Multi-Factor Authentication: OTP Manager Initial Setup Guide

This is a manual for installing and configuring OTP Manager on a Mac PC.

STEP.1 Install the OTP Manager Software

1 Install the OTP Manager software from the Mac App Store.



STEP.2 Initial Setup for Multi-Factor Authenticator

Web Browser

 Using a web browser to sign in to the Multi-Factor Authentication page (<u>https://aka.ms/mfasetup</u>) with your APU email address and password.

2 When the [More information required] box shows up, click [Next].



• When the [Start by getting the app] screen appears, click [<u>I want to use a different authentication</u> <u>app</u>] as this manual will set up the authentication method using OTP Manager.

Microsoft Authenticator				
	Start by getting the app			
	Or your phone, install the Microsoft Authenticator app. Download now er you install the Microsoft Authenticator app on your device, choose "Next".			
	I want to use a different authenticator app			
	Cancel Next			

4 On the [Set up your account] screen, click [Next].



⑤ On the [Scan the QR code] screen click [Can't scan image?].



6 Your [Account name] and [Secret key] will be displayed, so copy the [Secret key].





③ Enter the following information on the [Add New Token] screen of OTP Manager and click [Add Token].

Issuer: APU

Username: APU email address

Secret: Secret key of 6

	The second secon	ger - Local ^T oken		+ 幸
OTP Manager	Add New	Token	Drop Import Files	
↔ Import & Export		You	are adding Tokens to the Local Keychain	
More	Issuer:	APU		0
E About	Username:	An r ∎ ⊉apu.ac.jp		
₽? FAQ	Secret:	scription (Sector)		
 Changelog 				
Send Feedback		Advanced Settings >		
③ Support us		Clear		Add Token
🛛 Legal				

9 Make sure that a 6-digit number is displayed on the OTP Manager screen.



Web Browser

Oclick [Next] on the [Scan the QR code] screen in your web browser.



① On the [Enter Code] screen, enter the six-digit number ② and click [Next].

Authenticator app			
xxx xxx	Enter code Enter the 6-digit code shown in the Authenticator app.		
	Enter code		
<u> </u>		Back	Next

Dick [Done] on the [Success!] screen.



(B) Once you have confirmed that [Authenticator app] has been added to the [Security info] screen, the setup is complete. Please close OTP Manager and your web browser.

	My Sign-Ins \vee				
A Overview	Security info These are the methods you use to sign into your account or reset your password.				
Devices	Default sign-in method: Authenticator app or hardware token - code				
ୠ Password	+ Add sign-in method				
🖻 Organizations	Password ① Last updated: Ch.	ange			
A Settings & Privacy	Authenticator app Time-based one-time password (TOTP)				
🕚 Recent activity	Lost device? Sign out everywhere				

STEP.3 How to sign in after initial settings

After completing STEP.2, you will be able to use the service starting the next day. If you need to sign in via MFA again, please follow the steps below.

Multi-Factor Authentication is required when signing in from an off-campus network such as at home, a public Wi-Fi network, or a mobile phone network.



Web Browser

2 Enter your APU email address and password on the university's authentication screen, and click [Sign in].

3 Once [Enter code] is displayed in your web browser, enter the 6-digit number displayed in OTP Manager, then click [Verify].



You can remember Multi-Factor Authentication information as follows.

- Web browser: 90 days if you check [Don't ask again for 90 days] when signing in.
- · Desktop application: One-time authentication for a long period of time regardless of the above
- *Some desktop applications behave the same as web browsers