



HKSCC Report Access Platform (RAP)

Technical Guide

Version: 7.2

Date: December 2024

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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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”

Latest updates are highlighted in orange

TABLE OF CONTENTS

TABLE OF CONTENTS	3
1 OVERVIEW	4
1.1 BACKGROUND.....	4
2 TECHNICAL INFRASTRUCTURE.....	5
2.1 SFTP STANDARD.....	5
2.2 PRIMARY AND BACKUP SFTP FACILITIES	5
2.3 AUTHENTICITY OF RAP.....	5
3 ACCESS TO RAP VIA SFTP FACILITY	6
3.1 USER ID	6
3.2 SECURE SHELL (SSH) KEY.....	6
3.3 PUBLIC KEY	6
3.4 PUBLIC KEY FINGERPRINT	7
4 OPERATION OF RAP	8
4.1 OPERATION HOURS AND TIME SCHEDULE.....	8
4.2 FOLDER STRUCTURE	8
4.3 SIGN-ON SESSION	9
5 REGISTRATION OF RAP USER ID	10
5.1 INITIAL REGISTRATION	10
5.2 SELF-SERVICE RENEWAL OF PUBLIC KEY	10
5.2.1 <i>Public Key Acknowledgement File</i>	11
5.2.2 <i>Public Key Rejection File</i>	11
5.2.3 <i>Public Key Expiry Warning File</i>	11
5.3 RE-REGISTRATION OF PUBLIC KEY (ONLY WHEN PRIVATE KEY IS BEING COMPROMISED)	12
6 NETWORK CONFIGURATION.....	13
6.1 CONNECTIVITY OF RAP	14
7 IMPORTANT NOTES	15
7.1 USAGE GUIDELINES.....	15

1 OVERVIEW

1.1 Background

This document serves as a technical reference guide for HKSCC's **Cash** Clearing Participants 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 ID
- 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 **Cash** Clearing Participants 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, **Cash** Clearing Participants 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.

2.3 Authenticity of RAP

Cash Clearing Participants can verify the validity of HKSCC's SFTP facility by checking the server SSH host key fingerprint. The fingerprint should match the following value according to the fingerprint algorithm and format supported by their SFTP client.

Algorithm (Format)	Fingerprint
SHA-256 (Hex)	ca:82:3d:60:8b:24:eb:b6:78:b2:d7:8a:ee:2c:34:b9:c1:b1:3f:9f:9a:1c:78:af:80:37:79:c1:80:b8:33:82
SHA-265 (Base64)	yoI9YIsk67Z4steK7iw0ucGxP5+aHHivgDd5wYC4M4I
MD5 (Hex)	83:2b:c1:53:ff:a6:94:88:f5:15:6b:71:78:31:70:b0

3 ACCESS TO RAP VIA SFTP FACILITY

3.1 User ID

To retrieve reports/files, each **Cash** Clearing Participant will be issued with one RAP User ID by HKSCC for access to the RAP, in the following format:

- **CXnnnnn001**

where Xnnnnn is the Participant ID. For example, RAP User ID **CB00001001** would be assigned to **Cash** Clearing Participant with Participant ID B00001.

For **Cash** Clearing Participant, 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), **Cash** Clearing Participant may use its assigned RAP User ID together with the SSH private key to login to the RAP for retrieval of NG reports/files. **Cash** Clearing Participant is recommended to verify and ensure its assigned User ID can access the RAP.

3.2 Secure Shell (SSH) Key

SFTP facility adopts Secure Shell (SSH) public-key authentication. For **each RAP User ID**, **Cash** Clearing Participant 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
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GD1B3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM41oWgV
---- 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:

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

where C stands for Cash Clearing, Xnnnnn is the Participant ID of Cash Clearing Participant.

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.

Cash Clearing Participant SHOULD NOT submit its private key to HKSCC for registration.

4 OPERATION OF RAP

4.1 Operation Hours and Time Schedule

Operation hours of RAP are from 07:00 - 24:00 on each business day.

All reports/files will be available via RAP for retrieval for 10 calendar days after generation. **Cash** Clearing Participant 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 SFTP facility to ensure reports are being retrieved Once Daily Only.

4.2 Folder Structure

Each RAP User ID can access the following folders via RAP:

Folder	Description
download/VAR/yyyymdd	<ul style="list-style-type: none"> For retrieval of common reports/files applicable to all Cash Clearing Participants and reports/files applicable to specific Cash Clearing Participant <Xnnnnn only> yyyyymmdd is the system-generated subfolder for each calendar day Cash Clearing Participants should retrieve reports/files generated and available on specific day from the corresponding date subfolder
download/RPF_COMMON/yyyymdd	<p><i>[Only available to RAP User with folder subscription]</i></p> <ul style="list-style-type: none"> For retrieval of Risk Parameter Files (RPF) only yyyyymmdd is the system-generated subfolder for each calendar day Cash Clearing Participants should retrieve the RPF generated and available on specific day from the corresponding date subfolder
submission	<i>NOT applicable for Cash Clearing</i>

	<i>Participants</i>
key_management	<ul style="list-style-type: none"> For submission of public keys for renewal by Cash Clearing Participants

- a. Each assigned RAP User ID can access the download/VAR folder. Both Participant specific and common reports/files are available in this folder.
- b. Access to RPF folders are 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.
- c. The key_management folder is for submitting public keys for renewal, each RAP User ID will be assigned with an individual key_management folder and it cannot be shared with other RAP User ID.
- d. 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 ID should only be sign-on to one of the designated RAP client workstation at a time. Cash Clearing Participant should sign-out from the current session before signing onto another workstation with the same RAP User ID.

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 ID

5.1 Initial Registration

To register for RAP User ID, **Cash** Clearing Participant should generate a pair of SSH public & private keys per User ID; then upload its public key and input public key fingerprint and IP addresses of its designated RAP client workstations to the RAP Registration and Maintenance Form (eService: TechS 8) **via Client Connect**.

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

- CXnnnnn001.pub

where C stands for Cash Clearing and Xnnnnn is the Participant ID of **Cash** Clearing Participant

DO NOT UPLOAD private keys to **Client Connect**. **Cash** Clearing Participants 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, **Cash** Clearing Participant should generate a new set of keys, register and submit the new public key, public key fingerprint in the RAP Registration and Maintenance Form (eService: TechS 8) which is available from 9 Aug 2021 onwards 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). Cash Clearing Participants should refer to the [CCASS/ VaR Online/ RAP Technical Guide](#) for the network configuration requirement.

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

Upon registration of public keys and IP addresses, Cash Clearing Participants can access RAP with their assigned RAP User ID 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	10.176.0.0/14
10.136.0.0/16	

6.1 Connectivity of RAP

a. By IP Address

Cash Clearing Participants can connect RAP using the following IP addresses directly. Subject to **Cash** Clearing Participants' 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, **Cash** Clearing Participants 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	10.243.66.141 port 18801
10.243.2.142 port 18801	10.243.66.142 port 18801

7 IMPORTANT NOTES

7.1 Usage Guidelines

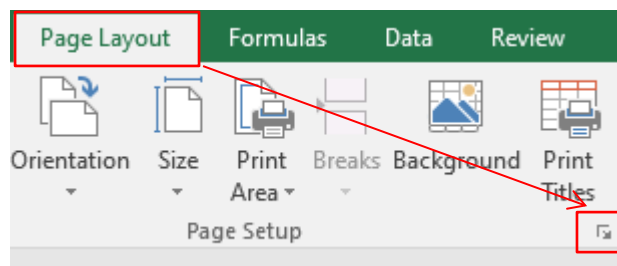
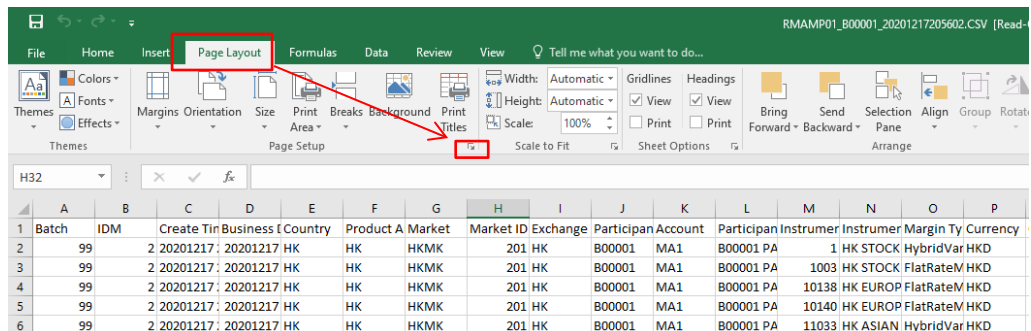
1. **Cash** Clearing Participants are recommended to poll and retrieve reports/files from RAP ONLY when needed e.g. around the time when the reports/files being available. In addition, any intensive polling should be avoided.
2. Usage management
Cash Clearing Participants are recommended to retrieve the reports/files that have not been downloaded before. For example, they can use command “mget –r /download/VAR/YYYYMMDD/” or “get –r /download/VAR/YYYYMMDD/” to download the files/reports from the current date folder. (where YYYYMMDD being the current date)

For efficient use of network bandwidth and shorten download time, **Cash** Clearing Participants 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.

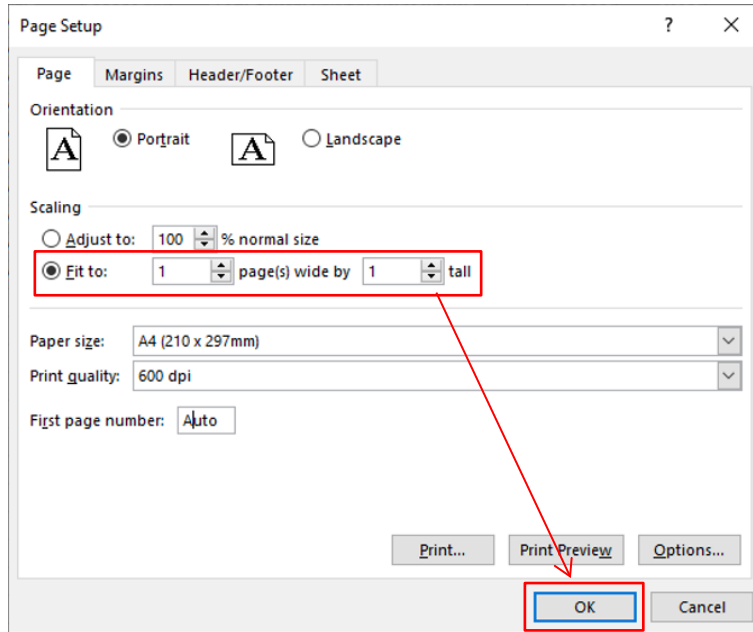
3. CSV file format
Cash Clearing Participants should note that the CSV files downloaded from RAP are in UNIX format in which the end of line is signified by only Line Feed (\n).
4. Convert csv file to PDF format via Excel

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

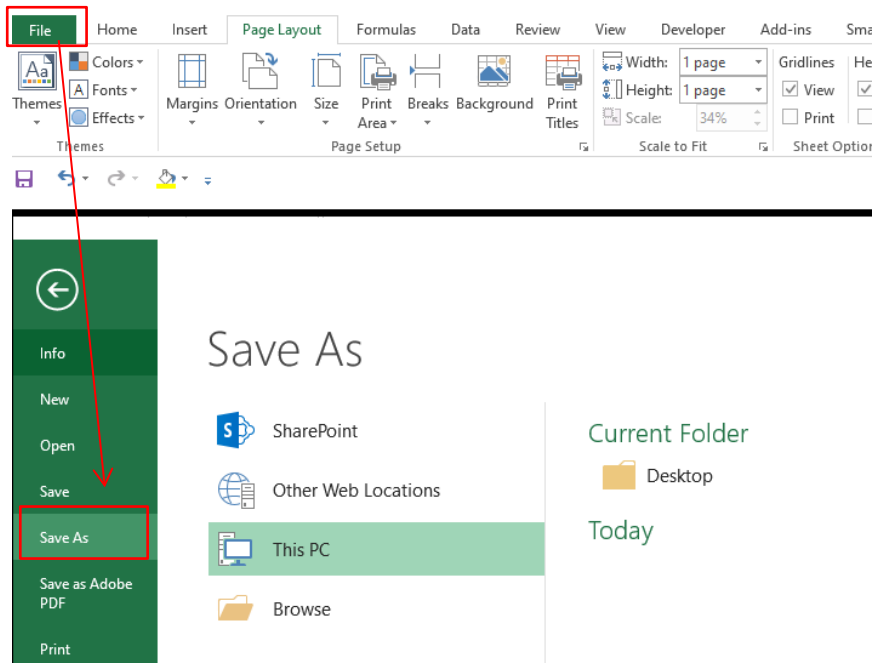
- (i) Open the CSV file in “Excel”
- (ii) Go to **Page Layout** tab, and click the **Page Setup launcher** at the bottom right corner



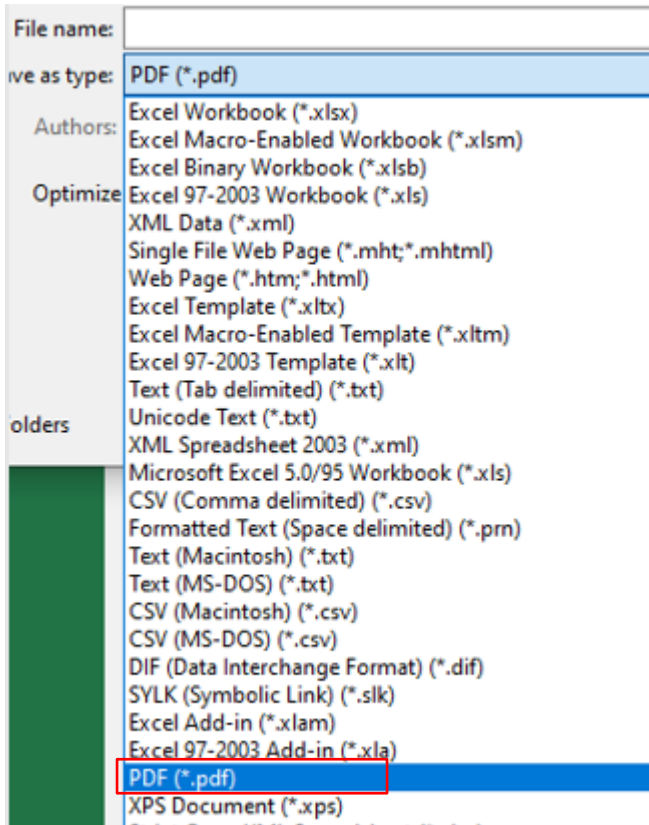
- (iii) In the pop-up window, select the Scaling option: “Fit to: 1 page(s) wide by 1 tall”, then click “OK”.



- (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 CCASS Terminals or 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.