

Two-factor Authentication with Duo - FAQ

Brief description of the service and overview of purpose of Q&A

- [Do I need a smartphone to use Two-Factor Authentication \(2FA\)?](#)
- [What devices are supported by Duo Mobile?](#)
- [Can I generate backup codes for when I don't have access to my devices?](#)
- [I have an Apple Watch. Will it work with Two-Factor Authentication \(2FA\)?](#)
- [How long do I have to enter my Duo security code or reply to a Push notification?](#)
- [I seem to be locked out of the Two-Factor Authentication \(2FA\) service. What should I do?](#)
- [What do I do if I get a Duo notification and I haven't attempted to log into any Lehigh system?](#)
- [How do I set up an older cell phone, or use a smartphone without the Duo app installed?](#)
- [What do I do if I don't have my mobile phone with me?](#)
- [I signed up for 2FA and would like to un-enroll till the end of 2019. How can I do this?](#)
- [I will be getting a new phone soon. How can I make a smooth transition to a new phone?](#)
- [Can I reuse a passcode?](#)
- [How long are passcodes good for?](#)
- [I clicked on the 30 day checkbox -- why do I keep getting prompted for 2FA?](#)
- [My phone was stolen, damaged, or dropped in the ocean. Now what?](#)
- [I already have Duo setup at another institution, can I add Lehigh?](#)
- [What data is stored by Duo Security?](#)
- [How do I add or remove 2FA devices and manage my Duo settings?](#)
- [I use a landline for Two-Factor Authentication \(2FA\), and I'm going away for a week. Can I still use the service?](#)
- [Will Duo work while I'm traveling outside the U.S.?](#)
- [I will be using the Internet only at wifi hotspots and won't have cell phone access while traveling, will Duo still work?](#)
- [I'm an employee who will be retiring soon. Will I be required to use 2FA after I retire?](#)
- [Requested a push notification but did not receive one on iPhone?](#)
- [Mac version of Cisco AnyConnect does not allow setting the "30 Day" cookie in the Duo Authentication app](#)

Do I need a smartphone to use Two-Factor Authentication (2FA)?

A smartphone is the recommended device since the Duo Mobile app provides the greatest level of security and flexibility. The app generates passcodes for login (even without cellular connectivity) and can receive push notifications for easy, one-tap authentication. Duo Security offers multiple other ways to authenticate with Duo. Besides a smartphone, you can use an older cell phone, landline (such as your office or home phone), tablet, or security key.

What devices are supported by Duo Mobile?

The Duo Mobile App is available on iOS, Android, and Apple WatchOS.

Can I generate backup codes for when I don't have access to my devices?

It is highly recommended that you generate and print backup codes that you can use when you do not have access to your other devices, such as phone. Connect to <https://accounts.lehigh.edu/duocodes/generate> to generate and print these codes. Remember to store the codes in a safe location such as your wallet.

I have an Apple Watch. Will it work with Two-Factor Authentication (2FA)?

Yes, it will work for 2FA. You will need to have an iPhone enrolled in the service, and then follow the [set up instructions from Duo Security](#).

How long do I have to enter my Duo security code or reply to a Push notification?

The Duo 2FA prompt will remain on-screen for one minute before returning you to the login prompt.

I seem to be locked out of the Two-Factor Authentication (2FA) service. What should I do?

A user is automatically locked out when there are 10 consecutive failed log in attempts. This could happen if you don't respond to multiple push notifications, or if you selected the wrong device (calling an office landline when at home), or automatic log-in attempts by a 2FA-protected system when a user isn't expecting them.

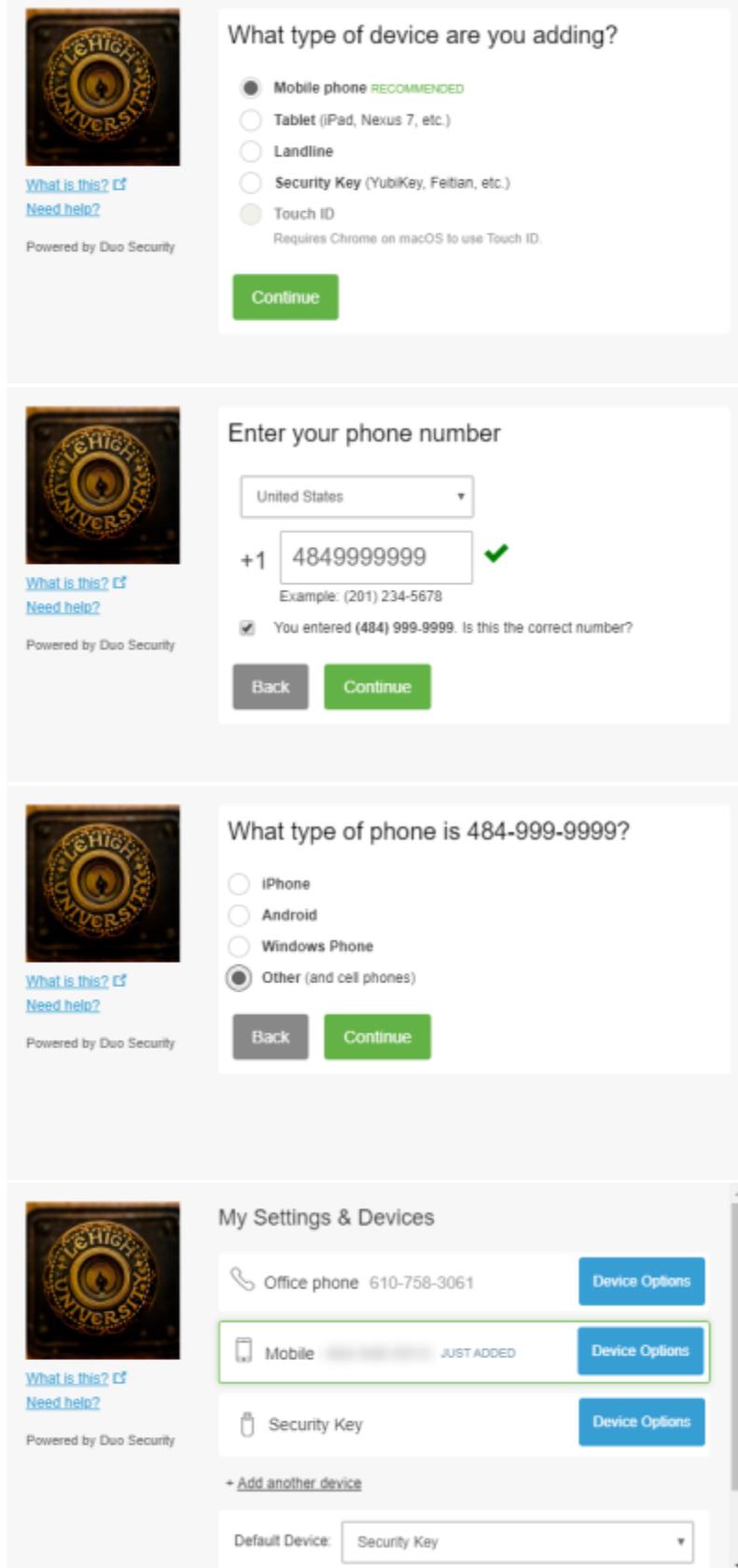
Once you have been locked out, you will need to call the LTS Help Desk (610-758-4357) for assistance in unlocking the account.

What do I do if I get a Duo notification and I haven't attempted to log into any Lehigh system?

This could be an indication that your account has been compromised. The first thing to do is change your password by visiting the [Password Change](#) page. After changing your password, please notify us by calling or emailing the Help Desk.

How do I set up an older cell phone, or use a smartphone without the Duo app installed?

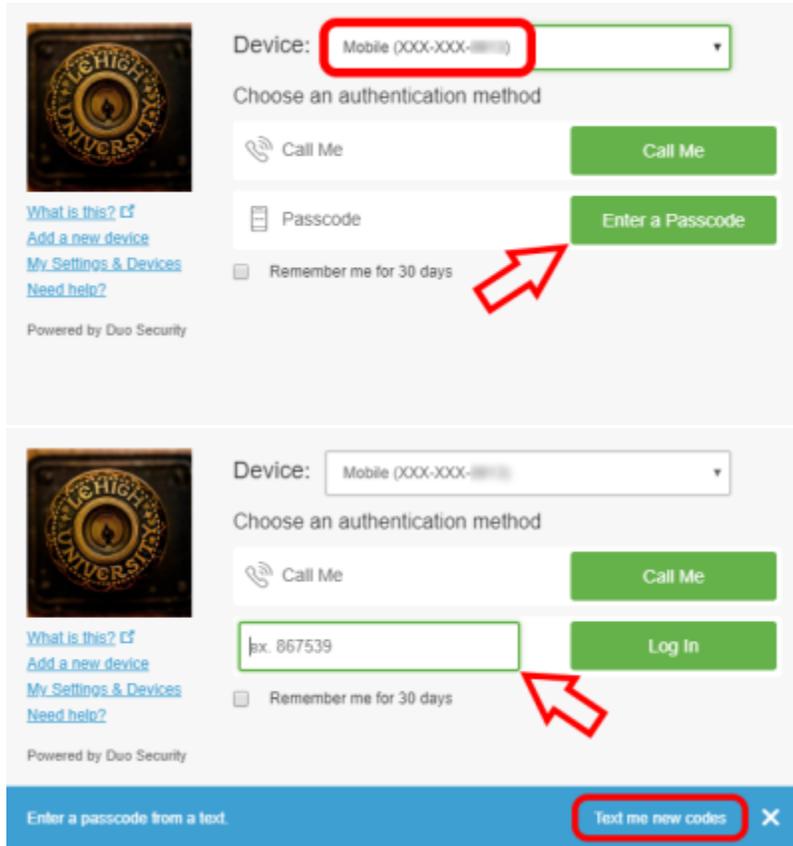
Duo will work with any cell phone that can receive text (SMS) messages. When adding a device in this mode, first choose "Mobile Phone," and on the next screen enter the phone number. After confirming the phone number, set the phone type as "Other (and cell phones)" and the mobile device will be added.



The image shows four sequential screenshots of the Duo Security setup interface for adding a mobile phone. Each screenshot includes the University of North Carolina logo and the text "Powered by Duo Security".

- Step 1: What type of device are you adding?** The "Mobile phone" option is selected and marked as "RECOMMENDED". Other options include Tablet, Landline, Security Key, and Touch ID.
- Step 2: Enter your phone number** The user enters the number +1 4849999999. A dropdown menu shows "United States". A green checkmark indicates the number is valid.
- Step 3: What type of phone is 484-999-9999?** The "Other (and cell phones)" option is selected.
- Step 4: My Settings & Devices** The mobile phone is listed as "Mobile" with the status "JUST ADDED". The "Default Device" is set to "Security Key".

Now that your phone has been added, whenever you see the Duo Authentication screen, you can select your Mobile phone as the device to use. After choosing Mobile, click on the green "Enter a Passcode" button, then in the blue bar at the bottom, click on the link to "Text me new codes. Take a look in your phone's text message app. You should see new message with a list of five codes you can use one time each. Enter one of the codes in the box shown below, and you're in!



What do I do if I don't have my mobile phone with me?

1. Duo can call your office line if you have set it up as an alternate number. We recommend adding at least your office line, and possibly other lines as appropriate. For example, you may want to have a spouse's mobile number as an option in case of emergency.
2. It is highly recommended that you generate and print backup codes that you can use when you do not have access to your other devices, such as phone. Connect to <https://accounts.lehigh.edu/duocodes/generate> to generate and print these codes. Remember to store the codes in a safe location such as your wallet.
3. You can use a USB Security Key, available from YubiKey and other vendors. Again, this must be set up in advance.

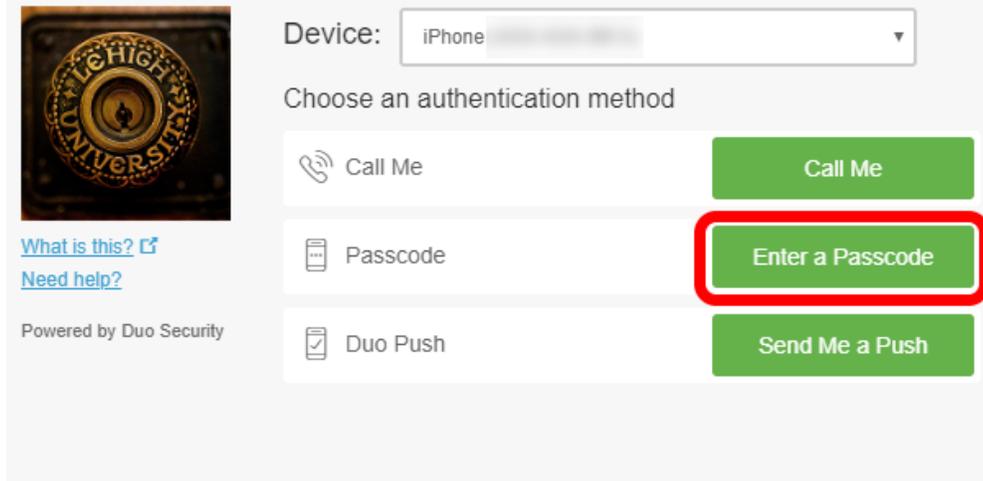
I signed up for 2FA and would like to un-enroll till the end of 2019. How can I do this?

Two factor authentication will be required going forward. If you have extenuating circumstances that require a temporary bypass of 2FA, please contact helpdesk@lehigh.edu

I will be getting a new phone soon. How can I make a smooth transition to a new phone?

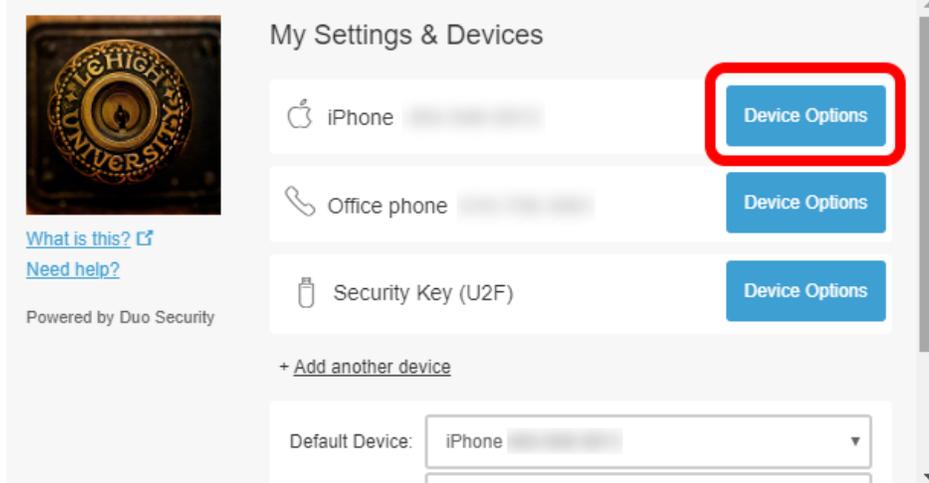
Before wiping your old phone, you should [print out a new set of one-time-use codes](#) to help with enrolling your new phone. Once you have the print-out, download the Duo Mobile app on your new phone. Then open a web browser and go to the [Duo Device Management](#) page.

On the Device Management page, press the green "Enter a Passcode" button, and enter one of the codes you printed out.



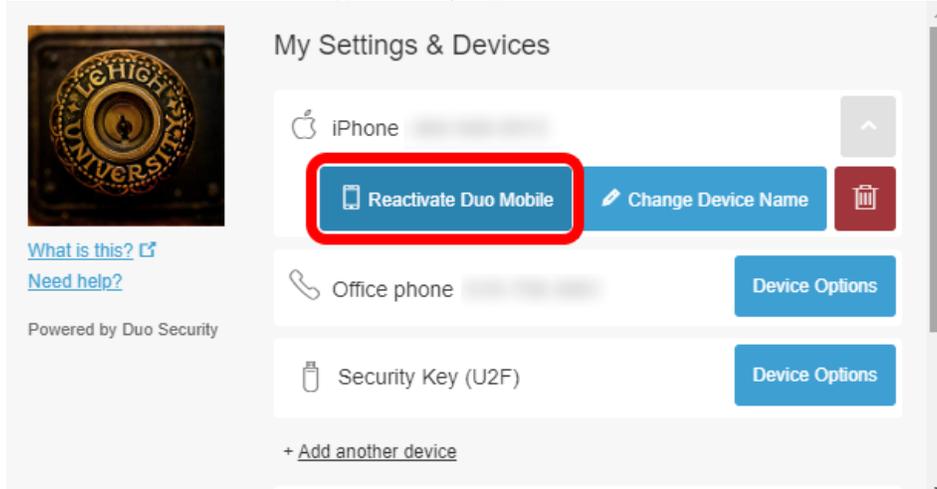
The screenshot shows the 'Device Management' page. On the left is the Lehigh University logo and links for 'What is this?' and 'Need help?'. Below that, it says 'Powered by Duo Security'. The main content area has a 'Device:' dropdown menu set to 'iPhone'. Below this is the heading 'Choose an authentication method'. There are three rows of options: 'Call Me' with a green 'Call Me' button; 'Passcode' with a green 'Enter a Passcode' button (highlighted with a red rectangle); and 'Duo Push' with a green 'Send Me a Push' button.

You will see your existing iPhone or Android phone in the list of devices. Click the Device Options button next to your phone.



The screenshot shows the 'My Settings & Devices' page. On the left is the Lehigh University logo and links for 'What is this?' and 'Need help?'. Below that, it says 'Powered by Duo Security'. The main content area has the heading 'My Settings & Devices'. Below this is a list of devices: 'iPhone', 'Office phone', and 'Security Key (U2F)'. Each device has a blue 'Device Options' button next to it. The 'Device Options' button for the iPhone is highlighted with a red rectangle. Below the list is a '+ Add another device' link and a 'Default Device:' dropdown menu set to 'iPhone'.

A Reactivate Duo Mobile button will appear below your phone.



The screenshot shows the 'My Settings & Devices' page. On the left is the Lehigh University logo and links for 'What is this?' and 'Need help?'. Below that, it says 'Powered by Duo Security'. The main content area has the heading 'My Settings & Devices'. Below this is a list of devices: 'iPhone', 'Office phone', and 'Security Key (U2F)'. Each device has a blue 'Device Options' button next to it. The 'Device Options' button for the iPhone is highlighted with a red rectangle. Below the list is a '+ Add another device' link and a 'Default Device:' dropdown menu set to 'iPhone'.

Clicking on the button will show you a QR code. On your new phone, bring up the Duo Mobile app and tap the Add Account button. It will switch to your phone's camera. Point the camera at the QR code (2d bar code). Lehigh University will now appear in your Duo Mobile app. You're done!

Can I reuse a passcode?

No. Passcodes are only good for a single use.

How long are passcodes good for?

Passcodes never expire. They last until they are used, or until you generate a new set.

I clicked on the 30 day checkbox -- why do I keep getting prompted for 2FA?

The "remember me" option is tied to a particular browser on a device. So if you are using a different browser, or a different device to login, you will need to check the box again.

My phone was stolen, damaged, or dropped in the ocean. Now what?

Call or email the Help Desk for assistance removing the device from your account.

I already have Duo setup at another institution, can I add Lehigh?

Yes! Duo supports multi-factor authentication across many institutions. To add Lehigh, simply visit your [Duo Options page](#) and proceed with the setup until you see the QR code. Open the Duo Mobile app on your phone and tap on the "+" sign in the upper right corner. Point your phone's camera at the QR code and Lehigh is added! That's all there is to it.

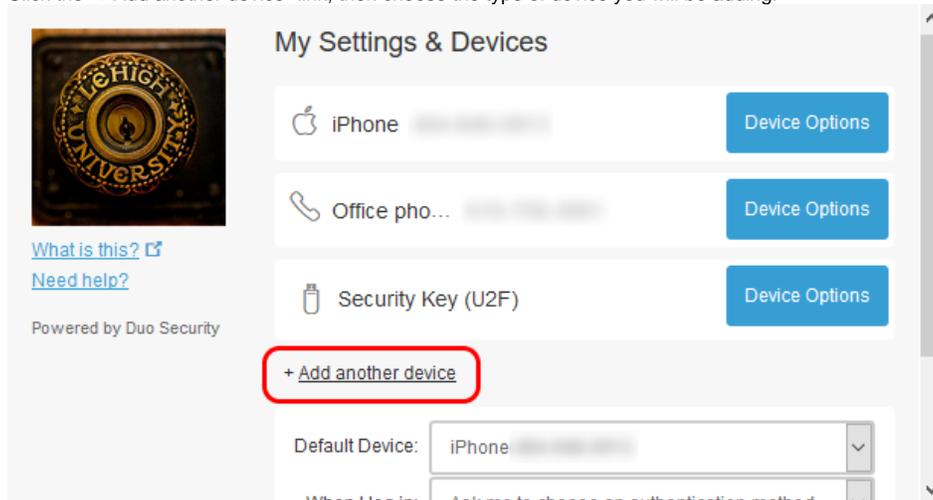
What data is stored by Duo Security?

The only data stored by [Duo Security](#) is the client's Lehigh user ID (Duo does NOT know your password) and information about your second factor, such as a phone number (if using a phone for the service) or the serial number of your Duo Token (if not using a phone for the service).

How do I add or remove 2FA devices and manage my Duo settings?

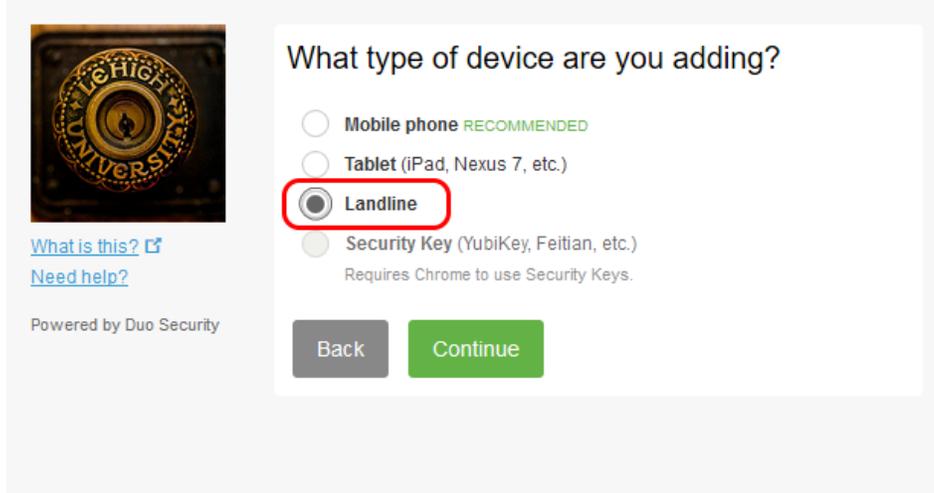
Visit www.lehigh.edu/account and follow the "Two-factor authentication with Duo" link. You will first need to authenticate with Duo, after which you will see the settings screen as pictured below.

Click the "+ Add another device" link, then choose the type of device you will be adding.



The screenshot shows the "My Settings & Devices" interface. On the left, there is a Lehigh University logo and links for "What is this?" and "Need help?". Below the logo, it says "Powered by Duo Security". The main content area lists three devices: "iPhone", "Office pho...", and "Security Key (U2F)". Each device entry has a "Device Options" button. At the bottom of the list, there is a red-bordered button labeled "+ Add another device". Below this button, there is a "Default Device:" dropdown menu currently set to "iPhone", and a "When Use in:" dropdown menu.

If you're adding your office phone, select Landline.



What type of device are you adding?

Mobile phone **RECOMMENDED**

Tablet (iPad, Nexus 7, etc.)

Landline

Security Key (YubiKey, Feitian, etc.)
Requires Chrome to use Security Keys.

Back Continue

Powered by Duo Security

You will receive a confirmation call on that number. Answer the phone and press any key on the phone's number pad. This will confirm the device and finish the process. Repeat as necessary for additional phone numbers.

I use a landline for Two-Factor Authentication (2FA), and I'm going away for a week. Can I still use the service?

Yes, you can forward your enrolled phone to another number (or add the other number temporarily at the [2FA self-service portal](#)).

Will Duo work while I'm traveling outside the U.S.?

Yes, Duo will work from pretty much anywhere you can access the Internet. We recommend that you have the Duo mobile app installed on your phone while traveling. If you're planning to travel without your phone, please contact us in advance for assistance.

I will be using the Internet only at wifi hotspots and won't have cell phone access while traveling, will Duo still work?

Yes, Duo Mobile application can be used to generate passcodes on airplanes or in remote regions where Duo Push, SMS-delivered passcodes, phone callback or cellular service may be unavailable or difficult to use. Duo Push can use a Wi-Fi connection to function. If you can access the Internet from your mobile device, you can receive push notifications.

I'm an employee who will be retiring soon. Will I be required to use 2FA after I retire?

When you leave Lehigh your staff affiliation will change to retiree, and as such, you will no longer be required to be enrolled in 2FA.

Requested a push notification but did not receive one on iPhone?

Sometimes when prompted for re-authentication and the user selects push notification but did not receive one on iPhone. The Duo application icon was displayed on home screen with no indication of offloaded status. When icon was tapped, icon changed to superimposed standard iOS loading wheel. After loading was completed, push notification worked as normal. This may be a result of the application being considered as an "unused" application. Apple has not published the criteria on when it considers an app 'unused' but reports are common for apps unopened for as little as one week. In older devices that have 8 or 16gb of storage, this could be a common issue as those users are quickly faced with storage issues.

Mac version of Cisco AnyConnect does not allow setting the "30 Day" cookie in the Duo Authentication app

When Mac users connect to Lehigh's VPN server, they are prompted to enter their username and password, followed by a Duo 2FA screen. On the Duo screen there is a checkbox to "Remember me for 30 days" but it is greyed out with an error below, prompting the user to enable cookies in order to remember the device. Enabling cookies in Safari does not fix this error. This is a known bug with the Mac version of Cisco Anyconnect, and we are waiting on a fix from the manufacturer.



Device:

Choose an authentication method

Duo Push Used automatically

Call Me

Passcode

- [What is this?](#)
- [Add a new device](#)
- [My Settings & Devices](#)
- [Need help?](#)

Powered by Duo Security

Remember me for 30 days

You need to enable cookies in order to remember this device.

There are no related labels.