



# FINI Testing Environment Setup and Access Guide

25 November 2022

**HKEX**  
香港交易所

For External User Testing (EUT), FINI users must set up a Virtual Private Network (VPN) for connecting to HKEX's testing environment.

The purpose of document is to guide your firm through the steps to set up the VPN on employee desktop computers and corporate networks.

**1** Intended Audience

**2** Testing Registration

**3** VPN Setup

- Client-to-Site VPN
- Site-to-Site VPN

**4** Test Site Access

**5** Support



# 1 Intended Audience

- All FINI users who want to test and familiarise with the FINI platform functions

## Sponsor

For Designated Sponsor +  
Other Sponsors

## Legal Counsel

For Sponsor Counsel  
+ Issuer Counsel

## Intermediary

For Designated OCs, other OCs &  
distributors

## HK Share Registrar

## HKSCC Participant

For users of the EIPO service

## FINI Bank

For Designated EIPO Banks &  
Issuer's Receiving Banks

- HKEX recommends this guide to be read by your firm's IT department or system vendor staff with administrator rights to install software on corporate desktop computers or perform configurations on Network/VPN equipment



## 2

# Registration

\*\*\* Your firm must be on-boarded as a FINI user before registering for VPN access (Online FINI Registration Form)

- Complete Online FINI Testing Registration Form on behalf of your firm
- Input and submit the required information (e.g. company name, VPN connectivity type)
- **NO** signature from your firm's authorised signatory(ies) is required for this form

**HKEX**  
香港交易所  
HKEX Online FINI Registration Form

This form should be used for:  
i) New Applicants - applying to register your company as a new FINI User;  
ii) Existing FINI Users - applying to register your company for additional FINI User Type(s).

Before you get started, please:  
1) read carefully the [Explanatory Notes](#) on FINI webpage;  
2) ensure that supporting documentation (where applicable) are prepared ahead (refer to Explanatory Notes) for submission in the Supporting Document section of this form.

More information about FINI can be found on FINI webpage:  
<https://www.hkex.com.hk/fini>

0% ————— 100%

**HKEX**  
香港交易所  
HKEX FINI Testing Registration Form

This form is used for FINI testing registration.

**Notes:**  
1) Before you register for FINI testing, please ensure your firm (except for HKSCC Participants with existing access to HKEX Client Connect) has submitted an [Online FINI Registration Form](#) and received HKSCC's approval for the use of FINI.  
2) Upon your submission of this form, we will process your registration request and provide you the access information within 10 business days.  
3) In case you need to change your FINI testing registration details (such as contact persons, VPN users information, etc.), please submit a new FINI Testing Registration Form.

For further information about FINI, please visit the [HKEX FINI webpage](https://www.hkex.com.hk/fini).

Please complete the following Captcha:

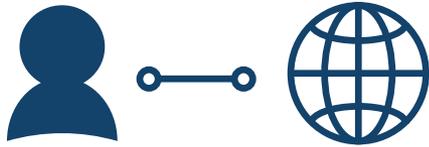
I'm not a robot

0% ————— 100%

### 3

## VPN Setup

Your firm is required to choose one of the following options during registration:



### Client-to-Site VPN

Recommended for easy setup

- Use provided client application for connecting to FINI's testing environment VPN
- Each FINI user company limited to 4 user accounts \*



### Site-to-Site VPN

Recommended for advanced setup  
(dedicated network support team required)

- Use own corporate VPN site for connecting to FINI's testing environment VPN
- No limit to user accounts per FINI user company



\* More user accounts available upon request.

3a

# Client-to-Site VPN

## Pre-requisites



### Corporate Desktop Computer

Connect to the FINI  
testing environment VPN

- Operating System (  /  /  )
- Web Browser (  /  /  )
- Active internet connection
- Administrator rights to install software



### Personal / Work Mobile Phone

Log in using Multi-Factor  
Authentication (MFA)

- An Authenticator App, e.g.:
  - Google Authenticator 
  - Microsoft Authenticator 
  - Symantec VIP 
  - Twilio Authy 

Functional purpose

### Additional requirements

Officially supported by HKEX



## 3a

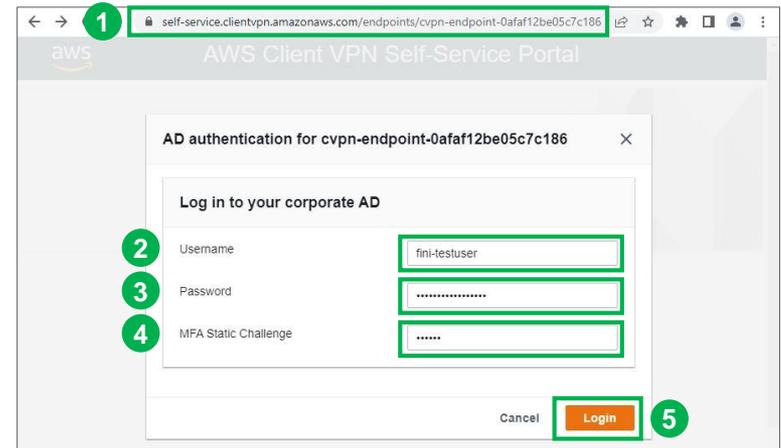
# Client-to-Site VPN

## Installation (1/2)

After registration, each user will receive two emails from [projectfini@hkex.com.hk](mailto:projectfini@hkex.com.hk) containing a **Username**, **Password** and QR Code.

The QR Code should be scanned using the user's authenticator app, which will generate a new **MFA Static Response** every 30 seconds.

- 1 Go to: <https://self-service.clientvpn.amazonaws.com/endpoints/cvpn-endpoint-0afaf12be05c7c186>
- 2 Input **Username** (provided from email)
- 3 Input **Password** (provided from email)
- 4 Input **MFA Static Response** (generated from authenticator app)
- 5 Click **Login**



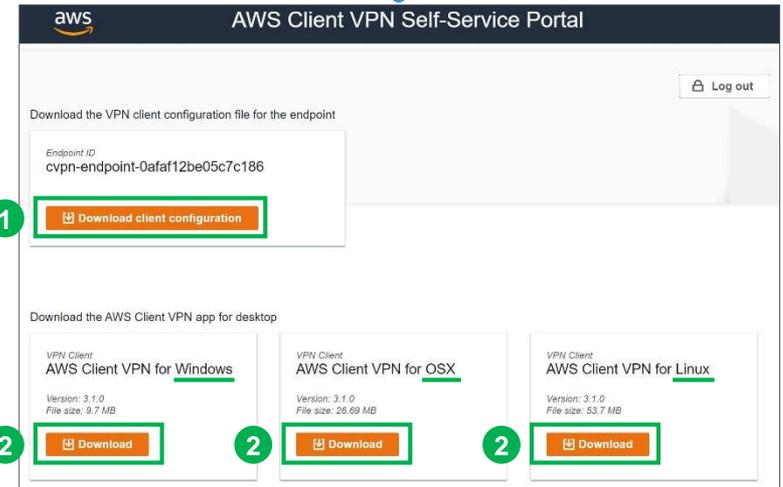
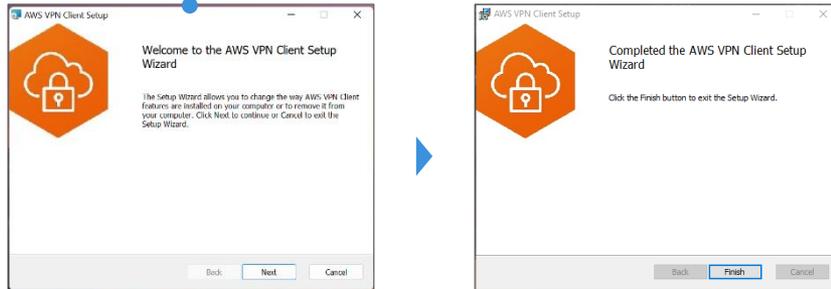
# 3a

# Client-to-Site VPN

## Installation (2/2)

After successful login, the AWS Client VPN Self-Service Portal will appear:

- 1 Download **VPN Configuration File** and save for next step
- 2 Download **AWS Client VPN installer** (based on the desktop computer's operating system) and install software

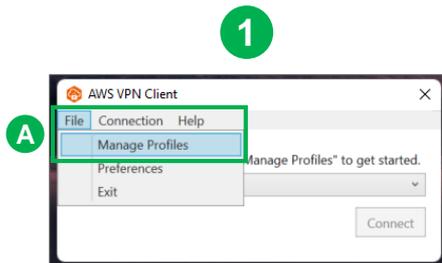


# 3a

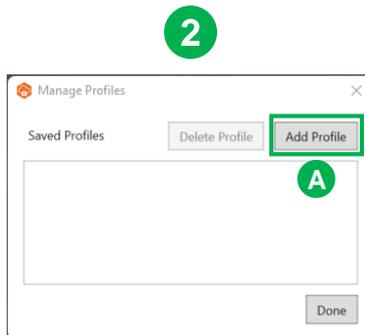
## Client-to-Site VPN

### Connection (1/3)

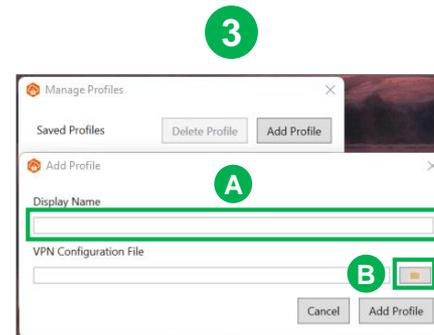
After successful installation, the AWS Client VPN may be opened for establishing the connection:



A Click **File** > **Manage Profiles**



A Click **Add Profile**



A Input **Display Name** of choice

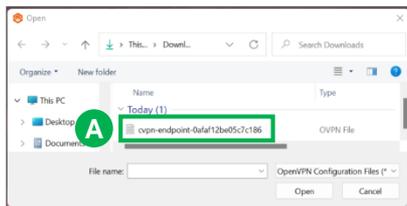
B Click folder icon to import **VPN Configuration File**



# 3a Client-to-Site VPN

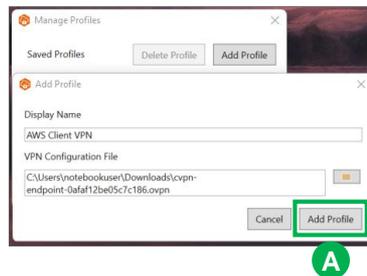
## Connection (2/3)

4



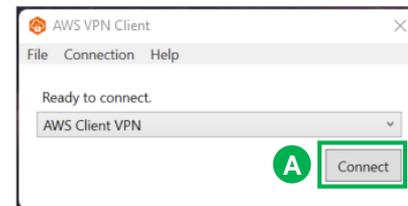
A Select **VPN Configuration File** for import

5



A Click **Add Profile**

6



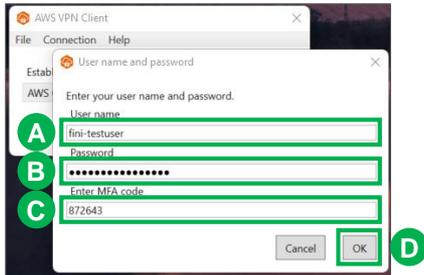
A Click **Connect**



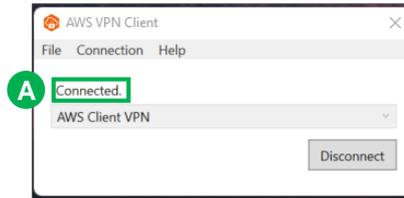
**3a**

# Client-to-Site VPN

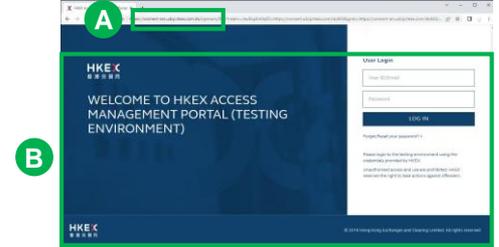
## Connection (3/3)

**7**

- A** Input **Username** (from email)
- B** Input **Password** (from email)
- C** Input **MFA Static Response** (generated from authenticator app)
- D** Click **OK**

**8**

- A** Upon successful login, the system will display **Connected**

**9**

- A** Use any web browser and connect to: <https://connect.u4cp.hkex.com.hk>
- B** Successfully loaded webpage indicates successful VPN setup



## 3b VPN Setup

### Pre-requisites



#### Corporate VPN Peer Gateway

Set up connectivity the FINI  
testing environment

- Gateway Device\*
- Command line interface
- Active internet connection



#### Corporate Desktop Computer

Connect to the FINI  
testing environment VPN

- Operating System (  /  /  )
- Web Browser (  /  /  )
- Active internet connection

#### Functional purpose

#### Additional requirements

Officially supported by HKEX



\* See the Appendix for a list of supported gateway devices.

## 3b

## VPN Setup

## Installation (1/3)

After completing the [Online FINI Testing Registration Form](#), a VPN setup form will be available to download for further supplementation.

The completed form should be returned to [projectfini@hkex.com.hk](mailto:projectfini@hkex.com.hk) for further setup. After HKEX ITD has completed its setup, a public IP and configuration file will be provided via email.

HKEX VPN PEER		CUSTOMER VPN PEER	
Device (Make/Model): AWS		Device Vendor (Make/Model) <sup>1</sup> :	
		Device Platform:	
		Device Platform Software:	
Test Target Host (Default: 10.2.0.2 [DNS])		Public IP:	

VPN PARAMETERS PREFERENCE		
IKE Parameters	Default Settings	Client Optional Settings
IKE Negotiation Mode	Main Mode only	Main Mode only
IKE version <sup>1</sup>	Rev2	Rev1 / Rev2
Rekey margin time (seconds) <sup>2</sup>	540	
Rekey fuzz (percentage) <sup>4</sup>	100	
Replay window size (packets) <sup>3</sup>	1024	

PHASE 1		
IPSEC Parameters	Defaults Setting	Client Optional Settings
Authentication Method	Pre-shared key <sup>1</sup> (send separately)	To use HKEX pre-shared key
Security Association Lifetime (min) <sup>2</sup>	480 min	min (keyfile)
Encryption Algorithm / Authentication Algorithm <sup>3</sup>	AES-256	
Hashed Message Authentication Code (HMAC) / Hash Algorithm / Integrity Algorithms <sup>4</sup>	SHA2-256	
Diffie-Hellman Group (DH Group) <sup>11</sup>	Group 14	Group
DPD timeout (seconds) <sup>11</sup>	30	
DPD timeout action <sup>11</sup>	Clear	

PHASE 2		
IPSEC Parameters	Defaults Setting	Client Optional Settings
Security Association Lifetime (min) <sup>11</sup>	60 min	min (keyfile)
Encryption Algorithm / Authentication Algorithm	AES-256	
Hashed Message Authentication Code (HMAC) / Hash Algorithm / Integrity Algorithms	SHA2-256	
Diffie-Hellman Group (DH Group)	Yes, Group 14	

(After HKEX received user input, we would set up customer gateway in AWS, public IP for tunnels will then be generate from that user in a configuration file (.bat))

SECURED NETWORKS/HOSTS	
HKEX NETWORK / HOSTS / TARGET VPC	CUSTOMER NETWORK / HOSTS / Device Subnet <sup>11</sup>
CIDR Block (Default: 10.2.0.0/22)	

CLIENT INFORMATION		
Company Name: ..... Fill in by Business partner: .....		
Customer Contact Name:	Phone:	Email
Primary contact -		
Secondary contact -		
Customer Support Contact:	Phone:	Email:
Additional comments:		

If your firm has no preference, use the following default settings.



## Installation (2/3)

HKEX VPN PEER		CUSTOMER VPN PEER	
Device (Make/Model): AWS		Device Vendor (Make/Model) <sup>1</sup> :	
		Device Platform:	
		Device Platform Software:	
Test Target Host: (Default: 10.2.0.2 [DNS])		Public IP:	

VPN PARAMETERS PREFERENCE		
IKE Parameters	Default Settings	Client Optional Settings
IKE Negotiation Mode	Main Mode only	Main Mode only
IKE version <sup>2</sup>	ikev2	<input type="checkbox"/> ikev1 <input type="checkbox"/> ikev2
Rekey margin time (seconds) <sup>3</sup>	540	
Rekey fuzz (percentage) <sup>4</sup>	100	
Replay window size (packets) <sup>5</sup>	1024	
PHASE 1		
IPSEC Parameters	Defaults Setting	Client Optional Settings
Authentication Method	Pre-shared key <sup>6</sup> (send separately)	To use HKEX pre-shared key
Security Association Lifetime (min) <sup>7</sup>	480 min	min (keylife)
Encryption Algorithm / Authentication Algorithm <sup>8</sup>	AES-256	
Hashed Message Authentication Code (HMAC) / Hash Algorithm / Integrity Algorithms <sup>9</sup>	SHA2-256	
Diffie-Hellman Group (DH Group) <sup>10</sup>	Group 14	Group
DPD timeout (seconds) <sup>11</sup>	30	
DPD timeout action <sup>12</sup>	Clear	

Field	Description	Supported Values
IKE version	Version of Internet Key Exchange	ikev1, ikev2 (default: ikev2)
Rekey margin time (sec)	The period of time before phase 1 and 2 lifetimes expire, during which AWS initiates an IKE rekey	60 and half of phase 2 lifetime
Rekey fuzz (%)	The percentage of the rekey window during which the rekey time is randomly selected	0 to 100
Replay window size (pkts)	The number of packets in an IKE replay window	64 to 2048

Field	Description	Supported Values
Authentication Method	String (length: 8 to 64) with alphanumeric characters, underscore ('_') or dot('.') (cannot start with 0)	
Security Assoc. Lifetime (min)		15 to 480 minutes
Encryption Algo. / Authentication Algo.		AES128, AES256, AES128-GCM-16, AES256-GCM-16
HMAC / Hash Algo. / Integrity Algos.		SHA1, SHA2-256, SHA2-384, SHA2-512
DH Group		2, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24
DPD timeout (sec)	The number of seconds after which a DPD timeout occurs.	≥ 30
DPD timeout action	The action to take after dead peer detection (DPD) timeout occurs.	Clear, Restart, None (default: Clear)

## Installation (3/3)

PHASE 2		
IPSEC Parameters	Defaults Setting	Client Optional Settings
Security Association Lifetime (min) <sup>13</sup>	60 min	min (keylife)
Encryption Algorithm / Authentication Algorithm	AES-256	
Hashed Message Authentication Code (HMAC) / Hash Algorithm / Integrity Algorithms	SHA2-256	
Diffie-Hellman Group (DH Group)	Yes, Group 14	

(After HKEX received user input, we would set up customer gateway in AWS, public IP for tunnels will then be generate from that user in a configuration file(.txt))

SECURED NETWORKS/HOSTS	
HKEX NETWORK / HOSTS / TARGET VPC	CUSTOMER NETWORK / HOSTS / Device Subnet <sup>14</sup>
CIDR Block (Default: 10.2.0.0/22)	

CLIENT INFORMATION		
Company Name: ..... Fill in by Business partner.....		
Customer Contact Name: Primary contact - Secondary contact -	Phone:	Email
Customer Support Contact :	Phone:	Email:
Additional comments:		

Field	Description	Supported Values
Security Assoc. Lifetime (min)		15 and 60 minutes, must be < Phase 1 Lifetime
Encryption Algo. / Authentication Algo.		AES128, AES256, AES128-GCM-16, AES256-GCM-16
HMAC / Hash Algo. / Integrity Algos.		SHA1, SHA2-256, SHA2-384, SHA2-512
DH Group		2, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24
Field	Description	Supported Values
Customer Network	Network subnet in CIDR format. This subnet must not overlap with each other customer and HKEX. It will be reviewed by HKEX.	

**HKEX will set up a customer gateway and site-to-site VPN connection in AWS based on the information provided in the form, then return an updated form with a public IP and a HKEX network subnet.**

**The necessary setup information, including the configuration commands generated for your firm, will be provided in a configuration file.**

## 3b

# VPN Setup

## Connection (1/4)

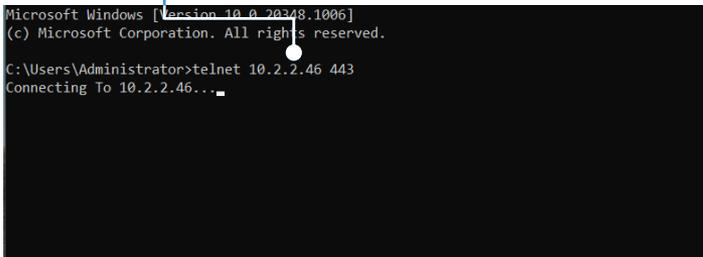
After completing the setup, the following steps should be taken for connecting to the target host:

### 1 Connect Target Host

Use a cli command to connect to the specific IP addresses / ports below are accessible (e.g. telnet for Windows CMD)

```
>telnet 10.2.2.42 443
```

```
>telnet 10.2.2.46 443
```



```
Microsoft Windows [Version 10.0.20348.1006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>telnet 10.2.2.46 443
Connecting To 10.2.2.46...
```

Blank screen indicates success



**NOTE:** the first command used to set up the connectivity may prompt an unsuccessful response, but the subsequent commands should then return the blank screen (above right) to indicate successful connectivity.



## 2 Connect Target Host

The following IP addresses should be added to the **HOSTS** table or **DNS**

```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host
#
# localhost name resolution is handled within DNS itself.
# 127.0.0.1 localhost
# ::1 localhost
10.2.2.46 connect.u4cp.hkex.com.hk
10.2.2.46 connect-am.u4cp.hkex.com.hk
10.2.2.46 connect-idm.u4cp.hkex.com.hk
10.2.2.42 fini.u4cp.hkex.com.hk
```

10.2.2.46 connect.u4cp.hkex.com.hk  
10.2.2.46 connect-am.u4cp.hkex.com.hk  
10.2.2.46 connect-idm.u4cp.hkex.com.hk  
10.2.2.42 fini.u4cp.hkex.com.hk



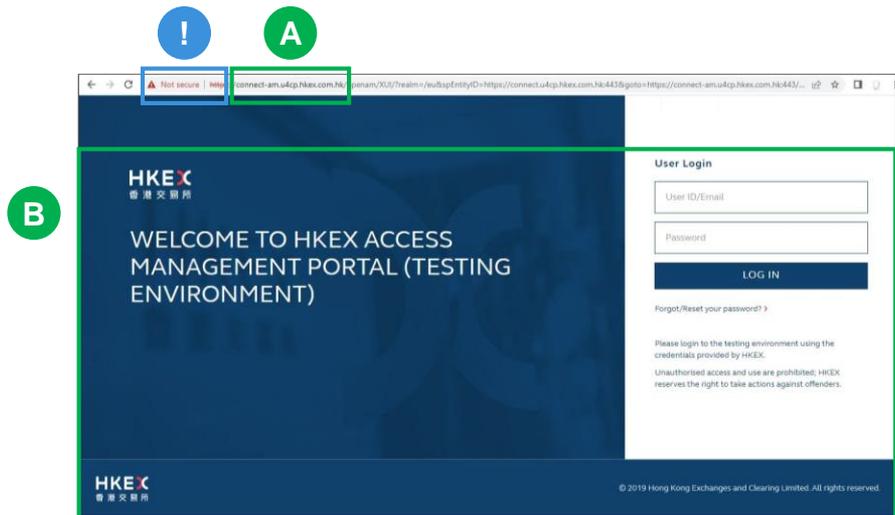
## 3b

# VPN Setup

## Connection (3/4)

The setup should now be completed, and the following verification tests should be conducted:

### 3 Test FINI Platform (user interface)



**A** Use any web browser and connect to:  
<https://connect.u4cp.hkex.com.hk>

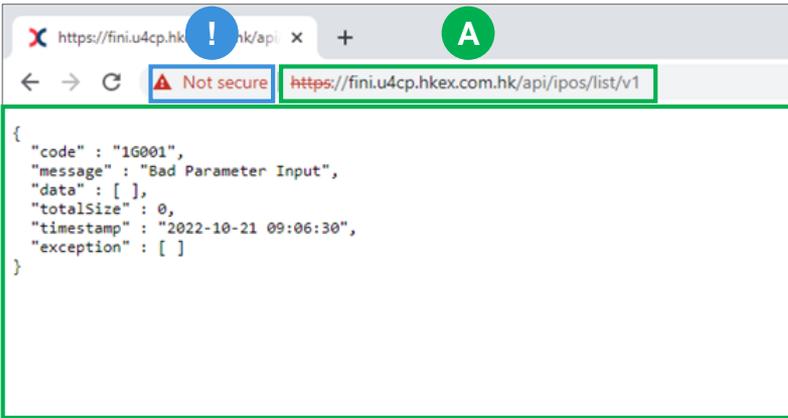
**B** Successfully loaded webpage indicates  
successful VPN connectivity

**!** At your firm's request, an extra certificate can be  
provided for importing into the local browser for  
a secure TLS/SSL connection

## 3b VPN Setup

### Connection (4/4)

#### 4 Test FINI Platform (API)



The screenshot shows a web browser window with the address bar displaying `https://fini.u4cp.hkex.com.hk/api/ipos/list/v1`. A red warning icon and the text "Not secure" are visible in the address bar. The main content area displays a JSON error response:

```
{
  "code" : "1G001",
  "message" : "Bad Parameter Input",
  "data" : [ ],
  "totalSize" : 0,
  "timestamp" : "2022-10-21 09:06:30",
  "exception" : [ ]
}
```

**A** Use any web browser and connect to:  
<https://fini.u4cp.hkex.com.hk/api/ipos/list/v1>

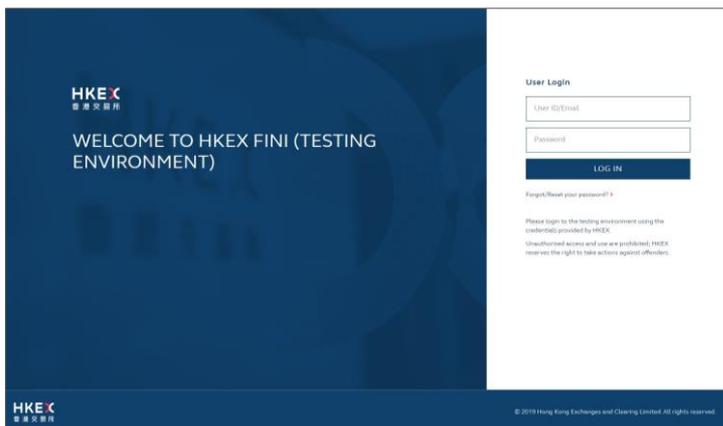
**B** Successfully loaded webpage indicates  
successful VPN connectivity

**!** At your firm's request, an extra certificate can be  
provided for importing into the local browser for  
a secure TLS/SSL connection

# 4

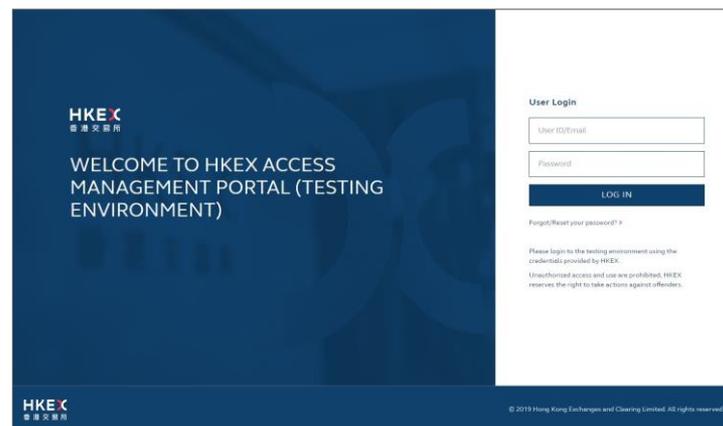
## Test Site Access

Once the VPN setup has been completed, your firm's business users may start accessing the FINI and HKEX Access Management test sites:



<https://fini.u4cp.hkex.com.hk>

(available in February 2023)



<https://connect.u4cp.hkex.com.hk>

## 4

# Test Site Access

## HKEX will provide your firm's test site user credentials by email:

Dear [redacted], —● Name of your firm's business user

A new Client VPN account for accessing the FINI External User Testing (EUT) environment has been created for you on Amazon Web Services (AWS). Please follow the steps below:

- Navigate to: <https://self-service.clientvpn.amazonaws.com/endpoints/cvpn-endpoint-0afaf12be05c7c186>
- Log in with your **Username, Password** and MFA Static Challenge

Your assigned **Username** is [redacted]. Note the **Password** and QR code for setting up the MFA Static Challenge will be sent to you via separate emails.

↓  
● **VPN username**

Once you have VPN connection established, you may access the HKEX Access Management Portal (Testing Environment) (<https://connect.u4cp.hkex.com.hk>) using the following credentials.

You will need to use the Delegated Administrators below to setup the API profiles (if you will test FINI API). The Business Users will be used for accessing FINI application. The URL will be provided (and hyperlink will be added on the HKEX Access Management Portal (Testing Environment)) in Feb-2023.

- Delegated Administrator (Maker)
  - Login ID : [redacted] ●
  - Password : [redacted] ●
- Delegated Administrator (Checker)
  - Login ID : [redacted] ●
  - Password : [redacted] ●
- Business User (Maker)
  - Login ID : [redacted] ●
  - Password : [redacted] ●
- Business User (Checker)
  - Login ID : [redacted] ●
  - Password : [redacted] ●

If you have any issues connecting to your Client VPN, please contact us by responding to this email or calling us at +852 2211 5888.

User Login

User ID/Email

Password

LOG IN

- Input **Login ID** here
- Input **Password** here

ForgeRock Authenticator (OATH)

REGISTER DEVICE

SKIP THIS STEP

Note: this message will appear during a user's first login.

Since Multi-Factor Authentication (MFA) is not required for the test sites, please select **SKIP THIS STEP**.



# 5

## Support

**Operating Hours: 09:00 to 18:00, Mondays to Fridays (excluding Public Holidays)**

- HKEX warmly welcomes market participants to reach out for any enquiries



+852 2211 5888



[projectfini@hkex.com.hk](mailto:projectfini@hkex.com.hk)

## A

# Appendix: List of Supported Gateway Devices

Vendor	Platform	Software
Checkpoint	Gaia	R80.10+
Cisco Meraki	MX Series	15.12+ (WebUI)
Cisco Systems, Inc.	ASA 5500 Series	ASA 9.7+ VT1
Cisco Systems, Inc.	CSRv AMI	IOS 12.4+
Fortinet	Fortigate 40+ Series	FortiOS 6.4.4+ (GUI)
Juniper Networks, Inc.	J-Series Routers	JunOS 9.5+
Juniper Networks, Inc.	SRX Routers	JunOS 11.0+
Mikrotik	RouterOS	6.44.3
Palo Alto Networks	PA Series	PANOS 7.0+
SonicWall	NSA, TZ	OS 6.5
Sophos	Sophos Firewall	v19+
Strongswan	Ubuntu 16.04	Strongswan 5.5.1+
Yamaha	RTX Routers	Rev.10.01.16+



Please refer the list here for the latest list: <https://docs.aws.amazon.com/vpn/latest/s2svpn/your-cgw.html#CGRequirement>