Internet Banking through "Customer Service" > "Security Code Device" > " Report loss of Security Code Device". Otherwise, please contact

master operator to report the loss via Corporate Internet Banking through " Service Management" > "Operator Management"> "Operator Maintenance". In case impacting customers' business operations, please obtain the brand-new authentication tools through below mentioned methods after reporting the loss of the security devices.

1. Customers can activate the mobile security code device via Corporate Mobile Banking and consider it as dual authentication tool.
2. Please visit any of branches to apply for new security code device and we will send you new one after the handling person complete the authentication.

1.3.6. Authorizing Transactions

There are two methods for 2FA authentication via the "Security Device". One is direct generation of the "Security Token" by the device, where clients input the "Security Token" for transaction authentication; alternatively, clients input a system-generated 6-digit random challenge factor (a random 6-digit number provided on the transaction page) into the "Security Device" to obtain the corresponding "Transaction Confirmation Code" for transaction authentication.

For the scenarios described below, both initiating and reviewing transactions require 2FA authentication.

Table 1 2FA Transaction Table

No.	Transaction Type	Transaction Data (Challenge Factor)	Password Type	Electronic Channel
1	Corporate Account Activation (First Login/Password Reset/Security Device Replacement)	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
2	Corporate Internet BankingLogin (Setup of Accounts Requiring Two-Factor Authentication)	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
3	Corporate Internal Transfer Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking, Corporate Mobile Banking

4	Corporate Internal Transfer Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking, Corporate Mobile Banking
5	Batch Corporate Internal Transfer Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
6	Batch Corporate Internal Transfer Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
7	Transfer/Remittance Initiation	Randomly Generated 6-digit Numeric	Transaction Confirmation Code	Corporate Online Banking, Corporate Mobile Banking

		Challenge Factor		
8	Transfer/Remittance Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking, Corporate Mobile Banking
9	Batch Transfer/Remittance Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
10	Batch Transfer/Remittance Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
11	Proxy Payment Initiation	Randomly Generated	Transaction Confirmatio	Corporate Online Banking

		6-digit Numeric Challenge Factor	n Code	
12	Proxy Payment Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
13	Proxy Deduction Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
14	Proxy Deduction Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking

15	Currency Exchange Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking, Corporate Mobile Banking
16	Currency Exchange Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking, Corporate Mobile Banking
17	Time Deposit Account Opening Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking, Corporate Mobile Banking
18	Time Deposit Account Opening Review	Randomly Generated 6-digit Numeric	Transaction Confirmation Code	Corporate Online Banking, Corporate Mobile Banking

		Challenge Factor		
19	Time Deposit Maturity Instruction Change Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking, Corporate Mobile Banking
20	Time Deposit Maturity Instruction Change Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking, Corporate Mobile Banking
21	Reward-Plus Time Deposit Account Opening Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
22	Reward-Plus Time Deposit Account	Randomly Generated	Transaction Confirmatio	Corporate Online

	Opening Review	6-digit Numeric Challenge Factor	n Code	Banking
23	Scheduled Cash Pooling Single Collection Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmatio n Code	Corporate Online Banking
24	Scheduled Cash Pooling Single Collection Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmatio n Code	Corporate Online Banking
25	Scheduled Cash Pooling Periodic Collection Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmatio n Code	Corporate Online Banking

26	Scheduled Cash Pooling Periodic Collection Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
27	Scheduled Cash Pool Collection Maintenance Application	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
28	Scheduled Cash Pool Collection Maintenance Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
29	Scheduled Cash Pool Single Disbursement Application	Randomly Generated 6-digit Numeric	Transaction Confirmation Code	Corporate Online Banking

		Challenge Factor		
30	Scheduled Cash Pool Single Disbursement Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
31	Scheduled Cash Pool Periodic Disbursement Application	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
32	Scheduled Cash Pool Periodic Disbursement Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
33	Scheduled Cash Pool Disbursement	Randomly Generated	Transaction Confirmatio	Corporate Online Banking

	Maintenance Application	6-digit Numeric Challenge Factor	n Code	
34	Scheduled Cash Pool Disbursement Maintenance Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
35	Scheduled Cash Pool Fund Submission Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
36	Scheduled Cash Pool Fund Submission Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking

37	Scheduled Cash Pool Submission Maintenance Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
38	Scheduled Cash Pool Submission Maintenance Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
39	Direct Payment Authorization Management	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
40	Direct Payment Authorization Review	Randomly Generated 6-digit Numeric	Transaction Confirmation Code	Corporate Online Banking

		Challenge Factor		
41	Direct Payment Authorization Batch Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
42	Import Letter of Credit Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
43	Import Letter of Credit Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
44	Export Bill of Exchange Initiation	Randomly Generated	Transaction Confirmatio	Corporate Online

		6-digit Numeric Challenge Factor	n Code	Banking
45	Export Bill of Exchange Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
46	International Letter of Credit/Standby Credit Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
47	International Letter of Credit/Standby Credit Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking

48	Export Bill Collection Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
49	Export Bill Collection Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
50	Payment - Bill Payment	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
51	Payment - Bill Registration	Randomly Generated 6-digit Numeric	Transaction Confirmation Code	Corporate Online Banking

		Challenge Factor		
52	Payment Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
53	Mandatory Provident Fund Contribution Initiation	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
54	Mandatory Provident Fund Contribution Review	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
55	Investment Transactions	Randomly Generated	Transaction Confirmatio	Corporate Online Banking,

	(Securities/Fund Trading Operations)	6-digit Numeric Challenge Factor	n Code	Corporate Mobile Banking
56	Account Statement Download	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
57	Monthly Consolidated Statement Download	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
58	Trade Finance Monthly Statement Download	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking

59	Account Alias Setting	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
60	Account Registration Management	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
61	Chequebook Application	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
62	Faster Payment System Account Registration and Management	Randomly Generated 6-digit Numeric	Transaction Confirmation Code	Corporate Online Banking

		Challenge Factor		
63	Cheque Stop Payment	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
64	Electronic Statement/Notification Management	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
65	Customized Process	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
66	Default Process	Randomly Generated	Transaction Confirmatio	Corporate Online Banking

		6-digit Numeric Challenge Factor	n Code	
67	Control Settings	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
68	Electronic Notification User Settings	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
69	Electronic Notification Registration Setting	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking

70	Corporate Mobile Banking Management	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
71	Operator Maintenance	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
72	Operator Rights Assignment	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
73	Login Name Setting	Randomly Generated 6-digit Numeric	Transaction Confirmation Code	Corporate Online Banking

		Challenge Factor		
74	Password Modification	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking
75	Synchronize Security Device (Token)	/	Security Code	Corporate Online Banking
76	Activate Security Device	Randomly Generated 6-digit Numeric Challenge Factor	Transaction Confirmation Code	Corporate Online Banking

1.4. Operator Management

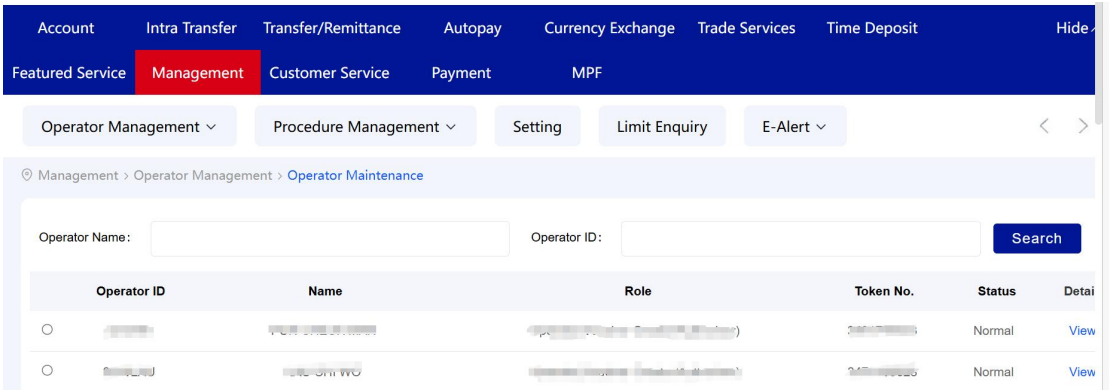
Operators in the Corporate Internet Bankingsystem consist of supervising operators and regular operators. The latter can be categorized into three roles: Maker, Authoriser, and Maker+Authoriser. A corporation can have multiple supervising roles (up to a maximum of 6). The permissions of administrators and regular operators are briefly outlined as follows:

Operator Type	Description
Supervising Operator	They hold service management permissions (operator account management, process configuration, electronic prompt settings, corporate mobile management, dual supervisor approval, login alias configuration), along with permissions to query and review transactions.
Regular Operator (Maker)	They have permissions to input financial transactions, input non-financial transactions, and query.
Regular Operator (Authoriser)	They have permissions to review financial transactions and query.
Regular Operator (Maker+Authoriser)	They simultaneously hold permissions of regular operator (maker) and regular operator (authoriser).

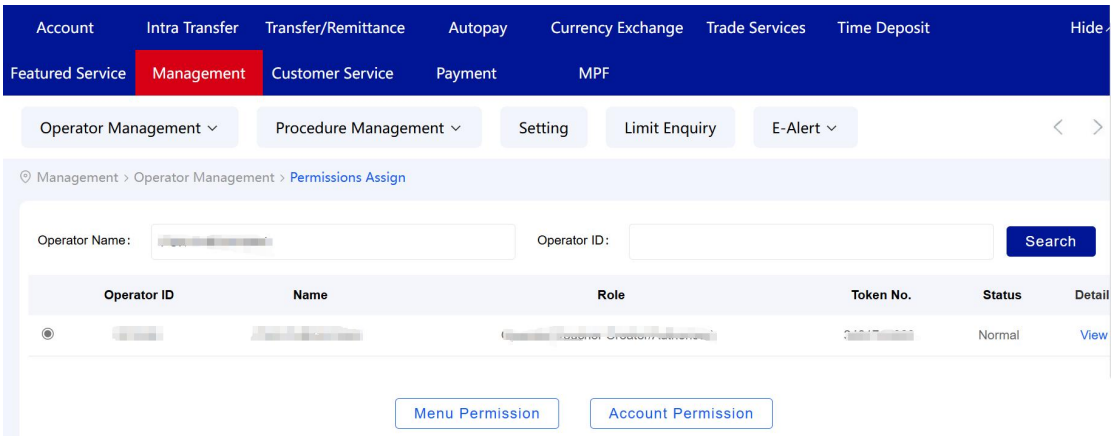
Operator management is the unique operator permissions of corporate supervisors.

(1) Maintenance of Operator Information: Corporate supervising operators can maintain the basic information of regular operators, including name,

identification, operator type, etc. They can maintain the status of operators (activate, deactivate, cancel); and set passwords for regular operators.



(2) Permission Maintenance. Supervising operators can maintain the menu and account permissions for regular operators. Menu permissions refer to the access granted to operators within the menus of Corporate Online Banking/Corporate Mobile. Account permissions refer to the privileges of operators during transactions such as transfers, remittances, currency exchanges, and queries.



1.5. Process Management

The process refers to the operational procedure involving the creation of a transaction by a maker, reviewed by none or multiple authorisers for every

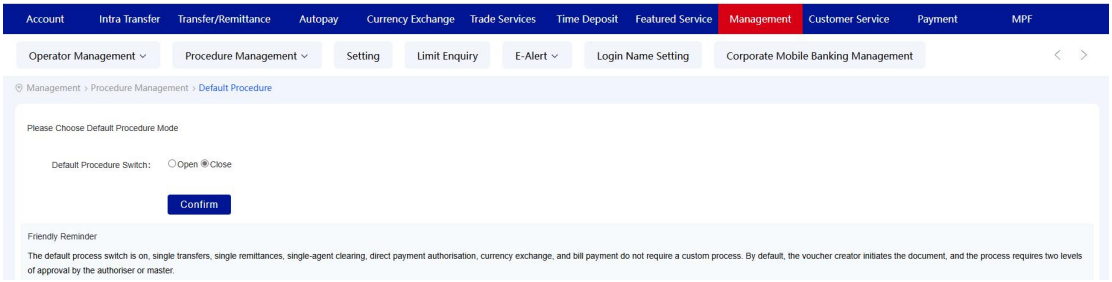
non-query transaction.

Maker Authoriser 1 Authoriser 2 Transaction Successful

All makers fall under the Level Maker category. Corporate supervising operators belong to Level A. Regular Operators with review authorization can set Authoriser levels from Level A to J based on the Corporate supervising operators' settings.

(1) Default Process

When the default process switch is activated, individual internal transfers, individual transfers/remittances, direct payment authorization, foreign exchange transactions, payments, and Mandatory Provident Fund (MPF) transactions do not require a customized process. With the default process switch activated, the default process entails a two-level transaction process: makers initiate transactions while authorisers/supervisors conduct the verification process.



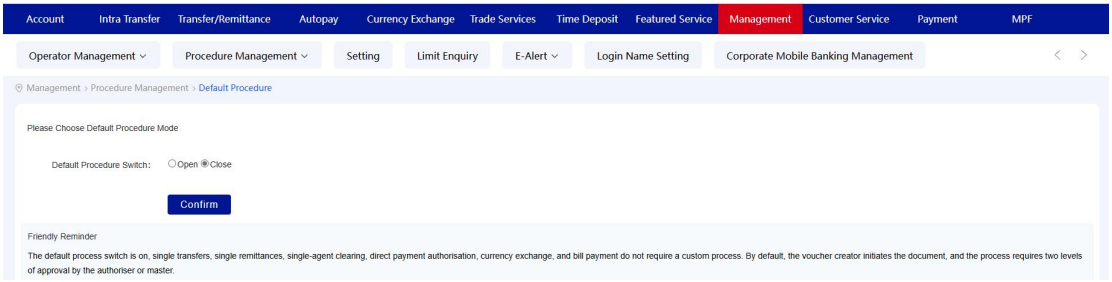
(2) Customized Process

Regardless of whether the default process is enabled or disabled, batch transfers/remittances, scheduled cash pooling, and automatic payment authorization require customized process settings. When the default

process switch is turned off, single transfers/remittances, foreign exchange transactions, and payments can be configured with specific processes.

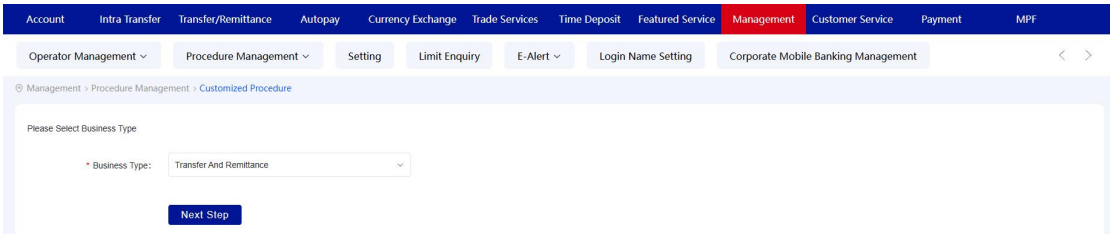
In setting authorisers, up to five monetary ranges can be established. Within each monetary range, multiple levels of authoriser classifications can be selected. Specific authorisers can be designated within a level or left unspecified, allowing any authoriser within that level to conduct verification. Each specific function or account can only have one process configured. Adding a new process is not permitted when an existing process is already in place. Deleting a process renders any incomplete transactions associated with it null and void.

- Turning off the default process. To configure processes for single transfers/remittances and currency exchanges, go to "Process Settings - Default Process", select "Off" and click "Confirm" to disable the default process.

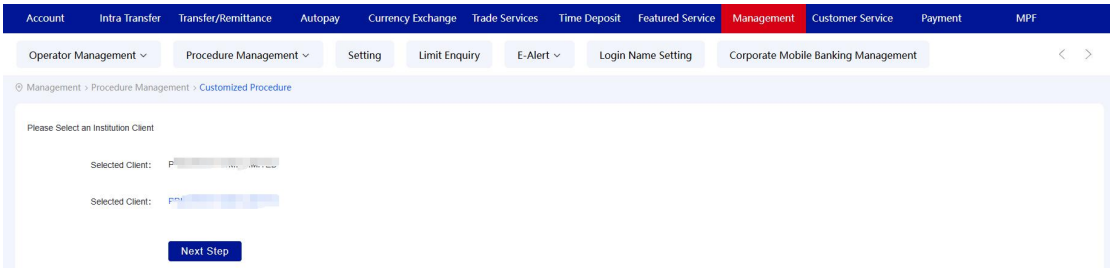


- Setting up single-step processes. A single-step process implies that a transaction only requires the maker's initiation, and upon authorization, the transaction can be executed without further verification. For instance, in the case of a single remittance:

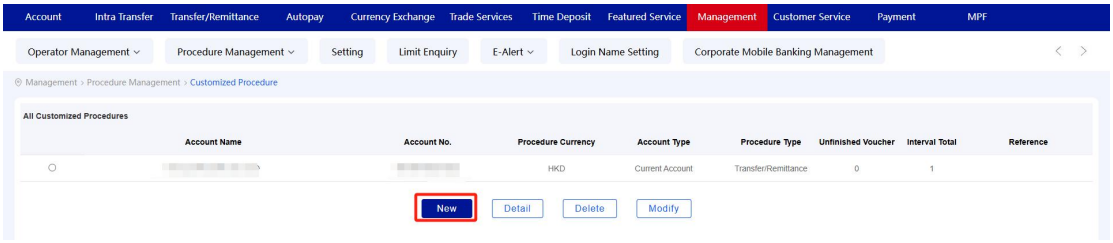
A. Go to Service Management-Process Management-Customized Process and select “Payment Contract”.

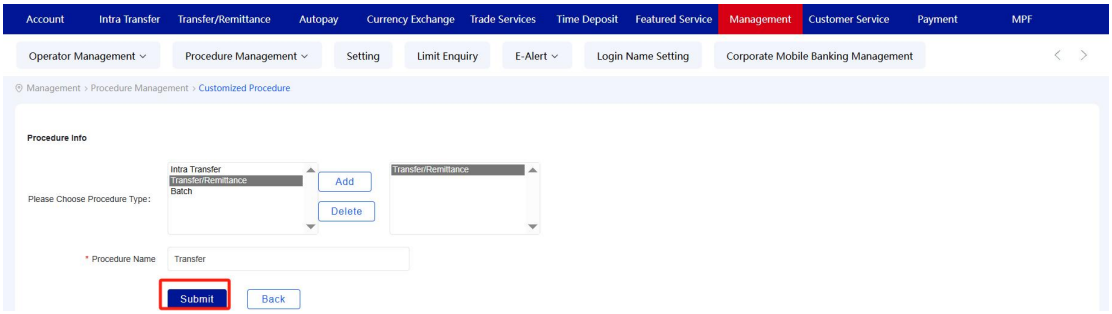


B. Choose the client and click “Next”.

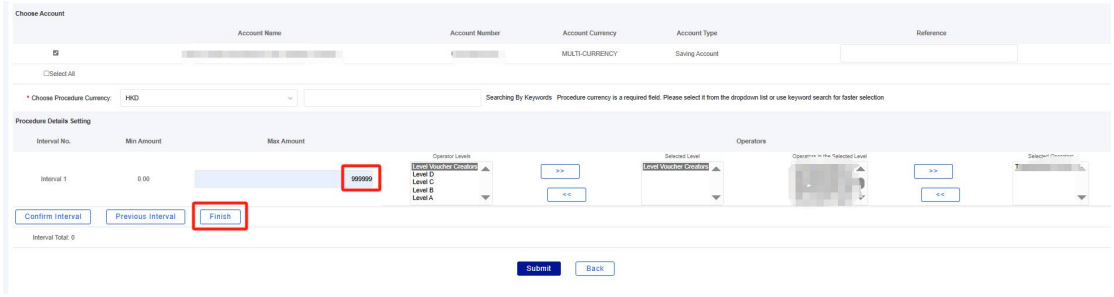


C. Click “Add” to enter the process details page, select the transaction type “Transfer/Remittance” and fill in the process name.

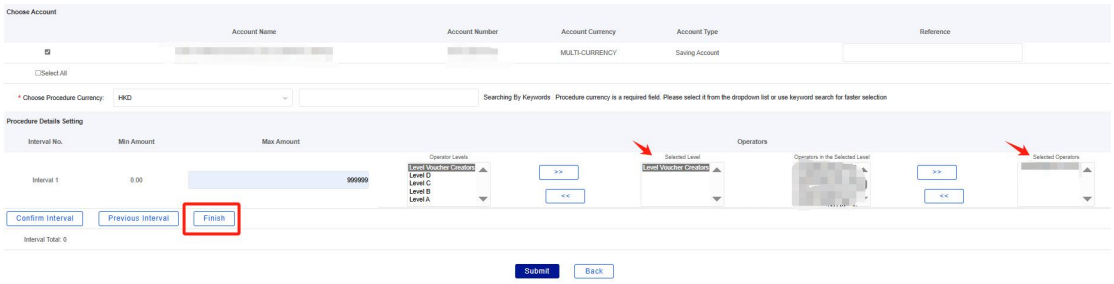




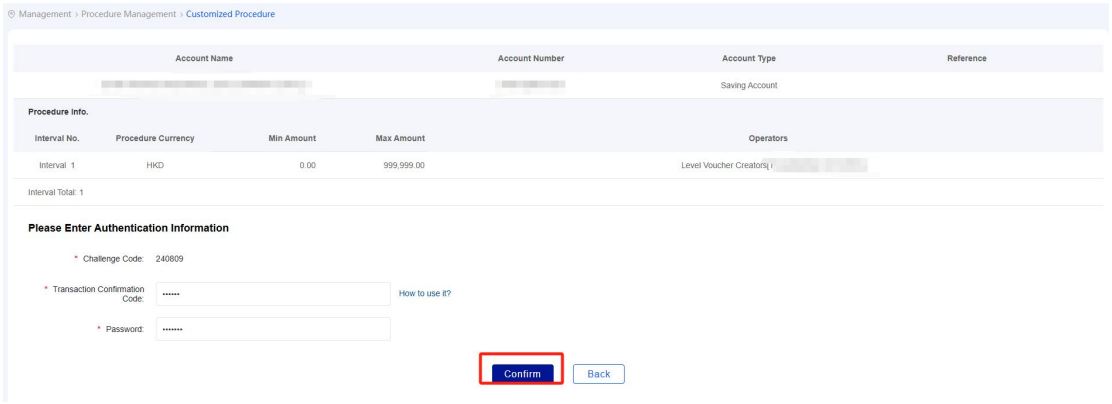
D. Select the debiting account, purpose, and currency for the process.

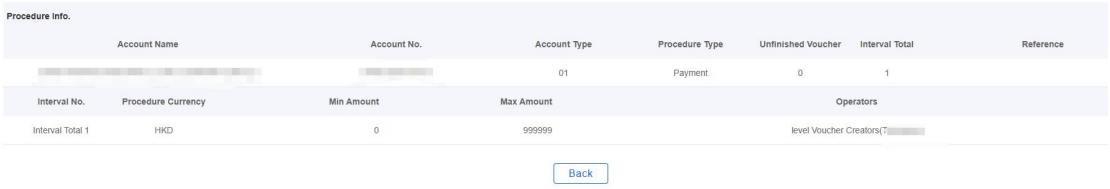


E. Input the maximum amount, select operator level "Level Makers" and click ">>" to move it to the "Selected Operator Level". Then click "Customize Success" and "Confirm". If specific operators need to be designated, select them from the "Operators in the selected operator level" and click ">>".



F. Enter authentication information to complete the setup. When the setting is finished, you can view the configured customized processes.



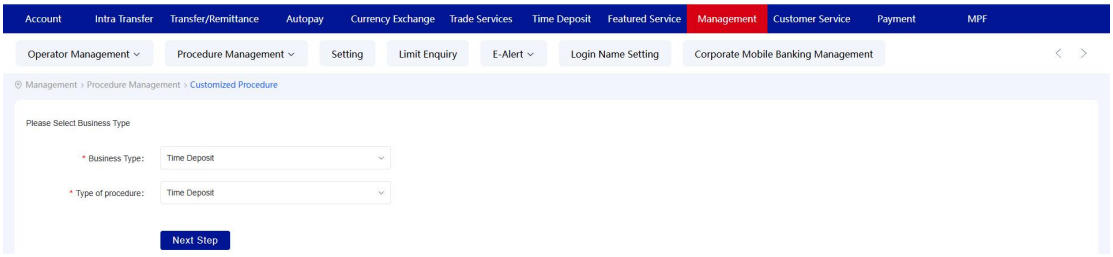


- Setting up two-level (or multi-level) processes. For clients requiring a three-level or higher process, involving two levels of review without hierarchical order, let's take the example of setting up a process for opening time deposits:

Amount Range	Process
0-3,000HKD	Maker -> Transaction Completion
3,000-100,000HKD	Maker -> Level B Authoriser
100,000-5000,000HKD	Maker -> Level B Authoriser -> Level A Authoriser

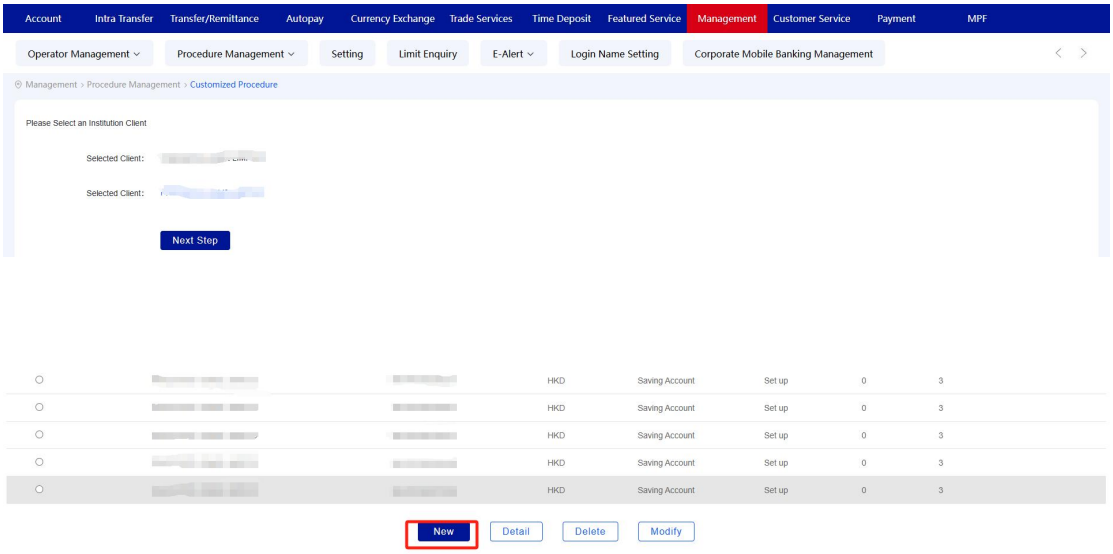
For the 0-1000 HKD process, only the Maker is required to complete and execute the transaction.

A. Go to Process Management-Customized Process, select Time Deposit.

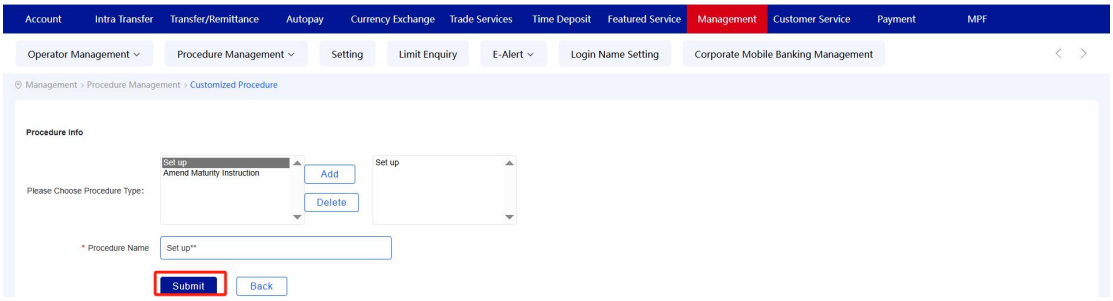


B. Choose the client and click “Next”, then add a new process in the process

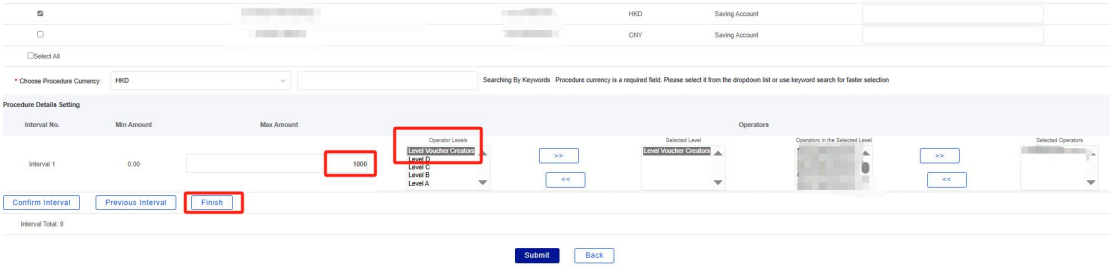
interface.



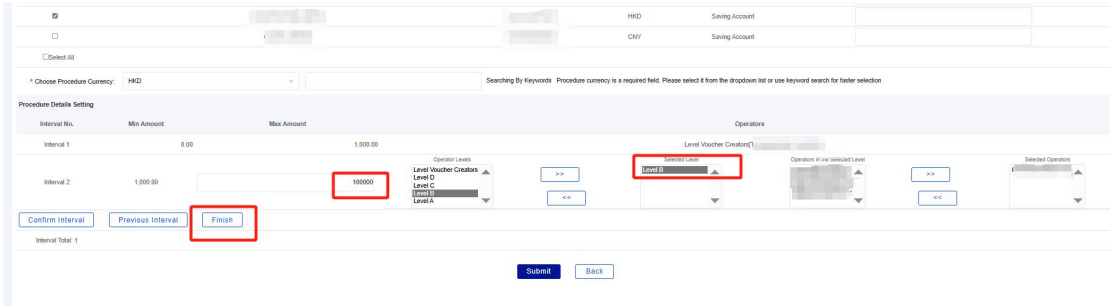
C. In the process configuration information page, select the transaction type as “Opening”, enter the process name, and click “Confirm”.



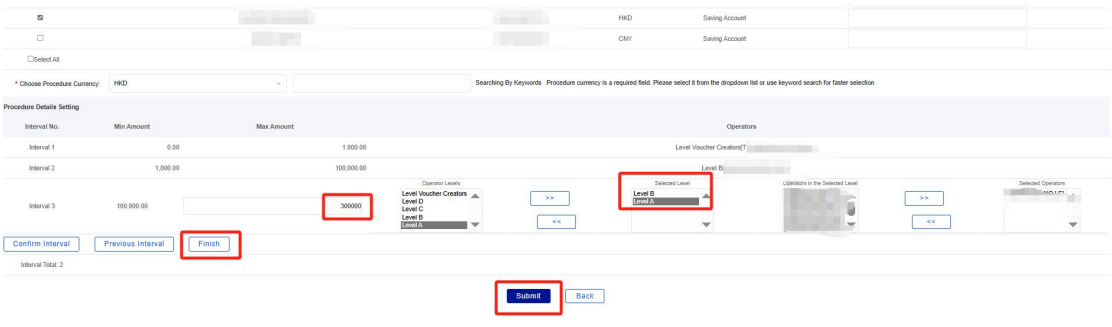
D. Choose the account, fill in the purpose and set the maximum amount, select “Level Makers” to move it to the “Selected Operator Level”, and click “Customize Success”.



E. For the Range 2 maximum amount, choose “Level B and Level A” in the “Operator Level” and click “>>”. Ensure “Level B and Level A” is selected under the “Selected Operator Level” and click “Customize Success”.



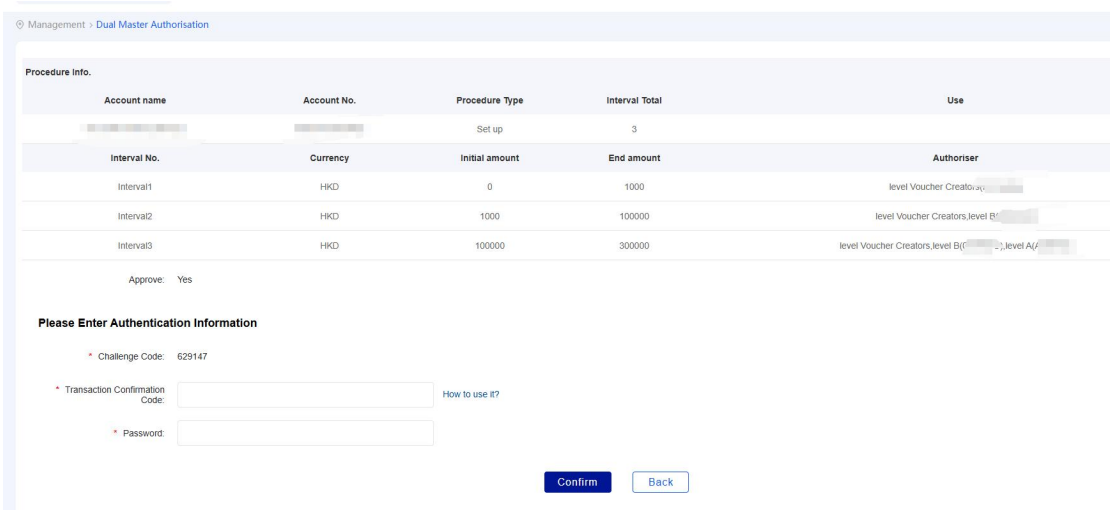
F. For Range 3, fill in the maximum amount and select “Level B” and “Level A” in the “Operator Level”, click “>>”, verify that both “Level B” and “Level A” are selected under the “Selected Operator Level”, and click “Customize Success”.

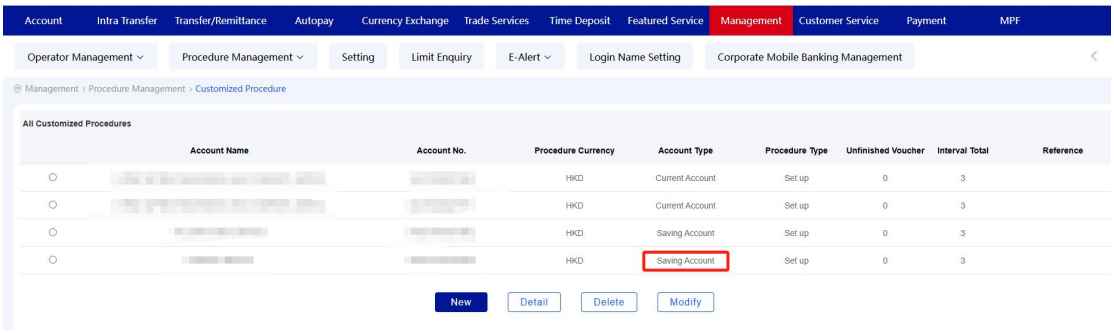


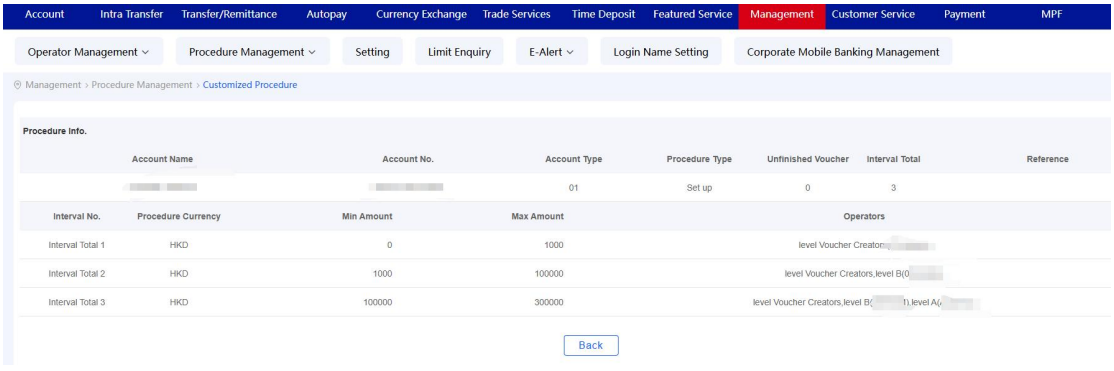
G. Click “Confirm” and enter authentication information to finalize the customized process.

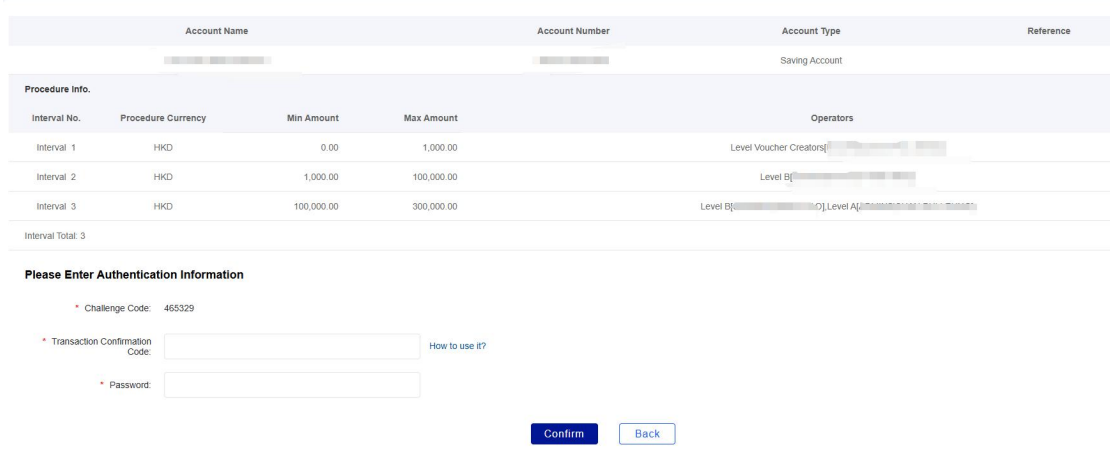
H. Visit “Service Management - Customized Process - Time Deposit” to

review the configured process.





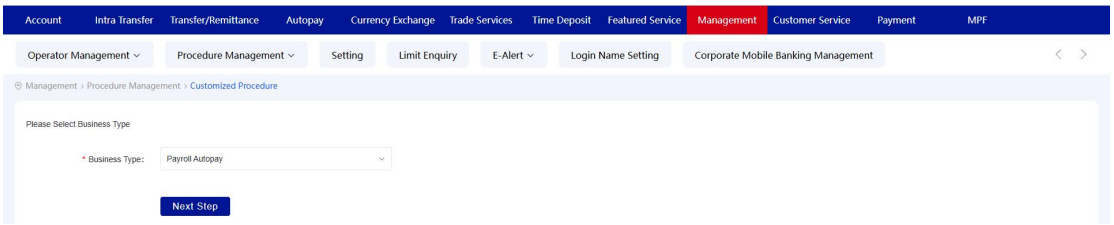




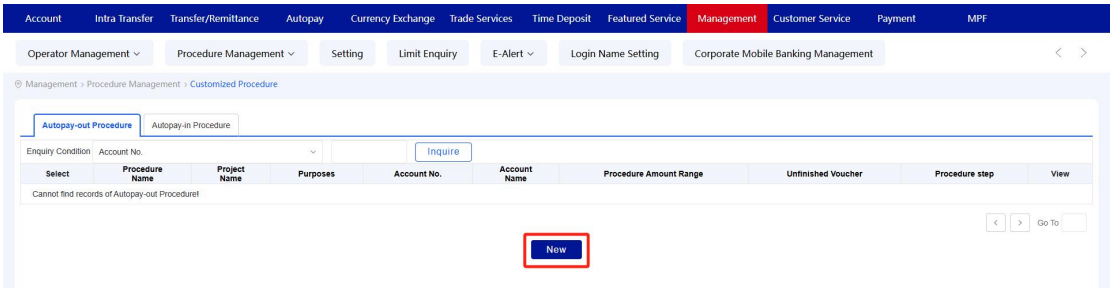
(3) Customized Process for Proxy Payment and Payroll Deduction

The prerequisite for setting up a customized process for Proxy Payment and Payroll Deduction is that the customer needs to visit the branch to handle Proxy Payment and Payroll Deduction business. For any inquiries, please consult your customer manager.

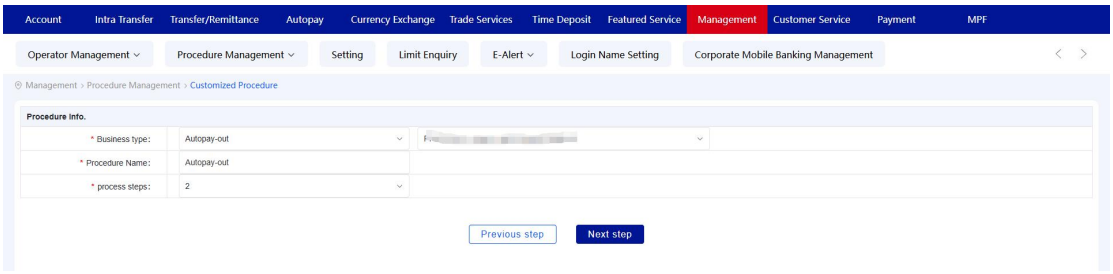
A. Navigate to "Service Management - Customized Process", choose the business type "Corporate Payment and Collection", then select "Next".



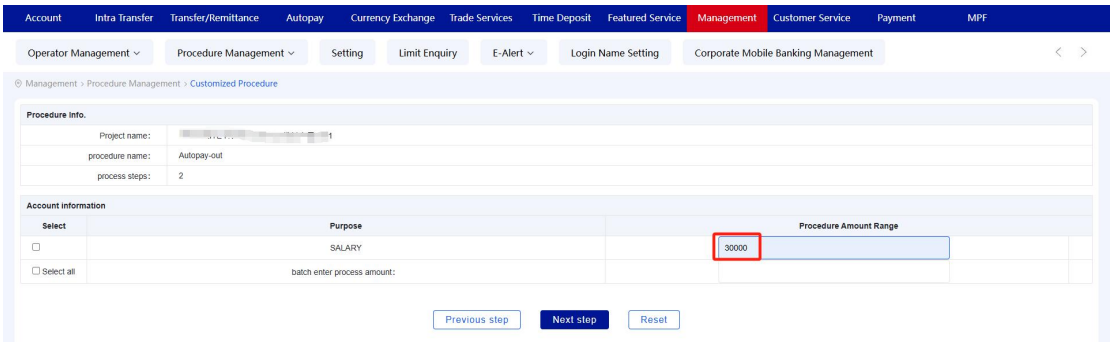
B. Click "Add" in the Proxy Payment process.



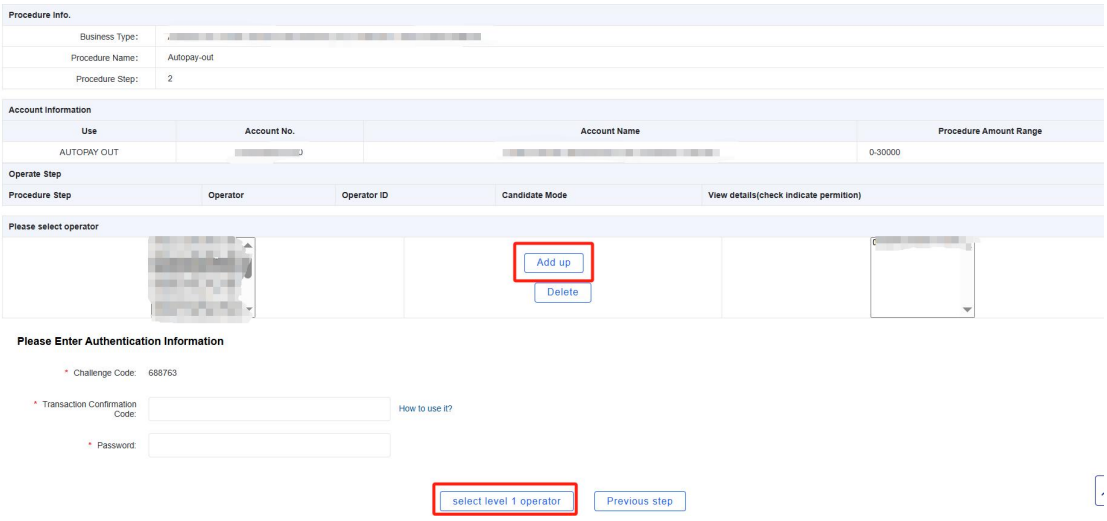
C. Fill in the process information. If only a single maker is needed to initiate and complete the transaction, select "1" for the process step. If a maker initiates and a authoriser verifies, choose "2" for the process step, and so forth.



D. Input the process amount. The process amount refers to the range set for Proxy Payment and Payroll Deduction transactions. The following example demonstrates setting up a process for the 0-456 monetary range.

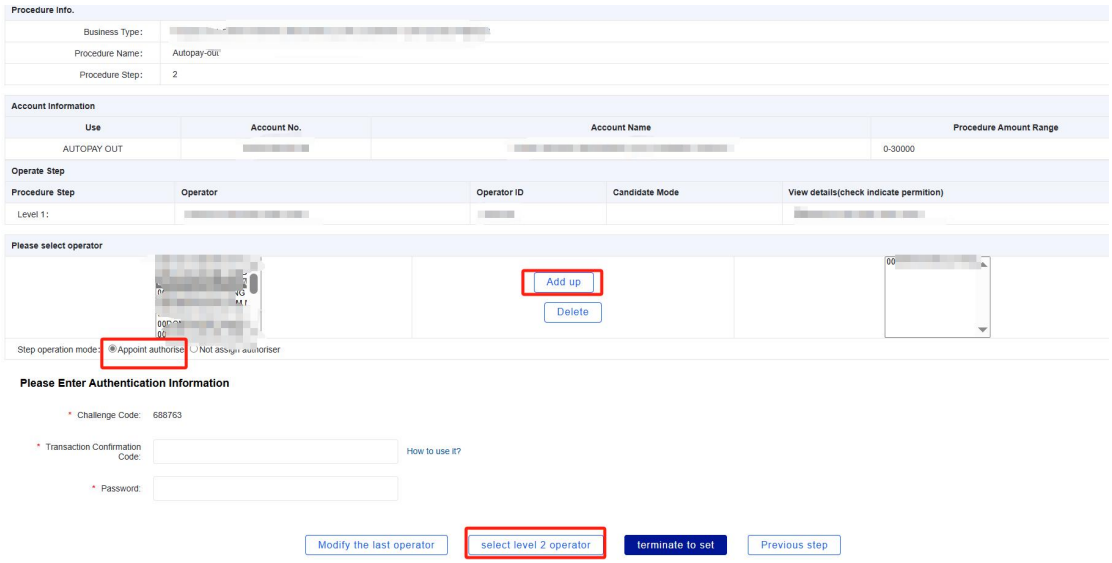


E. After selecting the operators, click “Choose First-Level Operator”. Under this, selecting “Designate Authoriser” allows for the choice of a designated authoriser for further approval after initiation/review completion. Conversely, selecting “Not Specify Authoriser” operates differently.

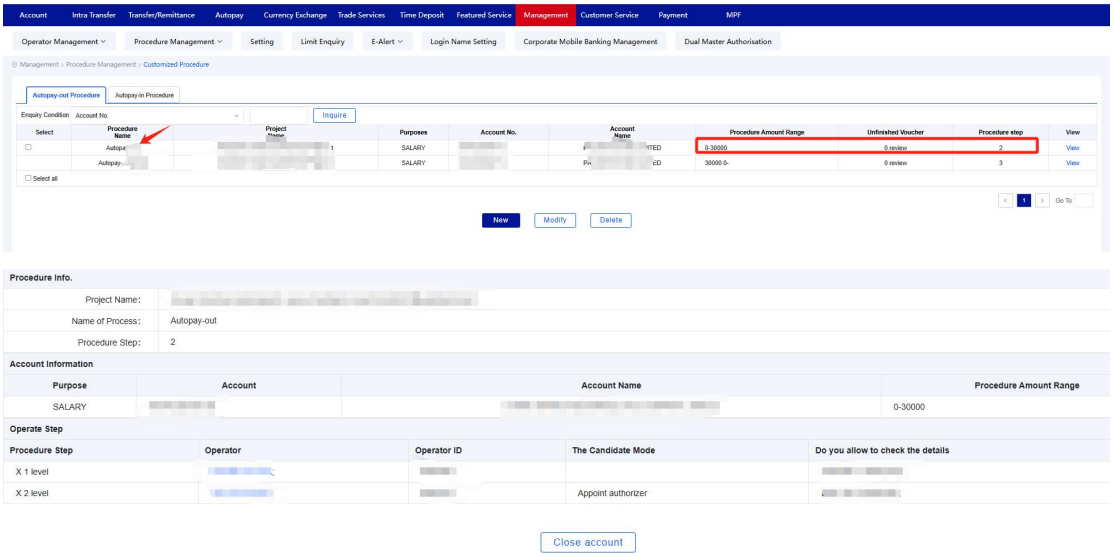


If previous process steps were "2" or higher, authoriser selection is required.

Then, click "Choose Second-Level Operator", and so on.



F. Upon completion of the setup, input authentication information and click "Finish Customization". In the Proxy Payment process list, the setup details of the payment process can be reviewed.

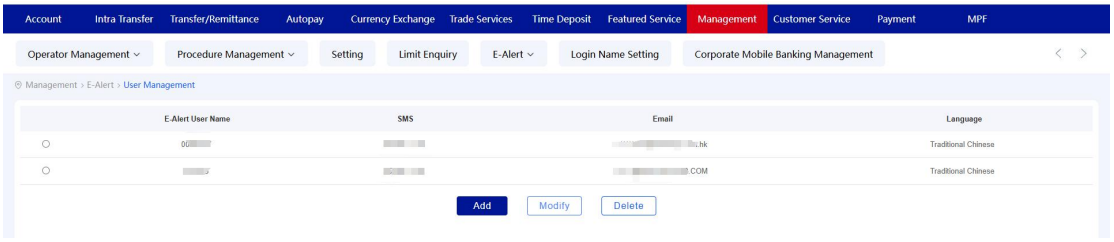


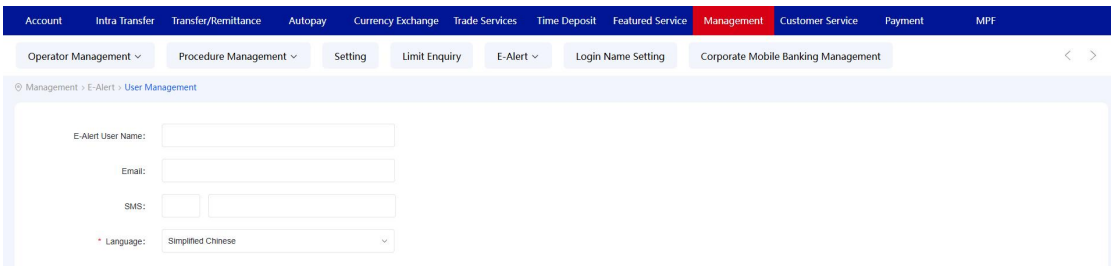
1.6. Electronic Notification Settings

Electronic notifications enable corporate supervising operators to send

transaction alerts to relevant personnel within the enterprise via email or text messages based on the business needs. Currently, the services supporting electronic notifications include maturity of time deposits, electronic statements, electronic notices, internal fund transfers, transfers to other accounts within the bank, transfers to other local banks' account, transfers to other bank account around the globe, proxy payment and payroll deduction services, direct payment authorization, bill payment services, real-time fund pool aggregation, and scheduled fund pool aggregation.

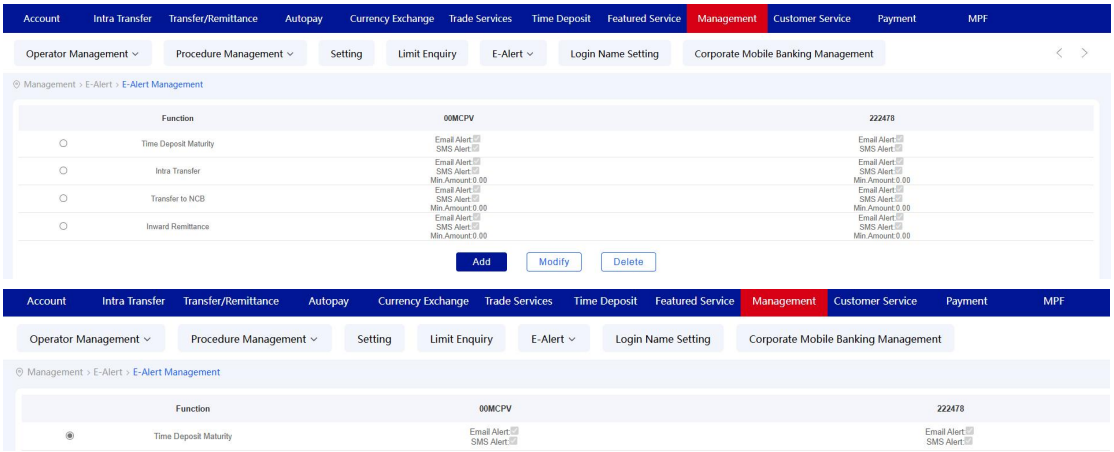
- User Configuration for Electronic Notifications. Corporate supervising operator can add up to three enterprise users to receive electronic notifications, allowing for settings related to email/mobile numbers and preferred language.





- Notification Settings. Businesses can tailor notifications according to their specific needs by selecting notification scenarios such as email

alerts, text message alerts, or both. For some transactions, minimum threshold settings for notifications are available (e.g., transfers, transfers to other accounts within the bank, transfers to other local banks' account, transfers to other bank account around the globe, incoming remittances, real-time fund pool aggregation, scheduled fund pool aggregation, and proxy payment and payroll deduction).

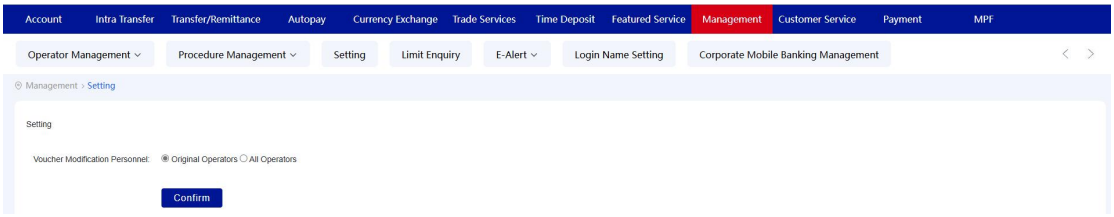


1.7.Service Management

Service management is exclusively accessible to the enterprise's supervising operator.

1.7.1. Control Settings

With this setting, you can choose personnel with the right to modify documents. "Original Operator" setting permits only the original maker to modify documents, while "All Operators" allows any operator to modify them. Choose according to the enterprise preference, then click "Confirm".



1.7.2. Transaction Limit Enquiry

You can view the single and daily cumulative limits for internal transfers, local remittances (registered accounts), local remittances (unregistered accounts), cross-border remittances (registered accounts), and cross-border remittances (unregistered accounts) for each account.

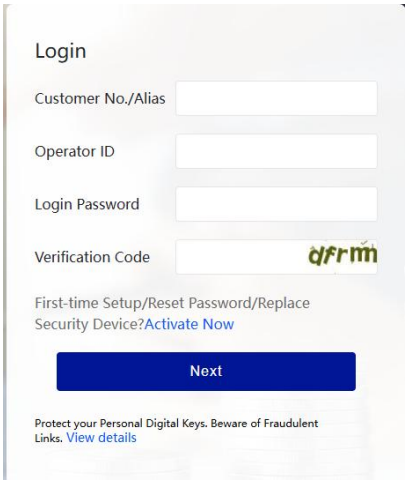
1.7.3. Corporate Mobile Management

- Enabling Corporate Mobile Banking Service. Corporate supervising operators activate the corporate mobile banking service within “Service Management - Corporate Mobile Management” in the Corporate Internet Bankingportal. After specifying the authorised operators and their mobile numbers, corporate clients can access the corporate mobile banking service.
- Disabling Corporate Mobile Banking Service. Corporate supervising operator can deactivate the corporate mobile banking service based on the corporate needs. After deactivation, all operators cannot use the corporate mobile banking service.

1.7.4. Login Alias Settings

To streamline client login procedures, supervising operator can set personalized login aliases for corporate clients, please log in via the log-in

window after setting.



1.7.5. Dual Supervisor Approval

1. Dual supervisor approval applies to relatively medium to large-scale enterprises. Specific actions by a supervising operator within the Corporate Internet Bankingsystem require approval from another supervising operator before they become effective. Clients need to choose the dual supervisor approval feature when opening their Corporate Internet Bankingaccounts at the counter.

2. The current functionalities supporting dual supervisor approval include “Service Management - Operator Management”, “Service Management - Process Management - Default Process”, “Service Management - Process Management - Customized Process - Payment Contracts/Time Deposits”, and “Service Management - Control Settings”. Functions beyond these areas do not support dual supervisor approval.

1.8. Security Information

● Click the "logout" button to exit from the system after you have finished all your online transactions. Additionally, close the browser and clear the cache and history in your browser after using our online service..

● For security reason, your online access will be disconnected automatically after a short period of inactivity in order to prevent unauthorised transactions. If you have not changed the Corporate Internet Banking password for a designated period, the notification for advising you to change password will be given when you login.

● To protect your privacy and assets, you should not disclose your client number/ client alias, operator code and Corporate Internet Banking password to anyone. You are advised to change your password regularly.

● Not to log into Online Service through hyperlinks or QR Code embedded in any third-party websites, mobile Apps, emails or SMS. The Bank will never ask customers to provide the account number, password or any personal information via e-mails.

● If you enter the wrong password six times consecutively, your online banking password will be frozen, and you won't be able to log in. General operator can contact the master operator to reset the password and unlock it in Corporate Internet Banking. Master operator must visit a branch to reset and unlock the password.

● Corporate operator can visit any branch to apply for a Security Device as a two-factor authentication tool .

● You may choose to use Mobile Token or Security Device as your two-factor authentication tool, please refer to the relevant promotional leaflet or contact the bank's staff for details.

● For more information on online banking security, please visit our website www.ncb.com.hk.

2. Corporate Mobile Banking

2.1. Corporate Mobile Banking Service Overview

2.1.1. Activation Procedure

Corporate supervising operators activate the Corporate Mobile Banking service through the "Service Management - Corporate Mobile Management" module in the Corporate Online Banking. They enable the usage permissions for supervising/regular operators, allowing the respective users to follow the steps in 2.4 for Corporate Mobile Banking login.

2.1.2. System Requirements

Our bank's Corporate Mobile Banking is an independent channel catering to corporate clients and is available on the Apple App Store and Google Play in the Hong Kong region. It supports a wide range of mobile models. Simply download the Corporate Mobile Banking app to effortlessly access the service. Recommended operating systems include:

iOS 12.0 or higher

Android 10.0 (excluding) or higher

2.1.3. Overview of Corporate Mobile Banking Services

2.1.3.1. Account Enquiry

NCB provides query services for current accounts, time deposit accounts, and loan contract accounts. It also supports account list and detailed account information inquiries.

2.1.3.2. Time Deposits

NCB offers the option to open suitable time deposit services.

NCB supports review of processed time deposits.

NCB allows modification of maturity instructions for time deposits not yet due.

NCB allows makers to recall unreviewed documents and modify or delete documents if the review does not pass.

2.1.3.3. Currency Exchange

- NCB offers cross-currency exchange services for HKD, CNY, and more than 10 different foreign currencies.

2.1.3.4. Corporate Internal Transfers

- Enterprises can directly transfer funds to their accounts held with Nanyang Commercial Bank.

- NCB supports 24/7 transactions.

- NCB supports forward dated and standing transactions.

- Enterprises can swiftly initiate maker applications via mobile banking.

2.1.3.5. Funds Transfer and Remittance

Enterprises can swiftly initiate the following transfer/remittance transactions via mobile banking:

(1) Transfer to Local Accounts within the Bank

Enterprises can transfer funds directly to other individuals' NCB accounts.

(2) Transfer to Other Local Bank Accounts

Enterprises can transfer funds in HKD,USD,EUR and CNY to other banks' accounts directly and normally it should be instant.

(3) Transfer to Global Accounts

Enterprise can transfer funds to global different banks accounts in different currencies.

(4) Faster Payment System (FPS) Transfers

Through the Faster Payment System (FPS), you can transfer funds in HKD and CNY to other local banks' accounts. You can get your funds transferred to the account at the receiving bank instantly under normal circumstances..Additionally, it supports mobile phone numbers, email addresses, or FPS identifiers as account identifiers.

2.1.3.6. Funds

- Subscriptions for funds distributed by the bank, including specified open-end funds and guaranteed funds during the selling period, can be done through mobile banking.
- You can enquire the balance of your Open-end Funds and Guaranteed

Funds under custody and in the name of bank nominees held under designated investment account.

- The transaction records, processing statuses, and dividend records for all fund transactions carried out through branches, online banking, and mobile banking within the current day or the past 1 year can be queried via mobile banking.
- Comprehensive market information, including fund prices, asset allocations, fund performance, and sales files, can be accessed through mobile banking.

2.1.3.7. Securities

- Securities Trading

1) Conduct securities trading, amend or cancel trading orders and enquire the status of your trading orders.

2) Deliver corporate operation instruction like subscribe for new shares,public offering of shares, issue of shares, subscribe for preferred shares, scrip dividend and acquisition (it is up to the operation and provisions of corporate) via Corporate Mobile Banking.

3) Deposit stick in via Corporate Mobile Banking.

4) Real-time stock price quote and alert service.

- Monthly Stock Savings Plan

1. More than 10 types of stocks can be selected as long investment under

one plan via Corporate Mobile Banking.

2. Frictional shares under monthly stock saving plan can be sold as market value via Corporate Mobile Banking, Corporate Internet Banking, Mobile Investment Line or any branches.

3. No additional charge of custodian fee and premium of collection of shareholders' return

● Subscribe for new shares service

1. Subscribing for new shares with yellow sheet via Corporate Mobile Banking.

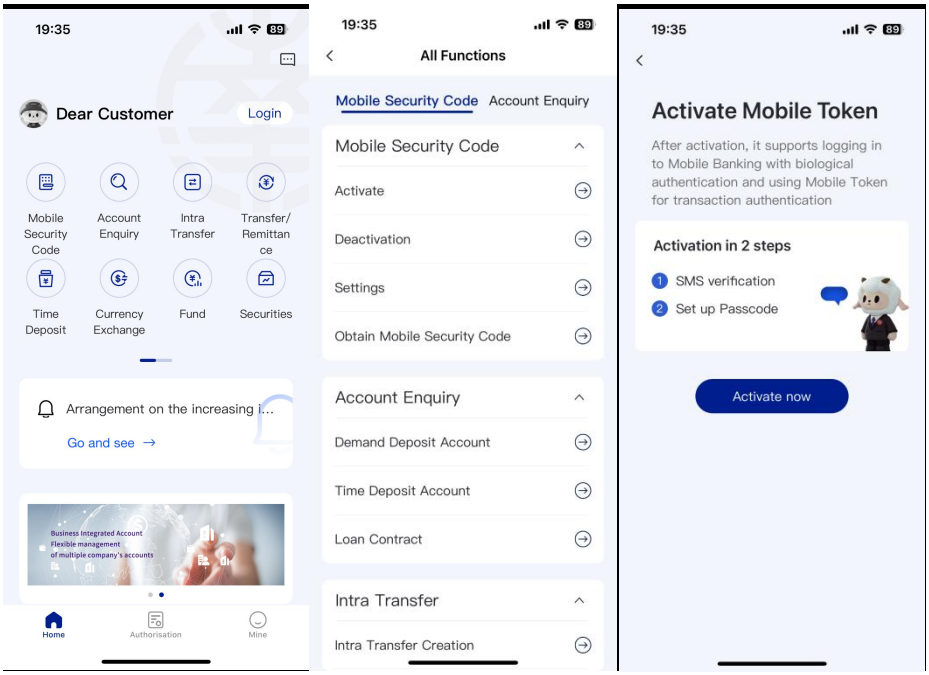
2. If using yellow sheet for subscribing, the distributed new shares will be deposited in security account and it can be traded until the new shares listed.

2.2. Mobile Security Device

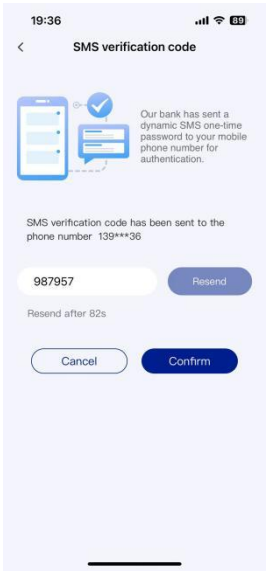
2.2.1. Activating the Mobile Security Device

Operators can activate the "Mobile Security Device" within the Corporate Mobile Banking app to use it as a 2FA authentication tool.

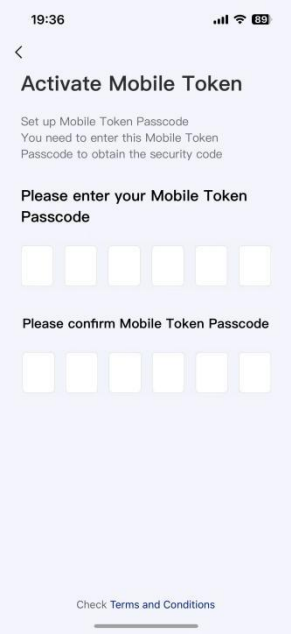
Step 1: After logging into Corporate Mobile Banking, select "More > Mobile Token > Activate".



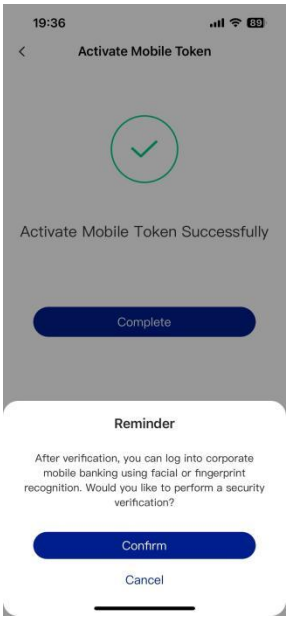
Step 2: The operator’s registered mobile number with the bank will receive a “one-time SMS verification code”. Enter this code correctly to proceed.



Step 3: Enter a customized “Mobile Token Passcode” twice, then submit to activate the “Mobile Security Device”.



Step 4: Register biometric authentication (only applicable for phones supporting biometric authentication) is used to log into Corporate Mobile Banking with biometric authentication.

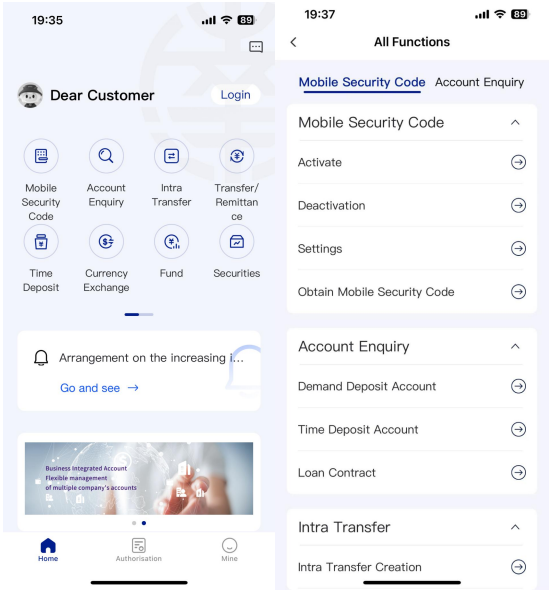


2.2.2. Enabling/Disabling Biometric Authentication

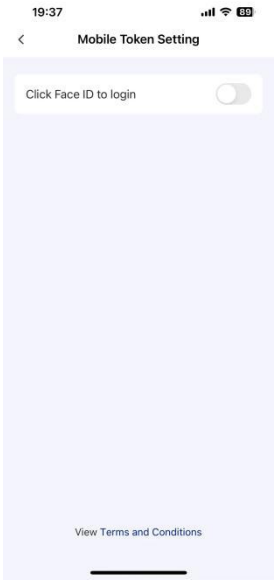
Operators can enable or disable "Fingerprint/Face ID Authentication" within

Corporate Mobile Banking. When "Fingerprint/Face ID Authentication" is enabled, clients can access Corporate Mobile Banking through biometric authentication.

Step 1: After logging into Corporate Mobile Banking, select "More > Mobile Token > Settings".



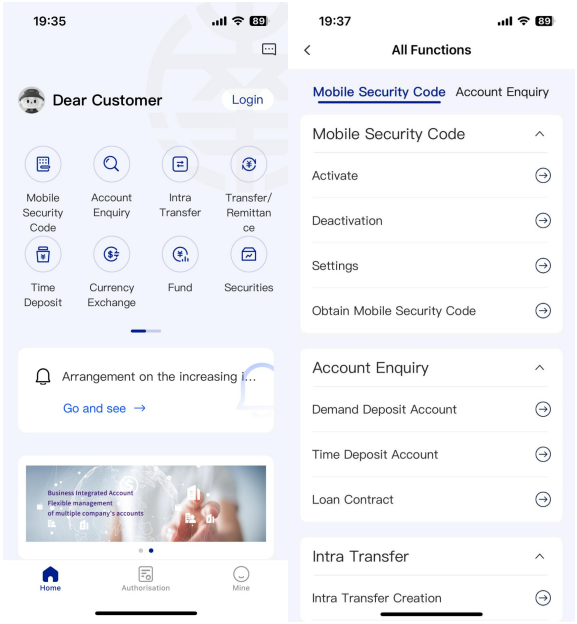
Step 2: Enable/Disable "Fingerprint/Face ID Authentication".



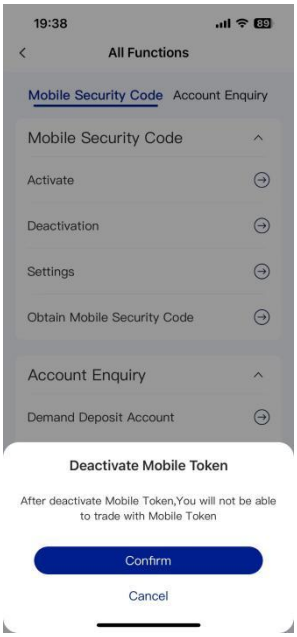
2.2.3. Disabling the Mobile Security Device

Operators can disable the “Mobile Security Device” within Corporate Mobile Banking.

Step 1: After logging into Corporate Mobile Banking, select “More > Mobile Token > Disable”.



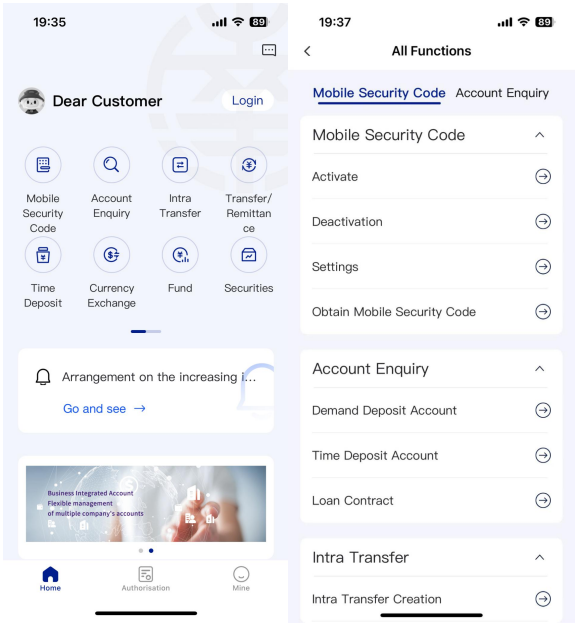
Step 2: Confirm to disable the “Mobile Security Device”.



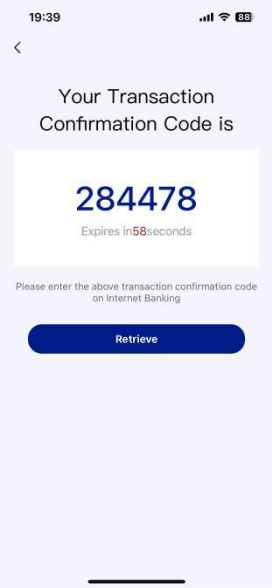
2.2.4. Authorizing Transactions

Using the "Mobile Security Device" for 2FA authentication, clients must enter the system-generated 6-digit random challenge factor (i.e., a 6-digit random number provided on the transaction page) in the "Mobile Security Device" to obtain the corresponding "Transaction Confirmation Code" for transaction authentication.

Step 1: After logging into Corporate Mobile Banking(Please don't log in), select "More > Mobile Token > Obtain Transaction Confirmation Code".



Step 2: Enter the challenge factor, authenticate through "Mobile Token Passcode", and obtain the "Transaction Confirmation Code".



Step 3: Enter the "Transaction Confirmation Code" on Online Banking to complete the transaction confirmation.

2.3. How to Conduct Transactions Using Corporate Mobile Banking

Step 1: Open Corporate Internet Bankingservice at the counter.

Step 2: Corporate supervising operator sets up transaction processes in Corporate Online Banking.

Step 3: Corporate supervising operator enables Corporate Mobile Banking service and set permissions for users in Corporate Internet Bankingunder "Service Management - Corporate Mobile Management".

Step 4: iOS users download Corporate Mobile Banking from the App Store, and Android users download it from Google Play.

Step 5: Follow Step 2.4 to log into Corporate Mobile Banking.

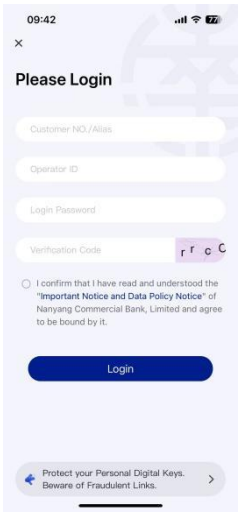
Step 6: Input transactions in Corporate Mobile Banking and review

transactions in Corporate Mobile Banking or Corporate Internet Bankingif required.

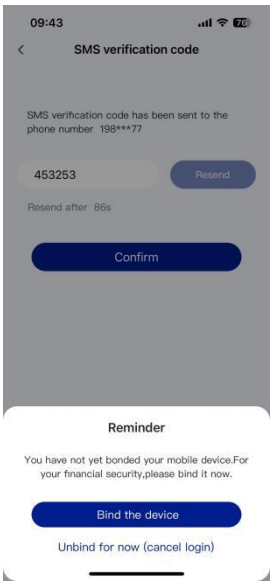
2.4. Logging into Corporate Mobile Banking

1) You can log into Corporate Mobile Banking using your account password.

Step 1 - On NCB Corporate Mobile Banking app on your mobile device, input your “Client Number/Client Alias”, “Operator ID”, “Login Password”, and “Additional Code” to access Corporate Mobile Banking.



Step 2 – For first-time login on a particular mobile device, clients will need to verify an SMS verification code to link the device. Once verified, access to Corporate Mobile Banking will be granted.

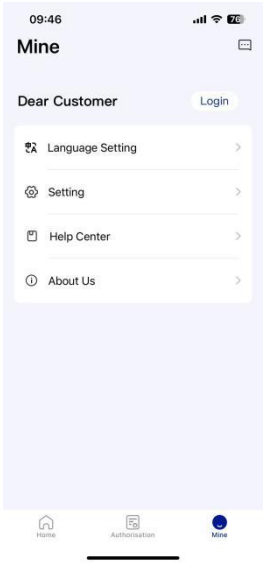


If you enter the wrong password six times consecutively, your online banking account will be frozen, and you won't be able to log in. Clients with the general operator can contact the master operator to reset the password and unlock it in the corporate online banking.master operator must visit a branch to reset and unlock the password if its account is suspended.

2) You can log into Corporate Mobile Banking using biometric authentication

You can also use specific mobile devices to access Corporate Mobile Banking. Activate the "Mobile Security Device" and register for "Biometric Authentication" services (including fingerprint recognition and Face ID, among others) under "More > Mobile Token > Enable". This enables quick access to Corporate Mobile Banking.

After completing transactions, please click "Log Out" to exit from Corporate Mobile Banking services to prevent any potential exposure of personal information. For security reasons, the system will automatically log you out after a period of inactivity to prevent unauthorised transactions.



2.5. Security Information

- Click the "logout" button to exit from the system after you have finished

all your online transactions..

- For security reason, your online access will be disconnected automatically after a short period of inactivity in order to prevent unauthorised transactions. If you have not changed the Corporate Internet Banking password for a designated period, the notification for advising you to change password will be given when you login.
- To protect your privacy and assets, you should not disclose your client number/ client alias, operator code and Corporate Internet Banking password to anyone. You are advised to change your password regularly.
- Not to log into Online Service through hyperlinks or QR Code embedded in any third-party websites, mobile Apps, emails or SMS. The Bank will never ask customers to provide the account number, password or any personal information via e-mails.
- If you enter the wrong password six times consecutively, your online banking account will be frozen, and you won't be able to log in. General operator can contact the supervising operator to reset the password and unlock it in the Corporate Internet Bankingportal. Supervising operator must visit a branch to reset and unlock the password.
- Upon logging into mobile banking, you can activate the Mobile Security Device as a two-factor authentication tool by selecting "More > Mobile Token > Activate".
- Within Corporate Mobile Banking, upon logging in, you can choose

"More > Mobile Token > Settings" to enable or disable "Biometric Authentication". Please note that even after disabling the "Mobile Token" and/or "Biometric Authentication", your biometric authentication data remains stored on your mobile device. You may consider deleting the data at your discretion.

- Once you have successfully registered for "Biometric Authentication", any biometric records stored on your mobile device can be used for authentication. You must ensure that only your biometric data stored on your device is used for this purpose, and keep secure the security password or code used to store biometric records and log in using "Biometric Authentication". For security reasons, do not register other's biometric data on your device or use a compromised phone.
- If your mobile device's biometric records have changed at any point, your "Biometric Authentication" will be suspended, requiring you to reset the "Mobile Token".
- You must not use Biometric Authentication if you have reasonable belief that other persons may share identical or very similar biometric credential(s) of you or your biometric credential(s) can be easily compromised. For example, you must not use Face ID recognition for authentication purpose if you have identical twin or triplet siblings.
- You must not use Biometric Authentication if your biometric credential(s) are or will be undergoing rapid development or change. For example,

you must not use Face ID recognition for authentication purpose if you are an adolescent with facial features undergoing rapid development.

- You must exercise reasonable caution in securely keeping your phone. If you suspect or discover that your phone is lost or stolen, or if unauthorised transactions occur, you must promptly notify the bank.
- Operator can apply for a Security Device as a two-factor authentication tool at any of our branches.
- You may choose to use Mobile Token or Security Device as your two-factor authentication tool, please refer to the relevant promotional leaflet or contact the bank's staff for details.
- For more information on mobile banking security, visit our website www.ncb.com.hk.

3. Bank-Enterprise Direct Link Services

3.1. Brief Introduction to the Bank-Enterprise Direct Link Service

3.1.1. Activation Procedure

1 Clients present their requirements

2. Sign the NDA and obtain detailed requirement

3 Sign the formal contract

4 Joint-Testing, and service activation

3.1.2. Bank-Enterprise Direct Link Service Overview

Through the Bank-Enterprise Direct Link, companies can integrate their ERP systems with the bank's core systems via dedicated lines or the internet. This integration allows direct access to various electronic services offered by the bank within their proprietary systems. It enables business clients to focus on managing business development, ensuring peace of mind while exploring new opportunities.

*Interface document, please refer to the traditional Chinese interface

3.2. Security Information

- To protect your privacy and assets, you should not disclose your client number/ client alias, operator code and Corporate Internet Banking password to anyone. You are advised to change your password regularly.
- Safeguard your Bank-Enterprise Direct Link U Shield and CFCA certificate. Avoid disclosing the U Shield and CFCA certificate numbers to any third party.
- If you enter the wrong password six times consecutively, your Bank-Enterprise operator password will be frozen, preventing login. In that case, contact the enterprise's supervising operator to reset the password and unlock the account via Corporate Online Banking.
- For more information on online banking security, please visit our website www.ncb.com.hk.

4. Technical Support and Queries

If you have any enquiry about "Corporate Internet Banking" "Corporate Mobile Banking " "Bank-Enterprise Direct Link ", please contact us during service hours:

NCB Customer Service Hotline: (852) 2616 6638

24-hours Security Incidents Hotline (Online Banking): (852) 2616 6638

Or visit our website www.ncb.com.hk.

Service Hours:

Monday to Friday: 9:00 - 18:00

Saturday: 9:00 - 13:00

Except Sundays and public holidays

5.Important matters

1. In order to protect your rights perfectly, please access our Bank official website click to view ''Service Item'', "Important Notice and Policy Notice", "Security Information" and "Hyperlink Policy"

2. All contents of this article files , its copyright are owned by Nanyang Commercial Bank Limited

NCB 南洋商業銀行