

Latest updates are highlighted in orange

Getting Started

VaR Online is only accessible by authorized users. The assignment of Delegated Administrators is centralized and administered by HKSCC while the Delegated Administrators of the Clearing Participants are responsible for creating and managing the Business Users access to VaR Online. This section is divided into the following sub-sections to introduce the access and user management of VaR Online.

- 2.1 Access Management
- 2.2 User Management via VaR DA Platform
- 2.3 Password and Authentication Settings
- 2.4 Login and Logoff

2.1 ACCESS MANAGEMENT

Access management is implemented to ensure that only authorized users are allowed to access VaR Online. Clearing Participants should apply for VaR Online Delegated Administrator (VaR DA) from HKSCC. VaR DAs are responsible to manage Business Users' profile and grant VaR Online access to Business Users.

This sub-section provides details on VaR Online access management, covering the following key information:

- Setup of VaR DAs / Business Users
- Initial Password Setup
- Authentication Setting
- Locked / Unlock User Account
- Inactivity Timeout

Setup of VaR DAs / Business Users

To apply for VaR DAs, please submit the "VaR Online Delegated Administrator Rights Application / Maintenance Form" via [Client Connect](#) (eService ID: DA 1) by Client Connect Delegated Administrators (CCDAs) or Business Users with the access right "EU_UserMaintenance". Please ensure a valid corporate email address is provided for each VaR DA. When HKSCC completed the creation of VaR DA accounts, a notification email will be sent to VaR DAs.

The same applies to VaR Business Users, when VaR DAs set up VaR Business User accounts, corporate email addresses of the Business Users should be provided.

Initial Password Setup

Once VaR DA or VaR Business User account is created, DA or Business User would receive email notification with complete user ID and instructions to set up password via:

- VaR DA platform <https://idm.hkexposttrade.com.hk/user-management/>
(Available from 7:00 a.m. to 1:00 a.m. on Mondays to Fridays, except for public holidays)
- VaR Online <https://rmcd.hkexposttrade.com.hk>
(Available from 10:00 a.m. to 7:30 p.m. on Mondays to Fridays, except for public holidays)

Please refer to section 2.4.1 for initial password set up.

Authentication Setting

VaR DA platform & VaR Online adopt 2-Factor Authentication, being

1. VaR DA / VaR Business User self-defined password, plus
2. One Time Password (OTP) received via email or ForgeRock Authenticator mobile application

Please refer to section 2.3.2 for changing password and changing channel/ mobile device to receive OTP.

Locked / Unlock User Account

VaR DA or VaR Business User access will be locked after 5 consecutive unsuccessful attempts of login within 30 minutes. An email will be sent to the VaR DA or VaR Business User to notify the account status. To unlock the account:

- VaR DA – please request HKEX to unlock account via email to VaRDA_unlock@hkex.com.hk.
- VaR Business User – please request VaR DA to unlock the user access, VaR DA may refer to section 2.2.1 for detailed steps to unlock an account.

After the account is unlocked, you will receive an email. Please click <Forgot/Reset your password> at VaR DA platform/ VaR Online login page to reset login password and re-register mobile device. Detailed steps please refer to steps 2 to 8 under section 2.4.1 FIRST TIME LOGIN ON VAR DA PLATFORM/ VAR ONLINE.

Inactivity Timeout

To prevent unauthorized access to VaR DA Platform and VaR Online, the idle time for both systems is set at 15-minutes. Users please re-login if needed.

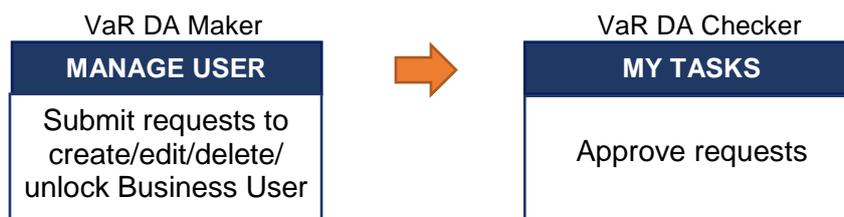
2.2 USER MANAGEMENT VIA VAR DA PLATFORM

Delegated Administrators can access VaR DA Platform by below URL via Google Chrome:

<https://idm.hkexposttrade.com.hk/user-management/>

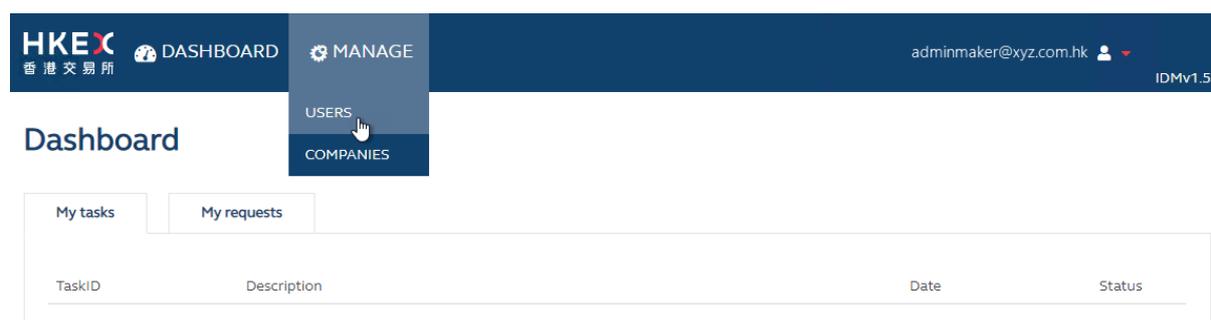
(Available from 7:00 a.m. to 1:00 a.m. on Mondays to Fridays, except for public holidays)

To create/ edit/ delete/ unlock a Business User account:



2.2.1 DA MAKER – SUBMIT REQUEST FOR USER MAINTENANCE

On the main page of DA Platform, DA (maker) can go to <MANAGE> and then click on <USERS> to access manage user related functions.



Create Users

1. Click on <+ CREATE USER>

Users



2. Fill in the user details and note below:

- **User ID** Must be alphanumeric and no special character is allowed (e.g. DA100). System will auto append company ID of the user's company in the front when submitted the request. (e.g. 000123_DA100)
- **Company** DA (maker) can only input the **Company** that he/ she manages. Once the company name is filled in, **ROLES** tab will appear.
- **Email** Must be a unique corporate email.
- **Business Application Name** Default as **VaR Online**.

Section 2 Getting Started

- User Type
- User Status

Default as **Business**, should NOT be changed.
Default as **Active**, should NOT be changed. If it is changed to **Inactive**, created Business User would be unable to access VaR Online.

User CANCEL CREATE

Create User

Details Roles

User ID

First Name

Last Name

Company

Title (optional)

Email

Team Email (optional)

Contact Number (optional)

Business Application Name VaR Online

User Type Admin Business

Internal/External Internal External

User Status Active Inactive

3. Click <Roles> tab and then DA (maker) should click + sign next to company name to expand and click on the role EU_ORP_EXTERNALCOREDESKTOP

User CANCEL CREATE

Create User

Details Roles

ADD MORE COMPANIES

XYZ Company Limited	-	<input checked="" type="checkbox"/> EU_ORP_EXTERNALCOREDESKTOP
HKSCC Participant	-	
VaR Online		

4. After completing all required information, click <CREATE> to submit the request. A pop-up window will display to request for confirmation. Please review and click <CREATE> to confirm. The submitted request requires checker's approval.

Edit Users

1. If there are existing users, a user list will display after clicking <MANAGE> and then <USERS>.
2. On the user list, click on the particular Business User row to edit.
3. Click <EDIT> on the <Details> page to edit user information.

Note: Roles of Business Users is default as EU_ORP_EXTERNALCOREDESKTOP, NO change is allowed

User
Business User A [DELETE](#) [EDIT](#)

Details Roles

User ID	999999_businessuser1
First Name	Business
Last Name	User A

User
Business User A [CANCEL](#) [SUBMIT](#)

Details Roles

User ID	999999_businessuser1
First Name	<input type="text" value="Edit"/>
Last Name	<input type="text" value="User"/>
Company	XYZ Company Limited
Title (optional)	<input type="text"/>
Email	<input type="text" value="businessusera@xyz.com.hk"/>
Team Email (optional)	<input type="text"/>
Contact Number (optional)	<input type="text"/>
Business Application Name	<input checked="" type="checkbox"/> VaR Online
User Type	<input type="checkbox"/> Admin <input checked="" type="checkbox"/> Business
Internal/External	External
User Status	<input checked="" type="radio"/> Active <input type="radio"/> Inactive

4. Amend user information and click <SUBMIT> to submit the change. A pop-up window will display to request for confirmation. Please review and click <SUBMIT> to confirm. The submitted request requires checker's approval.

Note: DAs (maker) may suspend/ reactivate a user by changing the User Status, i.e. <Active> or <Inactive>. Business Users are not required to reset password/ mobile device registration after account reactivation.

Delete Users

1. If there are existing users, a user list will be shown after clicking <MANAGE> and then <USERS>.
2. On the user list, click the particular Business User row to delete.
3. Click <DELETE> on the <Details> page to submit the user deletion.
4. A pop-up window will display to request for confirmation. Please review and click <DELETE> to confirm. Deletion will require checker's approval.

Remarks: Upon approval, Business User is no longer found in VaR DA platform and user status shown in user listing report will be changed to "INACTIVE". This account will be deleted from database within 72hrs.

Edit or Delete VaR DAs

To request for user maintenance of VaR DAs including:

- Edit user information
- Delete VaR DA's roles from certain managed company(ies)
- Delete VaR DA account from VaR DA Platform

Please submit "VaR Online Delegated Administrator Rights Application / Maintenance Form" via [Client Connect](#) (eService ID: DA 1) by Client Connect Delegated Administrators (CCDAs) or Business Users with the access right "EU_UserMaintenance".

Unlock Account/ Reset Device Registrations

A user account will be locked after five unsuccessful attempts to login within 30 minutes. Locked VaR DA accounts can only be unlocked by HKEX, while VaR DAs can unlock their Business User accounts.

1. Retrieve the user details by clicking <MANAGE>, <USERS>, then click on the particular Business User from user list to unlock.
2. On the Business User <Details> page, scroll to the bottom and click on <Unlock Account/Reset Device Registration> hyperlink.

User Type	Business
Internal/External	External
User Status	Active
Is Deleted	No
Is Locked	No

[Unlock Account/Reset Device Registration](#)

3. A pop-up window will display to request for confirmation. Please review and click <UNLOCK> to confirm. Unlock account request will require checker's approval.

Remarks: Upon the unlock account request is approved by DA (checker), Business User's account will be unlocked, he/ she must re-register mobile device registration.

View Submitted Requests

1. Go to <DASHBOARD> and then <My Requests>, a list of submitted requests is displayed here.

The screenshot shows the HKEC Dashboard interface. The top navigation bar includes the HKEC logo, 'DASHBOARD', and 'MANAGE' options. The user's email 'adminmaker@xyz.com.hk' and version 'IDMv1.5' are displayed on the right. The main content area is titled 'Dashboard' and features two tabs: 'My tasks' and 'My requests'. The 'My requests' tab is active, displaying a table with the following data:

TaskID	Description	Date	Status
0010	CREATE USER	28-Jan-2021	Pending
0011	EDIT USER	28-Jan-2021	Pending

2. Click on the particular request row to see details of requests.

Remarks: Once a request is processed, it will be removed from Dashboard.

Notification Email to DA (maker)

For requests submitted for checker's approval, DAs (maker) within the same company will receive acknowledgment email. An example is shown below:

HKSCC System

Creation of a new user is submitted

Reference Number	0010
Status	Pending approval
Notification Type	For reference
Requested by	Admin Maker
Message	Nil



For enquiries, please contact us via [link](#).

Please do not reply this e-mail as this is system generated.

Disclaimer

The information contained in this email is intended only for the use of the individual or entity named above and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this message in error, please immediately notify us and delete the email. Internet communication cannot be guaranteed to be timely, secure, error-free or virus-free. The sender does not accept liability for any errors or omissions. Thank you.

2.2.2 DA CHECKER – APPROVE REQUEST FOR USER MAINTENANCE

Notification Email to DA (Checker)

User maintenance requests must go through DA (checker)'s approval. Once DA (maker) has submitted request, DA (checker) will receive a notification email like below for follow-up action.



View and Approve/ Reject Requests

1. Go to <DASHBOARD> and <My Tasks>, all requests pending for action are listed here.



Dashboard

My tasks		My requests	
TaskID	Description	Date	Status
0010	CREATE USER	28-Jan-2021	Pending
0011	EDIT USER	28-Jan-2021	Pending

2. Click the particular pending request to view details.

Section 2 Getting Started

Task

CREATE USER

	REJECT	APPROVE
Task Status	Pending approval	
User ID	999999_businessuser2	
First Name	Business	
Last Name	User B	
Company	XYZ Company Limited	
Title (Optional)		
Email	businessuserb@xyz.com.hk	
Team Email (Optional)		
Contact Number (Optional)		
Business Application Name	VaR Online	
User Type	Business	
Internal/External	External	
User Status	Active	
Roles	XYZ Company Limited - HKSCC Participant Roles: EU_ORP_EXTERNALCOREDESKTOP	
Date	28-Jan-2021	

3. After review, checker can click <APPROVE> or <REJECT> directly.
4. A confirmation pop-up window will display. DA (checker) can input his/ her comment on the request. Then, checker can click <APPROVE> or <REJECT> to complete the process.

CONFIRM

Are you sure you want to approve 0010 request?

Type your comments here

CANCEL **APPROVE**

Remarks: If a DA (checker) rejects a request, he/she must provide comment.

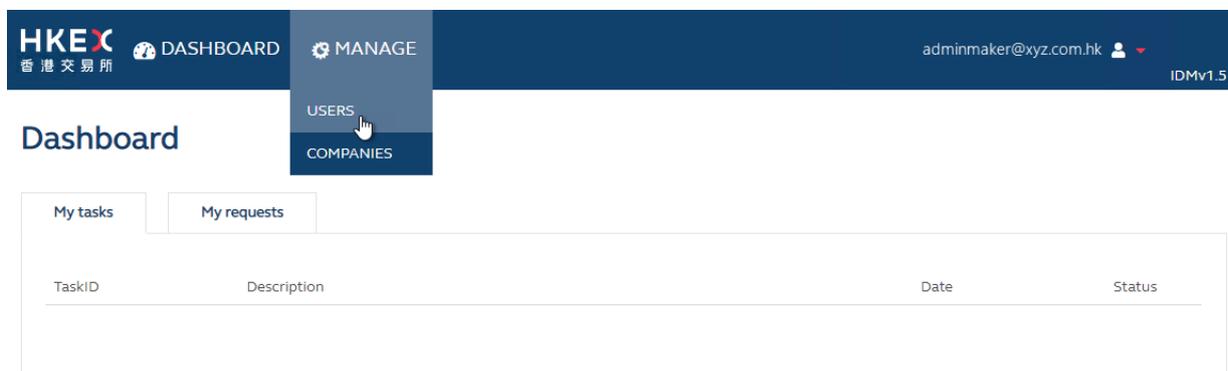
Notification Email to DA (maker)

Upon approval/ rejection of request, DA (maker) will receive a notification email like below:

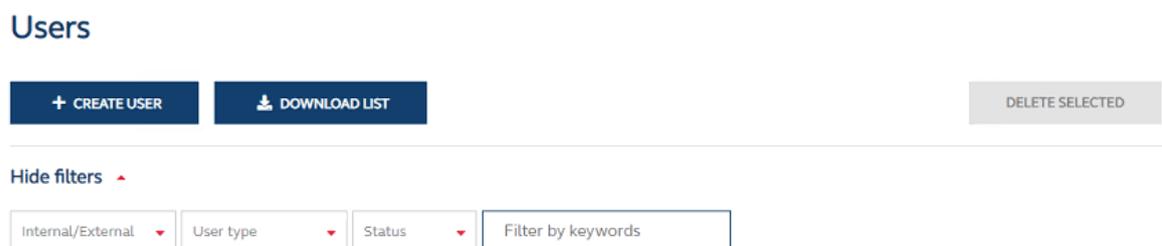


2.2.3 VIEW USER

Both maker and checker of DA can go to <MANAGE> and then <USERS> to view user list.



Then, a list of users is displayed. Users can also click <Show filters> to apply filters and search for a particular user.



Section 2 Getting Started

To view details of a particular user, DAs may click the related user row.

Users

+ CREATE USER
DOWNLOAD LIST
DELETE SELECTED

Show filters ▾

<input type="checkbox"/> NAME ▾	INTERNAL/ EXTERNAL ▾	USER TYPE ▾	COMPANY ▾	STATUS ▾
<input type="checkbox"/> Business User A	External	Business	XYZ Company Limited	Active
<input type="checkbox"/> Business User B	External	Business	XYZ Company Limited	Active

From the list of users, DAs can click <DOWNLOAD LIST> to export the user list. The file will be downloaded as “users.csv” into your local PC.

Users.csv

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1 The function may contain "Personal Data" that must not be used for any purpose other than that for which they were originally collected.																			
2 Once the data contained in this database or printed reports have ceased to service their legitimate purpose, they must be appropriately destroyed.																			
3																			
4 List of Users																			
5 Business Application	User ID	First Name	Last Name	Title	Email	Team Email	Department	Contact Number	User Status	Is Locked	Is Deleted	Deleted By	Company	Managed Companies	Internal/External	Employee Type	Last Password Change Time	Roles	
6 ORP	999999_damaker	Admin	Maker	adminna					Active	No	No		XYZ Company Limited	XYZ Company Limited	External	Admin		XYZ Company Lin	
7 ORP	999999_dachecker	Admin	Checker	adminchi					Active	No	No		XYZ Company Limited	XYZ Company Limited	External	Admin	20210413 19:19:58		XYZ Company Lin
8 ORP	999999_businessuser1	Business	User A	businessi					Active	No	No		XYZ Company Limited		External	Business			XYZ Company Lin
9 ORP	999999_businessuser2	Business	User B	businessi					Active	No	No		XYZ Company Limited		External	Business	20210413 18:52:27		XYZ Company Lin
10																			
11 Total no. of external users: 4																			
12 No. of Admin users: 2																			
13 No. of Business users: 2																			
14 No. of Admin and Business users: 0																			
15																			
16																			

Description of fields:

Field	Description
Business Application	<ul style="list-style-type: none"> Always “ORP”
User ID	<ul style="list-style-type: none"> User ID assigned to user i.e. [company ID]_[User ID]
First Name	<ul style="list-style-type: none"> First name of user
Last Name	<ul style="list-style-type: none"> Last name of user
Title	<ul style="list-style-type: none"> Title of user, optional field
Email	<ul style="list-style-type: none"> The unique corporate email address of user
Team Email	<ul style="list-style-type: none"> Email for a team of users, optional field
Department	<ul style="list-style-type: none"> Not in use, always blank
Contact Number	<ul style="list-style-type: none"> Contact number of user, optional field
User Status	<ul style="list-style-type: none"> Status of user i.e. “Active” or “Inactive”
Is Locked	<ul style="list-style-type: none"> “Yes” = user account is locked

	<ul style="list-style-type: none"> • “No” = user account is not locked
Is Deleted	<ul style="list-style-type: none"> • “Yes” = user account is deleted • “No” = user account is existed
Deleted By	<ul style="list-style-type: none"> • Indicates the execution of deletion • i.e. “Admin” or “System” • Appear as blank when “Is Deleted = No” • “Admin” when user is deleted by HKEX or VaR DA • “System” when user is deleted automatically due to the user is only attached to a deactivated HKSCC identity of a company
Company	<ul style="list-style-type: none"> • Assigned company of user
Managed Companies	<ul style="list-style-type: none"> • The assigned companies to DA for user management • Applicable to DAs only
Internal/External	<ul style="list-style-type: none"> • Always “External”
Employee Type	<ul style="list-style-type: none"> • Type of the user • i.e. “Admin”, “Business” or “Admin; Business”
Last Password Change Time	<ul style="list-style-type: none"> • The date and time when user changed his/ her login password last time
Roles	<ul style="list-style-type: none"> • Role(s) assigned to user
Total no. of External Users	<ul style="list-style-type: none"> • Show the total number of external users
No. of Admin Users	<ul style="list-style-type: none"> • Show the number of users with “Employee Type = Admin”
No. of Business Users	<ul style="list-style-type: none"> • Show the number of users with “Employee Type = Business”
No. of Admin and Business Users	<ul style="list-style-type: none"> • Show the number of users with “Employee Type = Admin; Business”

A User Management Audit Trail Report will be available via Report Access Platform (RAP) on each business day. This report generates in .csv file format and lists user management activities on that day.

2.2.4 VIEW COMPANY AND COMPANY IDENTITY

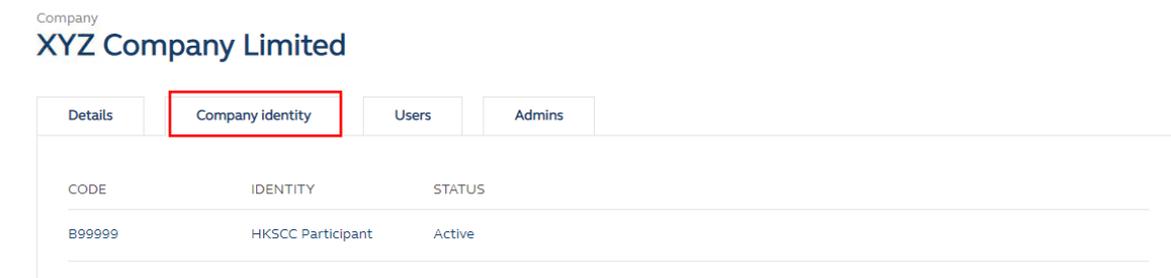
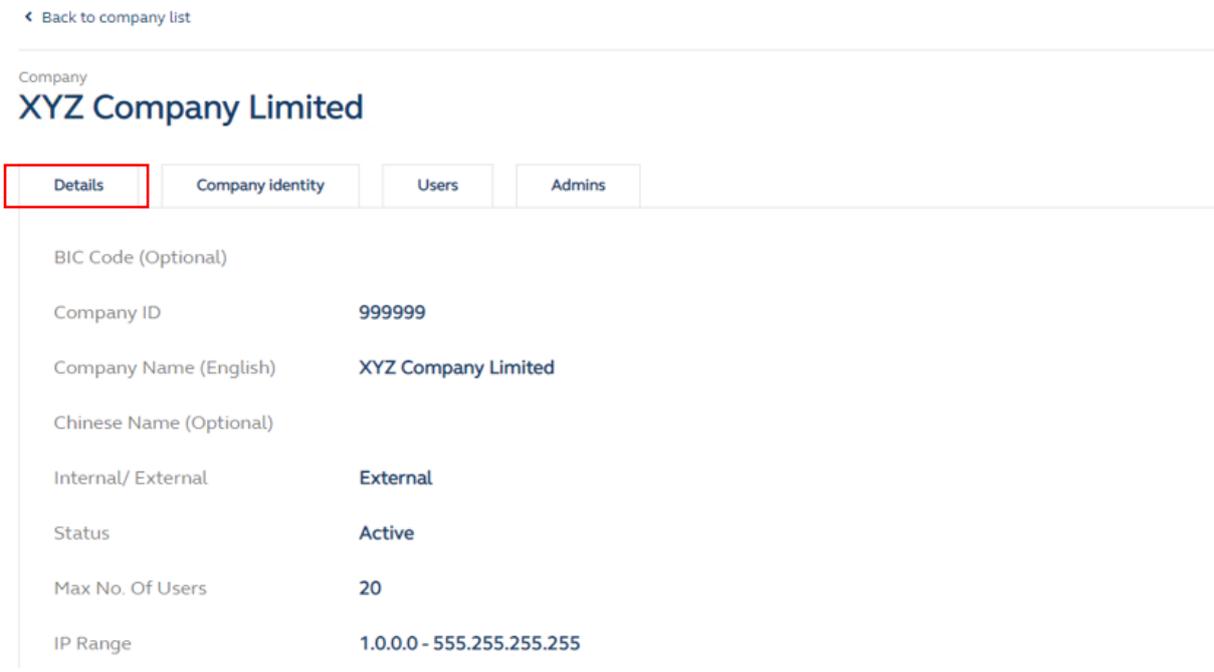
DA (maker) and DA (checker) can view details of their own company from <MANAGE> and then <COMPANIES>.

Section 2 Getting Started



1. After clicking <COMPANIES>, your company's name will be listed. Click the company row to view details.
2. Details will be displayed. DA can click <Company identity>, <Users> or <Admins> tabs to view different information.

Remarks: For DA (maker) viewing <Users> tab, option to <+ CREATE USER> and <DELETE SELECTED> will be displayed.



[← Back to company list](#)

Company

XYZ Company Limited

Details Company identity **Users** Admins

+ CREATE USER DELETE SELECTED

<input type="checkbox"/>	NAME ▾	USER TYPE ▾	STATUS ▾	
<input type="checkbox"/>	Business User A	Business	Active	⋮
<input type="checkbox"/>	Business User B	Business	Active	⋮

Company

XYZ Company Limited

Details Company identity Users **Admins**

NAME ▾	INTERNAL/ EXTERNAL ▾	USER TYPE ▾	COMPANY ▾	STATUS ▾
Administrator Maker	External	Admin	XYZ Company Limited	Active
Administrator Checker	External	Admin	XYZ Company Limited	Active

2.3 PASSWORD AND AUTHENTICATION SETTINGS

2.3.1 PASSWORD REQUIREMENT

To access VaR DA Platform/ VaR Online, user has to setup a login password for his/her account during first time login. Below listed out the login password's requirements:

1. 8-15 characters
2. At least 1 number
3. At least 1 lower letter
4. At least 1 capital letters
5. At least 1 special character from !@#\$\$%^&*()

The password is confidential and should not be disclosed to unauthorized persons. New password shall not be the same as any of the last 5 passwords. If a user is assigned as both Delegated Administrator in VaR DA Platform and Business User in VaR Online, the same set of User ID and Login password will be used to access both platforms.

2.3.2 CHANGE PASSWORD AND AUTHENTICATION SETTING

Delegated Administrators (DAs):

After login to VaR DA Platform, DAs can access to change password site via URL:

<https://sso.hkexpostrade.com.hk/sso?realm=ex>

Business Users:

After login to VaR Online, Business Users can change password from the main view.

Section 2

Getting Started



After clicking CHANGE PASSWORD hyperlink, the change password window will be displayed, please input and confirm new password; then click <Update>.



Change password

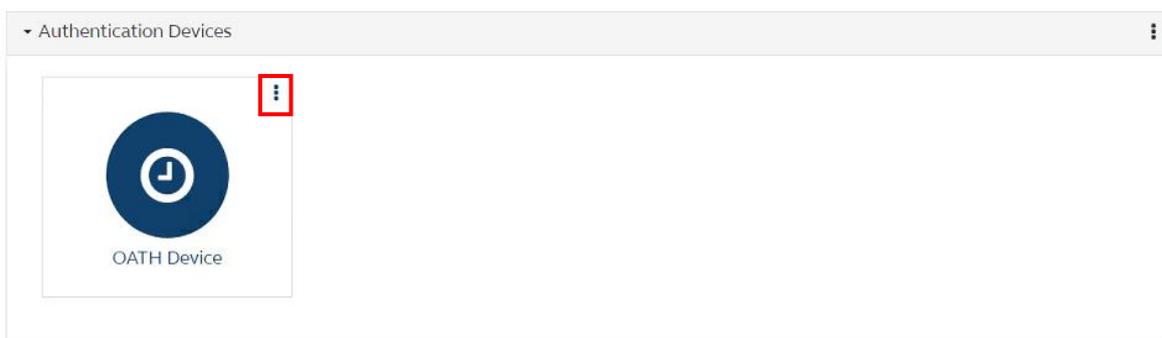
A screenshot of the "Change password" form. It features two input fields: "New password" and "Confirm new password", both containing masked characters (dots). Below the fields are "Reset" and "Update" buttons. The form is set against a light gray background.

Remark: For VaR DAs, password changed via VaR Online will also be applicable to login to VaR DA platform and vice versa.

Users can also click <AUTHENTICATION SETTINGS> to choose OTP delivery method.



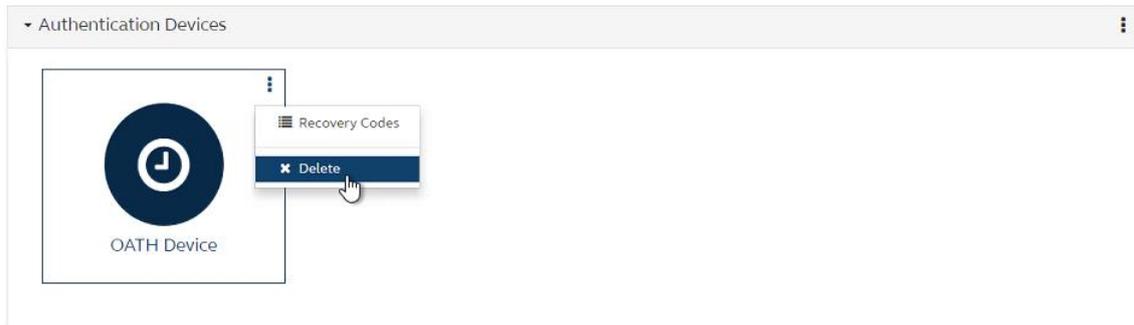
Authentication settings



To change the One-time Password (OTP) mobile device, users may click  to delete the registered mobile device for OTP. Then they should re-register a new mobile device for authentication during next login.



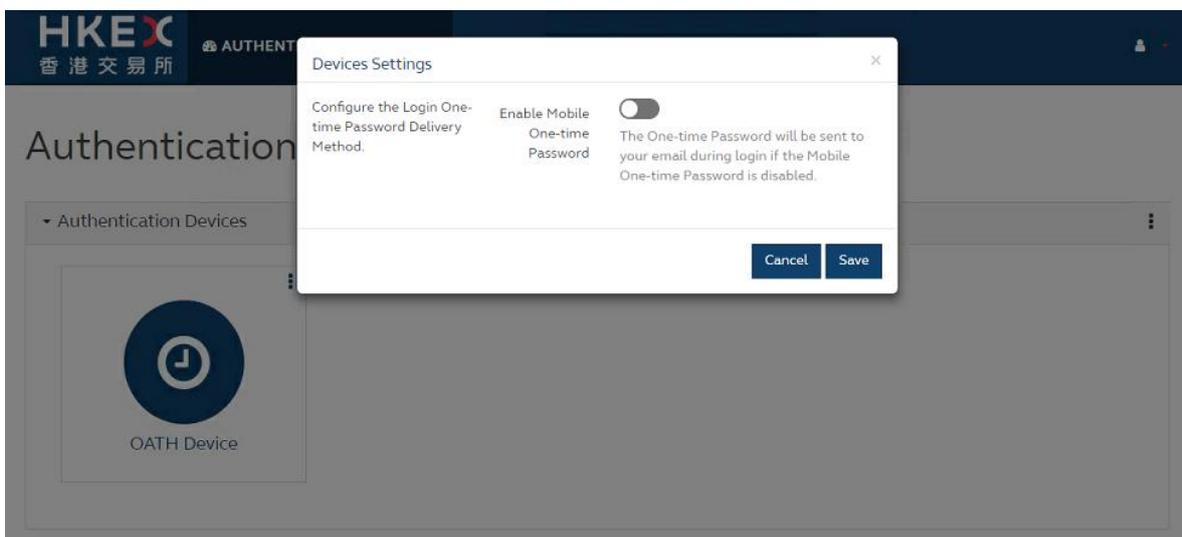
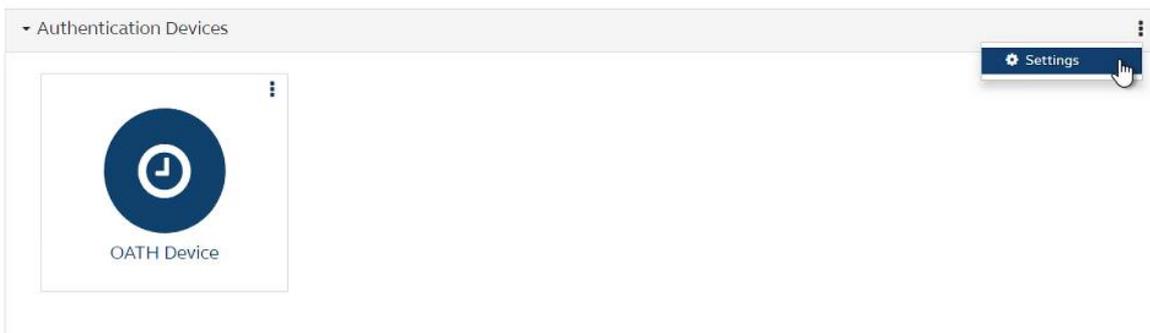
Authentication settings



If users opt to choose email as OTP delivery method instead of mobile device, please click  on the right then choose <Settings>. Users can disable <Mobile One-time Password> and click <Save>.



Authentication settings



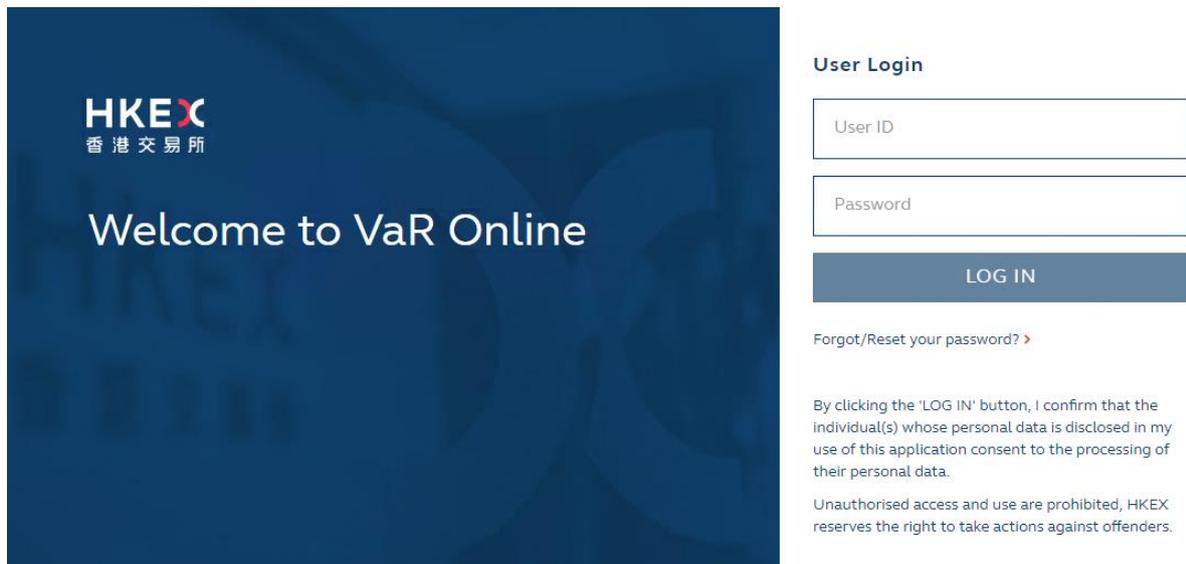
Remarks: HKEX suggests users to enable mobile One-time Password for optimal account security.

2.3.3 FORGOT/ RESET PASSWORD

In case of forgot or reset password, users who enabled mobile OTP may use “Self-service Reset Password” function on login page. For users who disabled OTP sent via mobile device, please contact your VaR DAs (applicable to VaR business user) or HKEX (applicable to VaR DA) to reset mobile device registration before using “Self-service Reset Password”.

Self-service Reset Password

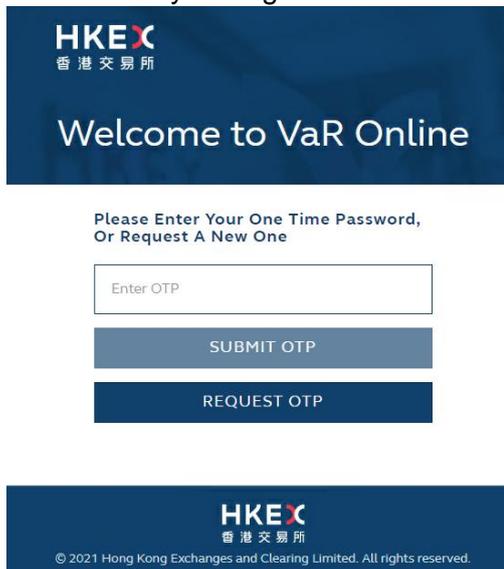
1. Click <Forgot/Reset your password>.



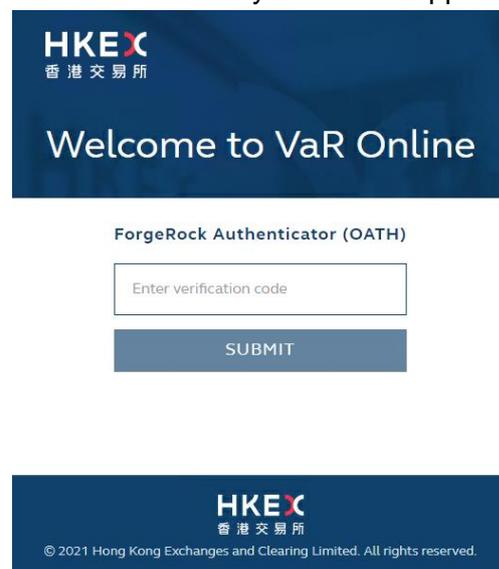
2. Please enter your User ID and click <SUBMIT>.

3. You will be required to enter two OTPs.

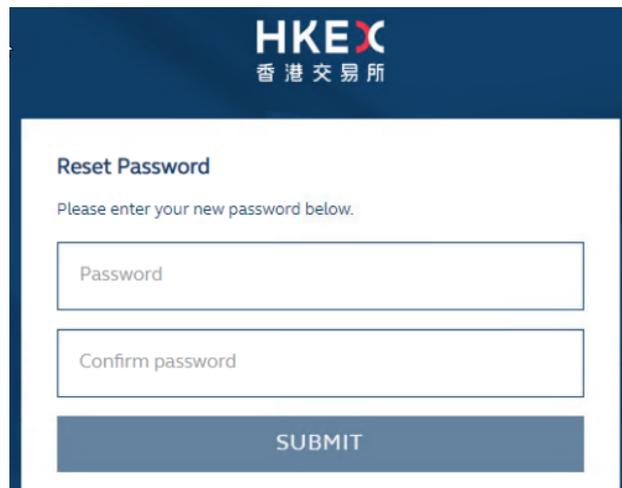
The 1st OTP from your registered email.



The 2nd OTP from your mobile app.



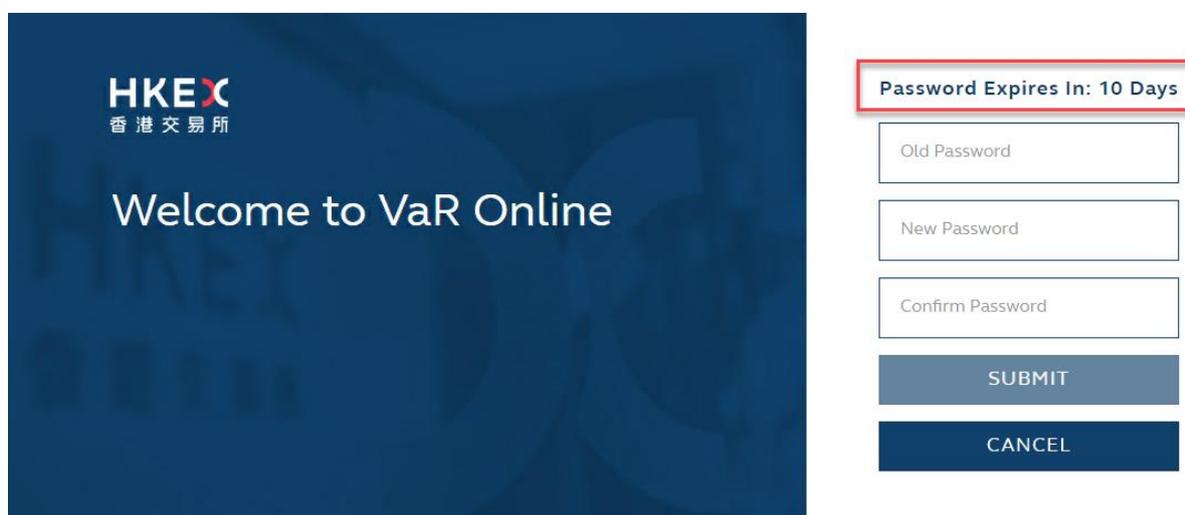
- Please input your new password and click <SUBMIT>.



- Upon successful validation of new password, please close the “Self-service Reset Password” window. Navigate back to login page to login with User ID and new login password.

2.3.4 EXPIRED ACCOUNT PASSWORD

Both Delegated Administrator and Business User account’s login password expires every 90 days. 10 days before expiry, users will start to receive reminder for changing password after login.



You should change your login password. If DA or Business User click <CANCEL> to skip this reminder, he/ she may continue to login with existing password.

After expiry of password, user still have one-time grace login. Then, user will be asked to change password. If user still DO NOT change his/her password, then such user will be UNABLE to login and access VaR DA Platform/ VaR Online until reset of password. The user must click <Forgot/Reset your password> to perform “Self-service Reset Password”. Please refer to last sub-section, 2.3.3 FORGOT/ RESET PASSWORD for details.

2.4 LOGIN AND LOGOFF

2.4.1 FIRST TIME LOGIN ON VAR DA PLATFORM/ VAR ONLINE

1. Delegated Administrators and Business Users will receive below notification email for successful creation of their accounts.

HKSCC System

Your account is ready

Dear Admin,

Welcome to HKSCC System. Your user ID is 999999_damaker.

Please follow instructions below to setup password:

1. On Login page click on "Forgot/Reset your password?"
2. Enter your user ID



For enquiries, please contact us via [link](#).

Please do not reply this e-mail as this is system generated.

Disclaimer

The information contained in this email is intended only for the use of the individual or entity named above and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this message in error, please immediately notify us and delete the email. Internet communication cannot be guaranteed to be timely, secure, error-free or virus-free. The sender does not accept liability for any errors or omissions. Thank you.

2. Access the login page via the following URL:
VaR DA platform <https://idm.hkexposttrade.com.hk/user-management/>
VaR Online <https://rmcd.hkexposttrade.com.hk>
3. Click <Forgot/ Reset your password> to set up login password.

User Login

User ID

Password

LOG IN

[Forgot/Reset your password? >](#)

By clicking the 'LOG IN' button, I confirm that the individual(s) whose personal data is disclosed in my use of this application consent to the processing of their personal data.

Unauthorised access and use are prohibited, HKEX reserves the right to take actions against offenders.

4. Enter your user ID (as mentioned in the notification email) and click <SUBMIT>. Then, you will receive a One-time Password (OTP) from your registered email. Please input the OTP and click <SUBMIT OTP>.

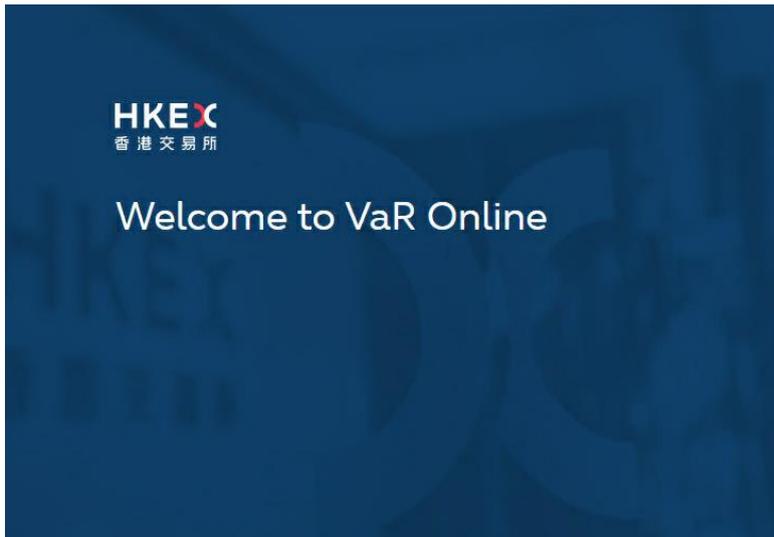
The image displays four screenshots of the VaR Online interface. The top-left and top-right screenshots show the 'Welcome to VaR Online' page. The left version has an 'Input User ID' section with a 'User ID' text box and a 'SUBMIT' button. The right version has a 'Please Enter Your One Time Password, Or Request A New One' section with an 'Enter OTP' text box, a 'SUBMIT OTP' button, and a 'REQUEST OTP' button. The bottom-left and bottom-right screenshots show the footer with the HKEX logo and copyright text: '© 2021 Hong Kong Exchanges and Clearing Limited. All rights reserved.' The bottom-right screenshot also shows an email notification from 'no-reply@openam.org' dated 'Today 17:30' with the subject 'HKSCC System: One Time Password' and the message 'One Time Password (OTP) for HKSCC System: 27788148'.

Remarks: The screen for this login session will time out in 6 minutes. Email OTP is valid for 5 minutes and it can only be requested every 5 minutes.

5. Please set-up your login password according to the password requirements and click <SUBMIT>. A message for successful set-up of password will be displayed.

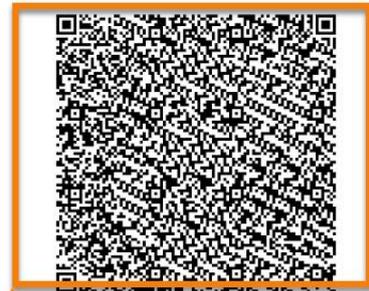
The image shows a 'Reset Password' form. At the top is the HKEX logo and the text '香港交易所'. Below that is the title 'Reset Password' and the instruction 'Please enter your new password below.'. There are two text input fields: the first is labeled 'Password' and the second is labeled 'Confirm password'. At the bottom of the form is a 'SUBMIT' button.

6. Navigate back to the login page and enter User ID, Password then click <LOG IN>.
7. You will be asked to register a mobile device, please click <REGISTER A DEVICE> and install ForgeRock Authenticator App in your mobile device. This application is available in both Google Play and Apple's App Store. If you have been using ForgeRock Authenticator for Client Connects' Logon, it is not necessary to download the same App again.



Register A Device

Scan the barcode image below with the ForgeRock Authenticator App. Once registered click the button to enter your verification code and login.



LOGIN USING VERIFICATION CODE

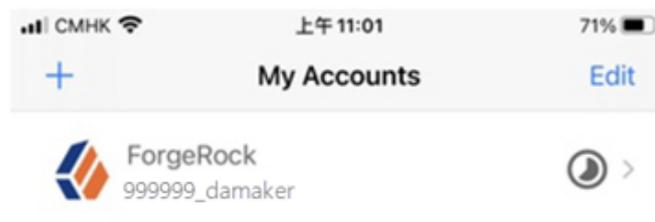
Note: This QR code will only display once. Please scan it using ForgeRock Authenticator App before clicking <LOGIN USING VERIFICATION CODE>. If not, your user account will require unlock to reset device registration. Please refer to section 2.1 ACCESS MANAGEMENT - Locked / Unlock User Account.



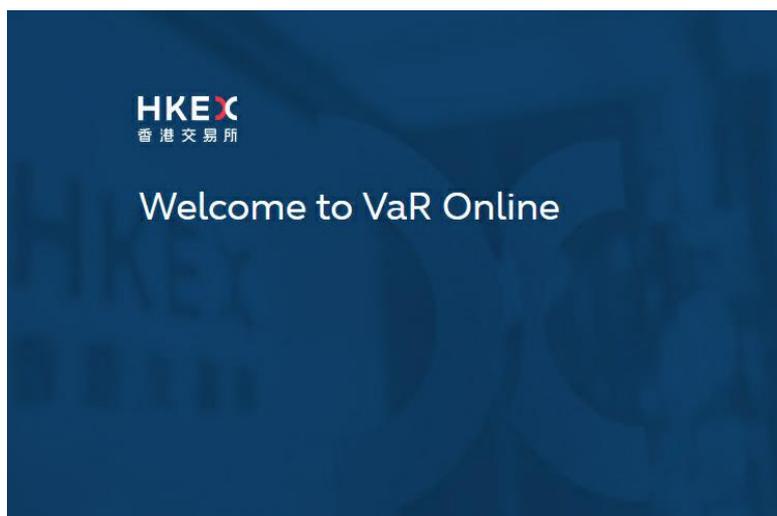
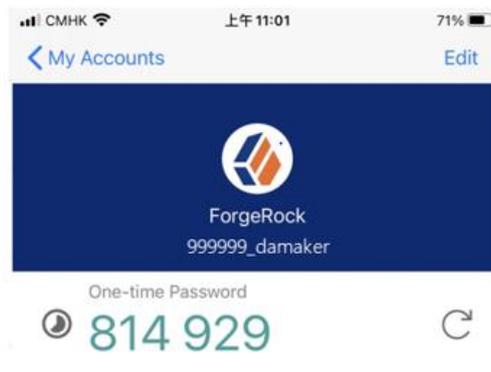
ForgeRock Authenticator 4+

Forgerock
Designed for iPad
★★★★★ 4.5 • 17 Ratings
Free

8. Click + sign to scan the QR code using your ForgeRock Authenticator App. You will see that your VaR DA Platform/ VaR Online account is registered in your App with your user ID. Then, click <LOGIN USING VERIFICATION CODE> via login page.



9. Your VaR DA Platform ID/ VaR Online user ID is stated on the list of accounts in ForgeRock Authenticator App. Click the account and then click  to generate a One-time Password. Input OTP on login page then click <SUBMIT>.



ForgeRock Authenticator (OATH)

10. You will be re-directed to VaR DA Platform/ VaR Online homepage when login is successful.

For subsequent login to VaR DA Platform/ VaR Online, users will have to provide (1) User ID, (2) Password; and (3) OTP from ForgeRock Authenticator App.

If a user is assigned with both VaR DA and VaR Online Business User roles, only one single login will be required. For example, after entering VaR DA Platform's URL and login successfully, user can enter VaR Online's URL to switch application without re-login and vice versa.

2.4.2 LOGOFF

To prevent unauthorized access of VaR DA Platform/ VaR Online, please logoff every time after usage.

Logoff via VaR DA Platform:

Click the user email address on top right hand corner and then click <Logout>. You will be re-directed to VaR DA Platform login page.



Logoff via VaR Online:

Click the  icon on the top right hand corner, then a confirmation message will display at the bottom. Please click <OK> to confirm.

