Two-Factor Authentication

2FA is a security system that requires two separate, distinct forms of identification to access a user's account. In this case, the first factor is a password, and the second is a one-time passcode that is sent to the user's cell phone through a specific two-factor authentication application.

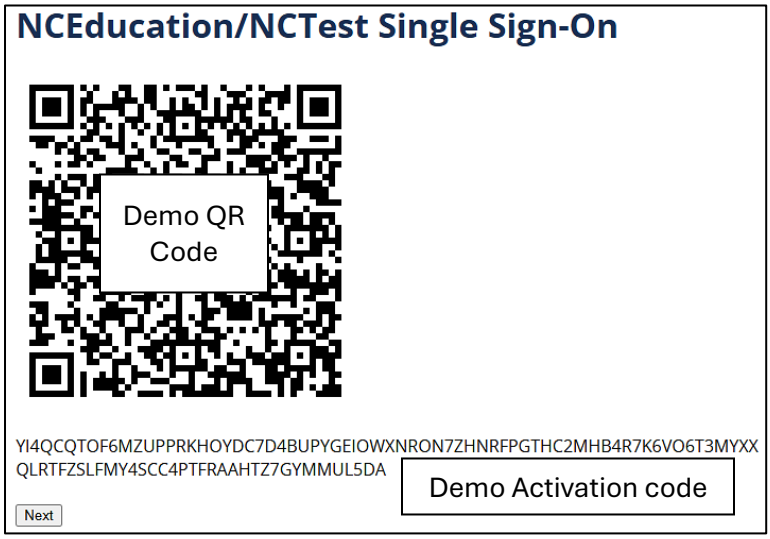
Using 2FA ensures that hackers will not be able to gain unauthorized access to an account even if they have stolen the password.

These mobile applications have been tested within NC Education and may be used for 2FA:

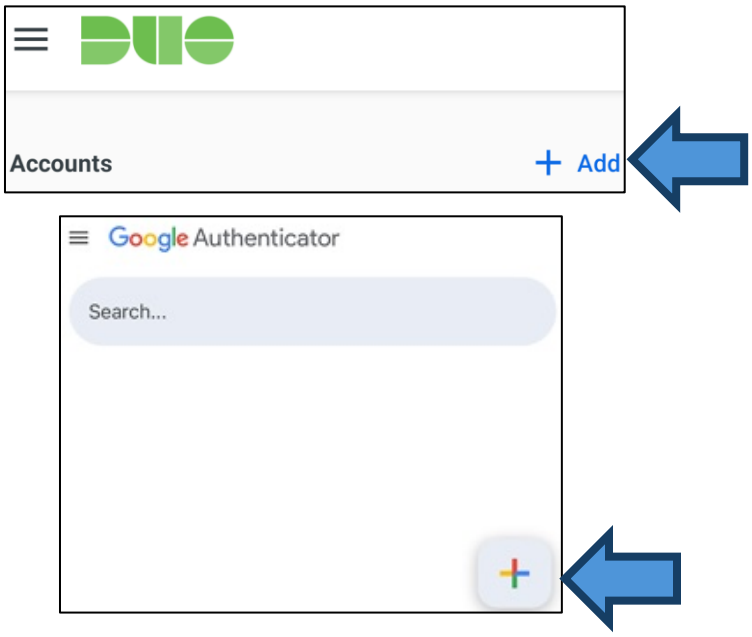
- Authy
- Microsoft Authenticator
- Google Authenticator
- Cisco Duo
- Step Two (iOS / iPadOS only)

Set Up 2FA

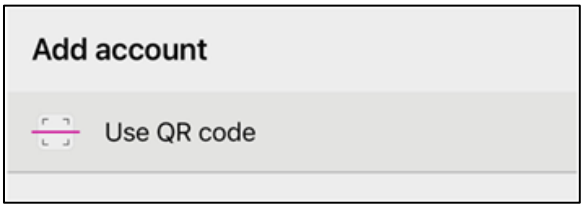
1. Install one of the authenticator applications above from the appropriate app store.
2. Log into NCAuth using your username and password. If 2FA has not already been set up for the account, the next screen will prompt the user to set up 2FA and provide a QR code to do so.



3. Open your authenticator app and select the ‘addition’ function to add a new authenticator. For most applications, it will include a “+” sign.



4. Select the ‘scan QR code’ option in the app and aim the camera at the QR code to scan it.
    - If the camera option is not available, manually enter the activation code provided on the NCAuth screen instead.



5. After successfully scanning the QR code or entering the application code, follow the instructions in your app. The app should begin generating one-time passcodes.
    - 2FA apps generate new one-time passcodes every 30 seconds for security purposes. OTPs are only valid for 30 seconds and must be entered before they expire.
6. On the NCAuth page, select ‘Next.’
7. Enter the one-time passcode from your app into the ‘Enter code’ box. This verifies the authenticator and NCAuth are properly synced.

8. Upon correctly entering the OTP, NCAuth and the 2FA application will be synced, and the user will successfully log in to NCAuth.
    - If an error occurs, re-enter the OTP (or enter the next one, if the previous has expired) in case the issue was caused by a mistyped code.
    - If the error persists, delete the NCAuth authenticator from your app and attempt the setup process again.
    - If you are still unable to set up your authenticator, contact the Help Desk.

After setup, the user will be prompted to enter the OTP from their 2FA application on every login after entering their username and password.