Multifactor Authentication (MFA)

What Is Multi-Factor Authentication (MFA)?

Authentication is the process of proving your identity. There are three primary methods to prove one's identity: something you know (like a password), something you have (like a security token), or something you are (like a fingerprint). Single factor authentication involves one identity factor – and generally involves just "something you know" - a password. As the name implies, multi-factor authentication is the process of using more than one authentication method to prove identity. Adding a second factor for authentication generally includes adding something you have – like a smart phone or security token.

Why Do I Need MFA?

EMCC has a legal duty to protect the student and employee information that we have access to. Adding a second identification factor makes it considerably more difficult for an attacker to compromise your employee account and access college information systems that you have access to. Increasingly, stolen passwords are traded and sold online and used to target you and the data you have access to for financial gain. Some studies suggest that adding multi-factor authentication to your account can block 99.9% of account compromise attacks.

How Does MFA work at EMCC?

We support **Microsoft Authenticator** app

- The Microsoft Authenticator app makes use of the one thing that most of us carry everywhere – a smartphone. This is the quickest and easiest way to use MFA at EMCC. This small app installed on your phone connects to your EMCC account and will receive a push notification when an attempt is made to login to your account. Simply approve the request if you attempted to login – otherwise, deny it. Phones and tablets are all supported. You do not need to have your phone connected to email, wi-fi, or other EMCC services to use this app, and it provides no control or visibility to EMCC regarding your personal device or how it is used and can be transferred to a new phone, as needed.

How to Setup MFA Using the Microsoft Authenticator App

1. You will need a computer, the smartphone that you normally use and about five minutes to complete. **On your smartphone**, visit the Apple App Store or Google Play Store to install the Microsoft Authenticator App. Search for "Microsoft Authenticator" or use the QR code below:

2. After installing the Microsoft Authenticator app, **go to the computer** and login to your Office 365 Account using the following URL - sign in using your EMCC email address and password:

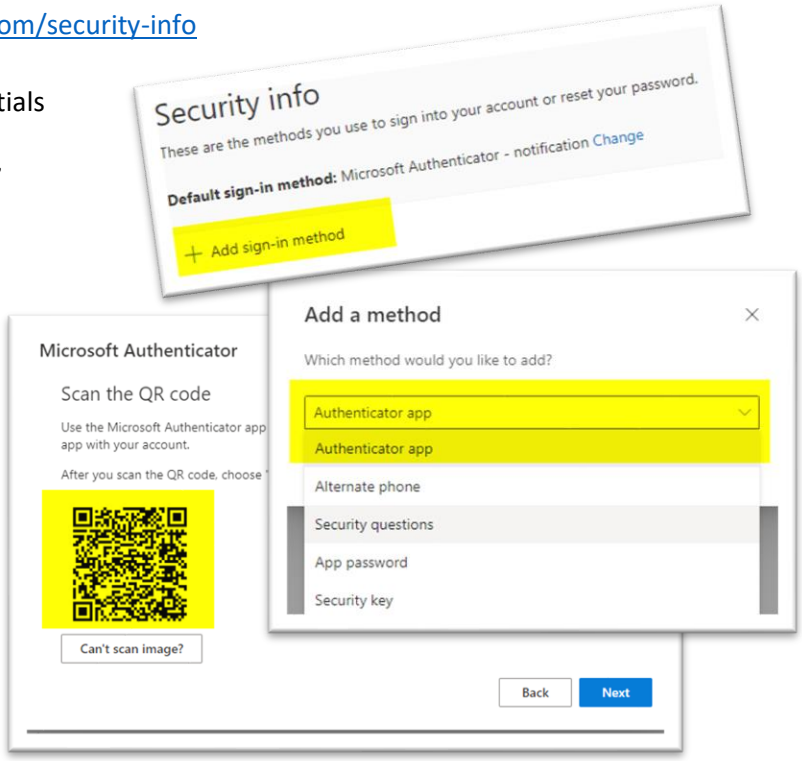
   a. https://mysignins.microsoft.com/security-info

   b. Login with your EMCC credentials

   c. Click on “Add sign-in method”

   d. Select “Authenticator App”

   e. Click the blue “Next” button twice (2x) until the QR code appears on the screen.



f. Open the Microsoft Authenticator App on your smartphone.

g. Locate the Plus (+) sign in the top right corner and tap it

h. Select the option for “Work or school account”

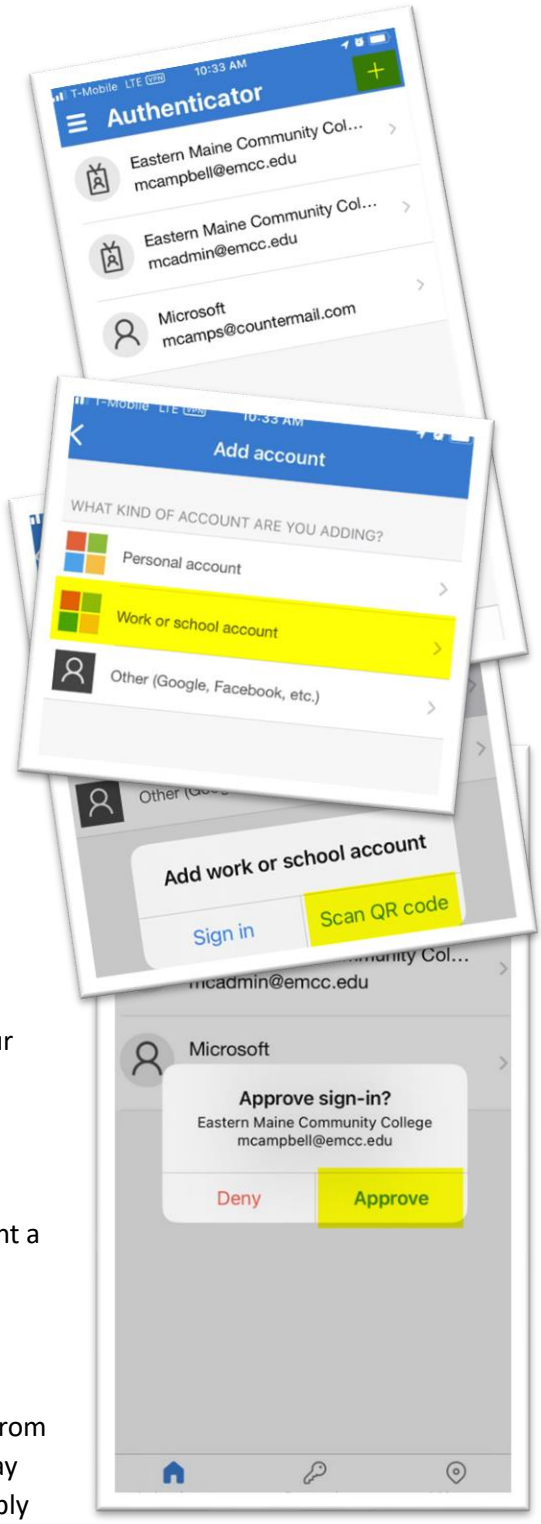
i. On the next screen select the option to “Scan QR code” (if it asks for permissions to your camera – tap “allow”)

j. Point your phone camera at the QR code that is displayed on the computer or other device. (Note that some devices may ask to use other forms of authentication such as using your pin to verify or scanning your face/fingerprint - this is only used to access your phone.)

k. Once you have scanned the QR code, hit the blue “Next” button to test the authenticator push on your phone. If not already open, go back to the authenticator app.

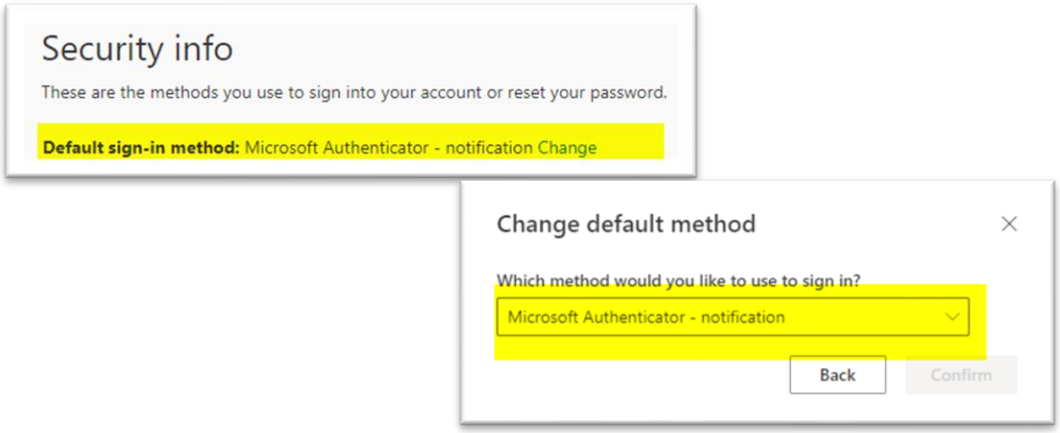
l. When signing in, Microsoft Authenticator will present a notification that asks for you to approve the sign-in attempt.

m. Periodically, or when signing in on a new device or from an unknown location, EMCC and Microsoft O365 may ask you for your second factor authentication – simply approve the sign-in attempt, in the same manner.



n. **IMPORTANT:** If you receive a notification, but you were **NOT** trying to access your EMCC account or a Microsoft product associated with your account, then someone else may be attempting to access your account. In this case, you want to **DENY the attempt** - you may also want to change your password and alert the IT help desk of the attempt.

o. The final step is to set the authenticator as the default method**. Return to the computer on the same site where you obtained the QR code.** If you closed that page, navigate to the link above in step A. Here, under "Default sign in method", you should see a link that says "Change" - click this link and select "**Microsoft Authenticator – notification**" and then click "Confirm".



p. The authenticator app is now setup and will be required for login when additional verification is needed to validate your identity – for example, when your account is used to sign in on a new device or when your password is changed.

q. Once you've setup MFA, please email the helpdesk and let us know! We will then enable the multi-factor requirement for your account. (If you forget, this will automatically be enabled and you may be required to go through these steps again.)