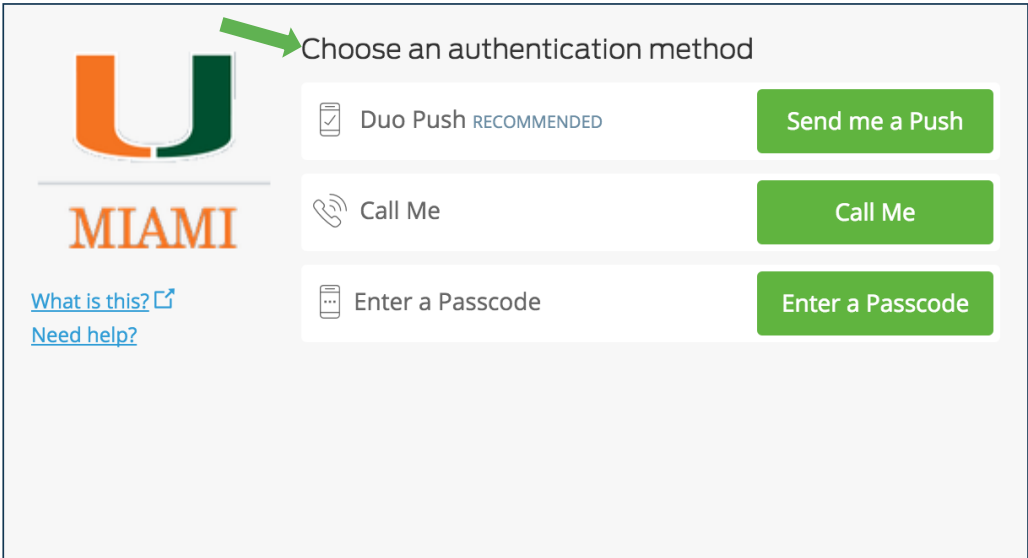


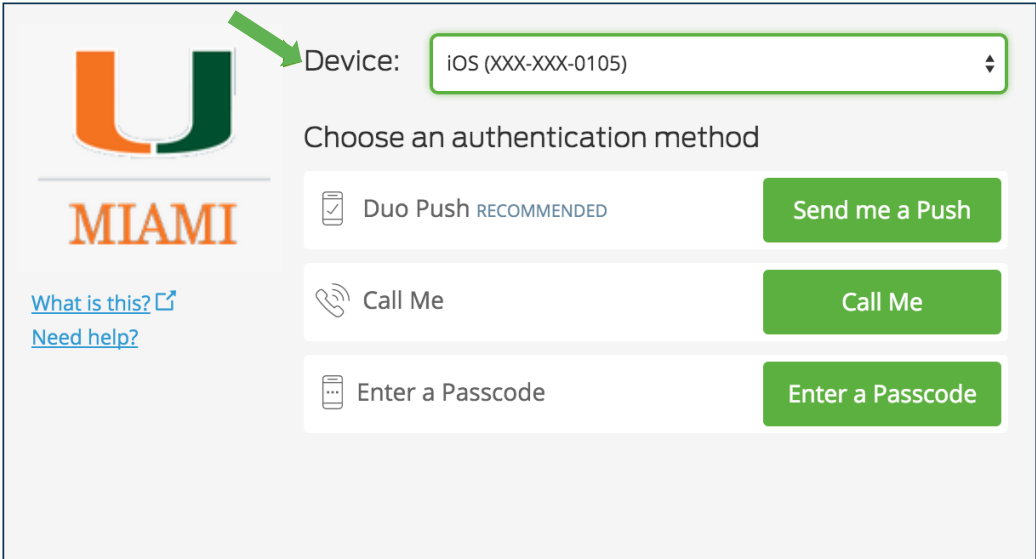
Duo Multi-Factor Authentication (MFA): Using the Authentication Prompt

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.



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



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

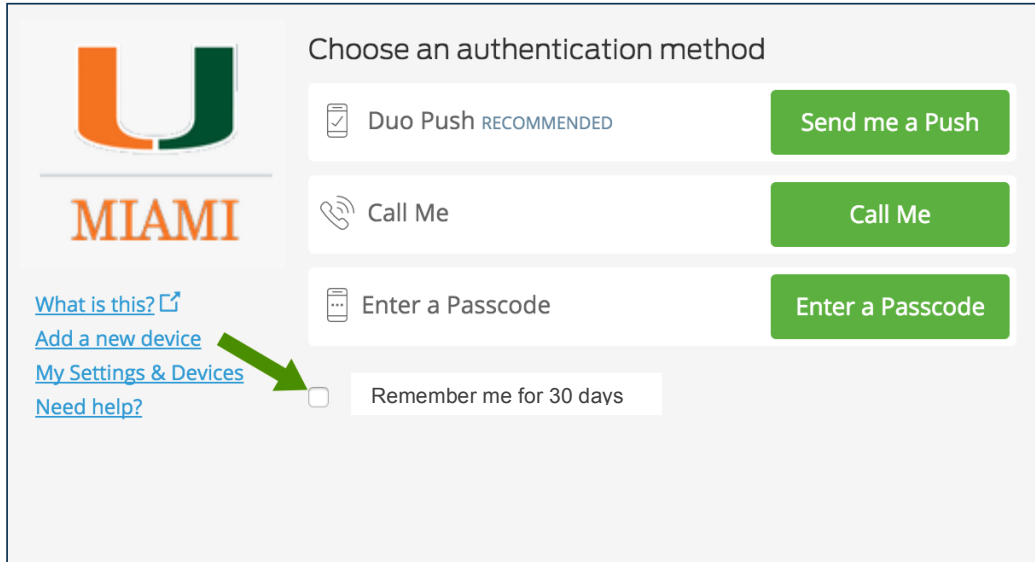
You can add an additional authentication device by clicking the “**Add a new device**” link, or update your setting and remove authentication methods by clicking “**My Settings & Devices.**”

The screenshot shows the Duo authentication selection interface. On the left, there is the Miami University logo (an orange 'U' with a green bar) and the word 'MIAMI' in orange. Below the logo are four blue links: 'What is this?', 'Add a new device', 'My Settings & Devices', and 'Need help?'. A green arrow points from the 'Add a new device' link to the 'Enter a Passcode' option. The main area is titled 'Choose an authentication method' and contains three options, each with an icon and a green button:

- Duo Push** (with a mobile phone icon and the word 'RECOMMENDED' in blue) and a green button labeled 'Send me a Push'.
- Call Me** (with a phone handset icon) and a green button labeled 'Call Me'.
- Enter a Passcode** (with a passcode icon) and a green button labeled 'Enter a Passcode'.

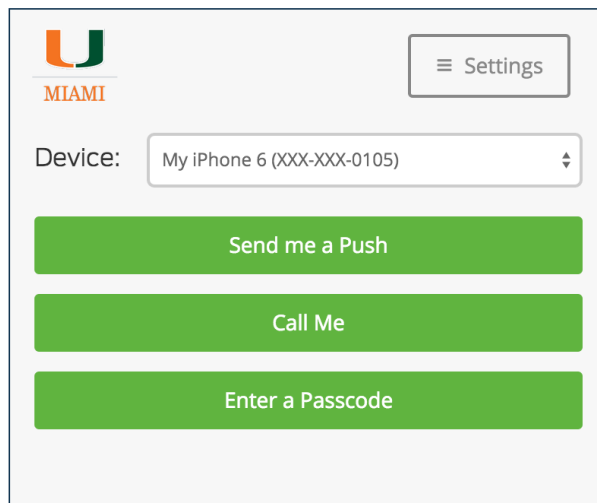
Trusted Devices

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.

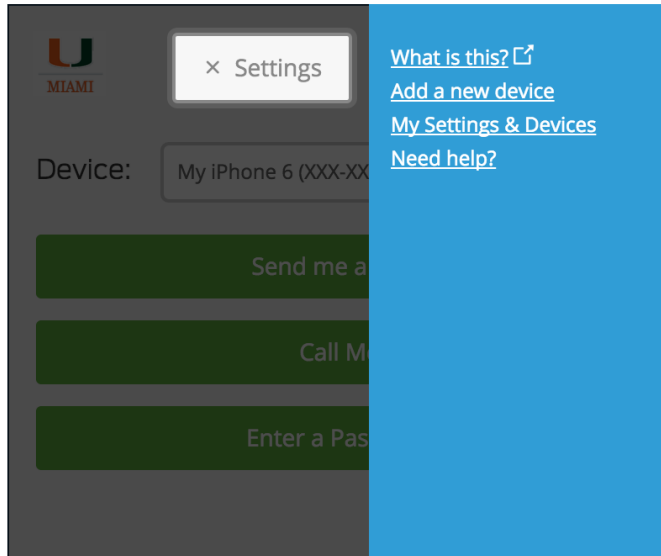


Authenticating from Smaller Screens

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.

The image displays a mobile application interface for authentication. On the left, the University of Miami logo (a green and orange 'U') and the word 'MIAMI' are shown. Below the logo are three links: 'What is this? [external icon]', 'Add a new device', 'My Settings & Devices', and 'Need help?'. On the right, there is a 'Device:' dropdown menu showing 'My iPhone 6 (XXX-XXX-0105)'. Below this is the heading 'Choose an authentication method' followed by three options, each with a green button: 'Duo Push RECOMMENDED' with 'Send me a Push' button, 'Call Me' with 'Call Me' button, and 'Enter a Passcode' with 'Enter a Passcode' button. At the bottom, there is a checkbox for 'Remember me for 8 hours'. An orange banner at the very bottom contains the text 'Your computer software is 28 days out of date.' and a white button with 'Let's update it' and a close 'x' icon.