Setup Multi-Factor Authentication (MFA)

With Google Authenticator App

Multi-Factor Authentication is a method that requires users to provide two or more verification factors in order to gain access to an account. This provides extra security for accounts that have rights to sensitive and/or confidential data. This document walks through MFA Setup for Hart District Active Directory Network and Google Accounts.

Setting Up Your MFA Authentication Device

You will be able to choose a primary authentication method when you register, which you can change or update at any time. We recommend using a mobile app on your mobile device. These apps generate a one-time code to be entered upon login as identity verification.

There are a variety of Authentication Apps available. We recommend:

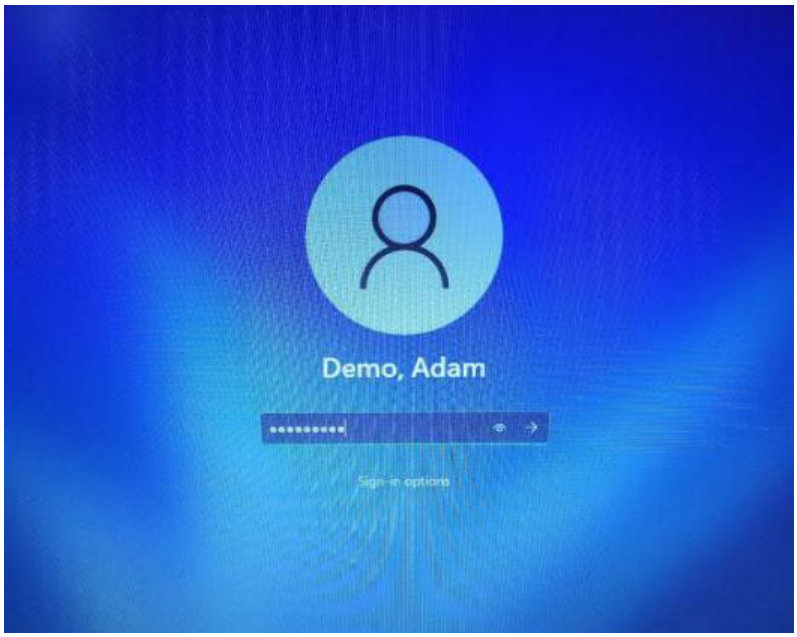
- Google Authenticator
  - Download for Apple iOS
  - Download for Android

- You may elect to have more than one method of Authentication in MFA, meaning you have the ability to use the Mobile App AND YubiKey as alternate ways of verifying your identity.
- We will walk through enrolling using Google Authenticator App in AD and Google.

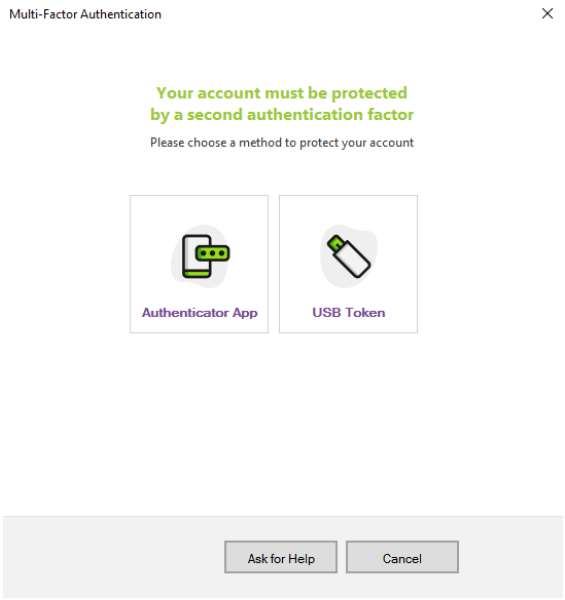
Setting Up MFA in Active Directory (AD)

Active Directory (AD) is how you sign into the Network at any of the William S. Hart Union High School District sites. This is how users sign into their computers as well as access their G: drive and any other shared network drives.

- Sign into your AD account as usual

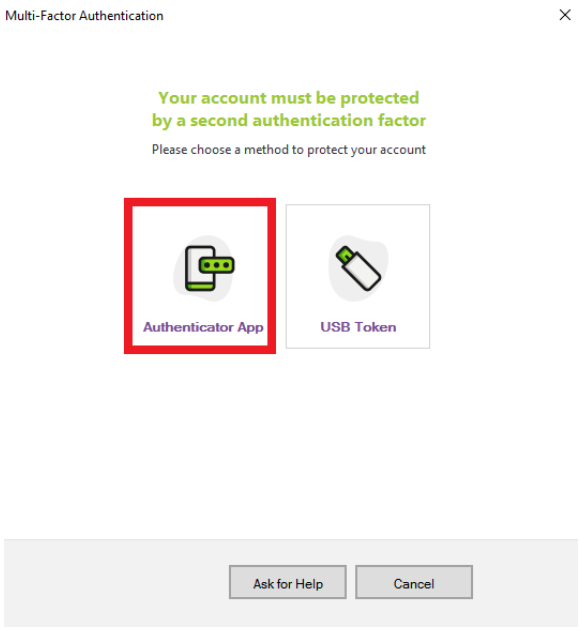


- You will receive a prompt from UserLock to set up Multi-Factor Authentication.
- Select which method of authentication you are using:
    - Authenticator App
    - USB Token

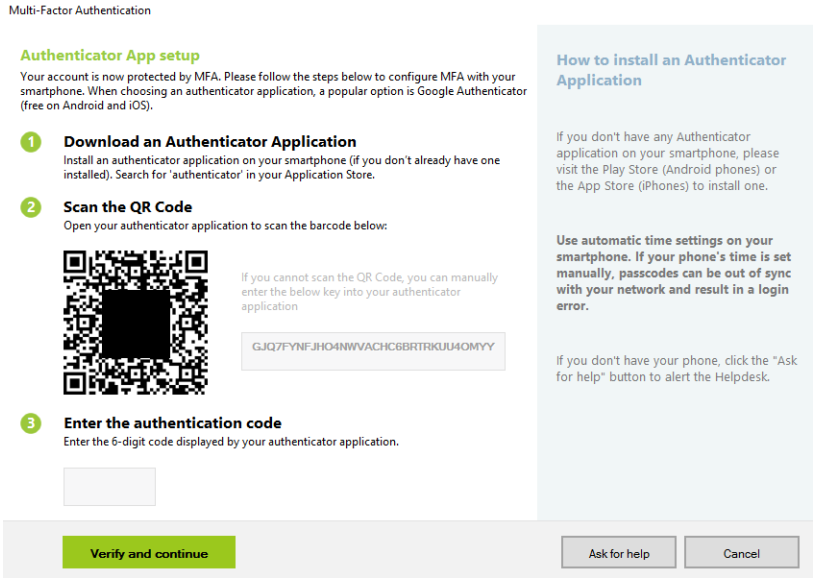


Enrolling AD in MFA with Google Authenticator

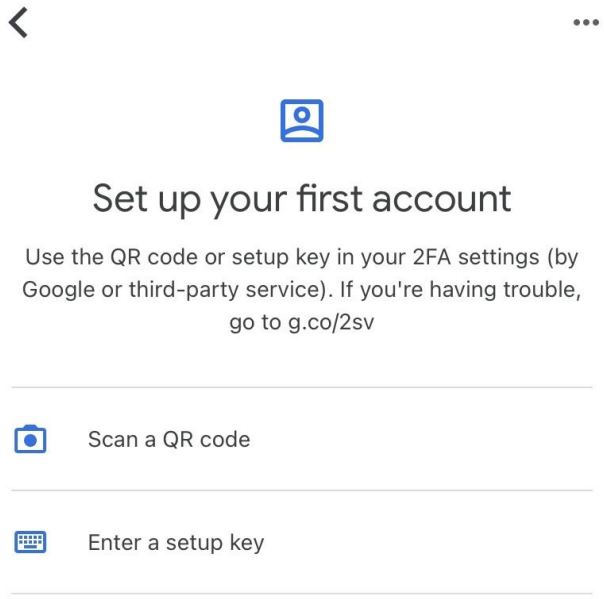
- Select Authentication App from the UserLock MFA Enrollment screen.



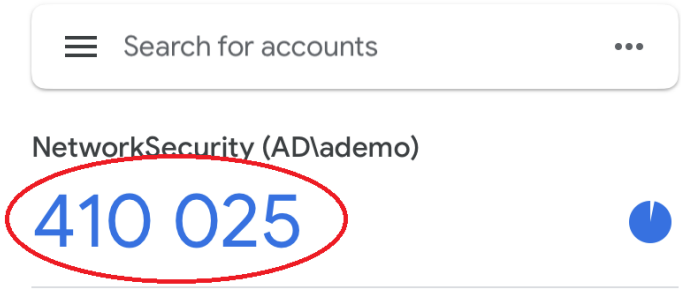
- You will be brought to a screen with instructions



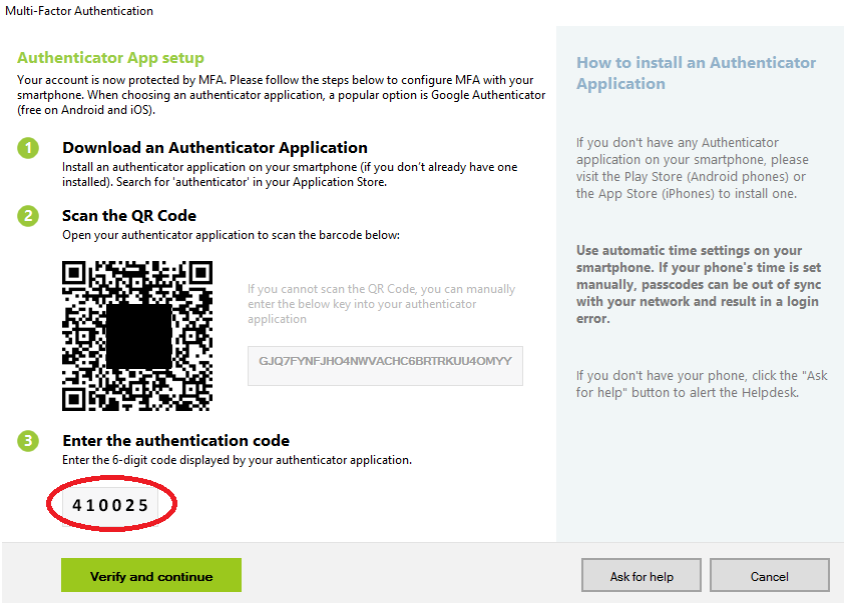
- Now open the Authenticator App on your mobile device.
- If using Google Authenticator you will be prompted to set up your account.



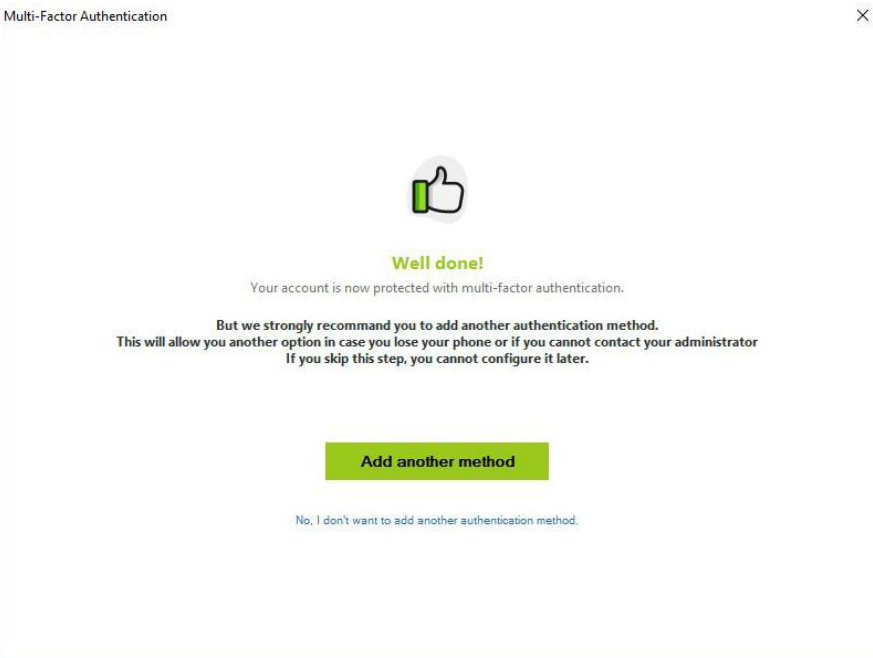
- Tap on Scan a QR code from the mobile app and line it up with the QR code on the UserLock screen on your desktop.
- A Code will appear on your mobile device.



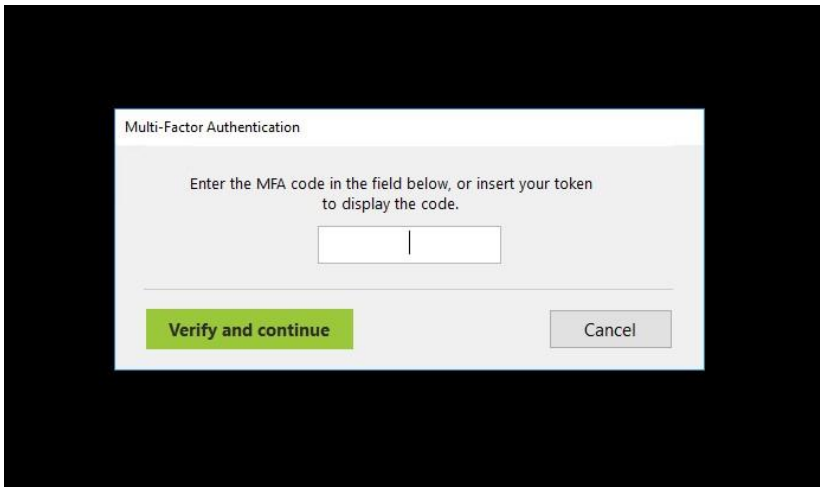
- Type the code provided in your Authenticator App into the field for the Authentication Code on your desktop.



- Click the Verify button to complete the enrollment process.



- At this point, you may enroll a secondary method with a token by clicking the Add Another Method button or choose to opt out.
- The next time you login to your desktop you will see an alert prompting you to use MFA to complete sign-in.



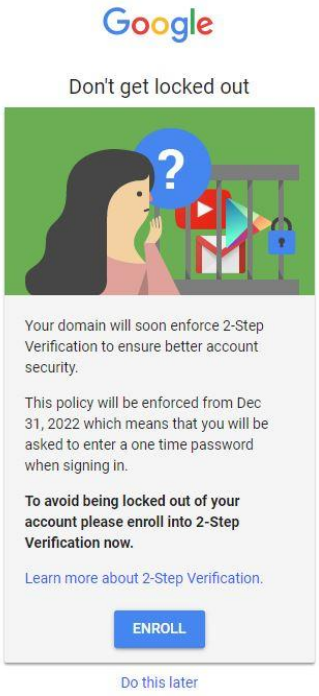
- Open your Authenticator App on your mobile device and type in the code provided
- <u>This will be required upon first AD network login to a unique device daily.</u>

Tip: Using an app on your mobile device will enable you to complete MFA without needing to carry an additional device for manual authorization.

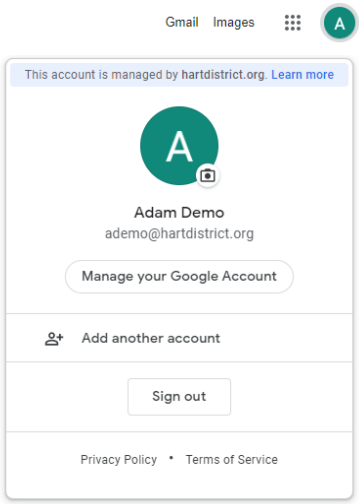
Setting Up MFA in Google

William S. Hart Union High School District uses the Google Workspace suite of applications such as Gmail, Classroom, and Drive . In addition to these widely used applications, Google is used to sign into multiple other systems with access to sensitive or confidential information.

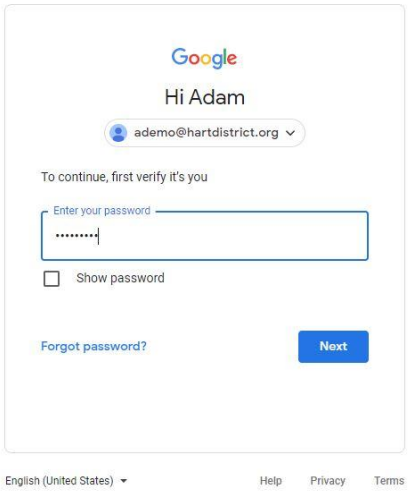
- When you sign into Google you will be prompted to set up MFA or what Google refers to as 2-Step Verification.



- Click Enroll to Begin.
- *If you do not get this prompt, you can click on your profile to* ***Manage Your Google Account***



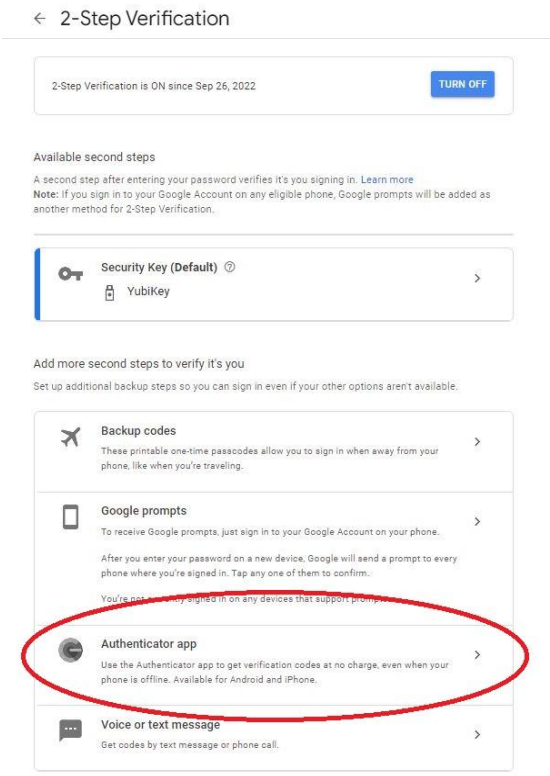
- You will be prompted to enter your Google password again.



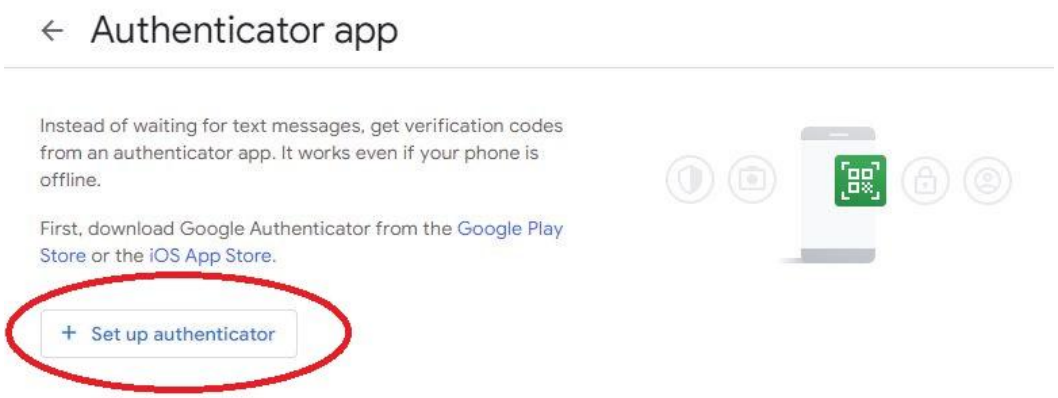
- Then you will be prompted to enter your mobile phone number or select more options.

Enrolling Google in MFA with Google Authenticator

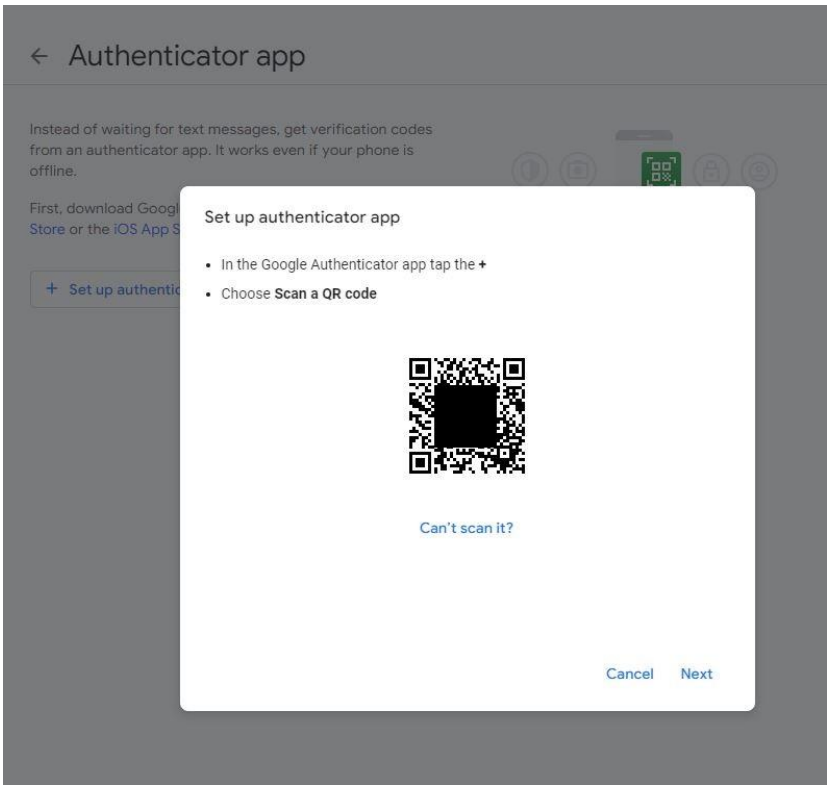
- Once your Google Account has been set up with MFA or 2-Step Verification using your phone number you may add an Authenticator App.



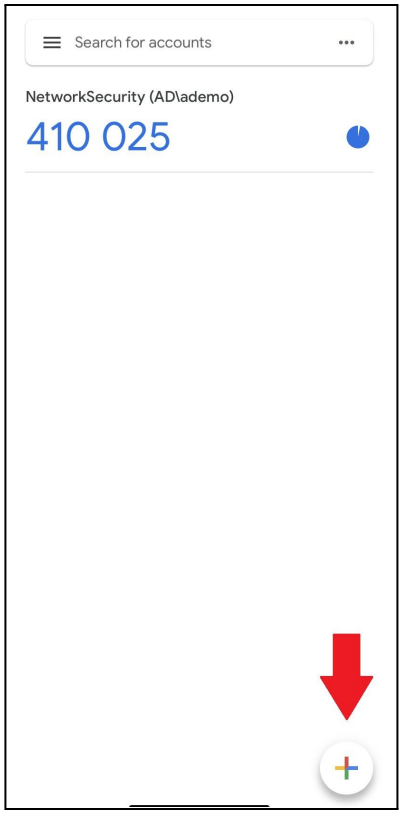
- Select Authenticator App under *Add more second steps to verify it's you* on the Google 2-Step Verification page.
- You will then be prompted to set up an Authenticator App.

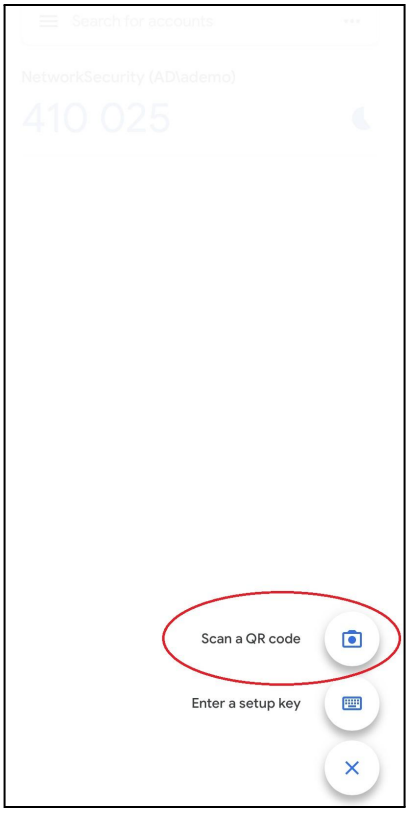


- Click on + Set up authenticator to begin the process.

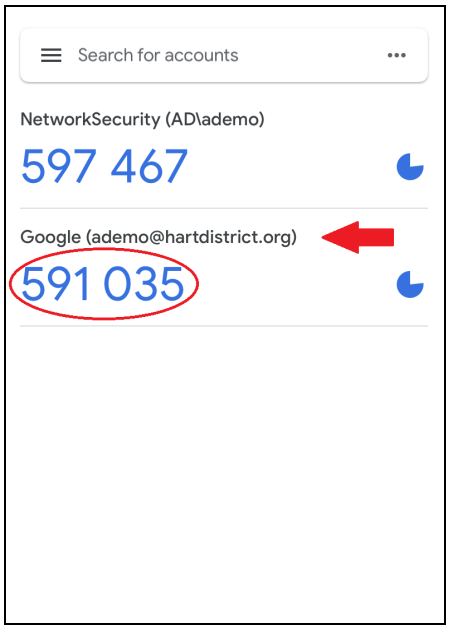


- A QR code will appear
- From your mobile device, open the Google Authenticator App
- Scroll down to the + icon at the bottom of the screen.

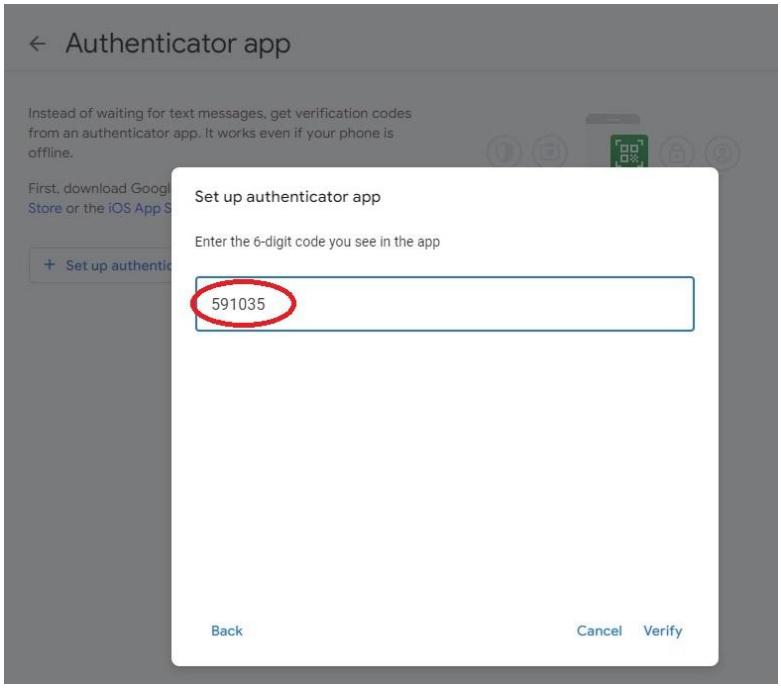




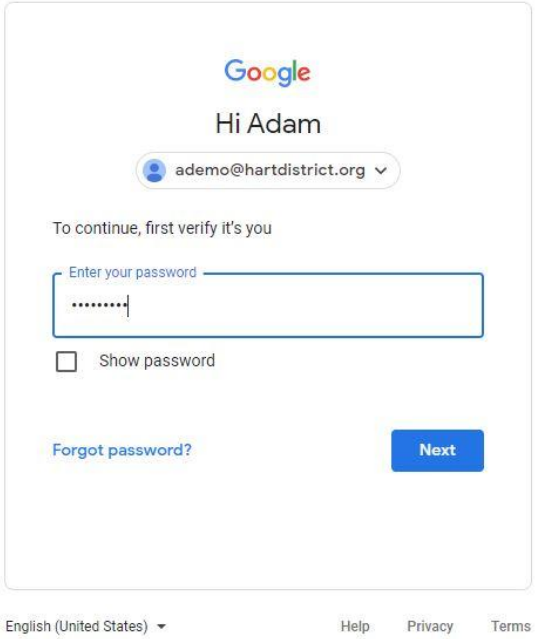
- Tap on the + icon for setup options
- Then tap on *Scan a QR code* and hold your mobile device up to the QR code displayed on your desktop screen.



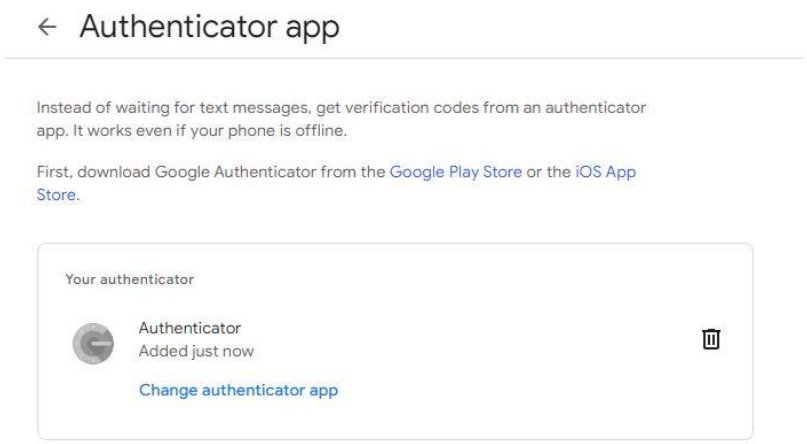
- You will now see your Google Account included in the list of active accounts with an active verification code.
- Enter that code into the prompt from Google on your desktop.



- You will then be prompted to re-enter your Google password.



- You now will be able to see your Authenticator app has been enrolled.



- Click the Back arrow to view all the enrolled MFA options.
- You're done!

Tip: For more information on Multi-Factor Authentication on your Google account visit: https://safety.google/authentication/