# Multi-Factor Authentication

Big Bend Technology

Helpdesk: 509-793-2206

# Table of Contents

# What is Okta?

Big Bend uses Okta to provide Single Sign-On (SSO) and Multi-Factor Authentication (MFA) functionality to our employees and students. One major component of our implementation is an application dashboard where you can quickly access and launch applications that are available to you. This dashboard is accessed from the 'My Apps' link at the top of the Big Bend Webpage.

The second component of our Okta implementation is for providing Multi-Factor Authentication services to help secure our network from hackers and phishing attacks. This document describes features and the use of Okta for Multi-Factor Authentication at Big Bend Community College.

# Activating your Big Bend Community College account

When being onboarded as either a student or an employee at Big Bend you'll be given a ctcLink ID (also known as your employee ID or EMPLID). You will also be given a network login account that is tied to that ctcLink ID. To use that login account, you must first activate and set a password for that account.

You will be notified as soon as your ctcLink ID is available. Students will be notified during the admissions process and employees will be notified during the hiring process.

1. Visit the New User Activation tool here: https://activateuser.bigbend.edu
2. Enter your First Name, Last Name, ctcLink ID and Date of Birth, and then click "Find Account". **Note**: These must match exactly as they're listed in the ctcLink system. If you need help at this point, please contact the Registration office (for students) or the HR office (for employees).
3. Next, make a note of your Big Bend Username and Email address as shown. This is what you'll use to login with from now on.
4. Enter a phone number in the 'SMS Phone' and/or 'Voice phone' fields to setup Self-Service password reset and MFA functionality. (**Note**: This is optional but highly recommended to make resetting a forgotten password much easier. Otherwise, you'll need to contact the BBCC Helpdesk to reset a forgotten password).
5. Finally, enter a new password to use for your account. Be sure to adhere to the password requirements shown on the screen.

# Changing your password

If you would like to change your password and know your current password, you can reset it in several different ways:

## Changing a password using Okta 'My Apps'

1. Click the 'My Apps' link at the top of the Big Bend Webpage
2. If you're already authenticated, you'll be automatically directed to your dashboard. Otherwise, you'll need to first login through Okta
3. From your Okta 'My Apps' dashboard, click your name in the upper right-hand corner, and select "Settings".

4. The account settings page appears. You may need to click on the green “Edit Profile” button to access

### Changing a password using a networked computer on campus

Log in to a networked computer on campus, press the Ctrl + Alt + Delete keys (at the same time), then select “Change a password”. Enter your existing password in the ‘old password’ field and then type a new password in the ‘new password’ and ‘confirm password’ fields.

## Resetting a forgotten password

If you’ve forgotten your password and have signed up for SMS/Voice Call authentication when you activated your account, you can reset it using the self-service password reset functionality in Okta:

1. Click the ‘My Apps’ link at the top of the Big Bend Webpage
2. At the sign in screen, click the link “Need help signing in?” at the bottom of the form, and then select “Forgot password?”
3. Enter your Big Bend username or email address and click either “Reset via SMS” to get a code sent to your cell phone via SMS, or “Reset via Voice Call” to receive a voice call that reads the code aloud.
4. Enter the code that was sent via SMS or Voice Call in the field provided and click “Verify”. (Note: in some instances, when requesting a code via SMS, you may have to first click the button “Send Code”)
5. Once Okta verifies the code, you’ll be asked to create a new password. Remember to adhere to the password requirements listed.
6. Click Reset Password.

### Enabling Forgot Password Text Message

If you did not initially setup SMS authentication during initial account activation, you can do so from within your Okta dashboard. If you’ve enabled SMS or Voice call factors for MFA, then it will also be used for self-service password reset. To verify or set the self-service password reset options:

1. Click the ‘My Apps link at the top of the Big Bend Webpage. (If you’re already authenticated, you’ll be automatically directed to your dashboard. Otherwise, you’ll need to first login through Okta.)
2. From your Okta ‘My Apps’ dashboard, click your name in the upper right-hand corner, and select “Settings”
3. The account settings page appears. You may need to click on the green “Edit Profile” button at the top (if shown) to enable access to the sections below
4. Scroll down to the section labeled “Forgot Password Text Message” and click “Add Phone Number”. (If this section already shows your phone number, then this feature is already setup and ready to use. You can edit or delete the phone number by using the buttons provided.)
5. Select the country where your phone is registered and enter a 10-digit phone number (with area code, but NOT country code). Click “Send Code”
6. An SMS text message with a 6-digit code will be sent to your mobile device. Enter the code in the field provided and click “Verify”.

### Enabling Forgot Password Voice call

If you did not initially setup Voice call authentication during initial account activation, you can do so from within your Okta dashboard. If you've enabled SMS or Voice call factors for MFA, then it will also be used for self-service password reset. To verify or set the self-service password reset options:

1. Click the 'My Apps link at the top of the Big Bend Webpage (If you're already authenticated, you'll be automatically directed to your dashboard. Otherwise, you'll need to first login through Okta.)
2. From your Okta 'My Apps' dashboard, click your name in the upper right-hand corner, and select "Settings"
3. The account settings page appears. You may need to click on the green "Edit Profile" button at the top (if shown) to enable access to the sections below
4. Scroll down to the section labeled "Forgot Password Voice Call" and click "Add Phone Number". (If this section already shows your phone number, then this feature is already setup and ready to use. You can edit or delete the phone number by using the buttons provided.)
5. Select the country where your phone is registered and enter a 10-digit phone number (with area code, but NOT country code). Click "Call"
6. An automated voice call will be made to the phone number you specified and will read a 5-digit number aloud. Enter the code in the field provided and click "Verify".

## What is the Security Image for?

Okta uses a Security Image to help you to identify a real Okta login prompt from a fraudulent or spoofed login prompt. Phishing emails will often link you to a spoofed login window that looks like the real thing to get you to unknowingly give them your login credentials. They then use those credentials to access your account to send more Phishing emails to others or to gain further access into our network.

The security image is used to help you identify if the login window is authentic. When you setup a security image, Okta will display that image during the login process after you type in your Big Bend Username. This is a sign to you that the login window is authentic and is not spoofed.

Okta will ask you to set a security image the first time you login. You can also set or change your security image through your Okta dashboard settings screen.

## What is MFA and why is it required?

MFA (Multi-Factor Authentication) is a method of securing your account by requiring two or more pieces of information, or 'Factors', to login. Factors can be something you know such as a password or pin number, something you have like an SMS text message or push notification to a mobile device or something you are such as a biometric scan. Combining two or more of these factors during login is what's called Multi-Factor Authentication.

MFA is used to help protect your account against hackers and phishing attacks by making it more difficult for the attacker to access your account. Many State and Federal laws and policies are now, or will soon be, requiring MFA authentication.

At Big Bend, there are several types of factors available to you to choose from in addition to your password. You can enable more than one type of factor available to be used:

- iOS/Android app that can be used to receive push notifications
- SMS text message to a mobile phone
- Voice Call to a mobile or landline phone
- Physical One Time Password 'token' which will display a random 6-digit number
- FIDO2 (WebAuthn) USB touch security key

Starting Summer of 2022, Big Bend Community College will be requiring MFA to be used for all network accounts to help keep our network secure. This includes both employees and student accounts. You'll be prompted for a second factor based on risk and behavior analysis, per device, at least once every 30 days although may be more frequent depending on where you are logging in from, what type of device, or service being accessed.

## Okta Verify iOS/Android mobile app (Recommended)

The recommended factor for students and employees that have a mobile device is to install the free "Okta Verify" app to receive push notifications. This would allow you to use your device as an MFA factor without relying on your wireless carrier's SMS reliability or security. SMS messages sometimes do not go through or can be delayed. With Okta Verify, it's all done securely through the lightweight app. The Okta Verify app can also be used without Wi-Fi or Cellular Data network signal.

### To setup Okta Verify as a factor

1. Click the 'My Apps' link at the top of the Big Bend Webpage

2. If you're already authenticated, you'll be automatically directed to your dashboard. Otherwise, you'll need to first login through Okta.
3. From your Okta 'My Apps' dashboard, click your name in the upper right-hand corner, and select "Settings".
4. The account settings page appears. You may need to click on the green "Edit Profile" button at the top (if shown) to enable access to the sections below.
5. Scroll down to the section labeled "Extra Verification" and click "Set up" next to Okta Verify.
6. On the Set up multifactor authentication window, click the "Setup" button.
7. Select your mobile device type (iPhone or Android) and then download the "Okta Verify" app from the app store on your mobile device. (**Note**: be sure to download the "Okta Verify" app not the "Okta Mobile" app). Click Next once the app is downloaded to your mobile device.


8. Launch the Okta Verify app on your mobile device and select "Add an account". Scan the QR code displayed on the screen using the app. (Click "Can't scan?" if you're unable to scan the QR code to have an activation link sent via SMS or Email)

### Using Okta Verify as a factor

1. When prompted for an authentication factor, select "Okta Verify (device name)" from the available factors list and click "Send Push"
2. The Okta Verify app will display a push notification on your device. Click "Yes, it's me" on the notification.
    a. If you're in an area with no Wi-Fi or mobile data signal, you can alternately enter a 6-digit code displayed in the Okta Verify app.

## SMS text

The SMS text factor works by sending an SMS text message with a 6-digit code to your mobile device. You then enter that code into the prompt to verify your identity.

When activating your account for the first time, you're given the opportunity to setup the SMS factor. Although it is optional, setting it will enable SMS to be used as an MFA factor and as an extra verification for Self-Service Password Reset. This is the easiest way to setup MFA and self-service password reset.

### Enroll SMS as a factor

1. Click the 'My Apps' link at the top of the Big Bend Webpage
2. If you're already authenticated, you'll be automatically directed to your dashboard. Otherwise, you'll need to first login through Okta.
3. From your Okta 'My Apps' dashboard, click your name in the upper right-hand corner, and select "Settings".

4. The account settings page appears. You may need to click on the green “Edit Profile” button at the top (if shown) to enable access to the sections below.
5. Scroll down to the section labeled “Extra Verification” and click “Set up” next to SMS Authentication.
6. On the Set up multifactor authentication window, click the “Setup” button.
7. Select the country where this mobile phone is registered (IE: This sets the Country Code that will be used for dialing this number).
8. Enter the 10-digit Phone Number (with area code) and click “Send code”
9. An SMS message with a 6-digit verification code will be sent to the phone number you entered. Enter this in the field provided and click “Verify”
10. If the code matches, you’ll be returned to the account settings page and a note will display showing that the SMS factor was successfully enrolled.

### Using SMS as a factor

1. When prompted for an authentication factor, select “SMS Authentication” from the available factors list
2. Click Send code. (**Note**: the SMS message is not automatically sent. You must first click Send code to initiate the SMS message)
3. You should receive an SMS message with a 6-digit code. Enter the code into the field provided and click “Verify”

## Voice Call

The Voice call factor works by calling you by phone and reading a 5-digit code aloud. You then enter that code into the prompt to verify your identity. Either a mobile or landline phone can be specified, but, if you’re prompted for this authentication factor, you will need to have access to the phone line provided to receive the call.

When activating your account for the first time, you’re given the opportunity to setup the Voice Call factor. Although it is optional, setting it will enable Voice Call to be used as an MFA factor and as an extra verification for Self-Service Password Reset. This is the easiest way to setup MFA and self-service password reset.

### Enroll Voice Call as a factor

1. Click the ‘My Apps’ link at the top of the Big Bend Webpage
2. If you’re already authenticated, you’ll be automatically directed to your dashboard. Otherwise, you’ll need to first login through Okta.
3. From your Okta ‘My Apps’ dashboard, click your name in the upper right-hand corner, and select “Settings”.
4. The account settings page appears. You may need to click on the green “Edit Profile” button at the top (if shown) to enable access to the sections below.
5. Scroll down to the section labeled “Extra Verification” and click “Set up” next to Voice Call Authentication.
6. On the Set up multifactor authentication window, click the “Setup” button.

7. Select the country where this voice phone is registered (IE: This sets the Country Code that will be used for dialing this number).
8. Enter the 10-digit Phone Number (with area code) and click “Call”
9. A voice call is placed to the phone number entered and when answered, an automated voice will read a 5-digit number aloud. Enter this number in the field provided and click “Verify”
10. If the code matches, you’ll be returned to the account settings page and a note will display showing that the SMS factor was successfully enrolled.

### Using Voice Call as a factor

1. When prompted for an authentication factor, select “Voice Call Authentication” from the available factors list
2. Click the Call button. (**Note**: the voice call is not automatically initiated. You must first click “Call” to initiate the voice call)
3. A voice call is placed to the phone number registered and when answered, an automated voice will read a 5-digit number aloud. Enter this number in the field provided and click “Verify”.

## One Time Password (OTP) token.

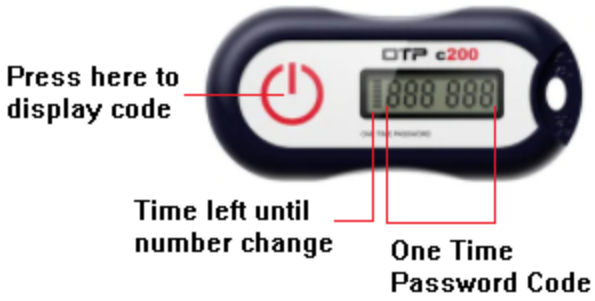
For students and staff that may not have or would prefer to not use a mobile device, an OTP token can be assigned by library staff. To get an OTP token assigned to you, you’ll need to provide proof of identity such as Employee or Student ID. Library staff will then register a token to your account to be used as your secondary MFA factor.

**Important Note**: Be mindful that this token is used to authenticate you to our systems. This means that the token is like a password and should be guarded just as you would your password. Don’t leave it lying around unattended and don’t give out the number listed on the token to anyone.

### Using the OTP token

1. When prompted for an authentication factor, select “OTP C200” from the available factors list (if not already selected)
2. Press the button on the token to display the current 6-digit number.
3. Enter the number into the field provided in the authentication prompt and click “Verify”.

   **Note:** The 6-digit number displayed on the token changes every 60 seconds. The lines on the left of the display show how soon the number displayed will change. There are a total of 6 lines each of which represents 10 seconds. If only one or no lines are shown when you press the button, it may be best to wait for the next code to display before typing it into the prompt.




If your token is lost, stolen or stops working, you'll need to notify library staff so they can deactivate the old token and assign a new token. If you no longer need the token, it can also be returned to the library for deactivation and re-use.

## FIDO Key (Employees only)

The FIDO keys that Big Bend uses are small touch-activated USB devices that are assigned to a specific user. The key can be removed and used by that user in another computer if needed.

If you have set up the Okta app or SMS text options for your mobile device, a FIDO key is not necessary. For employees that are unable to use a mobile device for MFA, FIDO keys are available in the library.

### Enroll a FIDO Key factor

1. Pick up a FIDO key from library staff (example shown below)

2. Insert the key into an available USB port on your workstation or laptop.
3. Open a web browser and click the 'My Apps' link at the top of the Big Bend Webpage
4. Once logged into Okta, click your name in the upper right-hand corner and select "Settings".
5. The account settings page appears. You may need to click on the green "Edit Profile" button at the top (if shown) to enable access to the sections below.
6. Scroll down to the section labeled "Extra Verification" and click "Set up" next to "Security Key or Biometric Authenticator".
7. On the Set up multifactor authentication window, click the "Setup" button.
8. Click the "Enroll" button to initiate the enroll process for your key
9. You'll be prompted to insert the security key and touch it to complete the enrollment. (A LED on the security key will be flashing).
10. Your browser may also ask if you want to allow the site (bigbend.okta.com) to see your security key. Click "Allow".

### Using the FIDO Key as a factor

1. When prompted for an authentication factor, select "Security Key or Biometric Authenticator" from the available factors list if not already selected.
2. Your browser will prompt you to insert and touch the security key to authenticate.

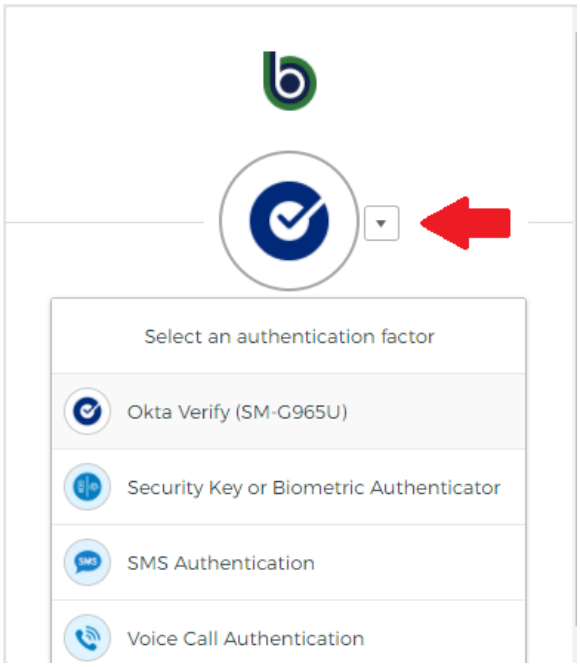
**Note**: Be sure to keep track of the FIDO key…. Because it's so small, it can be easily lost. Also, anyone that has physical access to your key can authenticate with that key (for MFA only). Be sure to not leave the key in the USB port if the computer is in a public location. Also, if this is the ONLY factor you have enrolled, you will need to have the key with you any time MFA is required.

## Selecting a factor to use

When prompted for a secondary authentication factor, you can select from any of the factors for which you've setup. The window will always default to the factor you last used.

To select a specific factor:

1. Click the drop-down arrow next to the icon at the top of the message to see the list of available factors, then select the factor you'd like to use.




## Unexpected Okta Verify, SMS, or Voice call prompts

If you receive an SMS, Voice call or Okta Verify prompt for secondary authentication but did not just attempt to authenticate, then your credentials may be compromised. This is a sign that someone other

than you may know your password and is trying to access your account but is being blocked by the MFA requirement.

With the Okta Verify app, you're presented with two options "Yes, it's me" or "No it's not me". Click the "No, It's not me" prompt to deny access and change your password as soon as possible.

With SMS or Voice call authentication just ignore the prompt and change your password as soon as possible.

Also, any time an MFA factor is unregistered from your account you'll receive a confirmation email to your Big Bend email account to let you know. If you receive an email but did not disable an MFA factor (or are not working with the Library or Big Bend Helpdesk to do so), please contact the Big Bend helpdesk immediately, as your account may already be compromised.

## Getting Help

For assistance with any of the above tasks or features, please contact the Big Bend Helpdesk at (509) 793-2206 M-Th 7:30am - 5:00pm, and Fridays 7:30am - 2:30pm.