

What is Multi-factor Authentication (MFA)?

Multi-factor Authentication (MFA) is an authentication method that requires user to provide multiple forms of verification to prove your identity when signing into an application. IITS will be introducing MFA for SMU IT services progressively as part of the security enhancement efforts to safeguard the SMU community.

How to Register MFA

1. Please click on the link "<https://aka.ms/mfasetup>".
2. Key in your SMU email address to sign-in.

****NOTE**** If the following message "Approve sign-in request" displayed on your browser, this mean you had previously setup Azure MFA, therefore **no further action required** from you for registration.



3. Upon successful login, you will see the page below. Follow the on-screen instruction to select any **one preferred verification option**. This is for you to decide how you like to be notified for authentication before accessing to the SMU services with MFA enabled, e.g. through App in your mobile phone; receive text message or call for one-time password (OTP) on your phone.

Additional security verification

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password. [View video to know how to secure your account](#)

what's your preferred option?
We'll use this verification option by default.

Notify me through app ▼

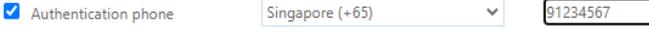
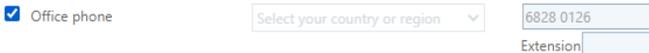
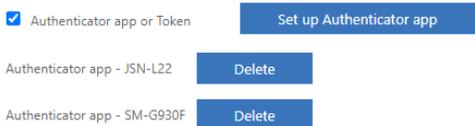
There are 5 options to choose from. You may select one default (primary) verification here

how would you like to respond?
Set up one or more of these options. [Learn more](#)

<input checked="" type="checkbox"/> Authentication phone	Singapore (+65) ▼	<input type="text" value=""/>	<input type="text" value=""/>
<input type="checkbox"/> Office phone	Singapore (+65) ▼	<input type="text" value=""/>	<input type="text" value=""/>
		Extension	<input type="text" value=""/>
<input type="checkbox"/> Alternative authentication phone	Select your country or region ▼	<input type="text" value=""/>	
<input checked="" type="checkbox"/> Authenticator app or Token	Set up Authenticator app		
Authenticator app - SM-G965F	Delete		

This option will guide you to setup Authenticator app on your android/iOS.

4.1 Breakdown of each option's configuration

Option	How authentication is done	What you will need to do to set this up
Call my authentication phone	Your mobile phone will ring and upon picking up, press “#” to approve the login.	Select the option, select country code and key in your mobile number under “Authentication phone” 
Text code to my authentication phone	An SMS will be sent to your mobile phone. Key in the code to approve the login.	Select the option, select country code and key in your mobile number under “Authentication phone” 
Call my office phone	Your office phone will ring and upon picking up, press “#” to approve the login.	Select the option. Your office number will be updated by the administrator. Please contact Help Centre if the number is not correct. 
Notify me through app	Your Wi-Fi or data must be switched on. Click on “Approve” when prompted	Select the option, download “Microsoft Authenticator” app on to your smart phone, and setup up the Authenticator app. Your phone model will appear in the list once setup is completed. 
Use verification code from app or token	Tap on “Microsoft Authenticator” app in your mobile phone, select “Singapore Management University”, read the code and key in to authenticate.	Select the option, download “Microsoft Authenticator” app on to your smart phone, and setup up the Authenticator app. Your phone model will appear in the list once setup is completed. 

4. Click on Save and close after selecting your desired verification options.