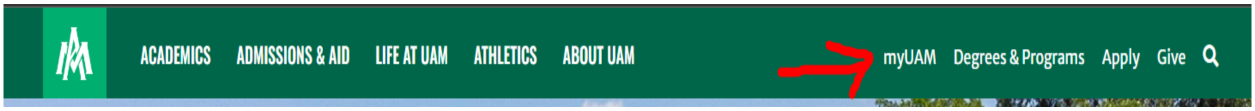
How To Set Up Your Multifactor Authentication Verification

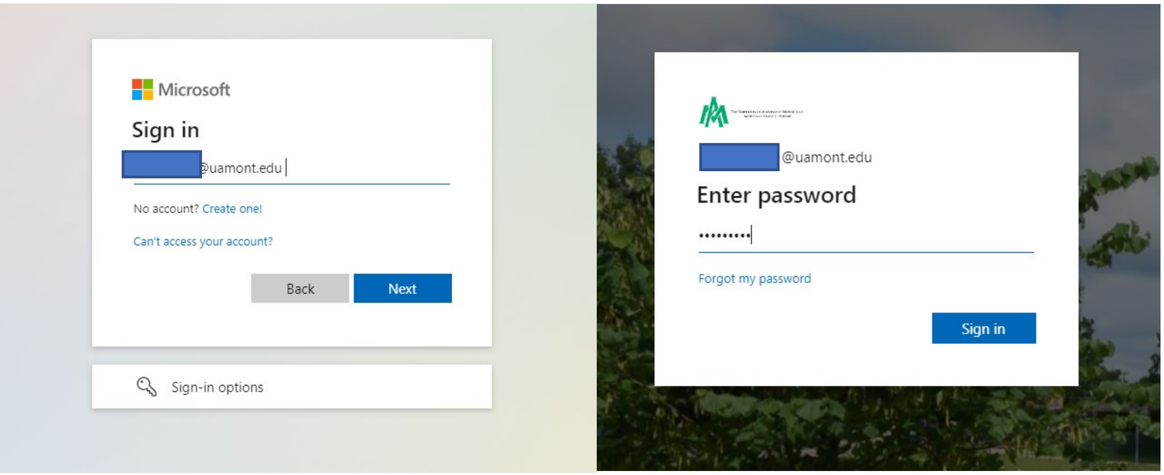
Multifactor Authentication is now being required on all Faculty, Staff, and Student accounts. Multi-Factor Authentication (MFA) is an additional layer of security that helps to protect your account. With MFA, you will be using something you know (your password) with something you have (your device/smartphone) to confirm your identity. MFA helps to better secure your email and other UAM resources by asking for a second form of authentication, which usually comes in the form of a notification from a mobile app, a text, or a call to your phone.

After MFA is registered on your account, you will have to log into your myUAM portal again. This also includes any Microsoft account that you are signed into on your desktop, phone, and/or tablet. For instance, if you use Outlook, Microsoft Teams, and OneDrive, you will have to sign back into all three services in all of the places where you use those services. When you log in, Microsoft does give you the option to trust the computer. If you check that box, Microsoft will not send an MFA notification for a period of time for the device you signed in on. Once some time has passed, you will have to log into everything again.

Step 1: Open Google Chrome and go to www.uamont.edu. On the UAM website, click on the myUAM portal link in the top right-hand corner of the page.



Step 2: Sign in with your UAM credentials (UAM E-Mail and UAM Password). Click "**Next**".


Microsoft

Sign in

[redacted]@uamont.edu

No account? Create one!

Can't access your account?

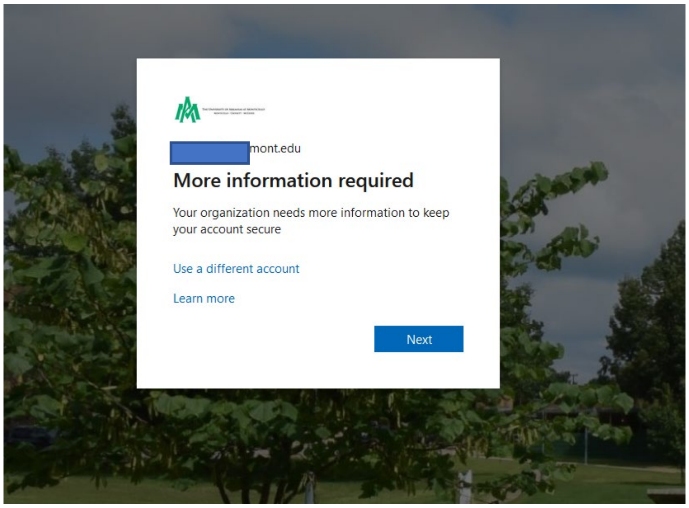
[redacted]@uamont.edu

Enter password

•••••••••

Forgot my password

Step 3: You should see an indicator saying “More Information Required”. You will now be prompted to set up your Multifactor Authentication. Click the “Next” button to continue.

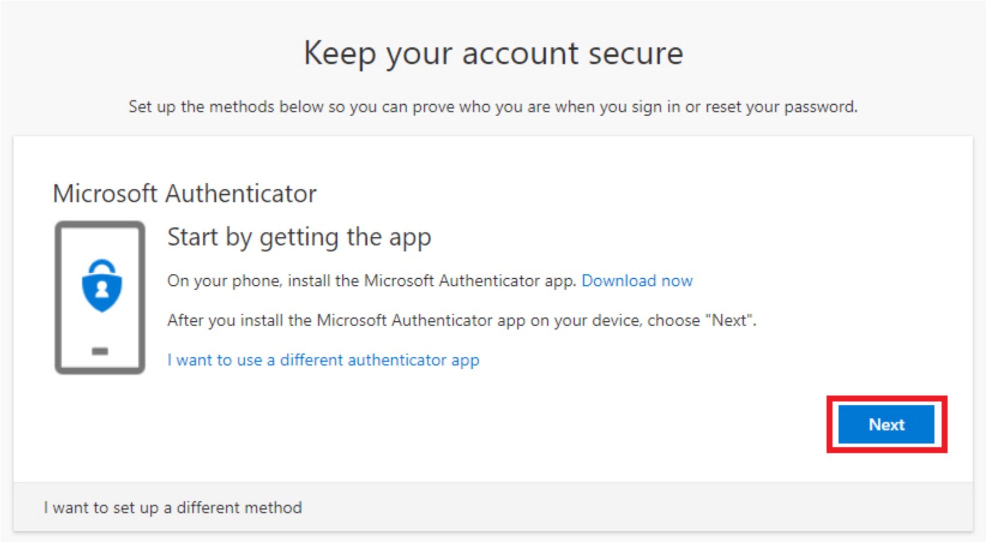


[redacted]mont.edu

More information required

Your organization needs more information to keep your account secure

Step 4: You will now be prompted to configure your Microsoft Authenticator App. **NOTE: Do NOT click the “Next” button until you have the Microsoft Authenticator App downloaded and ready to set it up. See Step 4 – A.**



Keep your account secure

Set up the methods below so you can prove who you are when you sign in or reset your password.

Microsoft Authenticator

Start by getting the app

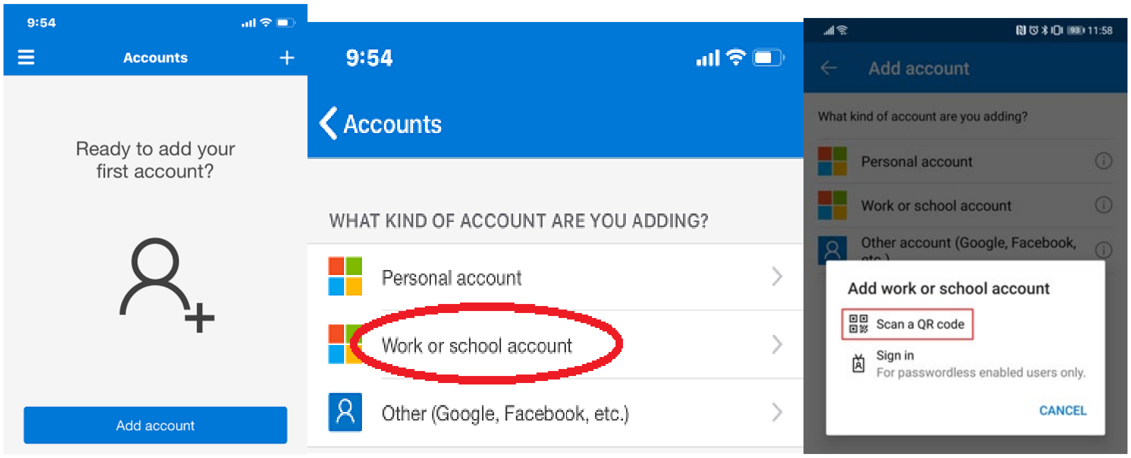
On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app
Next
I want to set up a different method

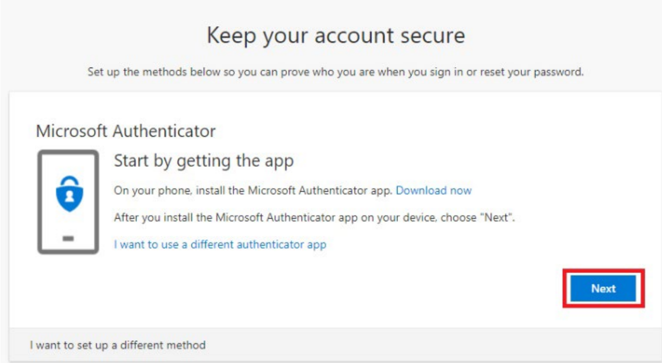
Step 4 - A: At this point, go to the Apple Store or Google Play Store on your mobile device. Download the Microsoft Authenticator app to your mobile device.

Step 4 - B: Open the app up on your mobile device. Click the **"Add Account"** button. Under "What Kind Of Account", click on **"Work Or School Account"**. Then click on the **"Scan a QR code"** button.



9:54
Accounts
Ready to add your first account?
Add account
9:54
Accounts
WHAT KIND OF ACCOUNT ARE YOU ADDING?
Personal account
Work or school account
Other (Google, Facebook, etc.)
11:58
Add account
What kind of account are you adding?
Personal account
Work or school account
Other account (Google, Facebook, etc.)
Add work or school account
Scan a QR code
Sign in
For passwordless enabled users only.
CANCEL

Step 4 - C: Going from Step 4, now you should be able to click the **"Next"** button to bring up the QR Code for you to scan. With your Authenticator app, scan the QR Code. You will then be prompted to approve the request. After that, you should see your account listed in your Microsoft Authenticator app on your mobile device.



Keep your account secure

Set up the methods below so you can prove who you are when you sign in or reset your password.

Microsoft Authenticator

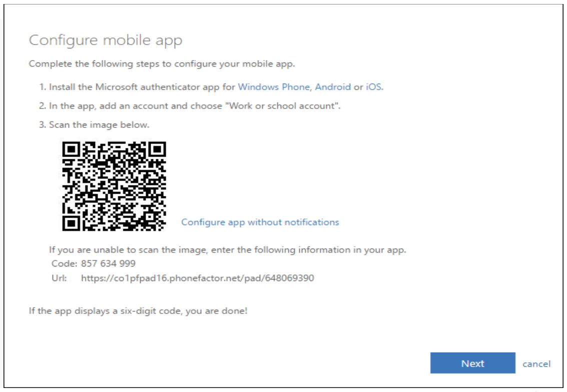
Start by getting the app

On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app

I want to set up a different method



Configure mobile app

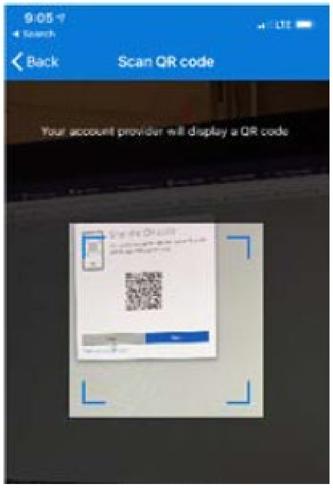
Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for Windows Phone, Android or iOS.
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.

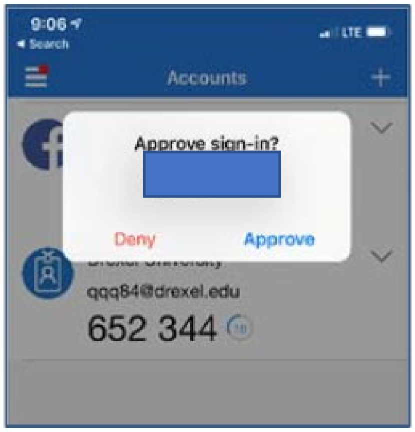
Configure app without notifications

If you are unable to scan the image, enter the following information in your app.
Code: 857 634 999
Url: https://co1pfpad16.phonefactor.net/pad/648069390

If the app displays a six-digit code, you are done!



Your account provider will display a QR code

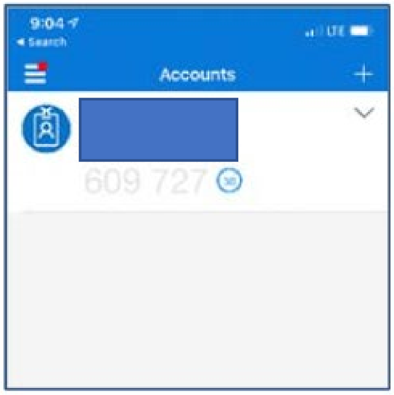


Approve sign-in?

[redacted]

qqq84@drexel.edu

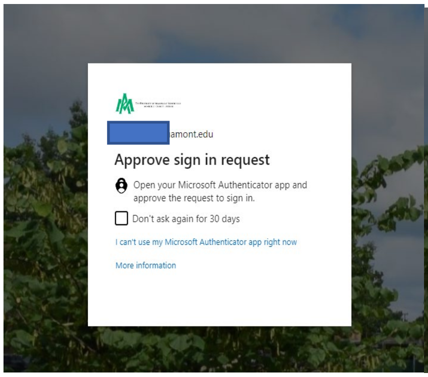
652 344



[redacted]

609 727

Step 4 - D: Verify your identity with your MFA method. On the Stay Signed In screen, if you are on a personal computer, you can select **YES** but if your using a public computer or someone else's computer then select **NO**.



[redacted]amont.edu

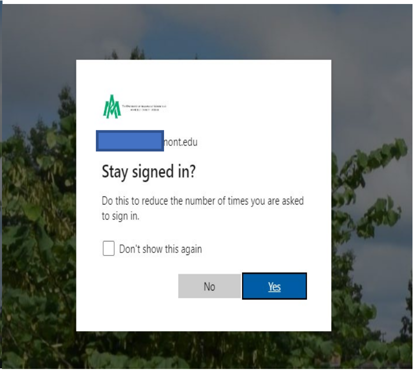
Approve sign in request

Open your Microsoft Authenticator app and approve the request to sign in.

□ Don't ask again for 30 days

I can't use my Microsoft Authenticator app right now

More information



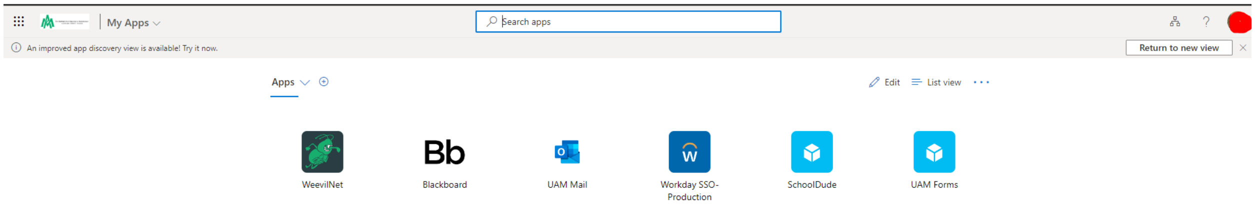
[redacted]ont.edu

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

Step 5: The following page will bring you to your "**MyUAM**" portal. You have now successfully set up your Multifactor Authentication



An improved app discovery view is available! Try it now.

Contact Information

Information Technology

Student Success Center 207
358 University Drive
P.O. Box 3626
Monticello, AR 71656
Phone: 870-460-1036
Fax: 870-460-1920

IT Support - UAM-ITHelp@uamont.edu
Blackboard - blackboard@uamont.edu
Report Spam - spam@uamont.edu
WeevilNet - weevilnet@uamont.edu
Workday - workdayhelp@uamont.edu