Multifactor Authentication FAQs

Contents

What is Multi-Factor Authentication at BC3 (MFA)?

Multi-Factor authentication (MFA) provides an extra layer of security in addition to passwords. This additional step ensures that your information, transactions, or online work is safer from unauthorized access by requiring a second method of authentication through the Microsoft Authenticator app or a physical hardware security key to verify your identity. Even if someone obtains your password, they cannot access your account without having your registered MFA device.

Is MFA required?

Starting in September of 2022 all staff, faculty, and students will be required to use MFA.

Does the Microsoft Authenticator App track my location?

The Microsoft Authenticator App does have the ability to check the device location. Location data is used to determine the device location at the time of authentication. For example: If there is a login attempt with a successful MFA verification but the MFA device location originated from North Korea we would block that until we could verify the authenticity of that login attempt.

How does Microsoft Multi-Factor Authentication (MS MFA) work?

Microsoft Multi-Factor Authentication (MS MFA), also known as MS MFA or "Two-Step Verification" uses mobile technology to send an authentication request to your registered device. When you log in, a notification will be sent immediately to your smartphone or another registered device. You simply tap Approve on the screen if using the authenticator app or use a numerical code sent to your device, which verifies that you are the person logging in.

Why should I use Microsoft Multi-Factor Authentication (MS MFA)?

Microsoft Multi-Factor Authentication (MS MFA) provides extra protection for the sensitive information our systems contain in case you are a victim of phishing or hacking. If someone steals your credentials and tries to access your account, your username and password will not be sufficient to log in. The thief will also need to have access to your device to complete the login process. If someone else tries to log in to your account, you will be notified on your device and you can deny them access instantaneously.

What devices are supported to register for Microsoft Multi-Factor Authentication (MS MFA)?

iOS devices (iPhone, iPad, iPod)
Android devices (phone, tablet)

Which services or systems currently require Microsoft Multi-Factor Authentication (MS MFA) for login?

Multifactor Authentication will be required when you log into most web-based applications such as the MyBC3 portal, Blackboard, Email, Colleague, Self Service, and Citrix just to name a few. At this time MFA is not required to log into the Windows operating system and local apps on a physical desktop but you will need it to access the web-based applications both on and off campus.

How often will I have to use Microsoft Multi-Factor Authentication (MS MFA)?

Each time you access one of the above services either in a new browser session or on a different device, you'll be required to sign in and use Multi-Factor Authentication. After that session is established you will not be required to reauthenticate with MFA for 10 hours. For this reason, it is NOT recommended that you use any shared device. If you do use a shared device do not save your login credentials and be sure you log out of all sessions, clear your browser history, and restart the device when you are done using it.

Why can't I use email as a second factor?

Having a second-factor verification sent to a designated email address is not considered to be a safe method, as it can more easily be intercepted by a cyber-criminal. Email account takeovers are a common form of cybercrime. A personal mobile device or security device is in your physical possession and therefore less likely to be intercepted by a cybercriminal. As a point of reference, many major online account service providers like Google and Apple no longer allow email as a second factor for many of their services.

How do I get started?

Configuring Your Account for Microsoft Authenticator App for Faculty and Staff

Configuring Your Account for Microsoft Authenticator App for Students

How many devices can I enroll in Microsoft Multi-Factor Authentication (MS MFA)?

Microsoft Multi-Factor Authentication (MS MFA) lets you register multiple devices to your account, so you can always access your account even if one device is temporarily unavailable. We recommend no more than necessary with a max of three devices just so you don’t lose track of a device with authentication privileges on it.

What if I do not have a smartphone or mobile device?

Although the use of the Microsoft Authenticator app on a mobile device is recommended, you can opt to use a physical hardware security key. To do so please contact the helpdesk at 724-287-8711 ext 8441 for assistance getting one

How do physical hardware security keys Work?

Physical hardware security keys must be requested. Please contact the helpdesk at 724-287-8711 ext 8441 for assistance getting one. Physical hardware security keys generate a one-time passcode, which can be used to enter on-screen when prompted as your secondary authentication method.

How do I authenticate with my smartphone app if I don't have a cell signal, data, or WiFi connection?

If you do not have internet access and cannot receive a “Push” notification through the Microsoft Authenticator app you can use a one-time passcode. You can generate a passcode in the Microsoft Authenticator app even without internet access and enter the six-digit code.

My account is locked out. What should I do?

The most common reason why your account is locked is that you have entered an incorrect password or the MFA has failed at least 5 times. In this case please contact the helpdesk at 724-287-8711 ext 8441.

I don’t have my Microsoft Multi-Factor Authentication (MS MFA) device with me. What can I do?

Contact the helpdesk at 724-287-8711 ext 8441.

What do I do if I get a Microsoft Multi-Factor Authentication (MS MFA) push notification on my device when I didn't log in?

If you get a push notification from the Microsoft Authenticator app that you did not request, that means someone else is trying to log in using your account and your account may have been compromised. Tap the Deny button in your Microsoft Authenticator app or take no action if a code is pushed to your device and contact the helpdesk immediately at 724-287-8711 ext 8441.

How Much Data Does a Microsoft Authenticator Request Use?

Microsoft Authenticator authentication requests require a minimal amount of data -- less than 2KB per authentication. For example, you would only consume 1 megabyte (MB) of data if you were to authenticate 500 times in a given month. If your device is connected to Wi-Fi, no mobile data will be used. If you use the code generated by the Microsoft Authenticator App, no data will be used and you can limit application updates to Wi-Fi only in the settings on most phones.

I replaced the phone that I had registered in Microsoft Multi-Factor Authentication (MS MFA). What should I do now?

In most cases, iPhone and Android phones automatically transfer your applications over to a new device when you switch to a new phone. In this case, the Microsoft Authenticator app should transfer as well. In some cases, you may need to reauthenticate on the new device. If you are having trouble after moving to a new device contact the helpdesk at 724-287-8711 ext 8441.

My mobile device is running an older operating system and I am unable to install the Microsoft Authenticator application from the App Store. What do I do?

Contact the helpdesk at 724-287-8711 ext 8441.

Does Using Microsoft Authenticator Give Up Control of My Smartphone?

No. The Microsoft Authenticator app has no access to change settings or remotely wipe your phone. The visibility Microsoft Authenticator requires is to verify the security of your device, such as operating system version, device encryption status, screen lock, etc. Microsoft uses this to help recommend security improvements to your device. You always are in control of whether or not you act on these recommendations.