



BCC SINGLE SIGN-ON MULTI-FACTOR AUTHENTICATION (MFA) & PASSWORD RESET

INSTRUCTIONS

OVERVIEW

BCC has recently introduced Multi-Factor Authentication (MFA) to provide an extra layer of protection for students' information.

INSTRUCTION GUIDE TABLE OF CONTENTS

STEP 1: Log in Using Default Password.....	1
STEP 2: Enroll in MFA	
OPTION 1 – Email (Non-BCC Email Address).....	2
OPTION 2 – Mobile Authenticator.....	3
OPTION 3 – Open Authenticator.....	4
STEP 3: Create a new password.....	6

THANK YOU for supporting a secure and connected learning environment at Barstow Community College.

For additional assistance, please watch our instructional YouTube video:

<https://youtu.be/GeVsWr9OFgU?si=ZCvlbh6NXjtuNfnY>

STEP 1: LOG IN USING YOUR DEFAULT PASSWORD

As part of this rollout, everyone must undergo a password reset. This process works on any web browser or a CD-networked Windows computer. We've simplified the process by creating a default password format using personal details you already have on hand.

Default Password Format:

- Last 4 of B number
- First 2 letters of **first** name in *UPPERCASE*
- First 2 letters of **last** name in *lowercase*
- @ symbol
- **Day (dd)** of Birth

Example:

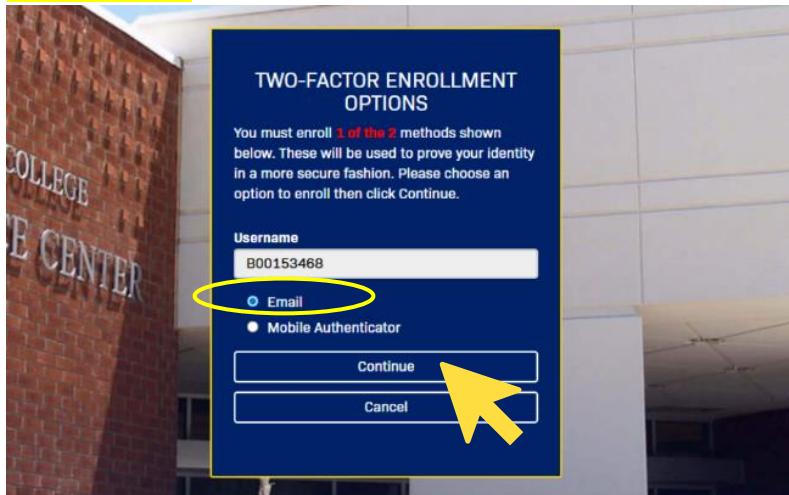
- Name: **Studious Viking**
- B number: B0040**4322**
- Birthday: June **21**, 1901

PASSWORD: 4322STvi@21



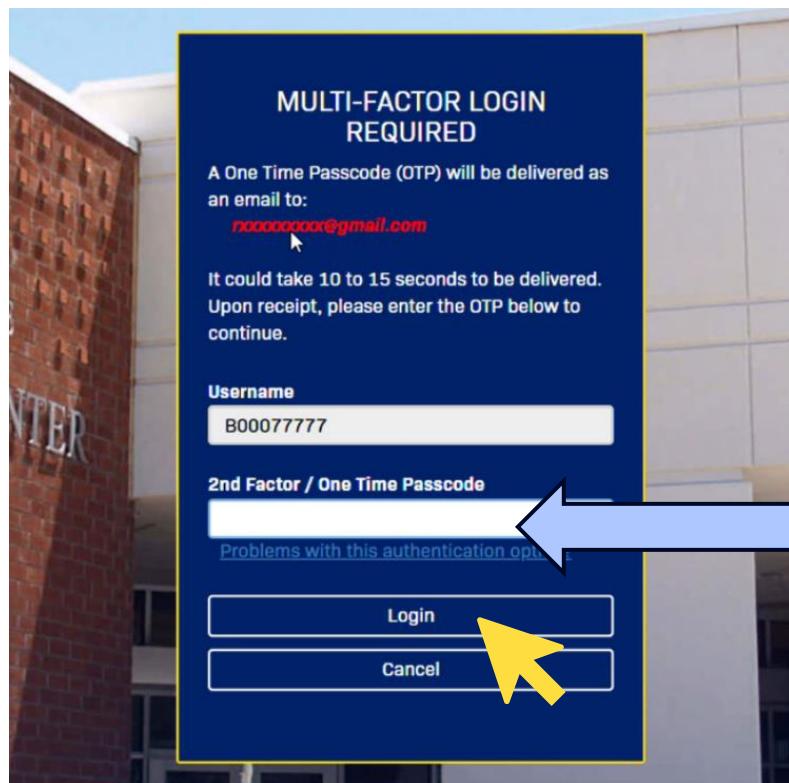
STEP 2: ENROLL IN MULTI-FACTOR AUTHENTICATION (MFA)

OPTION 1 – Email



You will be prompted to select an option.

To receive a One Time Passcode (OTP) **via a non-BCC email**, select 'Email' and press the 'Continue' button.



Once you enter a non-BCC email address, you will receive a code from My BCC or mybcc@bccd.onmicrosoft.com.

Enter the code you received in the 2nd Factor / One Time Passcode box and press the 'Login' button.

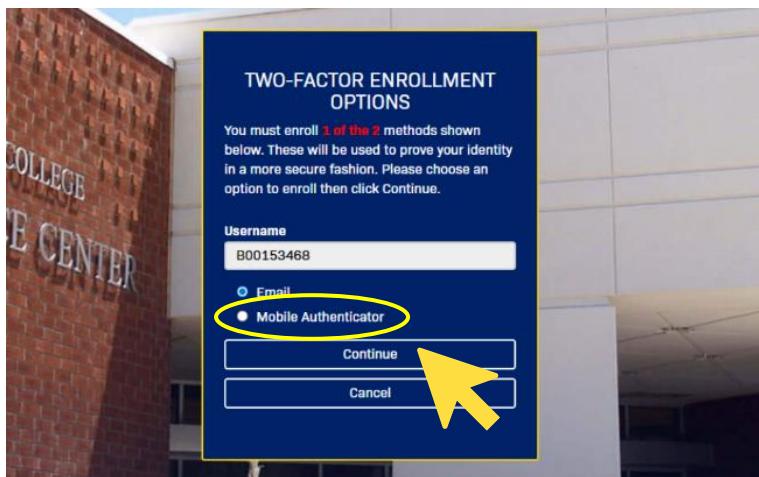


Successful enrollment!

STEP 2: ENROLL IN MULTI-FACTOR

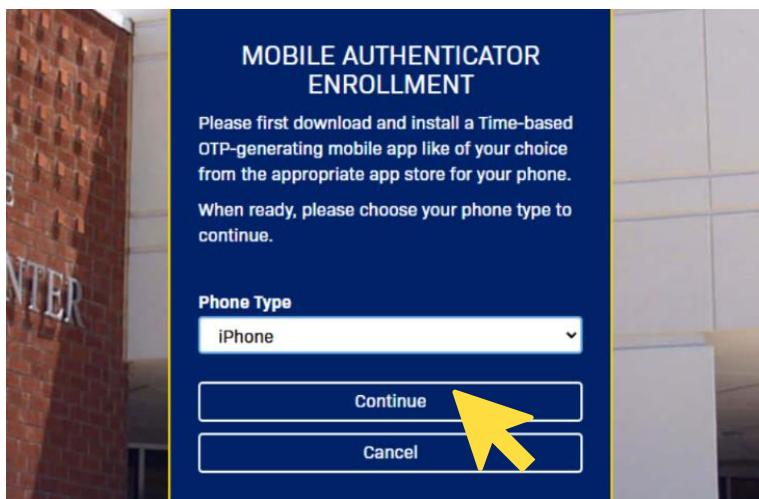
AUTHENTICATION (MFA)

OPTION 2 – Mobile Authenticator

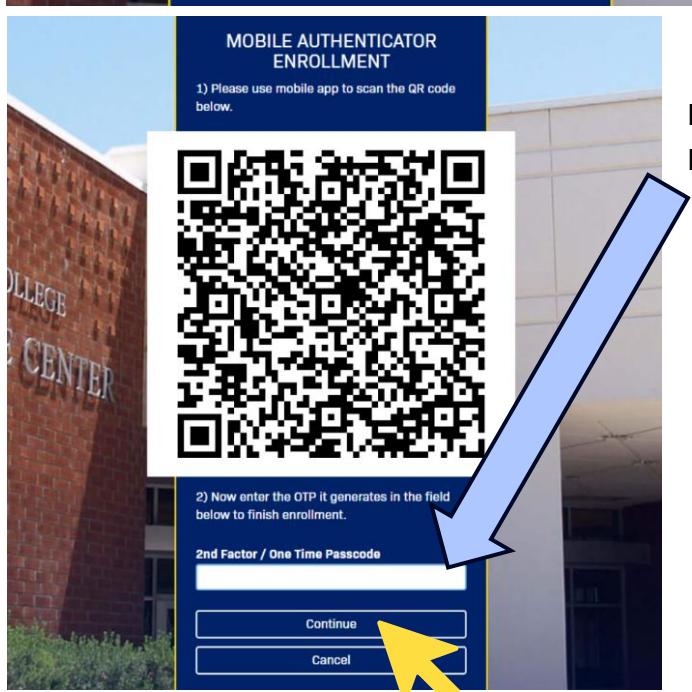


You will be prompted to select an option.

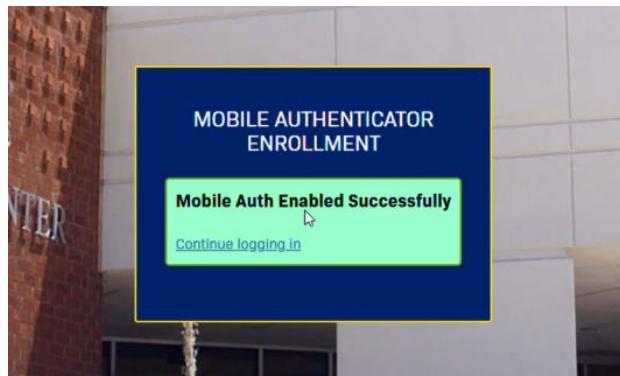
To receive a One Time Passcode (OTP) **via a Mobile Authenticator Application**, select 'Mobile Authenticator' and press the 'Continue' button.



Select a phone type (Android, iPhone, Windows) and press the 'Continue' button to generate a QR code to scan on your phone, and follow the instructions to complete enrollment.



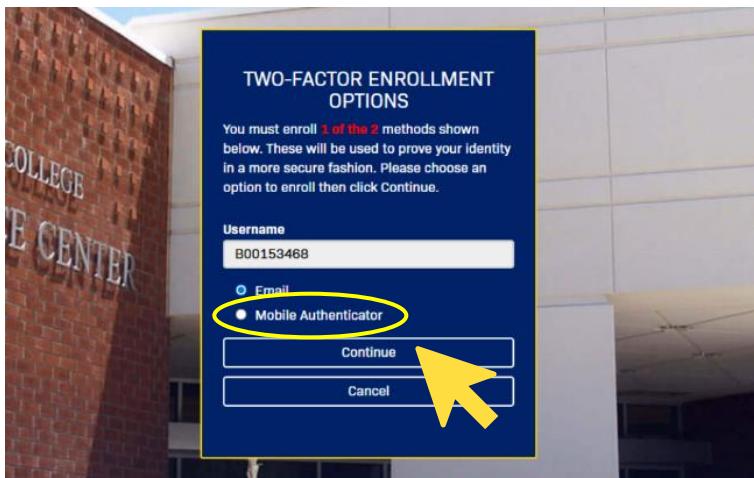
Enter the code you received in the 2nd Factor / One Time Passcode box and press the 'Continue' button.



Successful enrollment!

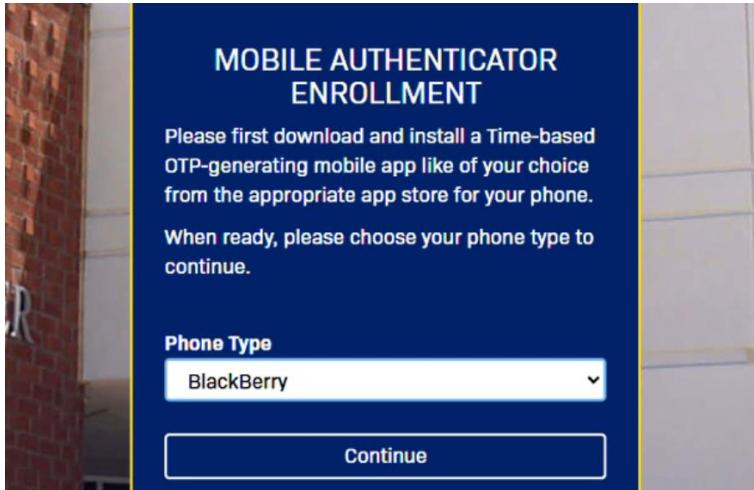
STEP 2: ENROLL IN MULTI-FACTOR AUTHENTICATION (MFA)

OPTION 3 – Open Authenticator (for those who prefer using a desktop computer app)



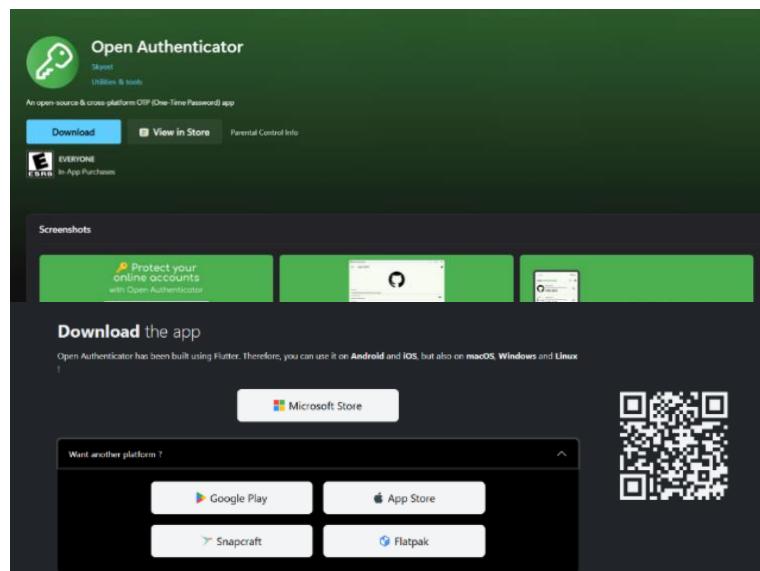
You will be prompted to select an option.

To receive a One Time Passcode (OTP) **via the Open Authenticator Application**, select 'Mobile Authenticator' and press the 'Continue' button.



For this option, select **Blackberry** as the phone type.

Download the free **Open Authenticator application** on your desktop using one of the links below.



For Microsoft:

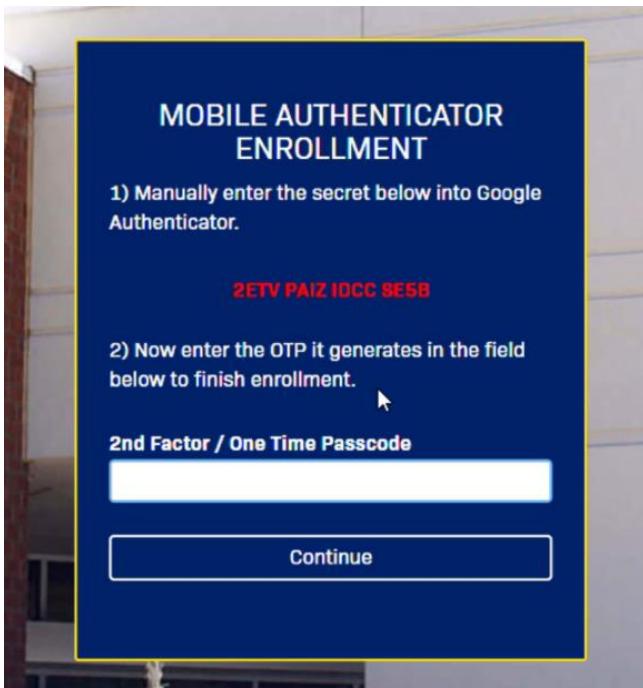
<https://apps.microsoft.com/detail/9pb8hfzfklt4?hl=en-US&gl=US>

For Android and Apple (CHROME):

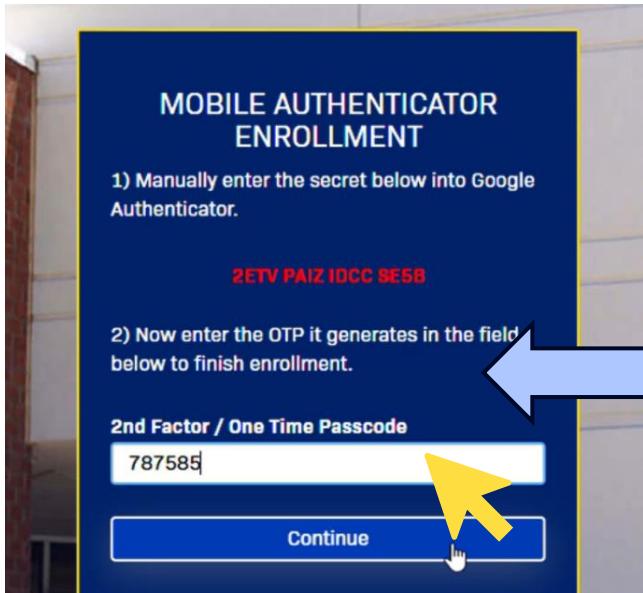
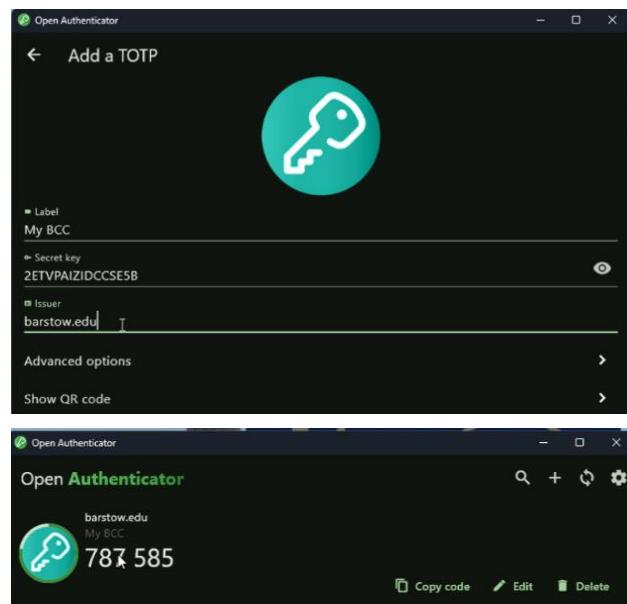
<https://openauthenticator.app/#download>

Your computer authenticator application

will generate a code.



Examples:

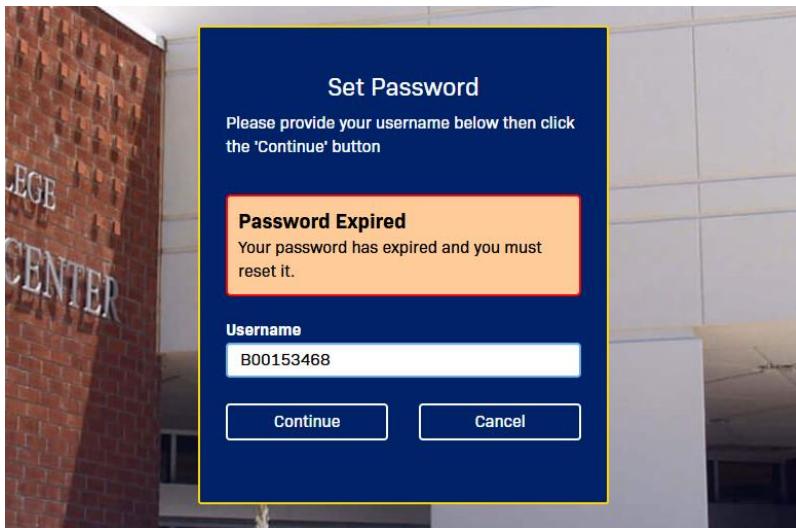


Enter the code you received in the 2nd Factor / One Time Passcode box **with no spaces** and press the 'Continue' button.

Successful enrollment!



STEP 3: CREATE A NEW PASSWORD

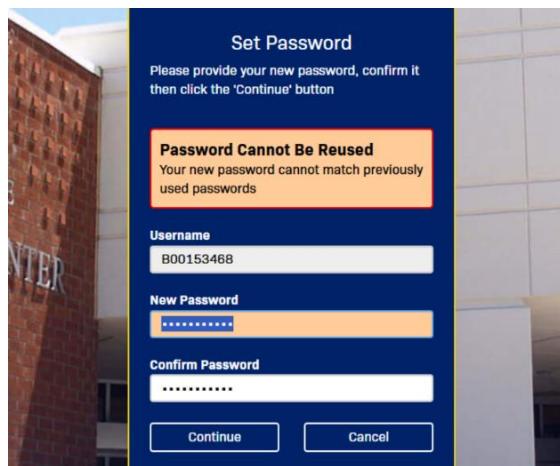


Once you have successfully enrolled in MFA, you will be prompted to set a new password.

A screenshot of a 'Set Password' page. The page title is 'Set Password' and the sub-instruction is 'Please provide your new password, confirm it then click the 'Continue' button'. A green box highlights the 'Password Complexity Rules' section, which states: 'Your new password must **always** satisfy the following rules:'. It lists two rules with green checkmarks: 'At least 8 characters long' and 'Not contain the < > & #'. Below this, it says 'It must also satisfy any **3** of the rules:' and lists four rules with green checkmarks: 'At least 1 lowercase character', 'At least 1 uppercase character', 'At least 1 numeric character', and 'At least 1 special character'. Below these are 'Username' and 'New Password' fields, and 'Continue' and 'Cancel' buttons.

Your new password must:

- Be at least 8 characters long
- Not contain <, &, or #
- Contain at least 1 **lowercase** character
- Contain at least 1 **uppercase** character
- Contain at least 1 **numeric** character
- Contain at least 1 **special** character



NOTE: Passwords **cannot** be re-used.



Successful password creation!