BARSTOW COMMUNITY COLLEGE DISTRICT

Student Multi-Factor Authentication (MFA) Setup Guide

PortalGuard MYBCC (https://login.barstow.edu)

Barstow Community College District is transitioning to Multi-Factor Authentication (MFA) to provide additional security for all user accounts.

MFA adds a second verification step to your normal username and password. BCCD's PortalGuard system allows you to use an authenticator application that generates a temporary one-time passcode (OTP).

Before You Begin

You will need:

- Your BCCD student username and password
- A computer with internet access
- A smartphone or tablet and one of the supported authenticator applications (Microsoft Authenticator or Google Authenticator) installed on your mobile device (if using a mobile device as your chosen form of authentication)

> It is easiest to complete enrollment using your **computer to display the PortalGuard QR code** and your **mobile device (smartphone or tablet) to scan the QR code**.

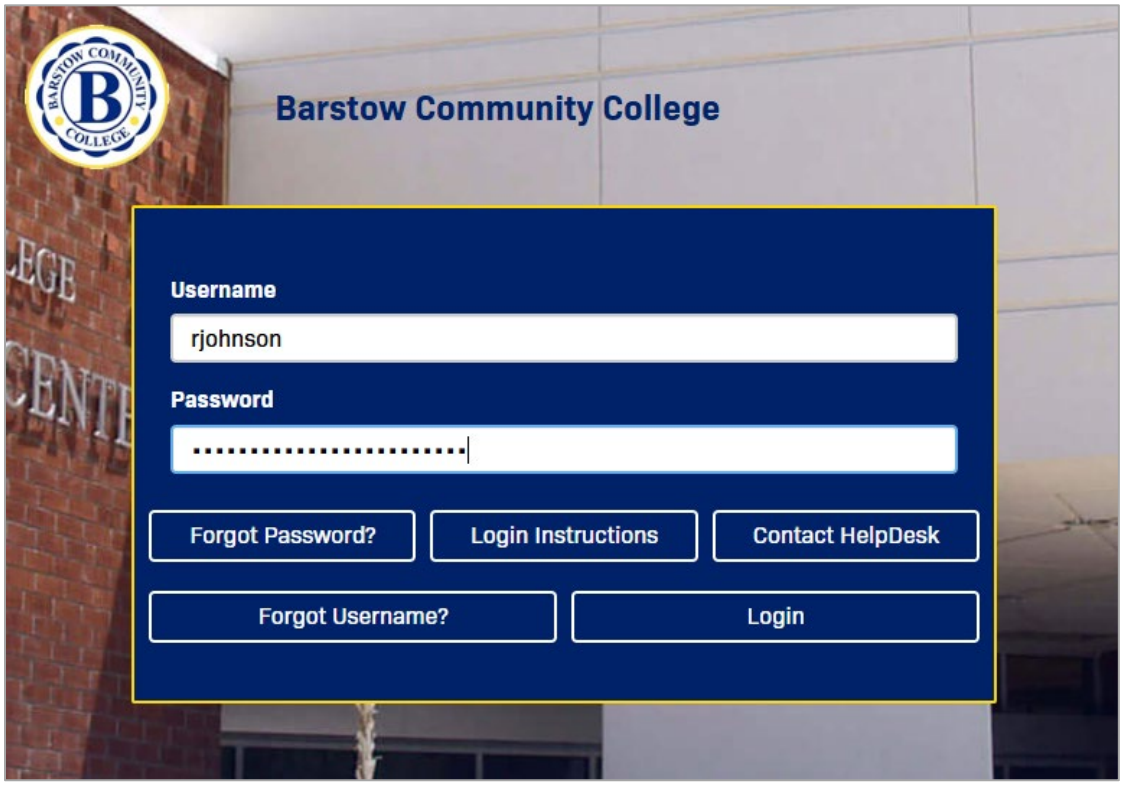
Step 1 - Sign In to PortalGuard

Open a web browser and go to:

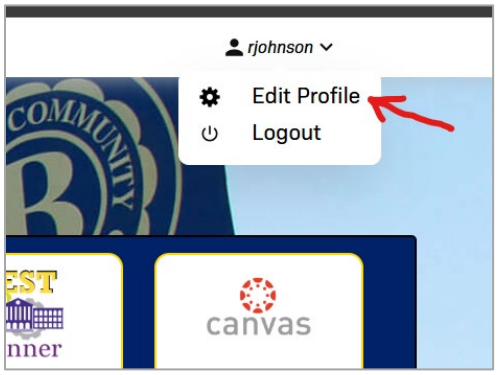
https://login.barstow.edu

Enter your BCCD login credentials:

Username: Your BCCD username (**NOT** YOUR EMAIL ADDRESS)
Password: Your current BCCD password



Once logged in, edit your profile on the Account Management page by clicking your username in the top right corner.



Step – 2 Enable Multi-Factor Authentication

On the Account Management page, locate Enable/Disable Multi-Factor, and expand by clicking the section.

Follow the instructions to Enable Multi-Factor Authentication for your account.



Once MFA has been enabled, return to the Account Management page to configure your authentication method.

Step 3 - Select Authentication Method

The Account Management page contains several security and authentication options. You only need one authenticator application for PortalGuard (MyBCC) MFA.

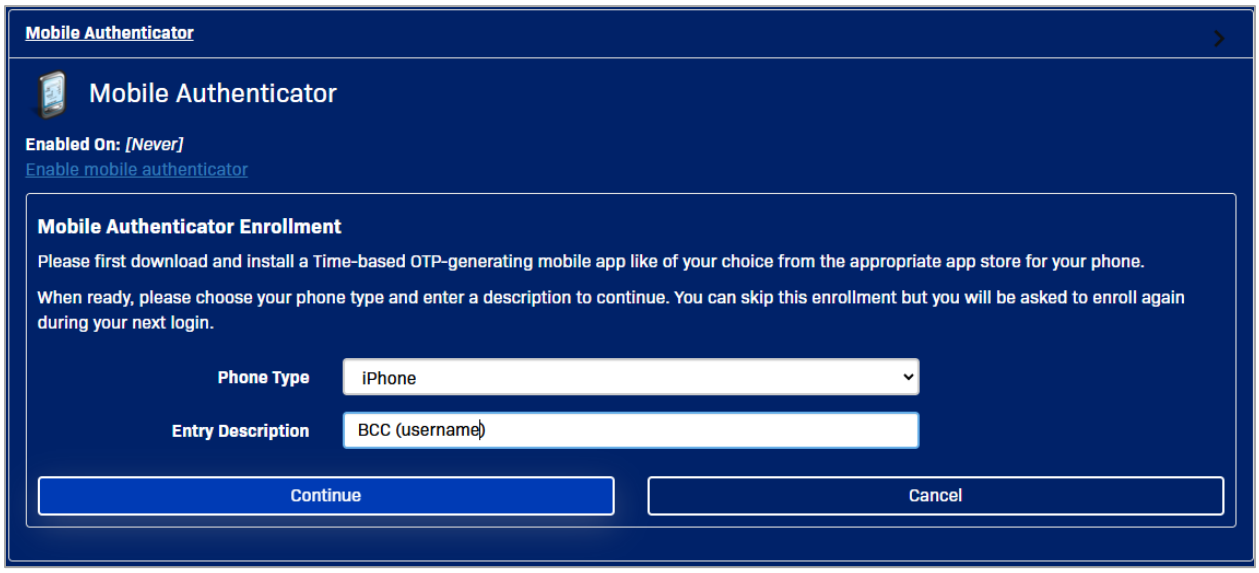
For this guide, use one of the following:

Your Situation	Recommended Option
Microsoft Authenticator already installed on your mobile device	Microsoft Authenticator **(Recommended)**
Google Authenticator already installed on your mobile device	Google Authenticator
No mobile device available	**Pin:YOU**

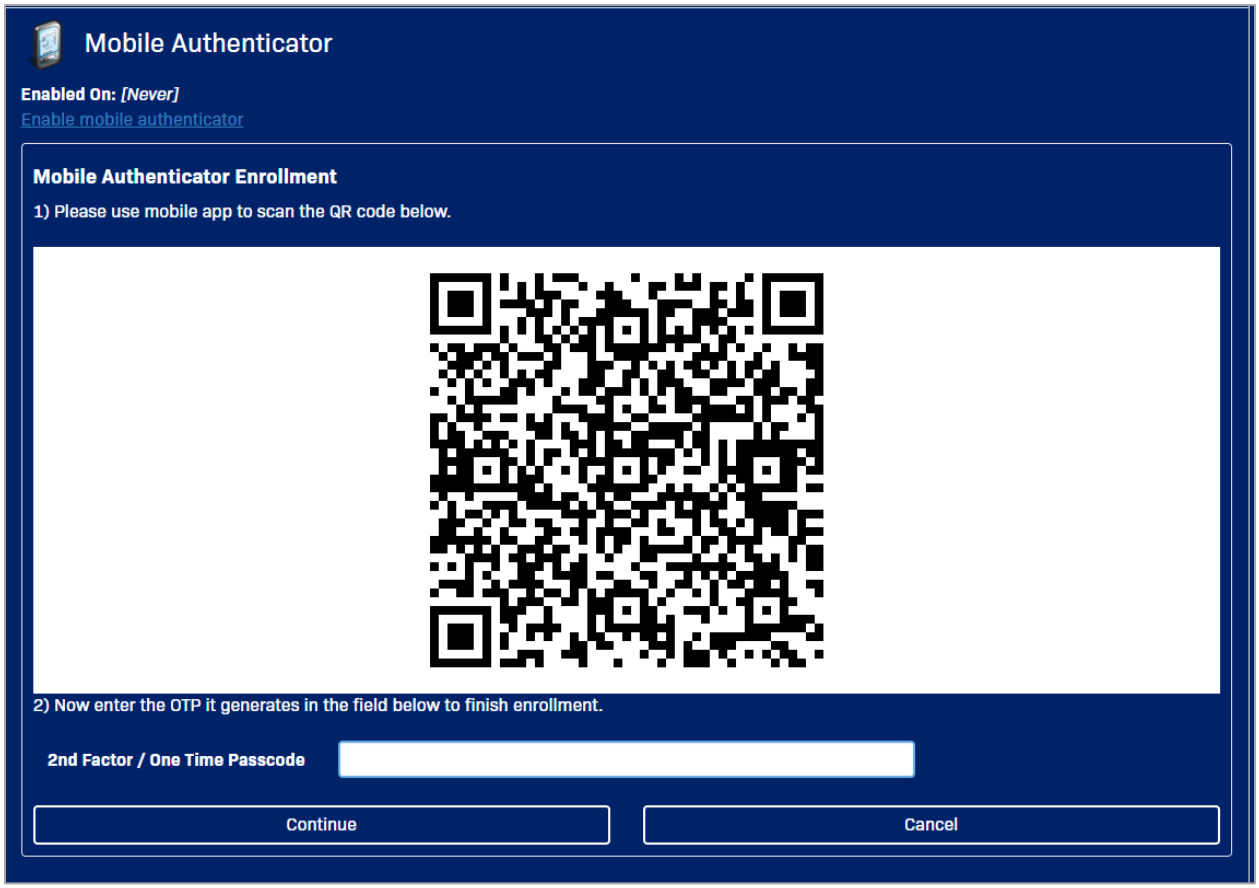
Mobile Authenticator (Smartphone or Tablet)

Mobile Authenticator

PortalGuard will display a **QR code**.



Do not share, photograph, email, or send this QR code to another person. The QR code contains information used to establish your MFA credential.



Add PortalGuard to Your Authenticator

Microsoft Authenticator ★ Recommended

- Microsoft Authenticator



1. Open Microsoft Authenticator.
2. Select the + button.
3. Select Scan QR code.
4. Scan the QR code displayed by PortalGuard.
5. Microsoft Authenticator will begin displaying a temporary verification code.

Google Authenticator

- Google Authenticator



1. Open Google Authenticator.
2. Select the + button.
3. Select Scan a QR code.
4. Scan the QR code displayed by PortalGuard.
5. Google Authenticator will begin displaying a temporary verification code.

6. Enter the verification code in PortalGuard when prompted to complete enrollment.

Step - 4 Verify Your Authenticator

Return to PortalGuard.

Your authenticator will display a temporary numeric code.

Enter the current code into the PortalGuard field labeled:

2nd Factor / One Time Passcode

Select Login.

PortalGuard will verify the code and complete your authenticator enrollment.

Pin:YOU

Your situation: No mobile device available

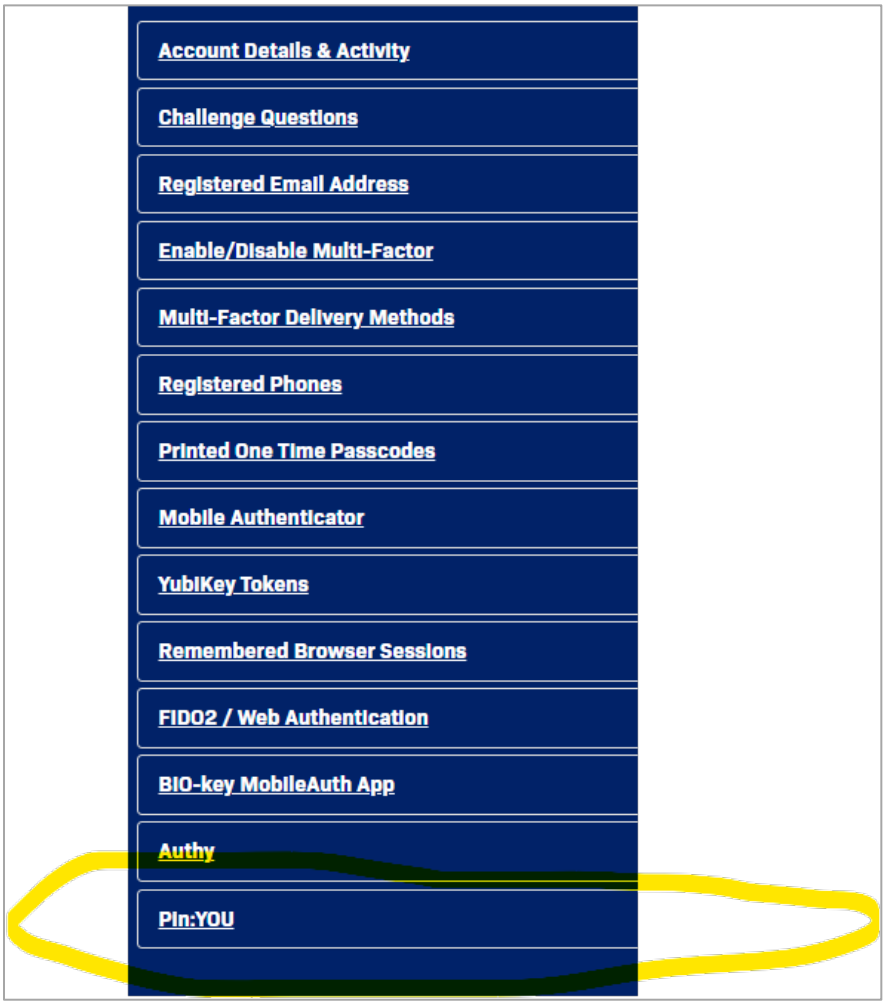
Pin:YOU

If you prefer to use Pin:YOU, select and click Enroll Pin:YOU

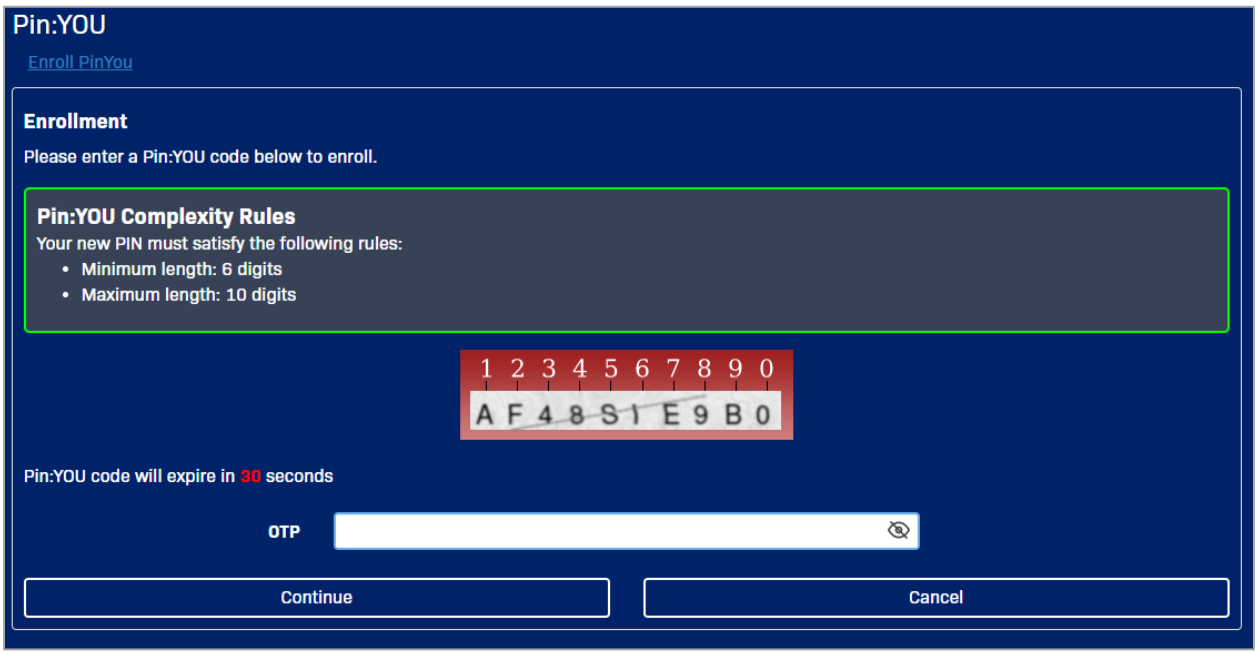


Enrolling in Pin:YOU

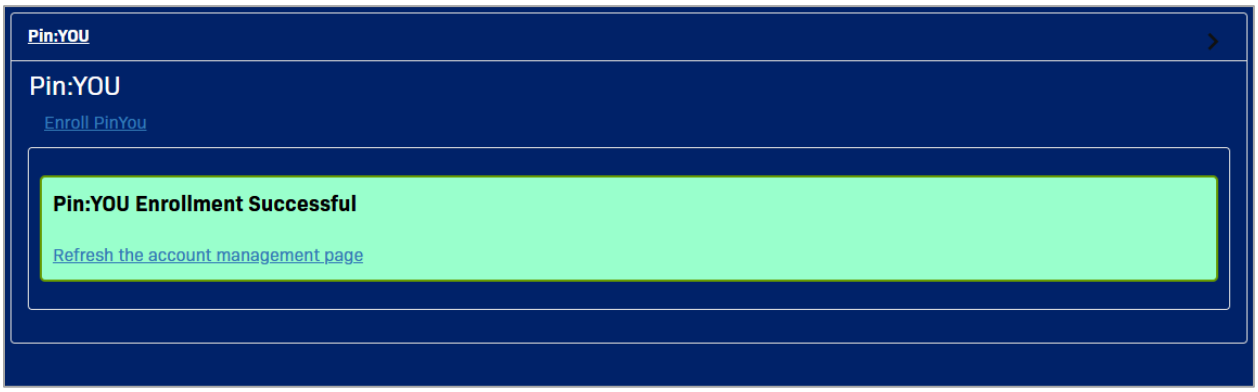
1. Select **Pin:YOU** from the available MFA enrollment options



2. Follow the PortalGuard instructions to establish your Pin:YOU Token.
3. Complete the verification process presented by PortalGuard.

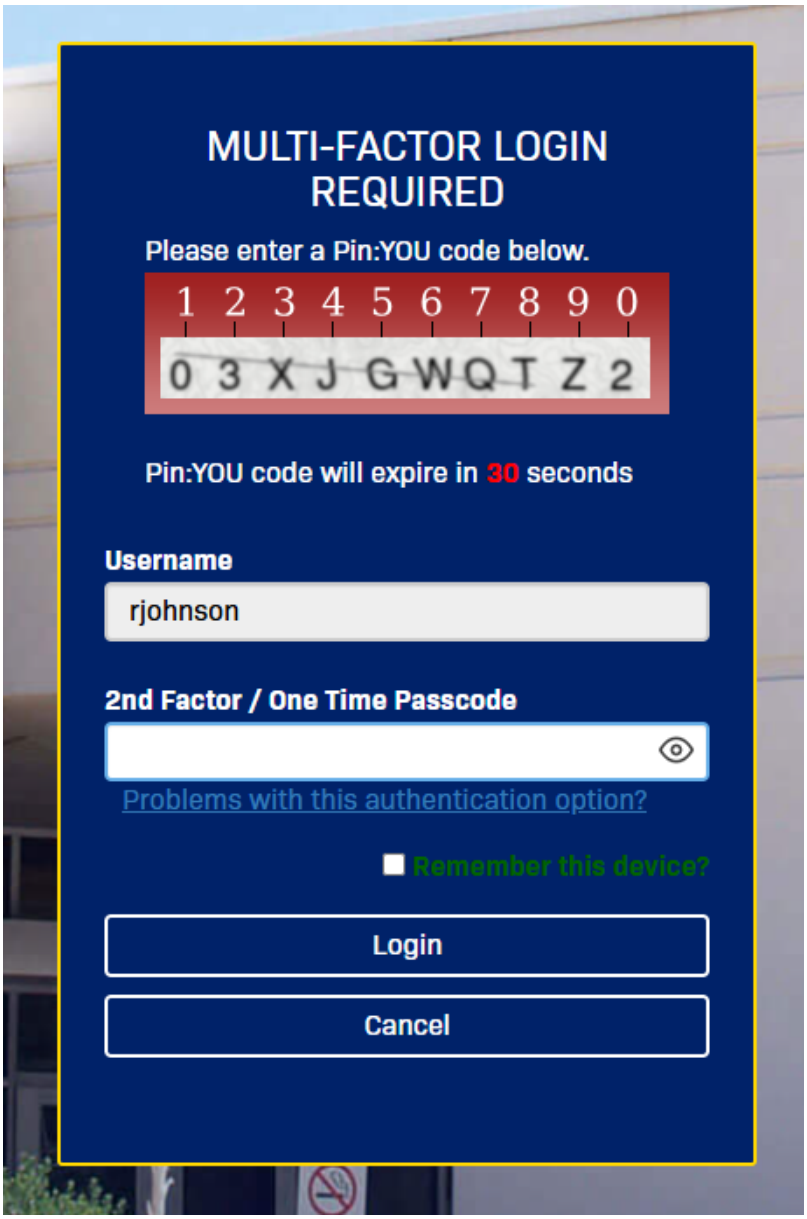


4. Confirm your enrollment.



Your Pin:You code is a security credential.
Do not share your Pin:YOU Code with anyone, including BCCD Information Technology personnel.

When you log in it will display another code for authentication:



If Your Code Does Not Work

Authenticator codes expire and are automatically replaced after a short period.

If a code is about to expire:

1. Wait for the next code or click refresh.
2. Enter the new code.
3. Select **Continue**.

Also verify that the date and time on your device are set correctly.