Multi-Factor Authentication for Login

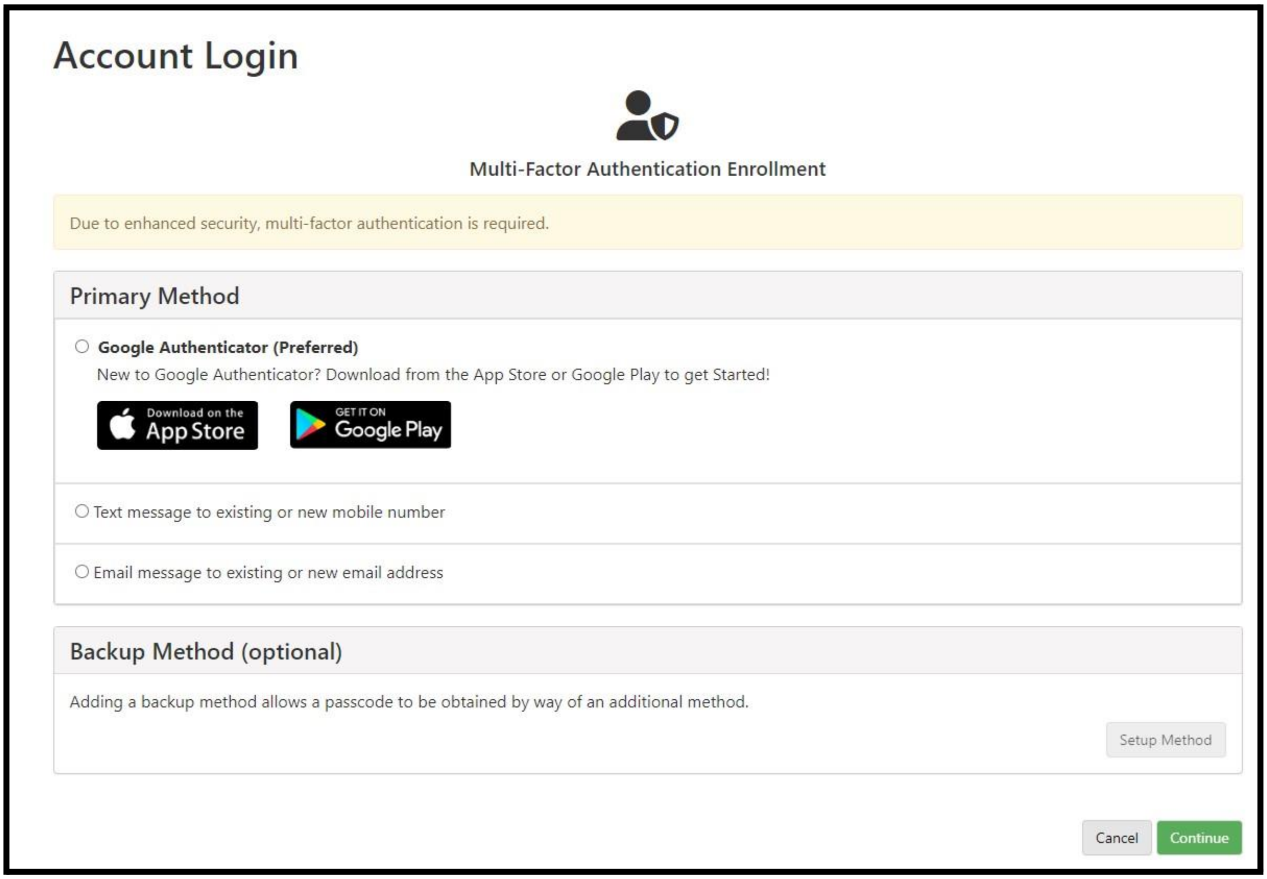
Step One: Creating a Multi-Factor Authentication profile to receive codes to login

With Multi-Factor Authentication (MFA) enabled, you will be required to create a MFA profile at your next login.

Authorized Users: once your username and password are entered, you will be directed to a page to select from the options below.

Students: you will be directed to the page after logging into your Towson Online Services Student Dashboard.

A. Authenticator Application - This is the most secure option and the preferred method to use. Examples are Google Authenticator and Microsoft Authenticator. These apps can be downloaded from the Apple App Store or Google Play.
B. Text Message - A mobile phone number will be entered to receive passcodes to login.
C. Email address - An email address will be entered to receive passcodes to login.



Account Login

Multi-Factor Authentication Enrollment

Due to enhanced security, multi-factor authentication is required.

Primary Method

○ **Google Authenticator (Preferred)**
New to Google Authenticator? Download from the App Store or Google Play to get Started!

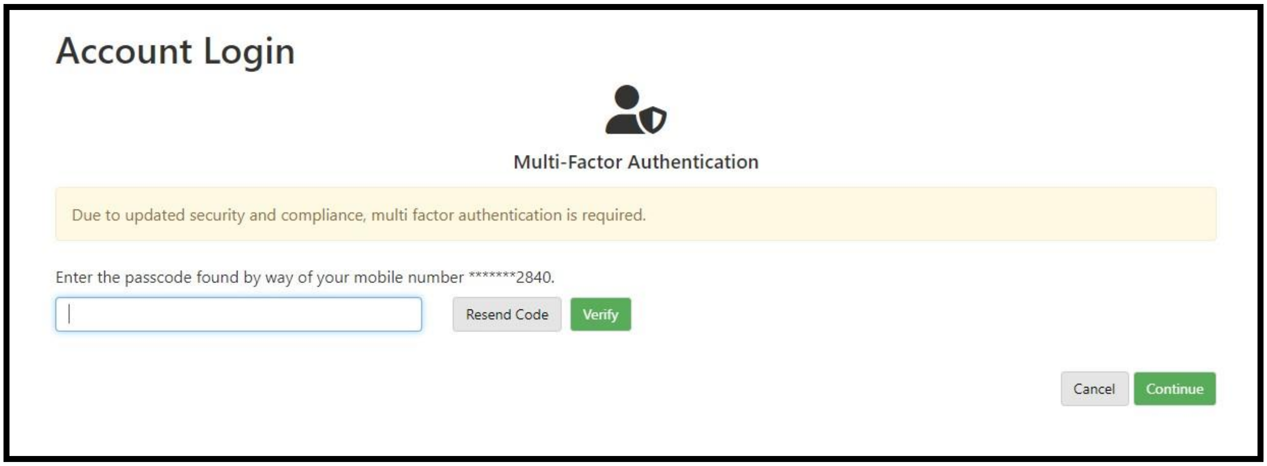
○ Text message to existing or new mobile number

○ Email message to existing or new email address

Backup Method (optional)

Adding a backup method allows a passcode to be obtained by way of an additional method.

Step Two: Enter the passcode and select verify



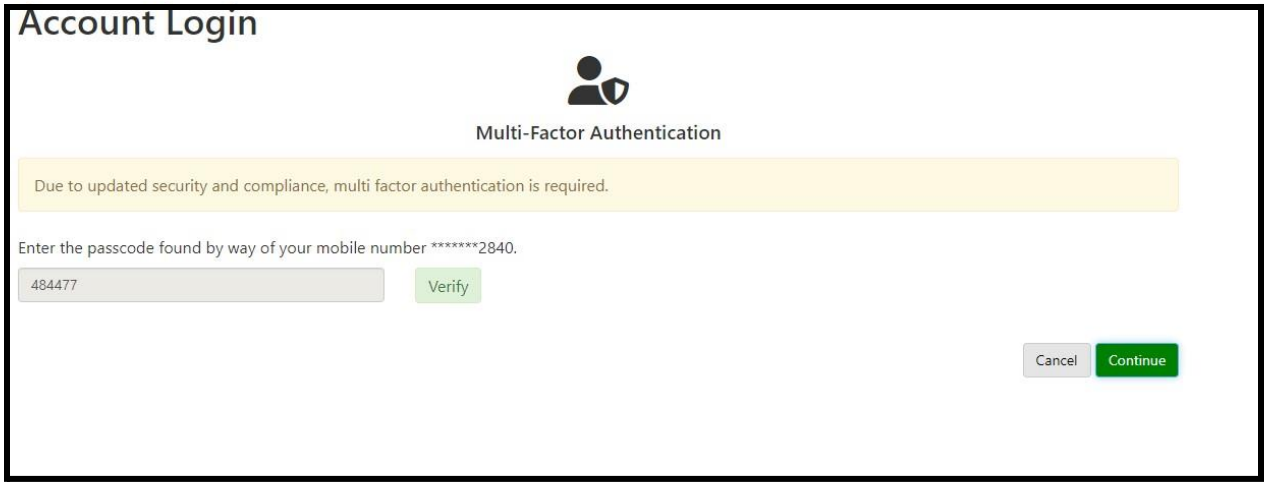
Account Login

Multi-Factor Authentication

Due to updated security and compliance, multi factor authentication is required.

Enter the passcode found by way of your mobile number *******2840.

Step Three: When the passcode is verified, select continue to access your account



Account Login

Multi-Factor Authentication

Due to updated security and compliance, multi factor authentication is required.

Enter the passcode found by way of your mobile number *******2840.

484477