Two-Factor Authentication with Mobile App

Two factor authentication enables you to provide extra security to your Concordia account, by requiring not only something you 'know' (password) but also something you 'have' (mobile phone) in order to successfully login.

A recommended way to do two-factor is through a app on your mobile phone. Any time you attempt to login, you open the mobile app and enter PIN code displayed into your browser window. Someone not in possession of that phone will be unable to login even if they know your password.

Setup

Before you can begin to use two-factor you must setup the app on your phone, then link it to your account. You must have your phone with you to set this up.

1. You need to install a mobile app to begin. We recommend the Google Authenticator app which is available for Android and iOS. The remainder of the instructions will reference this app, though others operate very similarly.

   Android:
   https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_CA

   iOS: https://itunes.apple.com/ca/app/google-authenticator/id388497605?mt=8

2. Browse to https://onlineservices.concordia.ab.ca/, logging in, and going to the Change Password page.

   There you will see options for managing your two-factor authentication.

TWO-FACTOR AUTHENTICATION

Two-factor authentication provides you with more security by adding an extra verification step when you login to your account. To add two-factor authentication to your account, please select your desired two-factor authentication method below and follow the instructions that appear.

Please select your desired two-factor authentication method

Please select ⌄

Your Devices

Serial	Description	Last Used	Action

If there are no devices listed under "Your Devices", two-factor is not enabled on your account.

2. From the drop-down select "Authenticator App" and fill in a description (optional).

Please select your desired two-factor authentication method
Authenticator App ∨

Option 1: Authenticator App

1. Download an authenticator app onto your mobile device. We suggest the Google Authenticator app. Android iOS
2. Optionally enter a description for your device.
3. Click the Add Device button to generate a QR code.
4. Scan the QR code with your authenticator app.
5. After scanning the QR code, an entry for the Concordia website will be saved into your authenticator app. A 6 digit number will appear in that entry and will regenerate every few minutes.
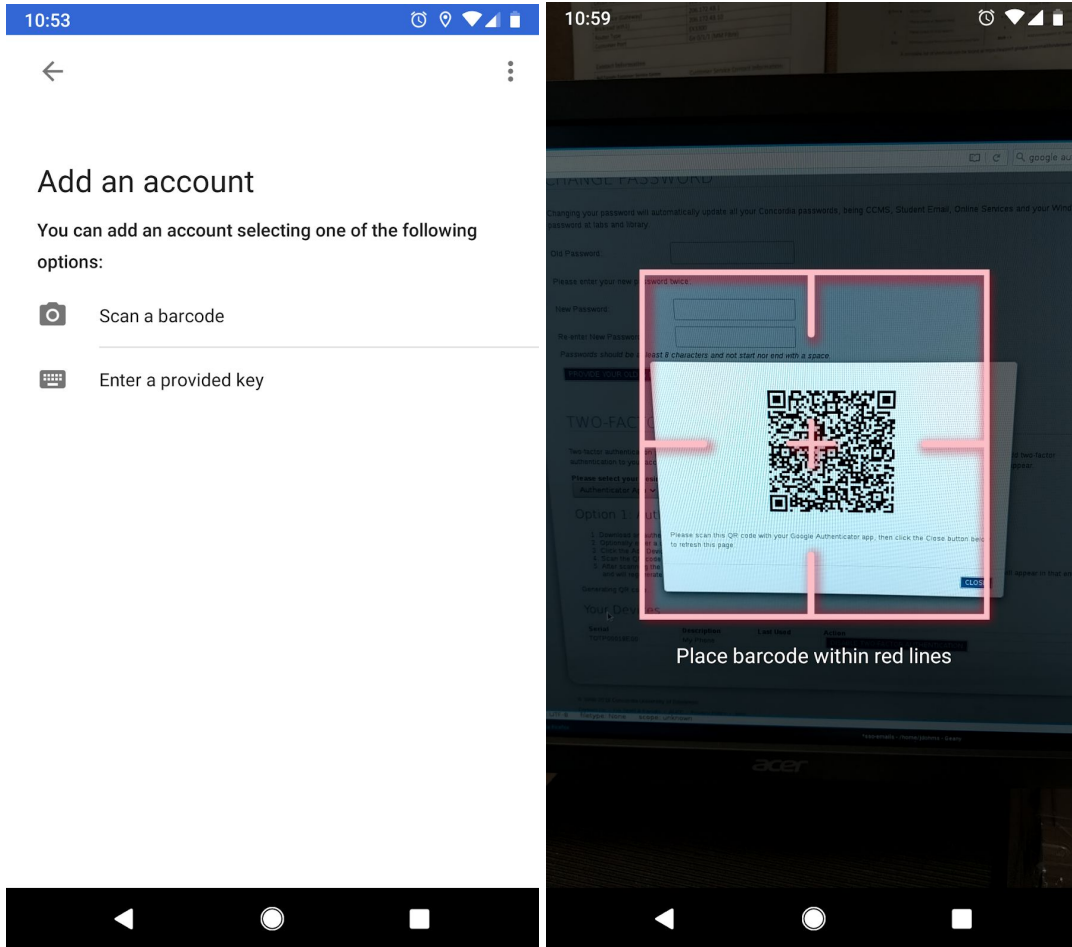
**Device Description (optional):** My Phone

ADD DEVICE

Your Devices

3. Click Add Device
4. A QR code will be displayed in your browser like below.

Please scan this QR code with your Google Authenticator app, then click the Close button below to refresh this page.

CLOSE

5. Open the Authenticator app on your mobile device and choose to "Scan a barcode". (Do not try to scan the barcode above, it will not work.)

10:53

Add an account

You can add an account selecting one of the following options:

◻ Scan a barcode

⌨ Enter a provided key

Place barcode within red lines

6. Once you successfully read the barcode from your mobile app, an entry will appear in your app, showing a six digit PIN code and a description like "privacyIDEA (Concordia: <your email>)".

10:56

Google Authenticator

Account added

745 086

privacyIDEA (Concordia: test3@concordia.ab.ca (…
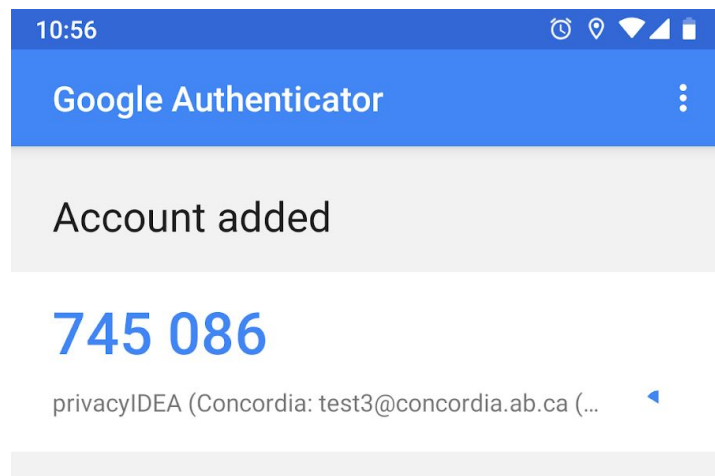
7. You can click "Close" on the QR code window, your device will be added to the system and your account will be enabled for two-factor authentication.

Note: The QR code will never be displayed again. If you need to switch mobile devices, be sure to setup a new device before you lose access to the old one. Alternatively, disable two-factor authentication before you lose access to your old device.

Using Two-Factor Authentication

Once two-factor authentication is enabled on your Concordia account it adds just one brief step to the single sign on login process.

After entering your username and password, the login page will prompt you to enter the PIN code that is displayed on your phone as seen below. The codes from the mobile app are time-based, so they change every 30 seconds.

Once you successfully enter the PIN code that was sent to your phone, your login will be completed.

Getting Help

If you enable two-factor authentication and attempt to login without access to one of your configured devices, you will not be able to login. If you have permanently lost access to all of your configured two-factor devices, you will need to speak with IT Services to regain access to your account.

IT Services can be reached at 780 479 9316 or helpdesk@concordia.ab.ca as well as in the Arnold Guebert Library in L356.