

Trade Repository
Enhancement for SWIFT WebAccess
Simulation Test Script
(Confidential)

Date : **October 2019**
Version : **1.0**

Copyright The Hong Kong Monetary Authority. All rights reserved.

This document, which contains confidential material, is the property of The Hong Kong Monetary Authority (HKMA). It is not to be used for any other purposes, copied, distributed or transmitted in any forms or any means without the prior written consent of the HKMA.

DOCUMENT HISTORY

Date	Updated By	Version	Amendment Summary
October 2019	HKMA	1.0	Initial Publication

This page is intentionally left blank

TABLE OF CONTENTS

1	INTRODUCTION	1
2	PRE-REQUISITE	2
3	TESTING ENVIRONMENTS.....	2
4	TEST PROCEDURE.....	3

This page is intentionally left blank.

1 Introduction

To align with SWIFT's initiative to migrate its Browse service, which is currently being used to provide graphical user interface (GUI) platform for participants to access the Trade Repository (TR) system's interactive functions through the SWIFT network, to its new WebAccess service, the TR system will be enhanced. The whole migration is conducted in 3 phases as follows:

Phase	Migration Process	Responsible Party
1	New WebAccess service provisioning and migration	SWIFT
2	Participants' setup	Participants
3	TR application migration	HKICL

For details on the migration schedule, please refer to circulars relevant to SWIFT WebAccess published by HKICL or the HKMA.

A big-bang approach will be adopted for the migration of TR application to WebAccess workflow and interface, after which SWIFT users can only log in via the WebAccess channel. To avoid disruption to TR reporting, it is important for TR Members who are going to adopt SWIFT WebAccess to be familiar with the new workflow and interface before the final migration. A simulation test is arranged for this purpose.

This document is the script for conducting the simulation test. This test script will work through with test cases, allowing participants to be familiar with TR's new features. Participants should complete all test cases to ensure they are 100% ready to manage user account and access the TR system, through the WebAccess channel, in the production environment.

2 Pre-requisite

Before performing the simulation test, make sure the following preparations have been completed.

- 1) Perform the connectivity test for Simulation Test and return the Test Result Reply Forms for simulation test / member test environment on or before 13 December 2019.
- 2) Prepare three SWIFT user accounts with unique certificates.
- 3) Possess login credentials for the default administrator accounts (i.e. defadmin1 and defadmin2) or equivalent administrative user accounts who have been configured “SWIFTNet” or “Both SWIFTNet and Internet” as User Access Method. Please contact HKTR if password reset is required.
- 4) Read relevant sections of User Manual (Administrative Functions) mentioned in the test cases below to get familiar with SWIFT user account association and its removal functions.

3 Testing Environments

The following testing environments are available for this SWIFT WebAccess Enhancement and the Simulation Test environment is recommended to conduct this test.

SWIFT WebAccess Service Name	URL	IP Address	SWIFTNet Environment	Purpose
hkicl.tr.gui!p4	https://hkicl-tr-pilot-memtest.browse.swiftnet.sipn.swift.com/tr/mem/login	149.134.1.176	Production (Pilot service)	Member Test
hkicl.tr.gui!p5	https://hkicl-tr-pilot-simtest.browse.swiftnet.sipn.swift.com/tr/sim/login	149.134.1.177	Production (Pilot service)	Simulation Test

4 Test Procedure

Test Case 1: Login as Default Administrator to Create New User		
Conduction Date: Day 1		
Description: By default, each TR participant has two default administrator accounts (defadmin1 & defadmin2) which can be used to perform administrative functions such as creating new users. In this test case, user is required to log in to TR as default administrator through the WebAccess channel and create a new user.		
Steps		Expected Result
1	Log in SWIFT WebAccess via SWIFT Alliance Web Platform (AWP) or personal token with SWIFT user account to be associated with TR default administrator (“defadmin1”).	If login is successful, a SWIFT application page will be shown.
2	Click the relevant link to access TR under specific environment.	User Browser is redirected to SWIFT login page (CUG).
3	Input the password of the SWIFT user account and press the “Login” button.	Another SWIFT login page (User Authentication) is displayed
4	Input the password of the SWIFT user account and press the “Login” button again.	User Browser is redirected to the SWIFT User Account Association screen if no association has been established for before <Go to step 5>. If the SWIFT user account has been associated with TR default administrator (“defadmin1”), a welcome page will be shown on user’s browser <Skip step 5>.
5	Input the TR login credentials (Participant ID, user ID and password) for default administrator (“defadmin1”) and click the “Associate” button.	The default administrator is associated with the SWIFT login user and then a welcome page is shown on user’s browser.
6	Navigate to User and Role Maintenance > Add User Account. Follow Section 7.1 in Admin User Manual to create a new user account with User ID “testuser1” and User Access Method “SWIFTNet”.	The user account creation is in pending approval status.
7	Log out both SWIFT and TR applications. Repeat Step 1 – 4 to log in to TR with another SWIFT user account and associate it with default administrator (“defadmin2”)	The default administrator is associated with the SWIFT login user and then a welcome page is shown on user’s browser.

8	Follow section 9 in Admin User Manual to approve the account creation.	The user account creation is completed.
---	--	---

Test Case 2: Behaviour of SWIFT User Account Association		
Conduction Date: Day 1		
<p>Description: SWIFT does not allow the sharing of one single SWIFT user certificate among multiple TR users in the sense that each User account (inter and intra TR Participant) must be associated with a unique SWIFT user account. In this test case, we will go through some common failures and system responses encountered during the SWIFT user account association process.</p>		
Steps		Expected Result
1	Use a new SWIFT user account to log in SWIFT WebAccess. This SWIFT user account will be associated with TR User ID (“ testuser1 ”).	If login is successful, a SWIFT application page will be shown.
2	Click the relevant link to access TR under specific environment.	User Browser is redirected to SWIFT login page (CUG).
3	Input the password of the SWIFT user account and press the “Login” button.	Another SWIFT login page (User Authentication) is displayed
4	Input the password of the SWIFT user account and press the “Login” button again.	User Browser is redirected to the SWIFT User Account Association screen.
5	Input the TR login credentials (Participant ID, user ID and password) for default administrator (“ defadmin1 ”) and click the “Associate” button.	The association fails and an error is displayed on system message screen since default administrator (“ defadmin1 ”) has already been associated with another SWIFT user.
6	Press the “Close” button. Repeat Step 1-4 if necessary.	User Browser is redirected to the SWIFT User Account Association screen.
7	Use an incorrect password to associate the SWIFT user account with “ testuser1 ”.	The association is failed and an error message is displayed on the SWIFT User Account Association screen.
8	Press the “Close” button. Repeat Step 1-4 if necessary.	User Browser is redirected to the SWIFT User Account Association screen.
9	Input the correct login credentials for “testuser1” and click the “Association” button.	“ testuser1 ” is associated with the SWIFT login user and then a welcome page is shown on user’s browser.
10	Log out TR application	System message screen is displayed.

Test Case 3: Remove a SWIFT User Account Association (Dissociation)		
Conduction Date: Day 1		
<p>Description: Once an association is established between a SWIFT user and a TR user, the SWIFT user will be able to log in SWIFT and TR simultaneously without entering login credentials for the TR user. The association can be removed using the “Maintain User Account” function. Once it is removed, the SWIFT user is required to establish the association again. User List Details report (ADMU0001) is a user requested report which shows the details of user selected in “View User List” function.</p>		
Steps		Expected Result
1	Use the SWIFT user account associated with “defadmin1” to log in SWIFT WebAccess.	If login is successful, a SWIFT application page will be shown.
2	Click the relevant link to access TR under specific environment.	User Browser is redirected to SWIFT login page (CUG).
3	Input the password of the SWIFT user account and press the “Login” button.	Another SWIFT login page (User Authentication) is displayed
4	Input the password of the SWIFT user account and press the “Login” button again.	Log in as “defadmin1” and a welcome page is shown on user’s browser.
5	Navigate to User and Role Maintenance > User List. Follow Section 7.8 in Admin User Manual to show a list of users belonging to the participant.	A list of users is displayed with a column “SWIFT User Name”.
6	Select the checkbox next to “testuser1”, click “Print Details” button to print selected user details, and click “Request” button.	A pop-up message dialog box stating the Report Reference is displayed.
7	Click the hyperlink on “testuser1” to view the user details.	“View User Account” function is invoked to show SWIFT User Name, SWIFT User DN and Last Associate Date/Time under SWIFT User Account Association section
8	Follow Section 7.2 and 7.3 in Admin User Manual to remove the SWIFT user account association for “testuser1”.	The user account maintenance is in pending approval status.
9	Navigate to Reports > Report List. Click “Search” button. Click the hyperlink on “Report ID” to download the ADMU0001report.	The report showing user details of “testuser1” before dissociation is downloaded.
9	Log out SWIFT and TR applications. Log in as “defadmin2” to approve the user account maintenance.	The user account maintenance is completed.

10	Log out SWIFT and TR applications. Log in to TR with the SWIFT user account that was associated with “testuser1”.	User Browser is redirected to the SWIFT User Account Association screen.
----	--	--

Test Case 4: Download Administrative Functions Audit Trail Report		
Conduction Date: Day 2		
Description: Administrative Functions Audit Trail Report (ADMD0001) is one of the system reports generated by TR during day end batch processing. This report shows information of each administrative function updates carried out by the TR Participant during the business day.		
Steps		Expected Result
1	Log in as “defadmin1”	Log in as defadmin1 and a welcome page is shown on user’s browser.
2	Navigate to Reports > Report List. Follow Section 11 in Admin User Manual to download the ADMD0001 report.	ADMD0001 report is downloaded.
3	Check the content in the ADMD0001 report.	The user account maintenance performed for “testuser1” on Day 1 can be found in the report.
4	Send the reports ADMD0001 and ADMU0001 saved in test case 3 to HKTR by email hktr@hkma.gov.hk.	HKTR will verify and confirm participant the test result.