Setup Multi-Factor Authentication (MFA)

With YubiKey

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 with the help of your site technology support staff. 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.

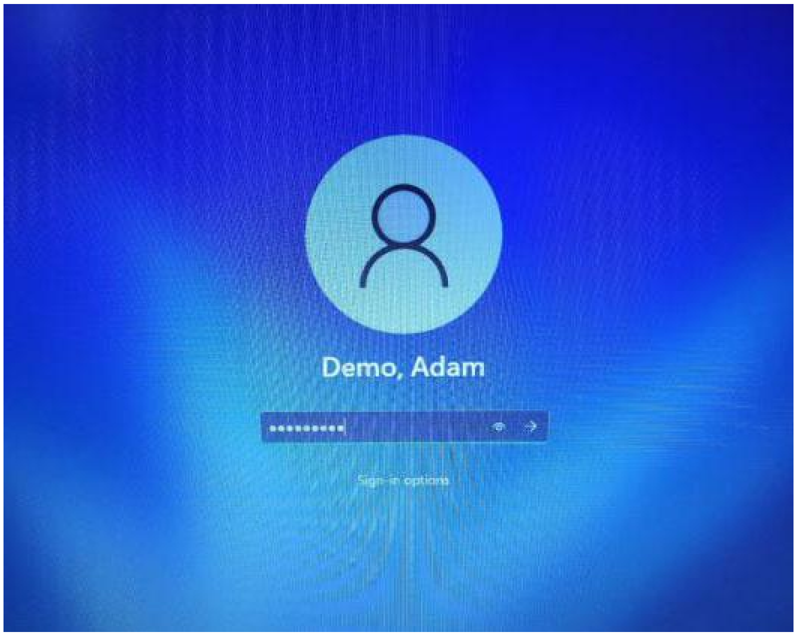
If you do not want to use a personal device or do not own a smartphone, Technology Services offers authentication tokens, or YubiKey, that generates verification codes similar to the Mobile Apps outlined previously. This small, lightweight key is about the size of a USB thumb drive, and has an opening so that it can be affixed to a keychain or lanyard. You will need to carry this key with you at all times to verify your identity for MFA.

- 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 YubiKey in AD and Google.

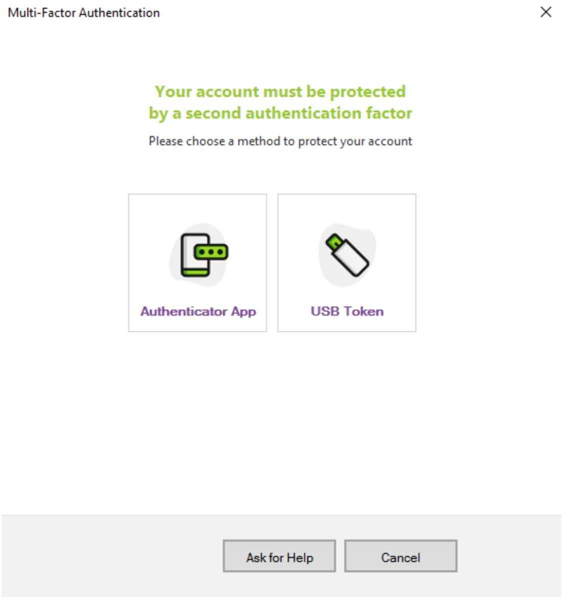
Setting Up MFA in Active Directory (AD)

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



Multi-Factor Authentication ×

Your account must be protected
by a second authentication factor

Please choose a method to protect your account

Authenticator App

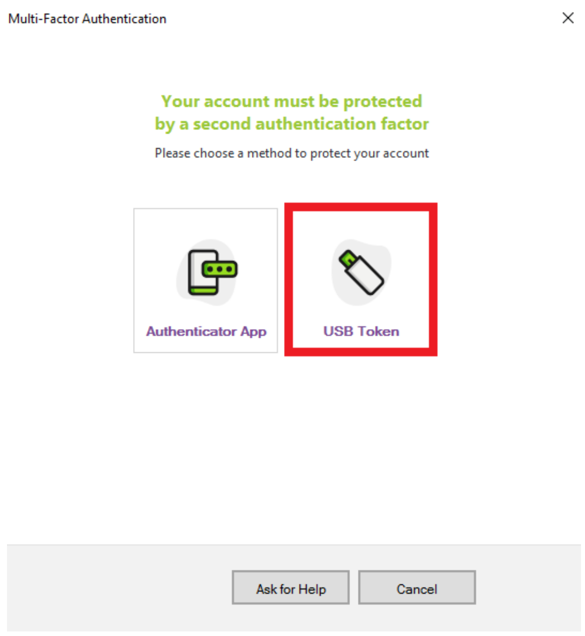
USB Token

Ask for Help

Cancel

Enrolling AD in MFA with YubiKey

- Select USB Token from the UserLock MFA Enrollment screen.

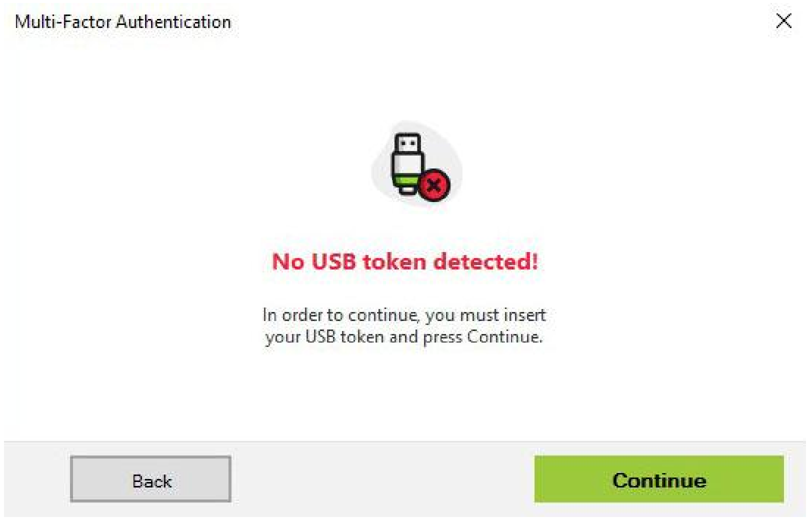


Multi-Factor Authentication

Your account must be protected by a second authentication factor

Please choose a method to protect your account

- Your computer will scan for the token. If it has not yet been inserted into a USB port on your device you may see the following message.



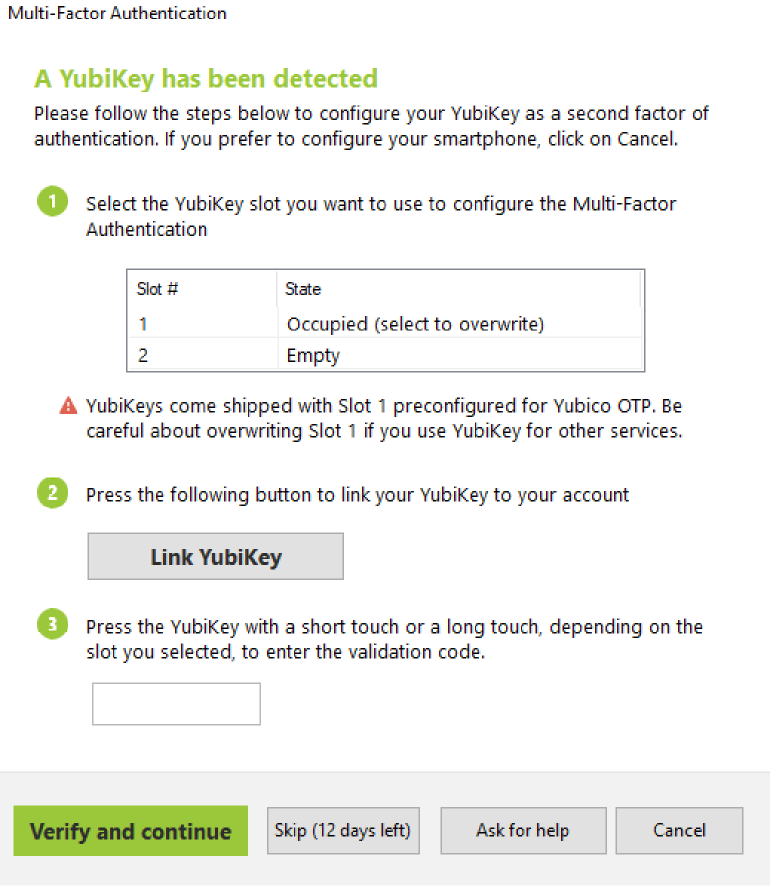
Multi-Factor Authentication

No USB token detected!

In order to continue, you must insert your USB token and press Continue.

- Insert your YubiKey into an available USB port on your computer and Click Continue.
- *Please note that the YubiKey must have the touch point facing upward. You will see a flash of light when it is inserted correctly.*

- Once the YubiKey is in place and UserLock identifies it, you will see a message confirming that the device has been detected and you will be able to move forward with next steps.



Multi-Factor Authentication

A YubiKey has been detected

Please follow the steps below to configure your YubiKey as a second factor of authentication. If you prefer to configure your smartphone, click on Cancel.

1 Select the YubiKey slot you want to use to configure the Multi-Factor Authentication

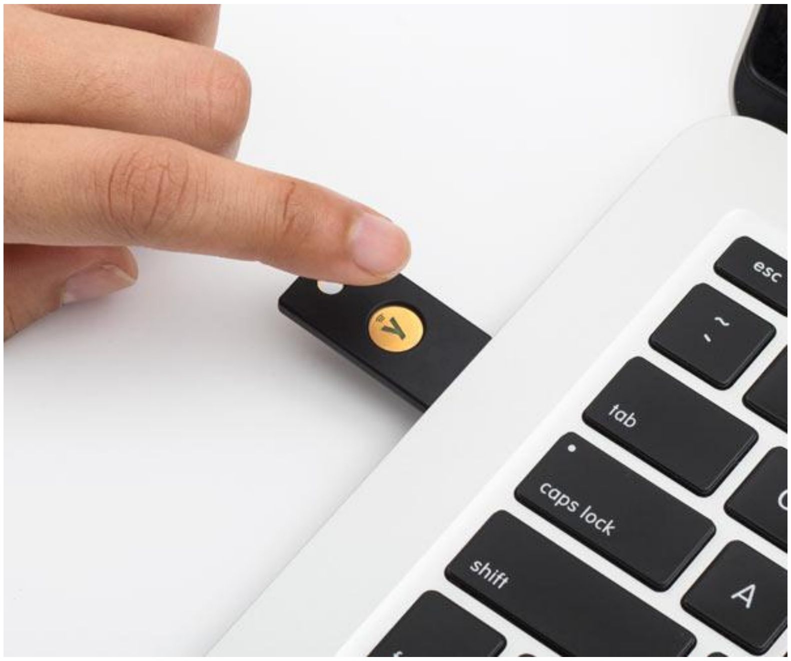
Slot #	State
1	Occupied (select to overwrite)
2	Empty

⚠ YubiKeys come shipped with Slot 1 preconfigured for Yubico OTP. Be careful about overwriting Slot 1 if you use YubiKey for other services.

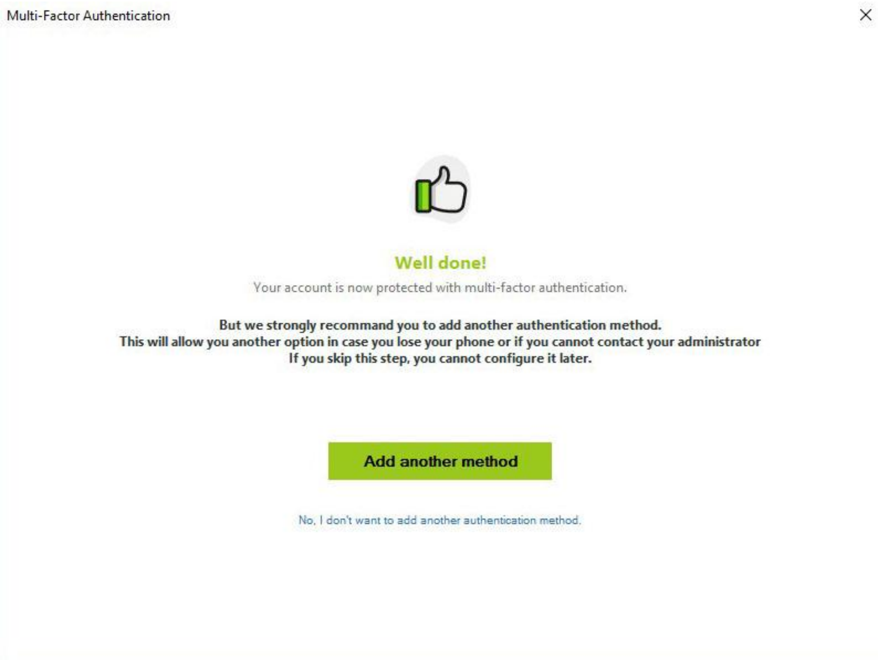
2 Press the following button to link your YubiKey to your account

3 Press the YubiKey with a short touch or a long touch, depending on the slot you selected, to enter the validation code.

- Step 1 - Select Slot 1
- Step 2 - Click Link YubiKey
- Step 3 - Place your finger on the gold touch point on the YubiKey.



- Touching this point will generate a one-time code that fills in the validation field in step 3.
- Touch the YubiKey touch point only long enough to generate the validation code.
- Click the Verify button to complete the enrollment process.


Multi-Factor Authentication
×

Well done!

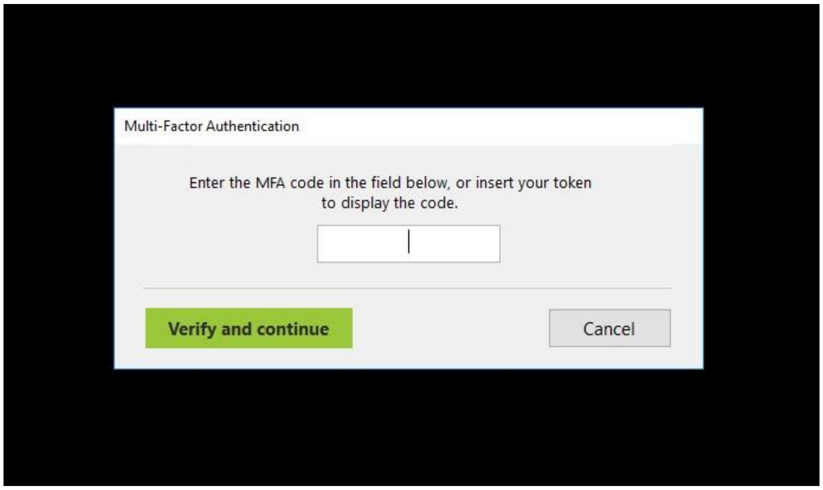
Your account is now protected with multi-factor authentication.

But we strongly recommand you to add another authentication method.
This will allow you another option in case you lose your phone or if you cannot contact your administrator
If you skip this step, you cannot configure it later.

Add another method
No, I don't want to add another authentication method.

- At this point, you may enroll your Authenticator Mobile App 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.



Multi-Factor Authentication

Enter the MFA code in the field below, or insert your token to display the code.

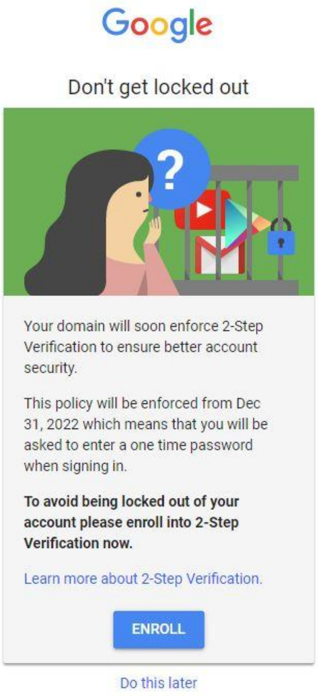
- You may use whichever method you have enrolled your account in.
    - Insert your YubiKey and tap the touch point to generate a code
    - Open your Authenticator App on your mobile device and type in the code provided
- <u>This will be required upon first AD network login to a unique device daily.</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.



Google

Don't get locked out

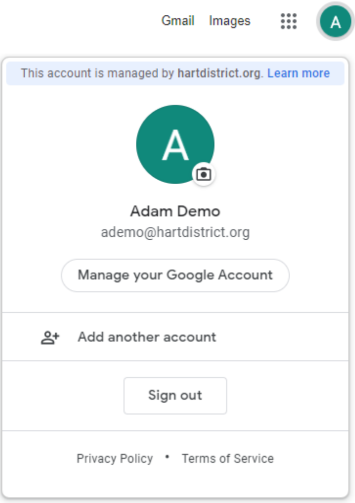
Your domain will soon enforce 2-Step Verification to ensure better account security.

This policy will be enforced from Dec 31, 2022 which means that you will be asked to enter a one time password when signing in.

To avoid being locked out of your account please enroll into 2-Step Verification now.

Learn more about 2-Step Verification.

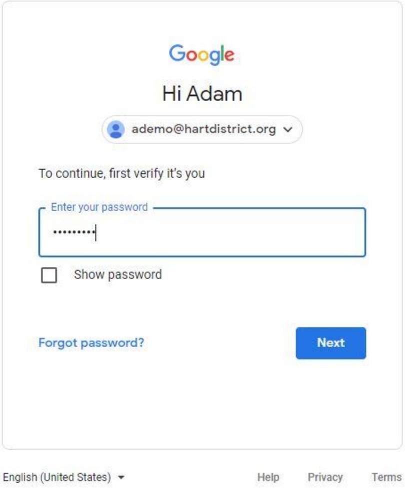
- Click Enroll to Begin.
- *If you do not get this prompt, you can click on your profile to* ***Manage Your Google Account***



This account is managed by hartdistrict.org. Learn more

Adam Demo
ademo@hartdistrict.org

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



Google

Hi Adam

ademo@hartdistrict.org

To continue, first verify it's you

Enter your password

•••••••••

□ Show password

Forgot password?

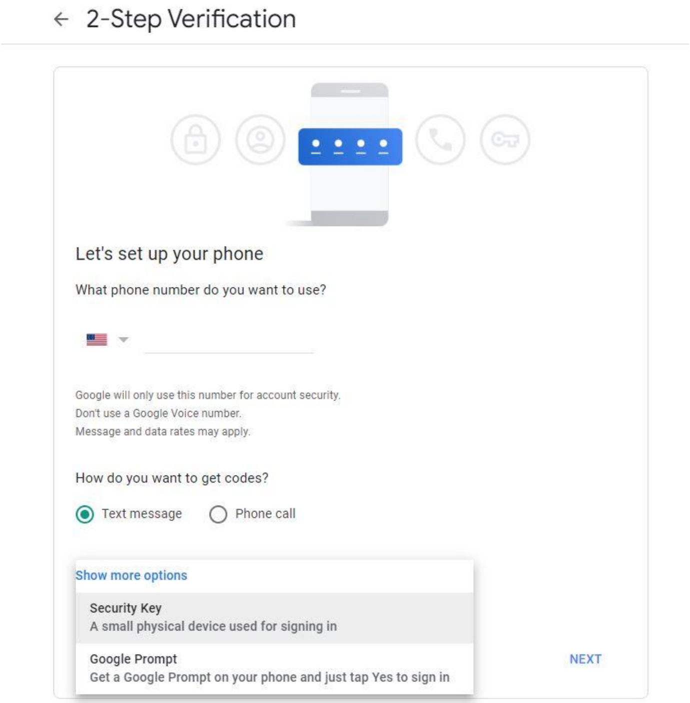
Next

English (United States) ▾ Help Privacy Terms

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

Enrolling Google in MFA with YubiKey

- Without entering a phone number click on Show more options



← 2-Step Verification

Let's set up your phone

What phone number do you want to use?

Google will only use this number for account security.
Don't use a Google Voice number.
Message and data rates may apply.

How do you want to get codes?

● Text message ○ Phone call

Show more options

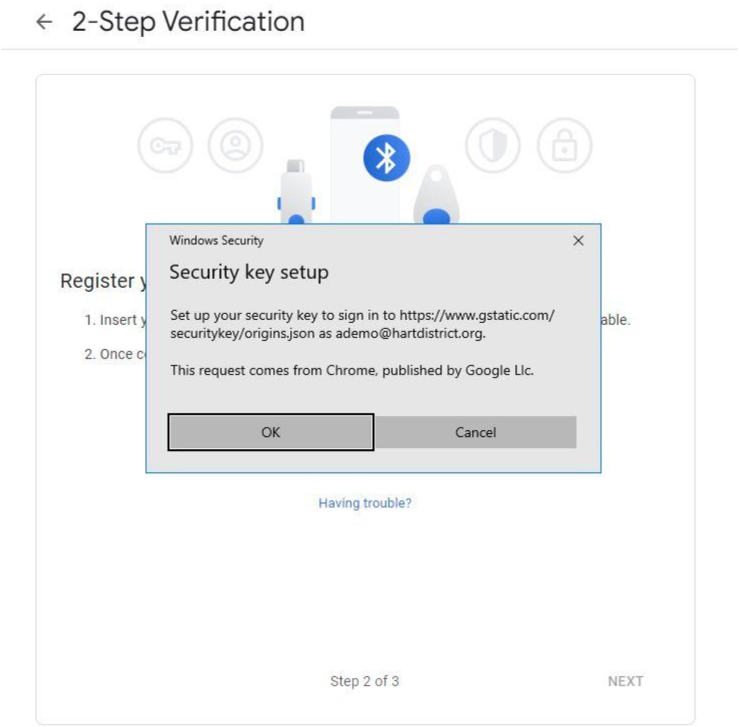
Security Key
A small physical device used for signing in

Google Prompt
Get a Google Prompt on your phone and just tap Yes to sign in

NEXT

- From the options drop down select Security Key
- Click Next

- You will then be prompted through your desktop to enable your authentication key to be recognized by your device and send information to Google Chrome on behalf of your account.



← 2-Step Verification

Register y

1. Insert y able.

2. Once c

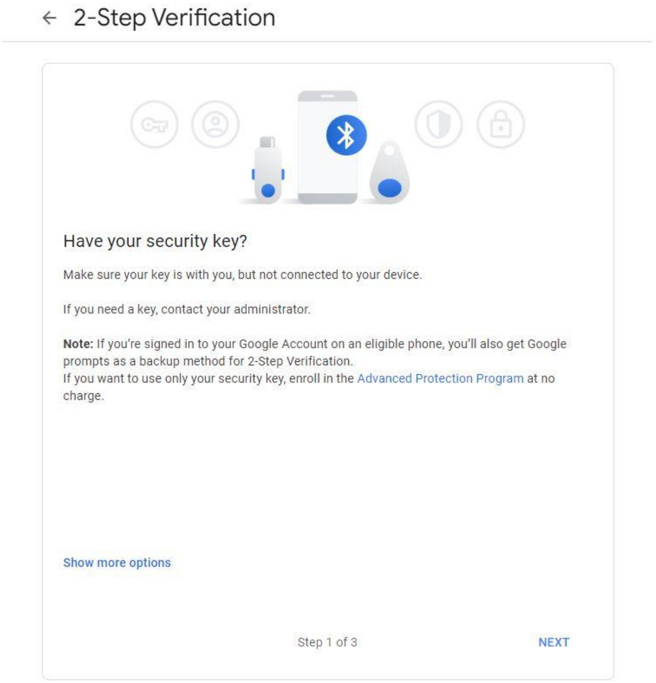
Windows Security

Security key setup

Set up your security key to sign in to https://www.gstatic.com/securitykey/origins.json as ademo@hartdistrict.org.

This request comes from Chrome, published by Google Llc.

- At the Security key setup prompt click OK



← 2-Step Verification

Have your security key?

Make sure your key is with you, but not connected to your device.

If you need a key, contact your administrator.

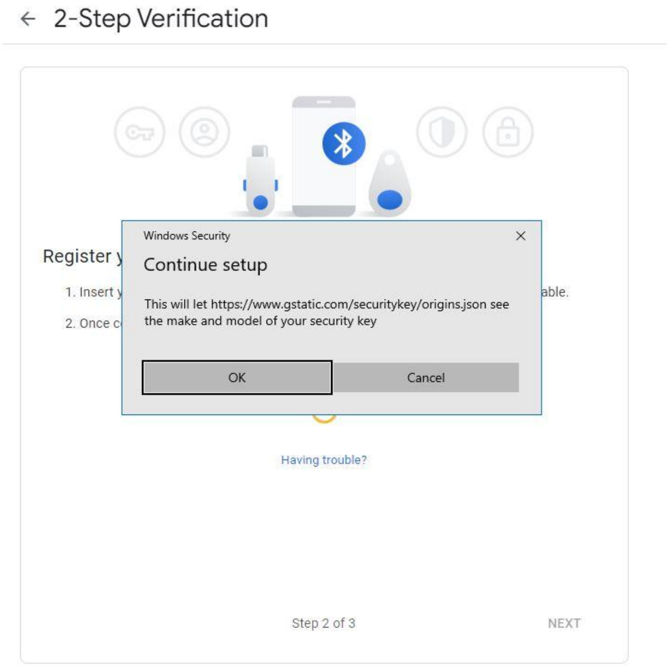
Note: If you're signed in to your Google Account on an eligible phone, you'll also get Google prompts as a backup method for 2-Step Verification.
If you want to use only your security key, enroll in the Advanced Protection Program at no charge.

Show more options

Step 1 of 3

NEXT

- Google will then remind you to have your security key available but not yet connected.
- Without inserting the YubiKey, click NEXT and follow the prompts.



← 2-Step Verification

Register y

1. Insert y

2. Once c

able.

Windows Security

Continue setup

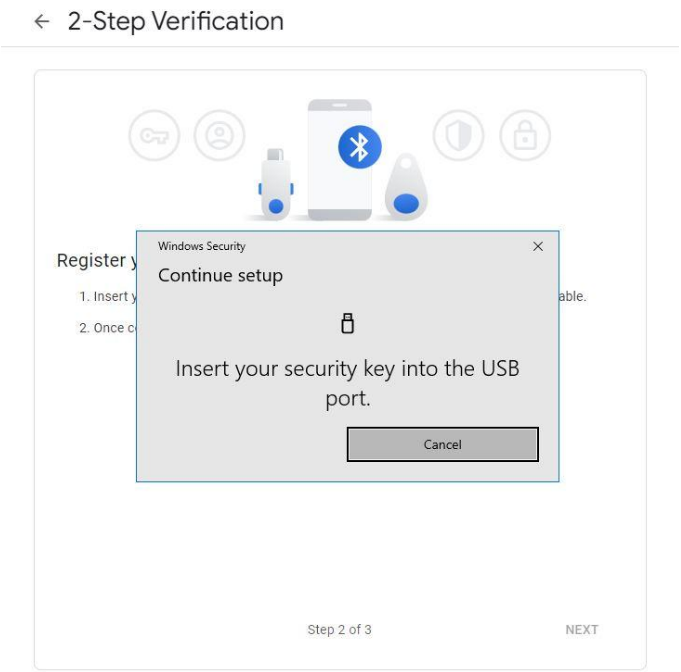
This will let https://www.gstatic.com/securitykey/origins.json see the make and model of your security key

Having trouble?

Step 2 of 3

NEXT

- Click OK



← 2-Step Verification

Register y

1. Insert y … able.

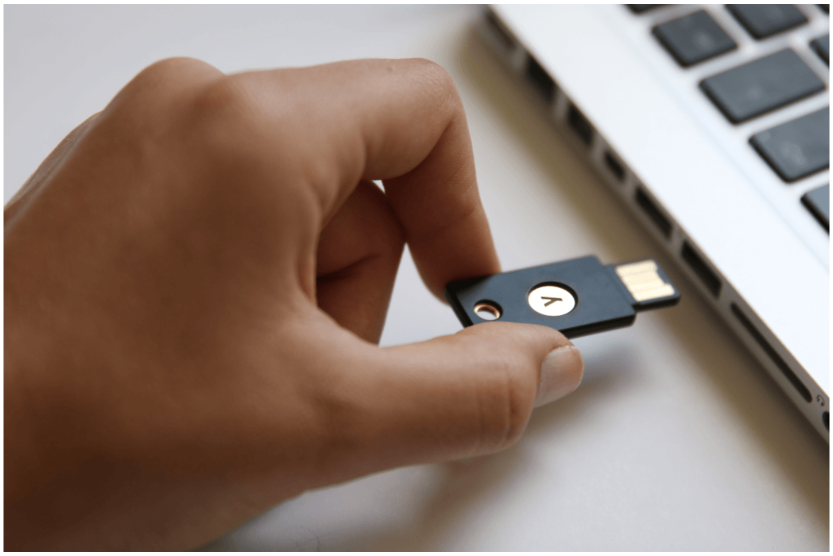
2. Once c

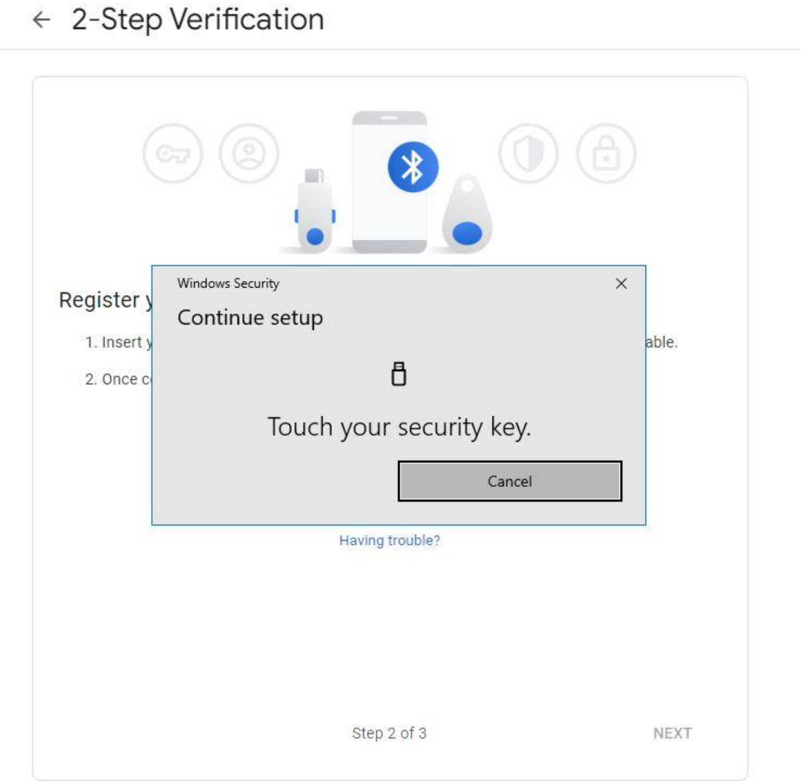
Windows Security

Continue setup

Insert your security key into the USB port.

- Insert your YubiKey into an available USB port on your computer and Click Continue.
- *Please note that the YubiKey must have the touch point facing upward.*





2-Step Verification

Register y

1. Insert y able.

2. Once c

Windows Security

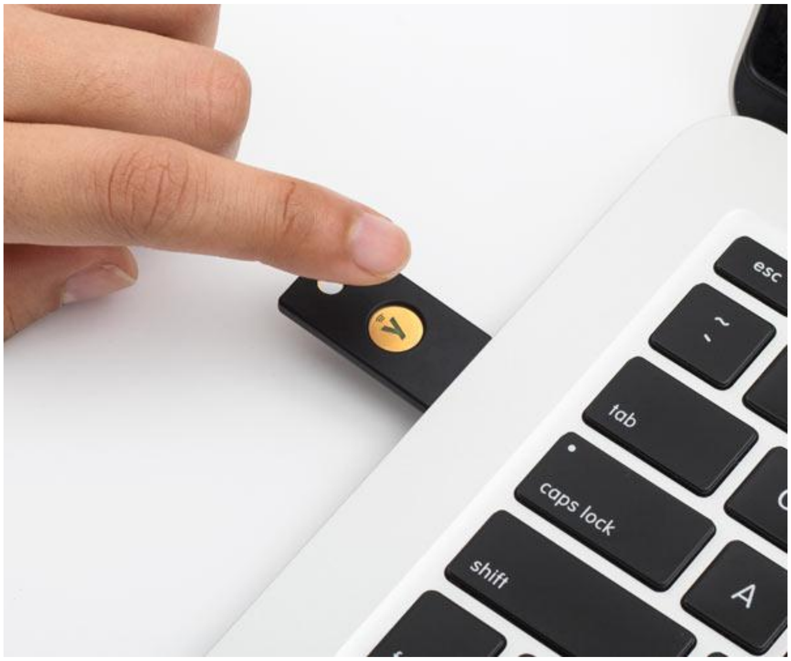
Continue setup

Touch your security key.

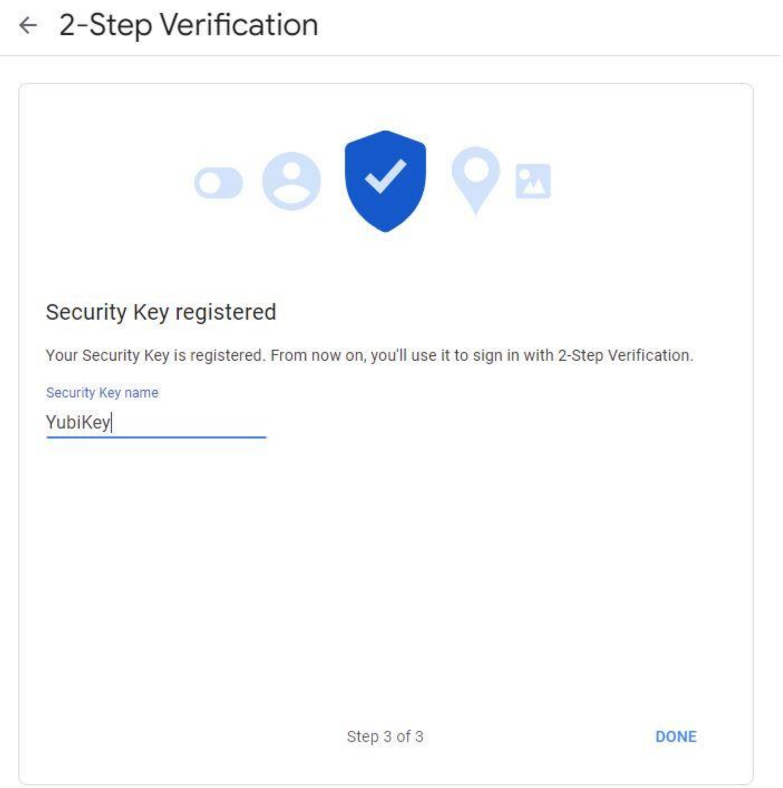
Step 2 of 3

- You will then be prompted to Touch your security key.

- Place your finger on the gold touch point on the YubiKey



- Touching this point will generate a one-time code that confirms enrollment with Google.



← 2-Step Verification

Security Key registered

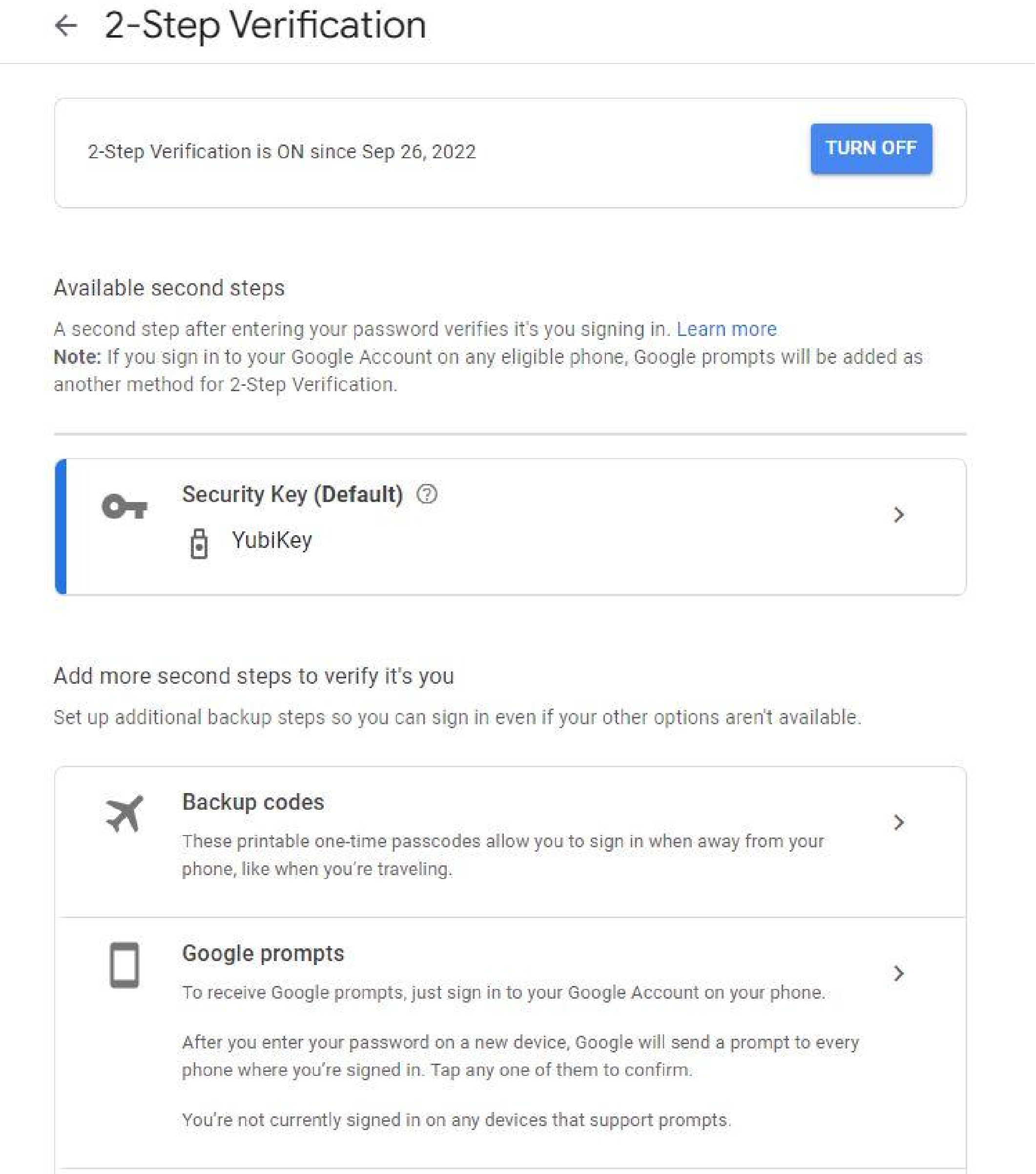
Your Security Key is registered. From now on, you'll use it to sign in with 2-Step Verification.

Security Key name

YubiKey

Step 3 of 3

- Give your Security key a name and click DONE.



← 2-Step Verification

2-Step Verification is ON since Sep 26, 2022

Available second steps

A second step after entering your password verifies it's you signing in. Learn more
Note: If you sign in to your Google Account on any eligible phone, Google prompts will be added as another method for 2-Step Verification.

Security Key (Default)
YubiKey

Add more second steps to verify it's you

Set up additional backup steps so you can sign in even if your other options aren't available.

Backup codes
These printable one-time passcodes allow you to sign in when away from your phone, like when you're traveling.

Google prompts
To receive Google prompts, just sign in to your Google Account on your phone.

After you enter your password on a new device, Google will send a prompt to every phone where you're signed in. Tap any one of them to confirm.

You're not currently signed in on any devices that support prompts.

- You will now see the Security Key is successfully installed and you can move onto enabling other forms of MFA if you want added security.

Tip: Keep your YubiKey with you at all times, as it will be needed anytime you sign into your Hart District Google account from a new device.