<table>
<thead>
<tr>
<th>Version</th>
<th>Update Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Feb 2018</td>
<td>Initial version</td>
</tr>
<tr>
<td>1.1</td>
<td>Jul 2020</td>
<td>Added Duo mobile app installation steps, under Section 2.1, for Android devices which can’t connect to Google Play Store</td>
</tr>
<tr>
<td>2.1</td>
<td>Oct 2020</td>
<td>Added Rescue Code generation in Section 2.2, and updated related screens</td>
</tr>
<tr>
<td>2.2</td>
<td>Dec 2022</td>
<td>Update the screens for Rescue Code generation and Duo mobile v4</td>
</tr>
<tr>
<td>3.0</td>
<td>Feb 2024</td>
<td>Update screen and steps for switching from Traditional Prompt to University Prompt in Device Management</td>
</tr>
</tbody>
</table>
Table of Contents

1. About DUO 2FA ................................................................. 4
   1.1. Duo 2FA integrated User Applications ......................... 4
   1.2. How It Works ............................................................... 4
2. Duo 2FA Enrollment ......................................................... 5
   2.1. User Enrollment, Mobile Device Registration ............... 5
   2.2. Rescue Code Generation ............................................ 12
3. Registered Device(s) Management .................................... 14
4. Use of Passcode and Duo Push ......................................... 17
1. About DUO 2FA

The traditional authentication method by just verifying the username and password is no more secure enough nowadays. In order to strengthen the protection of our account, two-factor authentication (2FA) is introduced. 2FA is an enhance authentication mechanism which requires user to provide any 2 of below factors for identity verification:

- Something you know: e.g. password
- Something you have: e.g. token, one-time passcode
- Something you are: e.g. fingerprint, voice

DUO 2FA is a two-factor authentication solution which requires users to provide the 2\textsuperscript{nd} factor, i.e. a Duo push response / one-time passcode, from a designated device (e.g. your mobile device) for identity verification when they login those 2FA integrated applications.

1.1. Duo 2FA integrated User Applications

The latest list of Duo 2FA Integrated User Applications can be found in Duo 2FA website (https://www.itsc.cuhk.edu.hk/all-it/information-security/two-factor-authentication-2fa/) > under Tab ‘2. Implementation Scope’.

1.2. How It Works

Steps:

You need to:

i. Enroll your O365 account and designated mobile device (e.g. your mobile phone, tablet) via the Duo 2FA Self-Service User Portal (https://duo.itsc.cuhk.edu.hk).

ii. Install DUO Mobile App on above enrolled mobile device for linking up your account and receiving DUO Push notification or generate the one-time passcode for your login request.

Afterwards, when you are logging in to those 2FA integrated applications, you will need to:

i. first login the application with your username and password;

ii. then provide the 2\textsuperscript{nd} factor (either one of below) to the application for authentication:

a. DUO Push response, it is the authorization response to the Duo Push notification which sent from the login request of the application to your DUO Mobile App; or

b. One-Time Passcode, it is generated from your DUO Mobile App for inputting to the application.

Once the above verification is passed, your access to the application is granted.
2. Duo 2FA Enrollment

2.1. User Enrollment, Mobile Device Registration

Before you can use the 2FA to login those 2FA integrated applications, you need to **enroll your account & register a designated mobile device** via DUO 2FA Self-Service User Portal, and **install the DUO Mobile App** on your designated mobile device for one-time passcode generation or Duo Push authorization.

**Steps:**

i. Open a web browser, visit Duo 2FA Self-Service User Portal at [https://duo.itsc.cuhk.edu.hk](https://duo.itsc.cuhk.edu.hk).

ii. Login with the account that is going to enroll Duo 2FA, i.e. your O365 staff/student/project account (@cuhk.edu.hk or @link.cuhk.edu.hk).

After login, **read** the on-screen information carefully. Then click **START SETUP**.
iii. Then, you will be redirected to a webpage hosted by DUO at “*.duosecurity.com/” for the enrollment process. Click ‘Next’.

iv. Click ‘Next’.

v. By default, your mobile device will be used to receive and approve the Duo push notification or generate passcode for 2FA login. Click ‘Duo Mobile’.
vi. In this screen, you will be asked to provide the mobile phone number for Duo to send the passcode to you via SMS, or register your mobile device as a tablet.

In CUHK’s deployment, no SMS will be sent to user’s mobile phone and the phone number will not be used, so we highly recommend users to select ‘I have a Tablet’ even you are using a mobile phone.

vii. Follow the on-screen instruction to download the Duo Mobile app to your mobile device, then click ‘Next’.
If you are using iOS device:

- Open the App Store on your mobile, tap search and search ‘Duo Mobile’.
- Tap ‘Get’ and then ‘install’ to download and install the app.

If you are using Android device:

- Open the Google Play Store on your mobile, and search ‘Duo Mobile’.
- Then tap ‘install’ to download and install the app.

If you are using Android device bought in China, where Google Play Store is not available:

- Open the browser on your mobile, and download the Duo Mobile APK directly from official Duo website, details can be found at https://help.duo.com/s/article/2094?language=en_US. *Please do not download and install any untrusted APK files into your mobile since they may be altered by hackers for malicious purposes.
- After the file is downloaded, open Downloads, tap on the APK file, and tap ‘Yes’ when prompted or follow the onscreen instruction for installation, the app will begin installing on your device.
viii. After the mobile app is installed, back to your computer screen, a QR code to add your account to the Duo mobile app is generated.

Note: Please make sure to allow the Duo Mobile app to access the camera, otherwise, it would not be able to scan the activation code.

Open the ‘DUO Mobile’ app on your mobile device, then tap “Add +” icon on the top right hand corner, then select “Use QR code” and scan the QR code image appear on your screen.

Then, you should find your account is added to the Duo Mobile app.
ix. Click ‘Continue’.

![Image of Duo setup confirmation message]

x. The setup is completed, click ‘Log in with Duo’.

![Image of Duo setup completion screen]

xi. A Duo Push notification will be sent to your registered mobile device.

![Image of Duo push notification]

xii. Click ‘Approve’ to verify your authentication.
xii. Accept the Duo push notification on your mobile device if the login is triggered by you.

![Duo Security - Device Manager](image)

xiii. It’s Almost done, the following screen should be shown. Please **follow the steps in Section 2.2 for Rescue Code Generation**.
2.2. Rescue Code Generation

The Rescue Code provides a backup measure for you to generate a bypass code when emergency, i.e. when both your mobile device and CU Link Card are not available. User should generate a set of 5 rescue codes in advance when you can login Duo 2FA Self Service User Portal and keep them in a safe place but where you can find when emergency.

**Usage of Rescue Code:**
- the rescue code can ONLY be used to generate the bypass code;
- the rescue code CANNOT be used as the 2nd factor to login any 2FA integrated application; and
- each rescue code can only be used ONCE.

**Steps:**

i. The last step of the enrollment process is to generate the Rescue Code.

Read the on-screen information carefully, then click GET MY RESCUE CODES.

![Two Factor Authentication](image-url)
ii. A set of 5 Rescue Codes should be generated. You can save it or print it for keeping.

The enrollment process is finished. You can click the “ENROLL DEVICE” button on the top menu to manage your registered mobile device(s). More details can be found in Section 3.
3. Registered Device(s) Management

You can manage (view, add, or edit) the registered device(s) for Duo 2FA via the Duo 2FA Self-Service User Portal.

Steps:

i. Open a web browser, visit Duo 2FA Self-Service User Portal at https://duo.itsc.cuhk.edu.hk.

ii. Login your account, i.e. your O365 staff/student/project account (@cuhk.edu.hk or @link.cuhk.edu.hk).

After login, read the on-screen information carefully. Then tick ‘Okay, I am ready now.’ and click ‘GO TO ENROLL/MANAGE DEVICE’.
iii. You will be redirected to a webpage hosted by DUO at “*.duosecurity.com/” and a Duo push notification is sent to your registered mobile device for the 2FA authentication. **Ignore the Duo push notification and click ‘Other options’**.

![Duo Security Screen](image1)

iv. Then click “Manage devices”.

![Duo Security Screen](image2)
v. You need to verify your identity first. Select one of the options for identify verification.

vi. After your identity is verified, you can manage your device(s) for Duo 2FA. You can:
   a. Rename your registered device
      i. Click ‘Edit’, ‘Rename’, and then input a new name.
   b. Add a new device
      i. Click ‘I have a new phone’ if you need to register a new device with the same mobile number, or, click ‘Add a device’ if you need to register a new device with different mobile number or device type.
      ii. Then follow the steps in Section 2.1 for device registration.
   c. Delete an obsolete device
      i. Click ‘Edit’ and ‘Delete’.
4. Use of Passcode and Duo Push

Below demonstrates the use of the 2 authentication methods, i.e. Duo Push and Passcode, for logging in those DUO integrated applications.

Steps:

i. Take an example of logging in to the Duo 2FA-integrated web applications, e.g. O365, it will redirect to CUHK Central Authentication Login page.

ii. Input your CUHK account credential in the fields for
   a. Login ID, i.e. alias@cuhk.edu.hk / alias@link.cuhk.edu.hk
   b. OnePass Password, i.e. the 1st factor
      then click Sign in.

   ![CUHK Login Page](image)

iii. Then, you will be redirected to a webpage hosted by DUO at “*.duosecurity.com” for 2nd authentication, and you can continue using your last authentication method or select “Other options” to choose another authentication method.

   - **Duo Push**

   If you used Duo Push in last authentication, it will automatically send a Duo Push notification to your registered mobile device.

   ![Duo Push Notification](image)
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 to login the application.

a. Passcode

If you used Duo Passcode in last authentication, it will prompt you to enter a Duo passcode which can be generated from your Duo Mobile app.
Open the Duo Mobile App on your mobile device, then tap on your account, a one-time passcode is generated.

Input the passcode in the webpage, then click Verify button.
After you pass the authentication, it will show a “Trust This browser?” message. It is a remember device feature which allows you to skip Duo 2FA when you login any Duo-2FA integrated web application again within 12 hours with the same browser and device.

- Click "Yes, trust browser", only if you trust the browser from your own computer.
- Otherwise, click "No, do not trust browser" if you don't trust the browser, especially when using a public/shared/untrusted computer.

iii. A Success page will be shown once you are authenticated successfully.

And it should return to the application automatically.

- END –