

Introduction

Griffith has introduced MFA to ensure the security of your information by adding an additional layer of authentication to your Single Sign-On. PingID is the MFA tool used by Griffith. This guide shows how to setup MFA using a third-party Authenticator App such as Google, Microsoft, LastPass or Authy Authenticator

Step 1 Select and install a third-party Authenticator App of your choice

Select the Authenticator App of your choice – from the Apple App Store or Android Play Store, search for **Authenticator** and you will find several applications which you can choose from including Google, Microsoft, LastPass and Authy Authenticators. For these instructions we will use Google Authenticator, all setups are very similar.

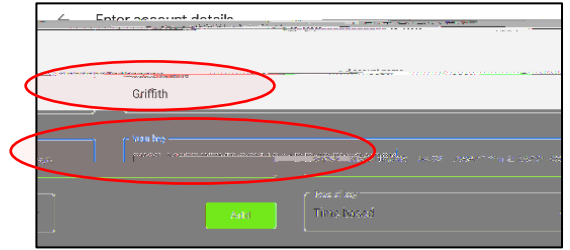
Select the App, click **Install** and **Open**.

Select **Enter a setup key**.

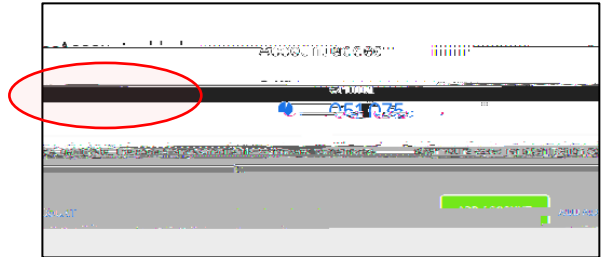
In

Select **Start** at the **Welcome to Multi**

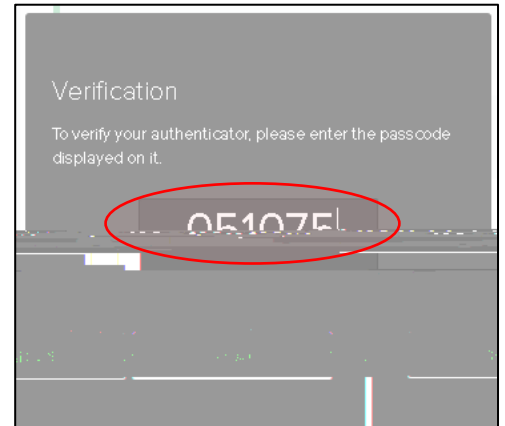
- 8 In the Google App, enter **Griffith** in the Account Name, then paste the Manual Pairing key into **Your Key** field and select **Add**.



- 9 Google App will present a 6-digit code, copy this code.



- 10 Enter the 6-digit code you copied from the Authenticator Verification Windows and select **Next**. Setup is completed.



Your Griffith MFA is now synced to your Google Authenticator or the third-party Authenticator App that you selected.

To use the App you will need to open it each time you wish to authenticate, and copy the code into the MFA screen after SSO login each time.



For more information contact:

Digital Solutions Corporate Services

Phone 07 3205 5555 or email griffith@griffith.edu.au

Email

