

# Connect to CUHK SSL VPN on iOS platform

*(This user guide uses iOS 13 as illustration.)*

## Table of Contents

A. Get Started .....	1
B. Install SSL VPN client - Aruba Virtual Intranet Access (ArubaVIA) .....	2
C. Set up CUHK SSL VPN Profile .....	2
D. Connect to CUHK SSL VPN .....	3
E. Disconnect from CUHK SSL VPN .....	5

For enquiries, please contact ITSC

- Hotline: 3943 8845 (during office hours)
- Online Service Desk: <http://servicedesk.itsc.cuhk.edu.hk> > **Get help** > **General Enquiries**

## A. Get Started

Secure Sockets Layer Virtual Private Network (**SSL VPN**) provides CUHK staff with a secure remote access to on-campus resources over an Internet connection. Once connected, all traffic for accessing on-campus resources go through the VPN tunnel. The rest traffic goes through your original Internet connection.

### Prerequisites:

- **Aruba Virtual Intranet Access (Aruba VIA)**, as SSL VPN client, installed on your iOS device.

### Maximum Connection Time Per Session:

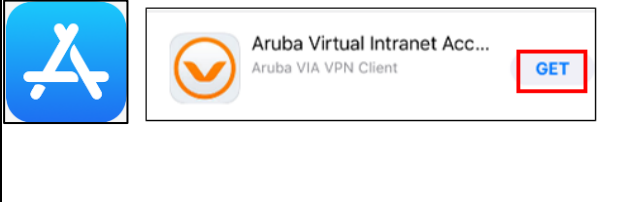
- 12 hours with 1-hour idle time out, you can make the connection again when the session expires.

### Known Issue:

- You may experience an unstable VPN connection from mainland China with the gradual upgrade of China's Great Firewall.
- For MacOS / iOS / iPadOS: With the network policy in Mainland China, you may not able to download the SSL VPN client (Aruba VIA) from Apple App Store. Please download the app before you go to the mainland. You can then connect to SSL VPN in the mainland.

## B. Install SSL VPN client - Aruba Virtual Intranet Access (ArubaVIA)

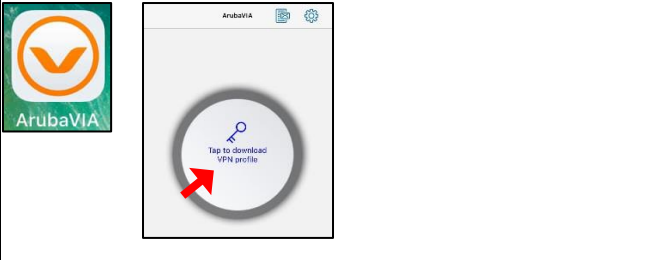
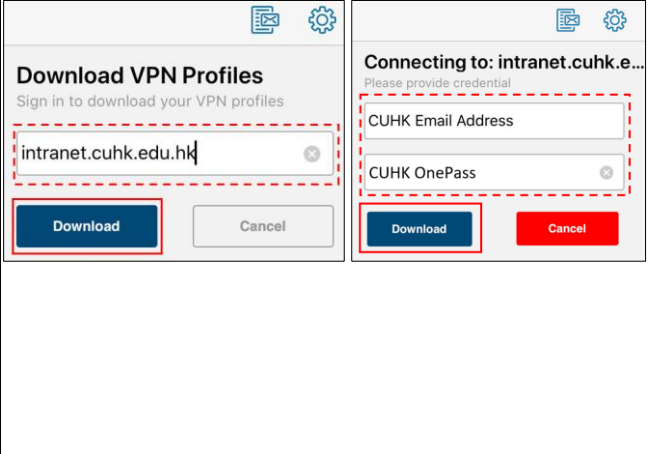
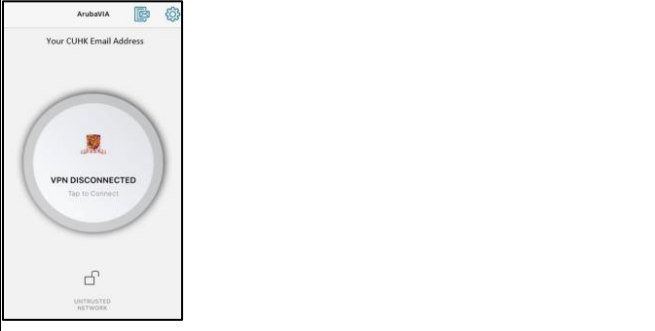
Aruba Virtual Intranet Access (ArubaVIA) is used as SSL VPN client. You can download it direct from App Store.

<p>1. Open <b>App Store</b>. Search and Install <b>Aruba Virtual Intranet Access</b>.  <b>Tip:</b> Please ensure you install <b>Aruba Virtual Intranet Access</b>, <u>NOT Aruba Networks VIA</u>.</p>	
---	--

## C. Set up CUHK SSL VPN Profile

Note: Before setting up ArubaVIA client for SSL VPN service, please ensure that

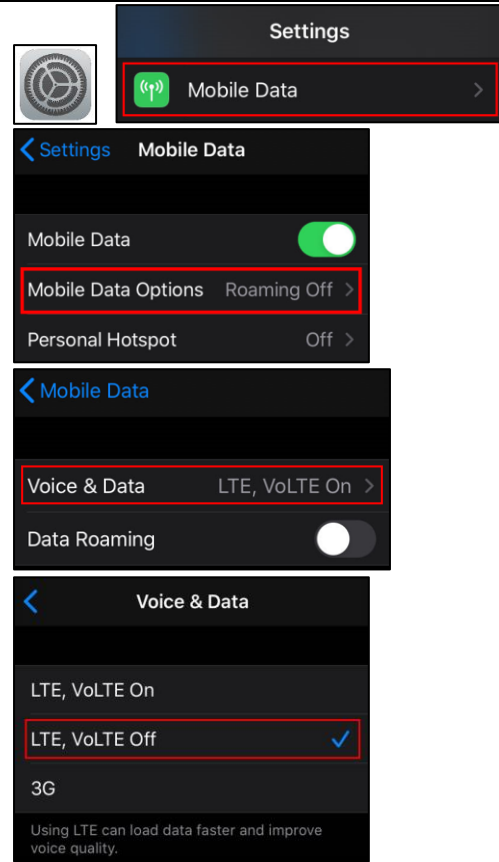
- (1) DUO Two Factor Authentication (2FA) has been enabled on your account.
- (2) DUO Mobile has been properly installed on your mobile device.

<p>1. Open <b>ArubaVIA</b> &gt; Tap to download VPN profile</p>	
<p>2. Enter</p> <ul style="list-style-type: none"> <li>• VPN Server URL: <i>intranet.cuhk.edu.hk</i></li> </ul> <p>Tap <b>Download</b>.</p> <p>Enter below to Download VPN Profiles</p> <ul style="list-style-type: none"> <li>• Username: <i>CUHK email address</i> (e.g. Student: <a href="mailto:student_id@link.cuhk.edu.hk">student_id@link.cuhk.edu.hk</a> Staff: <a href="mailto:alias@cuhk.edu.hk">alias@cuhk.edu.hk</a>)</li> <li>• Password: <i>CUHK OnePass</i></li> </ul> <p>Tap <b>Download</b>.</p>	
<p>3. Your SSL VPN profile setup is completed.</p>	

**D. Connect to CUHK SSL VPN**

**NOTE:** There's a known issue with SSL VPN connection in iOS 13. If you are using iOS 13, please disable VoLTE as below.

- i. Tab **Setting > Mobile Data**
- ii. Tab **Mobile Data Options > Voice & Data**
- iii. Tab **LTE, VoLTE Off**



1. Open **ArubaVIA** , VPN DISCONNECTED will then be prompted.

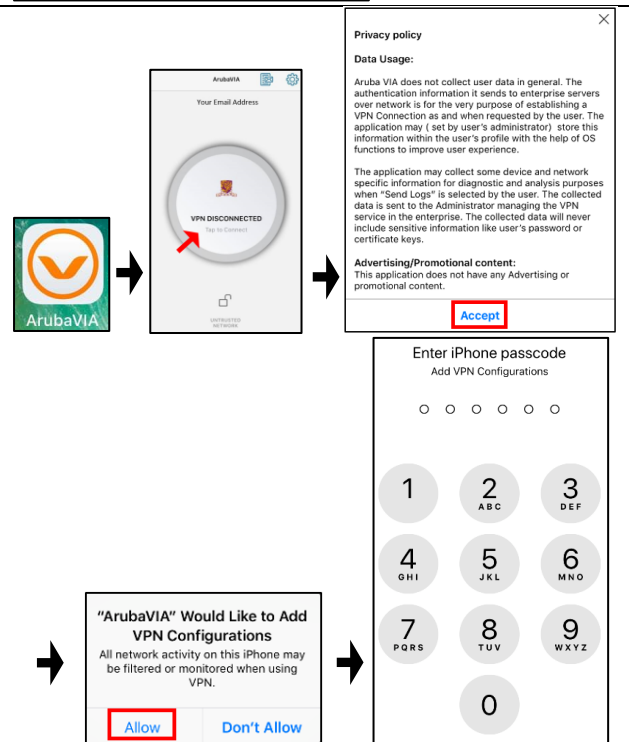
**Tap to Connect** to establish SSL VPN connection.

Then input either one of the following forms of password (2A, 2B or 2C), follow the format exactly the same as shown:

**Note:** The Privacy policy will prompt for your first connection.

To continue, you must agree to the Privacy policy and allow ArubaVIA to add VPN configurations on your device.

If you do, tap **Accept > Allow > Enter your iPhone passcode** to complete the set up.



2A. Password (Duo Mobile App – Push)

Login with

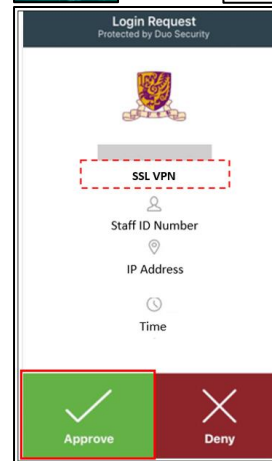
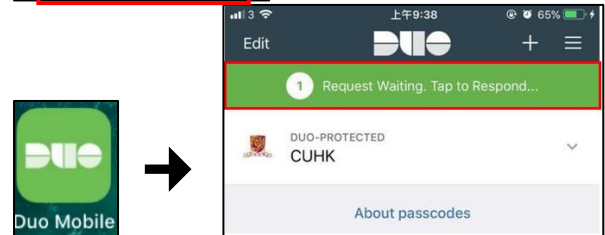
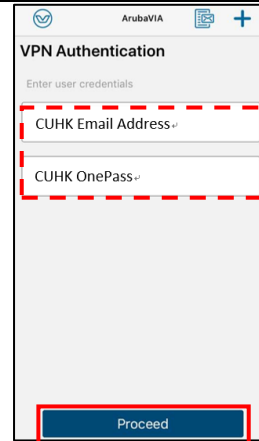
- **CUHK Email Address**  
(e.g. Student: [student\\_id@link.cuhk.edu.hk](mailto:student_id@link.cuhk.edu.hk)  
Staff: [alias@cuhk.edu.hk](mailto:alias@cuhk.edu.hk))
- **CUHK OnePass**

Tap **Proceed** to connect.

Open the **DUO Mobile App** on your mobile device, then **tap on the notification message**, a Login Request with the information of requesting source is displayed.

Tap **Approve**, the VPN connection should be established successfully.

Reminder: Duo Push is not available offline. Please ensure you got a good Internet connection when using this method. Or, you switch to log in with passcode which does not required an Internet connection.



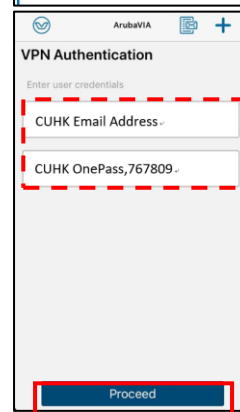
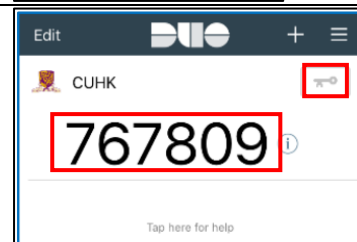
2B. password, passcode (Duo Mobile App – Generate Codes)

You can get the passcode from your DUO Mobile App. Open the **DUO Mobile App** on your mobile device, then **tap on the key icon** next to your account, a one-time passcode is generated.

Login with

- **CUHK Email Address**  
(i.e. Student: [student\\_id@link.cuhk.edu.hk](mailto:student_id@link.cuhk.edu.hk)  
Staff: [alias@cuhk.edu.hk](mailto:alias@cuhk.edu.hk))
- **CUHK OnePass, Passcode**

Tap **Proceed**, the VPN connection should be established successfully.



2C. password, bypasscode (Use a temporary Duo Bypass Code)

In case you have problem with your mobile (e.g. forgot to bring, malfunction, lost or stolen) and cannot provide the 2<sup>nd</sup> factor for VPN connection, you can generate a temporary DUO Bypass Code by yourself via DUO Self-Service Portal at <https://duo.itsc.cuhk.edu.hk>.

Login with

- **CUHK Email Address**  
(i.e. Student: [student\\_id@link.cuhk.edu.hk](mailto:student_id@link.cuhk.edu.hk)  
Staff: [alias@cuhk.edu.hk](mailto:alias@cuhk.edu.hk))
- **CUHK OnePass, Bypasscode**

Tap Proceed.

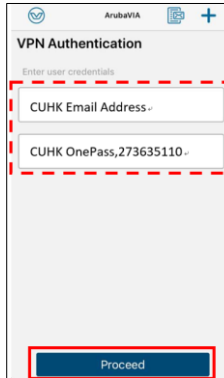
The VPN connection should be established successfully.

**Bypass 2FA**

**Done.**

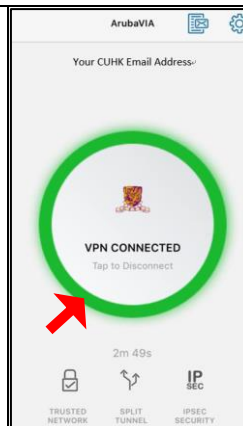
Please find your bypass code below, that will work for 20 times or expires on Thursday, 22 March, 2018 4:46 AM, whichever occurs first.

**Bypass Code** 273635110  
**Expires** Thursday, 22 March, 2018 4:46 AM  
**Remaining Uses** 20 times



**E. Disconnect from CUHK SSL VPN**

1. Open **ArubaVIA**
2. When **VPN CONNECTED** is shown, tap **TAP TO DISCONNECT** to terminate the current SSL VPN connection.



**Prepared by:** User Support Services, Information Technology Services Centre

**Last Update:** 5 February 2021

Copyright © 2021. All Rights Reserved. Information Technology Services Centre, The Chinese University of Hong Kong