

The University of Texas Southwestern REDCap instance requires Two Factor (2FA) authentication to access REDCap. In addition to entering username and password, you will also need to use Duo or the Google or Microsoft Authenticator app. **Please note:** this requirement only applies when logging into the REDCap application and will not affect survey respondents.

What You Need to Do

For Internal Users:

1. Internal users (Users that login to REDCap using their UTSW ID and Password) will use their existing DUO authentication setup, like other UTSW enterprise applications. After entering your REDCap username and password, a popup will appear with the available two-factor options. Select Duo, approve the request through your mobile device, and then the REDCap home page will open.

 **Two-step verification for REDCap login**


Select an option below to complete the second half of REDCap's two-step verification login process. You will not be able to access REDCap until you have completed this verification step.

☐ Don't prompt me with two-step login on this computer for 24 hours

☐	 Duo: Use Duo Push on the Duo mobile app, or alternatively use the SMS passcode or phone call method.
☐	 Google Authenticator or Microsoft Authenticator: Open the Google Authenticator or Microsoft Authenticator app on your mobile device to get the verification code associated with your REDCap user account.

Cancel

2. Additional information on Duo is available here: [Two-Factor Authentication: Information Security - UT Southwestern](#)
3. **IMPORTANT:** UTSW Project Administrators managing collaborative projects with external colleagues must share this information with their collaborators to ensure a smooth transition

External users (Users that login to REDCap using a non UTSW ID and Password) are now **required** to use Google or Microsoft Authenticator for 2FA.

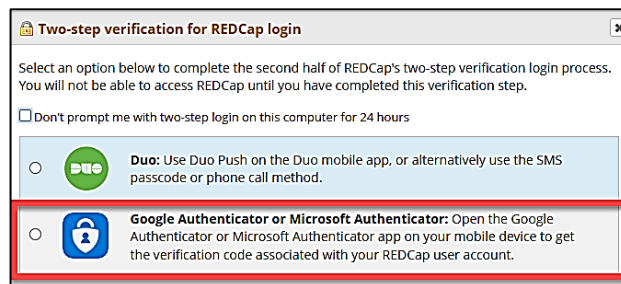
For External Users:

1. External users (Users that login to REDCap using a non UTSW ID and Password) are required to authenticate using **Google or Microsoft Authenticator**.
2. Upon account creation in REDCap, you will receive an email from the REDCap Administrator containing a link to your unique QR code and instructions for using Google or Microsoft Authenticator. Please follow the steps below to log in to REDCap successfully.

1. Google or Microsoft Authenticator will need to be downloaded to your mobile device from the relevant app store links:
 1. [Google store](#) (Android)
 2. [Apple store](#) (iPhone)
2. In the email you received, click the QR code link and the QR code should open in a new window.

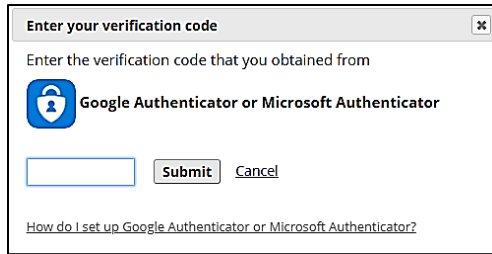


3. Open the app and scan the QR code.
4. Use the app to generate a verification code. After you have scanned the QR code using the Google Authenticator or Microsoft Authenticator app, you can open the app at any time in the future to obtain your verification code for REDCap. The verification code is always changing, so it will be different each time you log in. NOTE: The app does not require an internet connection on your device in order to work.
5. Enter the code in the Google or Microsoft Authenticator window, and then click Submit to log into REDCap. The next time you log into REDCap, select:



Follow the instructions on screen to generate a verification code and enter it to login.

3. A second dialog will pop up asking you to input a verification code: enter the verification code from Google or Microsoft Authenticator. Click **Submit** and you should be authenticated!



Enter your verification code

Enter the verification code that you obtained from

 Google Authenticator or Microsoft Authenticator

[How do I set up Google Authenticator or Microsoft Authenticator?](#)

If you need further assistance, or if you did not setup your profile before the email option was removed, please submit a [SERVICEDESK](#) email so we can promptly assist you.

Thank you for your cooperation as we enhance the security of our REDCap environment.