



Change of Authentication Arrangement of Terminal Access to CCASS/ CCMS

Information Package for the Launch of 2FA Preparation

Issue Date: June 2023

Modification History

Version	Date	Modified By	Synopsis
1.0	May 2023	HKEX	First issue
2.0	June 2023	HKEX	Updated Appendix D for the self-service authentication settings function procedure.

Table of Contents

1. Introduction	4
2. Overview of this Information Package	4
3. Pre-launch Preparation.....	5
3.1. Register email address for Users and DAs	5
3.2. How to locate the User ID	5
3.3. Perform connectivity verification	7
3.4. Check CCASS/ CCMS Terminal URL bookmarks	7
3.5. Post-release connectivity test (10 June 2023).....	8
4. Launch of 2FA (12 June 2023)	8
4.1. Changes in DAs' Operations.....	10
4.1.1. Authentication and administration right.....	10
4.1.2. Password reset and account unlock	11
4.2. Changes in Users' Operations.....	12
4.2.1. Authentication method and user maintenance.....	12
4.2.2. Password reset and account unlock	13
4.3. Users migration	14
4.3.1. Additional user account	14
5. Decommissioning of Smartcard	15
5.1. Changes in DA account.....	16
6. Important Information	16
6.1. Retaining your smartcard and smartcard reader	16
6.2. Backup Centre	16
7. Contact Information.....	17
8. Other Information.....	17
8.1. Official Launch information.....	17
8.2. CCASS/ CCMS Terminal User Guides	17
9. Checklist.....	18
Appendix A. Email registration procedure for users and DAs	19
Appendix B. Post-release connectivity test Schedule and Arrangement.....	21
Appendix C. First Time Logon Arrangement.....	25
Appendix D. Account Maintenance for Users and DAs	33

1. Introduction

As set out in the circulars dated 24 May 2023 (Reference: CD/OES/CCASS/023/2023, CD/OEC/HKCC/137/2023 and CD/OEC/SEACH/138/2023), the launch of Two-Factor Authentication (2FA) is scheduled on 12 June 2023 (Monday) tentatively, subject to regulatory approval. Participants of HKSCC, HKCC and SEACH (CPs) and HKSCC Designated Banks (DBs) should be ready for the launch of 2FA through the briefing sessions held from 24 to 26 April 2023. CPs and DBs should start accessing CCASS/ CCMS via 2FA from 12 June 2023 (Monday) using existing User IDs, regular passwords and One-Time-Passwords (OTP) generated by soft token via mobile application or email. To facilitate CPs and DBs to have a smooth transition to the 2FA from smartcard, HKEX has set out a list of pre-launch preparation activities and checklist, CPs and DBs are encouraged to participate in the activities and go through the checklist to ensure their operational and technical readiness for the launch of 2FA.

The launch of 2FA will only be applied on the authentication method of Terminal access to CCASS/ CCMS, including Security Management Function (DMS) and Overnight Report Distribution (ONRD) function, while the terminal functions and operations remain unchanged.

HKSCC CPs and DBs who access to CCASS through Participant Gateway (PG) will not be affected by the launch of 2FA, and should continue to CCASS via smartcard.

The smartcard will be decommissioned on 4 September 2023 (Monday) tentatively, which is around 2 months after the launch of 2FA. After the decommissioning of smartcard, 2FA will be the only authentication method to access CCASS/ CCMS Terminal. CPs and DBs should retain the smartcards until the decommissioning.

2. Overview of this Information Package

This Information Package is designed to assist CPs and DBs in preparing for the launch of 2FA, covering the following:

- Pre-Launch Preparation
- Launch of 2FA
- Decommissioning of smartcard
- Important information
- Contact Information
- Other Information
- Checklist

CPs and DBs should read this Information Package carefully and make necessary preparation and arrangements for the launch of 2FA. A copy of this document should also be passed to their relevant teams, such as operations and/or IT team to ensure the availability of proper operational and technical support during the launch of 2FA.

3. Pre-launch Preparation

CPs and DBs should have completed the following pre-launch preparation tasks (except for the post-release connectivity test tentatively scheduled on 10 June 2023 (Saturday)), to ensure their operational and technical readiness before the launch of 2FA.

3.1. Register email address for Users and DAs

In order for users and DAs to setup regular password to enable 2FA upon the launch of 2FA, it is mandatory to register the designated email addresses of the users and DAs through the following channel:

Account Type	Procedure
Users	DAs to input email address of user by Change User Profile function in DMS
DAs	Client Connect DAs/ users with EU_UserMaintenance access right to submit eService DA3 - CCASS/ CCMS Terminal Delegated Administrator Application/ Maintenance Form in Client Connect through HKEX Access Management Portal .

For security reason, it is recommended that all users and DAs to make use of emails with corporate domains to receive OTP. In addition, group email address is not recommended given the OTP is served as an authentication for individual to access CCASS/ CCMS Terminal, but same email address can be registered in multiple user profiles to facilitate the operational need. CPs and DBs are responsible for ensuring that their organizations comply with such arrangements.

CPs and DBs should have registered email addresses for their users and DAs. If CPs and DBs haven't already done so, please do so as soon as possible. Mobile number is not required to input in the User Profile. For the detailed procedure of email registration, please refer to [Appendix A](#).

3.2. How to locate the User ID

The User ID will remain unchanged after the launch of 2FA, users and DAs shall continue to access to CCASS/ CCMS with their existing User ID. The format of the User ID for users and DAs across the Clearing Houses is shown as follows:

Change of Authentication Arrangement of CCASS/ CCMS Terminal Access Information Package for Launch of 2FA

	HKSCC CPs	HKSCC DBs	HKCC CPs	SEOCH CPs
User ID for Users (existing users were assigned by HKEX, new users to be assigned by DAs upon the launch of 2FA)	Participant ID + 2 custom alphanumeric, e.g. B0123401	Participant ID + 2 custom alphanumeric, e.g. BNK99901	HK + Customer Code + 1/2/3/4 + 2 custom alphanumeric, e.g. HKABC101	HK + Customer Code + 1/2/3/4 + 2 custom alphanumeric, e.g. HKABC201
User ID for DAs (to be assigned by HKEX)	Participant ID + X/Y/Z + 1-9, e.g. B01234X1	Participant ID + X/Y/Z + 1-9, e.g. BNK999X1	HK + Participant ID + 1/2/3/4 + X/Y/Z + 1-9, e.g. HKABC1X1	HK + Participant ID + X/Y/Z + 1/2/3/4 + 1-9, e.g. HKABC2X1

In case user and DA have no clue of their User ID, it can be found in either way below:

a) By User Profile Listing function - to be performed by DA via DMS

1 After logging into DMS

Click <View Listings>, then click <User Profile Listing>

2 The profile of all users including DAs will be displayed

User ID

Registered email address (if any)

b) By Enquire User Profile function - to be performed by DA via DMS

1 After logging into DMS

Click <Maintain User Profile>, then click <Enquire User Profile>

2

Click <List>

3 The User ID and the corresponding User Name will be displayed

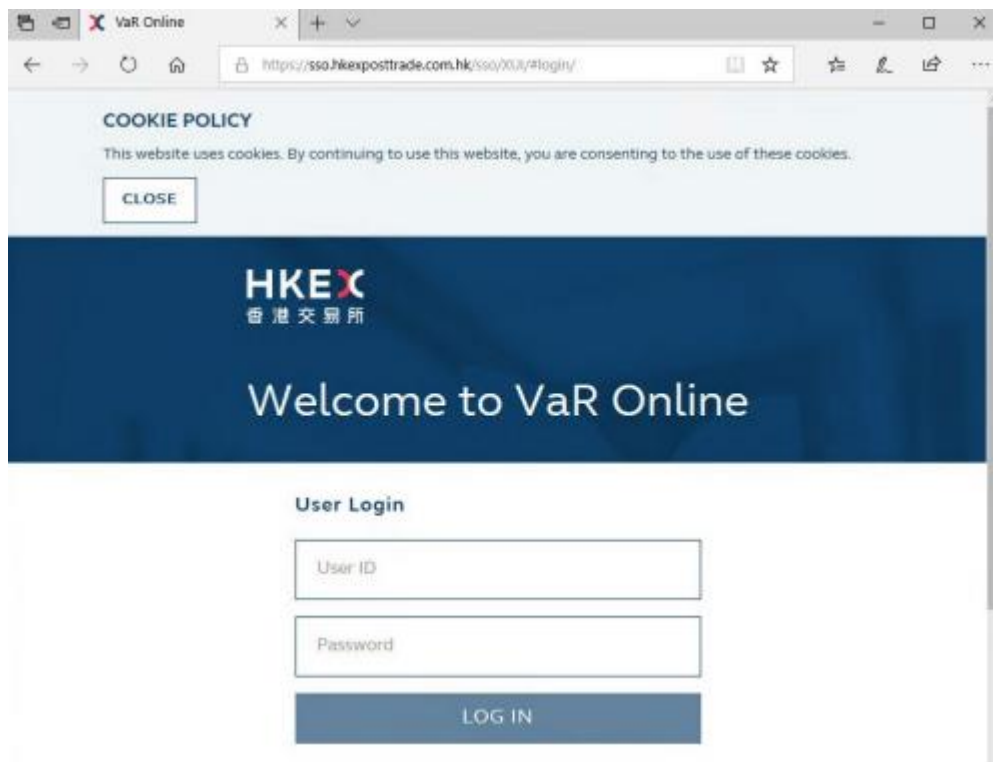
User ID

3.3. Perform connectivity verification

For any CP or DB that does not use the Domain Name System (DNS) services provided by HKEX to access CCASS/ CCMS, and/or has any additional access control between the PC and CCASS service, such as a firewall, it is recommended to arrange relevant IT staff to test the connectivity with the new 2FA server before the launch of 2FA. For network setup details, please refer to Section 4.7 to Section 4.9 of the CCASS/ CCMS Technical Guide available in Client Connect on [HKEX Access Management Portal](#).

After confirming the network settings, CPs and DBs can test the connection to the new 2FA server as follows:

- (i) On CCASS/ CCMS Terminal PC, open MS Edge browser to visit URL <https://sso.hkexposttrade.com.hk/sso>. No login required
- (ii) The below screen should be seen:



- (iii) Close the window without logging on

3.4. Check CCASS/ CCMS Terminal URL bookmarks

The URL of CCASS/ CCMS Terminal and DMS will remain the same as follow:

- CCASS/ CCMS: <https://www.ccass.com/>
- DMS: <https://www.ccass.com/dms>

For users who have bookmarked the URL in their workstation's browser, should check if the correct URL has been saved in the browser to re-direct to the correct webpage.

3.5. Post-release connectivity test (10 June 2023)

Once CPs and DBs has completed the connectivity verification as stated in [Section 3.3 - Perform Connectivity Verification](#) above, they should continue to access CCASS/ CCMS Terminal using their existing connectivity configuration during the post-release connectivity test. A post-release connectivity test will be available from 18:00 – 20:00 and 22:00 – 23:00 on 10 June 2023 (Saturday) for CPs and DBs to verify the connection to CCASS/ CCMS Terminal after 2FA is deployed to Production environment.

Interested CPs and DBs should register for the connectivity test via Event section in Client Connect via [HKEX Access Management Portal](#) on or before 2 June 2023 (Friday). For details of the schedule and arrangement, please refer to [Appendix B](#). CPs and DBs should note there will be NO report retrieval nor operational functions available during the post-release connectivity test. Also, there will be NO support on account unlock nor password reset for DAs during the post-release connectivity test.

4. Launch of 2FA (12 June 2023)

Upon the launch of 2FA on 12 June 2023 (Monday) tentatively, the terminal access to CCASS/ CCMS will be replaced by 2FA from smartcard. Given that users and DAs have completed email registration, they should initialize 2FA from 12 June 2023 (Monday), if they haven't already done so during the post-release connectivity test on 10 June 2023 (Saturday). Users and DAs shall access to CCASS/ CCMS Terminal or DMS to (i) setup password and; (ii) setup OTP channel (i.e. by mobile application or email)¹, it is suggested to reserve at least 30 minutes to complete 2FA initialization before the first operational task of the day (e.g. first batch settlement run at 10:30am) to avoid any hiccups in accessing to CCASS/ CCMS Terminal or DMS.

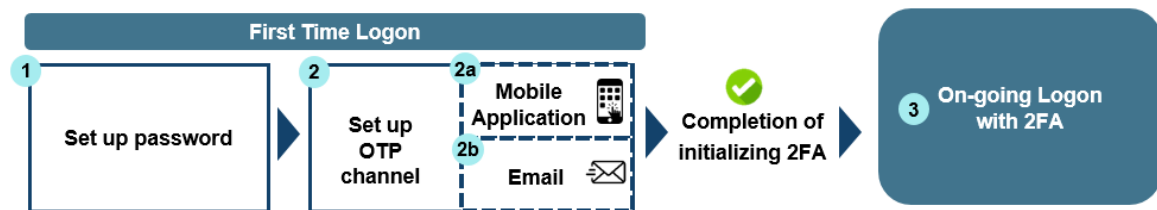
Also, please adhere to the new HKEX Password Policy² as follows to setup password for accessing CCASS/ CCMS Terminal and DMS by 2FA, while the smartcard password will be remain as is (i.e. 6-8 digits):

- (i) At least 16 characters
- (ii) At least 1 number
- (iii) At least 1 lower letter
- (iv) At least 1 special character from !@#\$%^&*()
- (v) At least 1 capital letter

¹ CPs and DBs should note that the operation hours of CCASS/ CCMS Terminal is from 07:00 to 21:30 on Mondays to Fridays, except for public holidays, while the operation hours of DMS is from 07:00 to 21:30 on Mondays to Fridays, 09:00 to 13:00 on Saturdays, except for public holiday.

² The new HKEX Password Policy will be applied on VaR Online logon along with the launch of 2FA on 12 June 2023 (Monday) tentatively, if applicable. The updated VaR Online user guide will be available in Client Connect on HKEX Access Management Portal on 2 June 2023 (Friday).

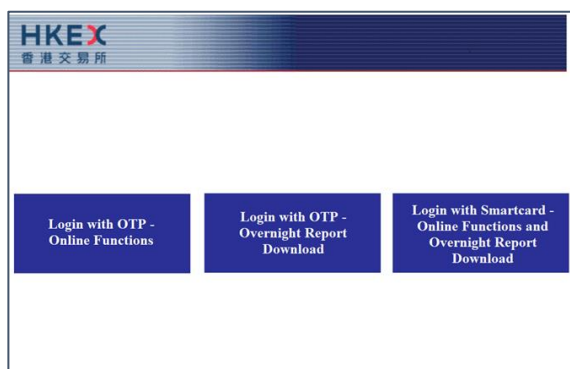
The following is an illustration of initializing 2FA:



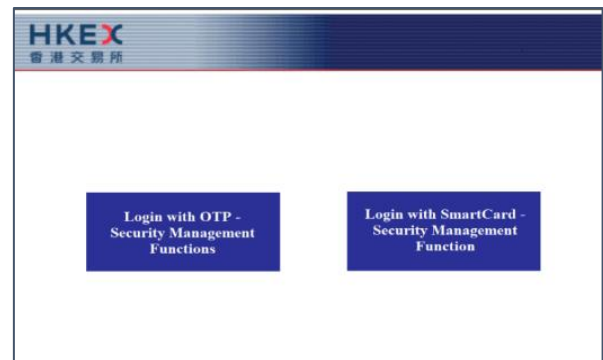
After completing the above steps, users and DAs should continue to access CCASS/ CCMS Terminal or DMS by 2FA. For the detailed procedure of first time logon and the on-going logon with 2FA, please refer to [Appendix C](#).

In addition, a new landing page will be displayed for accessing CCASS/ CCMS Terminal and DMS. Users and DAs will have to select the login authentication method and the function required (if applicable), as shown below:

CCASS/ CCMS Terminal:



DMS:




Smartcard authentication method will remain available in case of any issue in accessing DMS by 2FA. However, such authentication method will be decommissioned on 4 September 2023 (Monday) tentatively, therefore, users and DAs are encouraged to initialize 2FA as soon as possible.

4.1. Changes in DAs' Operations

The following tables have summarized the operational changes of each DA function.

4.1.1. Authentication and administration right

	Today	VS	Launch of 2FA
Authentication	<ul style="list-style-type: none"> Smartcard 	NEW	<ul style="list-style-type: none"> 2FA Smartcard (reserved) <i>DAs created upon launch of 2FA can only access by 2FA.</i>
DA Creation	<ul style="list-style-type: none"> By HKEX (submit eService SCard 1) 	NEW	<ul style="list-style-type: none"> By HKEX (submit eService DA 3 - <i>refer to the assigned User ID in DA 3 that is being processed by HKEX with "Completed" status</i>)
DA Maintenance	<ul style="list-style-type: none"> At least one DA maker and one DA checker By HKEX (submit eService SCard 1) 	NEW	<ul style="list-style-type: none"> At least one DA maker and <u>two DA checkers</u> By HKEX (submit eService DA 3) <p> DAs can be assigned with business user role upon the decommissioning of smartcard</p>

Authentication

DA should access to DMS by 2FA, while smartcard authentication method will be reserved in case of any issue in accessing DMS by 2FA. Also, DAs created upon launch of 2FA can only access by 2FA.

DA Creation

With available user account(s), CPs and DBs can create DA user profile by submitting Client Connect eService DA3 – CCASS/ CCMS Delegated Administrator Application/ Maintenance Form, such eService will be enriched on 5 June 2023 (Monday) along with the official launch of 2FA with more maintenance request types available, including Add, Unlock/ Enable/ Disable and Delete to facilitate the DA maintenance³. After HKEX processed the eService for adding DA, CPs and DBs should refer to the User ID assigned from the completed eService. User manual of DA3 is available in [HKEX website](#). For more information on checking the total number of user accounts available, please refer to [Section 4.3 - Users Migration](#).

DA Maintenance

Similar to DA Creation, CPs and DBs can also submit Client Connect eService DA3 for maintenance of DA's user profile. Meanwhile, Client Connect eService SCard 1 – Smartcard Maintenance for DA would still be available for smartcard password reset function only until the decommissioning of the smartcard. However, smartcard and

³ CPs and DBs should note that HKEX will start processing the new maintenance request types (i.e. Add, Unlock/ Enable/ Disable and Delete) from the submitted eService DA3 from 12 June 2023 (Monday) onwards.

smartcard reader will not be available for purchase upon the launch of 2FA. If the smartcard is lost, the DA must adopt 2FA to login DMS.

4.1.2. Password reset and account unlock

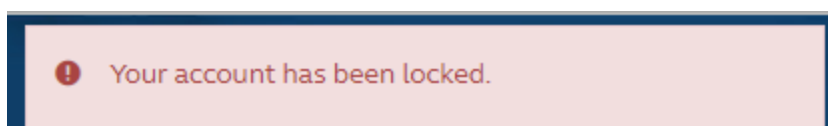
	Today	VS	Launch of 2FA
Password Reset			
Enabled mobile app OTP	• N/A	NEW	Self-service password reset by Forgot/ Reset Password function
Enabled email OTP	• N/A	NEW	By HKEX (Submit eService DA 3)
Forgot smartcard password	• By HKEX (Submit eService SCard 1)		
Account Unlock	• N/A	NEW	By HKEX (Submit eService DA 3)

Password reset

The self-service password reset is a new function implemented for DAs to reset their regular passwords in case they have lost it under the condition that they have enabled mobile application to obtain OTP. For security reason, the DA needs to enter the OTP generated by mobile application to verify their identity. If DAs have enabled email to obtain OTP instead, the CP or DB will need to submit Client Connect eService DA3 to HKEX to Unlock/ Reset OTP device registration for the DA. Therefore, it is recommended that DAs to enable mobile application to obtain OTP, so that they can complete password reset by themselves with relatively shorter lead time. Kindly note that smartcard password cannot be self-reset nor reset via submission of eService DA3, it will be remained by submission of eService SCard 1.

Account unlock

Access will be locked after 5 consecutive unsuccessful attempts of login within 30 minutes, while 3 consecutive unsuccessful attempts of entering OTP will be counted to 1 unsuccessful attempt of login. After the account is locked, an error message will be displayed starting from the next login attempt, as shown below:



Once the account is locked, DA cannot access to DMS by 2FA nor smartcard.

For the detailed procedure of password reset and account unlock, please refer to [Appendix D](#).

4.2. Changes in Users' Operations

CPs and DBs should ensure they have sufficient users to access CCASS/ CCMS Terminal to perform daily operations. The following tables have summarized the operational changes of each function.

4.2.1. Authentication method and user maintenance

	Today	VS	Launch of 2FA
Authentication	<ul style="list-style-type: none"> Smartcard 	NEW	<ul style="list-style-type: none"> 2FA Smartcard (reserved)
User Creation	<ul style="list-style-type: none"> By HKEX 	NEW	<ul style="list-style-type: none"> By DA (Assumption: available user accounts)
User Maintenance	<ul style="list-style-type: none"> By DA 		

Authentication

Similar to DA, user should access to CCASS/ CCMS Terminal by 2FA, while smartcard authentication method will be reserved in case of any issue in accessing DMS by 2FA. Also, users created upon launch of 2FA can only access by 2FA.

User Creation

With available user account(s), DA can create user profile and assign User ID for their users. For more information on checking the total number of user accounts available, please refer to [Section 4.3 - Users Migration](#).

User Maintenance

Similar to user creation, user maintenance is also managed by DA.

4.2.2. Password reset and account unlock

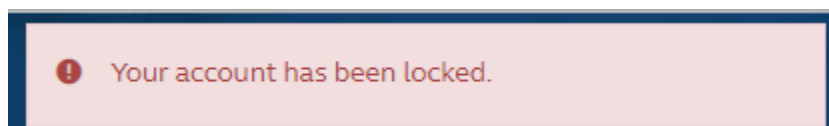
	Today	VS	Launch of 2FA
Password Reset			
Enabled mobile app OTP	• N/A	NEW	Self-service password reset by Forgot/ Reset Password function
Enabled email OTP	• N/A	NEW	• Unlock/ Reset OTP Device Registration by DA
<u>Forgot smartcard password</u>	• Smartcard Password Reset by DA		
Account Unlock	• N/A	NEW	• Reset account by DA

Password reset

The self-service password reset is a new function implemented for users to reset their regular passwords in case they have lost it under the condition that they have enabled mobile application to obtain OTP. For security reason, the user needs to enter the OTP generated by mobile application to verify their identity. If users have enabled email to obtain OTP instead, the corresponding DA would need to perform Unlock/ Reset OTP Device Registration for the user. Therefore, it is recommended that users to enable mobile application to obtain OTP, so that they can complete password with relatively shorter lead time. Kindly note that smartcard password cannot be self-reset, it has to be reset by their DA.

Account unlock

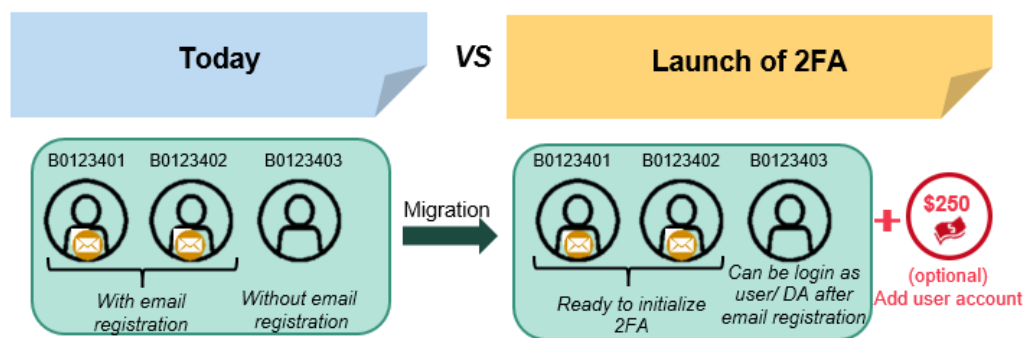
Access will be locked after 5 consecutive unsuccessful attempts of login within 30 minutes, while 3 consecutive unsuccessful attempts of entering OTP will be counted to 1 unsuccessful attempt of login. After the account is locked, an error message will be displayed starting from the next login attempt, as shown below:



Once the account is locked, user cannot access to CCASS/ CCMS by 2FA nor smartcard. For the detailed procedure of password reset and account unlock, please refer to [Appendix D](#).

4.3. Users migration

Upon the launch of 2FA, all the existing user accounts with smartcards in DMS (with or without email registration) will be migrated to 2FA, DAs can refer to “Enquire User Profile” function or “User Profile Listing” function (refer to [Section 3.2 - How to locate the User ID](#) above) in DMS for the existing user profile of users including DAs themselves. An example of the user account migration is illustrated below:



The user profile will display information related to 2FA. Once user or DA has initialized 2FA, the related fields “Locked” and “OTP Enabled” will then be available in the user profile in DMS, as shown below:

Locked	No	<input type="radio"/> Unlock/Reset OTP Device Registration
OTP Enabled	Yes	

While the smartcard related fields “SRN (for user using smartcard)” and “Certificate Expiry Date” will be removed;

SRN (for user using smartcard)	0101101200012AB2
Certificate Expiry Date	31-Dec-30 23:59:59

In an opposite case where the user or DA has yet to initialize 2FA, the smartcard related fields “SRN (for user using smartcard)” and “Certificate Expiry Date” will remain available, while the 2FA related fields “Locked” and “OTP Enabled” will not be displayed. CPs and DBs should note that the above information can only be viewed under “Enquiry User Profile” and “Delete User Profile” functions.

4.3.1. Additional user account

For any additional user account required, CPs and DBs can submit Client Connect eService DA4 - CCASS / CCMS User Account Application Form which will be available

through [HKEX Access Management Portal](#) on 12 June 2023 (Monday) along with the official launch of 2FA, a one-off fee of \$250 per each additional user account will be incurred.⁴

Once the eService DA4 is processed by HKEX and the additional user account is granted, DAs can check the available user account through “User Profile Listing” function (refer to [Section 3.2 - How to locate the User ID](#) above) in DMS, the maximum number of users, the total number of users with user profile and the respective number of users and DA will be available at the bottom of the user profile listing, a sample is as shown below:

MAX. NO. OF USERS	: 70
TOTAL NO. OF USERS	: 47
TOTAL NO. OF DELEGATED ADMINISTRATORS	: 22
TOTAL NO. OF USERS EXCEPT DELEGATED ADMINISTRATORS	: 25
*** END OF REPORT ***	

Given that there is spare user accounts, DA can create user profile and assign User ID for their users under “Create User Profile” function in DMS as displayed below:

Create User Profile - Detail

This is an end-user profile

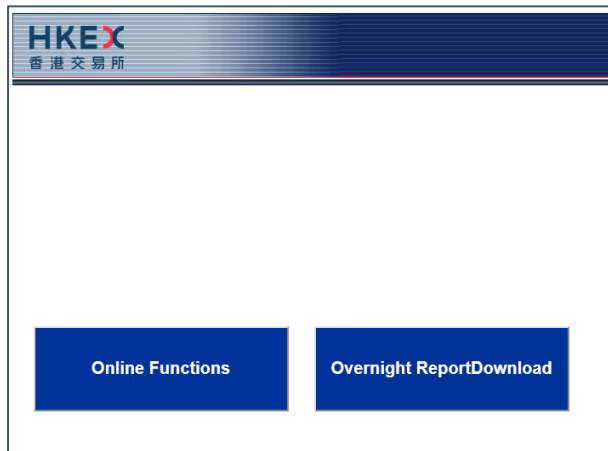
Organisation	B01234 ABC SECURITIES		
Internal/External	EXTERNAL		
User ID	B01234	<input type="text"/>	<input type="button" value="Generate User ID"/>
User Status	<input checked="" type="radio"/> ENABLED <input type="radio"/> DISABLED		
Surname	<input type="text"/>		
Other Names	<input type="text"/>		
Email	<input type="text"/>		
Enable From	<input type="text"/>	DD/MM/YY	
Disable After	<input type="text"/>	DD/MM/YY	
Clearing House Options	Cash ▼		
Access Channel	C3T		

5. Decommissioning of Smartcard

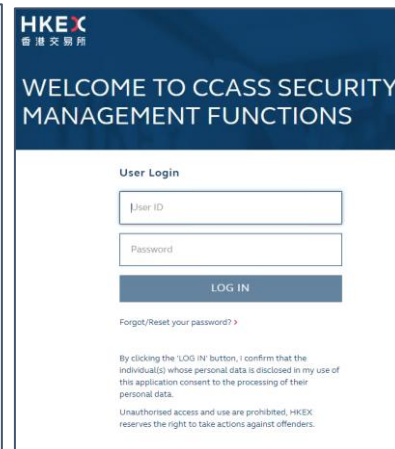
The smartcard authentication method will remain until the decommissioning on 4 September 2023 (Monday) tentatively, where the decommissioning date shall be announced via circulars. Starting from 4 September 2023 (Monday), 2FA will be the sole authentication method for terminal access of CCASS/ CCMS and DMS. The landing page of CCASS/ CCMS Terminal and DMS will be further updated with smartcard authentication method being removed, as shown below:

⁴ CPs and DBs should note that HKEX will start processing the submitted eService DA4 from 12 June 2023 (Monday) onwards.

CCASS/ CCMS Terminal:



DMS:



5.1. Changes in DA account

Upon the decommissioning of smartcard, DA can be assigned with business user groups through DMS with maker-checker mechanism. To avoid one-handed operation, checkers are not allowed to authorize the request related to them. Alternatively, CPs and DBs can submit Client Connect eService DA3 to assign DA role to existing users.

In order to ensure operations security, each participant should assign at least one DA maker and two DA checkers to perform the user profile maintenance functions for its users including DAs themselves through DMS.

6. Important Information

6.1. Retaining your smartcard and smartcard reader

PG users should retain their smartcard and smartcard reader for daily operations. Meanwhile, CPs and DBs should not dispose their smartcards and smartcard readers until the decommissioning of smartcard on 4 September 2023 (Monday) tentatively.

6.2. Backup Centre

Upon the launch of 2FA, CPs and DBs can only use 2FA to login CCASS/ CCMS Terminal at Backup Centre.

7. Contact Information

For any enquiries about the change of authentication method of CCASS/ CCMS Terminal access, please contact CCASS/ DCASS Hotline or Email indicated below:

Terminal	CCASS	CCMS
Hotline	2979 7111 <i>During normal office hours from 09:00 to 18:00 (Mondays to Fridays, excluding public holidays)</i>	2979 7222
Email	ClearingPS@hkex.com.hk	ClearingPSD@hkex.com.hk

8. Other Information

8.1. Official Launch information

Information related to the launch of 2FA including respective circulars, briefing material, guideline and this Information Packages are published on HKEX website ([for HKSCC CP & DBs/ for HKCC & SEOCH CPs](#)). CPs and DBs should read through such documentations and make all necessary arrangements to ensure proper operational procedures and technical support are available for pre-launch preparation, during post-release connectivity test and after the launch of 2FA.

8.2. CCASS/ CCMS Terminal User Guides

The CCASS/ CCMS Terminal User Guides will be modified to reflect the authentication and function changes upon the launch of 2FA will be available in Client Connect through [HKEX Access Management Portal](#) on 2 June 2023 (Friday).

8.3. General Rules of HKCC and Operational Procedures of CCASS and SEOCH

Corresponding amendments to Rules of HKCC and Operational Procedures of CCASS and SEOCH for implementing 2FA will be available via the HKEX website by June 2023 for reference.

9. Checklist

ITEMS TO BE CHECKED		✓
(A) CPs and DBs should have already done:		
1	Have you registered the designated email for all users and DAs for the regular password setup?	
2	Have you checked if the CCASS/ CCMS Terminal or DMS URL are bookmarked correctly?	
3	Have you performed connectivity verification for new CCASS/ CCMS 2FA servers? -Reference to circulars dated 3 April 2023 (HKSCC: CD/OES/CCASS/013/2023 , HKCC: CD/OEC/HKCC/092/2023 and SEOCH: CD/OEC/SEOCH/093/2023)	
4	Have you informed all users and DAs in your company for the change of authentication arrangement?	
5	Is each user and DA aware of their User ID?	
(B) Checklist on 10 June 2023 (Saturday)		
6	Have you read and understood this document ("Information Package for the Launch of 2FA")?	
7	Do you know the current network setting and configuration for CCASS/ CCMS Terminal and DMS remain unchanged upon the launch of 2FA (on 12 June 2023)?	
8	Do you know how to initialize 2FA?	
9	Please ensure the registered email address of the user and DA can be accessed to obtain OTP for password setup during post-release connectivity test.	
10	Please prepare a mobile device and download ForgeRock Authenticator App for receiving OTP by mobile application (if needed)	
11	If you are not using HKEX provided DNS services, do you know the IP addresses of the Primary Data Centre and Secondary Data Centre for the post-release connectivity test?	
(C) Checklist on 12 June 2023 (Monday) – Launch of 2FA		
12	Have you setup password and OTP channel to initialize 2FA?	
13	If the user is current Client Connect/ VaR Online user, same ForgeRock Authenticator app will be used for OTP generation.	
14	Have your ensured your operational teams will login CCASS/ CCMS Terminal and DMS by 2FA going forward?	
15	Do you know that you should retain the smartcard and smartcard reader until the decommissioning of smartcard in a later stage?	

Appendix A. Email registration procedure for users and DAs

Upon the launch of 2FA, users are required to setup their regular password to initiate the 2FA. An OTP email will be sent to users designated email address for authentication. Therefore, it is important for users to register their designated email addresses in advance.

1. Email Registration for Users

To be performed by DA Maker

a) Access to DMS via <https://www.ccass.com/dms>

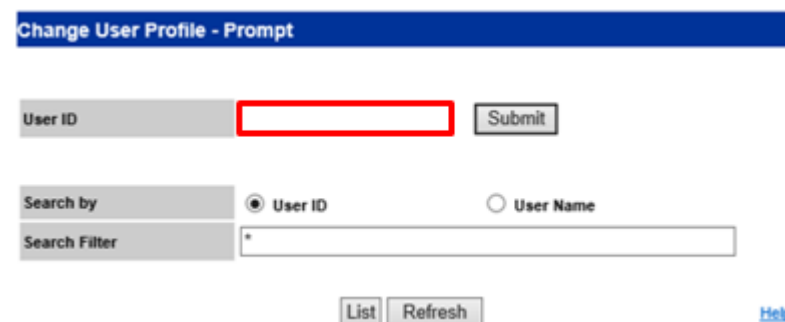
b) Enter smartcard password, then click <Logon>



c) Click <Maintain User Profile>, then click <Change User Profile>



d) Enter User ID, then click <Submit>



- e) Enter email address of the user, then click <Change>

Change User Profile - Detail

This is an end-user profile

User ID	B0124601		
User Status	<input checked="" type="radio"/> ENABLED <input type="radio"/> DISABLED		
Surname	TAI MAN		
Other names	CHAN		
Email	abc@abc.com.hk		
Enable from	01-Jan-03	DD-MM-YY	
Disable after		DD-MM-YY	
Clearing House Options	Cash		

➔ **Change** Refresh

To be performed by DA Checker

- f) On the same page, enter <Checker ID> and <Authorization Code>, then click <Confirm>. Confirmation message will be displayed on the bottom of the page.

Change User Profile - Confirmation

This is an end-user profile

User ID	B0124601		
User Status	ENABLED		
User name	TAI MAN CHAN		
Email	abc@abc.com.hk		
Enable from	01-Jan-03		
Disable after			
Clearing House Options	Cash		

Transaction limit (HKD)

Default	9,999,999,999.99	DI Requirement
DI		Recall Request
ISI		ATI
Cash Compensation Indicator		SI
Cash Prepayment		

Selected User Groups
11 12 13 14 15 16 17 18 19 20 21 22 23
24 51 52 54 55 A AA AB AC AD C CR D
DV GX E F F1 H I J K L M N NU NV
O P PD PM Q R RA RB RD RU RX RY RZ
SA SM ST WA WB WC WD WE WF WG

Checker ID: B01246X2
Authorisation Code: *****

Confirm Back

↓

THE ABOVE USER PROFILE IS CHANGED SUCCESSFULLY

2. Email Registration for DAs

- Refer to [Guideline for Email Registration for CCASS/ CCMS Delegated Administrators](#)

Appendix B. Post-release connectivity test Schedule and Arrangement

During the post-release connectivity test, CPs and DBs should follow the schedule as follows:

10 June 2022 (Saturday) – Post-release connectivity test	
Time	Activities
On-line Session at Primary Data Centre (Session 1)	
18:00 – 20:00	<p>Connectivity to CCASS/ CCMS</p> <p>By Smartcard (applicable to Users)</p> <ul style="list-style-type: none"> • Access to CCASS/ CCMS via https://www.ccass.com • In the landing page, click <Login with Smartcard - Online Functions and Overnight Report Download> to be redirected to the login page with smartcard authentication • Logon to CCASS/ CCMS using the production Smartcard and 9 June 2023 (Friday) password • Once you logon to CCASS/ CCMS, "Function not available" will be displayed, the connectivity is completed • Logout from CCASS/ CCMS <p>By Smartcard (applicable to DAs)</p> <ul style="list-style-type: none"> • Access to DMS via https://www.ccass.com/dms • In the landing page, click <Login with Smartcard – Security Management Functions> to be redirected to the login page with smartcard authentication • Logon to DMS using the production Smartcard and 9 June 2023 (Friday) password • Once you logon to DMS, the connectivity is completed • Logout from DMS <p>By 2FA - Initiation of 2FA⁵ (applicable to Users)</p> <ul style="list-style-type: none"> • Access to CCASS/ CCMS via https://www.ccass.com • In the landing page, click <Login with OTP - Online Functions> or <Login with OTP - Overnight Report Download> to be redirected to the login page with 2FA • Setup password & OTP channel following Appendix C – setup password & setup OTP channel procedure • Logon to CCASS/ CCMS using the User ID, password and OTP following Appendix C - on-going logon with 2FA procedure • Once you logon to CCASS/ CCMS, "Function not available" will be displayed, the connectivity is completed

⁵ Initiation of 2FA (setup of password & OTP channel) performed in Session 1 at the Primary Data Centre will be carried forward to Session 2 at the Secondary Data Centre and the next business day, 12 June 2023 (Monday).

	<ul style="list-style-type: none"> Logout from CCASS/ CCMS <p>By 2FA – Initiation of 2FA⁶ (application to DAs)</p> <ul style="list-style-type: none"> Access to DMS via https://www.ccass.com/dms In the landing page, click <Login with OTP – Security Management Function> for DMS to be redirected to the login page with 2FA Setup password & OTP channel following Appendix C – setup password & setup OTP channel procedure Logon DMS using the User ID, password and OTP following Appendix C - on-going logon with 2FA procedure Once you logon to DMS, the connectivity is completed Logout from DMS
On-line Session at Secondary Data Centre (Session 2)	
22:00 – 23:00	<p>Connectivity to CCASS/ CCMS</p> <p>By Smartcard (applicable to Users)</p> <ul style="list-style-type: none"> Access to CCASS/ CCMS via https://www.ccass.com In the landing page, click <Login with Smartcard - Online Functions and Overnight Report Download> to be redirected to the login page with smartcard authentication Logon to CCASS/ CCMS using the production Smartcard and the same password used in Session 1 Once you logon to CCASS/ CCMS, "Function not available" will be displayed, the connectivity is completed Logout from CCASS/ CCMS <p>By Smartcard (applicable to DAs)</p> <ul style="list-style-type: none"> Access to DMS via https://www.ccass.com/dms In the landing page, click <Login with Smartcard – Security Management Functions> for DMS to be redirected to the login page with smartcard authentication Logon to DMS using the production Smartcard and the same password used during Session 1 Once you logon to DMS, the connectivity is completed Logout from DMS <p>By 2FA (applicable for users)⁷</p> <ul style="list-style-type: none"> Access to CCASS/ CCMS via https://www.ccass.com In the landing page, click <Login with OTP - Online Functions> or <Login with OTP - Overnight Report Download> to be redirected to the login page with 2FA

⁶ Initiation of 2FA (setup of password & OTP channel) performed in Session 1 at the Primary Data Centre will be carried forward to Session 2 at the Secondary Data Centre and the next business day, 12 June 2023 (Monday).

⁷ Any user account changes such as password change performed in Session 2 at the Secondary Data Centre will NOT be carried forward to the next business day, 12 June 2023 (Monday).

	<ul style="list-style-type: none"> Logon to CCASS/ CCMS using the User ID, password that setup during Session 1 and OTP following Appendix C - on-going logon with 2FA procedure Once you logon to CCASS/ CCMS, "Function not available" will be displayed, the connectivity is completed Logout from CCASS/ CCMS <p>By 2FA (applicable for DAs)⁸</p> <ul style="list-style-type: none"> Access to DMS via https://www.ccass.com/dms In the landing page, click <Login with OTP – Security Management Function> for DMS to be redirected to the login page with 2FA Logon to DMS using the User ID, password that setup during Session 1 and OTP following Appendix C - on-going logon with 2FA procedure Once you logon to DMS, the connectivity is completed Logout from DMS
--	---

CPs and DBs should ensure that they have registered email address for their users and DAs in advance, so that they can initiate 2FA during the post-release connectivity test. Also, it is recommended to initialize 2FA during Session 1 in Primary Data Centre, as any account changes performed during Session 2 in Secondary Data Centre will not be carried forward to the next business day, 12 June 2023 (Monday). During the post-release connectivity test, DA should not perform any security management functions such as create/ change/ delete users' profile.

In case any CP or DB is not using HKEX provided Domain Name System (DNS) services to access CCASS/ CCMS Terminal, please arrange experienced staff to update the host table or change IP addresses during the test.

CP or DB using host table to access CCASS/ CCMS Terminal, should check and ensure the domain for CCASS/ CCMS will be resolved to the following IP addresses in the host table after completion of Session 1 to switch connection to Secondary Data Centre:

IP Address (Secondary Data Centre)	URL
10.243.66.15	sso.hkexpostrade.com.hk

After completion of Session 2, re-connect to Primary Data Centre, by resuming to the following primary IP addresses in the host table:

IP Address (Primary Data Centre)	URL
10.243.2.15	sso.hkexpostrade.com.hk

⁸ Any DA account changes such as password change performed in Session 2 at the Secondary Data Centre will NOT be carried forward to the next business day, 12 June 2023 (Monday).

For any queries during the post-release connectivity test, please contact CCASS/ DCASS Hotline at 2979 7111/ 2979 7222 respectively.

Appendix C. First Time Logon Arrangement

Upon the launch of 2FA, users and DAs should initialize 2FA immediately. Please refer to the following steps for the setup password and setup OTP channel procedure:

1. Setup password

- a) Access to CCASS/ CCMS via <https://www.ccass.com/>
OR access to DMS via <https://www.ccass.com/dms>

- b) Click the appropriate function under <Login with OTP>
CCASS/ CCMS



DMS



- c) Click <Forgot/Reset your Password>

User Login

User ID

Password

LOG IN

Forgot/Reset your password? >

- d) A pop-up box will be displayed. Enter User ID, then click <SUBMIT>

Input User ID

User ID

SUBMIT

- e) OTP will be sent to user's registered email address.
Input OTP, then click <SUBMIT OTP>

The image shows an email interface for 'CCASS: One Time Password'. The email is from 'noreply_pt@hkex.com.hk' and dated 'Today 11:59'. The body of the email states: 'One Time Password (OTP) for CCASS: 10767258', with the number '10767258' highlighted in a red box. Below the email, a purple arrow points to a web form. The form has the heading 'Please Enter Your One Time Password, Or Request A New One'. It contains a text input field labeled 'Enter OTP' (highlighted in a red box), a 'SUBMIT OTP' button, and a 'REQUEST OTP' button.

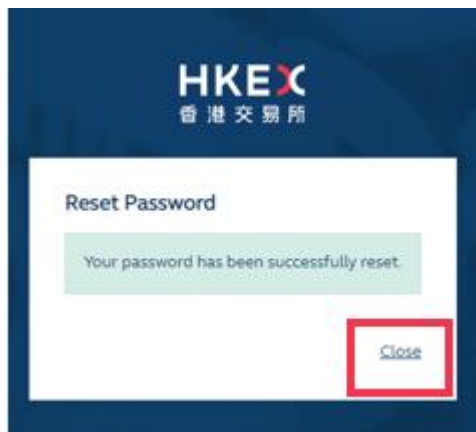
- Email OTP is valid for **5 minutes** and it can only be requested every 5 minutes.
- There is **no URL nor User ID** indicated in the email due to security reasons.

- f) Input new password twice, then click <SUBMIT>

The image shows the 'Reset Password' form on the HKEX (Hong Kong Exchange) website. The form is titled 'Reset Password' and includes the instruction 'Please enter your new password below.' Below this instruction are two text input fields: 'Password' and 'Confirm password'. Both fields have a red box around them and a red exclamation mark icon to their right, indicating a warning or error. Below the input fields is a 'SUBMIT' button and a 'Close' link.

- Set up the password based on password requirements:
 - (i) At least 16 characters
 - (ii) At least 1 number
 - (iii) At least 1 lower letter
 - (iv) At least 1 special character from !@#\$%^&*()
 - (v) At least 1 capital letter

- g) Password changed successfully, click <Close>, the pop-up box will be closed.



2. Set up OTP Channel:

- h) Return to the login page. Enter User ID and Password, then click <LOG IN>

CCASS/ CCMS

A screenshot of the CCASS/CCMS 'User Login' page. The page has a dark blue header with the HKEX logo and '香港交易所'. Below the header, the text 'WELCOME TO CCASS' is displayed. The 'User Login' section contains two input fields: 'User ID' and 'Password', both highlighted with a red border. Below these fields is a blue 'LOG IN' button. At the bottom, there is a link 'Forgot/Reset your password? >' and a disclaimer: 'By clicking the "/>

DMS

A screenshot of the DMS 'User Login' page. The page has a dark blue header with the HKEX logo and '香港交易所'. Below the header, the text 'WELCOME TO CCASS SECURITY MANAGEMENT FUNCTIONS' is displayed. The 'User Login' section contains two input fields: 'User ID' and 'Password', both highlighted with a red border. Below these fields is a blue 'LOG IN' button. At the bottom, there is a link 'Forgot/Reset your password? >' and a disclaimer: 'By clicking the "/>

For users who prefer to receive OTP via mobile application
-it is suggested for optimal account security and maintenance function

- i) Click <REGISTER DEVICE>

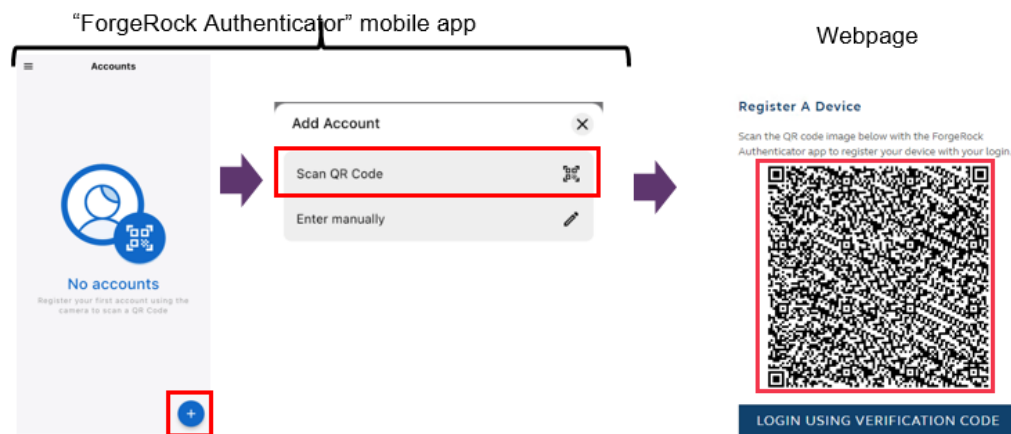
A screenshot of the 'ForgeRock Authenticator (OATH)' registration screen. The screen has a dark blue header with the text 'ForgeRock Authenticator (OATH)'. Below the header, there are two buttons: 'REGISTER DEVICE' and 'SKIP THIS STEP'. The 'REGISTER DEVICE' button is highlighted with a red border.

- j) In your mobile, search and install “ForgeRock Authenticator” from Google Play or Apple’s App Store.

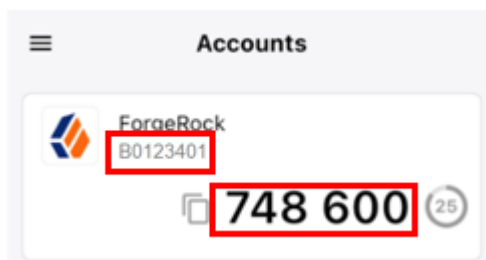


If the user is current Client Connect/ VaR Online user, same ForgeRock Authenticator app will be used for OTP generation

- k) In “ForgeRock Authenticator” mobile application, click + sign, then click <Scan QR Code>, and then scan the QR code by “ForgeRock Authenticator” mobile application, then click <LOGIN USING VERIFICATION CODE> in the page



- l) The OTP will be displayed in the “ForgeRock Authenticator” mobile application with CCASS/ CCMS User ID



- More than 1 User IDs and their respective OTP will be shown if users have registered for other HKEX systems:
 - Client Connect User ID = email address
 - VaR Online User ID = company code + Username

- m) Back to the CCASS/ CCMS login webpage, input OTP and click <SUBMIT>

ForgeRock Authenticator (OATH)

SUBMIT

- n) Successfully logon

CCASS/ CCMS

General Enquiries
New Settlement Act / Status
Delivery Instruction (DI)
A/C Transfer Inquiry (ATI)
Settlement Instruction (SI)
Investor Status Inquiry (ISI)
BS Counterparty List
Payment Instruction
Cash Payments
Stock Borrowing / Lending
BSL Bulletin Board
General Stock Collateral
Margin Withdrawal Order
Reaction Instruction
Business Option Instruction
Corp Voting Instruction
IPO Application
Transfer Instruction
Corp Communication
Revised Batch File
Report Profile Maintenance
View Circular

Maintain Broadcast Message
The Msg Announcement Information
Broadcast Message Email Download
Change Edit Logout
30 Apr 82 15:43

Last access on 30-Apr-82 at 15:26:16
B0300001
MMB 61
30 Apr 82 15:43

Enquire Broadcast Message Prompt
Market Code ALL
Broadcast Message Type All Information Event Completion Emergency
List Refresh

Apple loaded Internet

DMS

HKEX 香港交易所
User ID: B0124602

Welcome [User] Site Map Logout Change Password 21-Apr-23 13:43:32

Logon Success
B0124602 last access on 21-Apr-23 at 13:41:51

For users who prefer to receive OTP via email
-users should note that they cannot perform self-service password reset

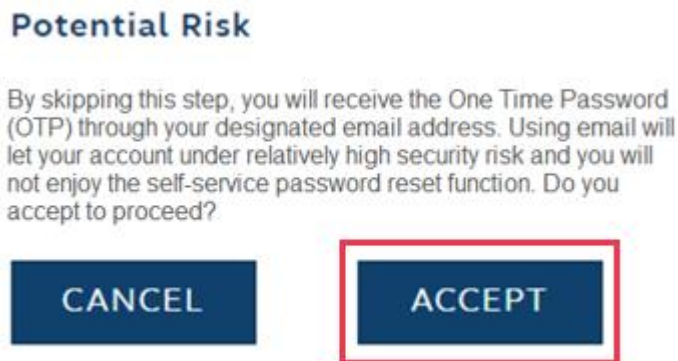
- o) Resume from step (h). Click <SKIP THIS STEP>.

ForgeRock Authenticator (OATH)

REGISTER DEVICE

SKIP THIS STEP

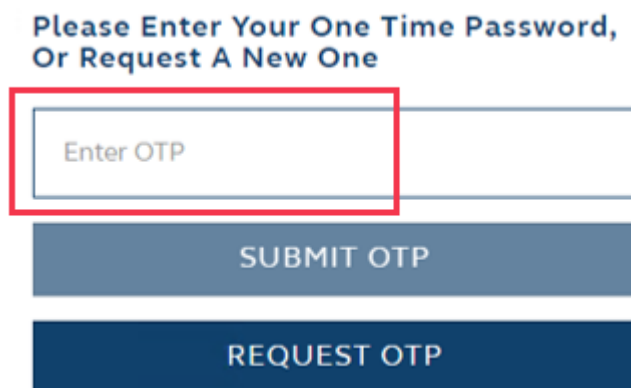
- p) Click <ACCEPT> on the warning message



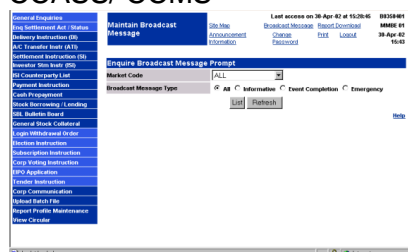
- q) OTP will be sent to user's registered email address



- r) Input OTP and click <SUBMIT OTP>



- s) Successfully logon
CCASS/ CCMS



DMS



3. On-going logon with 2FA:

- t) Access to CCASS/ CCMS via <https://www.ccass.com/>
OR access to DMS via <https://www.ccass.com/dms>

- u) Click the appropriate function
CCASS/ CCMS



DMS



- v) Enter User ID and Password, then click <LOG IN>
CCASS/ CCMS

DMS

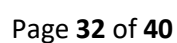
- w) Obtain OTP by mobile application or email (per user's setup), then input OTP and click <SUBMIT> or <SUBMIT OTP>

By Mobile Application
User to generate OTP from mobile application

By email

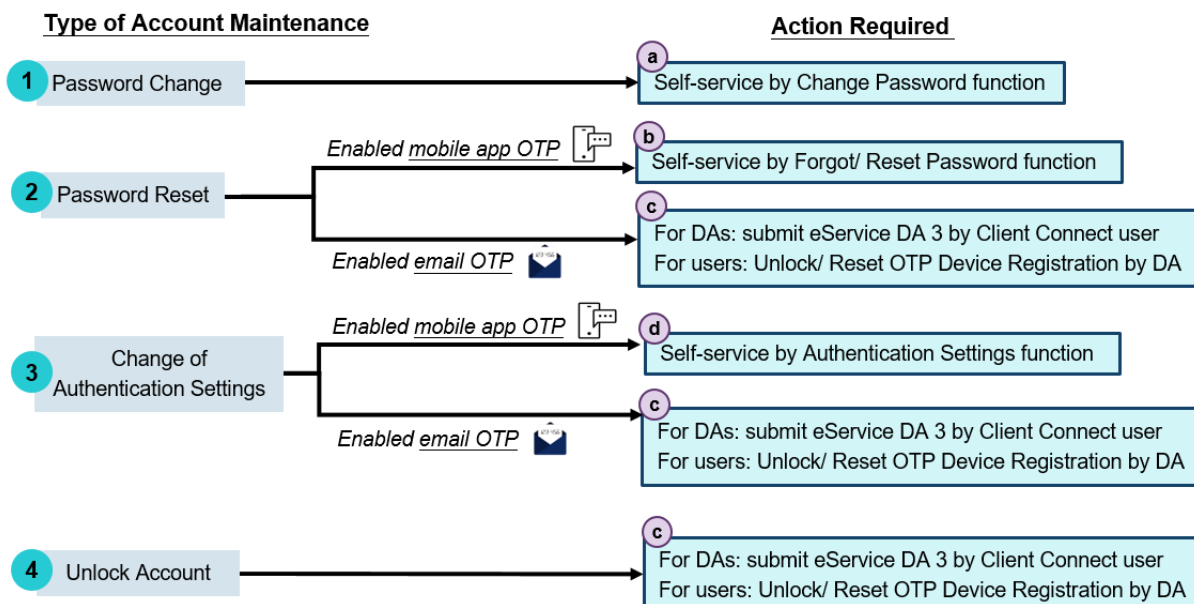
OTP will be sent to user's registered email address

g) Successfully logon
CCASS/ CCMS



Appendix D. Account Maintenance for Users and DAs

The following is the action required for the respective account maintenance functions, and also the demonstration of each action required:



a. Self-service by Change Password function – for Password Change

Password should be changed at least every 90 days. Once the password is expired, user or DA will be required to change password after inputting his/ her User ID and the expired password at the login page.

- a) Access to CCASS/ CCMS via <https://www.ccass.com/>
OR access to DMS via <https://www.ccass.com/dms>

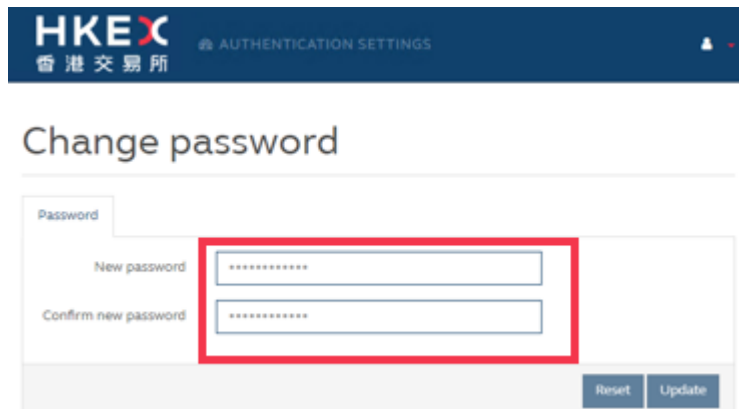
- b) Click <Change Password>
CCASS/ CCMS



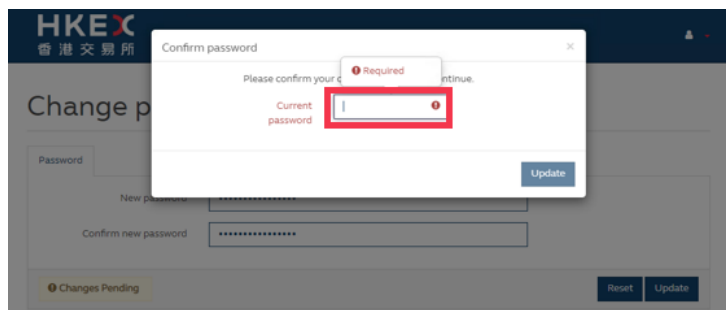
DMS



- c) A pop-up page will be displayed. Enter new password twice, then click <Update>



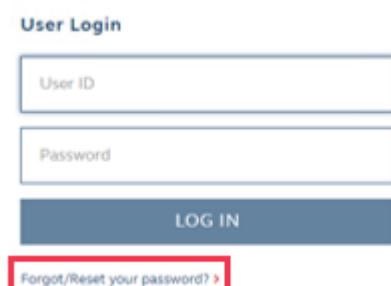
- d) Enter the current password, then click <Update>



- e) DA and user should enter the new password for accessing to CCASS/ CCMS or DMS in the next login.

b. Self-service by Forgot/ Reset Password function – for Password Reset (enabled mobile app OTP)

- a) Access to CCASS/ CCMS via <https://www.ccass.com/>
OR access to DMS via <https://www.ccass.com/dms>
- b) Click <Forgot/Reset your Password>



- c) A pop-up box will be displayed. Enter User ID, then click <SUBMIT>

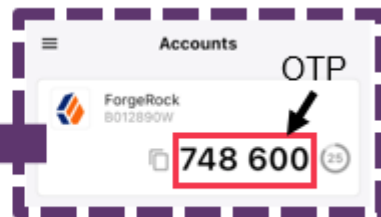
Input User ID

SUBMIT

- d) Enter OTP obtained from mobile application, then click <SUBMIT OTP>

ForgeRock Authenticator (OATH)

SUBMIT



- e) Enter new password twice, then click <SUBMIT>

Reset Password

Please enter your new password below.

SUBMIT

[Close](#)

- f) Password changed successfully, click <Close>. The pop-up box will be closed



- g) User and DA should enter the new password for accessing to CCASS/ CCMS or DMS in the next login.

c. Submit eService DA3 by Client Connect user – for Password Reset & Change of Authentication Settings (enabled email OTP) and Unlock Account for DAs

- a) Submit eService DA3 in Client Connect via [HKEX Access Management Portal](#)

- b) Under Details of Requests, enter User ID and the registered email address of the DA, and select <Unlock DA Account>.

- c) A system generated email notification will be available upon the completion of the request

DA 3 - CCASS/ CCMS Delegated Administrator Application/ Maintenance Form (DA3_00013361 from B01234)
From: HKEX Client Connect <noreply_connect@hkex.com.hk> Date: Mon 18:29

HKEX Client Connect

For reference: the eService is Completed

Reference Number	DA3_00013361
Workflow Status	Completed
Notification Type	For reference
Just Processed By	HKEX
Require action from	Nil

To view the record, please visit the HKEX Client Connect and search the Reference Number (DA3_00013361)

You may visit the record to download a PDF version of the eService for reference if needed.

- d) In the next login, DA will need to carry out both “Set up password” and “Set up OTP Channel” procedure as if first time logon as indicated in [Appendix C](#).

c. Unlock/ Reset OTP Device Registration by DA - for Password Reset & Change of Authentication Settings (enabled email OTP) and Unlock Account for Users

- a) After logging into DMS, click <Maintain User Profile>, then click <Change User Profile>

HKEX 香港交易所

Maintain User Profile Change User Profile Site Map Logout Change Password

View Listings Enquire User Profile

View Reports Logon Success

- b) Enter User ID and click <Submit>

User Profile Print Site Map Logout Change Password DUPC 01 15-Apr-23 12:56:56

Change User Profile - Prompt

User ID Submit

Search by ☒ User ID ☐ User Name

Search Filter

List Refresh

- c) Click the radio button of <Unlock/ Reset OTP Device Registration>, then click <Change>

Change User Profile - Detail

This is an end-user profile

Organisation	B01289 SOUTH CHINA SECURITIES LTD
Internal/External	EXTERNAL
User ID	B012890W
User Status	<input checked="" type="radio"/> ENABLED <input type="radio"/> DISABLED
Surname	EU01
Other Names	EU01
Email	ossa_eu1@hkex.com.hk
Enable From	<input type="text"/> DD/MM/YY
Disable After	<input type="text"/> DD/MM/YY
Locked	No <input checked="" type="radio"/> Unlock/Reset OTP Device Registration
OTP Enabled	Yes
Clearing House Options	Cash
Access Channel	CJT

Change **Refresh**

- d) Enter Checker ID and Authorization Code, then click <Confirm>. Confirmation message will be displayed on the bottom of the page

Change User Profile - Confirmation

This is an end-user profile

Organisation	B01289 SOUTH CHINA SECURITIES LTD
Internal/External	EXTERNAL
User ID	B012890W
User Status	ENABLED
Surname	EU01
Other Names	EU01
Email	ossa_eu1@hkex.com.hk
Enable From	
Disable After	
Locked	No <input checked="" type="radio"/> Will Unlock/Reset OTP Device Registration
OTP Enabled	Yes
Clearing House Options	Cash
Access Channel	CJT
Transaction limit (HKD)	0.00

Checker ID

Authorisation Code

Confirm **Back**

THE ABOVE USER PROFILE IS CHANGED SUCCESSFULLY

- e) In the next login, user will need to carry out both “Set up password” and “Set up OTP Channel” procedure as if first time logon as indicated in [Appendix C](#).

d. Self-service Authentication Settings function

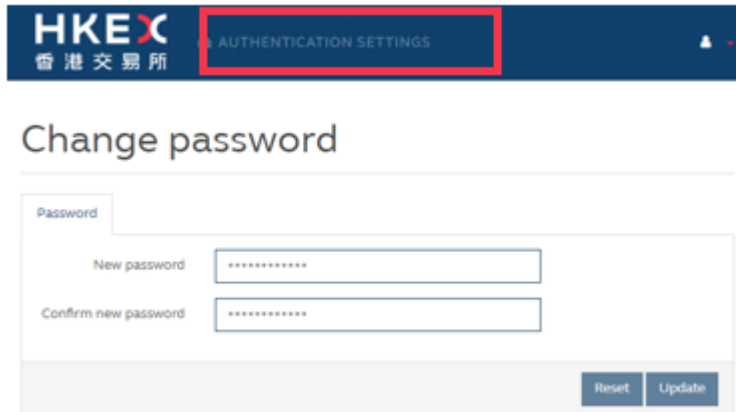
In case DA or user need to change another mobile device or authentication method to obtain OTP, given that the DA or user has registered mobile device to obtain OTP, they can perform self-service authentication settings; for those who have enabled email to obtain OTP or have lost the registered mobile device, please refer to Action Required (c) for the detailed procedure.


- a) Access to CCASS/ CCMS via <https://www.ccass.com/>
OR access to DMS via <https://www.ccass.com/dms>

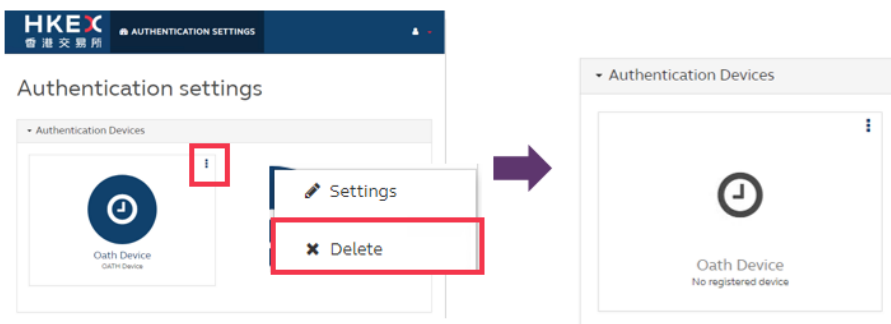
- b) Click <Change Password>
CCASS/ CCMS



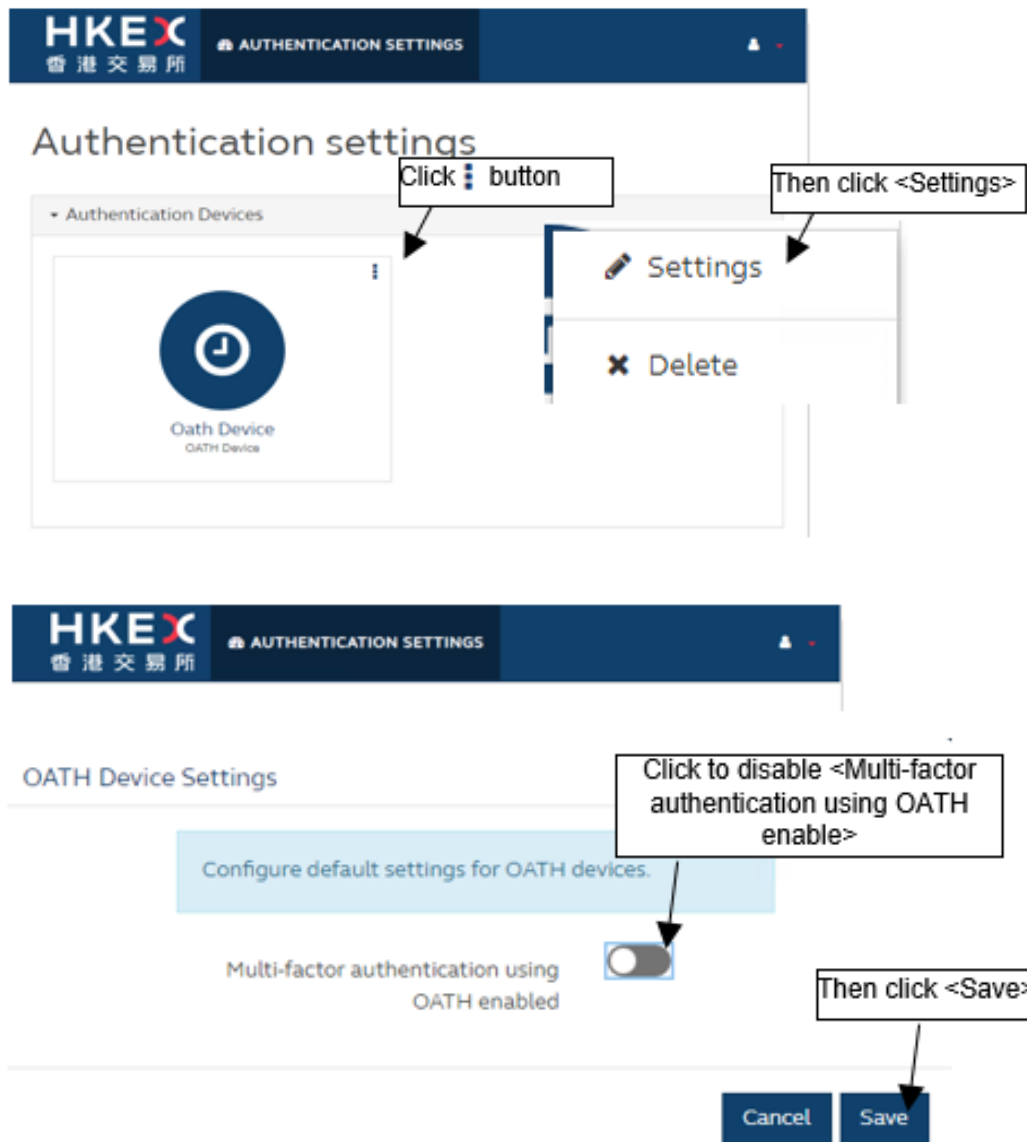
- c) A pop-up page will be displayed. Click <AUTHENTICATION SETTINGS>



- d) To change the mobile device, click  button, then click <x Delete> to delete the registered mobile device for OTP, then the registered device record will be removed. In the next login, user or DA will need to carry out “Set up OTP Channel” procedure to register another mobile device.



- e) If DA or users opt to choose email as OTP delivery method instead of mobile device, click <⋮> button then click <Settings>. Users can disable <Multi-factor authentication using OATH enable> and click <Save>. DA or user shall enter User ID, password and OTP obtained from the designated email address for the next login.



Remarks: HKEX suggests DAs and users to enable mobile OTP for optimal account security, and that they can make use of the self-service password reset function.