3 Getting Started For Client Connect

3.4 LOGIN AND LOGOFF

This section mainly explains the procedures for connecting to and disconnecting from Client Connect (i.e. **login** and **logoff** Client Connect).

Users can connect to Client Connect by logging in via desktop computer, tablet and mobile device to access eServices and other functions of Client Connect via https://connect.hkex.com.hk. Logging off Client Connect disconnects users from Client Connect. The login session will also be disconnected after 15 minutes of idle time to prevent any unauthorized persons to access Client Connect functions.

This section is divided into several parts:

- First Time Login to Client Connect
- Subsequent Login to Client Connect
- Changing One Time Password (OTP) Channel
- Logoff Client Connect
- Inactivity Timeout

FIRST TIME LOGIN TO CLIENT CONNECT

Before starting the login process, please make sure:

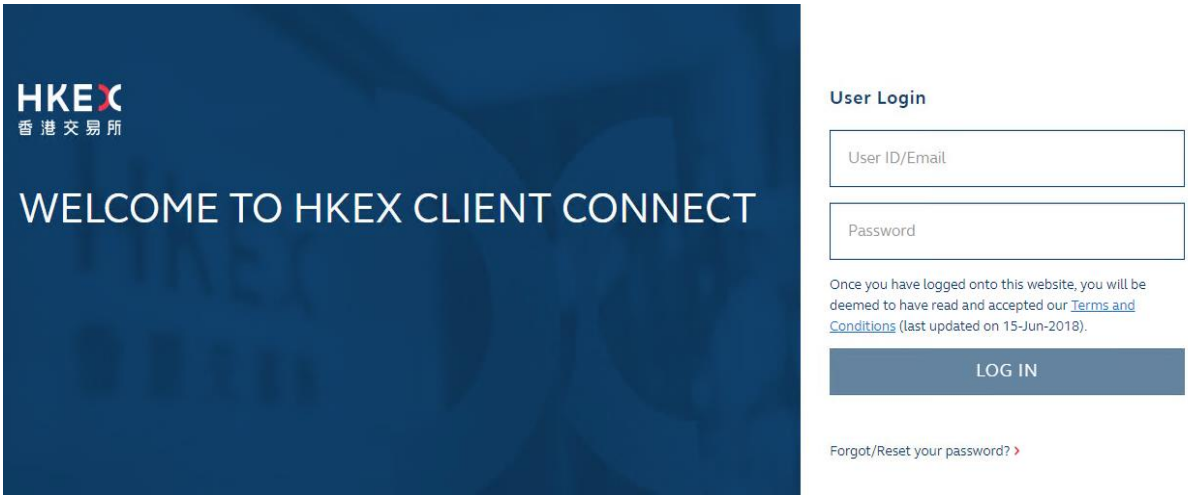
- The Client Connect account has been setup
- The Client Connect login password and OTP channel have been setup
- The mobile application **ForgeRock Authenticator** has been installed in the mobile device and Client Connect account has been registered if users choose to receive OTP through mobile device.

Operation Steps:

1. Launch the browser via desktop computer, tablet or mobile device.

2. Type Client Connect URL https://connect.hkex.com.hk in the address bar.

3. Enter Client Connect login user ID (email) and Password, then click **LOG IN.**

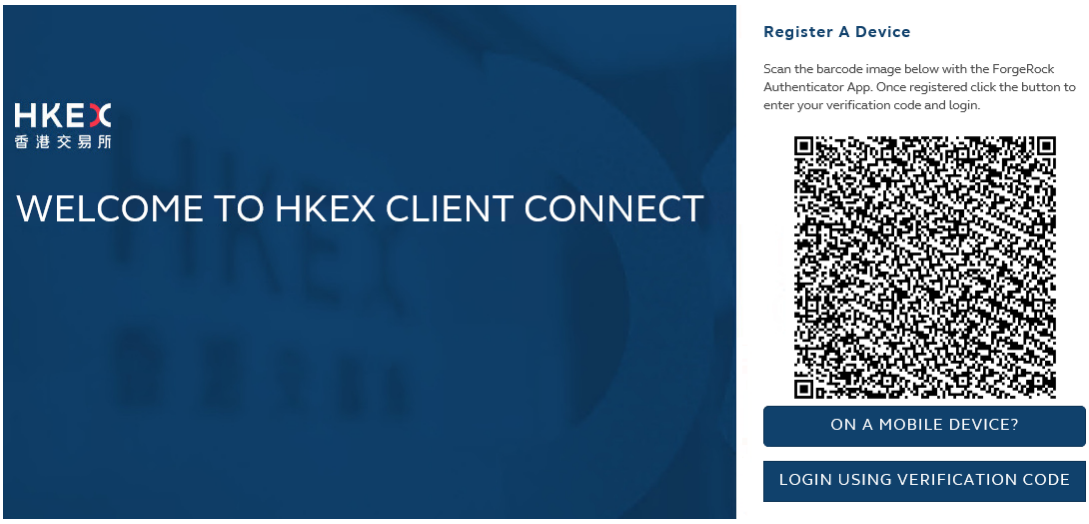


4. Choose the channel of receiving the OTP, either via (a) mobile application, or (b) email. Only one channel can be chosen at one time.

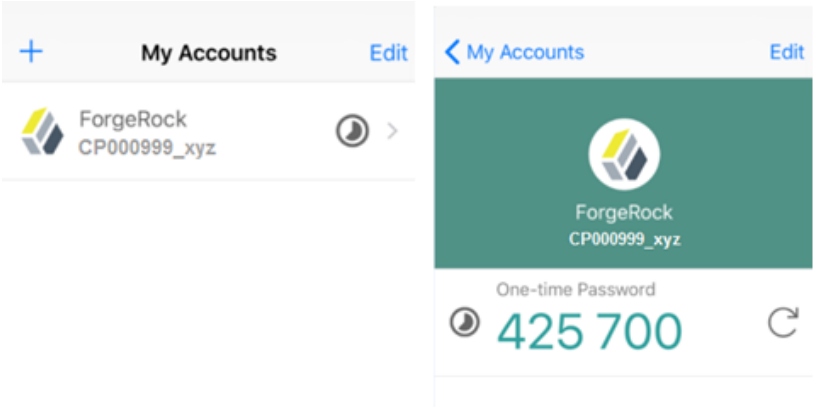
(a) Receiving OTP via mobile application:

Operation steps:

1. Users have to use ForgeRock Authenticator application to generate OTP. The application can be downloaded from Google Playstore for Android users or Apple iTunes Store for iOS users. Once the application is installed, click **REGISTER DEVICE** and a QR code will appear.



2. Use the + sign in the application to switch on the camera, then scan the QR code to register the account in the application. The account will appear in the application once successfully registered.



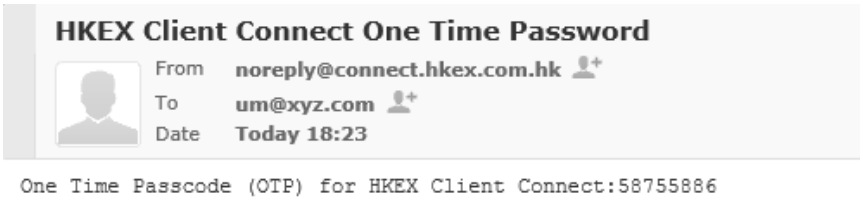
3. In Client Connect, click **LOGIN USING VERIFICATION CODE** to enter the code generated by the mobile application. OTP obtained via mobile application has no expiry period but can only be used once per generation.

4. If users are logging in to Client Connect using mobile devices, ensure the ForgeRock Authenticator application is already installed, then click **ON A MOBILE DEVICE?** to register the account.

(b) Receiving OTP via email

Operation steps:

1. Click **SKIP THIS STEP** and the OTP will be sent to users via the email address used to login to Client Connect. OTP obtained via email will remain valid for 5 minutes.



2. Input the OTP and click **SUBMIT OTP** to log in Client Connect.

3. A new OTP will be generated and sent via email if users click **REQUEST OTP**.

SUBSEQUENT LOGIN TO CLIENT CONNECT

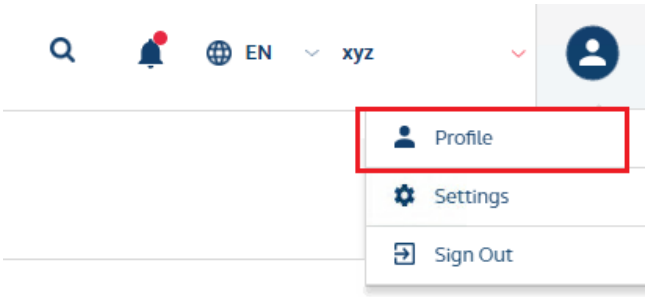
For subsequent login to Client Connect, users are not required to select OTP channel again. After inputting user ID and password, users will be prompted to input OTP via email or mobile application that they previously selected. Users can view Client Connect dashboard upon successful login.

CHANGING ONE TIME PASSWORD (OTP) CHANNEL

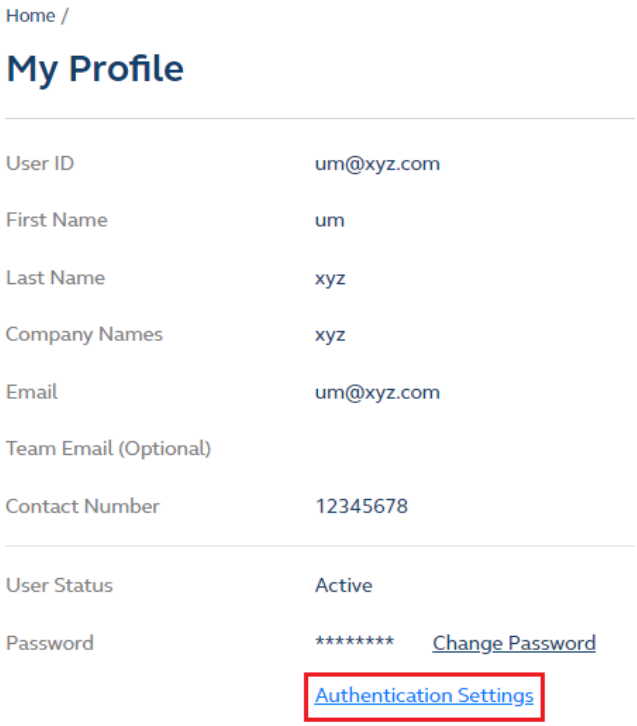
(a) Switch from email to mobile device

Operation steps:

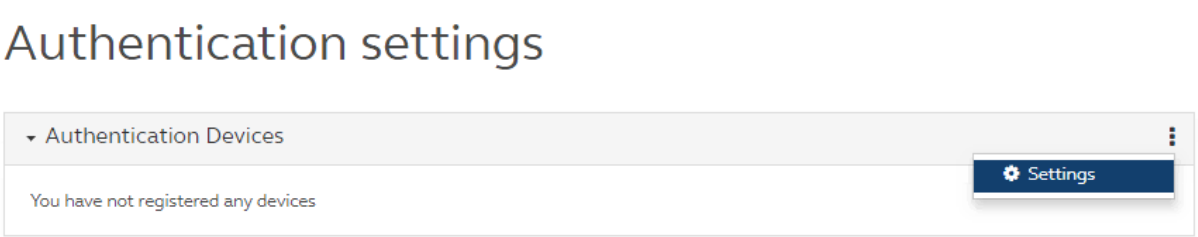
1. After logging in to Client Connect, click **Profile** at upper right corner.



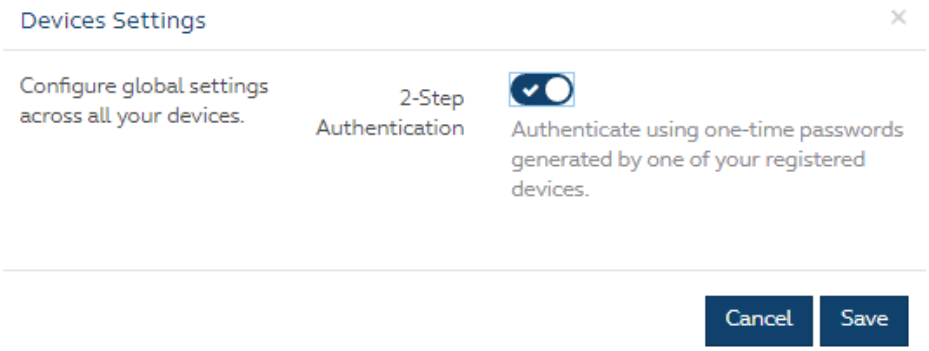
2. Go to **Authentication Settings**.



3. Go to **Settings**.



4. Reset the authentication method and generate OTP by registered device.

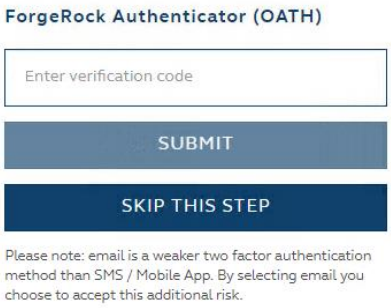


5. Users will be prompted to choose the OTP channel upon next login.

(b) Switch from mobile application to email

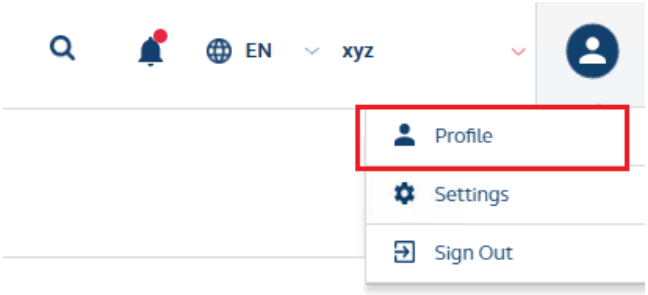
Operation steps (if users have not logged in to Client Connect)

1. Users click **SKIP THIS STEP** and then input OTP via email.

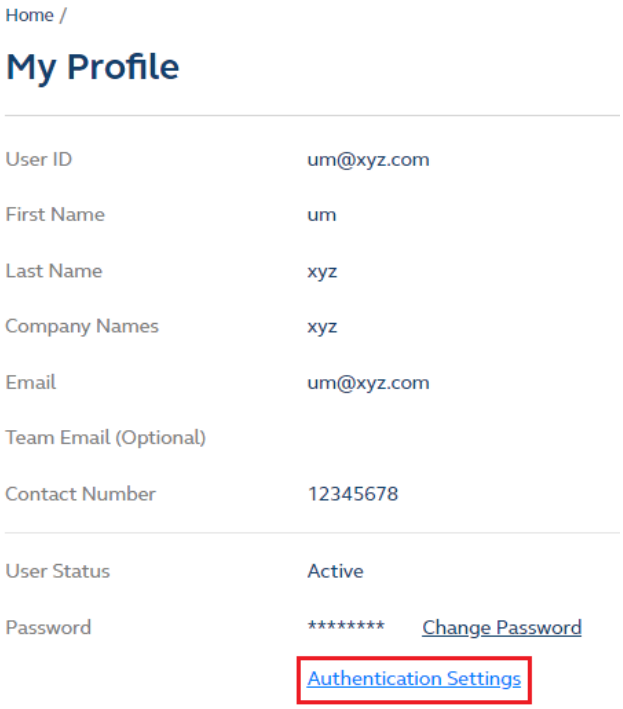


Operation steps (if users have logged in to Client Connect already)

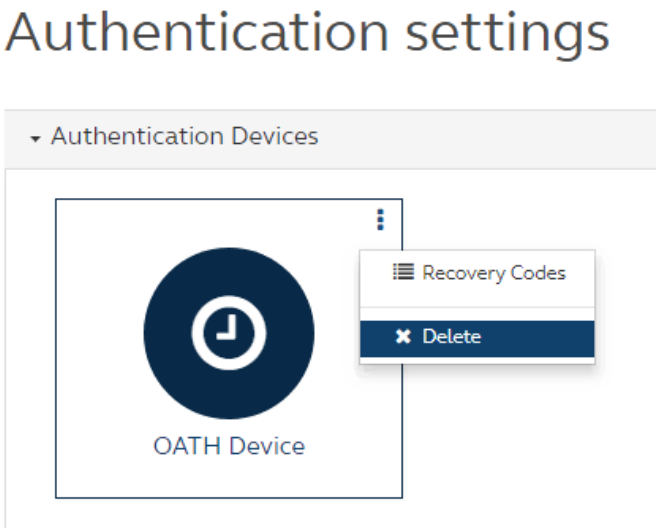
1. Go to **Profile** at upper right corner of Client Connect.



2. Go to **Authentication Settings**.



3. Go to existing registered device and click **Delete**.

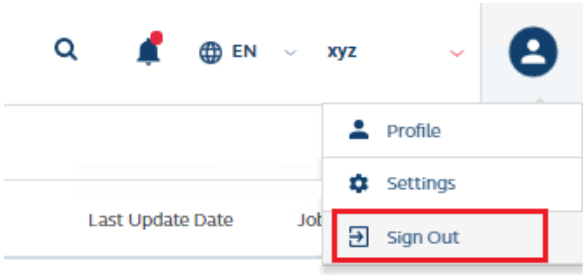


4. Users will be prompted to choose the OTP channel upon next login.

LOGOFF CLIENT CONNECT

Operation Steps (if users have logged in to Client Connect already):

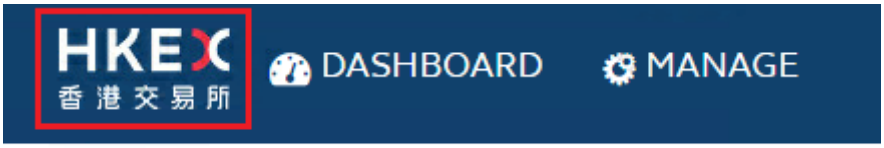
1. Click **Sign Out** at upper right corner.



2. You will return to the login screen upon successful log off.

Operation Steps (if CCDA is at Access Management):

1. Click **HKEX logo** at upper left corner to switch to Client Connect to sign out.



INACTIVITY TIMEOUT

For security purpose, Client Connect is automatically logged off after 15 minutes of idle time. This prevents other unauthorized persons from using the Client Connect account. Users will be navigated to the login screen upon session timeout. To access and use Client Connect again, users have to perform the login procedures.