Authenticating a Two-Factor Authentication (2FA) Request

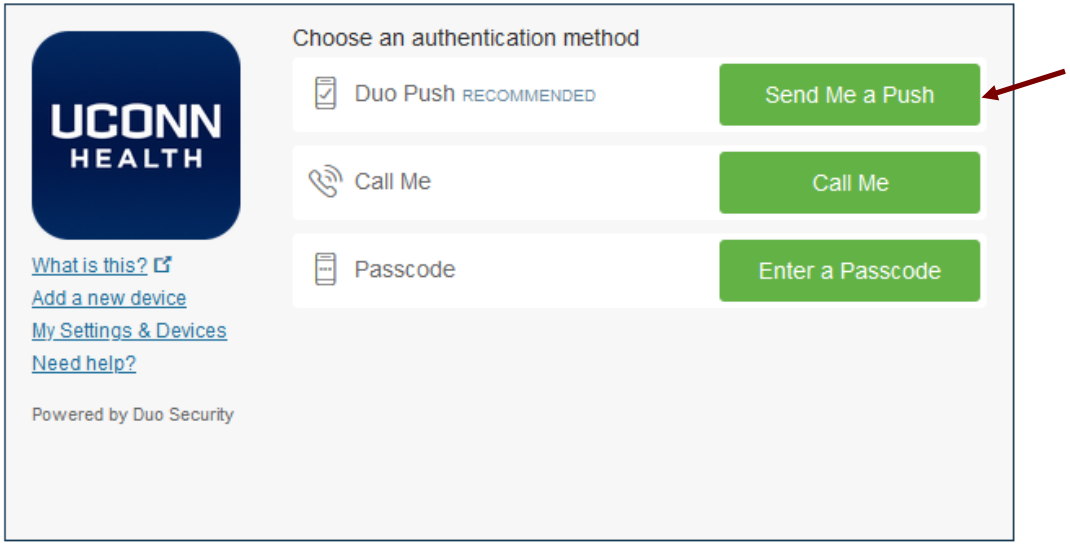
With the two-factor authentication (2FA) service, faculty, staff, and affiliates will be prompted to verify their identity on a second factor that they designate. Depending on the device chosen, they may also select the type of prompt or authentication method they wish to receive. This document covers the types of devices that may be used for this service and the notification options.

The simplest way to use 2FA at UConn Health while traveling is to download and set up the Duo Mobile app for authentication. Duo Mobile works both with and without internet access on your second device, and is IT Security's recommended second factor authentication method for all situations.

- **IMPORTANT NOTE: Once a push notification is sent you have 60 seconds to approve the request.**
- To authenticate using a push notification (smart phone app), you will need to have an internet or data connection.

When you login to one of our Duo protected services: Outlook Web Access (OWA); Pulse Secure VPN; Citrix (remote.uchc.edu), you will be presented with the 2FA authentication screen below. **To authenticate via a push notification:**

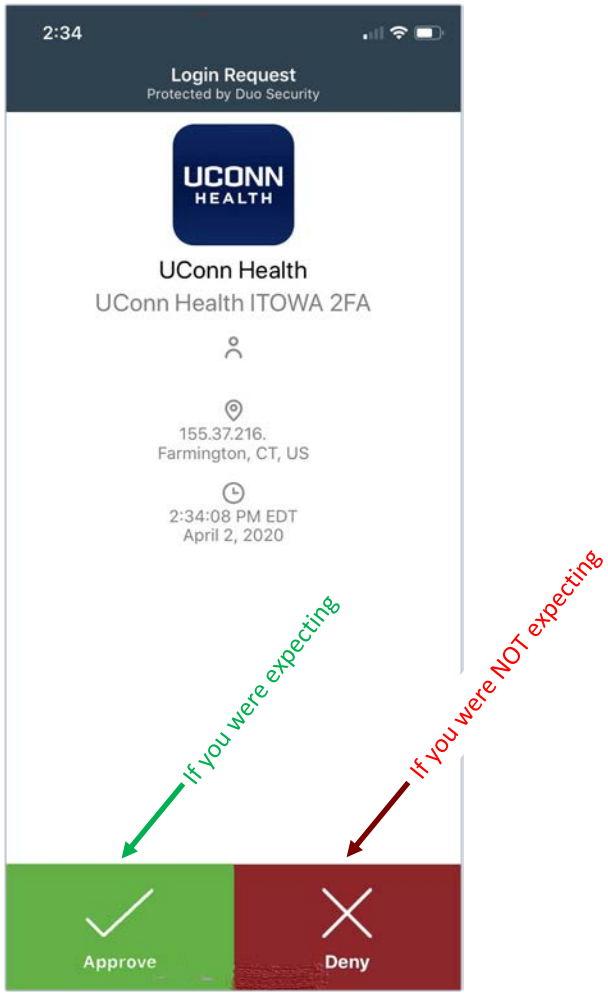
1) On the 2FA screen, click **Send Me a Push**.



2) A blue bar at the bottom of the 2FA authentication screen tells you that a push notification was sent to your device.

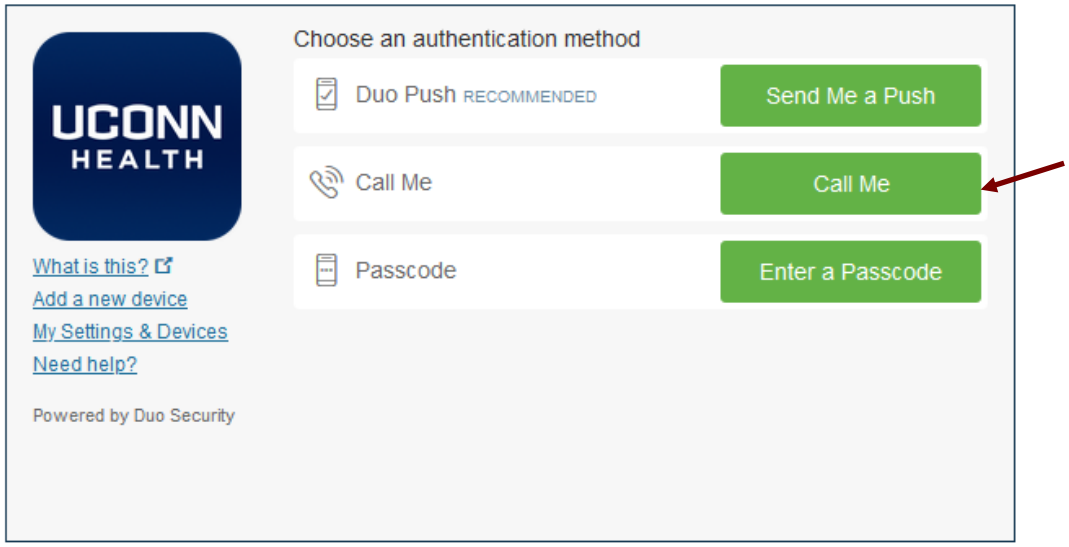
3) Tap the “Login request” message that displays on your smartphone or tablet, or open the Duo Mobile app on your device and tap the message.

4) **IMPORTANT!** If you were expecting this request tap **Approve** to authenticate. **If you get a request you were not expecting, tap Deny**.



To authenticate via a Phone Call:

1) On the 2FA screen, click **Call Me**.



2) Your phone will be automatically called if you chose that default authentication method in your settings.

3) A blue bar at the bottom of the 2FA authentication screen will indicate the phone number being dialed.

4) Answer the phone.

5) **If you were expecting this request**, press any key on your phone to authenticate.

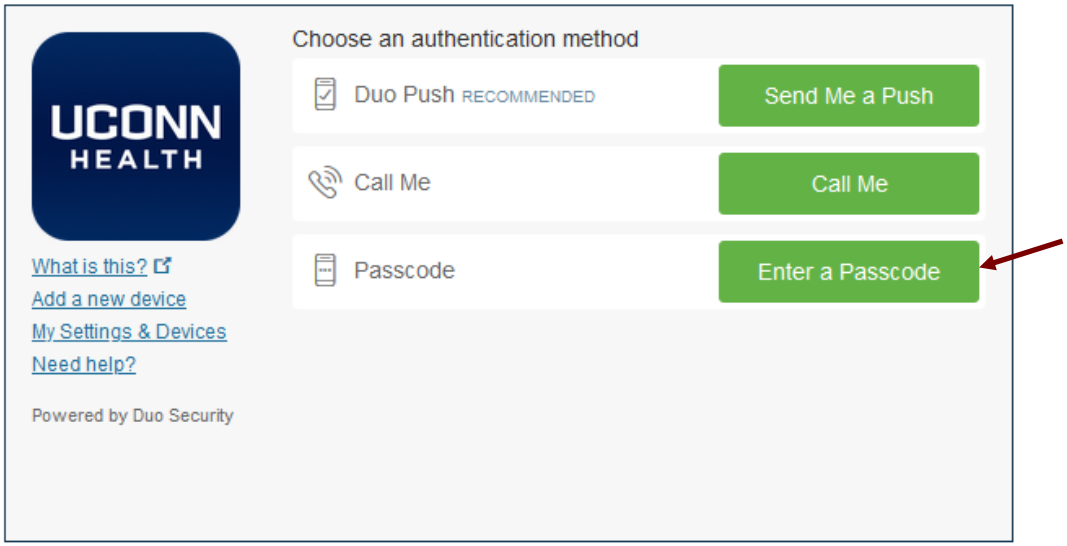
6) **IMPORTANT! If you were not trying to access a system that requires 2FA, press the asterisk key (*) to report fraud.**

To authenticate using a Passcode:

1) There are two ways to generate one-time passcodes with 2FA:
   a. **Duo Mobile:** Open the Duo Mobile app and expand your Uconn Health account. (**The passcode appears in the Duo app, NOT in a text!)**

   b. **Hardware Token:** If you have obtained a hardware token by calling the IT Service Desk, push the button on the front of the device to generate a code.

2) On the 2FA authentication screen, click **Enter a Passcode**. After doing so, new text field will appear and the **Enter a Passcode** button will change to **Log In**.



3) Type the 6 digit code that appears into the website that you are logging into, and click Log In.