HKEX
香港交易所

OTC Clear Secure File Transfer (SFTP) Configuration Guide

Version: 2.0

Date: 15 Nov 2024

INTRODUCTION

This document provides the Clearing Members and Sponsored Settlement Members of OTC Clear with the information and procedures to configure their systems and PCs for downloading reports from the OTC Clear Secure File Transfer service, using the Secure File Transfer Protocol (SFTP).

HKEX and/or its subsidiaries endeavour to ensure the accuracy and reliability of the information provided but accept no liability (whether in tort or contract or otherwise) for any loss or damage arising from any inaccuracy or omission or from any decision, action or non-action based on or in reliance upon information contained in this document. Also, all examples in this document are used for illustration purposes only and should not be considered the results of actual market circumstances. HKEX reserves the right to amend any details in this document at any time, without notice.

1. System Requirements

The OTC Clear Secure File Transfer service is provided by OTC Clear to Clearing Members and Sponsored Settlement Members (“Members”) of OTC Clear only.

To use the service, Members can use an SFTP Client supporting the Secure File Transfer Protocol (SFTP) Version 3, such as the following software, on any platform:

- OpenSSH SFTP Client
- WinSCP

Members can download the reports using the SFTP Client from a PC or a server, using a script, an automated system or by a user manually, according to their own preferences. In the sections below, we would refer to the OTC Clear Secure File Transfer service as the SFTP server.

2. Communication Line Setup

The configuration of SDNet/2 is the same for both OASIS and the SFTP server. If a user PC is already connected to OASIS, it can be used for access to the SFTP server as well, provided that the Member’s internal firewall has the additional IP address and ports opened.

Step 1: Connect to SDNet/2 Routers

Step 1.1:

Before the configuration, please ensure that the Metro Ethernet communication lines and routers have been installed and configured properly by the SDNet/2 service provider already.

Step 1.2:

Connect the SDNet/2 routers to the LAN switches with LAN cables. The LAN interface of the SDNet/2 router supports network speed up to Gigabit Ethernet and it is configured as “Auto Negotiation” (i.e. both speed and duplex mode are auto). The LAN switch ports (connecting the SDNet/2 routers) should also have “auto” configuration settings and should provide a single VLAN (Layer 2) for connecting SDNet/2 router and the SFTP client.

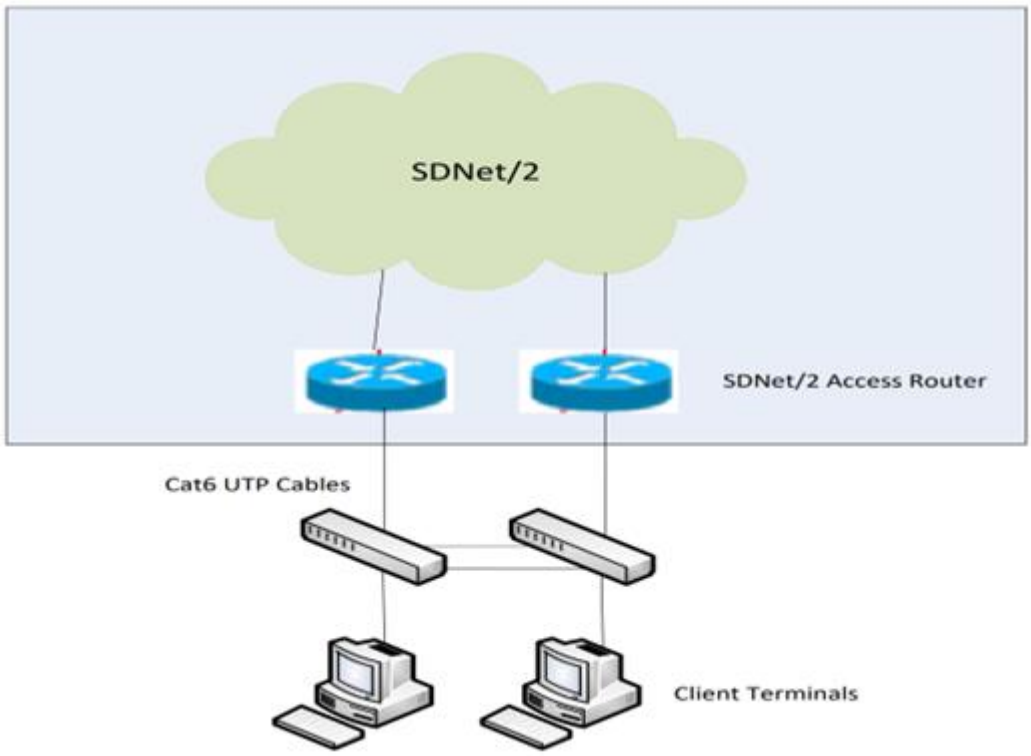
Step 1.3:

HSRP/VRRP group number on SDNet/2 router for OASIS will be assigned by the SDNet/2 service vendor. Members should avoid using the same HSRP/VRRP group number in their network for applications other than OASIS.

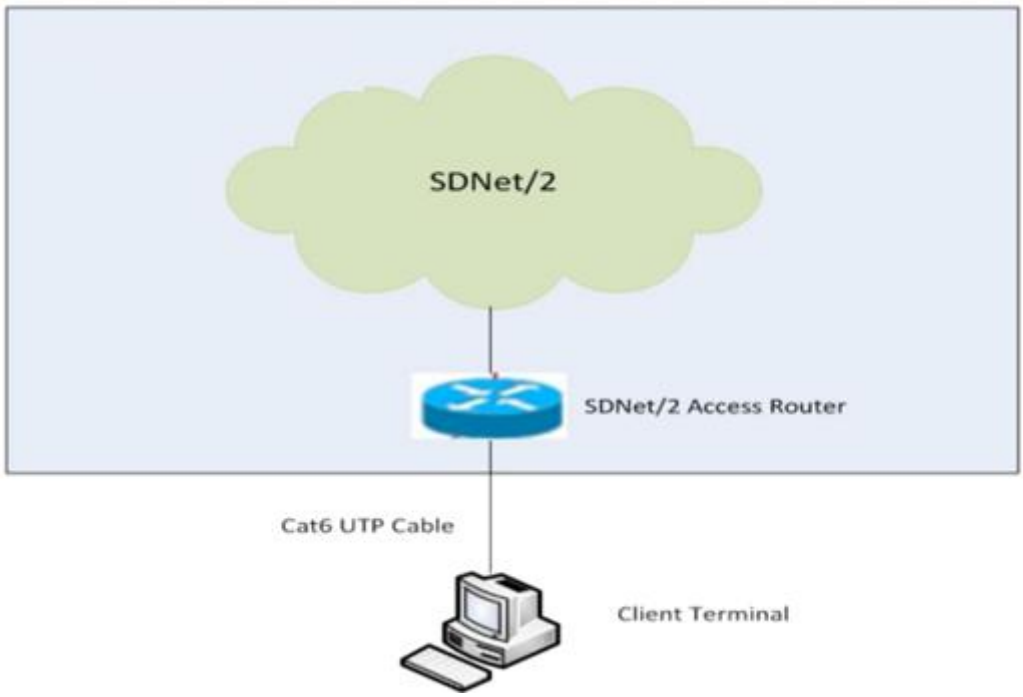
Step 1.4:

Connect the PC/Server to the routers and LAN switch with LAN cables. There are two possible options to establish the connection:

Option 1: Dual-link connection (for production site)



Option 2: Single-link connection



Step 2: Firewall Setup

The following IP addresses and ports need to be opened on the firewall for access to the production SFTP servers:

Site	Port	Production IP Address	Direction
Primary	18801 (TCP)	10.154.11.141 10.154.11.142	From Member's PC/Server to OTC Clear SFTP Server
Secondary/DR	18801 (TCP)	10.153.11.141 10.153.11.142	From Member PC/Server to OTC Clear SFTP Server

For development environment on SDNet/2 Testing Line:

Site	Port	Production IP Address	Direction
Development	18801 (TCP)	10.154.11.141	From Member's PC/Server to OTC Clear SFTP Server

As the IP Address is the same as production, it is highly recommended for the Member to set up a dedicated network segment or use NAT for the development environment.

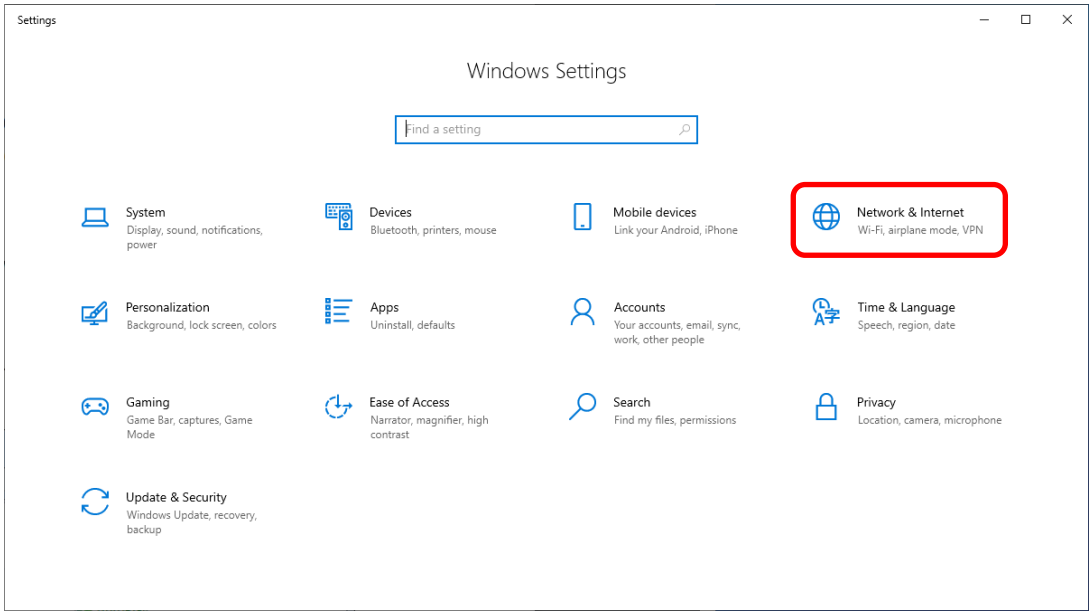
Source IP Address

A pre-defined range of IP addresses is assigned to each Member on SDNet/2 by their network provider. Members should ensure that the clients for SFTP should use an assigned IP address when connecting. If Network Address Translation (NAT) is used, the Member's firewall should translate the source IP address to the assigned range of IP addresses, otherwise login will fail.

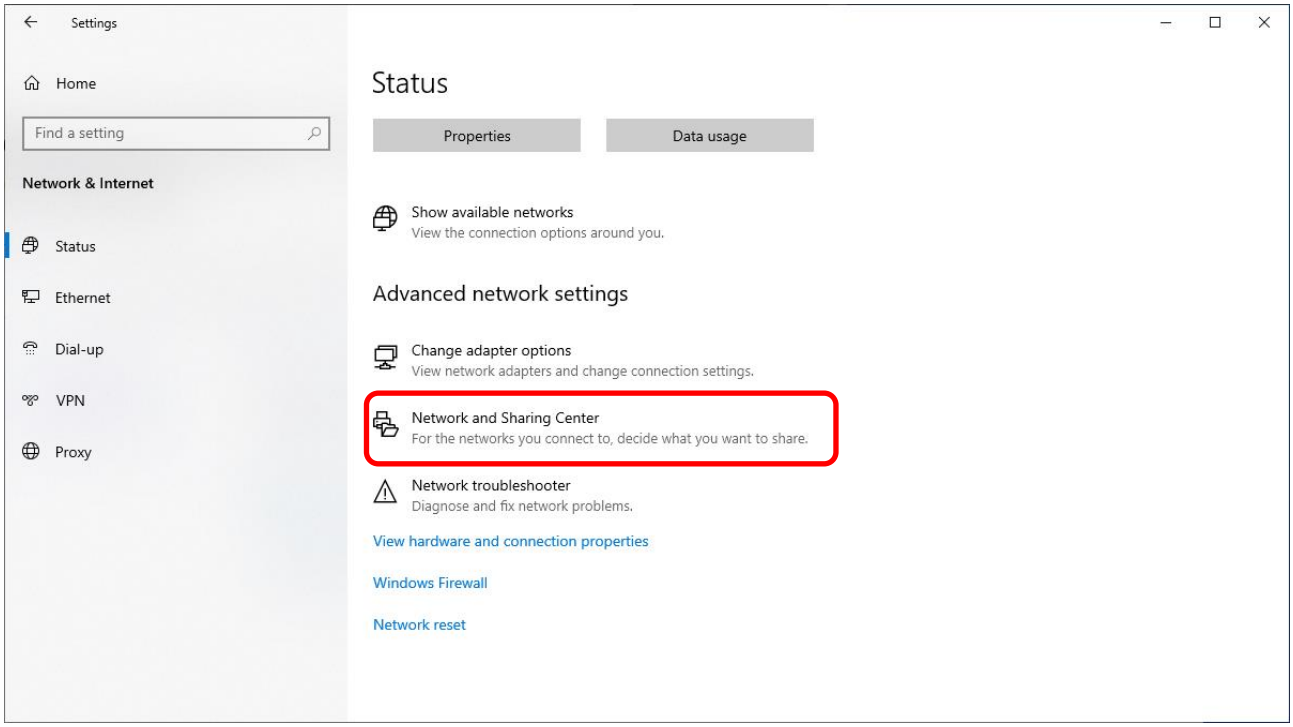
3. TCP/IP and Ethernet Card Configuration (for Windows 10 PC)

Step 1: Login in as an administrator to perform the following procedures.

Step 2: Click "Start", go to the "Control Panel", and then select "Network & Internet":

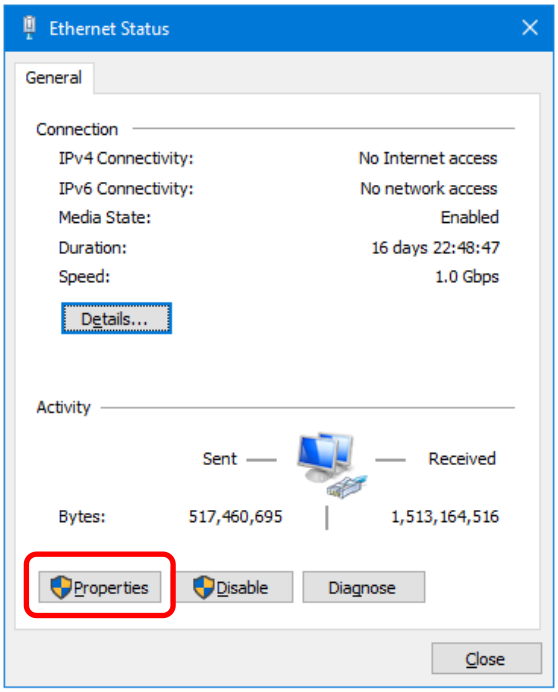


Step 3: Under “Advanced”, click on “Network and Sharing Center”:

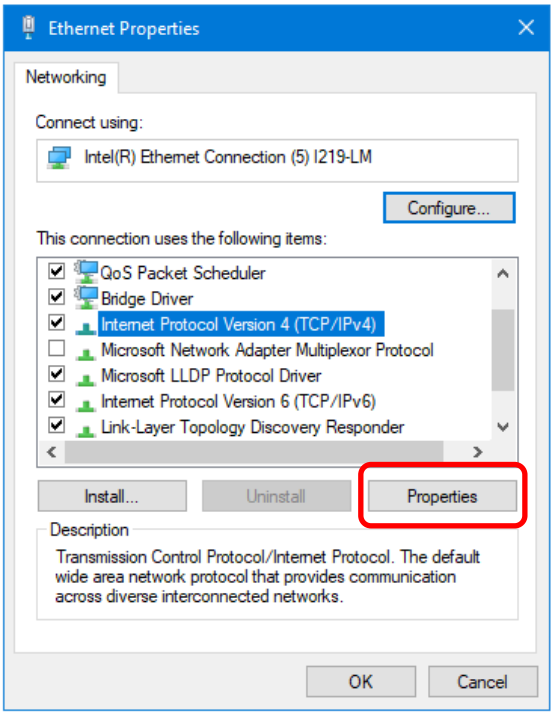


Step 4: Under “View your active networks”, click on the Connections you would like to configure. Depending on your current settings, it may be called “Ethernet” or “Local Area Network”.

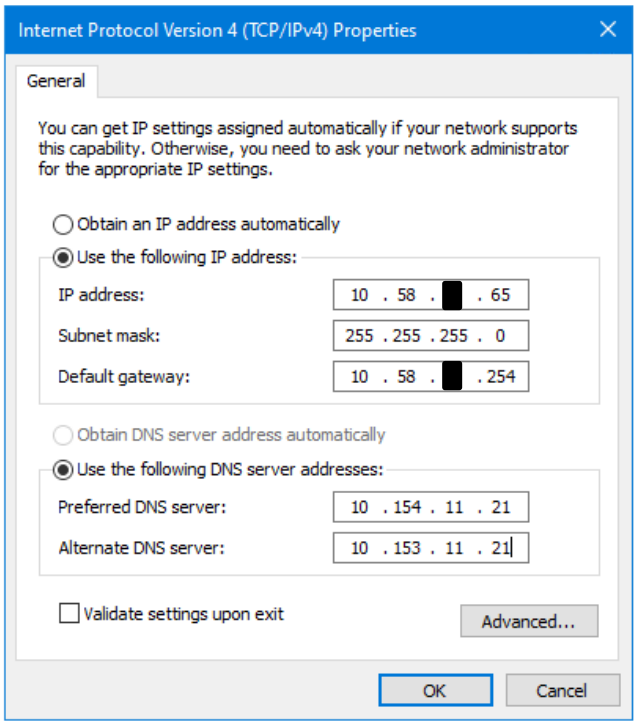
Step 5: In the Status window (e.g. “Ethernet Status”), click on the “Properties” button.



Step 6: Select “Internet Protocol Version 4 (TCP/IP)” and click on “Properties”.



Step 7: Select “Use the following IP address” radio button and enter the following information:



1. Enter the “IP address” and “Default gateway” assigned by your SDNet/2 service provider.
2. Enter “255.255.255.0” for “Subnet mask”.
3. If you would also use OASIS on this PC, you may select the “Use the following DNS server addresses” radio button and enter the Preferred DNS server” and “Alternate DNS server” as set out in the Step 2.2 of the OASIS Configuration Guide.
4. Click “OK”.

Step 8: Add static routes

1. Open a command prompt
2. Issue the following commands (please use the "Default gateway" assigned by your SDNet/2 service provider instead of x.x.x.254):

```
route add -p 10.153.11.0 mask 255.255.255.0 x.x.x.254
route add -p 10.154.11.0 mask 255.255.255.0 x.x.x.254
```

Step 9: Restart the Windows PC

Reference information

The following range of IP address / subnet mask may be assigned by SDNet/2 service providers (in CIDR):

- PCCW - 10.58.0.0/24 to 10.58.127.0/24
- HKBNES - 10.59.0.0/24 to 10.59.127.0/24

The last number in the IP address may be x.x.x.65 ~ x.x.x.190.

4. Public Key Management

Registration of Public Keys

For each SFTP account, the Member needs to generate a pair of SSH2 Private and Public Keys and register the Public Key with OTC Clear.

OTC Clear only accepts SSH2 Public Keys generated using the RSA algorithm, with a key length of 2048, 3072 or 4096 bits, stored in PEM 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 SSH2 Public Key should be saved in a separate file with the following requirements:

- The file extension must be ".pub"
- The file name must not exceed 128 characters
- The file name can only contain alphanumeric characters or the following special characters:

- '.' (dot)
- '-' (dash)
- '_' (underscore)
- ' ' (blank)
- '@' (ampersand)

To convert your SSH2 Public Key into the PEM format, you may use the ssh-keygen command, for example:

```
ssh-keygen -ef id_rsa.pub > id_rsa_pem.pub
```

The ssh-keygen command is available on Windows and Linux. Alternatively, you can use PuTTYgen for conversion if it is installed with your WinSCP.

The Member should send the SSH2 Public Key to OTC Clear by e-mail for initial registration.

Upon successful registration, the expiration date of the current SSH2 Public Key will be automatically set to 2 years from registration date.

Key Renewal Process

Members can renew the SSH2 Public Key by uploading it to the folder **/key_management/publickey/** on the SFTP server. After the upload has completed, an Acknowledgement File (.rcvd) or Rejection File (.rej) would be generated in the same folder.

The Public Key would be rejected if:

- The file name and extension does not meet the above criteria
- The SSH2 Public Key is not in PEM format
- The PEM header does not have the expected label (i.e. SSH2 PUBLIC KEY)
- The key length is not 2048, 3072 or 4096 bits
- The new Public Key is the same as the current one
- The file does not pass virus scanning

Notes:

- The Acknowledgement File (.rcvd) or Rejection File (.rej) are cleaned up after 24 hours
- If the SSH2 Public Key file name exceeds 124 characters, it will be rejected with no Rejection File generated.

5. Member Report Location

One SFTP account would be provided for each Member of OTC Clear. OASIS reports would be delivered to the SFTP account at specific time intervals each day, roughly hourly. The exact time of report publication in the SFTP server may fluctuate from day to day based on business volume and system run time.

Simultaneous login to the same SFTP account is not allowed. If a user has logged into an account and has not logged out yet, when a second user logs into the same account, the first user would be logged out. Any file transfer activity in progress by the first user may be interrupted.

Clearing Report Download

There are two folders in the account for clearing reports:

1. **/download/OTC_HOUSE/yyyymmdd/** for House Activity Reports
2. **/download/OTC_CLIENT/yyyymmdd/** for Client Clearing Activity Reports.

In the two folders above, there are 3 zip files for downloading:

Type	File Name	OASIS report included by generation time	Mode
SOD	SOD_yymmdd_<*Account Name*>.zip	04:00 to 08:45 (HKT)	Append
Intraday	INT_yymmdd_<*Account Name*>.zip	08:45 to 20:00 (HKT)	Append
EOD	EOD_yymmdd_<*Account Name*>.zip	20:00 to 04:00 (HKT)	Append

The file name format for the reports in the ZIP files are as below:

House Activity Report:

- **reportname_99999999_yyyy-mm-dd hh-mm-ss AM.csv** or
- **reportname_99999999_yyyy-mm-dd hh-mm-ss PM.csv**

Client Activity Report:

- **reportname_C_99999999_yyyy-mm-dd hh-mm-ss AM.csv** or
- **reportname_C_99999999_yyyy-mm-dd hh-mm-ss PM.csv**

where **99999999** is the sequence number generated by OCASS.

Notes:

1. The EOD zip file is ready for download after 22:00 normally.
2. In the Member Testing environment, reports will be provided on request basis and the file structure may be different.

SSM Client Activity Report Download

Clearing members would also be able to access the Sponsored Settlement Member (SSM) Client Activity Reports.

The following folder is used for SSM reports:

- **/download/OTC_SSM/yyyymmdd/**

There are 3 zip files for downloading in this folder:

Type	File Name	OASIS report included by generation time	Mode
SOD	SOD_yymmdd_<SSM_*Account Name*>.zip	04:00 to 08:45 (HKT)	Append
Intraday	INT_yymmdd_<SSM_*Account Name*>.zip	08:45 to 20:00 (HKT)	Append
EOD	EOD_yymmdd_<SSM_*Account Name*>.zip	20:00 to 04:00 (HKT)	Append

Notes: the EOD zip file is ready for download after 22:00 normally.

6. Report Housekeeping

The reports in the SFTP server will remain available for download for a maximum of eighteen calendar days after they are generated. Housekeeping of older reports is performed by the system daily.

7. Service Hours

The service hours for the SFTP server are Sunday 06:00 – next Sunday 01:30 (HKT).

8. Contingency Handling

Scenario 1: Cannot connect to one of the two IP addresses for the Primary SFTP server

OTC Clear provides two IP addresses for the Primary Site. If Members encounter a failure when connecting to one of the IP addresses, they should connect to the other IP address first. Both IP addresses in the Primary Site are active at the same time.

Scenario 2: Cannot connect to both IP addresses for the Primary SFTP server

If Members cannot connect to both IP addresses of the SFTP server in the Primary Site, they should download the reports using OASIS. Also, they should inform OTC Clear if further help is needed.

Scenario 3: Site failure declared by HKEX

If HKEX has declared a failure of the SFTP server in the Primary Site, Members should change their connection to use the Secondary/DR Site instead. Both IP addresses in the Secondary/DR Site are active at the same time.