DUO Two-Factor Authentication for Faculty and Staff

Duo mobile is for faculty and staff
Students will use Microsoft's Authenticator App

Setting up a New Phone for DUO
Change your DUO Settings/Options
Getting Started with DUO for the First Time
Using DUO with a Hardware Token

Already have DUO and just need to edit your settings?

Step 1: Login in at https://myaccount.millersville.edu/duo using your short username and password.

Step 2: Select to have DUO call you or text you a passcode

Getting started with DUO for the first time:

Step 1: You will get the message below when you try to sign in to Millersville resources.
Step 2: Next, you'll be asked to identify which device you will be adding for this example we chose mobile phone.

Step 3: Enter your phone number starting with the area code. The form will validate your phone number and then prompt you to approve the phone number again to continue.

Step 4: Next, specify the type of phone that is associated with your phone number:
Step 5: Install the DUO Mobile app on your mobile device. In our example, Duo Mobile for iOS will be installed from the Apple App Store.

Step 6: Here is the DUO Mobile for iOS product QR code which allows me to scan and download the app directly in your app store.

Step 7: Here is the DUO confirmation the app was successfully installed on your device.
Step 8: Please click "Allow" at the prompt "Duo Mobile' Would Like to Send You Notifications"

Step 9: Finally, confirm your device information, select "Automatically send this device a Duo Push" and then click the "Finish Enrollment" button

Step 10: Choose your authentication method:
Send me a Push (Local Wi-Fi or Cellular data needed)

- Smart Phone needed with the Duo Mobile App installed and configured.
- Note: In Settings it can be setup to automatically send you a push, thus saving you a step.
- This is the recommended way to use Duo MFA.

Call Me (Phone service needed. May not work out of country or if you swap SIMs)

- Any phone number that you can answer while attempting to logon.

Enter a Passcode

- Two options here
  - The Duo Mobile App generates these codes and you may enter it in in the field provided.
    - Can be used anytime, even when device is completely offline.
    - These codes are often called One Time Passwords or OTP.
  - Alternately you can have it text you a code via SMS text service on most mobile phones.

New Device:

Go to office.com or any webpage that prompts for a Duo Push authentication and sign in. Use incognito or private browsing, if necessary to get prompt.
If you **have your old device** you can use either “Send Me a Push” or “Enter a Passcode” to get the new device added.

If you **no longer have the old device**, but, you still have the same phone number use "Call Me".

Additional information can be found on Duo’s website: [https://guide.duo.com/prompt](https://guide.duo.com/prompt)

---

**Using DUO with a hardware token**

Tokens are only available for active MU faculty, staff, and administration.

To authenticate using a hardware token, click the "**Enter a Passcode**" button. Press the button on your hardware token to generate a new passcode, type it into the space provided, and click "**Log In**". Using the "Device:" drop-down menu to select your token is not necessary before entering the passcode.

If you have Duo automatically sending a push or calling you, press the X in the lower right corner of the Duo prompt, then enter the code from the hardware token.
Token FAQ

What is a Duo Multi-Factor Authentication (MFA) token?

A Duo MFA token – or hardware token, physical token, or “fob” – is a piece of hardware that is used to authenticate when a person is not using a phone to authenticate on the MFA service. The token is a small, battery-powered device that is usually attached to your keychain. Pressing a button on the token will display a code on the built-in display. (Note: usage of Duo Mobile generated passcodes on a token does not require cellular or Internet service on your phone.)

Who should have a Duo MFA token?

No one is required to have a Duo MFA token, and most people will not want (or need) a token. Only in special cases (when a phone cannot be used for MFA) should a token be used. (Note: using a phone (mobile and/or landline) is the preferred way to use Duo for greater security, having one fewer “thing” to keep track of, battery life, etc. Therefore, only in limited cases will a token be needed or required.)

How do Duo MFA tokens work?

A Duo MFA token generates a different series of digits each time that the token is used (button is pressed). To authenticate using a hardware token, click the “Enter a Passcode” button in the Duo MFA authentication prompt. Press the button on your hardware token to generate a new passcode, type it into the space provided, and click “Log In”. (Note: Using the “Device:” drop-down menu to select your token is not necessary before entering the passcode.)

Is there a charge for the Duo MFA token?

There is no charge for the initial Duo MFA token. If the token is lost there will be a replacement fee of $15

Where can Duo MFA tokens be obtained?

Duo MFA tokens will be issued via appointments scheduled through the MU IT Help Desk. To be issued a token, a person will need to visit a location and provide identification.

What if I need a replacement Duo MFA token?

If the Duo MFA token isn’t working, please verify that it is truly malfunctioning by attempting to troubleshoot (examples below). The following are signs that a token needs to be replaced:

- Battery is completely
- No digits (or some but not all digits) display when requesting a passcode (by pushing the button on the token).
- Button does not display a passcode when pressed or does not release when pressed

If any of the above symptoms are present, contact the Help Desk to arrange for a replacement.

Why does Duo say my passcode is invalid when I am entering it correctly?
The Duo token may go out of sync and not work correctly under certain circumstances. This error usually occurs when you have not used your Duo token device for an extended period of time.

It also may occur when you repeatedly press the button on a token (approximately 20 generated codes) and do not use the generated passcodes for authenticating successfully. This causes the token to fall out of sync. Note: this issue can happen inadvertently if you keep your token in your pocket or purse and the token button is pressed continuously against other objects. Should this happen, you may be able to re-sync the token device yourself by attempting to login with three consecutively generated passcodes. On the first and second tries, enter the generated passcodes but Duo MFA will say the passcodes are invalid. On the third try, enter the generated passcode and you will then be allowed to proceed. If this method does not work, please contact the MU IT Help Desk at: 717-871-7777 or help@millersville.edu.

I'm leaving the University. Do I have to return my Duo MFA token?

If you are leaving the University (retirement or termination), then you should return your Duo MFA token to MU IT for re-distribution.

Setting up a New Phone for DUO
Change your DUO Settings/Options
Getting Started with DUO for the First Time
Using DUO with a Hardware Token