

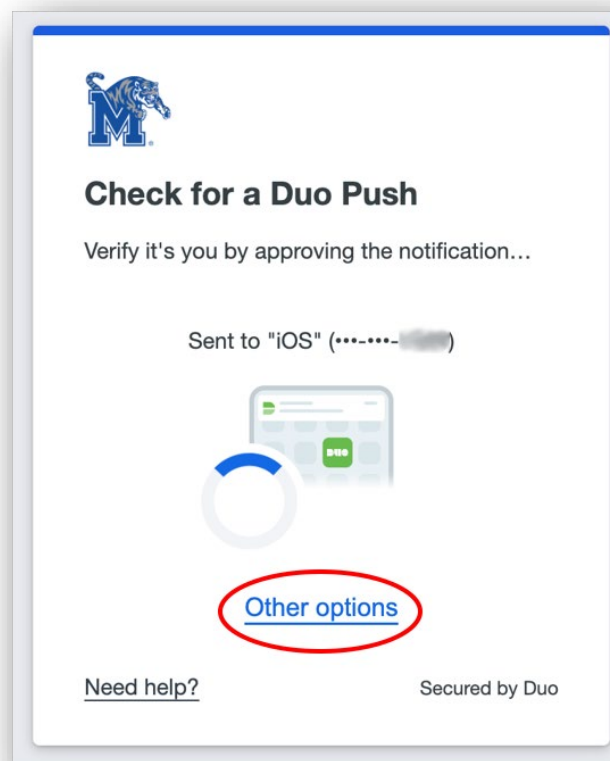
Duo Passkey Creation

A passkey is an authentication method that uses your device to verify your identity. A passkey might use your device's fingerprint scanner or camera to identify you.

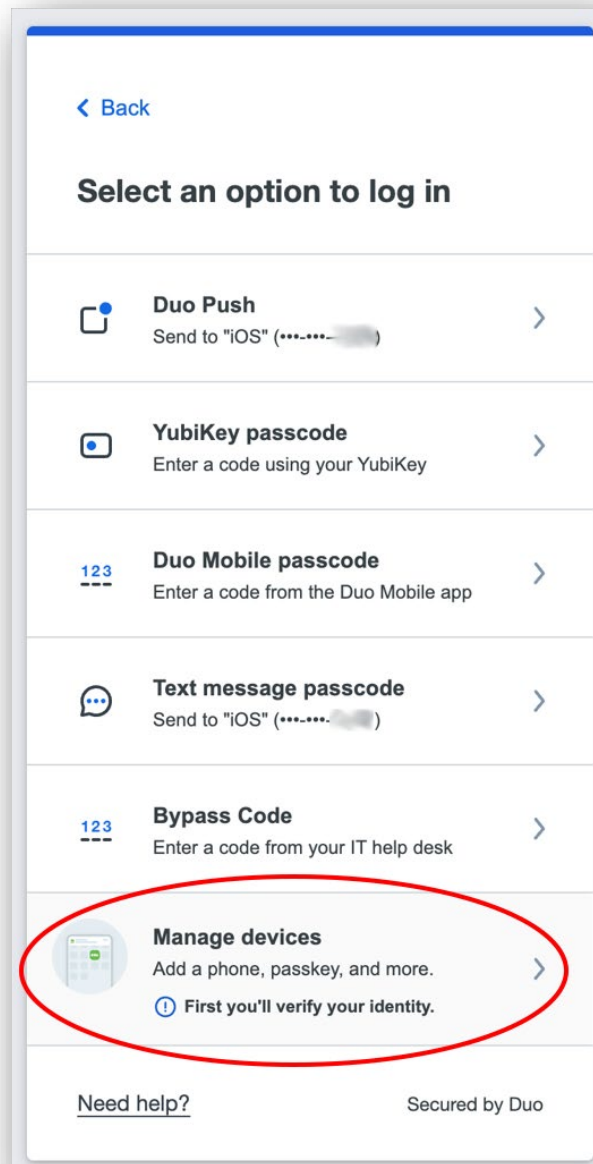
In most cases, a passkey can only be used on the device where it was created. Some passkeys, such as Touch ID and Windows Hello, are available system-wide and can be used for multiple apps or programs. Other passkeys may be specific to a particular app or software (e.g., a password manager or browser). In the latter case, the passkey you set up will not work for other apps.

To set up a passkey for Duo on your device, you'll need to initiate a Duo prompt and access the device management dashboard. **Be sure to use the device and/or app for which you want to create the passkey.** This process must be repeated for new passkeys on each device (or each app if using a software-specific passkey). To force a Duo prompt and create your passkey:

1. Open a new browser session (e.g., a browser you haven't used recently to access your UofM account or a private browser window)
2. Visit a webpage that requires signing in to your UofM account. For example, <https://iam.memphis.edu>
3. Enter your username and password.
4. You will see the usual Duo prompt. Do not approve or deny the request as you normally would. Instead, click or tap the "Other options" link at the bottom of the prompt window.

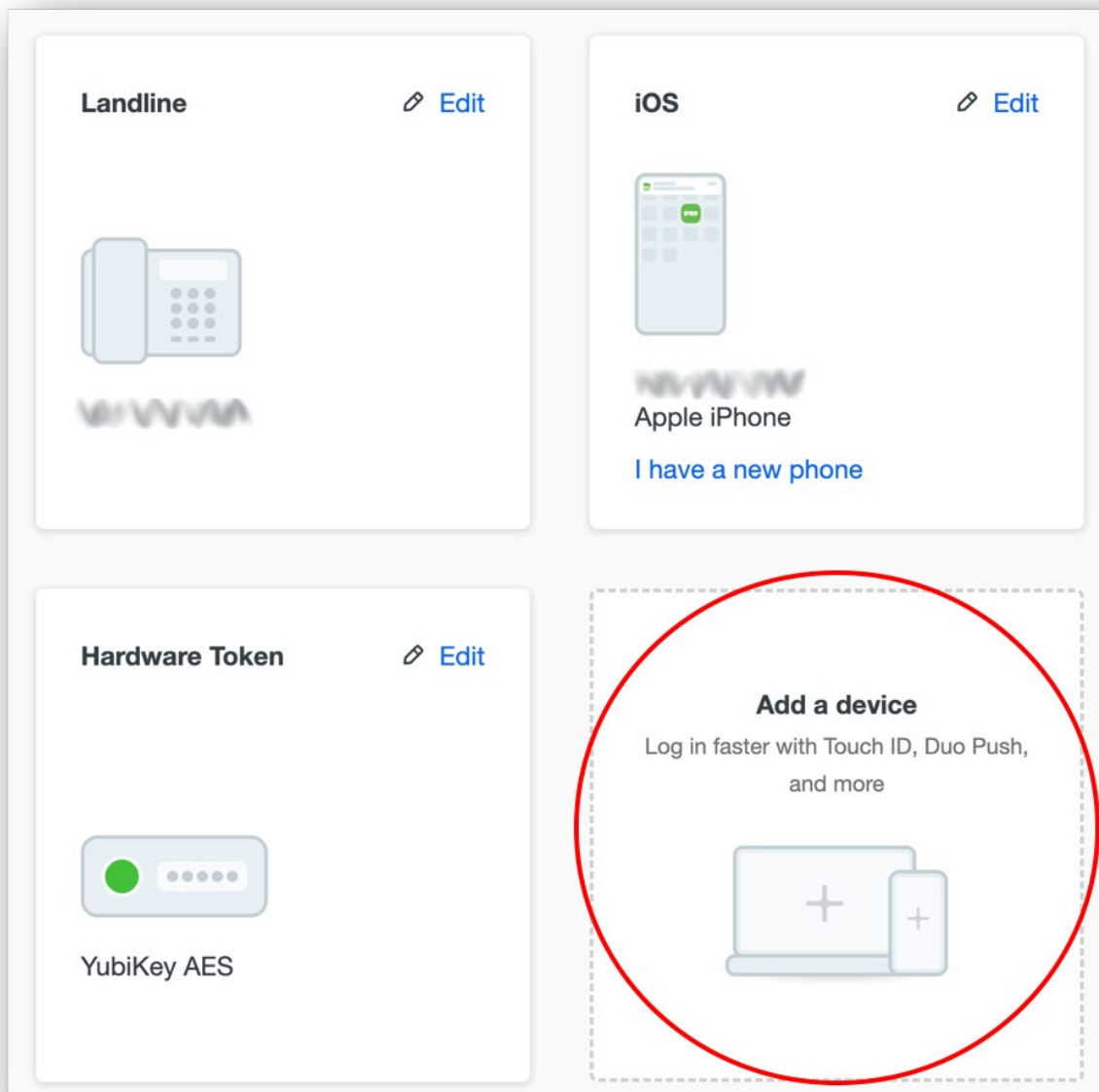


5. You will then see a list of your current authentication options. Select the “Manage devices” option at the bottom of the list.

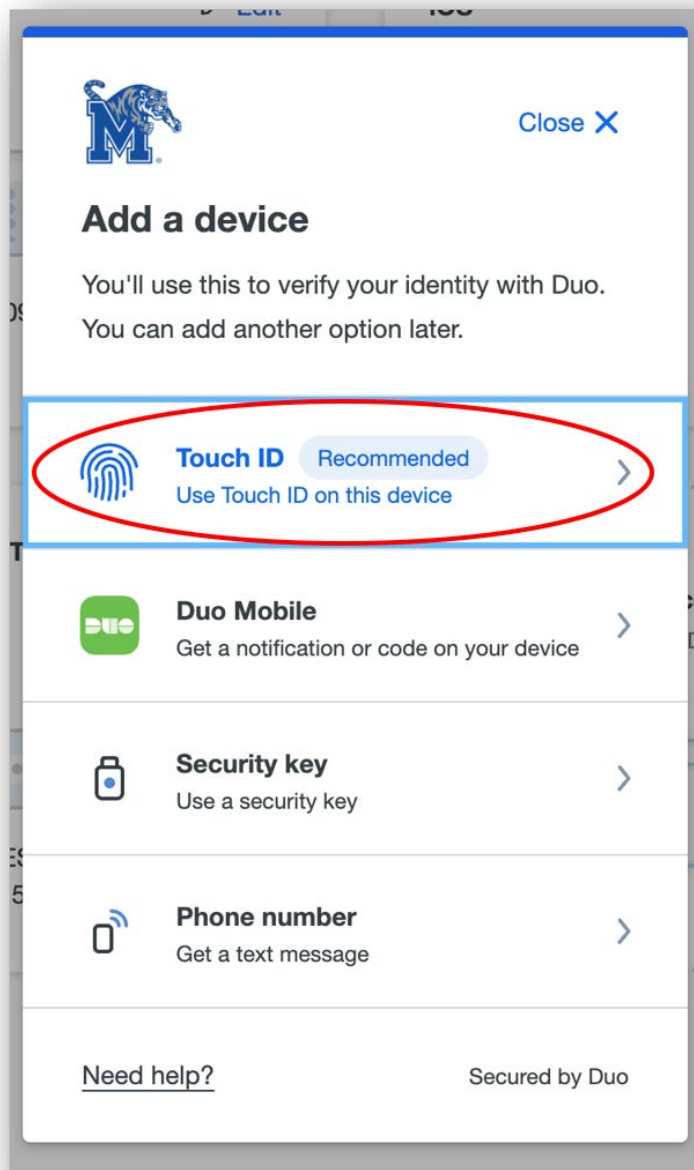


6. Another Duo prompt will appear to verify your identity before accessing the device management screen. Select your verification method and approve the request to continue.

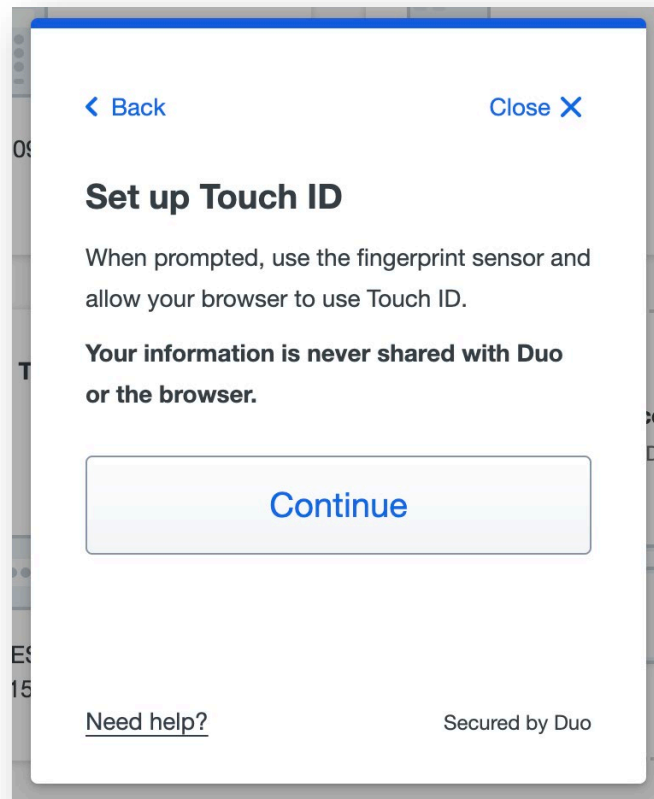
7. Next, you will see the Duo device management screen. This lists all the devices you have previously set up for Duo authentication. To add a passkey, select the “Add a device” option at the end of the list.



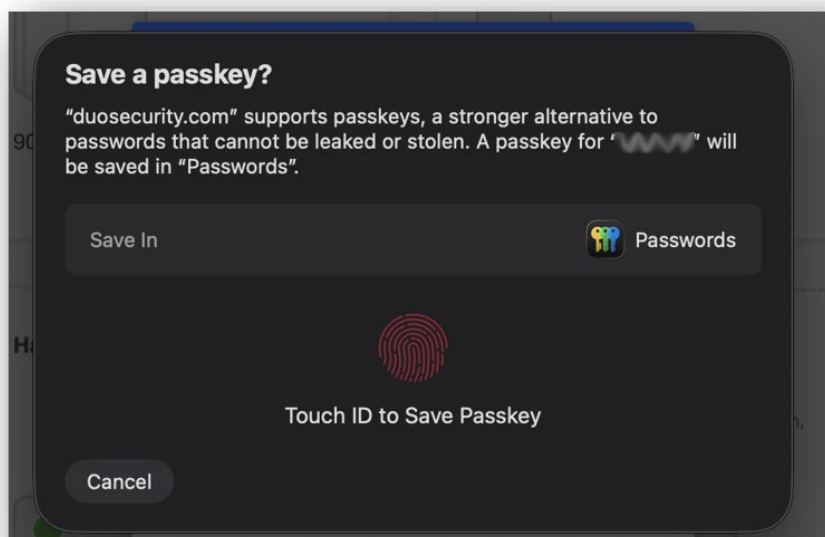
8. Select the appropriate option to create a passkey on your device. For example, to use your fingerprint on an iOS device, choose Touch ID.



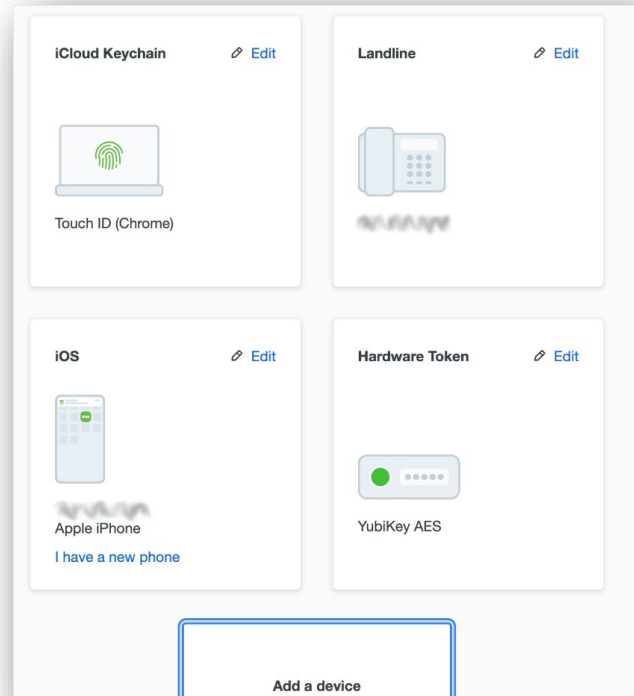
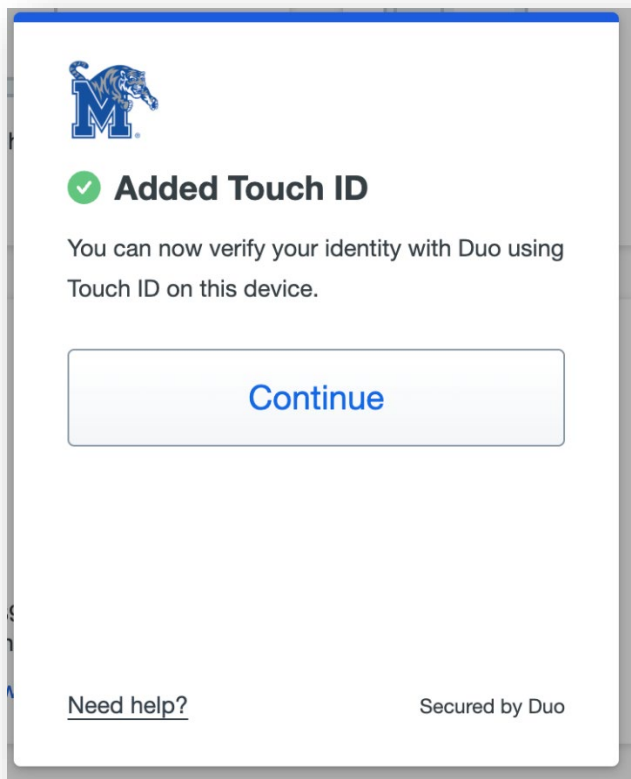
9. On the next window, click “Continue” to confirm and proceed.



10. The next screen you see will be specific to the device you are using. The example below is Touch ID for macOS. Your device will prompt you to create a passkey using your selected method. Follow the directions to create your passkey.

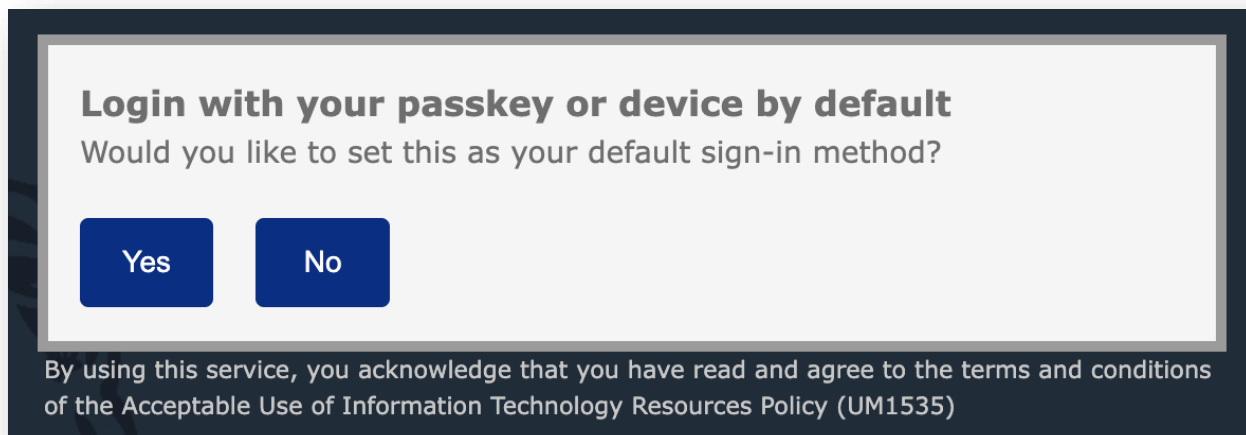


11. Duo will display a confirmation that your new device was added. Click or tap “Continue” to return to the device menu. You will see your new passkey at the top of the device list. You may now use this option to approve Duo authentication requests.



You may exit the browser window or click “Back to login” at the top of the screen to sign in to your selected UofM resource in the current browser.

12. The first time you log in with your passkey, you will see an option to make the passkey your default Duo device. Selecting “Yes” will automatically bring up your device’s passkey screen at next login.



Duo Passkey FAQ

Why doesn't my passkey look like the screenshots above?

Passkeys are available across a wide variety of devices and software. Your passkey might look different depending on which provider, device, software, and method you choose. For assistance setting up your preferred passkey, consult the support documentation available from the company that provides it or read [Duo's passkey documentation](#).

Why doesn't my Duo prompt match my passkey method? (e.g., Duo asks for a fingerprint scan but I don't have a scanner.)

Because passkeys can vary widely across devices and software, Duo may not display the exact authentication method you use to create your passkey. You should follow the prompts given by your chosen passkey software.

Why isn't my passkey working?

In most cases, a passkey can only be used for the device on which it was created. For example, if you created a passkey on your phone, it won't work on your laptop. Some passkeys are specific to an app (e.g., password managers or browsers). These app-specific passkeys will not work for other apps or programs.

If you set a passkey as your default authentication method, Duo will attempt to initiate that passkey each time you log in. If you attempt to log in using a different device (or app in some cases), your default passkey will not work. You will need to choose a different authentication method for Duo.

If you wish to create different passkeys for multiple devices or apps, follow the instructions above for each new passkey.

Why isn't Duo automatically using my default passkey?

In most cases, Duo will attempt to initiate the last authentication method you used. When you create a new passkey and use it to log in to your UofM account, you will have the option to set it as your default method. Occasionally, Duo may revert to a different authentication method, even if you have set your passkey as the default. You can select "Other options" and choose your passkey. If the issue persists after multiple logins, you might need to delete the passkey from your Duo device manager then set it up again.

Can I add passkeys in the UofM iAM service?

No. New passkeys must be created in the Duo device management menu, which can be accessed via the "Other options" link in the Duo authentication window.