Setup REDCap Two Factor Authentication: UH Credentialed Users

To provide more secure access and to further protect the UH network and applications, there will be an update to the UH REDCap login process that may impact you.

Two-factor authentication upon login will be required for any user accessing UH REDCap outside the UH Network. Two-factor authentication requires you to confirm your identity with additional information beyond your UH username and password. Two-factor authentication adds an extra layer of protection against fraudulent cyber activity.

Since additional security measures are already in place for users accessing UH REDCap while connected to the UH Network (e.g. onsite at a UH facility or connected via VPN/VDI), two-factor authentication will not be required upon login if you're already connected to the UH Network.

- On network: onsite at UH facilities or connected to VPN/VPI
  - Users accessing REDCap while connected to the UH network will not be impacted.
- Off network: on a public device not connected to VPN/VPI or via a device connected to UH GUEST network

UH credentialed users (anyone that has a UH email and/or UH network ID) accessing UH REDCap off network will use the UH preferred authenticator app, SECUREAUTH Authenticate.

Additionally, UH credentialed users will have the ability to setup two-factor authentication in two ways.

1. Proactively while on network via the user's REDCap Profile. This options allow users that anticipate accessing REDCap off network the ability to setup two-fact authentication before logging in Off Network. If not setup in advance, the user will be prompted to setup two-factor authentication at login when accessing REDCap off network.
2. Upon login post implementation as user accesses REDCap off network.

For both setup options, please see the UH REDCap two-factor authentication setup instructions below.

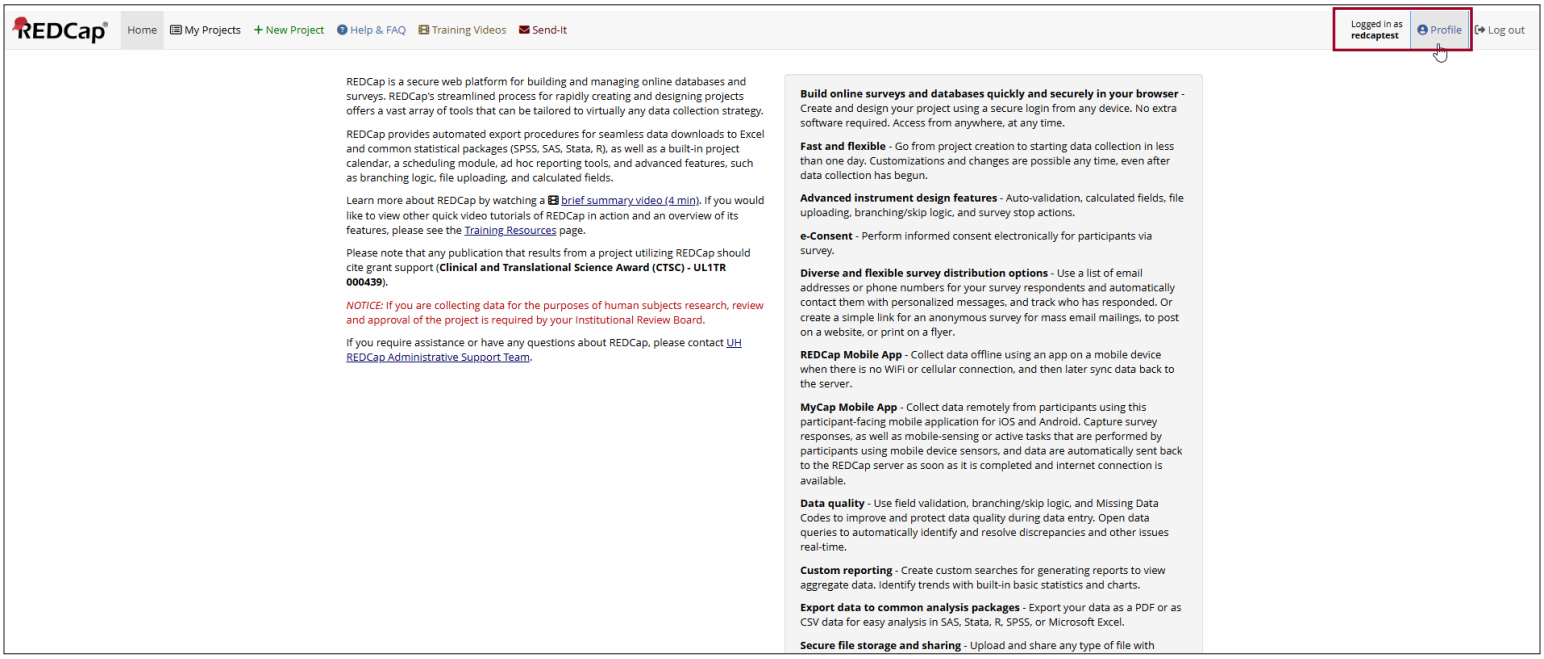
University Hospitals

University Hospitals Clinical Research Center

Setup UH REDCAP Two-Factor Authentication via REDCap Profile
(On UH Network)–UH Credentialed Users

Step 1: Ensure the SECUREAUTH Authenticate application has been installed on your mobile device. *If not already installed, UH Credentialed Users can reference the following instructions to download this application to your mobile device: UH Secure Remote Access (SecureAuth).*

Step 2: While connected to the UH Network, log into UH REDCap and navigate to the "Profile" icon.



Step 3: Navigate to the "Login-related options" section and select "Set up Google Authenticator or Microsoft Authenticator for two-step login" button which will prompt you to download an authentication application.

Step 4: The following popup will appear (the QR code will be present).

Step 5: Open the Authenticate application on your mobile device.

Step 6: Navigate to and select the QR code button.

Step 7: Scan the QR code provided in RedCap

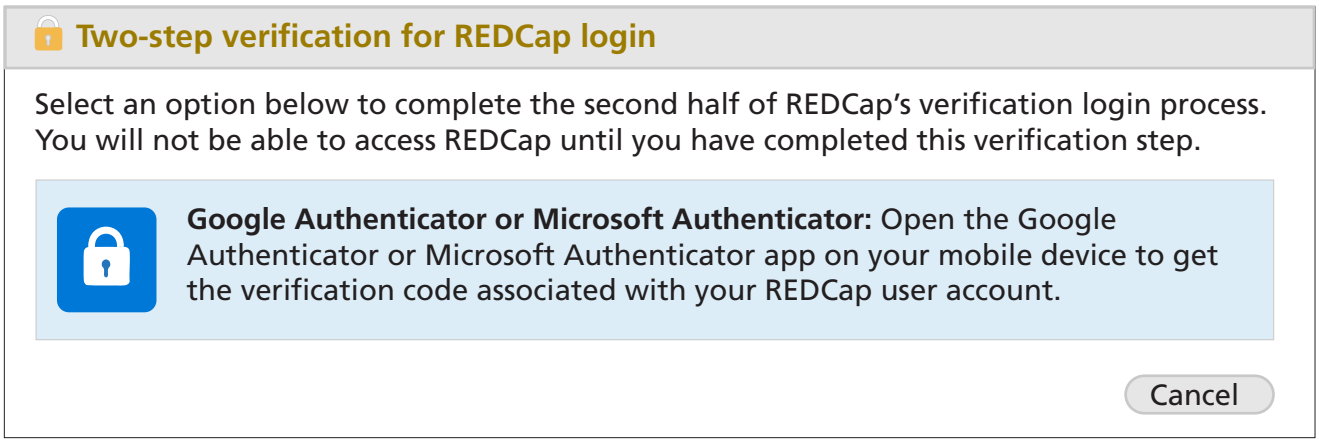
Step 8: On your dashboard, you will find the UH REDCap 6-digit web code.
You will notice a web code listed as "REDCap." Moving forward, you will use the verification code provided within the authentication application when logging into REDCap. This verification code cycles every 10 seconds, and therefore, will not be the same verification code every time you login

Step 9: Two-factor authentication setup is now complete!

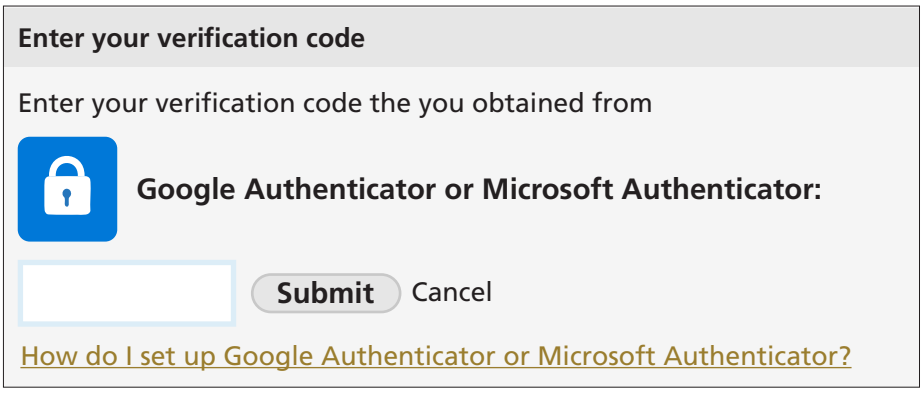
Setup UH REDCap Two-FActor Authentication via Login
(Off UH Network)–UH Credentialed Users

Step 1: Ensure the SECUREAUTH Authenticate application has been installed on your mobile device. *If not already installed, UH Credentialed Users can reference the following instructions to download this application to your mobile device: UH Secure Remote Access (SecureAuth).*

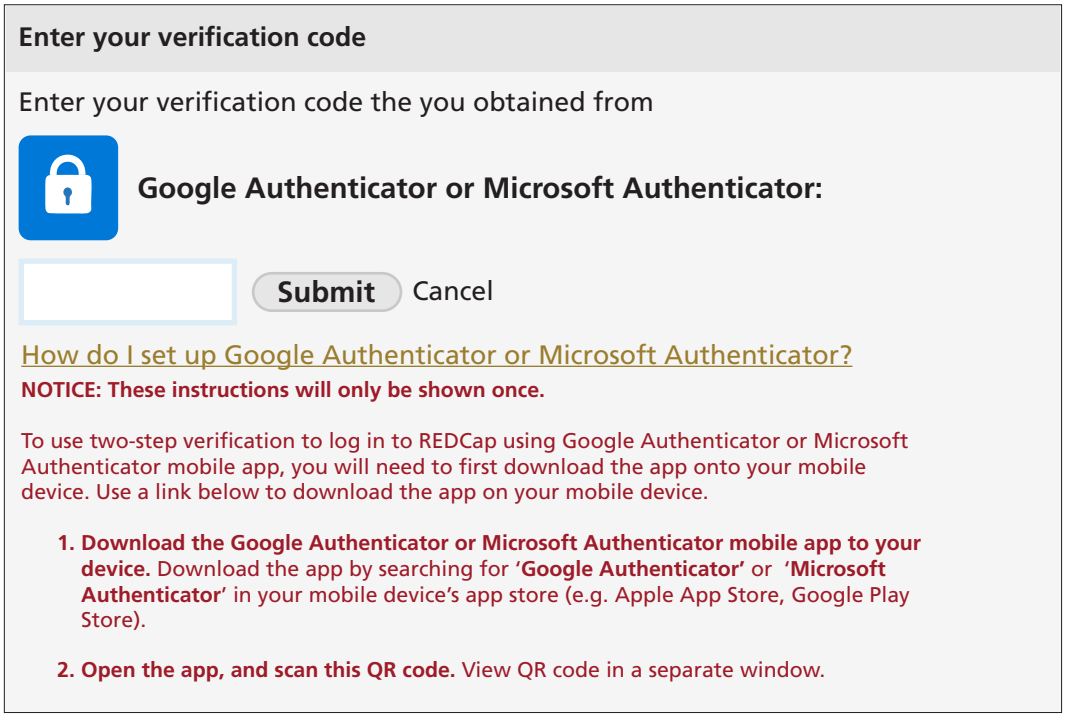
Step 2: Upon login select the option "Google Authenticator or Microsoft Authentication".



Step 3: Click the link: "How do I set up Google Authenticator or Microsoft Authenticator?"
Please note, for UH Credentialed Users, Secure Auth (which is the preferred authenticator for UH) is also supported. Please continue following these steps.



Step 4: The following popup will appear (the QR code will be present).



Step 5: Open the Authenticate application on your mobile device.

Step 6: Navigate to and select the QR code button.

Step 7: Scan the QR code provided in RedCap.

Step 8: On your dashboard, you will find the UH REDCap 6-digit web code.
You will notice a web code listed as "REDCap." Moving forward, you will use the verification code provided within the authentication application when logging into REDCap. This verification code cycles every 10 seconds, and therefore, will not be the same verification code every time you login.

Step 9: Two-factor authentication setup is now complete!