HKSCC Report Access Platform (RAP)

Technical Guide

Version:	7.3
Date:	March 2025

Modification History

Version	Date	Modified By	Synopsis
1.0	Oct 2019	HKSCC	First issue
2.0	Jan 2020	HKSCC	Updated Sdnet ip addresses subnet under section 6
3.0	Aug 2020	HKSCC	Updated the following • section 2.3 add verification of HKSCC SFTP facility • section 3 only one RAP User ID per Clearing Participant • section 4.2 add daily subfolders to both INBOX and COMMON folders, with handling of report retrieval from subfolders remove OUTBOX folder • section 4.4 new section on sign-on session • section 7 add notes on performance with shared SDNet line
4.0	Jan 2021	HKSCC	Added tips on concurrent setting under section 7
5.0	Jul 2021	HKSCC	Updated the following • section 4.2 add new RPF folder • section 7 add convert csv files to pdf format add performance of RPF file download
6.0	Oct 2021	HKSCC	Updated the following • section 4.2 (d) updated the handling of reports/files made available via RAP beyond mid-night (00:00)
7.0	Apr 2022	HKSCC	Updated the following • section 5.2 add procedure for public key renewal
7.1	Jan 2023	HKSCC	Update the following section 5.2 add procedure for public key renewal
7.2	Dec 2024	HKSCC	Update the following • 2.3 Authenticity of RAP • 3.1 User ID • 3.3 Public Key • 3.4 Public Key Fingerprint • 4.1 Operation Hours and Time Schedule • 4.2 Folder Structure • Remove 4.3 Frequent Sign-on Control • 5.1 Initial Registration • 5.2 Self-Service Renewal of Public Key • 6.1 Connectivity of RAP • 7.1 Usage Guidelines • General update “Clearing Participant” to “Cash Clearing Participant”
7.3	Mar 2025	HKSCC	Add CCASS and CCMS Report Access for Participants and DBs. General update “Cash Clearing Participant” to “Participants other than Investor Participants and Designated Banks” Update the following • 3.1 User ID • 3.3 Public Key • 4.1 Operation Hours and Time Schedule

			• 4.2 Folder Structure • 5.1 Initial Registration • 5.2 Self-Service Renewal of Public Key • 7.1 Usage Guidelines

TABLE OF CONTENTS

1 OVERVIEW

1.1 Background

This document serves as a technical reference guide for HKSCC's Participants other than Investor Participants ("Participants") and Designated Banks ("DBs") to retrieve reports/files through HKSCC Report Access Platform (RAP) via a secure file transfer protocol (SFTP) facility provided by HKSCC.

It covers the following areas of the RAP:

- Technical Infrastructure
- Access to RAP via SFTP Facility
- Operation of RAP
- Registration of RAP User Account
- Network Configuration
- Important Notes

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
SSH Public Key File Format	RFC4716	SSH2 Public Key File Format Fingerprint: MD5 message-digest

All Participants and DBs are required to ensure that the SFTP client (in house development or third party software) is installed in their RAP client workstations for report/file retrieval and it must adhere to the above standard.

2.2 Primary and Backup SFTP Facilities

There are two sets of SFTP facilities setup at HKSCC's primary and secondary data centres respectively. Under normal condition, Participants and DBs should only connect to the primary SFTP facility. Under contingency situation where the primary SFTP facility becomes unavailable, HKSCC will then activate and switch the RAP connection to the secondary SFTP facility.

3 ACCESS TO RAP VIA SFTP FACILITY

3.1 User Account

To retrieve reports/files, each Participant and DB will be issued with at most 3 RAP user accounts and at most 2 RAP user accounts respectively by HKSCC for access to the RAP, in the following format:

- *CXnnnnn001 - CXnnnnn003 for Participants, or*
- *CBNKnnn001 – CBNKnnn002* for DBs

where Xnnnnn is the Participant ID and *nnn is the Bank Code of DB*. For example, RAP user account CB99999001 would be assigned to Participant with Participant ID B99999; RAP user account CBNK999001 would be assigned to DB with Bank Code 999.

For Participants, who would like to develop their own tools to conduct margin and stress test calculation/simulation, can subscribe to access the optional "RPF folder" for retrieval of Risk Parameter Files (RPF). *Please note that due to large file size, retrieval of RPF would require a larger bandwidth, please refer to section 7.1 for the projected download time under different bandwidths*.

After registration (Note: Please refer to section 5 for registration information), Participants and DBs may use the assigned RAP user accounts together with the SSH private keys to login to the RAP for retrieval of CCASS, CCMS and VaR reports/files. Participants and DBs are recommended to verify and ensure the assigned user accounts can access the RAP.

Please note the RAP user accounts are CASE SENSITIVE. Participants and DBs should input their SFTP user accounts **in CAPITAL LETTERS** (i.e. CP with Participant ID B99999 should input the RAP user account as "CB99999001", DB with Bank Code 999 should input the RAP user account as "CBNK999001"). Participants and DBs input user accounts in small letters cannot login the RAP.

3.2 Secure Shell (SSH) Key

SFTP facility adopts Secure Shell (SSH) public-key authentication. For **each RAP user account**, Participants and DBs should generate a pair of SSH private and public keys, as well as a public key fingerprint, and register the public key together with the public key fingerprint with HKSCC.

3.3 Public Key

HKSCC 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 to be provided during the RAP user account registration:

For Participants:

- CXnnnnn001.pub (public key for RAP user account CXnnnnn001)

where C stands for cash market, Xnnnnn is the Participant ID of Participant.

For DBs:

- CBNKnnn001.pub (public key for RAP user account CBNKnnn001)

where C stands for cash market, nnn is the Bank Code of Designated Bank.

3.4 Public Key Fingerprint

Public key fingerprint is MD5 hash digests of public key 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"
```

SSH public key and public key fingerprint together with the IP address(es) of its RAP client workstation(s) used for accessing RAP should be submitted to HKSCC via Client Connect for registration. See Section 5 for details.

Participants and DBs SHOULD NOT submit its private key to HKSCC for registration.

4 OPERATION OF RAP

4.1 Service Hours and Time Schedule

	For CCASS and CCMS Reports	**For VaR Reports**
Service hours	07:15 – 24:00 on Monday to Friday including public holidays that fall on weekdays. and 07:15 – 13:00 on Saturday Except public holiday	07:00 - 24:00 on Monday to Friday except public holiday.

All reports/files will be available via RAP for the past 10 calendar days from the date the report/file is generated. Participants and DBs should retrieve and save their reports/files in a timely manner.

Please note that there are quite a number of reports, while some reports are generated multiple times daily, available for retrieval each day. In order to avoid heavily load network traffic due to unnecessary frequent report retrieval action, you should review your report retrieval mechanism through RAP to ensure reports are being retrieved <u>Once Daily Only</u>.

4.2 Folder Structure

Each RAP user account can access the following folders via RAP depends on the type of reports or data files subscription of the user account :

For CCASS and CCMS reports:

Folder	**Description**
• /download/CCASS_GLOB/yyyymmdd (for GLOB Market reports) • /download/CCASS_HKMK/yyyymmdd (for HK Market reports) • /download/CCASS_MAMK/yyyymmdd (for Shanghai Market reports) • /download/CCASS_SZMK/yyyymmdd (for Shenzhen Market reports)	• For retrieval of common CCASS reports/files that are applicable to all Participants and DBs <COMMON> and CCASS reports/files that are applicable to specific Participant <Xnnnnn> only or DB <BNKnnn> only • *yyyymmdd* is the system-generated subfolder for each

	calendar day • Participants and DBs should retrieve reports/files generated and available on specific day from the corresponding date subfolder • Market reports will be located in the folder appended with the corresponding Market Code (i.e. GLOB, HKMK, MAMK and SZMK)
● /download/HKSCC_CCMS_GLOB/yyyymmdd (for GLOB Market reports) ● /download/HKSCC_CCMS_HKMK/yyyymmdd (for HK Market reports) ● /download/HKSCC_CCMS_MAMK/yyyymmdd (for Shanghai Market reports) ● /download/HKSCC_CCMS_SZMK/yyyymmdd (for Shenzhen Market reports)	• CCMS reports are only applicable to Cash Clearing Participants • For retrieval of common CCMS reports/files that are applicable to all related Participants <COMMON> and CCMS reports/files applicable to specific Participants <Xnnnnn> only • *yyyymmdd* is the system-generated subfolder for each calendar day • Participants should retrieve reports/files generated and available on specific day from the corresponding date subfolder • Market reports will be located in the folder appended with the corresponding Market Code (i.e. GLOB, HKMK, MAMK and SZMK)

For VaR Platform reports (only applicable to Cash Clearing Participants):

Folder	**Description**
/download/VAR/yyyymmdd	• For retrieval of common reports/files applicable to all related Participants and reports/files applicable to specific Participants <Xnnnnn> only • *yyyymmdd* is the system-generated subfolder for each calendar day • Participants should retrieve reports/files generated and available on specific day from the corresponding date subfolder
/download/RPF_COMMON/yyyymmdd	*[Only available to RAP User with folder subscription]* • For retrieval of Risk Parameter Files (RPF) only

	• *yyyymmdd* is the system-generated subfolder for each calendar day • Participants should retrieve the RPF generated and available on specific day from the corresponding date subfolder

Common Folders:

Folder	**Description**
/key_management/publickey	• For submission of public keys for renewal by Participants and Designated Banks
/submission	• *NOT applicable for Participants and DBs*

a. Access to RPF folders is on subscription basis. Only Cash Clearing Participant subscribed for the RPF folder can access for retrieval of RPF. Please refer to section 7.1 for the project download time under different SDNet bandwidths.

b. The key_management folder is for submitting public keys for renewal, each RAP user account will be assigned with an individual key_management folder and it cannot be shared with other RAP user account.

c. Reports/files generated on a specific calendar day (with timestamp in the filename) will be available in the corresponding date (T) subfolder

4.3 Sign-on Session

Each RAP user account should only be sign-on to one of the designated RAP client workstation at a time. Participants and DBs should sign-out from the current session before signing onto another workstation with the same RAP User Account.

Note : When configuring the SFTP program connectivity, if there are parameter settings like "Number of simultaneous connections" or "Limit for concurrent download" , please set it to "1" to prevent concurrent login.

5 REGISTRATION OF RAP USER ACCOUNT

5.1 Initial Registration

To register for RAP user account, Participants and DBs should generate a pair of SSH public & private keys per user account; then upload its public key and input public key fingerprint and IP addresses of its designated RAP client workstations to the eService: TechS 8 via Client Connect.

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

- CXnnnnn001.pub (for RAP user account CXnnnnn001)

where C stands for cash market and *Xnnnnn* is the Participant ID of Participants.

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

- CBNKnnn001.pub (for RAP user account CBNKnnn001)

where C stands for cash market and *nnn* is the Bank Code of DBs.

DO NOT UPLOAD private keys to Client Connect. Participants and DBs shall keep their private keys confidential to prevent unauthorized usage.

5.2 Self-Service Renewal of Public Key

Users should renew their SFTP's public key by uploading it into sub-folder **/key_management/publickey** prior to expiry. After the upload has completed, an Acknowledgement File (.rcvd) or Rejection File (.rej) is generated.

Note:

- Acknowledgement File and Rejection File are per SFTP user based
- Acknowledgement File and Rejection File are retained for a maximum of 24 hours and will be subsequently removed by end of day housekeeping job
- If filename is longer than the system limit, i.e. 128 characters, the file will be rejected in SFTP level and no .rej file will be generated
- SFTP public keys submitted through SFTP and web interface will be registered in the same way and the expiration date is the same

If upload is successful, the uploaded key will be named as "Renewed Public Key", where:

- "Renewed Public Key" expiration date = 2 years from current date
- "Current Public Key" expiration date = its original expiration date or 2 weeks from current date, whichever is earlier

After "Current Public Key" has expired, it will be removed and "Renewed Public Key" will become the new "Current Public Key".

"Renewed Public Key" cannot be deleted. However, a user can upload another one to overwrite the existing "Renewed Public Key", and the expiration dates will be renewed.

User can login using either "Current Public Key" or "Renewed Public Key" as long as they are not expired.

5.2.1 Public Key Acknowledgement File

Acknowledgement File is a positive acknowledgement file to indicate the uploaded public key file is accepted.

The filename is formatted as **<original file name>.<timestamp – HHMMSS>.<seq>.rcvd** in **sub-folder /key_management/publickey** where ".<seq>" is optional and appears only when file of same name are uploaded within same second and is accepted.

The Acknowledgement File only contains one line, which is the uploaded public key fingerprint (MD5 hash digits of public key) in format of 16 octets printed as hexadecimal with lowercase letters and separated by colons, for example:

12:f8:7e:78:61:b4:bf:e2:de:24:15:96:4e:d4:72:53

5.2.2 Public Key Rejection File

Rejection File is a negative acknowledgement file to indicate the uploaded public key file is rejected.

The filename is formatted as **<original file name>.<timestamp – HHMMSS>.<seq>.rej** in **sub-folder /key_management/publickey** where ".<seq>" is optional and appears only when file of same name are uploaded within same second and is accepted.

The .rej file is a text file in window text file format (line ends with CR+LF) in the following format:

#	Field	Type	Size	Remarks
1.	Reject Code	Numeric	5	Reject code
2.	Reject Message	Alphanumeric	255	Reject Message in English

5.2.3 Public Key Expiry Warning File

Public Key Expiry Warning File ("SSHKeyExpireWarning.txt") will be shown in sub-folder **/key_management/publickey** if the public key is going to expire within 14 days (based on the time user login).

The warning file is a fixed width text file in window text file format (line ends with CR+LF) which includes the current key and renewed key (if available). For example:

Public Key	Creation Date	Expiration Date	Fingerprint
Current Public Key	2021-02-01	2021-07-15	90:4e:0d:c7:00:37:51:8d:56:5a:a2:d1:93:27:51:2c
Renewed Public Key	2021-07-01	2023-07-01	a2:d1:93:27:51:2c:4e:0d:c7:00:37:51:8d:56:5a:51

After the current public key has expired and has been removed from the system by housekeeping job, the warning file will not be shown in the folder in the next SFTP login.

5.3 Re-registration of Public Key (Only when private key is being compromised)

In case any of the private key is lost or damaged, Participants and DBs should generate a new set of keys, register and submit the new public key, public key fingerprint in the eService: TechS 8 which is available via Client Connect for re-registration.

6 NETWORK CONFIGURATION

The RAP is only accessible from the Securities and Derivatives Network (SDNet) which is designated for connection to Central Clearing and Settlement System (CCASS). Participants and DBs should refer to the CCASS/ VaR Online/ RAP Installation Procedures available in Client Connect for the network configuration requirement.

Participants and DBs can register at most 4 designated RAP client workstations for RAP. Follow Section 5 above, Participants and DBs should submit the IP addresses of their designated RAP client workstations to HKSCC for registration.

Upon registration of public keys and IP addresses, Participants and DBs can access RAP with their assigned RAP user account via either one of their designated RAP client workstations.

IP addresses of RAP client workstations must fall within the same subnet of SDNet for HKSCC, which is listed below table for reference.

SDNet IP addresses subnet	
10.135.0.0/16 10.136.0.0/16	10.176.0.0/14

6.1 Connectivity of RAP

a. By IP Address

Participants and DBs can connect RAP using the following IP addresses directly. Subject to Participants' and DBs' own setup, when there is a contingency that HKSCC needs to activate its secondary data centre; RAP connection will be interrupted. Once RAP service is resumed, Participants and DBs would need to change the IP address for RAP connection via the secondary data centre.

IP addresses of RAP

Primary data centre	Secondary data centre
10.243.2.141 port 18801 10.243.2.142 port 18801	10.243.66.141 port 18801 10.243.66.142 port 18801

7 IMPORTANT NOTES

7.1 Usage Guidelines

1. Participants and DBs are recommended to poll and retrieve reports/files from RAP ONLY when needed e.g. around the time when the reports/files being available. In addition, any intensive polling should be avoided.

2. Usage management
   Participants and DBs are recommended to retrieve the reports/files that have not been downloaded before. For example, they can use command "mget –r /download/CCASS_GLOB/YYYYMMDD/" or "get –r /download/CCASS_GLOB/YYYYMMDD/" to download the CCASS Global files/reports from the current date folder. (where YYYYMMDD being the current date)

   For efficient use of network bandwidth and shorten download time, Participants and DBs are advised NOT to use wild card command such as "mget –r * " or "get –r *" when downloading files, otherwise all files retained in the folder/subfolders (i.e. all reports/files for past 10 calendar days), will be downloaded.

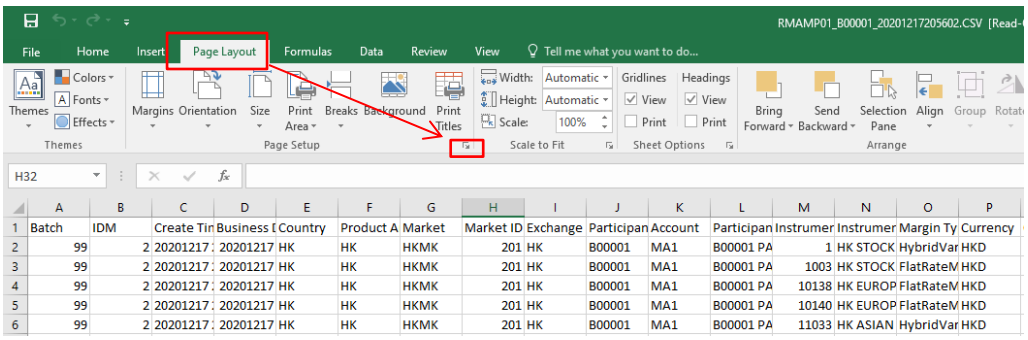
3. CSV file format (only applicable to VaR reports)
   Participants should note that the CSV files downloaded from RAP are in UNIX format in which the end of line is signified by only Line Feed (\n).

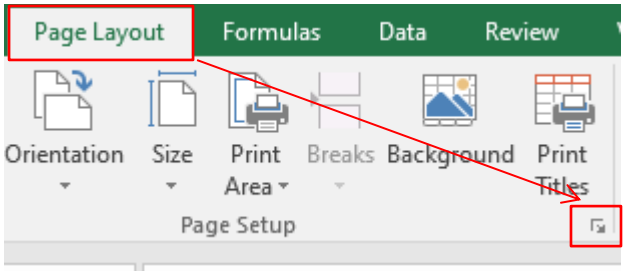
4. Convert csv file to PDF format via Excel (only applicable to VaR reports)

   Participants can also convert the CSV files to PDF format following the below steps:

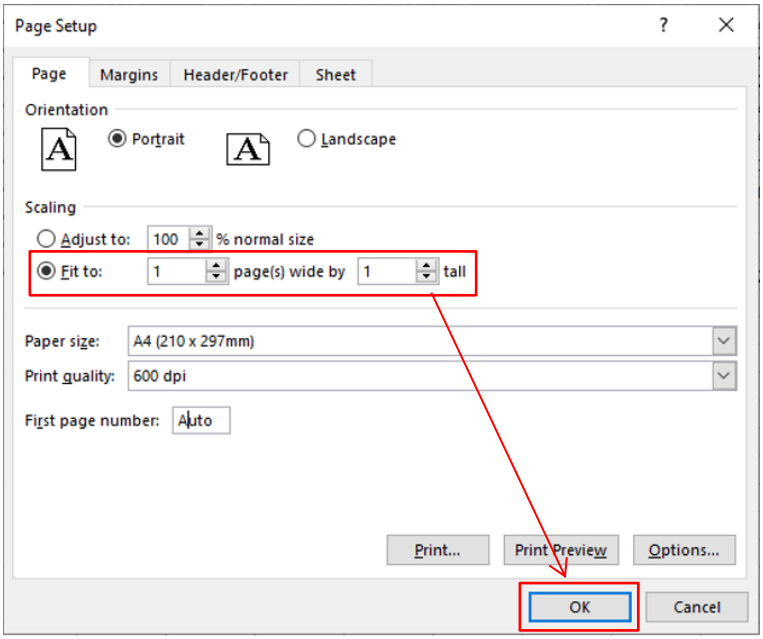
   (i) Open the CSV file in "Excel"

   (ii) Go to **Page Layout** tab, and click the **Page Setup launcher** at the bottom right corner

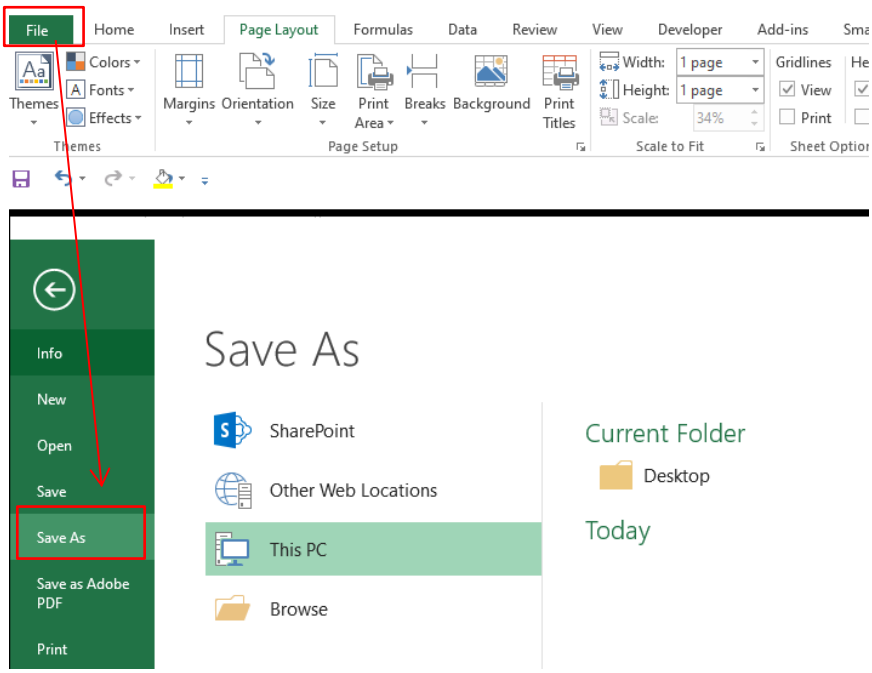




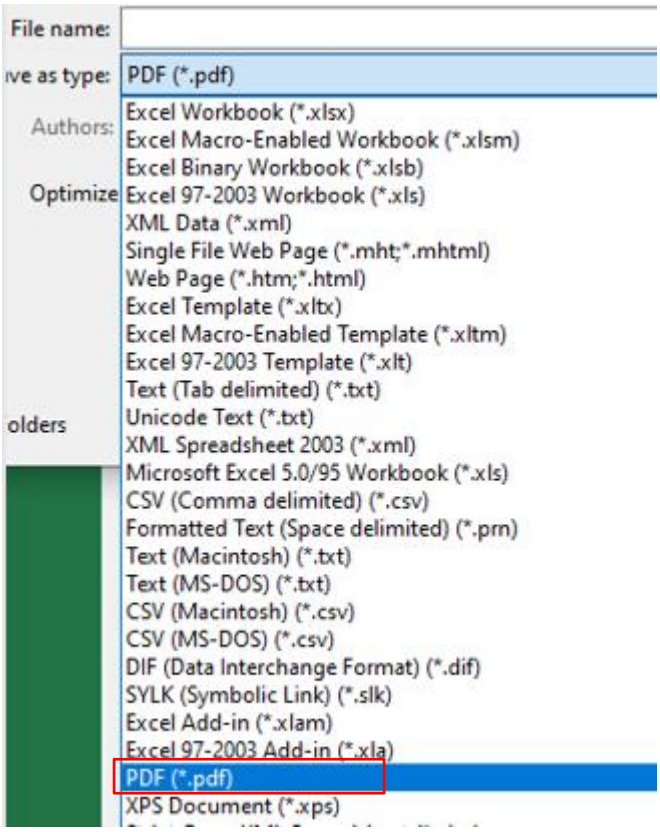
(iii) In the pop-up window, select the Scaling option: **"Fit to: 1 page(s) wide by 1 tall",** then click "OK".



(iv) Go to "File", click "Save As", then choose destination location to save the file



(v) Save file as type “PDF (*.pdf)’, and click “Save”.



5. Performance of file download
   Subject to the size of reports/files being retrieved, the retrieval time could be long and it will occupy the SDNet line bandwidth. If the RAP setup is to share the same SDNet line with other operations, such as CCASS Terminal and VaR Online, performance of corresponding operations e.g. report download via Participant Gateway, may be impacted.

6. Projected download time for RPF *(only applicable to Cash Clearing Participant who subscribed the RPF folder)*
   File sizes of Risk Parameter Files (RPF) is large, it would take a longer time to retrieve. The average total RPF size is approximately 1.3G Byte and is subject to increase along with the number of instruments, Cash Clearing Participants should ensure adequate bandwidth for retrieving RPFs. Please assess and make reference to the following projected file retrieval time under different SDNet bandwidths.

Bandwidth	Project download time for 1.5G Byte files	Bandwidth	Project download time for 1.5G Byte files
1M	~4.2 hr	7M	~ 36 min
2M	~2.1 hr	8M	~ 32 min
3M	~1.4 hr	9M	~28 min
4M	~1.1 hr	10M	~ 26 min
5M	~51 min	20M	~ 13 min
6M	~ 42 min	30M	~ 9 min

7. Connectivity configuration of SFTP program

If there are parameter settings like “Number of simultaneous connections” or “Limit for concurrent download”, please set it to “1” to prevent concurrent login.