IT Help Desk — Opt-in/Opt Out

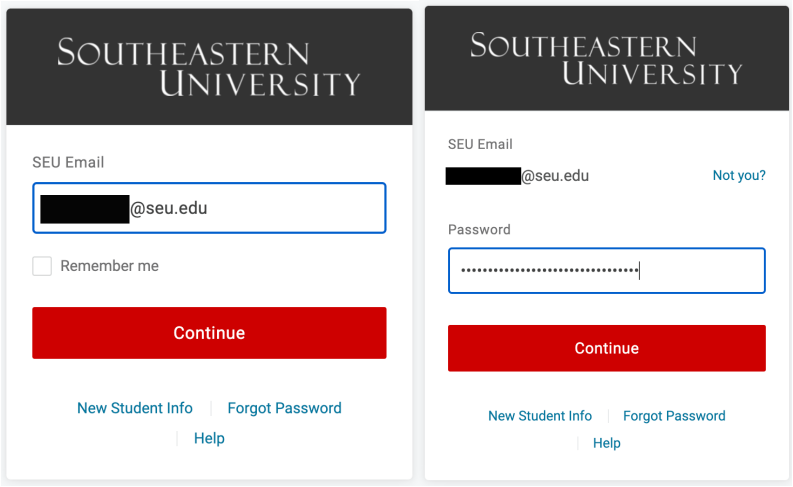
OneLogin: Southeastern University's Identity Provider (IdP) used to access most student services

Opt-in information: If you choose to use **SMS/Text** as your **Multi-Factor Authentication (MFA)** method for OneLogin, then you are **opting in** to receive messages. **Message and data rates may apply.**

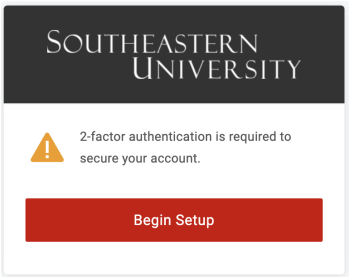
Opt-out information: If you choose to **opt-out** of receiving SMS texts from OneLogin, **then you must choose another method for Multi-Factor Authentication (MFA)**. To set up another authentication method, please see below.

Opt-out at first sign-in: If this is the first time you are signing into OneLogin and you wish to set up an MFA method other than SMS/Texting, please follow these steps:

1. On a computer, go to https://seu.onelogin.com.
2. Enter your **SEU email address** and select **Continue**. Enter your **SEU password** and select **Continue**.



3. Select **Begin Setup**.

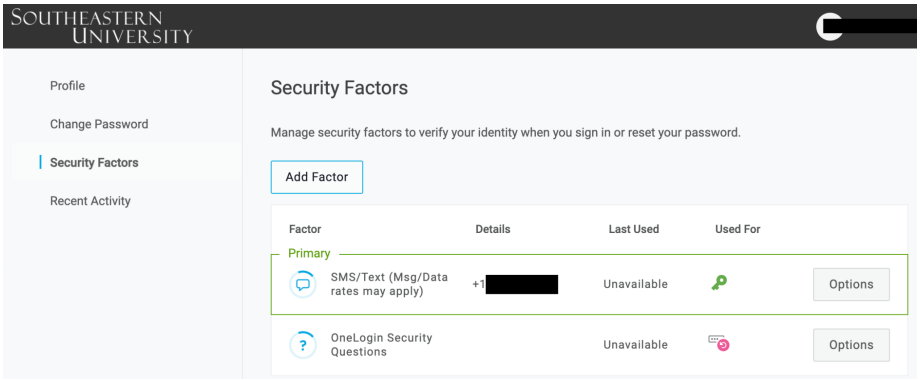


4. At this point, you will see several options for Multi-Factor Authentication besides SMS/Text. Go to the **Multi-Factor authentication methods besides SMS/Text** section below to choose which factor is best for you.

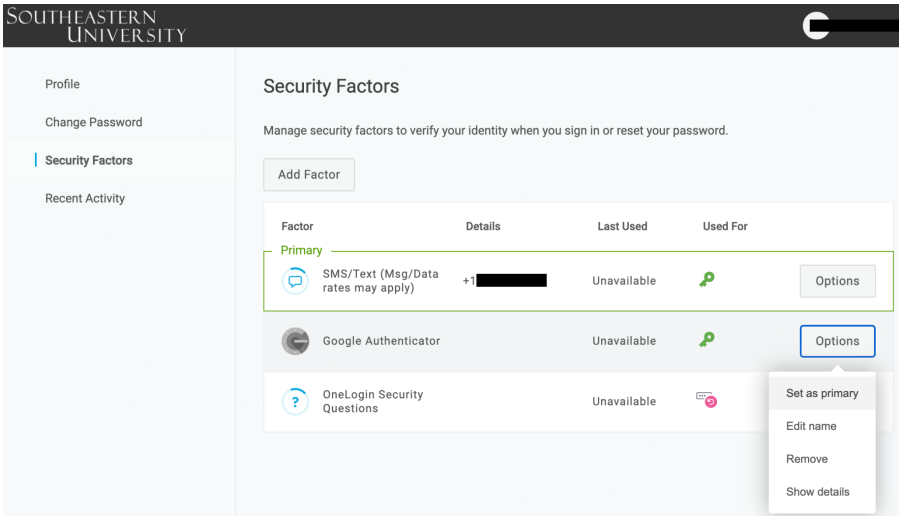
Opt-out if currently using SMS/Text: If you are currently receiving texts with your MFA code but you want to opt-out, please follow the steps below to be guided where you can change this:

1. On a computer, log into https://seu.onelogin.com like you normally would.
2. Select your name in the **upper-right corner** and select **Profile**.

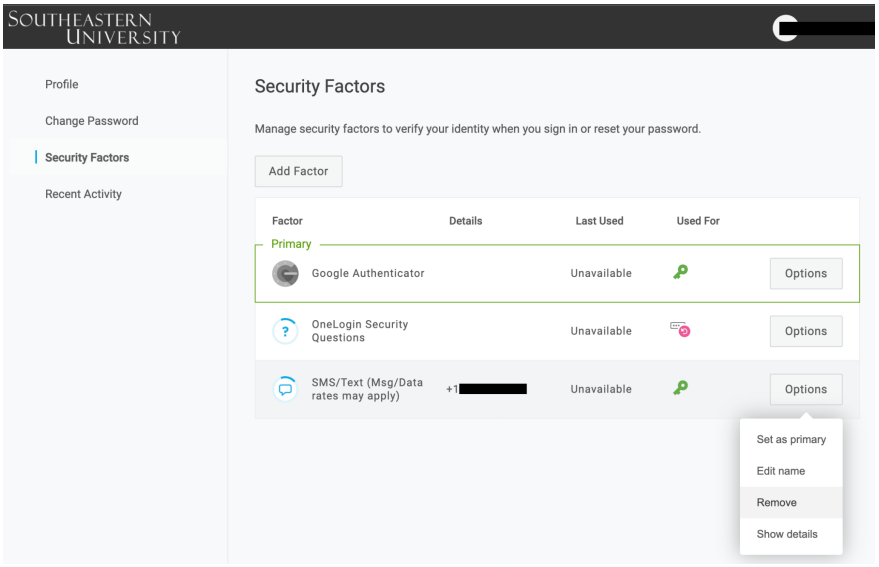
3. Select **Security Factors** on the left-hand side. Then select **Add Factor**.



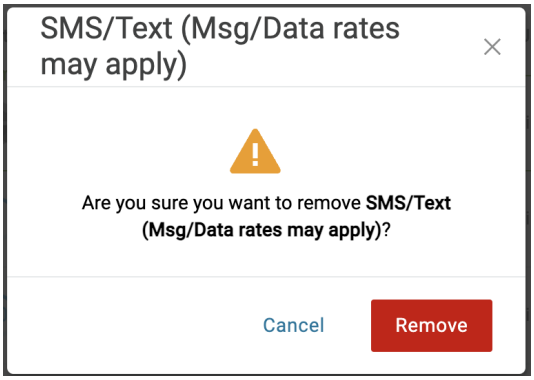
4. At this point, you will see several options for Multi-Factor Authentication besides SMS/Texts. Go to the **Multi-Factor authentication methods besides SMS/Text** section below to choose which factor is best for you. **Come back to these steps once you have set up another factor.**
5. Now that you have another factor set up, select **Options** to the right of the new factor and select **Set as Primary** (in this example, we chose Google Authenticator).



6. Select Options next to **SMS/Text (Msg/Data rates may apply)** and select **Remove**.



7. On the warning prompt, select **Remove** again.

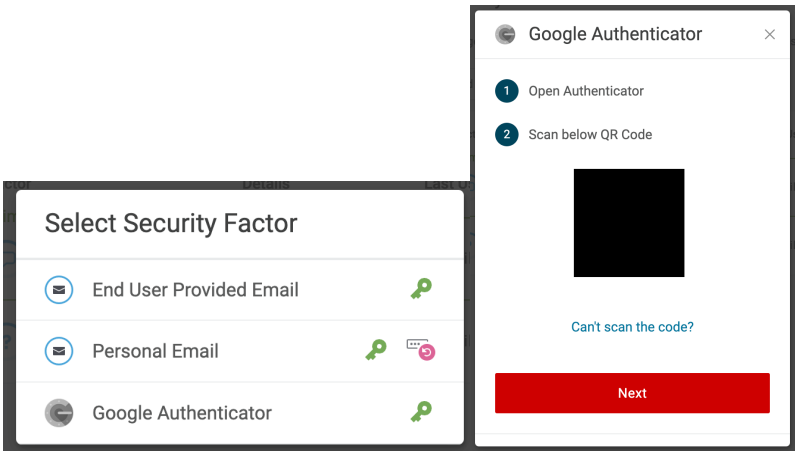


8. You are now opted out of SMS/Text.

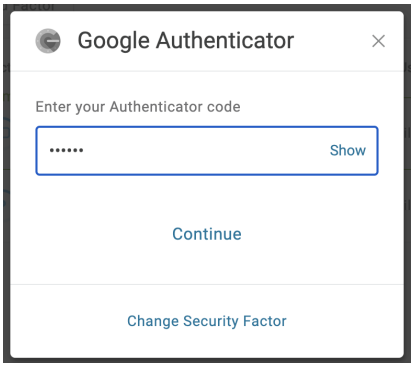
Multi-Factor authentication methods besides SMS/Text:

Google Authenticator: This is an app that you download from your phone from either the Play Store (Android) or the App Store (iPhone). It generates a 6-digit code every 30 seconds. It is highly recommended because the code will still let you log in even if your phone has no Internet access. To set up Google Authenticator, please do the following:

1. **Before** choosing Google Authenticator at the OneLogin prompt, you must download the app onto your mobile phone. Go to your app store and download **Google Authenticator**.
2. Once it is downloaded to your phone, **open Google Authenticator** and select **Get Started**. You will be presented with the options to Scan a QR code or Enter a setup key.
3. On the computer in OneLogin, choose **Google Authenticator** as your MFA method. A QR code will appear next.



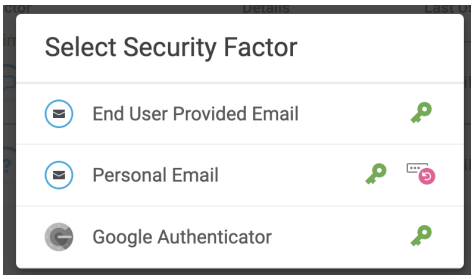
4. On your phone, select **Scan a QR code**. Use your phone's camera to scan the code.
5. Once it is scanned, you will be asked to enter a code. Enter the current code that Google Authenticator is generating and select **Continue**.



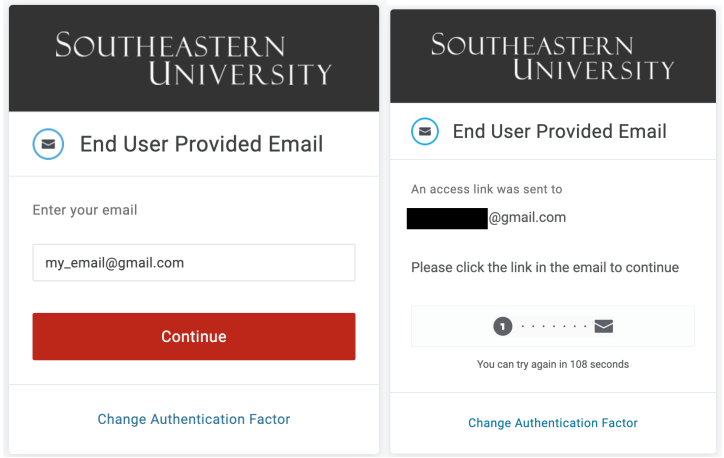
6. You can now use Google Authenticator as your MFA method. If you get a new phone in the future and the code does not carry over to the new device, you can contact the SEU IT Help Desk at (863) 667-5028 in order to receive assistance.
7. **IMPORTANT**: If you are replacing **SMS/Text** as your MFA method, please go back to the **Opt-out if currently using SMS/Text** section above to finish opting out.
8. If this was part of your first time logging in, please continue at the OneLogin website and follow the prompts until your profile is finished.

End User Provided Email: This option allows you to type in your personal email address (Gmail, Yahoo, iCloud, etc). If chosen, when you log into OneLogin, you will be sent an email to this personal email address. Click the link in the email and then you can log into OneLogin. To set up End User Provided Email, please do the following:

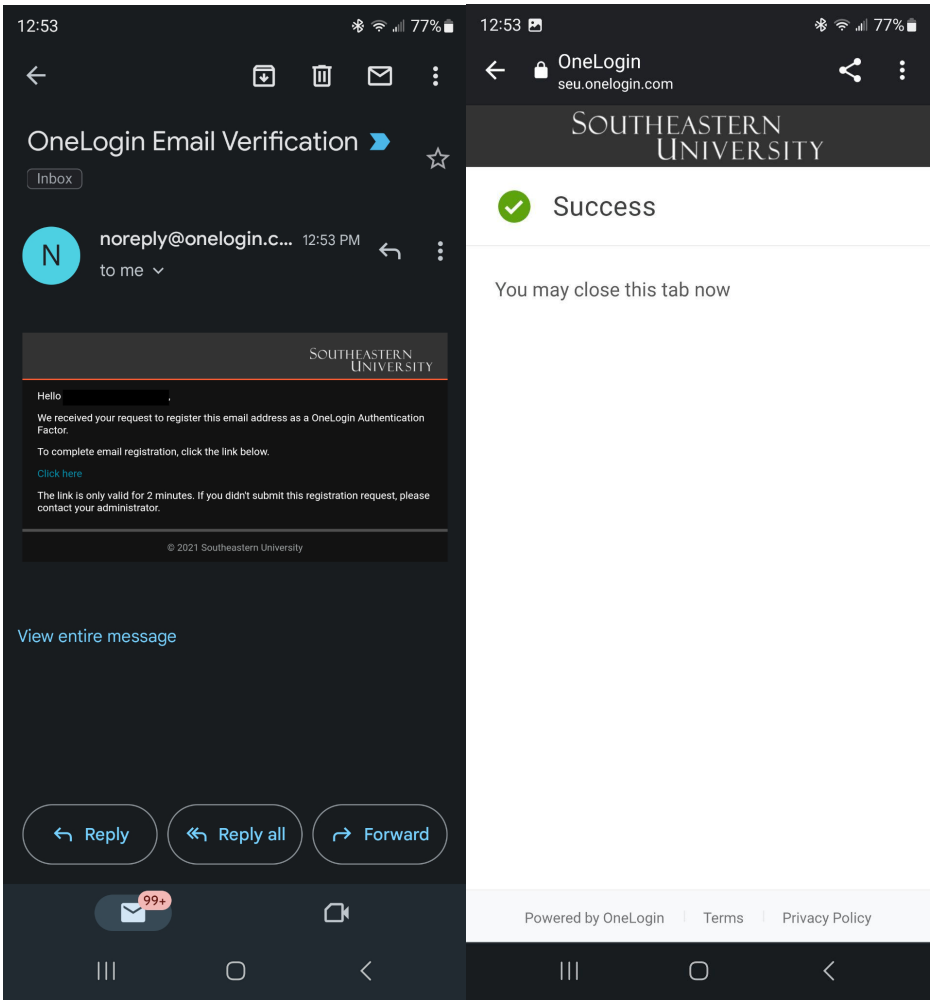
1. Choose End User Provided Email at the OneLogin prompt.



2. Enter your personal email address, one that you have consistent access to and select Continue.



3. You will be sent an email. Go to your email and open the message fromnoreply@onelogin.com with a subject of “OneLogin Email Verification”. Click the link in the email where it says **Click here**. A browser tab will open that will show a **Success** message.
    a. This is an example of what it looks like in the Gmail app on a phone.



4. The OneLogin page on your computer will refresh once the link is clicked. You now have **End User Provided Email** set as an MFA method.
5. **IMPORTANT**: If you are replacing **SMS/Text** as your MFA method, please go back to the **Opt-out if currently using SMS/Text** section above to finish opting out.
6. If this was part of your first time logging in, please continue at the OneLogin website and follow the prompts until your profile is finished.

Personal Email: This is the email that you used when you initially applied to SEU. While this works for most new students, it requires exact and up-to-date information. Because of this we recommend choosing the above option, **End User Provided Email** for both new students and returning students. That way, you have control and can type in exactly what email address you want to use to receive MFA messages.