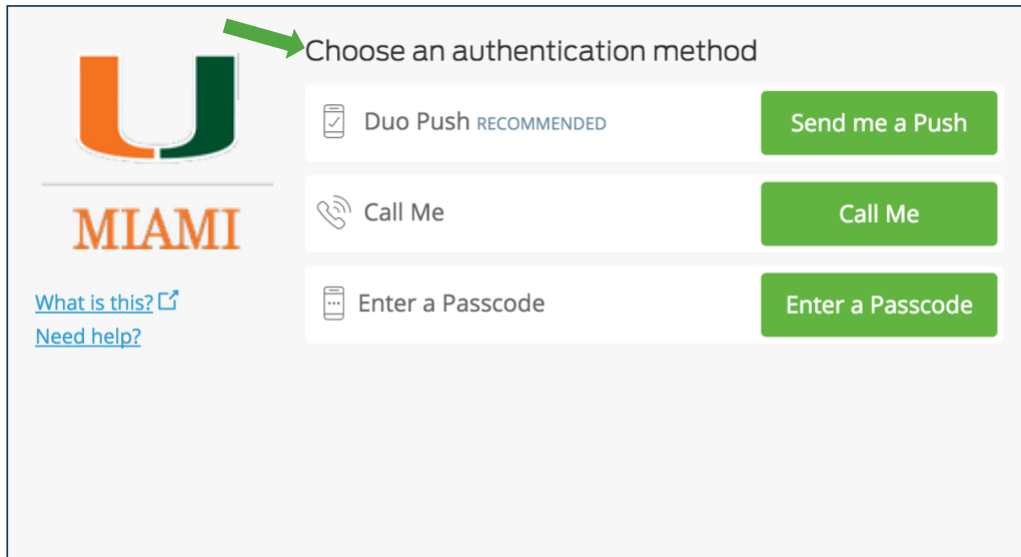


Duo Multi-Factor Authentication (MFA): Using the Authentication Prompt

The authentication prompt lets you choose how to verify your identity each time you log in.

Supported Browsers: Chrome, Firefox, Safari, Internet Explorer 8 or later, and/or Opera.

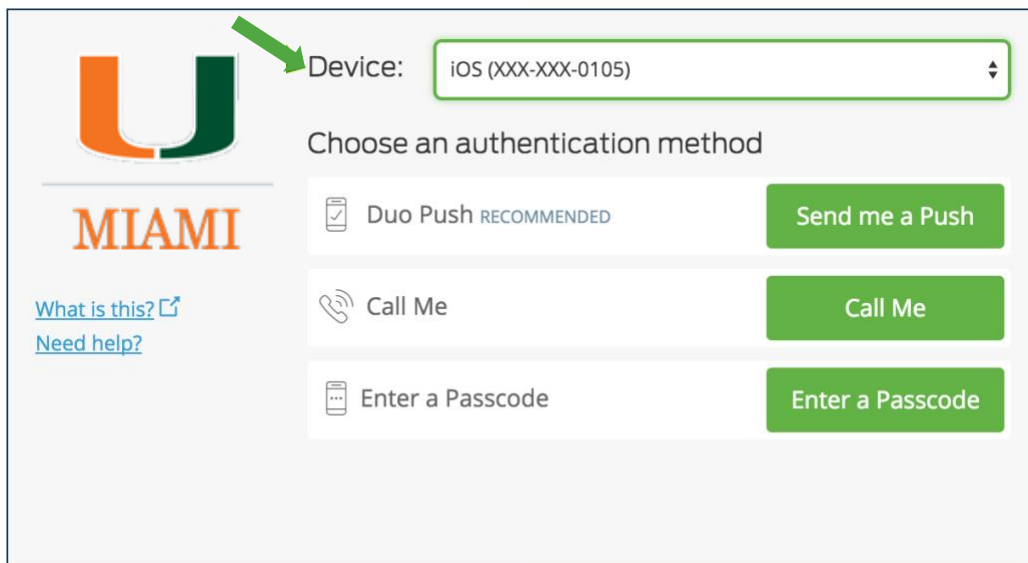


The screenshot shows the Duo authentication prompt interface. On the left is the University of Miami logo (a stylized 'U' in orange and green) and the word 'MIAMI' in orange. Below the logo are two links: 'What is this?' and 'Need help?'. On the right, under the heading 'Choose an authentication method', there are three options, each with a green button:

- Duo Push RECOMMENDED** with a 'Send me a Push' button.
- Call Me** with a 'Call Me' button.
- Enter a Passcode** with an 'Enter a Passcode' button.

A green arrow points from the text 'Choose an authentication method' to the top of the Duo Push option.

If you have more than one device enrolled, you'll see a device selector.



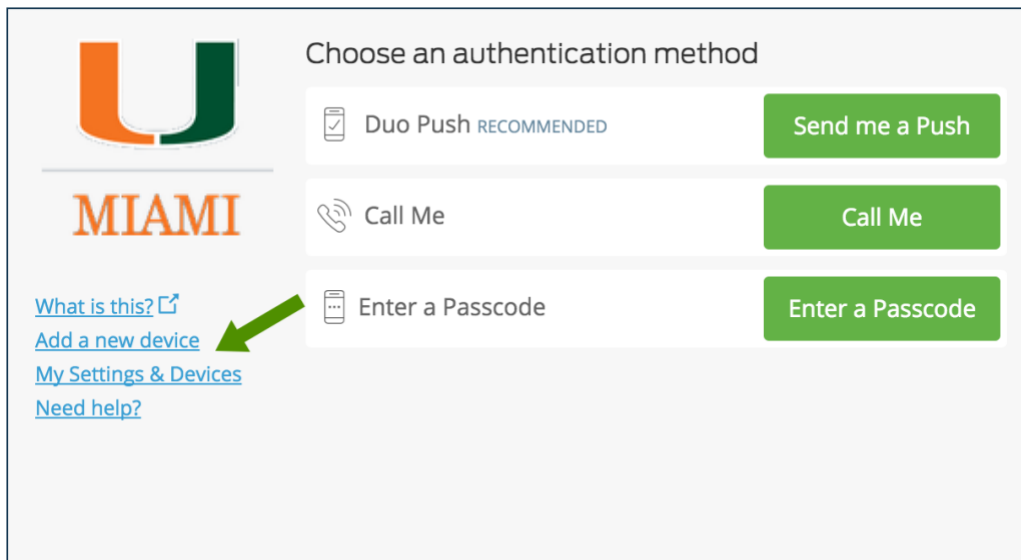
This screenshot is similar to the previous one but includes a device selector. At the top, there is a 'Device:' label followed by a dropdown menu showing 'iOS (XXX-XXX-0105)'. A green arrow points from the text 'Device:' to the dropdown menu. Below the device selector is the same 'Choose an authentication method' section with three options and their respective buttons: Duo Push (Send me a Push), Call Me (Call Me), and Enter a Passcode (Enter a Passcode). The University of Miami logo and links are also present on the left.

Select the device you want to use and then choose your authentication method.

Method	Description
Duo Push	Pushes a login request to your phone or tablet (if you have the Duo Mobile app installed and activated on your iPhone, Android, or BlackBerry device). Just review the request and tap “Approve” to log in.
Call Me	Authenticate via phone callback.
Enter a Passcode	Log in using a passcode, either generated with Duo Mobile, sent via SMS, generated by your hardware token, or provided by an administrator. Click “Send codes” to get a new batch of passcodes texted to your phone.

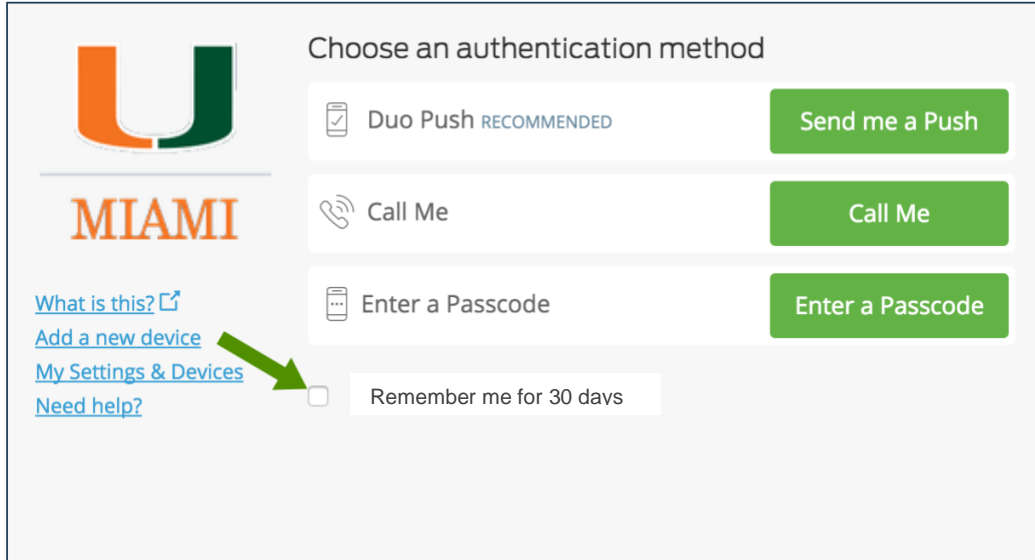
Self-Service Options

You can add an additional authentication device by clicking the **“Add a new device”** link, or update your setting and remove authentication methods by clicking **“My Settings & Devices.”**



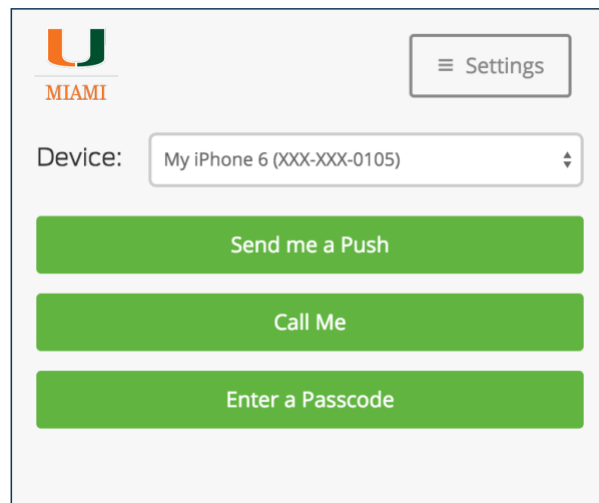
Trusted Devices

You'll also see a **“Remember me for 30 days”** option. If you check this box when authenticating, you won't need to perform Duo second-factor authentication again for the duration specified on the prompt.

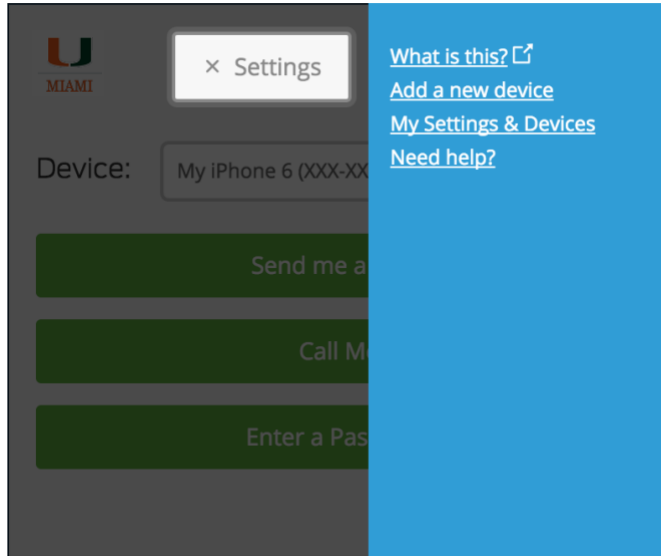


Authenticating from Smaller Screens

If you're logging in with Duo from a device with a smaller screen (like a tablet) or small browser window then your authentication prompt may look slightly different. Don't worry! All the devices and options shown in the full-size prompt are available for use, and you can enroll and manage devices by following the same steps.



Access “**Add a New Device**” or “**My Settings & Devices**” by clicking the “**Settings**” button at the top. Click the “**X**” on the Settings button to return to the authentication prompt.



Software Updates

You may be prompted to update outdated browser or plugin software when authenticating. You can take a few minutes to update your web browser, Flash, or Java version to the most recent before authenticating, or choose to update later and continue on to the protected resource.

