UCONN HEALTH

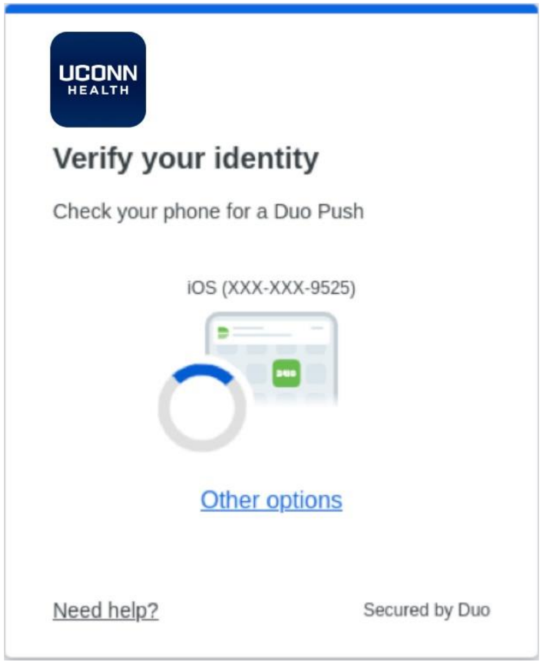
Authenticating a Two-Factor Authentication (2FA) Request

With the two-factor authentication (2FA) service, faculty, staff, and affiliates will be prompted to verify their identity with a second factor device 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 phone or tablet. The Duo Mobile App is the 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 e.g. web based mail or a remote access, you will be presented with the below prompt requesting you to **approve the 2FA Push request on your Duo Mobile App (or another primary 2FA option you selected):**



UCONN HEALTH

Verify your identity

Check your phone for a Duo Push

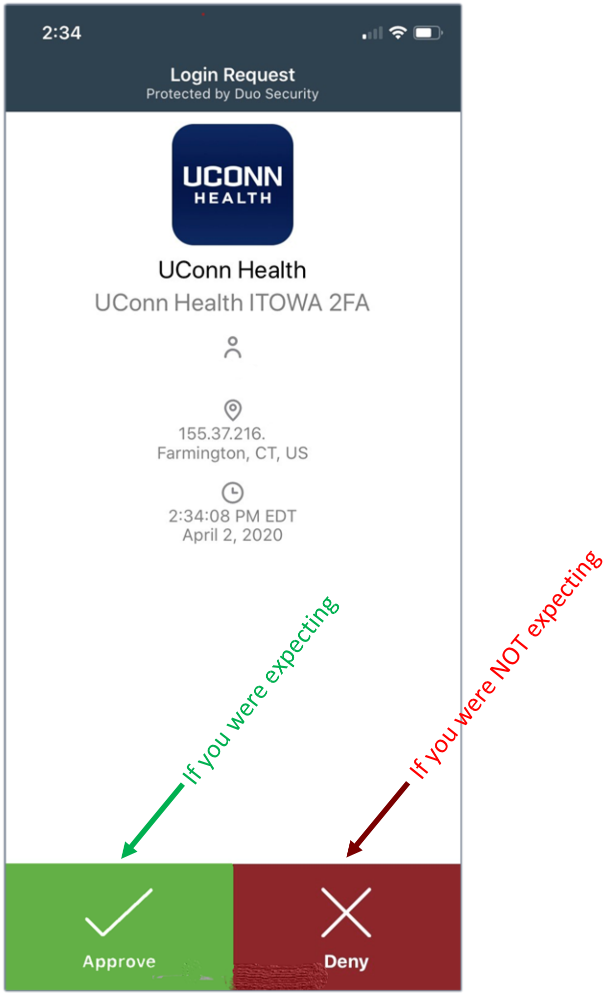
iOS (XXX-XXX-9525)

IMPORTANT! Open or access the Duo Mobile App

If you **were expecting** this request tap **Approve** to authenticate.

If you WERE NOT EXPECTING this 2FA request tap DENY

If you received an unexpected Push request, one you did not initiate DO NOT APPROVE THE REQUEST, INSTEAD TAP DENY. After you Tap DENY you will be prompted to submit the DENY as a Suspicious / Fraudulent 2FA Push, continue to submit the report.



2:34

Login Request
Protected by Duo Security

UConn Health
UConn Health ITOWA 2FA

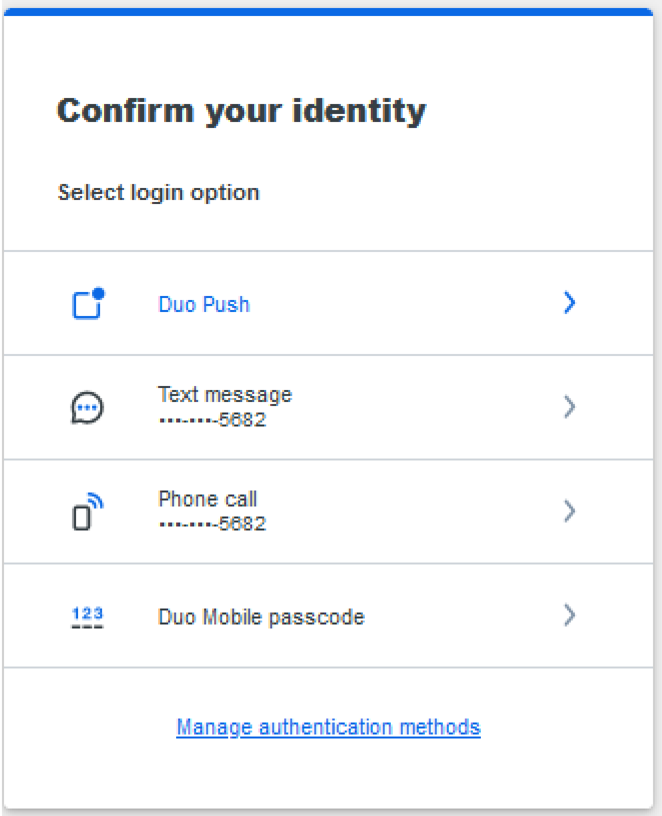
155.37.216.
Farmington, CT, US

2:34:08 PM EDT
April 2, 2020

If you were expecting

If you were NOT expecting

To authenticate with another Option click ‘Other Options’



Confirm your identity

Select login option

Duo Push

Text message
•••-•••-5682

Phone call
•••-•••-5682

Duo Mobile passcode

Manage authentication methods

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

The number under ‘Call phone’ will indicate the number being dialed.

Answer the phone.

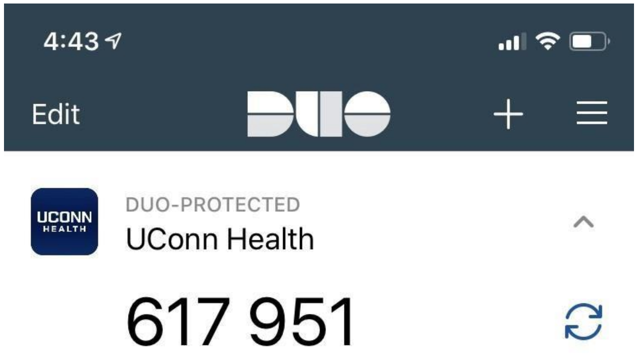
If you were expecting this request, press any key on your phone to authenticate.

IMPORTANT! If this phone call is NOT EXPECTED AND YOU DID NOT INITIATE THE 2FA PHONE CALL, PRESS THE ASTERISK KEY (*) TO REPORT FRAUD.

To authenticate using a Passcode:

There are two ways to use one-time passcodes with 2FA:

1) **Duo Mobile:** Open the Duo Mobile app and **expand your UConn Health account**. (**The passcode appears in the Duo app, NOT in a text!)**



DUO-PROTECTED

UConn Health

617 951

2) **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.

IMPORTANT! **Is an unusual website asking you to enter a Duo Passcode, one you didn't expect? DO NOT ENTER A PASSCODE.** Instead, exit your web browser and contact the UCH Service Desk x4400 and report the incident.

Entering a passcode:

On the 2FA authentication screen if required Click More Options then select the Passcode option you wish to use.

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