

OneLogin Instructions

Activation and Use of 2-Step Authentication

<u>OVERVIEW</u>	Page 2
<u>Option 1: GOOGLE AUTHENTICATOR PHONE APP</u>	Page 3
<u>Option 2: SMS TEXT MESSAGING</u>	Page 7
<u>How to Change Authentication Methods</u>	Page 11
<u>How To Change your Default Authentication Method</u>	Page 11
<u>To Temporarily Change your Authentication Method (for a single use)</u>	Page 12
<u>Group Accounts with Multiple Users</u>	Page 13

OVERVIEW:

In an effort to increase cyber security on Palo Alto University's IT networks, and in order to be compliant with liability insurance requirements, 2-step authentication (2SA) will be enabled on all PAU community members' **OneLogin** accounts. All Palo Alto University community members who utilize **OneLogin** to access University software applications, will need to enable at least one option of 2-step authentication on their **OneLogin** account.

The two options for 2-step authentication are: the **Google Authenticator App**, and **SMS Text Messaging** via a third party, Twilio, both using your smartphone. It is required to install at least one of these options, but recommended to install both so there is a back-up method in place in case one of the methods is not functioning properly. For example, SMS Text messages may be delayed or not work based on the quality of the cell service of where you are located at any given time (i.e. it may not work in a basement). Instructions on how to install and use both of these methods are detailed below.

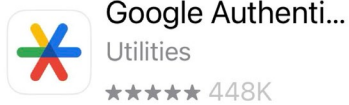
After the initial set up is complete, anytime that a PAU community member logs into OneLogin, they will be prompted to enter a unique access code into OneLogin, which will be delivered either to the Google Authenticator app on their smartphone, or via SMS text message to their mobile device. The code will need to be entered into OneLogin to gain access to any of the applications that are contained within OneLogin (i.e. GMail, Google Drive, Canvas, DocuSign, MyPAU portal, Pingboard, Qualtrics, Zendesk, etc.)

Option 1: GOOGLE AUTHENTICATOR PHONE APP

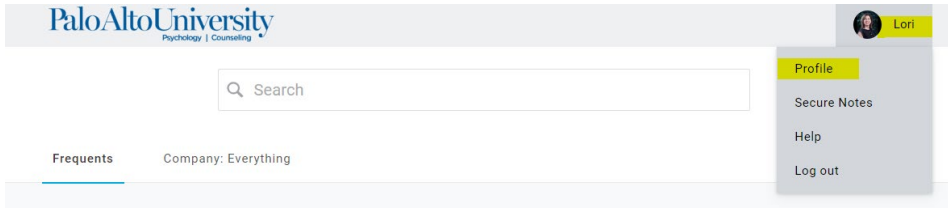
ONE-TIME Activation Steps (using your smartphone & the computer):

Overview: Associate OneLogin to your smartphone via the **Google Authenticator** app as follows:

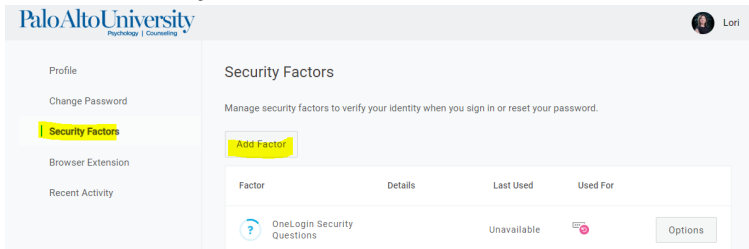
1. On your smartphone, download the **Google Authenticator** app:



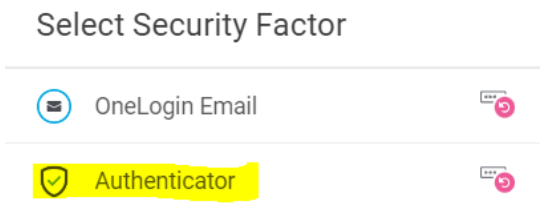
2. On your computer, log into **OneLogin** and go into your profile by clicking on your name in the top right corner:

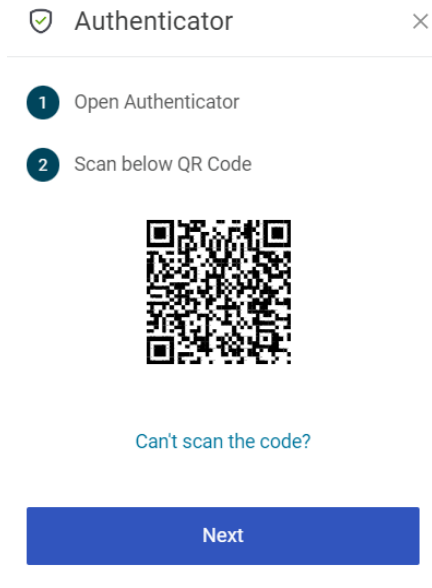


3. Click on **Security Factors**, and the **Add Factor** button:



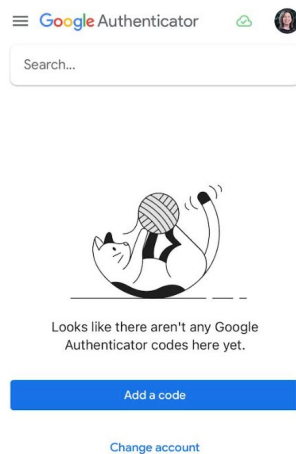
4. Click on **Authenticator** and a QR code will appear:



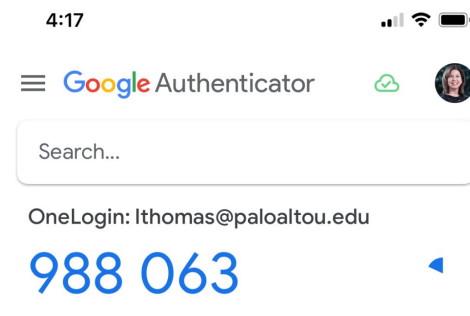


[Change Security Factor](#)

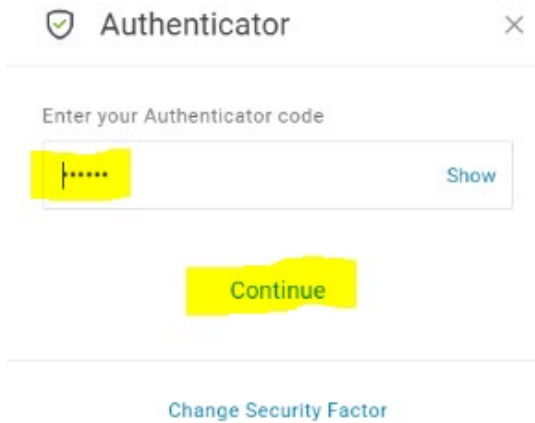
5. On your smartphone, open the **Google Authenticator** app and select **Add a Code**:



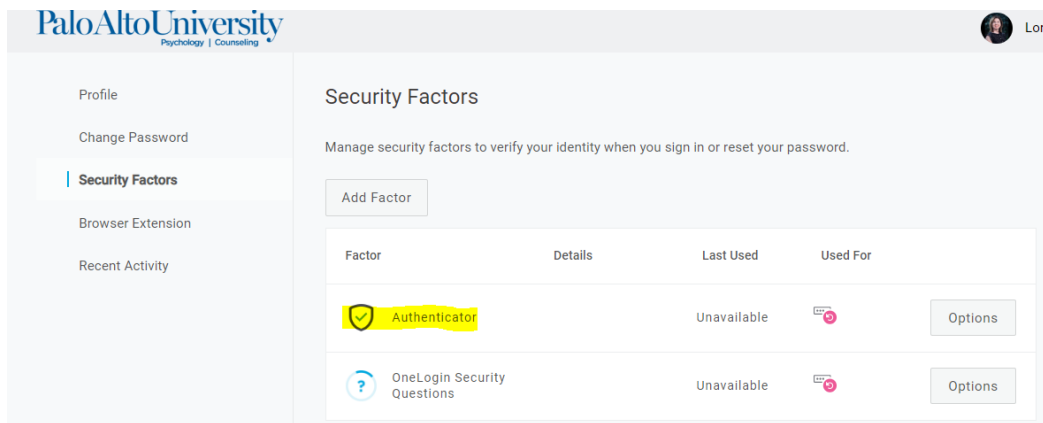
6. On your smartphone, click on **Scan a QR Code**; a 6-digit code will appear, which will change approximately every 30 seconds.



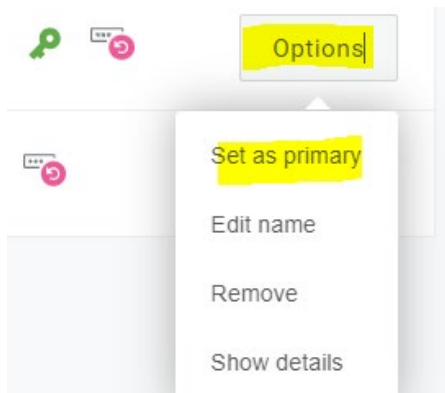
7. On your computer, click **Next** and enter the code, and then click on **Continue**



- When you see the Authenticator displayed in your profile, the one-time set up has been completed:

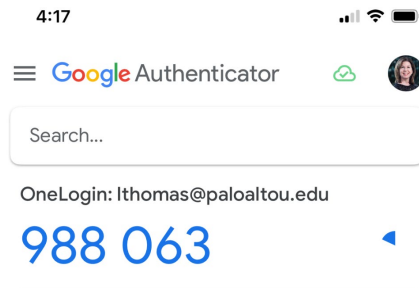


- AFTER YOU HAVE BOTH OPTIONS SET UP (AUTHENTICATOR AND TEXTING), you will need to select one as the default or “primary”. Click on the Options button to select as Primary. You may select either Authenticator, or SMS Texting as Primary:

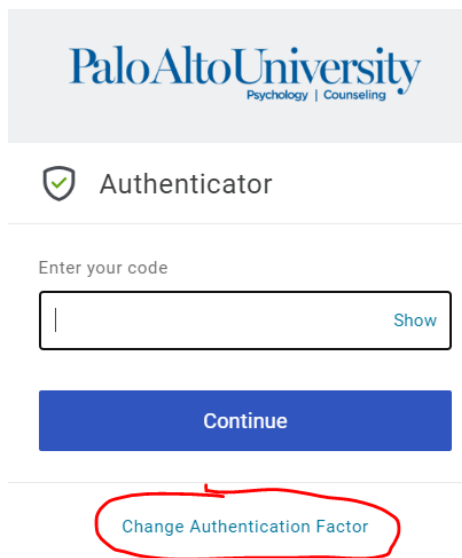


ON-GOING USE:

- Anytime that you log into OneLogin, you will be prompted to enter the unique access code (which changes every 30 seconds) that is contained within the Authenticator App on your mobile device. Depending on how the settings on your computer are configured, you may be prompted to enter the access code *only the first time* you log in each day or after rebooting, or you may be prompted to enter the access code *every time* that you log into OneLogin throughout the day.



Note: Each time you log into OneLogin, your primary option will be used. If it is not working, if you have installed the other option, you may “Change the Authentication Factor” by clicking the link as pictured below:

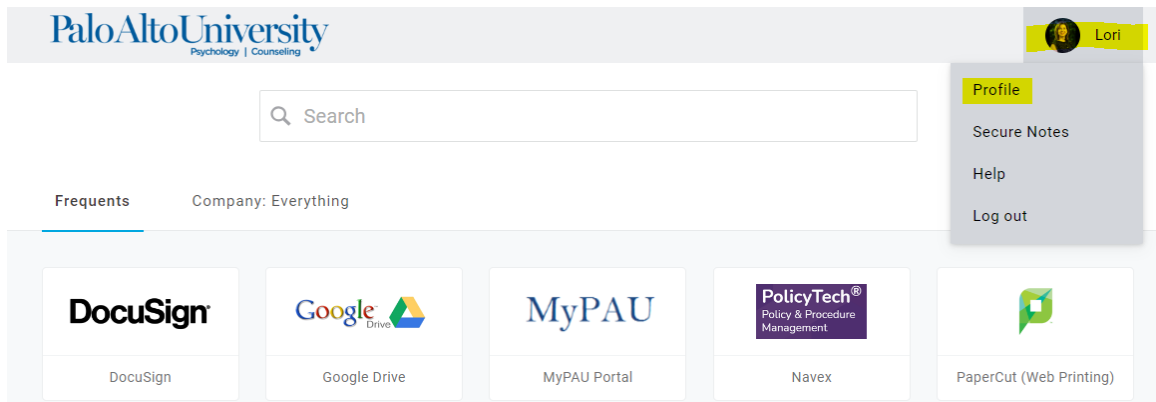


Option 2: SMS TEXT MESSAGING:

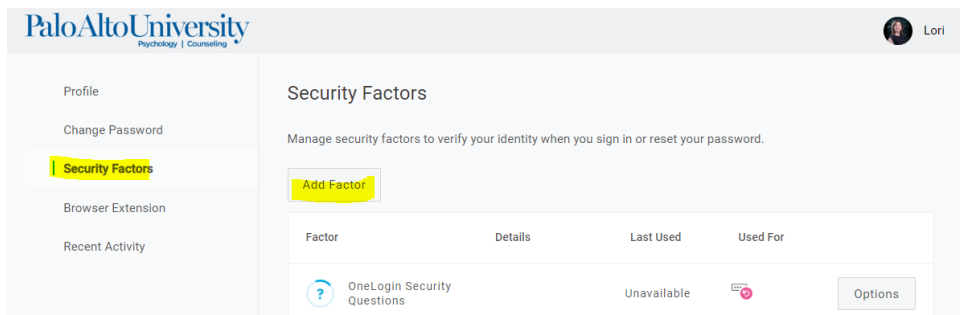
ONE-TIME Activation Steps (on your computer):

Overview: Set up your OneLogin account with SMS Texting via the third party vendor, Twilio as follows:

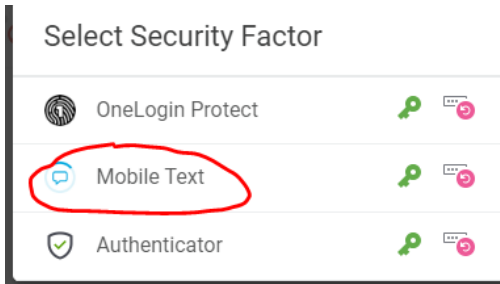
1. An Opt-In Form must be completed in order to receive SMS text messages from our vendor, Twilio. [Click here](#) to complete the form, which can also be found on the home page of the PAU Portal. The IT Department will reach out to you after they have received your form and sent your mobile phone number to Twilio.
2. Once the IT Department has given you the go-ahead, you will need to enable your OneLogin account as follows: From your computer, log into **OneLogin** and go into your profile by clicking on your name in the top right corner:



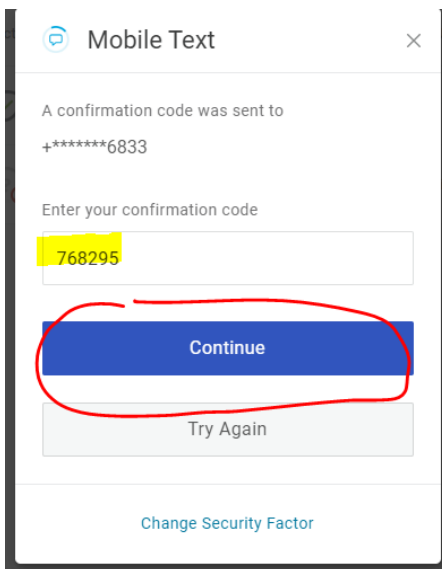
3. Click on **Security Factors**, and the **Add Factor** button:



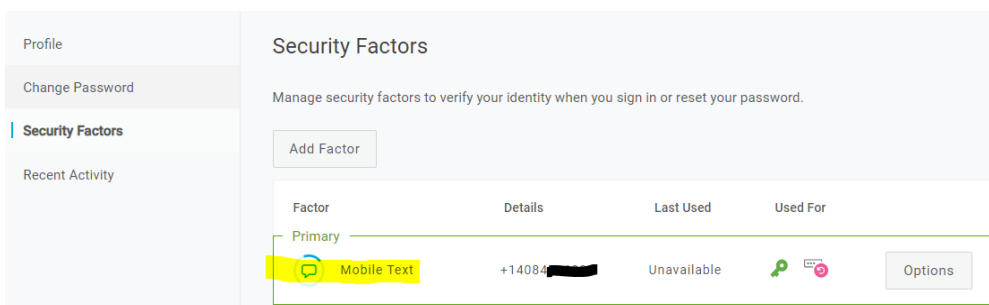
4. Select **Mobile Text**:



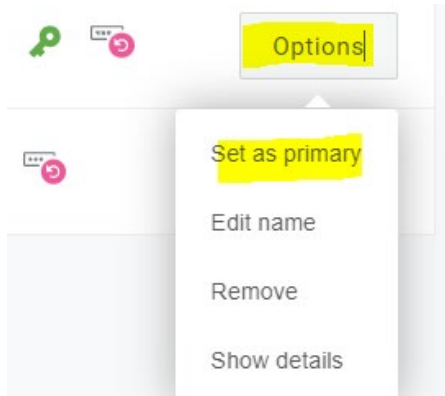
5. You will receive a code on your mobile device, **enter that code** into the OneLogin window and select **Continue**:



6. When you see the **Mobile Text** icon displayed under the Security Factors, the one-time set up has been completed:

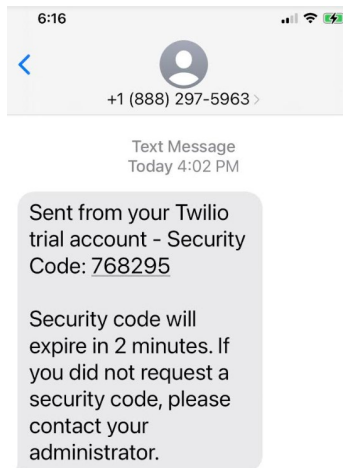


7. AFTER YOU HAVE BOTH OPTIONS SET UP (AUTHENTICATOR AND TEXTING), you will need to select one as the default or “primary”. Click on the Options button to select as Primary. You may select either Authenticator, or SMS Texting as Primary:




ON-GOING USE:

- Anytime that you log into OneLogin on your computer, you will be prompted to send a unique access code via text to your mobile device. You will need to enter the code into OneLogin to gain access. Depending on how the settings on your computer are configured, you may be prompted to enter the access code *only the first time* you log in each day or after rebooting, or you may be prompted to enter the access code *every time* that you log into OneLogin throughout the day.



Note: Each time you log into OneLogin, your primary option will be used. If it is not working, if you have installed the other option, you may “Change the Authentication Factor” by clicking the link as pictured below:

 PAU Mobile Text

Enter your code

Show

Continue

Having trouble?

[Resend SMS code](#)

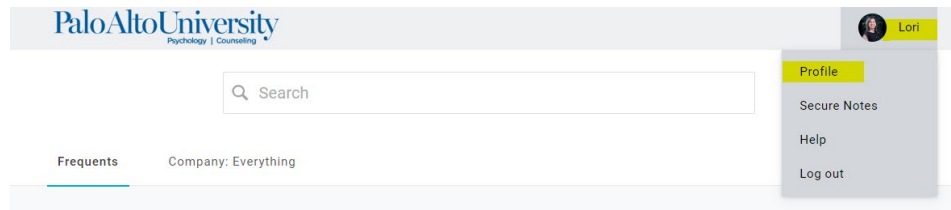
[Change Authentication Factor](#)

How to Change Authentication Methods

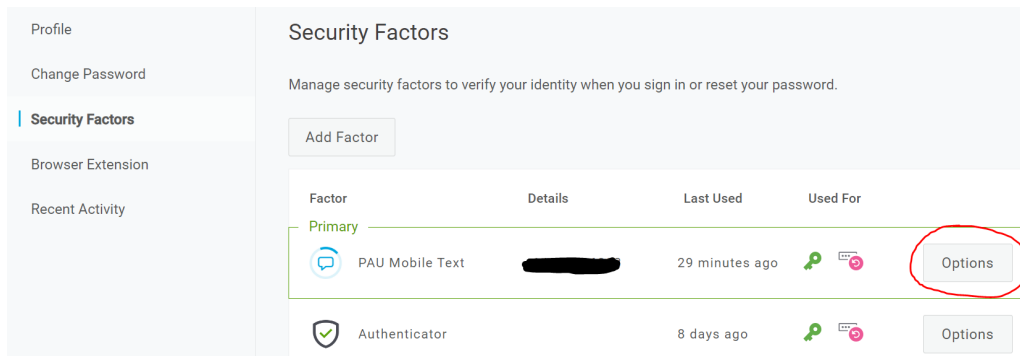
Each time you log into OneLogin, the option that is designated as the “primary”, in your OneLogin profile settings, will be used. **Only if you have both authentication methods activated in your OneLogin profile (Authenticator App and SMS Texting) can you change your method either by default (aka primary) or temporarily change the method for a single use.** You may toggle between them as often as you wish. You may decide to change methods for various reasons including: convenience of use, or if one method doesn’t work consistently, i.e. due to cell coverage is not optimal in certain circumstances to receive SMS text messages.

To Change your Default Authentication Method:

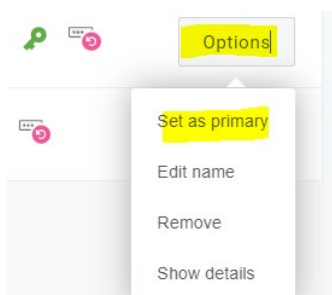
1. On your computer, log into **OneLogin** and go into your profile by clicking on your name in the top right corner:



2. Click on **Security Factors**, and click on “Options” next to the authentication method that you wish to make the default:

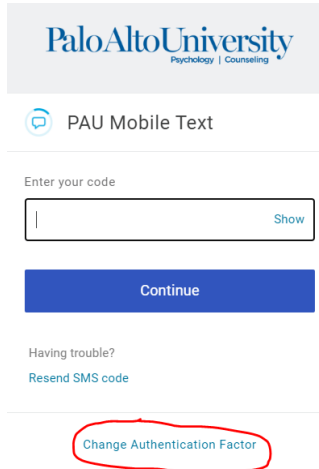


3. Select “set as primary”



To Temporarily Change your Authentication Method (for a single use):

- If your primary authentication method does not work when you log into OneLogin, you may “Change the Authentication Factor” by clicking the link as pictured below. This will change the method for a single use.



Palo Alto University
Psychology | Counseling

PAU Mobile Text

Enter your code

Show

Continue

Having trouble?
[Resend SMS code](#)

[Change Authentication Factor](#)

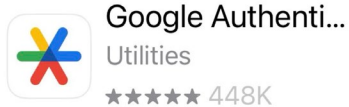
GROUP ACCOUNTS WITH MULTIPLE USERS

ONE-TIME Activation Steps for all Users who Log into the account (using your smartphone & the computer):

Overview: Group accounts that are accessed by multiple users will require each user who logs into that account to associate the group OneLogin account to their smartphone via an authentication method. It is recommended that all users use the **Google Authenticator** option. A single OneLogin account can be associated with multiple Authenticator app users. This will require some coordination via Zoom between the users as follows:

1. **The first user** who logs into the group account will need to set up the Authenticator app as follows:

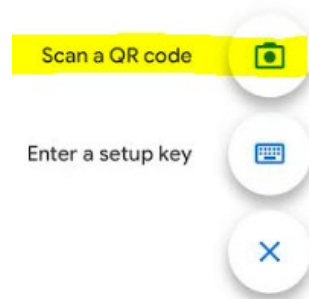
- a. On your smartphone, if you have not already downloaded the **Google Authenticator** app, you will need to do so:



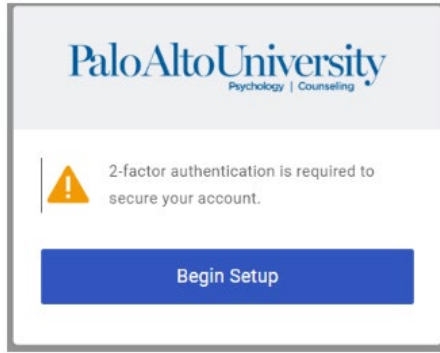
If you already have the app installed on your phone, open the app and click on the + plus sign on the bottom right corner:



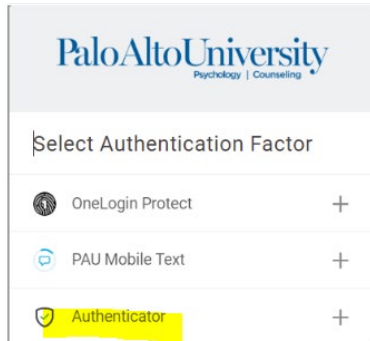
Then click on the “Scan QR” code - (keep that open and complete steps b



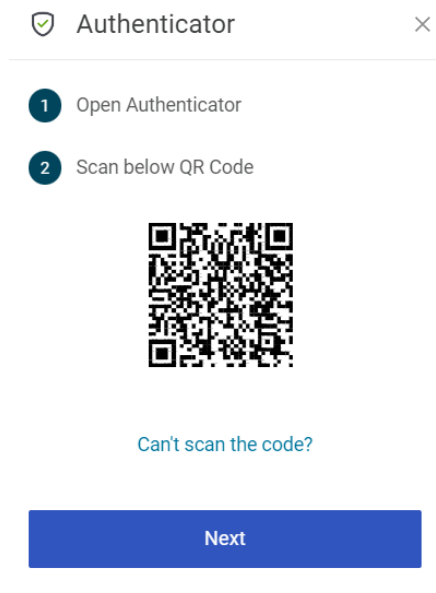
- b. On your computer, open an incognito window to log into the **OneLogin** group account. The first user to log in (before the authenticator has been set up) will see a pop-up window, click on “Begin Setup”:



c. Select the Authenticator option:

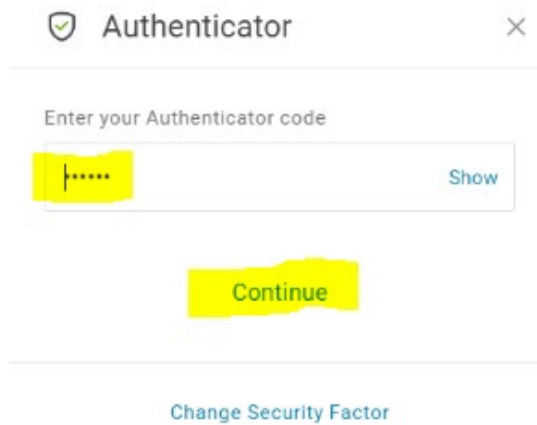


d. a QR code will appear on your computer screen, use your phone to scan it and click the "Next" button on the computer screen:

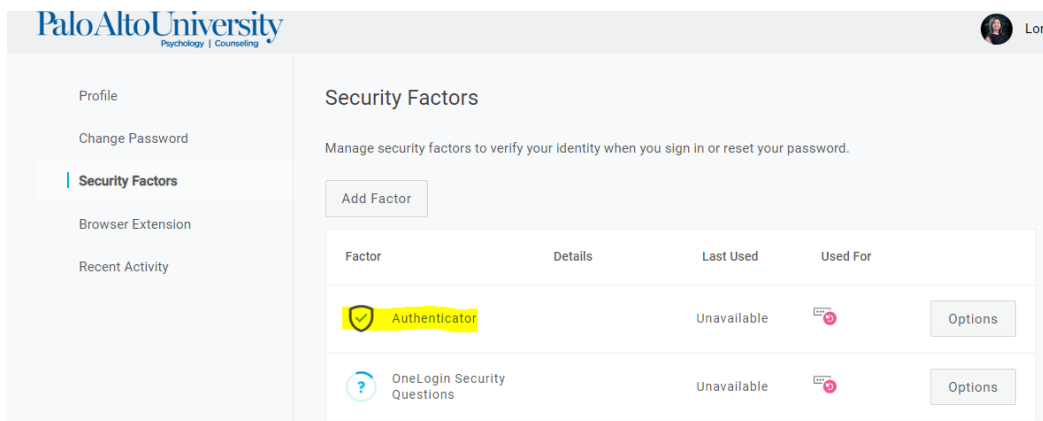


e. your phone will display a 6-digit code, enter that code on the computer screen and click "Continue":





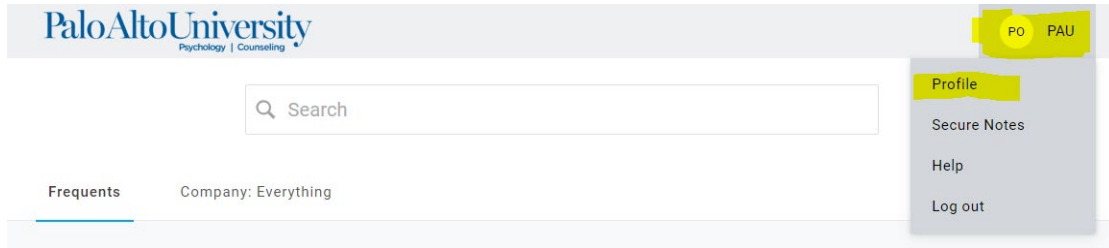
- f. When you see the Authenticator displayed in your profile, the one-time set up has been completed:



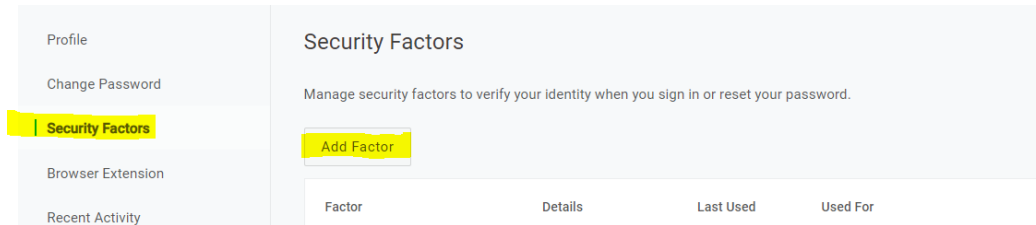
- g. You will now need to reach out to the other employees who log into the group OneLogin account and help them set up their authentication in the steps below.

2. **The first user** who has set up authentication in the group OneLogin account **will need to assist the others** who log into that account to set up theirs. A Zoom call with screen sharing will be necessary. Once one or all of the other users are on a Zoom screen share, follow these steps:

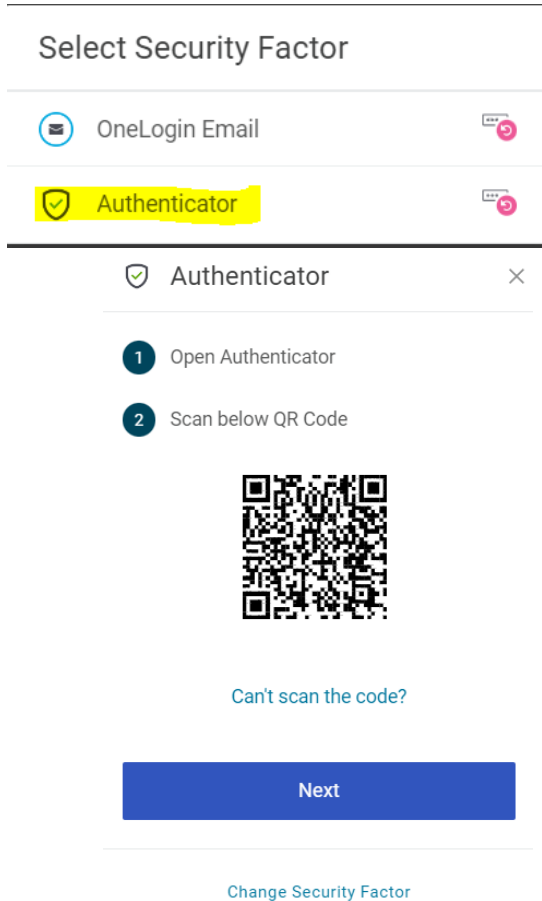
- a. **The first user** who has already set up authentication, will need to share their Zoom screen, and go into the group account's profile by clicking on the name in the top right corner:



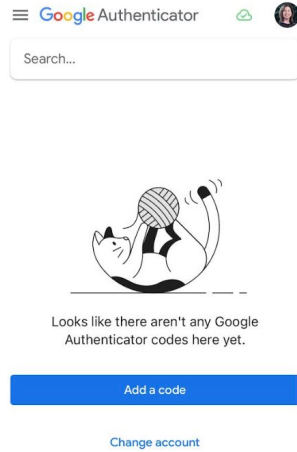
b. Click on **Security Factors**, and the **Add Factor** button:



c. Click on **Authenticator** and a QR code will appear:



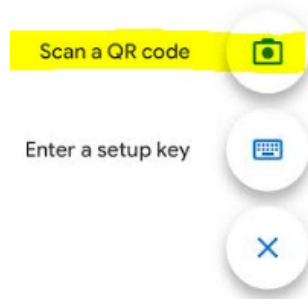
d. **One of the other users (i.e. User 2)**, will use their smartphone to open the **Google Authenticator** app and either select **Add a Code** if this is their first time using the app:



Or, if they already have the app installed, they should click on the + plus sign on the bottom right corner:



Then click on the “Scan QR” code - (keep that open and complete steps b

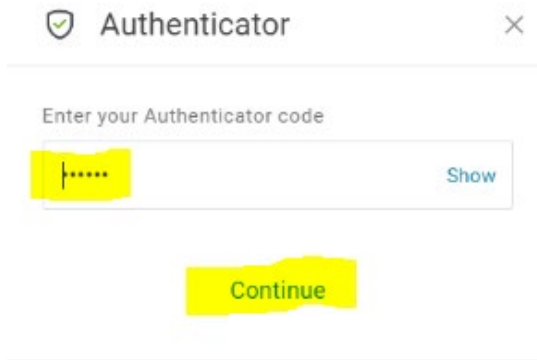


- e. **User 2** will scan the code that appears on the Zoom screen, and on their phone will appear a code that they should give to the **first user** to enter on the computer screen:

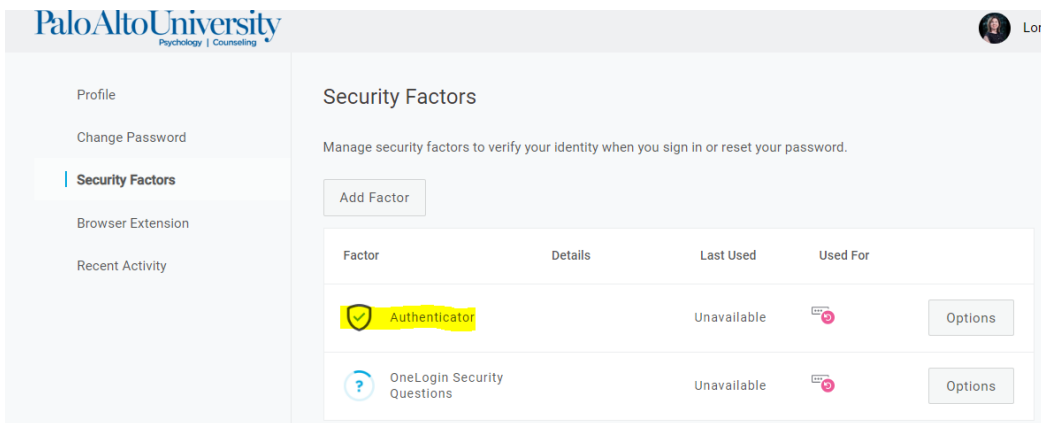
financeandops: paloaltou.onelogin.com

397 261

- f. **The first** user should enter the code on the computer, and then click on **Continue**



- g. When the **first user** sees the Authenticator displayed in the group account’s OneLogin profile, the one-time set up has been completed for that user:



- h. Steps 2a-2g should be repeated for each user who logs into the group account, until they are all added to OneLogin account successfully. The names can be changed by clicking on the “Options” button on the right, so that each user can be identified:

