



Title: Two-Factor Authentication (2FA)	Area: REDCap
	Version No.: 1.0
Owner: WE-SPARK Health Institute	Document Type: SOP
	Initial Issue Date: 05-Nov-2022
	Effective Date: 05-Nov-2022
	Pages: 4

1.0 Procedure Description

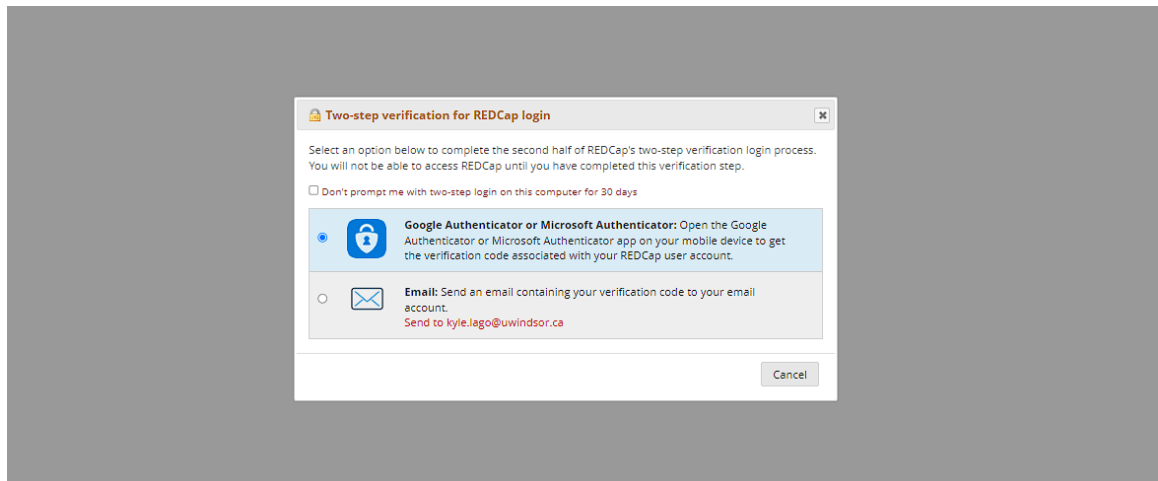
This Standard Operation Procedure (SOP) serves as the official documentation on using 2FA to log into REDCap.

2.0 Persons Affected

Applies to all REDCap Users.

3.0 Procedure

As of November 5th, 2022, the WE-SPARK Health Institute instance of REDCap will require all users to perform additional steps to log into REDCap. When logging in, users will notice an additional authentication step from simply entering their REDCap username and password.



DISCLAIMER: This material has been prepared solely for internal use at WE-SPARK HEALTH INSTITUTE. WE-SPARK HEALTH INSTITUTE accepts no responsibility for use of this material by any person or organization not associated with WE-SPARK HEALTH INSTITUTE. No part of this document may be reproduced in any form for publication without the permission of WE-SPARK HEALTH INSTITUTE. This is a controlled document. Any documents appearing in paper form are not controlled and should always be checked against the electronic version prior to use. The electronic version should always be considered the most current and accurate version.



Title: Two-Factor Authentication (2FA)	Procedure No.: REDCap 2FA 1.0
	Page No.: 2 of 6

Users will have to options for authentication to log into their REDCap accounts. They will be either need to have a verification code sent to the primary email associated with their REDCap account or utilize the Google or Microsoft Authenticator app on their smart devices.

3.1 Email log-in method

When prompted, users can select the email option to have the verification code sent to their email address. Once the email is received, they can copy the code into the field on the log-in screen to access their account.

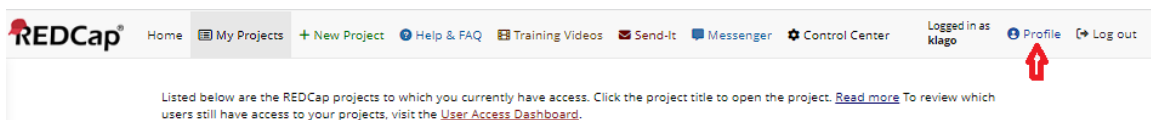
Users will need to use the email log-in method for their first sign-in attempt once 2FA is enabled.

They will then be able to access their REDCap profile to set up the Google or Microsoft Authentication method.

3.2 Google Authenticator or Microsoft Authenticator App

Users can also utilize the Google or Microsoft Authenticator app on their smart devices. These apps can be downloaded on the Google Play or Apple store.

Once the app is downloaded on their smart device, users must access their REDCap profile as seen in the following image.





Title: Two-Factor Authentication (2FA)

Procedure No.: REDCap 2FA
1.0

Page No.: 3 of 6

Within the “Edit Your User Profile” page, they will now see “Login-related options.” Select “Set up Google Authenticator or Microsoft Authenticator for two-step login.” They will then have a pop-up that will provide further instruction, including a QR code.

Follow the prompts in the Google or Microsoft Authenticator app to add an additional account, which will then request users to scan a QR code. Scan the QR Code in REDCap to finalize the account.

Edit Your User Profile

If you wish, you may edit your User Profile information below. This information will not be given out to anyone but will be used to help us better keep track of who is using REDCap and also in case you need to be contacted regarding your access to REDCap.


Basic Information

First name:


Kyle


Last name:

Lago

 Primary email:

kyle.lago@uwindsor.ca

 Phone number:


 Mobile phone number:

Tip: To enter a number with an extension, place a comma between the number and the extension.

Save Basic Info

Login-related options:

Reset password

 Set up Google Authenticator or Microsoft Authenticator for two-step login

Title: Two-Factor Authentication (2FA)	Procedure No.: REDCap 2FA 1.0
	Page No.: 4 of 6

If you wish, you may edit your User Profile information below. This information will not be given out to anyone but will be used to help us better keep track of who is using REDCap and also in case you need to be contacted regarding your access to REDCap.

Basic Information
First name:
Last name:
☒ Primary email
Phone number
Mobile phone

Login-related
Reset password
Set up two-step login

Super API Token
You have been using this method. To obtain a new token, click here.

Additional Options
While your primary email is used when sending verification codes, you can also specify a secondary email address.
Secondary email
Tertiary email

User Preferences
Set your preferences
Date and time

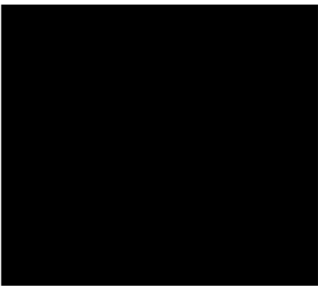
Set up Google Authenticator or Microsoft Authenticator for two-step login

To use two-step verification to log in to REDCap using Google Authenticator or Microsoft Authenticator mobile app, you will need to first download the app onto your mobile device. Use a link below to download the app on your mobile device.

1) Download the Google Authenticator or Microsoft Authenticator app to your mobile device

Download the app by searching for 'Google Authenticator' or 'Microsoft Authenticator' in your mobile device's app store (e.g., Apple App Store, Google Play Store).

2) Open the app, and scan this QR code [View QR code in separate window](#)



Scan the QR Code provided here in your authenticator app.

If you're having trouble scanning the QR code, enter the values below into your Google Authenticator app using the Manual Entry method. Also, make sure you set it as 'Time-based'.

Account: **klago@redcap.uwindsor.ca**
Key/secret: **4FEUOGX2CDFUUKT2**

3) Use the app when you log in to REDCap

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.**

Close



Title: Two-Factor Authentication (2FA)	Procedure No.: REDCap 2FA 1.0
	Page No.: 5 of 6

Now when logging into REDCap you can select the Google Authenticator or Microsoft Authenticator option. REDCap will ask you to enter your verification code. Open the Authenticator app on your smart device, and enter the code listed into the field in REDCap.

Codes are time-based so ensure you enter it before it expires. They will display the expiry time within both apps.

4. Authentication Interval

Users will have the option to have their trusted device/computer be remembered for **30** days. This will allow them to avoid 2FA on the trusted device for that time and they will be able to log-in with their username and password. We recommend enabling this on devices that are used frequently for REDCap.



Title: Two-Factor Authentication (2FA)	Procedure No.: REDCap 2FA 1.0
	Page No.: 6 of 6

5.0 Review/Revision History

Date	Revision No.	Revision Type (Minor edit, moderate revision, complete revision)	Reference Section(s)
2022-Nov-05	2.0	New SOP	

DISCLAIMER: This material has been prepared solely for internal use at WE-SPARK HEALTH INSTITUTE. WE-SPARK HEALTH INSTITUTE accepts no responsibility for use of this material by any person or organization not associated with WE-SPARK HEALTH INSTITUTE. No part of this document may be reproduced in any form for publication without the permission of WE-SPARK HEALTH INSTITUTE. This is a controlled document. Any documents appearing in paper form are not controlled and should always be checked against the electronic version prior to use. The electronic version should always be considered the most current and accurate version.