DCASS OAPI Connectivity Contingency Guide

1. Primary and Backup Gateways

Upon successful application to connect to DCASS, Clearing Participant ("CP") is assigned a primary gateway plus a list of backup gateways with designated port numbers for each provided login ID. CPs should connect their DCASS OAPI programs to the assigned primary gateway at the assigned port number. CPs should also keep the list of the backup gateways ready in their system so that in case a connected gateway has a failure, CPs' system could hunt the next gateway in the list for connection automatically.

1.1 Backup Gateways and Auto-Switching

The Exchange had provided all CPs backup gateway connection information for contingency purpose when they applied for OAPI user account. CPs are recommended to automate their systems firstly to auto-reconnect to the current DCASS Primary Central Gateway, and if the Primary Central Gateway remains inaccessible, then secondly to auto-switch to Backup Central Gateways. The purpose of attempting to reconnect to primary gateway aims to avoid the potential situation of a network interruption triggering all CPs to switch to backup gateways, whereas the backup gateways were designed for primary gateway failure. CPs should decide the number of reconnection attempts before auto-switching to backup gateway.

CPs are also recommended to coordinate with their IT teams and vendors for necessary preparation including but not limited to the firewall set up. Please note that contingency gateways are in standby mode and used for site-failover only.

Contingency Gateway List

HKEX's Data Centre	Central Gateway	IP Address Range
Primary	Primary	10.151.5.81 or 10.151.5.82
	Backup	10.151.5.83
Secondary	Primary	10.152.5.83 or 10.152.5.84
	Backup	10.152.5.85

1.2 General Connectivity Contingency Guidelines

OAPI disconnection from the HKEX derivatives market systems could be due to a variety of reasons. CPs should devise with their technical teams necessary recovery plans and follow their own troubleshooting procedures to determine the appropriate course of remedial actions according to their contingency plan.

Below are some general guidelines for reference by CPs when considering their own recovery plan.

- Investigate if the disconnection is caused by the CP's software or infrastructure. Take remedial steps where necessary before reconnection
- When recovering from an OAPI disconnection, the OAPI Programs shall first attempt to reconnect to the current DCASS Primary Central Gateway
- If the Primary Central Gateway remains inaccessible, CPs shall attempt to reconnect to the Backup Central Gateways previously allocated by HKEX
- CPs should report connectivity issues for their SDNet communication links to the respective telecommunication service providers. Hosting clients shall contact the HKEX Hosting Services Hotline in case of communication link issues
- In the event HKEX announces a site failover, CPs shall switch their connections to the Backup Data Centre according to the arrangement previously provided

1.3 Other Troubleshooting Guidelines

- Review if there is any recent network, hardware or software changes
- Report to in-house support team for first-hand troubleshooting
- Report to clearingpsd@hkex.com.hk if suspecting that there is a breach in password security
- Report to clearingpsd@hkex.com.hk if the CP's system has switched to using a backup gateway, the current situation and the returned code/message from the failed OAPI function call previously for investigation