Set up Two-Factor Authentication

Install Google Authenticator on your Android device

1. Open the Google Play store

2. Type in “Google Authenticator” in the search field to download and install the app to your smartphone.
3. Once the application has installed on your smart phone, click the “OPEN” button to launch.

4. Once you have launched the Google Authenticator, click the “Begin” button to proceed.

5. You can click the “Skip” link to bypass the tutorial or the arrow link to review.
6. You will see the screen to “Add an account”. Google Authenticator has been successfully installed. Proceed to the next step.

Add an account
You can add an account selecting one of the following options.
- Scan a barcode
- Enter a provided key

**Configure two-factor authentication**

1. Open a [supported browser](#) on your laptop/PC and enter the URL [https://connect.ccc.edu](https://connect.ccc.edu) in the address bar.

   ![City Colleges of Chicago Employee VPN Portal](#)

   City Colleges of Chicago Employee VPN Portal
   
   Username
   Password

   ![Sign In](#)

2. Type your CCC credentials in the Username and Password fields, and click the “Sign In” button.

   The **FIRST TIME** you access CCC Anywhere, you will see the screen below. **Be sure to copy and print your backup codes in case you ever need to access CCC Anywhere and your mobile device isn’t available.** Each code can only be used once.
3. Return to the Google Authenticator app on your smartphone.
   a. Click “Scan a barcode”
   b. **Note:** if you already have Google Authenticator installed for another application, click on the red “+” on the bottom of the Authenticator screen to add an account for CCC Anywhere and then click Scan a barcode.

Google Authenticator will use your camera to capture the barcode (QR code). Align the red lines on the smartphone screen to the two-factor QR code on your laptop/PC.

4. Once Google Authenticator has captured the QR code, the app will advance to the Authenticator
screen displaying a randomly generated six digit token code.

5. Enter the six-digit token displayed on your smartphone into the field “Enter token codes that the application generates” on your PC/laptop screen and click the “Sign in” button. Please be aware, the six-digit token changes every 60 seconds. If the first code you try is not accepted, use the next code you see.

6. Once you successfully login, you will see the CCC Anywhere splash page, below.
Note: Your VPN access is limited to your open web browser. If you close or leave your browser, you will not have access to CCC resources. While in the browser, if you need to return to the main menu, use the CCC Anywhere menu “Home” button.

The CCC Anywhere Menu
You will see the CCC Anywhere menu in the upper-right hand corner of your browser window for the duration of your CCC Anywhere session.

1. Arrows move the menu to the left or right hand side of your browser
2. CCC Logo brings you back to the CCC Anywhere splash page
3. Arrow expands or collapses the menu
4. Home icon brings you back to the CCC Anywhere splash page
5. Tells you how much time remains in your VPN session
6. Opens the help documentation

Logging out of CCC Anywhere
1. Once you are ready to leave your VPN session, click the “Sign Out” button on the top right corner of the page to successfully log out and clear your session.

Logging into CCC Anywhere after two-factor authentication is configured
1. Now that you have configured two-factor authentication, the login process is as follows:
   a. Browse to: http://connect.ccc.edu
   b. Enter your CCC Credentials
c. A second login screen will appear requesting the two-factor authentication.

d. Open Google Authenticator and provide the code that appears on the screen.

Note: If you are ever without your device, you may use one of the backup codes you copied/printed during the initial setup.

**Configuring CCC Anywhere for a new device**

If you need to configure a new device for two-factor authentication, please open a support ticket to have your VPN account reset. Once this is complete, you will need to setup two-factor authentication on your new device.