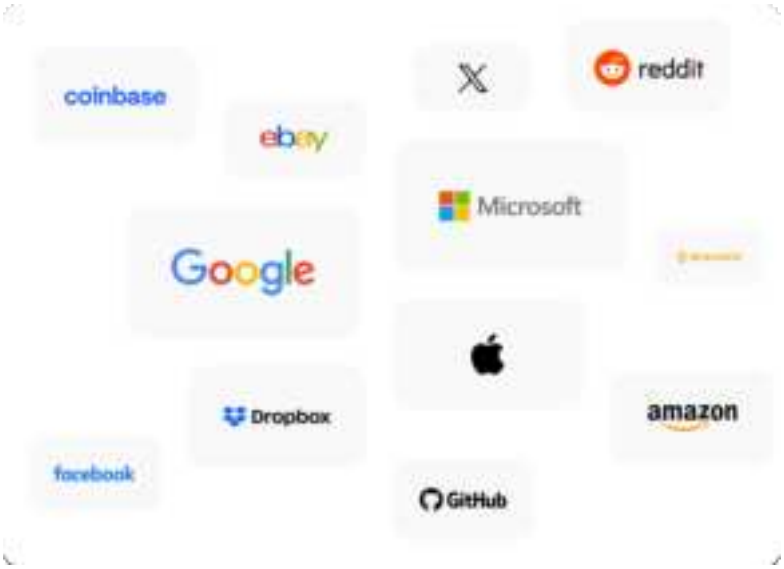
How to Set up your YubiKey for Use with KSI AuthentiKey Keyboards

First, are you setting up a new YubiKey Bio? If so, make sure to enroll your fingerprint before following the steps below. The method of enrolling fingerprints on your YubiKey Bio varies whether you are running Windows, macOS, Linux, or Chrome OS. You can enroll up to five (5) fingerprint templates to your Key to ensure access, and you are able to remove and re-enroll individual templates if an issue arises.

1. CHOOSE A YUBIKEY-COMPATIBLE SERVICE

Choose an online service that supports YubiKeys. Think of it as the place you want your YubiKey to protect. Some common examples include Google, Dropbox, and Microsoft.



It is up to each service as to how each support YubiKeys. Please see the following link for more information: See what works with YubiKeys

Services Yubico Recommends Setting Up First

Security keys are crucial tools for safeguarding your online presence, and knowing where to start is vital. Here is a brief guide on which services should take top priority:

KSI Keyboards
14494 Wicks Boulevard, San Leandro, CA 94577
(510) 562-5000 info@ksikeyboards.com

- **Email Accounts**
  Your email account is often the gateway to all your other online services. Once someone gains access to your email, they can reset passwords and access a plethora of sensitive information. Start by enabling two-factor authentication (2FA) for your email account using your security key.

- **Password Manager**
  Password managers are used to store and manage all your login credentials securely. Protecting this tool is essential because it contains the keys to your digital kingdom. Ensure your password manager is locked behind your security key.

- **Financial Services**
  Any accounts related to your finances, such as online banking, investment platforms, and payment apps, should be secured with your security key. Unauthorized access to financial accounts can lead to severe consequences.

- **Cloud Storage**
  If you use cloud storage services like Google Drive or Dropbox, add an extra layer of security by linking them to your security key. This protects your documents, photos, and other files from being accessed by unauthorized users.

- **Social Media Accounts**
  Social media accounts often contain personal information and may be used for identity theft. Enable 2FA and link your security key to protect your social profiles.

- **Work-Related Accounts**
  If you use online tools and platforms for work, secure them with your security key. This includes project management tools, communication platforms, and any other work-related services.

- **Online Shopping**
  For e-commerce platforms where you make purchases, ensure your payment information is protected with your security key. Unauthorized access to your online shopping accounts can lead to fraudulent transactions.

- **Cryptocurrency Wallets**
  If you're involved with cryptocurrencies, your wallet should be fortified with the highest level of security. Many cryptocurrency wallets offer hardware wallet integration, which is an ideal match for your security key.

- **Healthcare Portals**
  Medical records are highly sensitive, and unauthorized access can lead to privacy breaches and identity theft. Protect your healthcare portal with your security key.

- **Travel and Booking Services**
  Airline accounts, hotel bookings, and travel rewards programs should be secured. Unauthorized access can lead to inconveniences during your travels.

2. CHECK ACCOUNT SECURITY OPTIONS

Check which security settings are offered. This can be accomplished by logging into your account and navigating to your security settings on the platform you have chosen.

Look for language such as:

- Two-step verification
- Two-factor authentication
- Multi-factor authentication

Within the settings listed above, identify one or more of the following security options:

- **Security Key:** Security Key MFA uses physical devices and offers a high level of protection against phishing. It's considered one of the most secure forms of MFA.

- **Authentication App** (may go by other names): Yubico Authenticator as MFA is a software-based solution that relies on generating one-time codes. While it provides good security, it may not be as resistant to phishing as physical security keys. Unlike other Authenticators that store codes on vulnerable devices, our Authenticator ensures maximum safety by securely storing authentication codes on the YubiKey itself. Trust in a solution that prioritizes your security, setting us apart as the superior choice for safeguarding your digital assets.

- **Passkey:** Passkeys work using public key cryptography and proof that you own the credential is only shown to your online account when you unlock your phone. To sign into a website or app on your phone, just unlock your phone — your account won't need a password anymore.

Once you have a good idea of what security options your account supports, follow the corresponding instructions in the next step.

3. ADDING YOUR YUBIKEY

Plug your YubiKey into the USB port on the KSI AuthentiKey keyboard top, or if using NFC, have it ready to tap. If this is your first time using your YubiKey and you plan to use NFC, you must plug the YubiKey into any powered USB outlet first, to activate the Key. Find details here.

Please note that the following steps are intended as a general guide and support will vary by service. Because each service has its own unique security settings, you might notice some differences in the setup process.

Option 1: Security Key MFA (YubiKey's Preference)

1. Log in to your chosen service and navigate your account's security settings.
2. Look for the option to add a "Security Key."
3. Follow the instructions given by your service to add a security key, including instructions prompted by your browser.

Option 2: Authentication App (Widely Supported)

1. Download the Yubico Authenticator app to a device that is compatible with your YubiKey.
2. Log in to your chosen service and navigate your account's security settings.
3. Look for options to add an "Authentication App."
4. Scan the QR code or enter the key code generated by your service to pair to your Yubico Authenticator.
5. Enter the 6-8 digit code generated by the Yubico Authenticator into your service to finalize setup.

Option 3: Passkey (New)

1. Log in to your chosen service and navigate to your account's security settings.
2. Look for options to add a "Passkey."
3. Your browser will prompt you to create a passkey using a variety of methods. Make sure to select the option that is named or mentions "Security Key." If this is not chosen, you could accidentally create a passkey that is not protected by your YubiKey.

Follow the steps prompted by your browser once the passkey option is selected. Learn more about passkeys.

Note: Please note that certain services may prompt you to create a PIN or verify the PIN if one is already set. This is the FIDO2 PIN and it can most easily be viewed or set using the Yubico Authenticator.

4. SPARE KEYS

It is recommended to have more than one YubiKey. In this way, one key can be used as a primary Key, and the other can be used as a spare Key, just as you would for your house or car.

Having a spare Key gives you the assurance that if you lose your primary Key, you will not be without access to your accounts when needing them most.

You can set up your spare YubiKey by following the same steps listed above. It is encouraged to set up both your primary and spare Keys at the same time. Shop for a spare YubiKey

YubiKey 5 NFCUSB-A + NFC wireless

YubiKey 5C NFCUSB-C + NFC wireless

5. IMPORTANT TIPS

Test it out

Now that you have set up your YubiKey, try logging in to your account. It should ask for your YubiKey. If you're not being asked for your YubiKey, something may have gone wrong, or this service is using something called "Trusted Devices." Some services have a feature called "Trusted Devices", which means the service you are using recognizes the device without needing to re-enter your verification codes or using your Security Key.

Keep it Safe

Treat your YubiKey as you would your house keys. Keep it in a safe place and do not share it with anyone.

Software

The YubiKey is ready to be used right out of the box. Additional applications, such as the Yubico Authenticator are generally not needed unless components like key configuration or authenticator codes are required.

Please note that, in many cases, it is not necessary to configure your key prior to using it with online services. It is recommended that you make a configuration change only if instructed to do so.

Information courtesy of Yubico.com