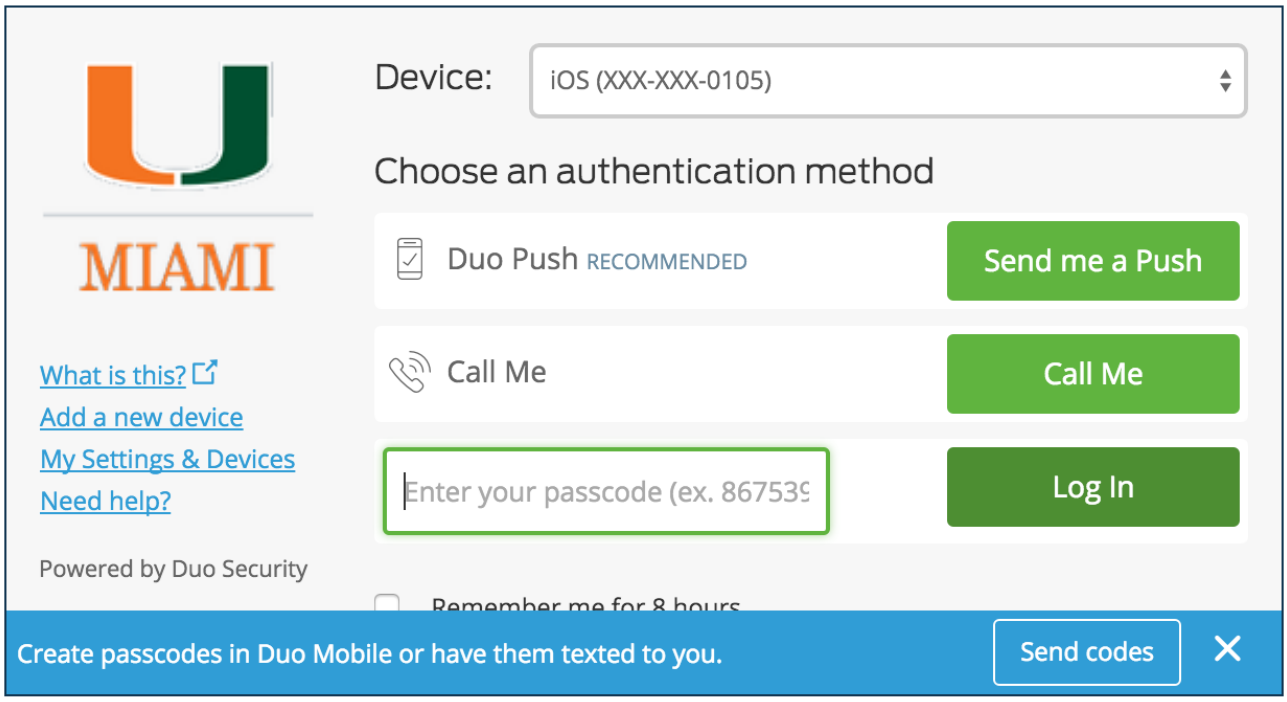
Duo Multi-Factor Authentication (MFA): **Using Duo with a Hardware Token**

Note: tokens are only available for active UM faculty, staff, and students.

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**" (or type the generated passcode in the "second password" field). Using the "Device:" drop-down menu to select your token is not necessary before entering the passcode.



If you have a Duo MFA token, click into the passcode entry field and tap your token's button to generate and submit a passcode.

Tokens can get "out of sync" if the button is pressed too many times in a row and the generated passcodes aren't used for login. If your token stops working, please contact the UMIT Service Desk at (305) 284-6565 or help@miami.edu.

Hardware Token FAQs

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"** (or type the generated passcode in the "second password" field). *(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.

Where can Duo MFA tokens be obtained?
Duo MFA tokens will be issued via walk-in centers located on each UM campus*. To be issued a token, a person will need to visit a location and provide identification. In some cases, tokens will also be issued to IT departmental partners who can distribute to their colleagues.

Current Duo MFA token distribution walk-in centers are located at:

- Coral Gables campus: Student Technology Help Desk (STHD) (Modular B, 1305 Stanford Dr., open Monday-Friday, 9 a.m.-5 p.m.)
- RSMAS campus: RSMAS Computing Facility (open Monday-Friday, 8 a.m.-5 p.m.)

**Note: If you are a Medical campus employee, please contact the UMIT Service Desk at: (305) 243-5999 or help@med.miami.edu and an incident will be created for a new Duo MFA token.*

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 dead.
- 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, bring the token to one of the walk-in centers detailed above for examination and 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 UMIT Service Desk at: (305) 284-6565 or help@miami.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 your department for re-distribution and re-use.