

**Multi-Factor Authentication is a security service that utilizes multiple forms of verification to log you in safely and securely to Microsoft on your devices. We strongly recommend using the Authenticator app, but it is possible to setup text verification at your discretion.**

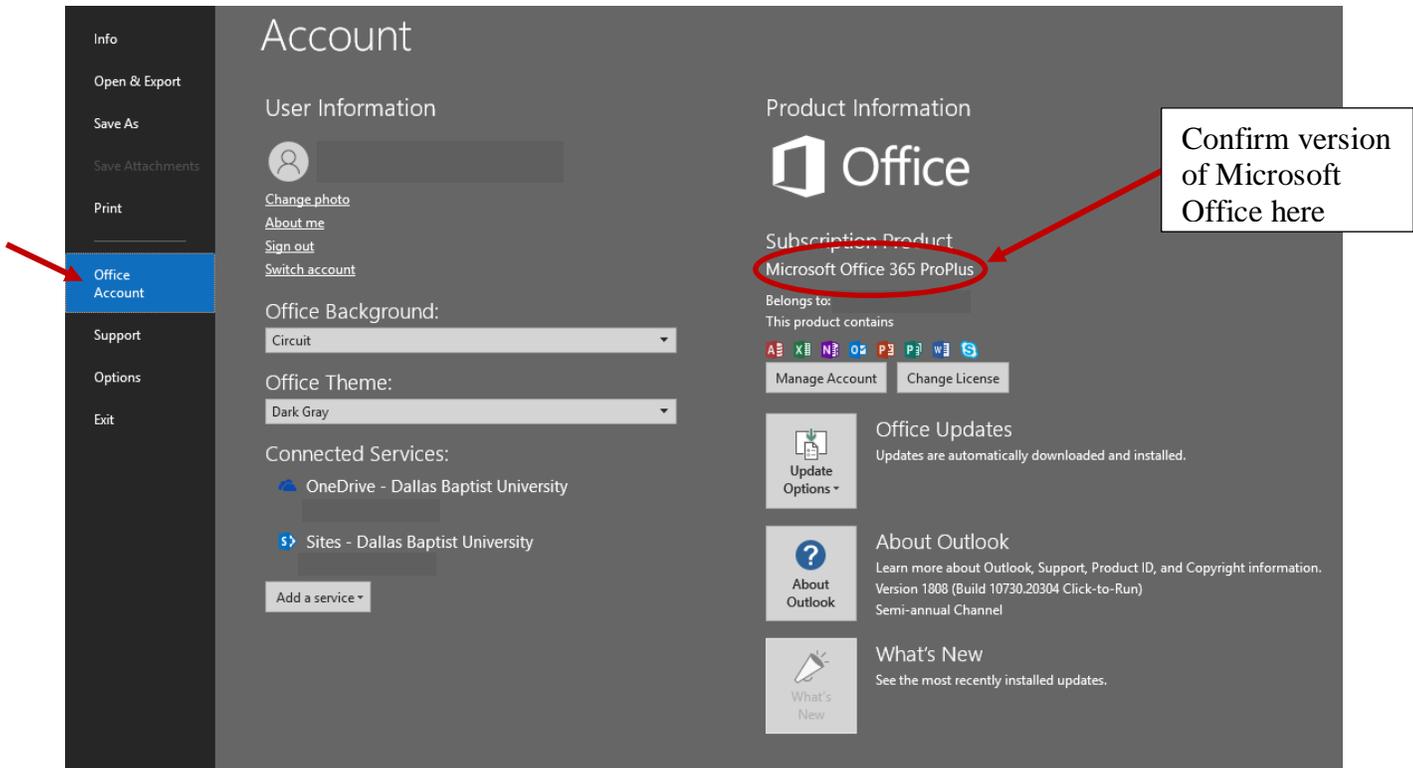
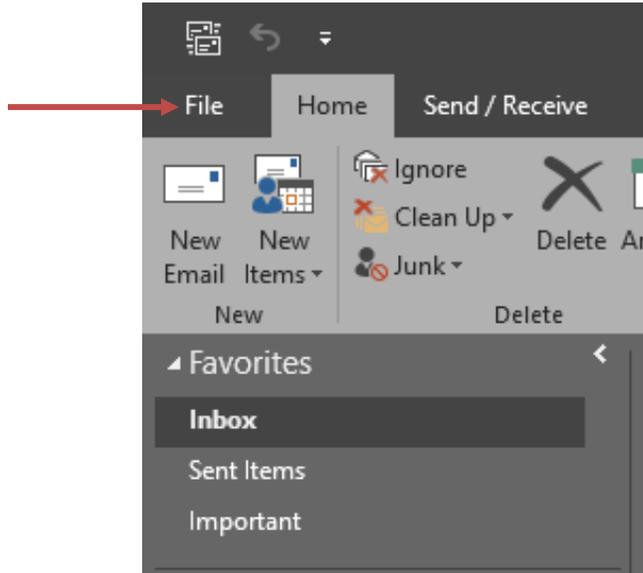
### What is Microsoft Authenticator - Video



### 1. Confirm Office 2016

**Before configuring this feature, your DBU workstation computer must have Office 2016 or newer installed. To confirm this, you can click on the File tab in the top left corner of Outlook, and then click "Office Account" or "Account" on the left pane. Under this menu, it should read "Microsoft Office Professional Plus 2016" or "Microsoft Office 365 ProPlus."**

**If the device runs an older version of Office (2013, 2010, etc.), please call the I.T. Help Desk @5500 to request a newer version.**



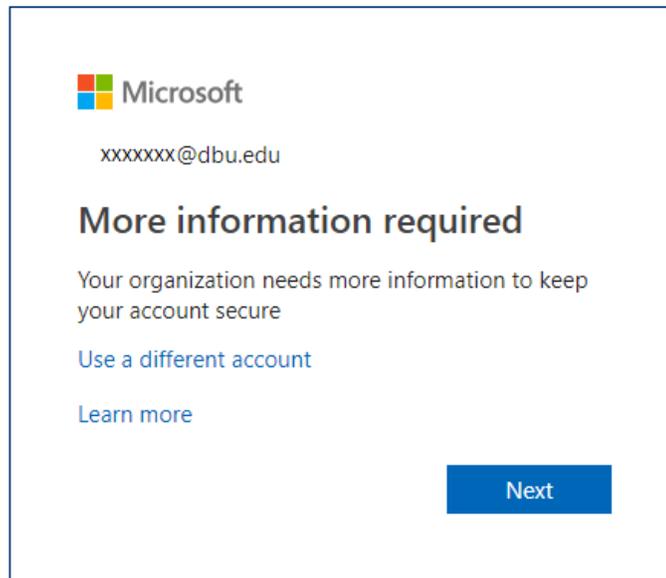
---

## 2. Setup

---

In your web browser, navigate to the webpage [Portal.Office.com](https://portal.office.com) and sign in using your DBU employee credentials (your user ID must be your full email address). Once logged in, you should be prompted to setup multi-factor authentication. On this menu, click "Next."

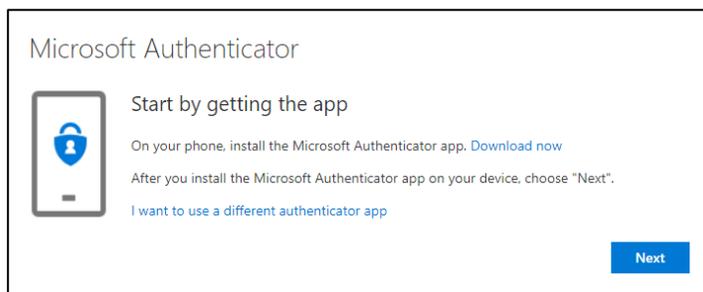
---



---

During setup, you will be prompted to download the Microsoft Authenticator app from your mobile phone's app store.

---



---

Upon opening the Microsoft Authenticator app, you should now be prompted to continue the setup.

---

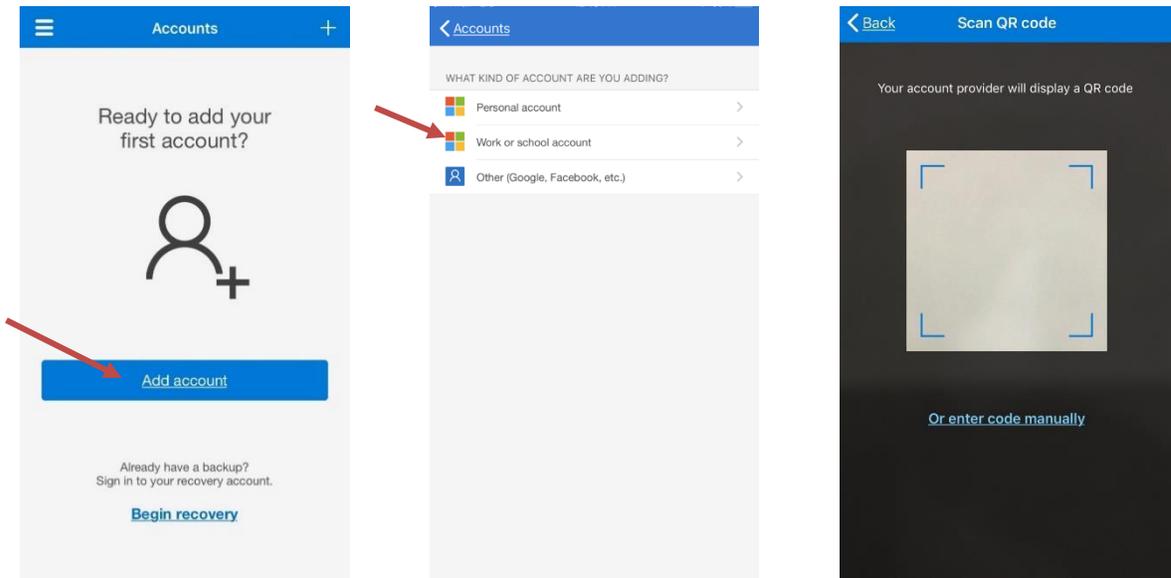
---

### 3. App Setup

---

Once the app is uploaded to your phone, select the button to “Add account,” and select “Work or school account,” which opens the camera to scan the QR code provided on your computer display.

---



Your unique QR code will be displayed on the monitor at this time. Scan the QR code with the scanner displayed on your mobile phone.

### Microsoft Authenticator



Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

[Can't scan image?](#)

[Back](#) [Next](#)

Once you scan the QR code displayed on your monitor, a notification should be sent to your authenticator app to verify authentication for the first time. Select "Approve" to continue setup.

### Microsoft Authenticator



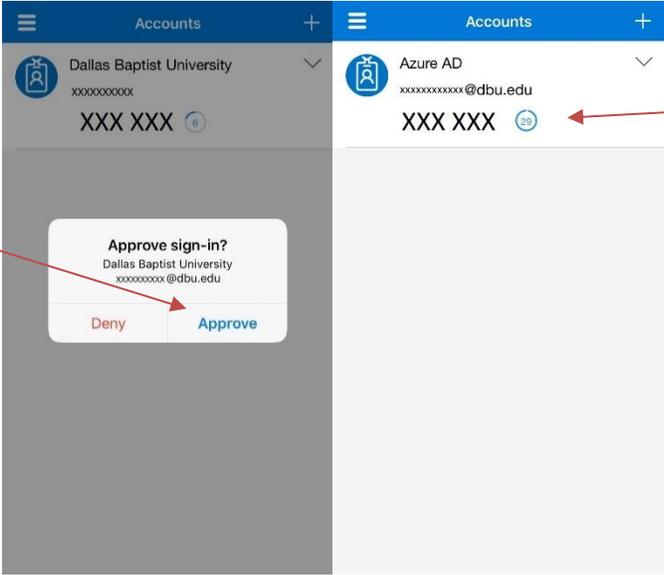
Let's try it out

Approve the notification we're sending to your app.

[Resend notification](#)

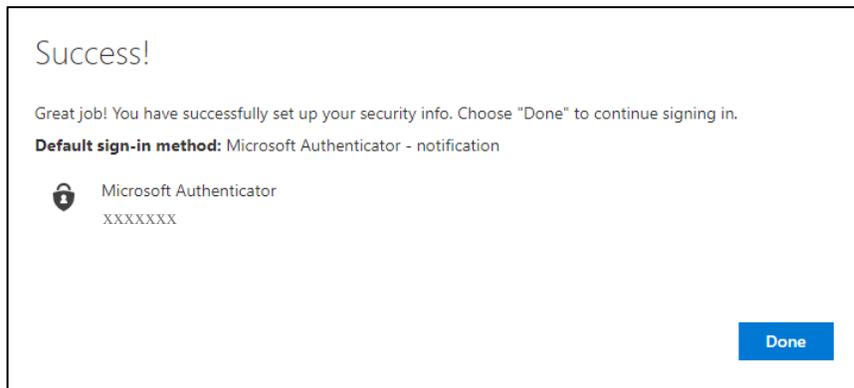
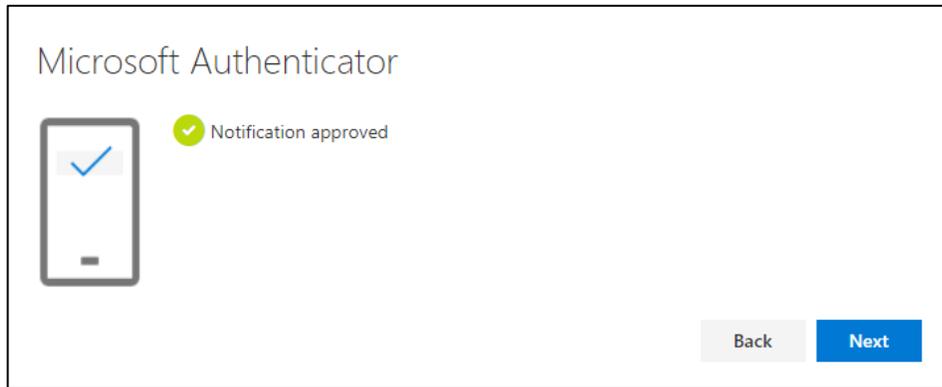
[Back](#) [Next](#)

Authenticator notification



Timed passcode

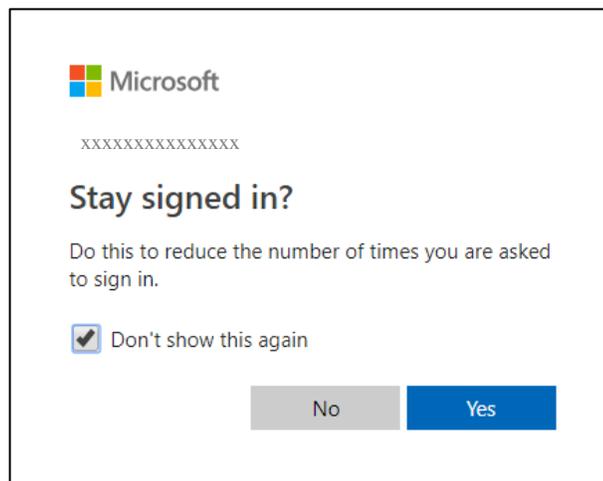
\*This small timer next to the six-digit passcode indicates the remaining seconds until the passcode expires and resets.



---

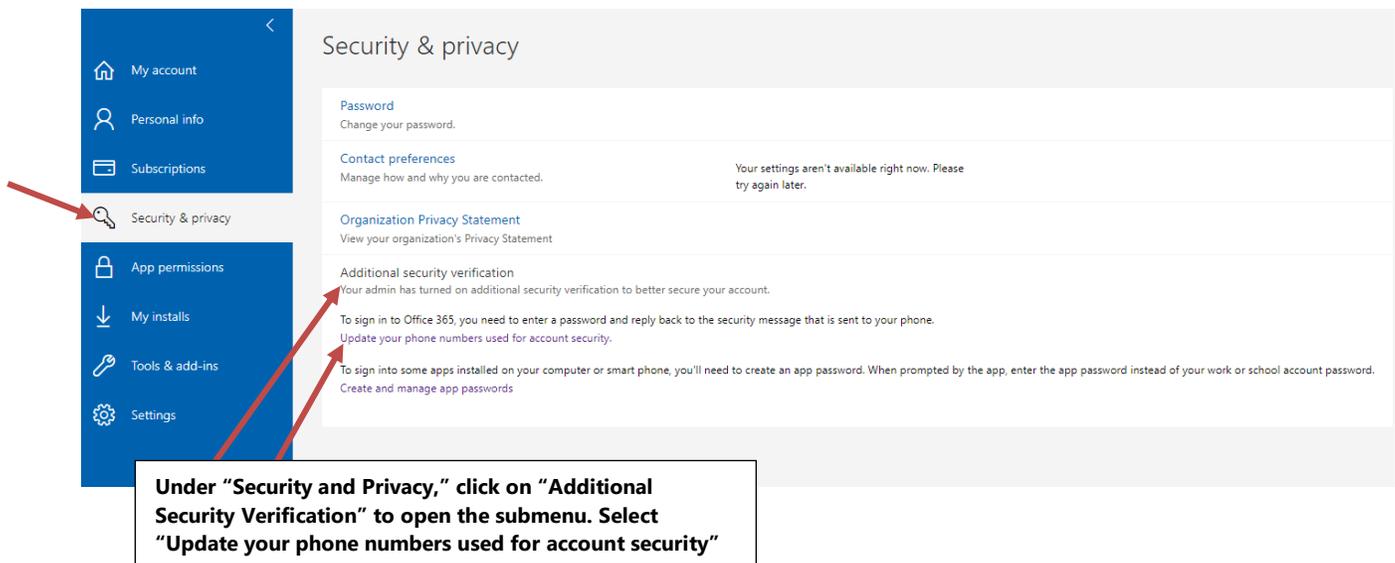
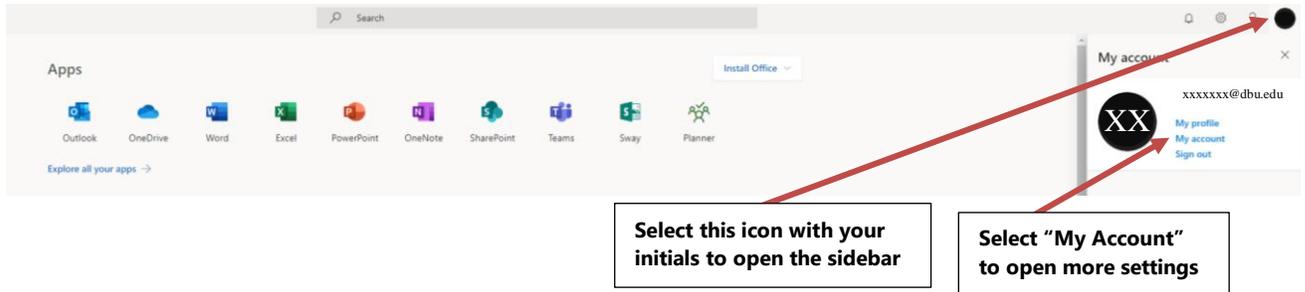
**After completing setup, you can select to keep your device or browser signed in to reduce number of times you are asked to sign in.**

---



## 4. Additional Security Verification

It is suggested that you also setup an additional verification method should you lose access to your mobile device. You can do this after setup by returning to [Portal.Office.com](https://portal.office.com) and configuring your settings for authentication. You can add a separate number under authentication that will be contacted in the event that your mobile device is inaccessible. Please do not use your office phone number as this alternate contact method.



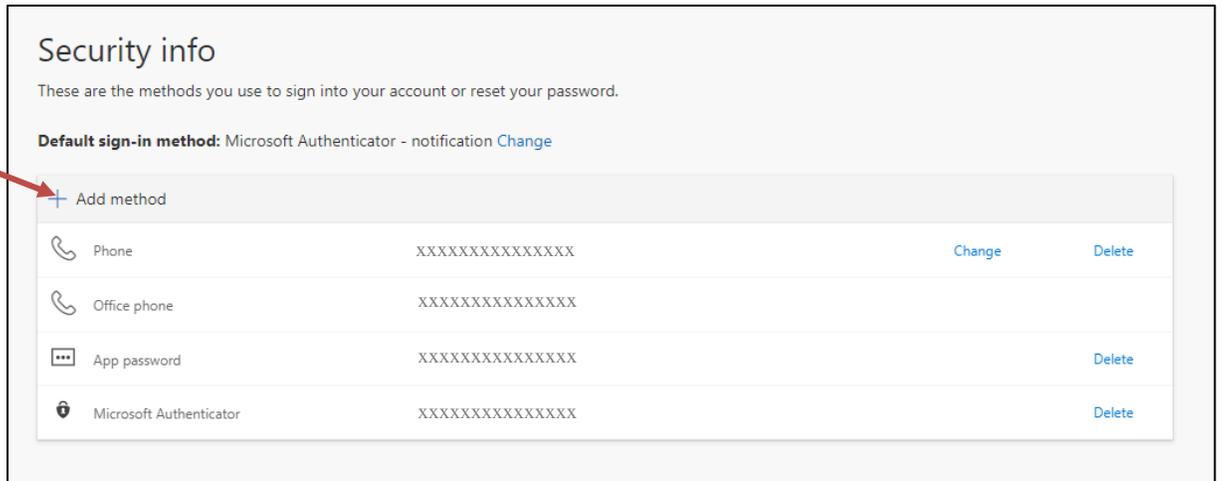
While it may seem convenient to use your office phone as your alternate authentication phone, we recommend using a more readily accesible phone (friend or spouse's phone) for the purpose of being able to login to Microsoft while outside of the office, especially in the case of emergencies.

**Example:** It is 2:00 a.m. and you have to take your child to the emergency room, but you've forgotten your cell phone at home in the rush. You need to send an email through Outlook on your spouse's device to alert your supervisor that you will not make it into the office that day. Having already confirmed your friend or spouse's phone will allow you to login to your account. Setting your office phone as your alternate authentication method is not practical in this situation.

---

Select the button to "Add Method." Using the drop down menu, select the method that you would like to use to verify authentication. In this case, you would select "Alternate phone."

---

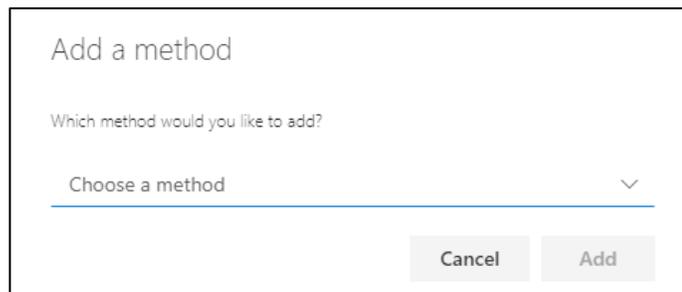


**Security info**  
These are the methods you use to sign into your account or reset your password.

**Default sign-in method:** Microsoft Authenticator - notification [Change](#)

[+](#) Add method

Phone	XXXXXXXXXXXXXXXXXX	<a href="#">Change</a>	<a href="#">Delete</a>
Office phone	XXXXXXXXXXXXXXXXXX		
App password	XXXXXXXXXXXXXXXXXX		<a href="#">Delete</a>
Microsoft Authenticator	XXXXXXXXXXXXXXXXXX		<a href="#">Delete</a>

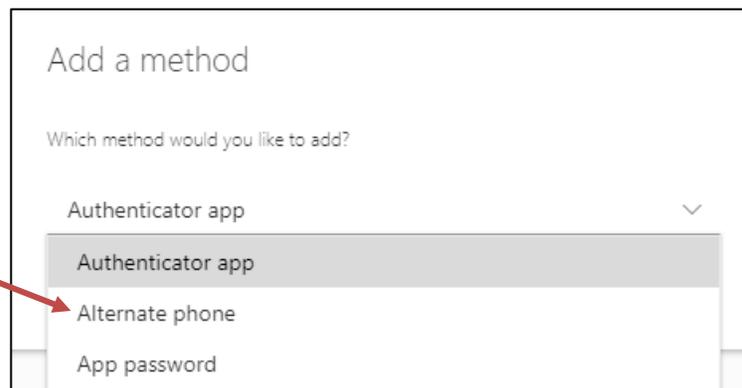


**Add a method**

Which method would you like to add?

Choose a method ▼

[Cancel](#) [Add](#)



**Add a method**

Which method would you like to add?

Authenticator app ▼

- Authenticator app
- Alternate phone**
- App password

---

**Input the number that you would like to use as your alternate phone number for authentication verification. Select "Next" and a call will be made to the alternate device.**

---

Phone

You can prove who you are by answering a call on your phone.  
What phone number would you like to use?

United States (+1)

Call me

Cancel Next

Phone

We're calling xxxxxxxxxxxx now.

Back

---

**Follow the instructions on the call and the call should finish by saying "your sign-in was successfully verified." The menu on the screen will change to display the following message and your alternate device will now be registered.**

---

Phone

Call answered

Done

Ensure your default authentication method at the top of the "Security info" page is set to the option that reads "Microsoft Authenticator – notification," for ease of use, the authenticator app will send a notification that can be approved when prompted to verify authentication. Follow the steps below to change the default options on how you would like to be notified upon login.

Security info

These are the methods you use to sign into your account or reset your password.

**Default sign-in method:** Microsoft Authenticator - notification [Change](#)

+ Add method			
Phone	XXXXXXXXXXXXXXXXXX	<a href="#">Change</a>	<a href="#">Delete</a>
Office phone	XXXXXXXXXXXXXXXXXX		
App password	XXXXXXXXXXXXXXXXXX		<a href="#">Delete</a>
Microsoft Authenticator	XXXXXXXXXXXXXXXXXX		<a href="#">Delete</a>

Change default method

Which method would you like to use to sign in?

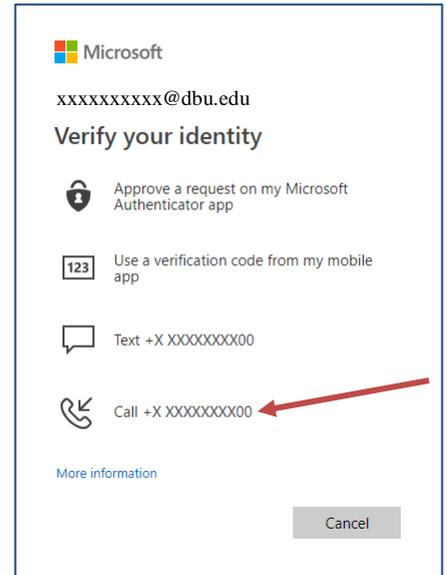
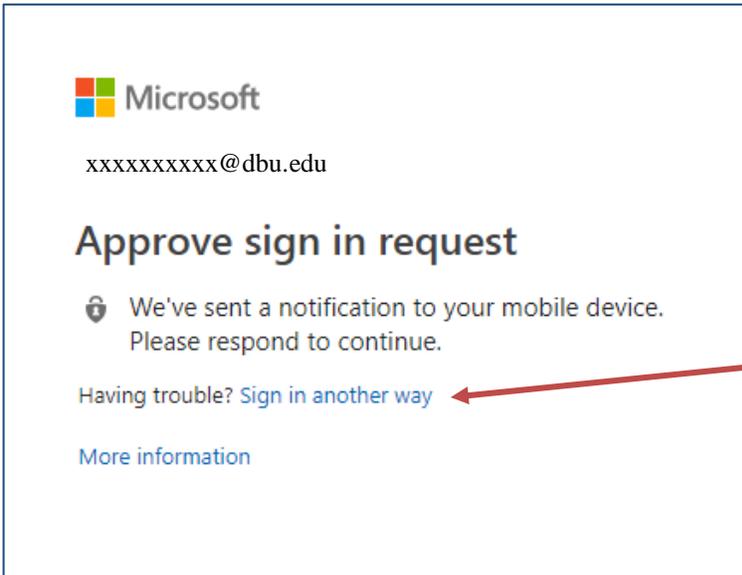
Microsoft Authenticator - notification

- Phone - call XXXXXXXXXXXXXXXXXXXX
- Phone - call XXXXXXXXXXXXXXXXXXXX
- Phone - text XXXXXXXXXXXXXXXXXXXX
- Microsoft Authenticator - notification**
- Authenticator app or hardware token - code

---

If you need to use an alternate method of verification when prompted to authenticate after signing in, select "Sign in another way" and choose the method you'd like to use to verify authentication.

---



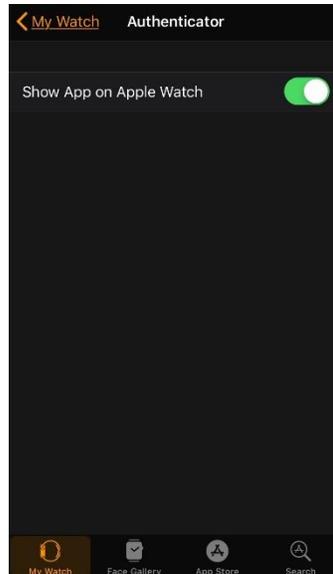
---

## 5. Apple Watch Setup

---

If you have an Apple Watch, you can setup Microsoft Authenticator on your Apple Watch to receive notifications to approve authentication. Once you have setup the Microsoft Authenticator app to your iPhone, you may need to manage your smartwatch's apps from the Watch app.

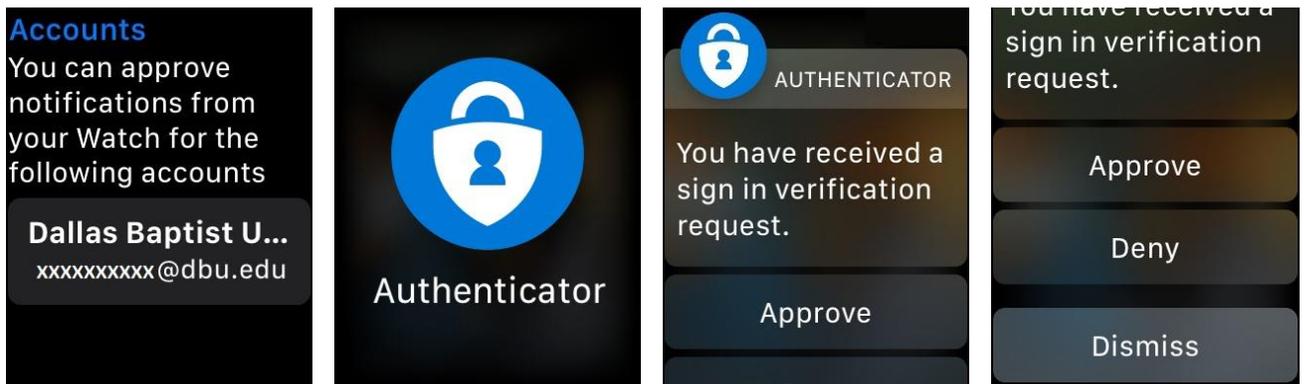
---



---

Once downloaded to your Apple Watch, the app should automatically receive access to your account. You will now receive notifications to your smartwatch that you can approve.

---



---

If you need assistance with other brands/types of smartwatches, please contact the I.T. Help Desk @5500.

---