Setting up Two-Factor Authentication

- Initial Set Up (First Login)
  - Using Google Authenticator
  - Using Phone or SMS Options
  - Generating Backup Tokens
- Subsequent Logins
  - Change your Authentication Method

Some project spaces require users to login using two factor authentication (2FA). This is an extra security step that requires you to input a token from generated by your phone (via call, SMS, or Google authenticator app) before you can complete your login to CommCare.

Initial Set Up (First Login)

When a web user or web apps user first logs in, they will be prompted to set up their 2FA as seen below. To begin, click “Enable Two-Factor Authentication”:

There are three methods you can use to generate a 2FA token—Google authenticator (an app that runs on Android or iOS smartphones), a phone call, or a text message. Select the method you would like to use for receiving tokens.

Using Google Authenticator

If using Google Authenticator, you’ll need to first download the Google Authenticator app from the PlayStore or App Store. Once you install it, you’ll need to confirm your account, and then press the + button on the upper right hand corner.
Click scan barcode, and then scan the QR code CommCare has generated for you. Google Authenticator will produce a token that you can put into the Token box, and proceed. Note that tokens in Google Authenticator change every 10 seconds, so you need to type this in a timely manner.

**Using Phone or SMS Options**

If you select phone or SMS, you'll be promoted to put in your phone number, including + and the country code.

Once you've entered your phone number, you will receive a phone call or SMS with your token.

**Generating Backup Tokens**

You can also generate backup tokens to use whenever you're unable to generate a fresh token (e.g. you're not near your phone, or you're out of country using a different SIM card). It's always good to keep these on hand for situations where you think you might not be able to access your normal 2FA method. To generate backup tokens:

1. Go to the settings widget at the upper right hand corner, that looks like a gear icon
2. Select "My Account Settings"
3. Click on Two Factor Authentication
4. Click on "Show Codes" under the heading Backup Tokens
Subsequent Logins

Every time you sign into CommCare HQ you will be asked to enter a token. Keep your phone nearby so you can easily get the token from your Google Authenticator app, the phone call, or SMS that CommCare sends you.

If you are using the Google Authenticator app for two factor authentication then you will have 30 seconds to enter the code displayed otherwise a new randomly generated code will be created and the timer will reset. Please enter the code displayed by the Authenticator app before the 30 second timer expires, but if you miss the first 30 second window it will still be valid for an additional 30 seconds.

For SMS codes, once received please enter them within 2 minutes for the code to be accepted, if you miss this window please resend a new valid code to be entered.

Change your Authentication Method

Users are able to change their authentication method. To do this, please:

1. Go to the settings widget at the upper right hand corner, that looks like a gear icon
2. Select "My Account Settings"
3. Click on Two Factor Authentication
4. Select "Re-Set Two Factor Authentication" (see image above). This will make you go through the process of updating your two-factor process. Before doing this, please make sure you have tokens available to confirm your original two-factor, as the system will make you go through the process again.