Kishwaukee College - MFA Setup Guide

What is Multi-factor Authentication?

Multi-factor authentication (MFA) is a way to make sure your online accounts are secure. It means you must provide more than just a password to access your account. MFA is important because it adds an extra layer of protection. Even if someone guesses or steals your password, they still won't be able to get into your account without the additional verification. MFA helps keep your personal information safe and reduces the risk of unauthorized access to your KishID account.

Configuring MFA for Kishwaukee College:

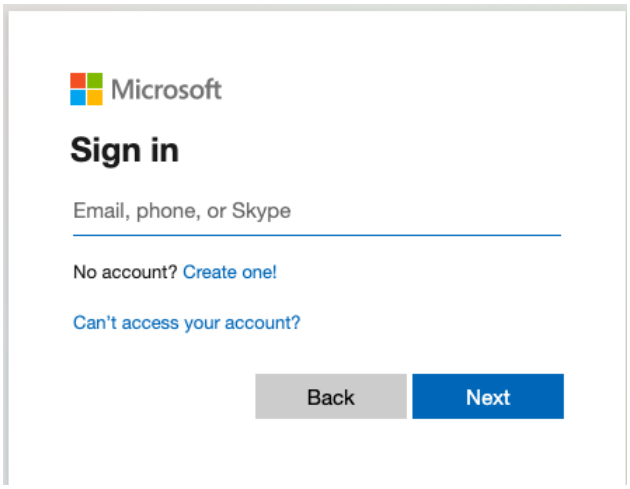
Step 1:

You will need a smart device (ipad, iphone, tablet, android phone) or a phone that can receive text messages/phone calls.

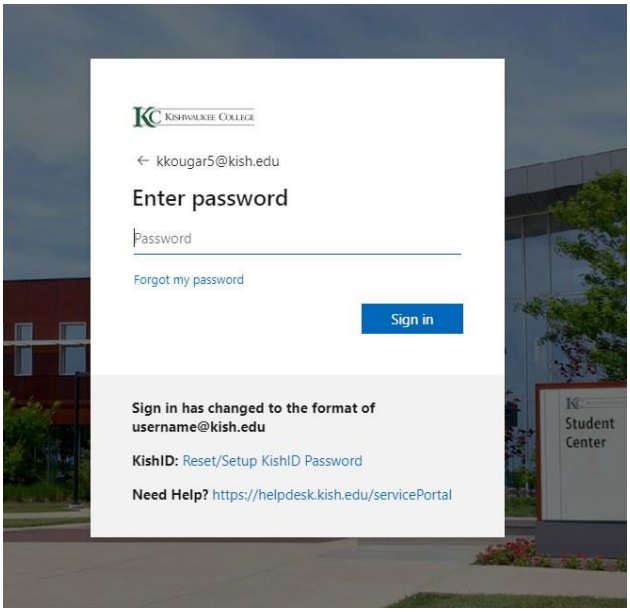
Step 2:

Using a computer or smart device, sign in to https://outlook.office.com or https://www.office.com/ To sign-in, enter your Kish email address, then click next.

Note: Username is your full KishID Email address. Example: kkougar6@kish.edu

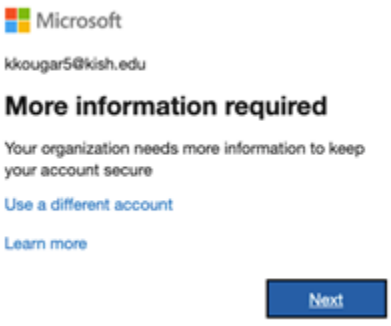


1 - Once at our sign-in page, enter your KishID username and password to complete the sign-in.



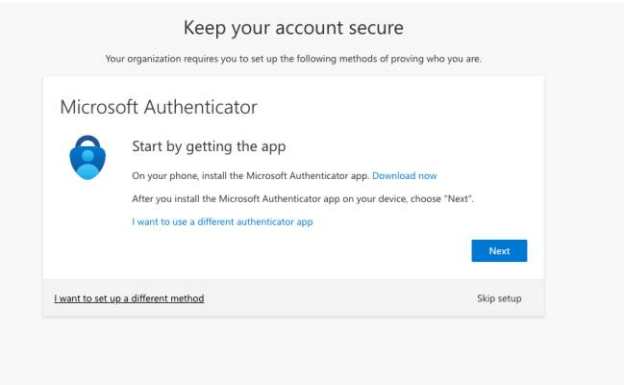
2 - On the password page, if you do not see the Kishwaukee College logo or the photo of the student center, you didn't enter the full email address. Hitting back on the browser will take you back to the login screen to add the full email address.

Step 3:



3 - Upon login, you will see the message prompting you for more information, this is to configure MFA. Click next to start the configuration process.

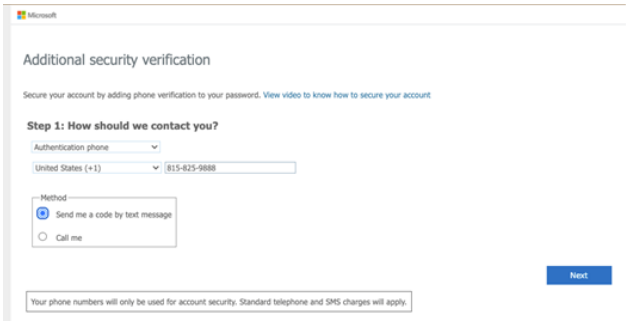
There are currently two options: ***Option A*** is for Authentication Phone (SMS/Phone Call), ***Option B*** is for the Mobile App (installed on smart your smart device). **Only one option is required** and may be switched with assistance from IT. If you would like to change your MFA type, contact us at the helpdesk and we can help reset the options back to default.



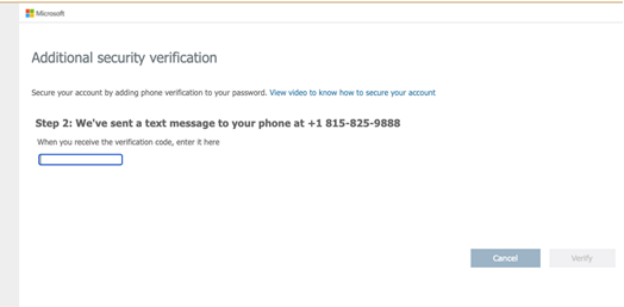
4 - To select Option A, click on the link that says I want to set up a different method and select Phone from the drop down box. For Option B, click the Next button

Option A (SMS/Phone Call) Setup:

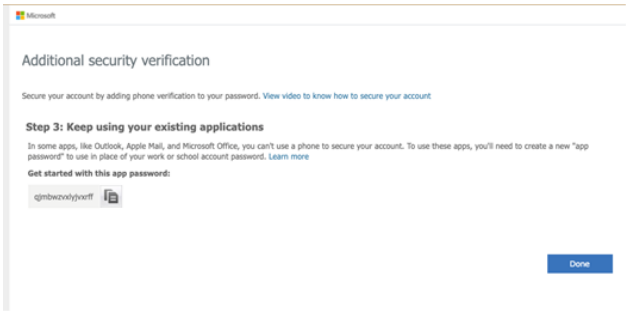
Note, if choosing Authentication Phone, please use a cell phone number not a desk phone/office phone. Make sure you put in United States (+1). This will text you a code to this phone and you will enter that into the step 2. If there is an error, it will prompt you and you will be able get a new code sent to you. If the code is correct you will get to the final step, which you can ignore as we do not use this feature.



5 - Enter your phone number



6 - A code will be texted to you or a phone call will happen to give you the code to enter

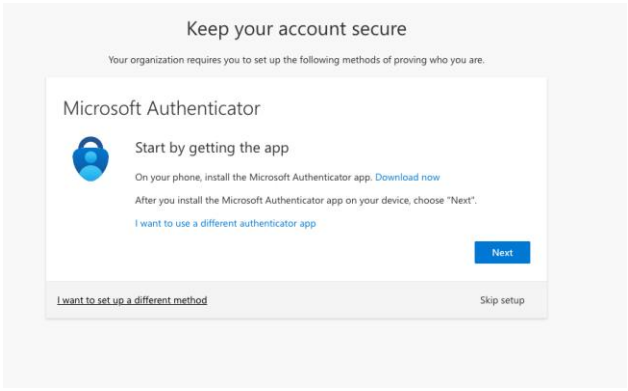


7 - This screen can be ignored it prompted.

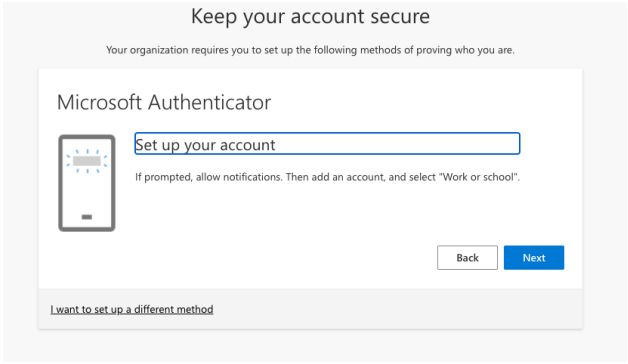
Option B (Mobile App) Setup:

Choosing the mobile app is the more secure way of completing MFA. A push notification will come to your phone when you do an MFA request.

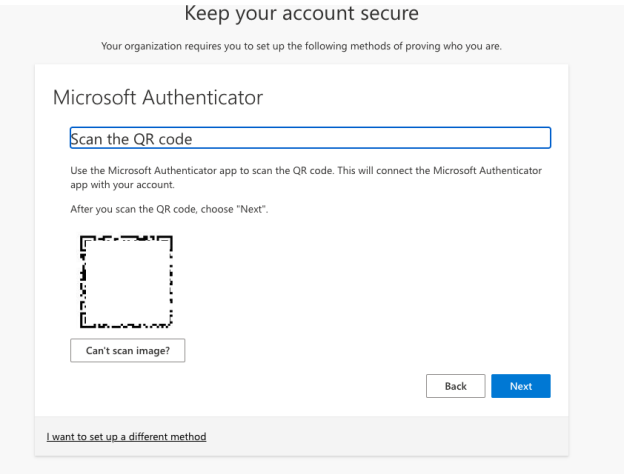
When the Authenticator app is downloaded, while opening up the app for the first time, you may be prompted for “Work or School Account”, choose this option. If you have already used the Microsoft Authenticator for another account, clicking the + in the app will get you to this same prompt.



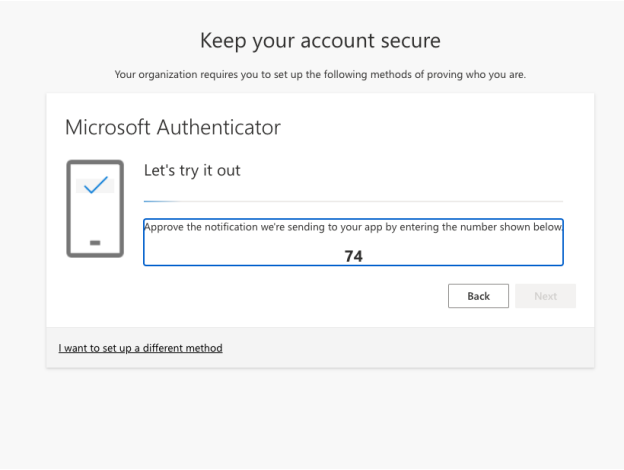
8 - Click the link Download now to download the app from either the Google Play Store or the Apple App Store.



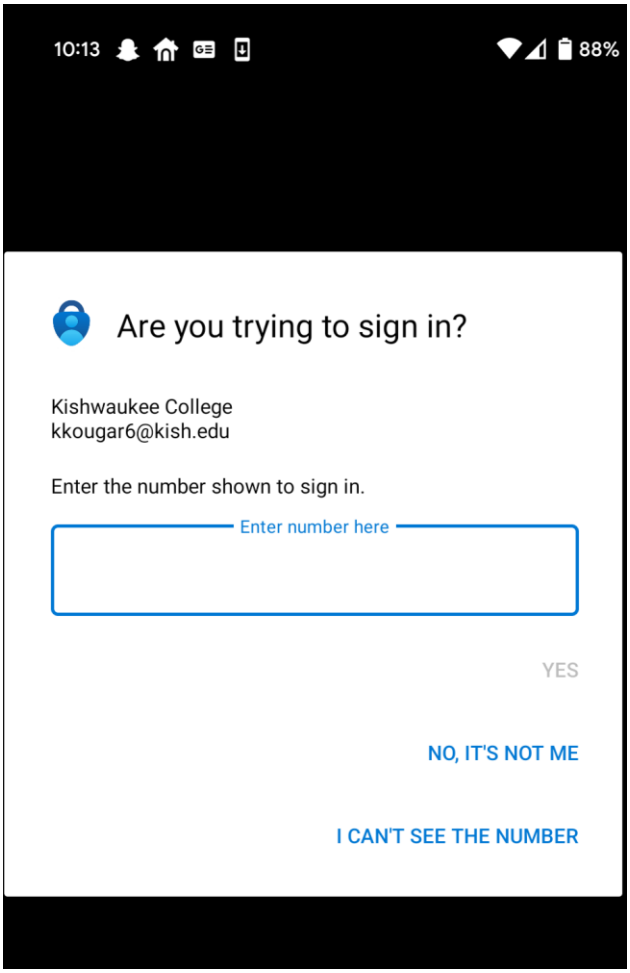
9 - Clicking Next to continue the setup



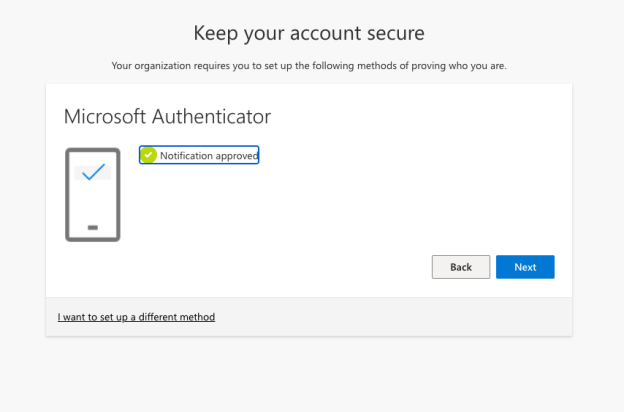
10 - Once the option is selected, you will be taken to the configuration screen for the app. This screen will display the QR code you need to scan to link your KishID account to your authenticator app.



11 - Once the accounts are linked, you should see the following prompt on the setup screen. You will enter that two digit code into the Authenticator app.



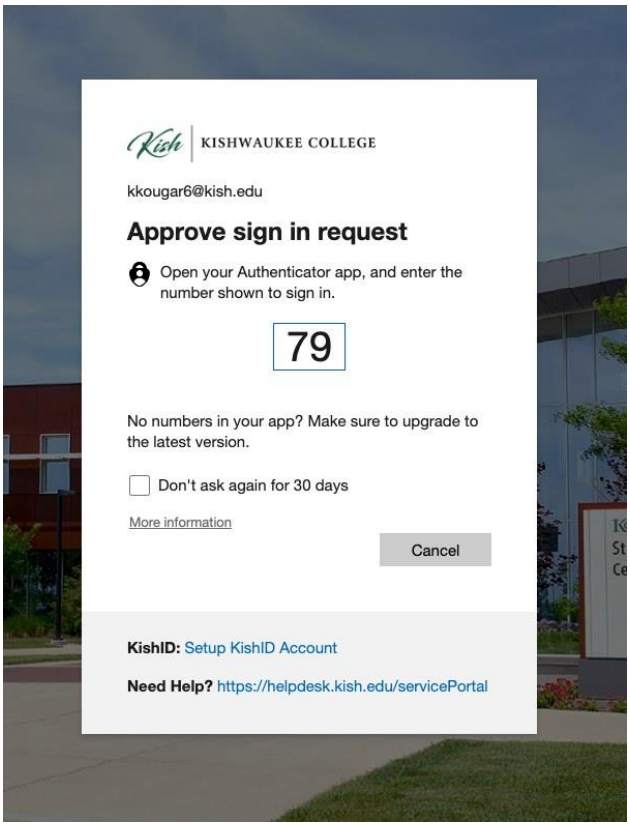
12 - This is what the prompt will look like on the mobile device



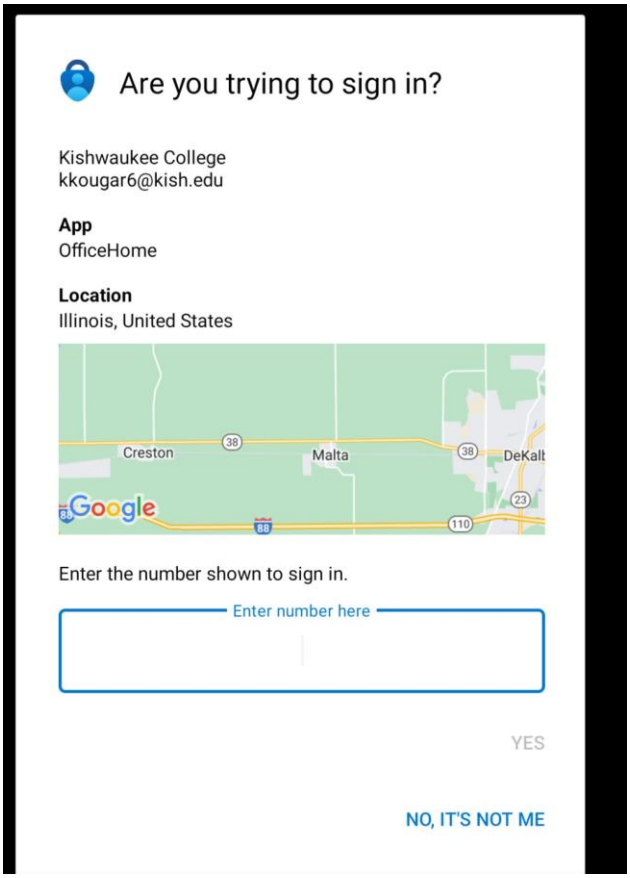
13 - Once the linking process has completed, you will receive a notice like this:

Clicking Next will complete the process. Your MFA setup is now completed.

What does a valid request look like?



14 - Notice the box that says Don't ask again for 30 days, clicking this box is a per-device setup. You will take this code on this screen to your push notification for the Authenticator app.



15 - On the push notification you can see what application is calling the MFA request and where the request is coming from. Note, depending on your Internet Service provider, this might not exactly show you the direct location, but within a small distance

NOTE: if you didn't make this request or the location is not near you or your ISP, mark this as "NO, IT'S NOT ME" and call the Kishwaukee College IT Helpdesk at 815-825-9888.