HKCC and SEOCH Report Access Platform (RAP)

Technical Guide

Version:	2.2
Prepared by:	HKEX
Last Update:	Nov 2025

Modification History

Ver.	Update Date	Section	Description
1.0	12 Sep 2018	-	First issue
1.1	Feb 2020	4.1 Operation Hours	Inserted reminder notes for report retrieval mechanism
1.2	Mar 2020	6 Renewal of Public Keys	Inserted procedures for renewal of public key
1.3	May 2020	3 Access to SFTP Facility	Inserted reminder notes for format of SFTP user accounts
1.4	Jun 2020	8 LOP Reports	Inserted LOP reports submission information
1.5	Sep 2020	2.1 SFTP Standard	Inserted reminder note for SFTP endurance feature
1.6	Sep 2021	2.1 SFTP Standard	Added SFTP Supported Key exchange algorithms, MAC algorithms and Ciphers
1.7	May 2022	4.1 Operation Hours	Updated operation hours for implementation of Derivatives Holiday Trading
1.8	Nov 2022	8 LOP Reports	Removed LOP Submission features and Section 8 LOP Reports
1.9	Apr 2023	3.2 Secure Shell Keys 4.2 Folder Structure 5 Registration of SFTP User Account	Updated SSH key submission means to HKEX Removed LOP folders Updated SFTP user account registration means to HKEX
2.0	Aug 2024	Various sections except 2.2	• Added a prefix “D” to the existing user account • Updated the Folder Structure • Updated the Login Control • Updated the Frequent Upload Control • Updated the IP Address and Port of the HKEX SFTP Facility

Ver.	Update Date	Section	Description
2.1	Mar 2025	1.1 Background 3.1 User Accounts 4.1 Service Hours 4.2 Folder Structure	• Change of official name from “Report Retrieval Solution” to “Report Access Platform” • Add download for CCMS reports • Update the Folder Structure
2.2	Nov 2025	4 Operation of RAP 8 Important Notes	• Report/ file download guideline • Important notes to Clearing Participants

Table of Contents

1 Overview

1.1 Background

This technical guide serves as a reference document for Clearing Participants (CPs) to retrieve DCASS, pre-trade risk management and Common Collateral Management System (CCMS) reports from HKEX through Report Access Platform (RAP) via the secure file transfer protocol (SFTP) facility.

It covers the following areas of the RAP:
- Technical Infrastructure;
- Access to RAP via SFTP Facility;
- Operation of RAP;
- Registration of RAP User Account;
- Renewal for public key; and
- Network configuration

2 Technical Infrastructure

2.1 SFTP Standard

The SFTP facility uses industry standard SFTP and the following protocols are supported:

Protocol	RFC	Remarks
SFTP	RFC 4251-4254	Secure Shell File Transfer Protocol (Endurance feature is not supported #1)
SSH Public Key File Format	RFC4716	SSH2 Public Key File Format Fingerprint: MD5 message-digest

Below are the supported Key Exchange algorithms, MAC algorithms, Ciphers algorithms and Public/Host Key Algorithms

Key Exchange Algorithms	curve25519-sha256@libssh.org,ecdh-sha2-nistp521, ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
MAC Algorithms	hmac-sha2-512-96, hmac-sha2-256
Ciphers Algorithms	aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
Public/Host Key Algorithms	ssh-rsa,rsa-sha2-256,rsa-sha2-512

CPs are required to ensure that the SFTP software they use for report/file retrieval must adhere to the above standard.

#1: Some CPs enabled endurance feature in their SFTP client software. Please note that endurance feature is not supported in Report Access Platform (RAP), CPs should turn this feature off, otherwise "Permission Denied" will be shown when they attempt to upload files, e.g. SSH key.

2.2 Primary and Backup SFTP Facilities

The SFTP facility is set up at both the HKEX primary and secondary data centers. For normal operations, only the primary SFTP facility is in active mode. Under contingency situation where the primary SFTP facility becomes unavailable, HKEX will notify CPs to connect to the secondary SFTP facility.

3 Access to RAP via SFTP Facility

3.1 User Accounts

For each CP, HKEX will assign at most four RAP user accounts for retrieval of DCASS reports, pre-trade risk management reports (e.g. TP001, RPI03, RX_AUDIT, etc.) and CCMS reports.

The four RAP user accounts are in the following format:
- DCXXX001
- DCXXX002
- DCXXX003 (optional)
- DCXXX004 (optional)

where <CXXX> is the DCASS customer code of the CP. For example, CP with DCASS customer code CXYZ, two RAP user accounts “DCXYZ001” and “DCXYZ002” would be assigned.

After registration, CPs may use either one of the assigned RAP user accounts together with the respective SSH private key to login to the RAP for retrieval of DCASS, pre-trade risk management and CCMS reports.

Please note the RAP user accounts are CASE SENSITIVE. CPs should input their RAP user accounts **in CAPITAL LETTERS** (i.e. CP with DCASS customer code <CXYZ> should input the RAP user account as “**DCXYZ001**” or “**DCXYZ002**”). CPs input user accounts in small letters cannot login RAP.

3.2 Secure Shell Keys

The SFTP facility adopts Secure Shell (SSH) public-key authentication. For **each RAP user account,** CPs need to generate a pair of SSH private and public keys, as well as a public key fingerprint, and register the public key and the public key fingerprint with HKEX.

3.2.1 Public Key

HKEX accepts RSA 2048-bit and 4096-bit public keys in SSH2 format.

For example:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: SSH KEY
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PUBLIC KEY ----
```

Each public key should be saved in a separate file with the following naming convention and sent to HKEX via Client Connect for registration:

- DCXXX001.pub (public key for RAP user account DCXXX001)
- DCXXX002.pub (public key for RAP user account DCXXX002)

Where <CXXX> is the DCASS customer code of CP.

3.2.2 Public Key Fingerprints

Public key fingerprints are MD5 hash digests of public keys in the format of 16 octets printed as hexadecimal with lowercase letters and separated by colons.

For example:
"c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87"

The fingerprints need to be provided during the SFTP user account registration.

CPs SHOULD NOT submit their private keys to HKEX.

4 Operation of RAP

4.1 Service Hours

	For DCASS and pre-trade risk management reports	**For CCMS Reports**
Service hours	07:00 to 03:30 on trading days	07:15 to 24:00 on trading days and 07:15 to 13:00 on Saturday except public holiday.

All DCASS, pre-trade risk management and CCMS reports will be available for the past 10 calendar days from the date the report is generated. CPs should retrieve and safe keep their reports in a timely manner.

Please note that there are large number of reports and data files for both HKCC & SEOCH per trading day. To avoid causing heavy load network traffic to the CPs' SDNet network traffic and occupy logging of the system due to unnecessary frequent report download action, CPs are highly recommended to review their report retrieval mechanism through RAP so as to assure reports (except reports which are relating to intraday margin) are downloaded only once per day and strictly for the specified date.

4.2 Folder Structure

Each RAP user account can access up to 5 folders on the RAP depending on the type of reports or data files subscription of the RAP user account:

For DCASS and pre-trade risk management reports:

Folder Name	**Content**
/download/DCASS	DCASS Daily and Monthly reports / files applicable to CP <CXXX>
/download/DCASS_OTHERS	Other reports / files applicable to CP <CXXX> for derivatives market

For CCMS reports:

Folder Name	Content
/download/HKCC_SEOCH_CCMS_GLOB	For retrieval of common CCMS reports / files applicable to all CPs and CCMS reports / files applicable to CP <CXXX> for both HKCC and SEOCH

Common Folders:

Folder Name	Content
/key_management/publickey	For public key renewal. Allowed for key upload and file download only, modification and deletion are not allowed. Please refer to Section 6 for details.
/submission	Not used for Derivatives Markets

If the RAP user account of a CP is configured to receive DCASS report, the account can access both folders /download/DCASS and /download/DCASS_OTHERS. If the RAP user account of a CP is configured to receive CCMS report, the account can access folder /download/HKCC_SEOCH_CCMS_GLOB.

4.3 Login Control

A user account is allowed to log on through pre-registered IP addresses. However, concurrent login is not allowed.

For example, DCXYZ001 has logged on via IP “10.10.10.10”. If DCXYZ001 then logs on via IP “11.11.11.11”, session at IP “10.10.10.10” will be closed.

5 Registration of RAP User Account

To register for RAP user accounts, CP should generate a pair of SSH keys per account; and submit their public key, public key fingerprint, and IP addresses for the designated RAP client workstations to HKEX via Client Connect TechS 8 form. For more detail, please refer to Section 3.2.

The file name of the public key should follow the naming convention below:

- Public Key file name (DCXXX001.pub; DCXXX002.pub; DCXXX003.pub; DCXXX004.pub)

CPs please **DO NOT** attach private keys in the zip file. CPs shall keep their private keys confidential and prevent any unauthorized usage.

6 Renewal of Public Keys

CPs are required to renew their public keys at least every two years. CPs should re-register their keys with HKEX immediately if the corresponding private keys are being compromised. See Section 5.

Self-service Renewal of Public Keys

After generation of the new SSH public and private keys, CPs should renew their SSH public keys with HKEX by submitting the keys to the /key_management/publickey folder. After submission, a result file will be generated and available for retrieval in the /key_management/publickey folder.

CPs should follow the below steps to perform self-service public key renewal:

1) Login RAP user account, e.g. DCXXX001.
2) Locate /key_management/publickey folder.
3) Upload the newly generated SSH public key into /key_management/publickey folder, e.g. DCXXX001.pub. (Fingerprint is not necessary for public key renewal).
4) Renew SSH public key for each RAP user account separately, i.e. log in DCXXX001 to renew DCXXX001's SSH public key and log in DCXXX002 to renew DCXXX002's SSH public key, etc.
5) Verify the renewal result file in the same folder.

Results:

- Result file will be generated under /key_management/publickey folder immediately[#2] after the key has been uploaded.
- For successful outcome, the result file will be named as "<keyfile>.HHMMSS[.seq].rcvd". In case of failure, it will be named as "<keyfile>.HHMMSS[.seq].rej" for failure case.
- The result file of successful outcome will specify the fingerprint and file name of the uploaded SSH public key.
  Example:

– The result file of failed outcome will specify the error code and error message of the attempted key upload.
  Example:

```
4007 File name contains invalid characters
```

– Result file will be available for retrieval within 24 hours after generation. CPs should retrieve and safe keep their file in a timely manner.
– New SSH public key will be effective immediately if it is uploaded successfully. The old SSH public key will be expired in 14 calendar days after the new SSH public key has been uploaded. (If old SSH public key will be expired in less than 14 calendar days before new key renewal, the expiration day of old SSH public key will not change)

#2: Some SFTP client software requires users to refresh files list manually to show the result file.

6.1 Validity of Keys

Once the SSH public key has been successfully renewed, CPs can use either the existing or the newly generated private key to login in the following 14 calendar days. If the expiration date of existing key is less than 14 calendar days, the expiration date will not extend to 14 calendar days. After the SSH key has been renewed, the existing SSH key will be expired and removed automatically on the 15th calendar day, CPs can only use the newly generated private key (which will pair with the renewed public key) to login.

The validity of renewed public key is 2 years, the expired SSH key will be automatically removed, i.e. CPs cannot login RAP if they do not renew the SSH key before the expiry date. In this case, CPs are required to follow Section 5 to re-register the public key again with HKEX.

For example, a RAP user account, e.g. DCXXX001, is using “Key A” as existing key and the CP successfully renewed the public key “Key A” by “Key B” on 1 March 2024, then the validity timeline for the keys illustrates as below:

From	To	Valid Key(s)
1 March 2024	14 March 2024	Both “Key A” and “Key B” can be used for login.
15 March 2024	28 Feb 2026	Only “Key B” can be used for login.
1 March 2026	~	“Key B” is expired and no key can be used

From	To	Valid Key(s)
		for login. CPs **must** renew their SSH keys before the expiry date. If not, CPs are required to follow Section 5 to re-register the public key with HKEX

6.2 Expiry Notification

When there is a SSH key to be expired in coming 14 days, a report named "SSHKeyExpireWarning.txt" will be generated under /key_management/publickey folder.

CPs should check the /key_management/publickey folder regularly and follow the renewal procedure in Section 6 to timely renew their SSH key before the SSH key expires, so as to avoid any interruption to their operational processes.

Since the to-be-expired SSH key and the renewed key co-exist continue to be valid for 14 days, the expiry report will be generated daily until the to-be-expired SSH key is expired and removed by system. CPs can ignore the expiry report if they have successfully renewed the SSH key.

6.3 Frequent Upload Control

Each RAP user account is limited to either one or two keys, which include the old key and the renewed key.

For example, if a CP uploads a third key using their RAP user account, the third newly upload key will replace the renewed key, while the validity of the old key remains unaffected. Consequently, the RAP user account would still maintain two valid keys.

7 Network Configuration

The RAP is only accessible from the Securities and Derivatives Network/2 (SDNet/2) or HKEX Service Network (HSN).

CPs can register at most 4 designated RAP client workstations for report retrieval. Follow Section 5 above, CPs should submit the IP addresses of their designated RAP client workstations to HKEX for registration.

Upon registration of public keys and IP addresses, CPs can access HKEX RAP with the assigned user accounts via either one of the registered RAP client workstations.

IP addresses of the RAP client workstations must be within the same subnet (first 3 octets) of SDNet/2 or HSN.

7.1 Connectivity of RAP

IP addresses of RAP are as follows:

Primary data center	**Secondary data center**
10.151.14.141 port 18801 10.151.14.142 port 18801	10.152.14.141 port 18801 10.152.14.142 port 18801

8 Important Notes

8.1 Usage Guidelines

To promote efficient and secure usage of RAP, CPs should coordinate with their internal IT teams and/or vendors to ensure that the setup for RAP operations aligns with the guidelines below. Regular checks should be performed to ensure that RAP usage remains compliant.

1. Login / Access to RAP

   Concurrent logins are not permitted. Each RAP user account should only be logged in on one designated RAP client workstation at a time. After the files are downloaded, CPs shall log-off and disconnect from RAP.

   RAP users are advised to limit **login attempts to no more than once per minute**. Login attempts exceeding this recommended frequency may potentially result in a **temporary lockout of the RAP user account for 5 minutes**.

2. Retrieval of reports/ files

   CPs should access RAP according to the schedule of the files they need to download. After the files are downloaded, CPs should log-off and disconnect from RAP. If the required files are not available, CPs should also disconnect from RAP and then sign-on again after a brief timeout period of at least 1 minute.

   When multiple report files are required at the same time, they should be downloaded within a single RAP logon session. Each report file should be downloaded from RAP only **once per day**. Historical report files are provided for contingency recovery purpose. CPs must keep the report files on their storage device(s) and use their local copies. Repeated download of the same report/ file is not recommended.

   For efficient use of network bandwidth and shortening download time, CPs must NOT use wild card command such as “mget *” or “get *” when

downloading files apart from those of current date, otherwise all files retained in the folder (i.e. all reports/files for past 10 calendar days) will be downloaded.

CPs should therefore use command "mget /download/DCASS/*_YYYYMMDD_*" or "get /download/DCASS/*_YYYYMMDD_*" to download the DCASS files/reports of the current date (where YYYYMMDD being the current date).

CPs should download required reports for a specific day only, and avoid intensive access to RAP and repeated download of reports/ files.