YubiKey Bio Series Technical Manual

Yubico

Dec 06, 2022

CONTENTS

CHAPTER

ONE

INTRODUCTION

The YubiKey Bio Series offers the familiar YubiKey experience users have come to know and trust, but adds the convenience of a new biometric touch feature.

The series is comprised of two keys:

- The YubiKey Bio - FIDO Edition (USB-A form factor)
- The YubiKey C Bio - FIDO Edition (USB-C form factor)

1.1 Protocols Supported

Both keys in the YubiKey Bio Series support the FIDO authentication protocols, and will work with sites and applications that support the FIDO2 and FIDO U2F protocols (for more information, see *YubiKey Bio and FIDO2* and *YubiKey Bio and FIDO U2F*). FIDO2 (sometimes referred to as WebAuthn) builds upon FIDO U2F, and is the standard which enables the replacement of password-based authentication.

The YubiKey Bio Series provides firmware applications to support two modes of authentication via the FIDO2 and U2F protocols (see *YubiKey Bio and FIDO2* and *YubiKey Bio and FIDO U2F*). Even though the firmware applications are separate from one another, they both share the same PIN and FIDO reset capability. In fact, a FIDO reset will reset both applications (to manage these applications, see *Troubleshooting and Tools*).

1.2 Using the YubiKey Bio

To just start using the keys in the YubiKey Bio Series without going into any details, refer to Yubico's setup page, which functions as a **quick start guide**.

The current guide, however, gives:

- An explanation of the way the YubiKey Bio works and descriptions of the different user experiences with the various protocols
- Full instructions for enrolling fingerprints using platform support:
  - *Using Chrome to Enroll Fingerprints* and
  - *Using Windows to Enroll Fingerprints*
- Brief descriptions of the protocols supported in *YubiKey Bio and FIDO2* and *YubiKey Bio and FIDO U2F*
- A brief explanation of the role the Yubico Authenticator for Desktop plays in managing the YubiKey Bio, plus links for downloading it and to its documentation.

1.3 Usage Notes

The YubiKey Bio implements biometrics as outlined in the CTAP 2.1 specification. The best user experiences are provided by the YubiKey Bio with client applications and browsers that also implement CTAP 2.1. Applications and browsers that implement CTAP 1 or CTAP 2.0 will also work with the YubiKey Bio; however, the UI on client devices will not be as intuitive, and there may be some limitations.

To get in touch with Yubico Support, click here.

CHAPTER TWO

PHYSICAL ATTRIBUTES

The YubiKey Bio - FIDO Edition is available in the USB-A format, while the YubiKey C Bio - FIDO Edition is available in the USB-C format, both with a maximum transfer rate of 12 Mbps.

The sensors and LEDs behave the same way in both formats.

YubiKey Bio - FIDO Edition

YubiKey C Bio - FIDO Edition

2.1 Sensors

The YubiKey Bio recognizes **two interactions**, one a **touch**, and the other a **fingerprint**. Its recognition of the fingerprint - or lack thereof - is communicated through the LEDs (see *LED Behavior*).

On the YubiKey Bio, the silver-colored bezel encircling the fingerprint sensor provides the grounding plane required to read the fingerprint.

Biometric Touch

When prompted to have the YubiKey Bio read your fingerprint from the fingerprint sensor, be sure to touch at least a tiny part of the ring. If you use your little finger to touch only the center of the fingerprint sensor, the key will not read the fingerprint.

Plain Touch

When prompted to touch the YubiKey Bio but not explicitly asked for the fingerprint, touch **both** the bezel and the fingerprint sensor, even though the fingerprint will not be read.

Tips provides detailed instructions on using the fingerprint sensor.

2.2 LEDs

The YubiKey Bio has a green LED and an amber LED to provide direct feedback, flashing when the key is ready for interaction or communicating something about the interaction. *LED Behavior* provides detailed descriptions.

2.3 Ratings

The YubiKey Bio has been IP68-rated under the IEC standard 60529.

2.4 Care and Cleaning

To clean the YubiKey and sensor, use only wipes impregnated with no more than 70% isopropyl alcohol.

2.5 Operational Data

- Dimensions
  - YubiKey A Bio: 18mm x 45mm x 3.35mm
  - YubiKey C Bio: 18mm x 45mm x 3.75mm
- Weight: YubiKey Bio A: 4.5g; YubiKey Bio C: 5.0g
- Operating Temperatures: 0 °C - 40 °C (32 °F - 104 °F)
- Storage Temperatures: -20 °C - 85 °C (-4 °F - 185 °F)

To get in touch with Yubico Support, click here.

CHAPTER

THREE

INTERFACES AND APPLICATIONS

3.1 Interfaces

Like all other YubiKeys, the YubiKey Bio Series are USB 2.0 devices.

Note: **Developers**: The USB PID and iProduct string are `0x0402` and `YubiKey FIDO` respectively (see YubiKey USB ID Values).

3.2 Applications

All keys in the YubiKey Bio Series support WebAuthn sites and applications that support the FIDO2 and FIDO U2F protocols (for more information, see *YubiKey Bio and FIDO2* and *YubiKey Bio and FIDO U2F*). FIDO2 (also sometimes referred to as WebAuthn) is also the standard that enables the replacement of password-based authentication.

Each application can be enabled and disabled independently. Up to five fingerprints can be stored on a YubiKey Bio. For management, see *Tools*.

To get in touch with Yubico Support, click here.

CHAPTER

FOUR

REQUIREMENTS: PLATFORM AND BROWSER COMPATIBILITY

4.1 Desktop

The YubiKey Bio Series works with the latest versions of most browsers and desktop operating systems. Currently, the best experience can be had on macOS, Chrome OS, and Linux, running up-to-date Chromium-based browsers.

On **Windows 10**, browsers are not currently able to tell the user when the YubiKey has failed to match the fingerprint, so the user must watch out for the YubiKey's amber LED blinking to indicate when an attempt has failed. **Windows 11** does not have this problem.

On other platforms, browsers such as Firefox and Safari have not yet (at the time of writing) implemented CTAP 2.1 and therefore the user will typically be prompted to enter the PIN even if the key is not in the "biometrics blocked" state.

4.2 Mobile

- The YubiKey Bio does not have NFC capabilities.
- The YubiKey Bio can be used with mobile, but it is reliant on mobile operating system support as well as on browser support for the FIDO protocols. For more information, please refer to the relevant manufacturer's web sites for your mobile device.
- When the YubiKey Bio has fallen back to requiring the PIN, users may need to resort to computers (as opposed to mobile devices) to unblock biometrics .

To get in touch with Yubico Support, click here.

CHAPTER

FIVE

HOW THE YUBIKEY BIO WORKS

For the full technical explanation of this from a developer perspective, start with the Yubico's WebAuthn Developer Guide.

Note: In the following, "credentials" will be referenced repeatedly. There are different kinds of credentials. To pursue all the distinctions, consult the FIDO2 page on the Fido Alliance web site.

5.1 Enrollment

Before you can start using the YubiKey Bio with services and applications, you need to first set a fido2-pin-label and then enroll at least one fingerprint. The YubiKey Bio needs to have the PIN as a fallback in case it cannot recognize your fingerprint.

Although there are two FIDO *applications* on the YubiKey Bio, namely FIDO2 and U2F, it is the FIDO2 PIN that is required as fallback for both. The PIN is not associated with any *site*. When the fingerprint does not work and the key falls back to the PIN, it is the *key* that needs the PIN for authentication to all sites, including U2F sites (even though U2F has no concept of PIN). With fallback to PIN, it is easy if the user is authenticating to a WebAuthn/FIDO2 site, because the browser/client app *can* prompt for the PIN. Otherwise the user must unblock biometrics by using either:

- The YubiKey Bio start page
- Yubico Authenticator for Desktop.

The "working" of the fingerprint is described in the following. For information on how and why the fingerprint might not "work", see *Tips*.

5.1.1 Risk Mitigation

To mitigate the risk of being shut out of your account or service, it is always advised to register a second YubiKey. For more information, see https://www.yubico.com/spare/.

5.1.2 Fingerprints and Templates

An enrolled fingerprint is stored on the YubiKey Bio not as an image, but in the form of a template, similar to a one-way hash. It is not possible to recreate an image of a fingerprint from a template, nor does the template ever leave the YubiKey.

After enrollment, each time you apply your fingertip to the fingerprint sensor, the key tries to match the fingerprint against the template stored on the key.

5.2 Parties Involved in Registration and Authentication

Closely related to *Requirements: Platform and Browser Compatibility*, registering and authenticating with a YubiKey Bio to an app or a service that supports WebAuthn or U2F involves several parties:

- The user (with their fingerprints and knowledge of the PIN)
- The YubiKey Bio
- The FIDO2 application or the U2F application on the YubiKey Bio
- The FIDO2/WebAuthn or U2F-supporting **browser** or **client**
- The service or app

All these work together. For example, if your YubiKey does not work as expected, you might be using a browser or an app that does not support FIDO2 security keys.

5.3 Registration

Registration of a YubiKey Bio with a site, service, or application is the same as for other YubiKeys.

5.4 Authentication

Depending on the protocol supported by the site or service, there are several possible user experiences (scenarios). These are described below.

5.4.1 User Experiences

The user experience with the YubiKey Bio is dictated by a combination of the site or service that the user is authenticating against and the browser or client. Different service and client combinations will yield different results. The user experiences are determined by the different options for developers implementing FIDO2 with the WebAuthn and CTAP protocols. Please note that the following descriptions of user scenarios are only **high-level overviews**. The experiences will change every time the various forms of support change.

Passwordless

This scenario provides the best user experience by enabling a passwordless flow backed by strong authentication. To achieve it, discoverable credentials must be used. When the user authenticates to the site or service,

1. The client or browser prompts the user to insert the YubiKey.
2. The client makes a request to the YubiKey to see if any credentials on the key have been registered for use with this site or service.
3. If the right credentials are found, the *client or browser* prompts the user to apply their fingertip to the YubiKey Bio's sensor.
   - If the fingerprint match is successful, the appropriate response is sent to the client or browser to complete authentication.
   - If the fingerprint match is unsuccessful three times in a row, the client or the browser prompts instead for the PIN. After correctly inputting the PIN, the user is then prompted to touch the key to prove presence (as opposed to verifying identity). In this situation, the YubiKey Bio behaves like any other key in the YubiKey 5 Series.

Multifactor Authentication (MFA)

When a user authenticates to the site or service,

1. The client or browser prompts the user to insert their username and password. These are what the server uses to identify the user and determine whether they have registered.
2. If username and password match the server's records, the site or service prompts the user for an additional form of identification to prove their identity. This is called **multifactor** authentication.
3. The user proves their identity *to the key* either by providing a fingerprint that the key can match to its template, or by entering the PIN.
   - If the fingerprint match is successful, the appropriate response is sent to the client or browser to complete authentication.
   - If the key is unsuccessful at matching fingerprint to template three times in a row, the YubiKey Bio goes into the biometrics blocked state, signaling this by slow constant flashing of the amber LED. The client or the browser prompts instead for the PIN and for the user to touch the key (checking for user presence). In this situation, the YubiKey Bio behaves like any other key in the YubiKey 5 Series.

U2F

This scenario only works well if the fingerprint match is successful and the user flow is the same as the multifactor flow. If the fingerprint match is unsuccessful, any prompts from the site or service are unlikely to be clear and unambiguous. The user would likely end by having to unblock the YubiKey, which can be done by visiting the YubiKey Bio start page or by using the Yubico Authenticator for Desktop.

5.5 Locking/Blocking

Fingerprint

If the YubiKey cannot match fingerprint to template three times in a row, fingerprint recognition is blocked. The YubiKey Bio falls back to PIN.

PIN

If you enter the wrong PIN eight times in a row, the YubiKey FIDO2 application will be **locked**, which means it cannot communicate with you or with any site or service. It indicates the blocked state by flashing its amber LED slowly and continuously. In order to restore this functionality, the FIDO2 application must be reset. For more details, see fido2-pin-label.

Unblock

Unblock the YubiKey Bio's biometric function (its ability to read fingerprints) by going to the unblocking FAQ on the YubiKey Bio start page. Otherwise you can use any of the other methods given in *Tools*.

Reset

You can also **reset** it, but doing so erases all the discoverable credentials on it, setting it back to factory defaults. See *Resetting Your YubiKey Bio with the Yubico Authenticator for Desktop*.

5.6 Managing Credentials

If you decide to discontinue using a site or service, you can delete its discoverable credential. This frees up space on the YubiKey Bio, which can contain up to 25 such credentials.

To view the discoverable credentials on your YubiKey and delete them selectively, use the Yubico Authenticator for Desktop version 5.1.0 and above.

For more information on credentials in general, and in particular on managing them, see Enhancements to FIDO 2 Support for details.

For more **developer-oriented** information on this, see Discoverable Credentials / Resident Keys on Yubico's developer site.

To get in touch with Yubico Support, click here.

CHAPTER

SIX

USING CHROME TO ENROLL FINGERPRINTS

Set a PIN and enroll the *first* fingerprint using the Chrome browser on a macOS, Linux or Chrome OS device. To enroll more fingerprints use the Chrome settings as described in *Enrolling Additional Fingerprints*.

Note: A YubiKey Bio is a FIDO2 *hardware* authenticator. Both Windows and Mac have *built-in* FIDO2 authenticators - i.e., software authenticators that in this case are also platform authenticators. The prompts in both Windows and Mac *might assume* you will be using their own authenticators. Therefore it is quite easy to register *their* authenticators with a site or service by mistake, without realizing that you are not registering your YubiKey. Read the prompts carefully to avoid this. And remember that the PIN is associated with the authenticator, not the site or service.

Although there are two FIDO *applications* on the YubiKey Bio, namely FIDO2 and U2F, it is the FIDO2 PIN that is required as fallback for both. The PIN is not associated with any *site*. When the fingerprint does not work and the key falls back to the PIN, it is the *key* that needs the PIN for authentication to all sites, including U2F sites (even though U2F has no concept of PIN). With fallback to PIN, it is easy if the user is authenticating to a WebAuthn/FIDO2 site, because the browser/client app *can* prompt for the PIN. Otherwise the user must unblock biometrics by using either:

- The YubiKey Bio start page
- Yubico Authenticator for Desktop.

For information on the YubiKey Bio's sensor and tips on working with fingerprints see *Tips*. For detailed information on FIDO2 PINs and their requirements, see Understanding YubiKey PINs.

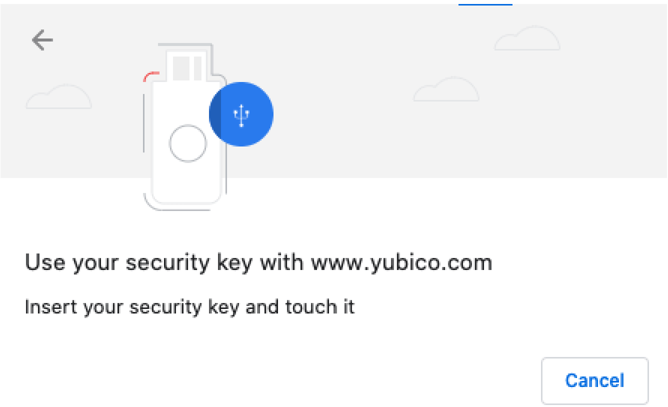
6.1 Enrolling the First Fingerprint

Step 1

Use an up-to-date Chrome browser to open the YubiKey Bio Series setup website. Insert your YubiKey Bio into your computer.

Step 2

Scroll down to the green button, **Enroll using Chrome**, and click it. The **Use your security key with Yubico.com** popup appears, taking you through the PIN setup (if no PIN is set) and later the fingerprint enrollment:

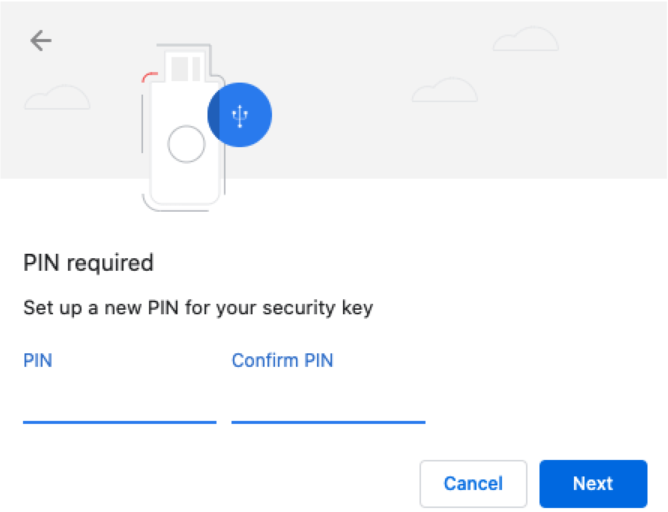


Use your security key with www.yubico.com

Insert your security key and touch it

Step 3

If the amber LED flashes slowly, it means that either no fingerprint is enrolled or biometrics is blocked. If you have reason to believe biometrics is blocked, go to the appropriate link on the YubiKey Bio Series setup page or to *Troubleshooting and Tools*. Otherwise, *touch the key*:



PIN required

Set up a new PIN for your security key

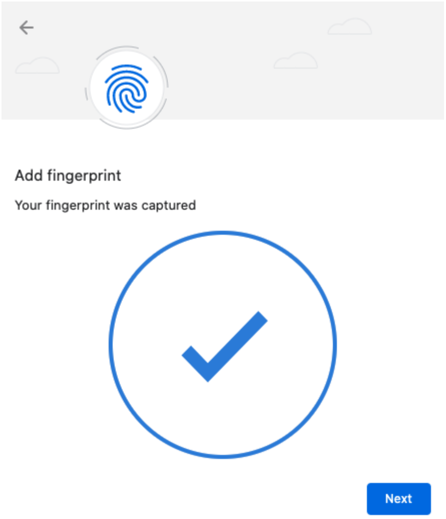
Step 4

If no PIN is set, set one by entering at least 4 digits, then confirming this PIN by re-entering it. If the YubiKey Bio already has a PIN set you are prompted to enter it.

Step 5

When prompted, touch the fingerprint sensor and the bezel. You are prompted to touch the sensor several times, as set out below. Change the angle of finger to sensor slightly each time.

Continue lifting and re-applying the same finger until the gray circle is entirely blue, the fingerprint icon is replaced by a tick mark, and the message in the popup reads “Your fingerprint was captured.”

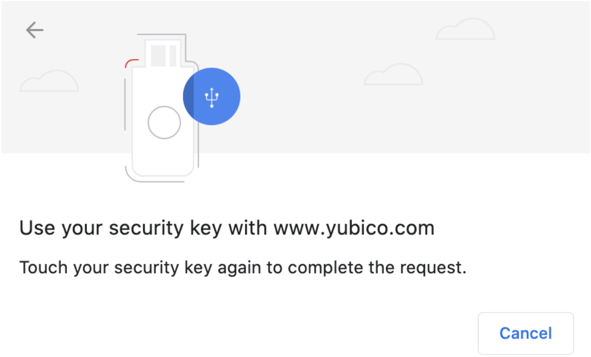


Add fingerprint

Your fingerprint was captured

Step 7

Click **Next**. The **Touch your security key again to complete the request** popup appears:



Use your security key with www.yubico.com

Touch your security key again to complete the request.

Step 8

Touch the bezel and sensor one last time. The final popup announces that enrollment was successful. The YubiKey Bio now has a template for that fingerprint.

6.2 Enrolling Additional Fingerprints

If the YubiKey Bio already has fingerprint(s) enrolled on it, repeating the procedure for the first fingerprint does not work for subsequent fingerprints. Instead follow these steps.

Note: You can also use this method for setting a PIN for a new YubiKey Bio and enrolling all fingerprints.

Step 1

Either paste `chrome://settings/securityKeys` into the Chrome address field or click on the three vertical dots to the right of the URL field to navigate to **Settings->Security->Advanced->Manage security keys**.

Step 2

Click **Fingerprints** and follow the instructions in the popup.

To get in touch with Yubico Support, click here.

CHAPTER SEVEN

USING WINDOWS TO ENROLL FINGERPRINTS

These are the instructions for setting a PIN on a YubiKey Bio and enrolling fingerprints on it using the Sign-in options on a Windows 10 or Windows 11 system.

Note: A YubiKey Bio is a FIDO2 *hardware* authenticator. Both Windows and Mac have *built-in* FIDO2 authenticators - i.e., software authenticators that in this case are also platform authenticators. The prompts in both Windows and Mac *might assume* you will be using their own authenticators. Therefore it is quite easy to register *their* authenticators with a site or service by mistake, without realizing that you are not registering your YubiKey. Read the prompts carefully to avoid this. And remember that the PIN is associated with the authenticator, not the site or service.

Note: To get to the popup (prompt) for the YubiKey, you might need to *cancel* out of the pop-up for the built-in authenticator.

Although there are two FIDO *applications* on the YubiKey Bio, namely FIDO2 and U2F, it is the FIDO2 PIN that is required as fallback for both. The PIN is not associated with any *site*. When the fingerprint does not work and the key falls back to the PIN, it is the *key* that needs the PIN for authentication to all sites, including U2F sites (even though U2F has no concept of PIN). With fallback to PIN, it is easy if the user is authenticating to a WebAuthn/FIDO2 site, because the browser/client app *can* prompt for the PIN. Otherwise the user must unblock biometrics by using either:

- The YubiKey Bio start page
- Yubico Authenticator for Desktop.

For information on the YubiKey Bio's sensor and tips on working with fingerprints see *Tips*. For detailed information on FIDO2 PINs and their requirements, see Understanding YubiKey PINs.

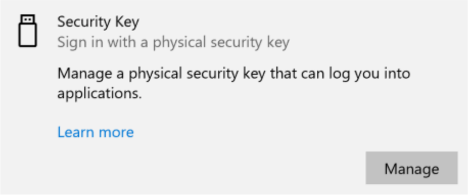
Step 1

On *Windows 10*, click **Enroll using Windows** on the YubiKey Bio setup page <https://www.yubico.com/setup/yubikey-bio-series/>`_.

On *Windows 11*, click **Enroll using Windows** on the YubiKey Bio setup page <https://www.yubico.com/setup/yubikey-bio-series/>`_. Then go to Step 3 below.

Step 2

On *Windows 10*, in the expanded **Security Key** field, click **Manage**.



Security Key

Sign in with a physical security key

Manage a physical security key that can log you into applications.

Step 3

On both *Windows 10* and *Windows 11*, follow the Windows setup directions. Insert the YubiKey Bio into your computer's USB port and set a PIN for your YubiKey Bio if the key does not already have a PIN. In the **Security Key PIN** field, click **Add**. Enter a security key PIN and click **OK**.

Step 4

To enroll your fingerprint, in the **Security Key Fingerprint** field, click **Set up** and follow the prompts.

Touch the YubiKey Bio sensor while the green LED is still flashing, making sure to touch the ring-bezel as well.

Vary the way you touch each time to include more of the fingerprint. If the fingerprint you enroll is smaller than the sensor, apply some pressure to help ensure a good image capture.

Continue lifting and re-applying the same finger until you see the **All set!** message.

Perform this step up to five times for a total number of 5 enrolled fingerprints.

To get in touch with Yubico Support, click here.

CHAPTER

EIGHT

TIPS

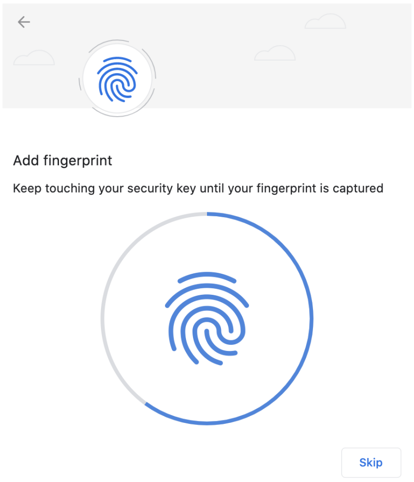
8.1 LED Behavior

The YubiKey Bio is not in a permanent state of readiness. It is therefore essential to wait for the key to signal its readiness by flashing the green LED before you touch it.

- If the key reacts to your touch by the flashing or blinking of the green LED, you used the right touch.
- If the amber LED flashes three times in quick succession, the attempt to match your fingerprint with the template was not successful.
- If the amber LED flashes slowly and continuously, it is in the biometrics blocked state.
- If the key does not react to your touch, you might not have touched both the bezel and the sensor. When you apply your fingerprint, always make sure you are touching the bezel at the same time. See *Tips for the Touch* below.

8.2 Fingerprint Enrollment Progress Indicators

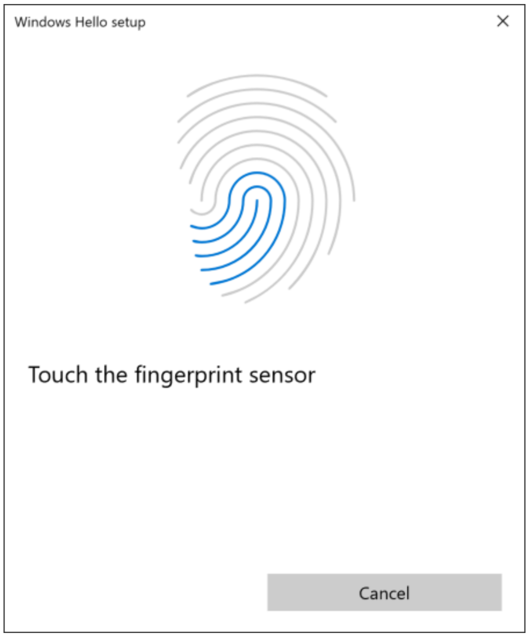
The progress of reading of your fingerprint is displayed on-screen. The way it is shown depends on the client platform and browser. It is generally not under the control of the site or the service. The screenshots below show enrollment using platform support:



Add fingerprint

Keep touching your security key until your fingerprint is captured

Fig. 1: Chrome on macOS, Linux, and Chrome OS: Capturing the Fingerprint



Windows Hello setup

Touch the fingerprint sensor

Fig. 2: Windows: Capturing the Fingerprint

8.3 Tips for the Touch

Because the fingerprint can be negatively affected by environmental conditions such as heat, cold, injury, etc., it is not always easy for the YubiKey Bio to interact with it. The following tips are helpful.

The YubiKey Bio recognizes **two interactions**, one a **touch**, and the other a **fingerprint**. Its recognition of the fingerprint - or lack thereof - is communicated through the LEDs (see *LED Behavior*).

On the YubiKey Bio, the silver-colored bezel encircling the fingerprint sensor provides the grounding plane required to read the fingerprint.

Biometric Touch
: When prompted to have the YubiKey Bio read your fingerprint from the fingerprint sensor, be sure to touch at least a tiny part of the ring. If you use your little finger to touch only the center of the fingerprint sensor, the key will not read the fingerprint.

Plain Touch
: When prompted to touch the YubiKey Bio but not explicitly asked for the fingerprint, touch **both** the bezel and the fingerprint sensor, even though the fingerprint will not be read.

Fingerprint
: For enrolling, when we say ‘fingertip’, we actually mean the pad on the tip of the finger where the whorls of the fingerprint are. The fingerprint could equally well be a thumbprint or a toeprint; the YubiKey Bio makes no distinction between fingers, thumbs, and toes.

Quality of print
: Dry or scarred skin can impede the key’s ability to perform a successful fingerprint match. If your hands are dry, use moisturizer or water to enable conduction. Do not apply wet fingertips.

Repeated readings
: Enrolling your fingerprint requires pressing your fingertip against sensor (and bezel) several times, usually 5 to 8 times. If an attempt to capture is unsuccessful the YubiKey Bio will need you to repeat it.

Vary the angle

When enrolling a new fingerprint, angle your finger so that different parts of the fingerprint come in contact with the sensor and bezel with each capture. This enables the YubiKey Bio sensor to collect a larger area of your finger.

Temperature

If the fingertip is too cold, the YubiKey Bio might not be able to read the fingerprint. If your hands are cold, rub them together to get the circulation going and warm them up.

Press firmly

Press the YubiKey Bio sensor and bezel with your fingertip gently but firmly and hold for a second or so. If you are using an adapter, it may be necessary to hold onto the adapter to prevent it from bending and interrupting the connection to the YubiKey.

Stabilize key

If the YubiKey Bio seems to wobble in the USB port, use your other hand to hold it steady in the port while you are applying your fingertip.

Stabilize dongle

If you are using a dongle as an adapter to your device's USB port, ensure the YubiKey Bio is stable enough for you to apply sufficient pressure with your fingertip.

Check the LEDs

When you start fingerprint enrollment, the green LED on your YubiKey Bio starts to flash. Start the fingerprint enrollment before the green LED on the YubiKey Bio stops flashing. The amber LED might flash slowly, indicating that no fingerprint is enrolled or that biometrics is in the blocked state.

Clean the sensor

If there is dust or oil residue on the YubiKey Bio sensor and bezel, clean it. See *Care and Cleaning*.

Change ports

Sometimes the USB port does not work well or the YubiKey Bio is loose in the port. Insert the YubiKey Bio in a different port on your device.

CHAPTER

NINE

TROUBLESHOOTING AND TOOLS

9.1 Troubleshooting

The primary source for troubleshooting tips is the FAQ on the YubiKey Bio Series setup page.

Fingerprint
If the YubiKey cannot match fingerprint to template three times in a row, fingerprint recognition is blocked. The YubiKey Bio falls back to PIN.

PIN
If you enter the wrong PIN eight times in a row, the YubiKey FIDO2 application will be **locked**, which means it cannot communicate with you or with any site or service. It indicates the blocked state by flashing its amber LED slowly and continuously. In order to restore this functionality, the FIDO2 application must be reset. For more details, see fido2-pin-label.

Unblock
Unblock the YubiKey Bio's biometric function (its ability to read fingerprints) by going to the unblocking FAQ on the YubiKey Bio start page. Otherwise you can use any of the other methods given in *Tools*.

Reset
You can also **reset** it, but doing so erases all the discoverable credentials on it, setting it back to factory defaults. See *Resetting Your YubiKey Bio with the Yubico Authenticator for Desktop*.

If you run into any issues with a YubiKey Bio, you can also refer to the Knowledge Base on Yubico's Support site and search for your issue. If your issue is not listed in the Knowledge Base, or if you have any technical questions, you can open a ticket with our Technical Support team.

9.1.1 Unblocking/Unlocking

Use the appropriate link on the YubiKey Bio Series setup page or the Yubico Authenticator for Desktop.

9.1.2 Other Issues

If you run into any issues with a key from the YubiKey Bio Series, refer to the Knowledge Base and search for your issue. If your issue is not listed in the Knowledge Base, or if you have any technical questions, you can get in touch with Yubico Support, http://yubi.co/support.

9.2 Tools

9.2.1 Yubico Authenticator for Desktop

Yubico Authenticator for Desktop can be used to manage the YubiKey Bio. It is open source and cross-platform, running on Windows, macOS, and Linux. The iOS and Android versions of Yubico Authenticator cannot be used to manage the YubiKey Bio.

To get in touch with Yubico Support, click here.

CHAPTER

TEN

RESETTING YOUR YUBIKEY BIO WITH THE YUBICO AUTHENTICATOR FOR DESKTOP

In this context, resetting means resetting the FIDO application. You can also perform a FIDO reset using the YubiKey Manager, Windows Sign-in options, or the Chrome browser settings.

The main cause for the biometric function blocking is failure to match the fingerprint three times in a row. If the YubiKey Bio was locked because the biometric function was blocked, you can just unblock it instead of resetting it: see *Tools*.

Resetting the key is not the same as unblocking it. Because resetting the FIDO2 and FIDO U2F applications returns the key to the factory default state, when it has neither fingerprints nor PIN nor credentials, you must enroll your fingerprints again after resetting it (see the relevant Enrolling chapter, either *Using Chrome to Enroll Fingerprints* or *Using Windows to Enroll Fingerprints*), and register your key again to your apps and services.

Note that resetting your YubiKey Bio deletes all credentials, the PIN, and stored fingerprint templates.

To review your options for tools to reset the YubiKey Bio, see *Tools*.

To get in touch with Yubico Support, click here.

CHAPTER

ELEVEN

FREQUENTLY ASKED QUESTIONS

The FAQs are on the YubiKey Bio Start Page.

To get in touch with Yubico Support, click here.

CHAPTER

TWELVE

YUBIKEY BIO AND FIDO2

The YubiKey Bio Series - FIDO Edition supports all FIDO2 scenarios supported by the YubiKey 5 Series and the Security Key Series. It can be used in both passwordless and second factor authentication scenarios. In both scenarios the fingerprint is used *in lieu of* the PIN, similar to the way biometrics is used on a smartphone. However, there are some scenarios in which the PIN is required. The PIN is required when enrolling or otherwise managing fingerprints, just as it is on a smartphone. However, the only opportunity to input the PIN is after 3 unsuccessful attempts at matching a fingerprint with an enrolled finger.

12.1 Discoverable Credentials

Like FIDO U2F, the FIDO2 standard offers the same high level of security, as it is based on public key cryptography. In addition to providing phishing-resistant two-factor authentication, the FIDO2 application on the YubiKey allows for the storage of discoverable credentials. (Fingerprint templates are not discoverable credentials.) Keys in the YubiKey Bio Series can hold up to 25 discoverable credentials. To manage them, see *Credential Management*.

12.1.1 FIDO2 PIN

The FIDO2 PIN is necessary for:

- Enrolling fingerprints
- Managing enrolled fingerprints
- Fallback after failure to match fingerprint with template.

The FIDO2 PIN must be between 4 and 128 characters in length (for more information, see https://support.yubico.com/hc/en-us/articles/4402836718866-Understanding-YubiKey-PINs)

- There is no PIN set by default
- Once a FIDO2 PIN is set, it can be changed but it cannot be removed other than by resetting the FIDO2 application.
- If the FIDO2 PIN is entered incorrectly 3 times in a row, the key will need to be reinserted before it will accept additional PIN entry attempts (reinserting “reboots” the key).
- To see the number of retries remaining, use YubiKey Manager and navigate to Applications > FIDO2.
- If the PIN is entered incorrectly a total of 8 times in a row (3+3+2), the FIDO2 application will be locked, and FIDO2 authentication will not be possible.
- To restore the FIDO2 functionality, the FIDO2 application must be reset.

Note: Resetting the FIDO2 application will also reset the U2F application. No site you have registered the YubiKey with using U2F will work until the YubiKey is re-registered with that site.

12.1.2 FIDO2 Credentials

The discoverable credentials can be used for passwordless authentication, or they can be used for two-factor authentication. In both scenarios the credentials can be protected by the FIDO2 PIN and in the case of a YubiKey Bio, biometrics can be used in lieu of the PIN provided that fingerprints have been enrolled and that the key is not in biometrics blocked state.

12.2 User Verification

The YubiKey Bio implements always-on user verification, or `alwaysUV`.

The user verification requirement asks for proof that the user logging in is the same user as the one who set the PIN, enrolled fingerprints, and registered the key with the app or service (Relying Party, or RP). For more information about user verification, see User Presence vs User Verification.

When `userVerification` is discouraged, the user experience is not optimal unless the platform has implemented CTAP 2.1. See *Multifactor Authentication (MFA)*.

12.3 Credential Management

If you decide to discontinue using a site or service, you can delete its discoverable credential. This frees up space on the YubiKey Bio, which can contain up to 25 such credentials.

To view the discoverable credentials on your YubiKey and delete them selectively, use the Yubico Authenticator for Desktop version 5.1.0 and above.

For more information on credentials in general, and in particular on managing them, see Enhancements to FIDO 2 Support for details.

For more **developer-oriented** information on this, see Discoverable Credentials / Resident Keys on Yubico's developer site.

12.4 Supported Extensions

The YubiKey Bio supports only the AppID extension (`appid`) as defined by the W3C Web Authentication API specification. This extension allows U2F credentials registered using the legacy FIDO JavaScript APIs to be used with WebAuthn. In practice, that means that if you register a YubiKey Bio on a website when it used U2F and that website later upgrades to FIDO2, previously registered U2F credentials will continue to work.

Note: Developers: For AAGUID values, see YubiKey Hardware FIDO2 AAGUIDs.

To get in touch with Yubico Support, click here.

CHAPTER

THIRTEEN

YUBIKEY BIO AND FIDO U2F

The FIDO U2F protocol does not require any special drivers or configuration to use, just a compatible web browser. The U2F application on the YubiKey can be associated with an unlimited number of WebAuthn sites supporting FIDO U2F authentication.

FIDO U2F on the YubiKey Bio Series requires that the touch be a successful biometric match with an already enrolled fingerprint. This is different from FIDO U2F on other YubiKeys.

13.1 PIN + U2F

As the concept of PIN does not exist in FIDO U2F, after three successive failures to match the fingerprint, the key goes into the "biometrics blocked" state without first prompting for the PIN. An amber LED blinks slowly and continuously to indicate this state. Biometrics can be unblocked with a FIDO2 operation using the PIN (e.g., authentication). See *Troubleshooting and Tools* for full instructions and more information.

Note: **Developers**: With regard to computer login tools that use FIDO U2F for second-factor authentication, some software may use a YubiKey and FIDO U2F as a second factor. Since FIDO U2F has no concept of fallback to PIN, the YubiKey Bio is not likely to be a good choice for this use case. For more information about software that falls into this category, visit Yubico's Support site and look for articles about the YubiKey Bio: https://support.yubico.com/hc/en-us/search?query=YubiKey+Bio

13.1.1 FIDO U2F Succeeded by FIDO2

FIDO2 is the umbrella term used to describe an amalgamation of two separate sets of specifications: WebAuthn and the Client-to-Authenticator Protocol, CTAP (currently version 2.1, and often referred to as CTAP2.1). The WebAuthn component provides a narrow scope of flexibility for developers on the service layer because it encompasses the logical interactions across a network. CTAP2.1, however, provides a much more open set of standards for the interaction between a security device and the user.

CTAP2.1 is also where biometrics such as fingerprint enrollment, management, and use were first defined. To create a cohesive user experience, adherence to this specification is required from:

- Authenticators such as the YubiKey Bio
- Clients such as the Chrome or Edge browsers
- Platforms such as Windows and macOS.

See *User Experiences*.

13.1.2 Supported Extensions

The YubiKey Bio supports only the AppID extension (`appid`) as defined by the W3C Web Authentication API specification. This extension allows U2F credentials registered using the legacy FIDO JavaScript APIs to be used with WebAuthn. In practice, that means that if you register a YubiKey Bio on a website when it used U2F and that website later upgrades to FIDO2, previously registered U2F credentials will continue to work.

Note: Developers: For AAGUID values, see YubiKey Hardware FIDO2 AAGUIDs.

To get in touch with Yubico Support, click here.

CHAPTER

FOURTEEN

COPYRIGHT

14.1 Trademarks

Yubico and YubiKey are registered trademarks of Yubico AB. All other trademarks are the property of their respective owners; in particular, Apple, Lightning®, Mac, and MacOS are trademarks of Apple Inc., registered in the U.S. and other countries.

14.1.1 Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

14.1.2 Contact Information

Yubico Inc.
5201 Great America Parkway
#122
Santa Clara, CA 95054
USA

To get in touch with Yubico Support, click here. More options for getting touch with us are available on the Contact page of Yubico's website.

14.1.3 Document Updated

2022-12-06 00:03:41 UTC