YubiKey Passkey Enabler User Guide

Yubico

Jun 22, 2026

CONTENTS

1 YubiKey Passkey Enabler Overview **1**
- 1.1 Getting started . . . 3

2 Platforms and Requirements **5**
- 2.1 Device requirements . . . 5
- 2.2 Security key requirements . . . 5
- 2.3 Compatible WebAuthn-enabled apps . . . 6
- 2.4 WebAuthn/FIDO2 website support . . . 6

3 Installation **9**
- 3.1 Next steps . . . 10

4 Configuration **11**
- 4.1 Enable the app as a passkey provider service in your Android settings . . . 11
- 4.2 Toggle NFC connectivity . . . 14
- 4.3 Always ask for PIN . . . 15
- 4.4 App colors . . . 15

5 Using the YubiKey Passkey Enabler App **17**
- 5.1 FIDO2 functionality support . . . 17
- 5.2 Using the YubiKey Passkey Enabler during a passkey registration flow . . . 17
- 5.3 Using the YubiKey Passkey Enabler during a passkey authentication flow . . . 23

6 Viewing Device Information **29**
- 6.1 Viewing AAGUID, PIN status, and supported interfaces . . . 29
- 6.2 Locating your device's NFC sensor . . . 31

7 Troubleshooting **33**
- 7.1 FIDO2 registration or authentication fails . . . 33
- 7.2 NFC scanning fails . . . 33
- 7.3 The PIN is blocked . . . 34
- 7.4 I'm not getting prompted for biometrics (fingerprint) during authentication . . . 34
- 7.5 I do not see the option to select the YubiKey Passkey Enabler during a FIDO2 operation . . . 35
- 7.6 Getting additional help . . . 35
- 7.7 Collecting application logs . . . 35

8 Release Notes **39**
- 8.1 2026 . . . 39

9 Copyright **41**
- 9.1 Trademarks . . . 41

9.2 Disclaimer 41
9.3 Contact Information 41
9.4 Document Updated 42

CHAPTER

ONE

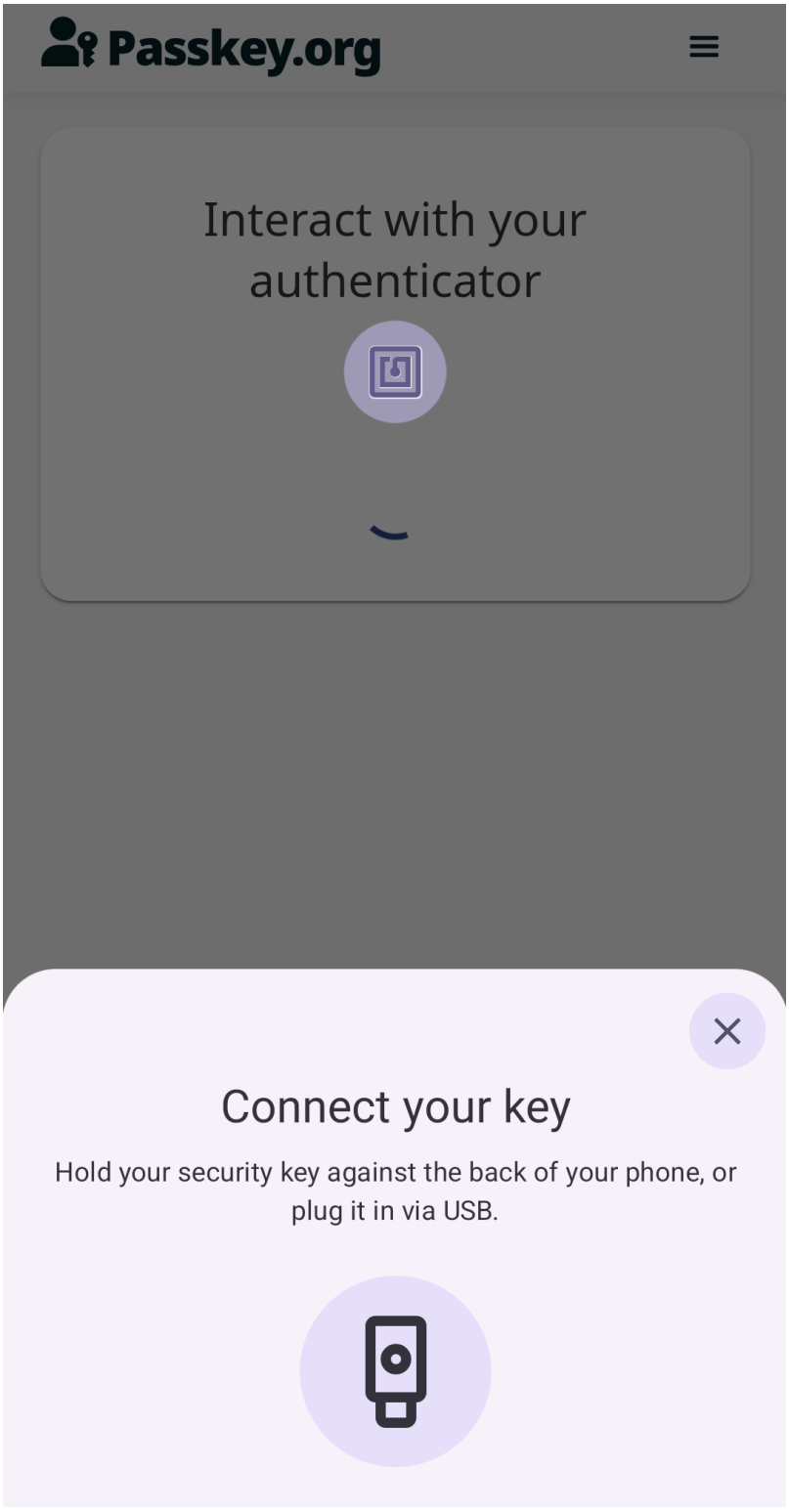
YUBIKEY PASSKEY ENABLER OVERVIEW

The YubiKey Passkey Enabler is a software application that improves the FIDO2 experience with hardware security keys on Android devices. As a passkey provider service, the app seamlessly integrates into passkey registration and authentication flows within WebAuthn-enabled applications.

The YubiKey Passkey Enabler provides support for:

- communication with security keys over USB and NFC connections
- PIN operations
- fingerprint biometric operations
- security key interaction

With the app's guided user interaction prompts and status messages throughout the passkey flow, you can use your FIDO2 security key with confidence on your Android device.


Passkey.org
Interact with your authenticator
Connect your key
Hold your security key against the back of your phone, or plug it in via USB.

1.1 Getting started

To use the YubiKey Passkey Enabler, you must have a compatible security key, Android device, and WebAuthn-enabled app (such as a browser). To perform passkey registration and/or authentication on a website *within* a WebAuthn-enabled browser, the website itself must also be WebAuthn-enabled. See *Platforms and Requirements* for more information.

Once the requirements have been satisfied, *download and install* the app from the Google Play Store. Next, *configure* your Android device to use the YubiKey Passkey Enabler as a passkey provider service.

After configuration, you can use the YubiKey Passkey Enabler for passkey registration and authentication flows. For information on how to select and interact with the app during these flows, see *Using the YubiKey Passkey Enabler App*.

If you run into issues, check the *Troubleshooting* chapter for possible solutions. The home screen of the YubiKey Passkey Enabler also displays some *device information* when connecting your security key, which can be helpful when debugging.

CHAPTER

TWO

PLATFORMS AND REQUIREMENTS

Using the YubiKey Passkey Enabler requires a compatible Android device, security key, WebAuthn-enabled app, and WebAuthn-enabled website. Refer to the following sections for more information on these requirements.

2.1 Device requirements

The YubiKey Passkey Enabler is supported for Android devices (mobile and tablet) running Android 14 and later.

To perform FIDO2 operations wirelessly over NFC, your Android device must have a built-in NFC reader. To verify device functionality, go to your device settings and search "NFC". If your search results return a mention of NFC connectivity settings, your device is NFC-capable.

Note: During device and app configuration, you will need to ensure that *NFC connectivity is toggled on*.

2.2 Security key requirements

Generally speaking, the app is compatible with FIDO2-capable security keys over USB and NFC connections. For Yubico products, this translates to the following YubiKey series:

- YubiKey 5 Series (standard, Enhanced PIN, FIPS, CCN, and CSPN)
- YubiKey Bio Series (FIDO Edition and Multi-protocol Edition)
- Security Key Series (standard and Enterprise Edition)

Note: To physically connect a USB-A YubiKey to an Android device with a USB-C or Micro-USB port, use a USB-A to USB-C adapter or a USB-A to Micro-USB adapter, respectively.

Some YubiKey Passkey Enabler features are dependent on security key capabilities. For example, the app will only prompt for a fingerprint if you have a security key that supports fingerprint biometrics, such as the YubiKey Bio Series.

Security keys from other vendors may work with the YubiKey Passkey Enabler, but complete compatibility is not guaranteed by Yubico.

Tip: To confirm if your security key supports NFC, connect your key to your Android device via USB and open the YubiKey Passkey Enabler app. Look for **Supported interfaces** on the home screen; if your security key supports NFC, you will see **NFC** listed here.

2.3 Compatible WebAuthn-enabled apps

Performing FIDO2 operations with the YubiKey Passkey Enabler requires a compatible WebAuthn-enabled app, such as a browser. The following apps have been tested and confirmed to be compatible by Yubico:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Samsung Internet
- Microsoft Teams
- Booking.com
- Roblox
- Uber
- Amazon Shopping

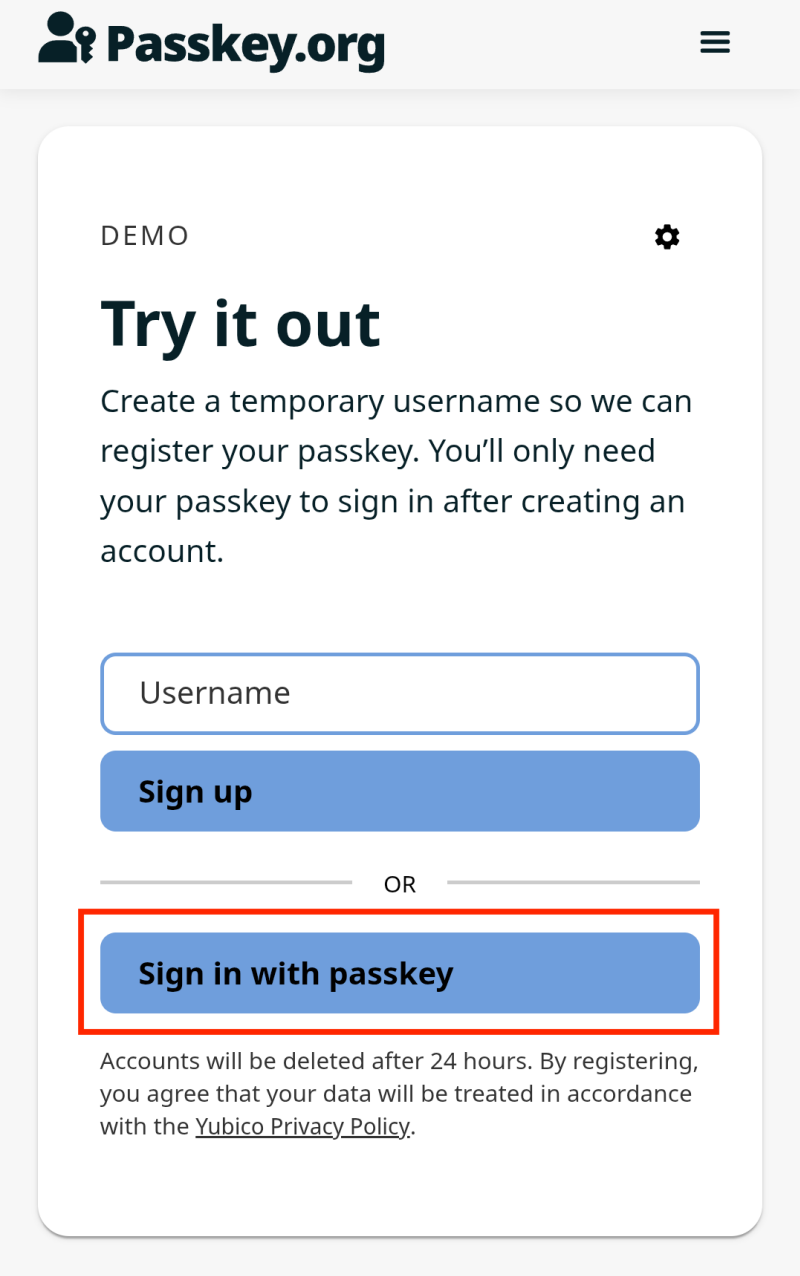
If you run into issues using the YubiKey Passkey Enabler with any of the compatible apps listed here, please report the issue by submitting a request with our customer support team.

Other apps may be compatible but have not been thoroughly tested by Yubico. WebAuthn implementation differs across apps, and nonstandard WebAuthn operations may affect compatibility with the YubiKey Passkey Enabler.

2.4 WebAuthn/FIDO2 website support

Once you have a compatible Android device, security key, and WebAuthn-enabled browser, using the YubiKey Passkey Enabler to perform FIDO2 operations (such as registering or authenticating with a passkey) requires a WebAuthn-enabled website.

To verify whether a site supports WebAuthn, look for terms like “passkey”, “security key”, and “FIDO2”. For an example of a WebAuthn-enabled site, see passkey.org.


Passkey.org
DEMO
Try it out
Create a temporary username so we can register your passkey. You'll only need your passkey to sign in after creating an account.
Username
Sign up
OR
Sign in with passkey
Accounts will be deleted after 24 hours. By registering, you agree that your data will be treated in accordance with the Yubico Privacy Policy.

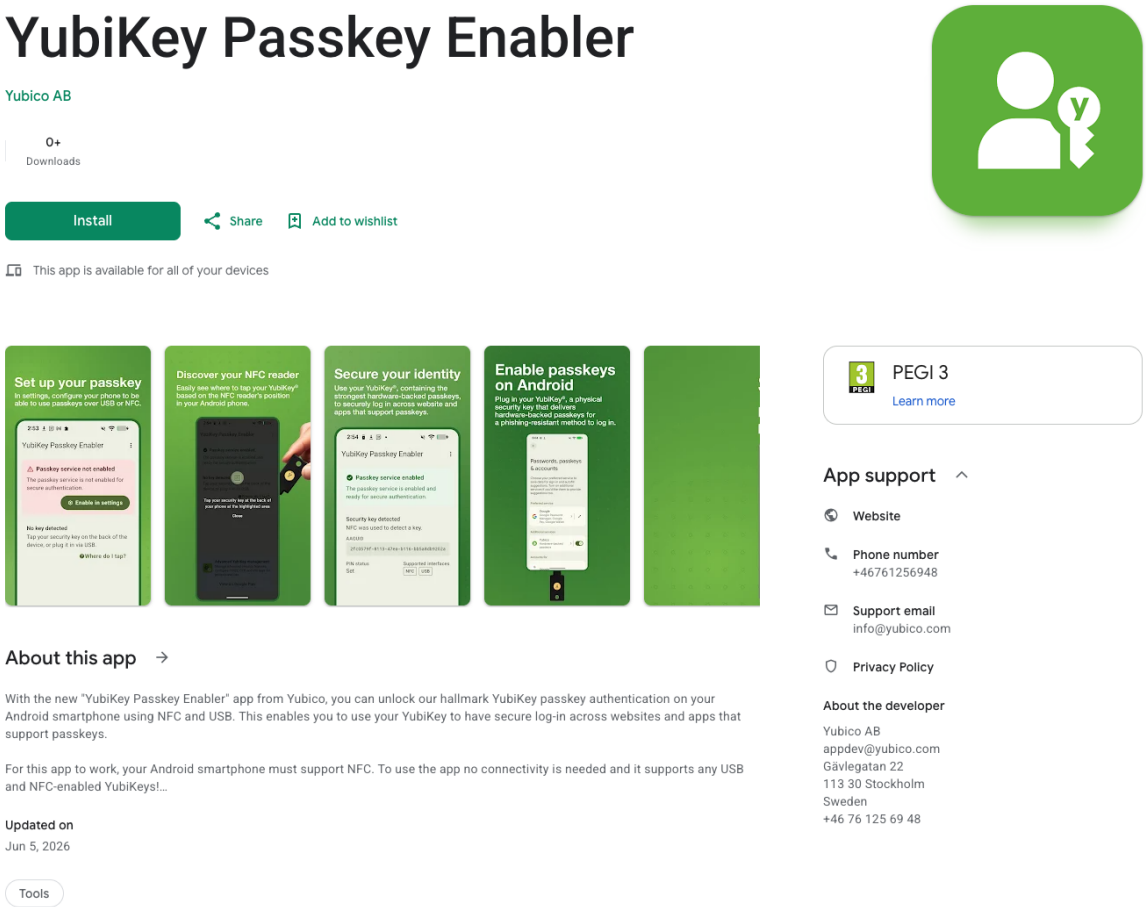
CHAPTER

THREE

INSTALLATION

The YubiKey Passkey Enabler can be installed via the Google Play Store.

On your Android device, go to the YubiKey Passkey Enabler page in the Google Play Store and click **Install**. Follow the prompts to complete installation.



3.1 Next steps

After installing the YubiKey Passkey Enabler, you must enable the app as a passkey provider service in your Android settings before it can be used in FIDO2 operations. See *Configuration* for guidance.

CHAPTER

FOUR

CONFIGURATION

After installing the YubiKey Passkey Enabler, your Android device must be configured before using the app. Configuration consists of the following:

- **Enabling the app as a passkey provider service (required)**

  This is a mandatory step that allows the YubiKey Passkey Enabler to be used to perform FIDO2 operations.

- **Ensuring that NFC connectivity is toggled on (recommended)**

  To use the YubiKey Passkey Enabler over NFC, NFC connectivity must be enabled on your Android device (if available). We recommend verifying the NFC connectivity status before use.

- **Changing the PIN entry requirement (optional)**

  If desired, you can configure the app to prompt for PIN entry *prior* to connecting your security key by toggling the **Always ask for PIN** setting in the YubiKey Passkey Enabler.

- **Adjusting your app colors (optional)**

  Don't like the colors in the YubiKey Passkey Enabler app? Toggle your Android device's theme and/or color scheme.

4.1 Enable the app as a passkey provider service in your Android settings

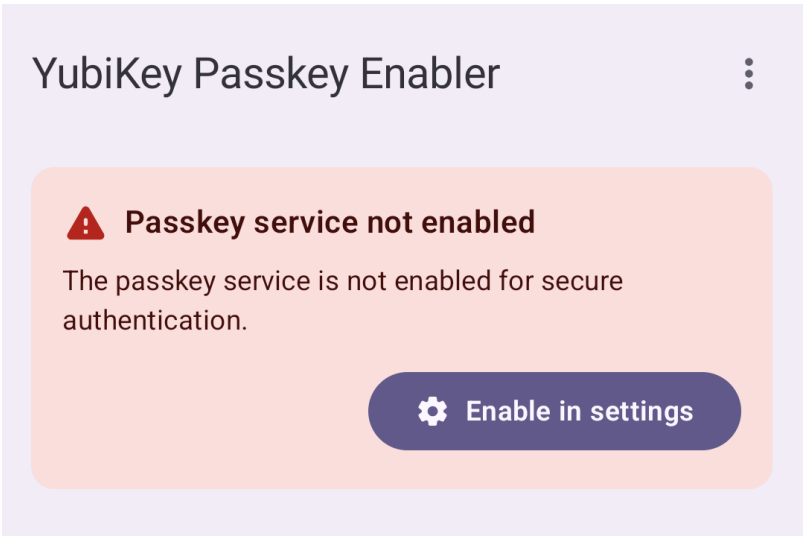
Before the YubiKey Passkey Enabler can be used to perform FIDO2 operations on your Android device, it must first be enabled as a passkey provider service in your Android settings. This allows the app to be used with Android's Credential Manager.

After configuring this setting, when you attempt to perform a FIDO operation (such as authentication), the YubiKey Passkey Enabler will appear on screen as a selectable option for interacting with your passkeys.

The YubiKey Passkey Enabler can be enabled as either the "preferred" service or an "additional service" in your Android passkey settings. When set as an additional service, you may be required to click through additional screens to select the YubiKey Passkey Enabler as the service to use during a FIDO2 operation.

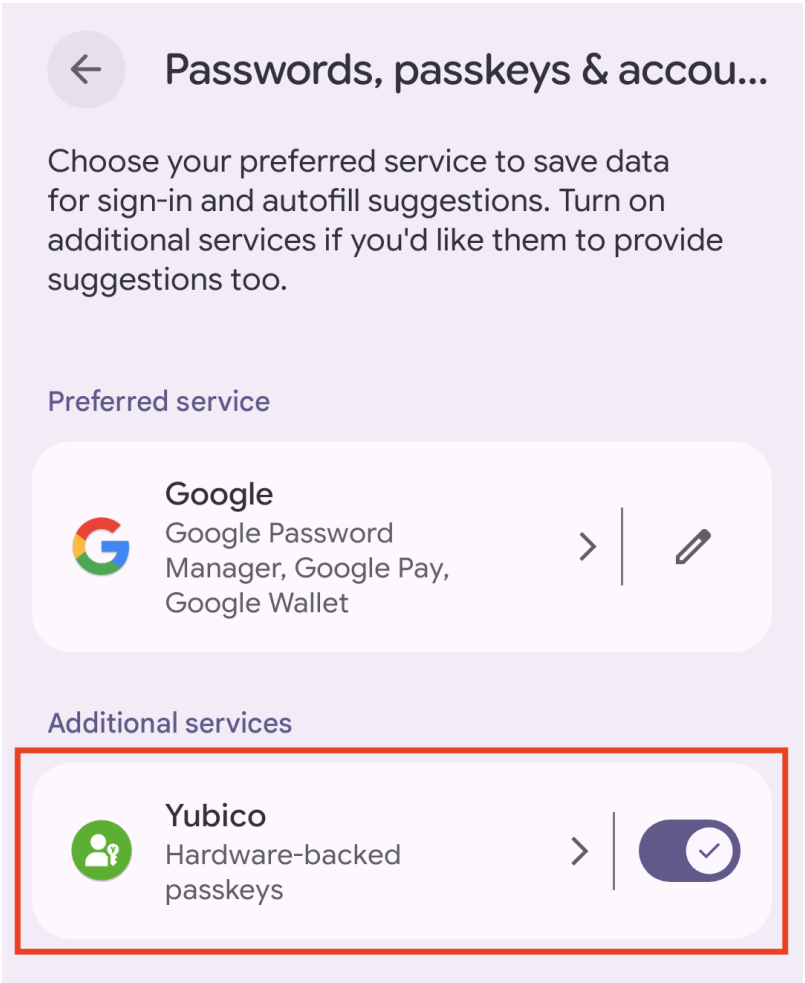
To configure your passkey provider service settings on your Android device, do the following:

1. Open the YubiKey Passkey Enabler and click **Enable in settings** on the app's home screen.

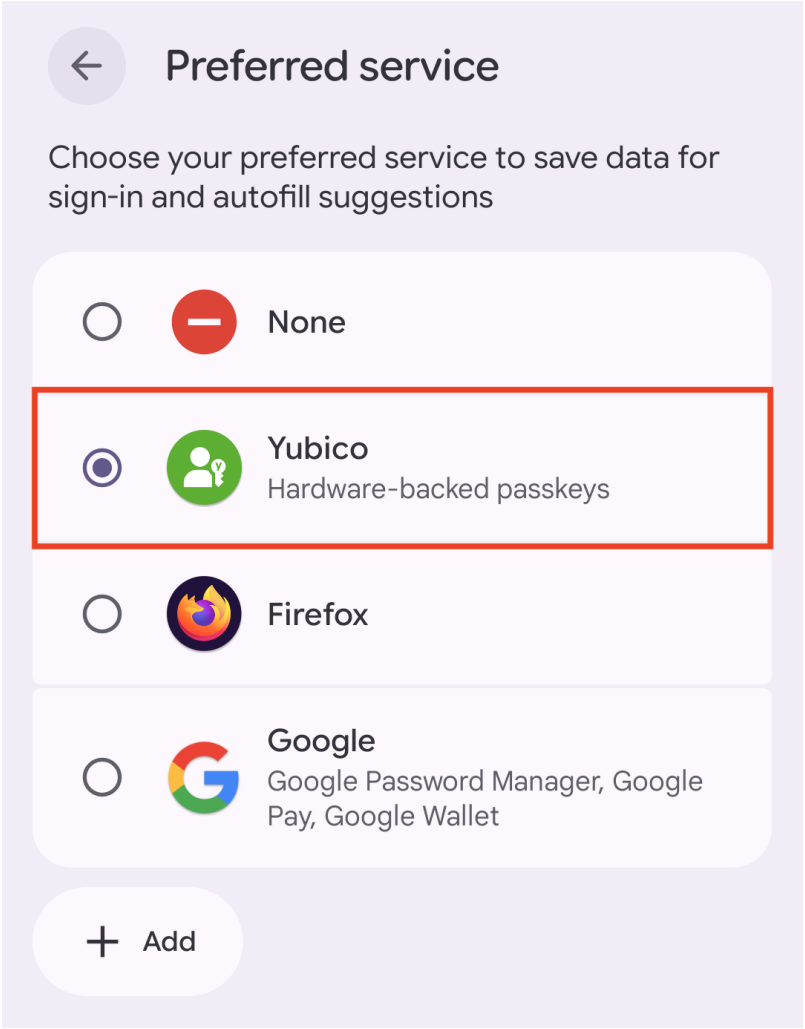


Alternatively, you can access these settings by clicking the menu icon in the upper right corner of the app and selecting **System Passkey Settings**.

2. To enable the app as an "additional service", move the toggle next to **Yubico** to the "on" position under the **Additional services** section.



To enable the app as the "preferred service", click the pencil icon next to the name of the current preferred service, and select **Yubico**.



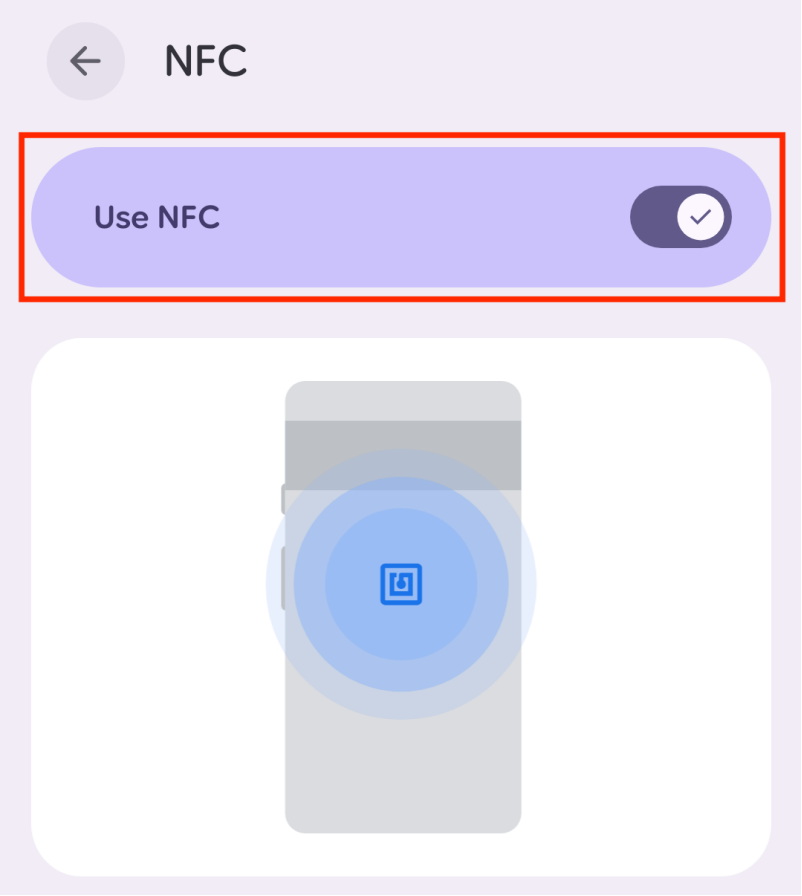
Note: If you set the YubiKey Passkey Enabler as the preferred service, you can always re-enable the previous preferred service (depending on your Android device, this is often Google Password Manager) as an additional service in your device settings.

3. Click the arrow icon in the upper left corner to return to the YubiKey Passkey Enabler home screen. If the app was successfully enabled as a passkey provider service, you will see a green **Passkey service enabled** message.

4.2 Toggle NFC connectivity

To use the YubiKey Passkey Enabler with an *NFC-enabled* Android device and security key, verify that NFC connectivity on your Android device is toggled on.

To do so, open the YubiKey Passkey Enabler app. If you see the "NFC is disabled on this device" message near the bottom of the screen, click the **Enable NFC** button to open your device's NFC settings. Toggle NFC connectivity to the "on" position and return to the YubiKey Passkey Enabler app. If the connectivity setting was correctly applied, the NFC message will have disappeared.



Alternatively, you can find your device's NFC connectivity settings by going to your device's main settings and searching "NFC".

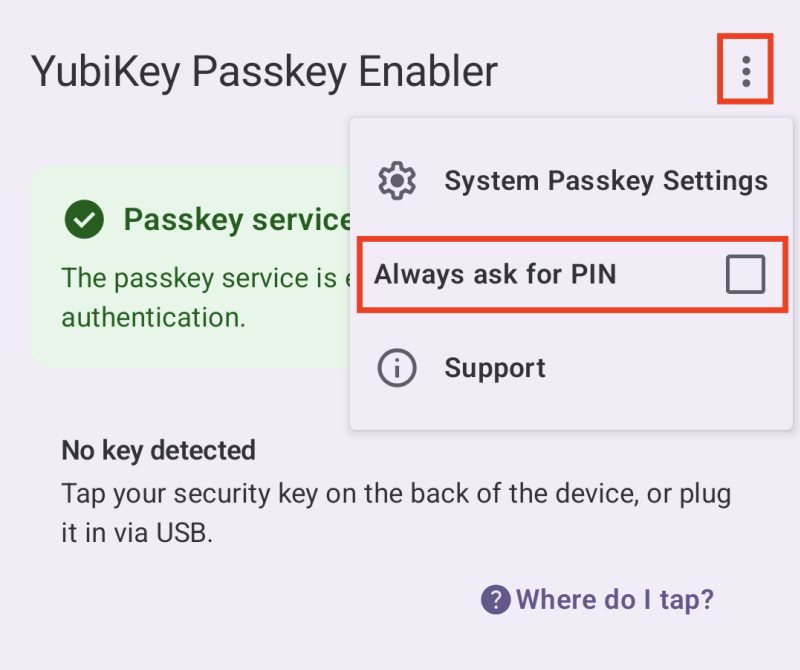
Tip: On Pixel phones, NFC settings can be found by going to **Settings > Connected devices > Connection preferences > NFC**.

4.3 Always ask for PIN

Always ask for PIN is an optional setting that is off by default. If the setting is enabled, the YubiKey Passkey Enabler app will prompt for the PIN *prior* to connecting your security key during a FIDO2 operation.

For NFC connections, this setting reduces the number of required NFC interactions by one, providing a faster passkey flow.

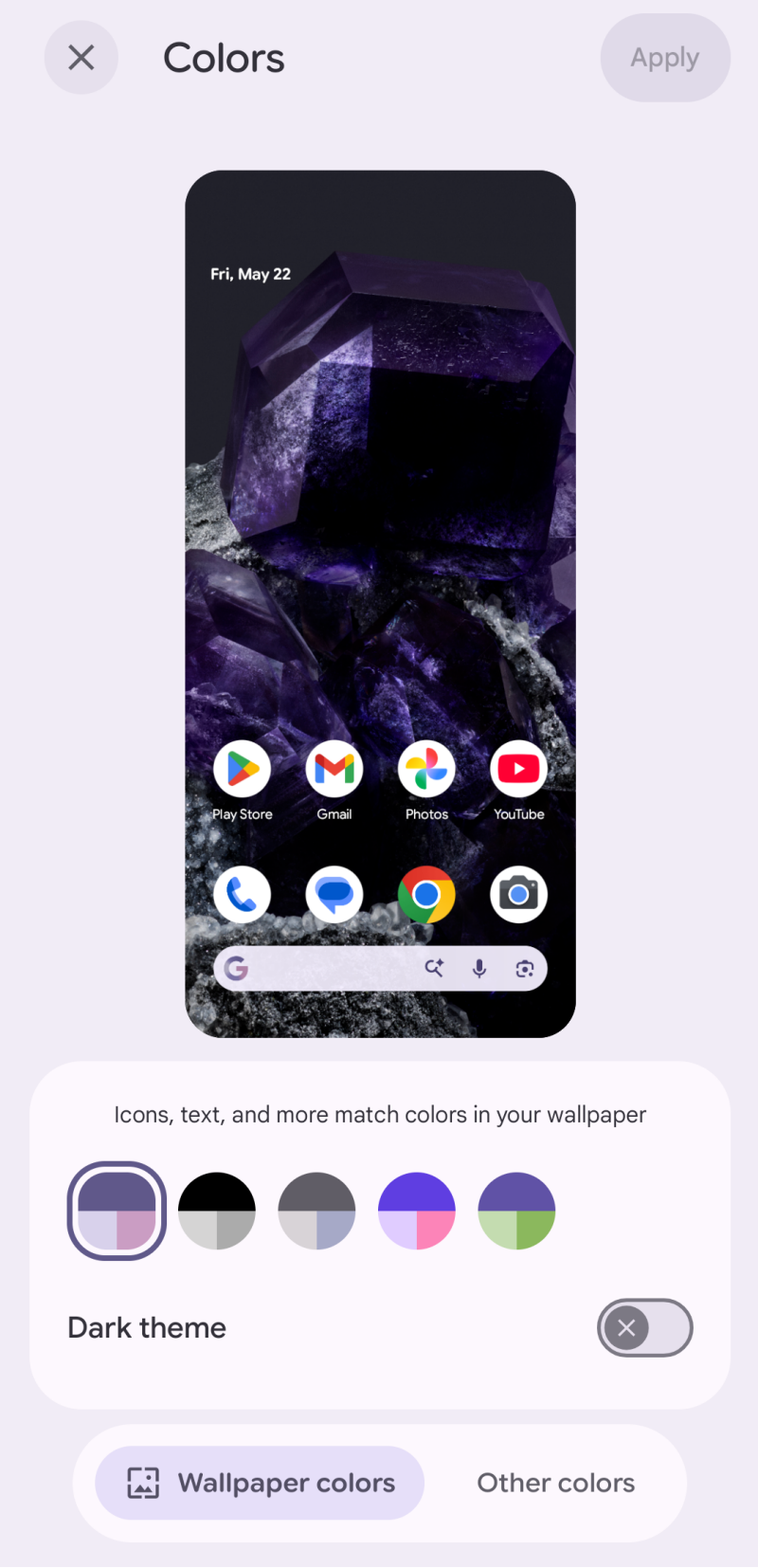
To enable or disable **Always ask for PIN**, click the menu icon in the upper right corner of the app and check (enable) or uncheck (disable) the box next to **Always ask for PIN**.



4.4 App colors

The colors used in the YubiKey Passkey Enabler are affected by two settings on your Android device: theme and color scheme. These settings are why the colors shown in screenshots in this user guide may differ from the colors observed in the app on your Android device.

Theme only has two options (light/dark), but several options are available for color scheme, which is typically part of the "Wallpaper & style" settings.



For information on changing your theme and color scheme, see the Android Help Center documentation.

CHAPTER

FIVE

USING THE YUBIKEY PASSKEY ENABLER APP

As a passkey provider service, the YubiKey Passkey Enabler acts as a helper app to facilitate various FIDO2 operations during passkey registration and authentication flows with your hardware security key.

For a general overview of what the YubiKey Passkey Enabler assists with in these flows, see *FIDO2 functionality support*.

And once you have correctly *configured* your Android device and are ready to use the app, see *Using the YubiKey Passkey Enabler during a passkey registration flow* and *Using the YubiKey Passkey Enabler during a passkey authentication flow* for a walkthrough.

5.1 FIDO2 functionality support

During passkey registration and authentication flows, the YubiKey Passkey Enabler will prompt for the following as needed:

- Connecting/tapping your security key
- PIN creation
- PIN change
- PIN entry
- Fingerprint entry (for security keys with fingerprint biometric capabilities only)
- Touch (user verification)

When creating or changing a PIN, the YubiKey Passkey Enabler will display PIN length and complexity requirements. If an incorrect PIN is entered (during a PIN change or standard PIN entry), the YubiKey Passkey Enabler will display the number of PIN retries remaining. Similarly, if fingerprint entry fails, the YubiKey Passkey Enabler will display the number of fingerprint retries remaining, and when retries have been exhausted, it will handle the PIN entry fallback.

5.2 Using the YubiKey Passkey Enabler during a passkey registration flow

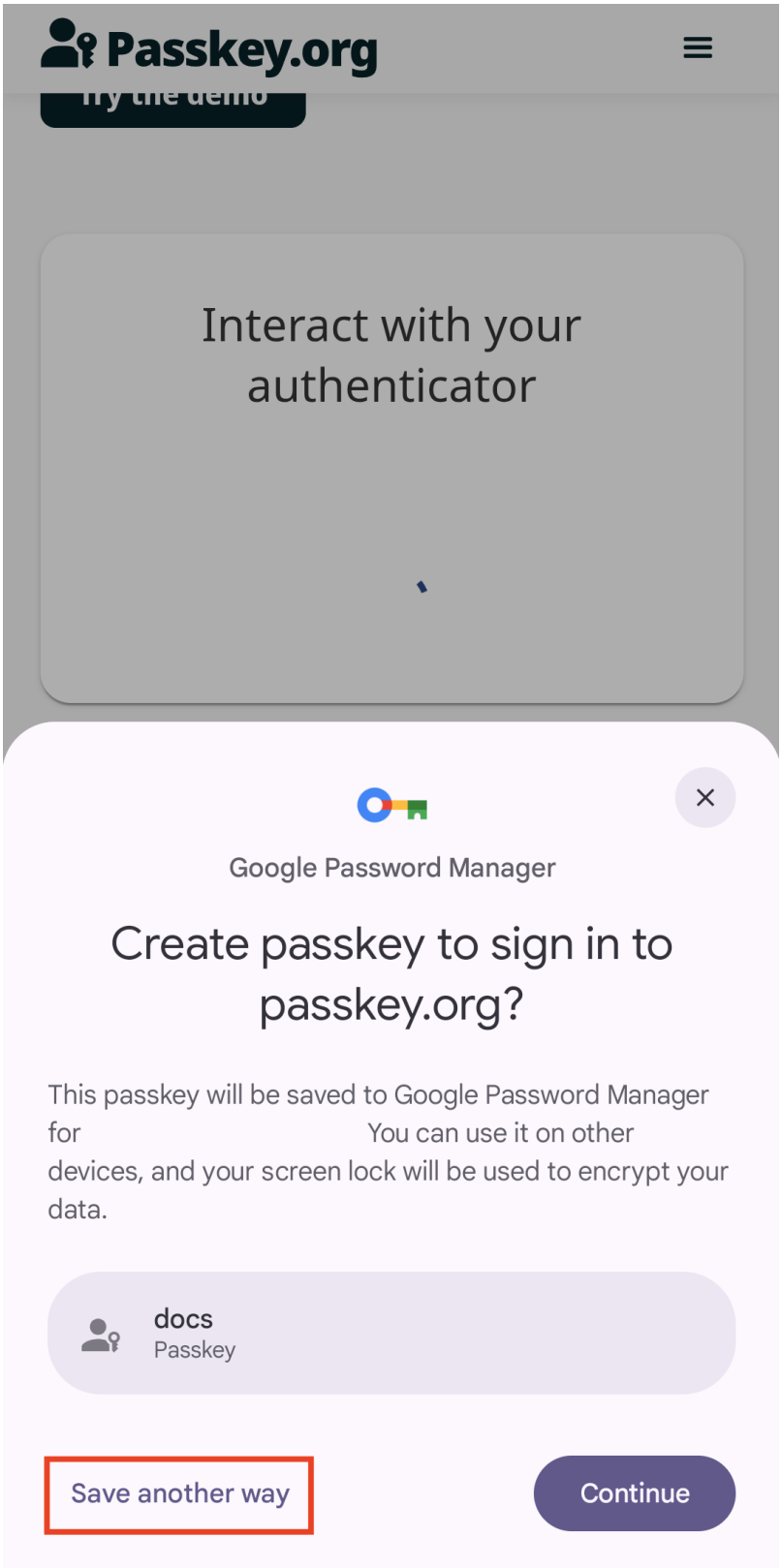
To register a passkey with your security key and the YubiKey Passkey Enabler, do the following:

1. On your Android device, navigate to the WebAuthn-enabled site or app you wish to create a passkey credential for. Make sure to use a *supported app or browser*.
2. Initiate the passkey creation process. This can occur through the creation of a new account or when registering a new passkey with an existing account. The location of these settings is different for every site/app, but look for

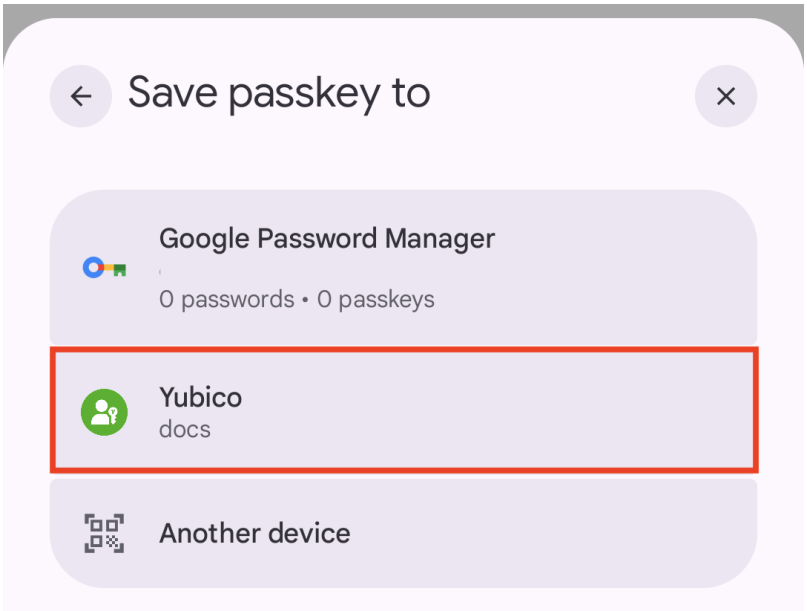
terms like “passkey”, “security key”, or “passwordless login” either during the account creation flow or in your account settings.

3. Once passkey creation has been initiated, you will see a window appear with Android’s Credential Manager at the bottom of your screen. From here, you will need to select how you want to save your passkey. Depending on how you configured your *Android passkey provider settings*, the YubiKey Passkey Enabler (shown as **Yubico** in the Credential Manager window) may be the default choice or it will need to be manually selected. If **Yubico** is the default option, click **Continue**.

   Otherwise, click **Save another way**.

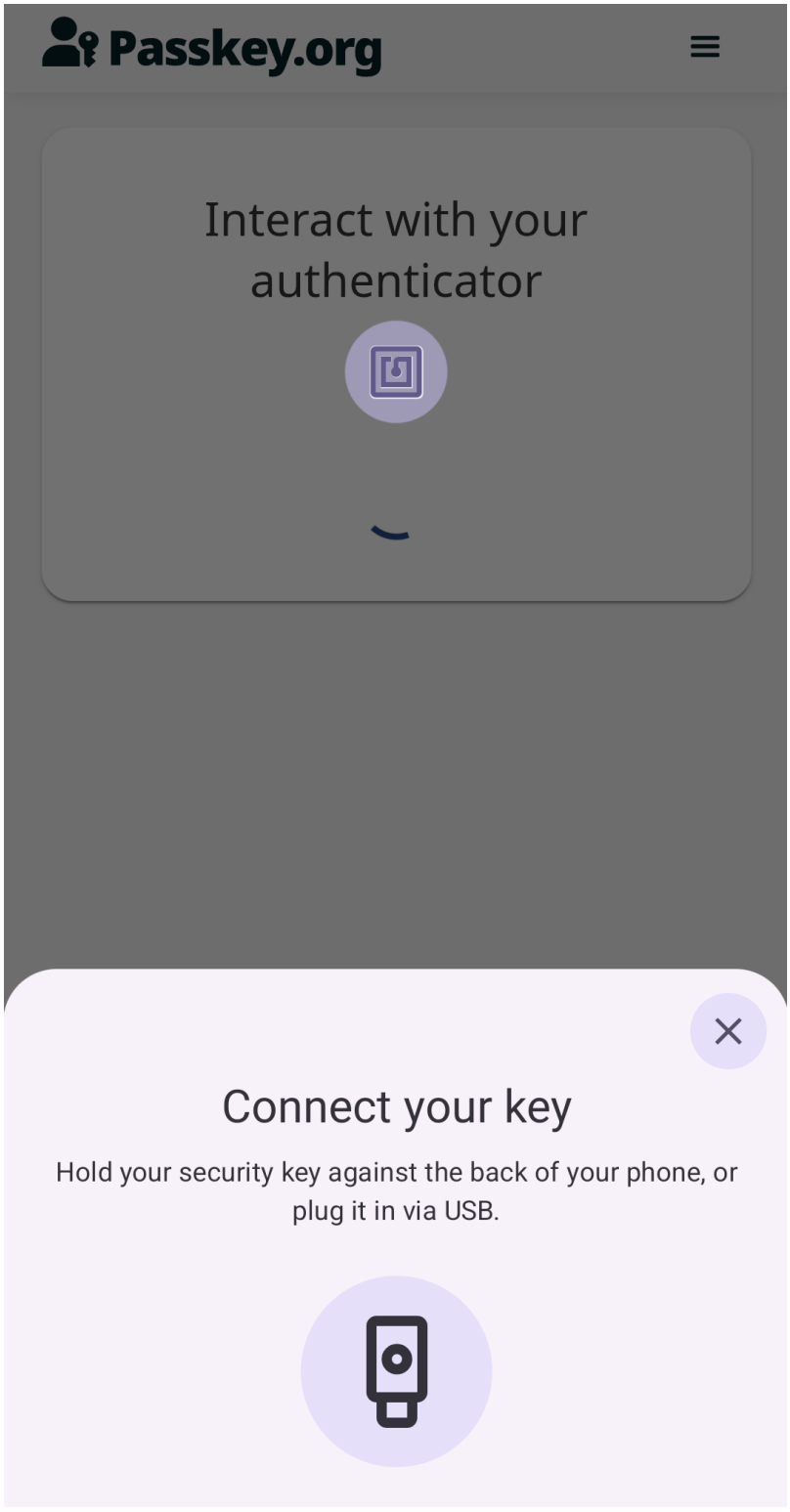


Next, select **Yubico** from the list of passkey providers, and then click **Continue**.



4. Next, you will be prompted to connect your security key. For USB connections, plug your security key into your Android device. For NFC connections, tap and hold your security key on the back of your device as close to the NFC antenna as possible.

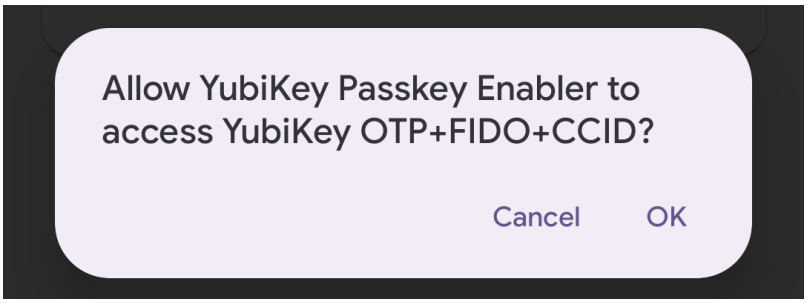
   If your device provides information about its NFC components to the app, an icon will appear on screen indicating the location of your Android device's NFC antenna.



If *Always ask for PIN* is enabled, the YubiKey Passkey Enabler app will prompt for the PIN prior to connecting your security key (see the next step).

Note: When connecting a YubiKey via USB, you may be asked to allow the app to communicate with your key.

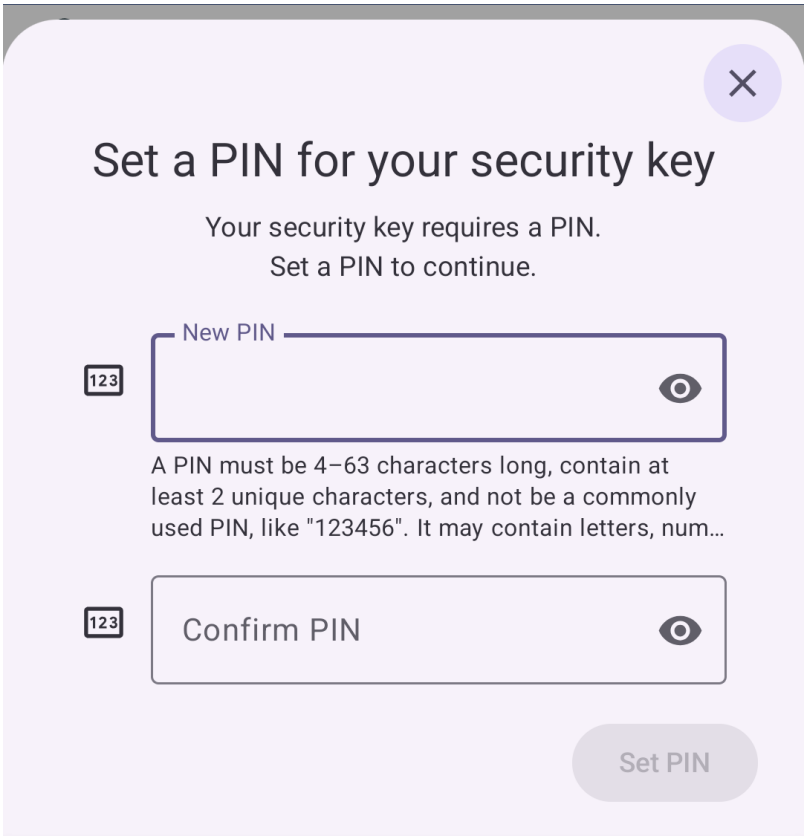
Click **OK** to continue.



5. Depending on the status of your FIDO2 PIN and the type of security key you have, do one of the following:
   a. If you do not have a PIN set on your security key, you will be asked to create one. On the **Set a PIN for your security key** screen, enter your new PIN twice and click **Set PIN**.

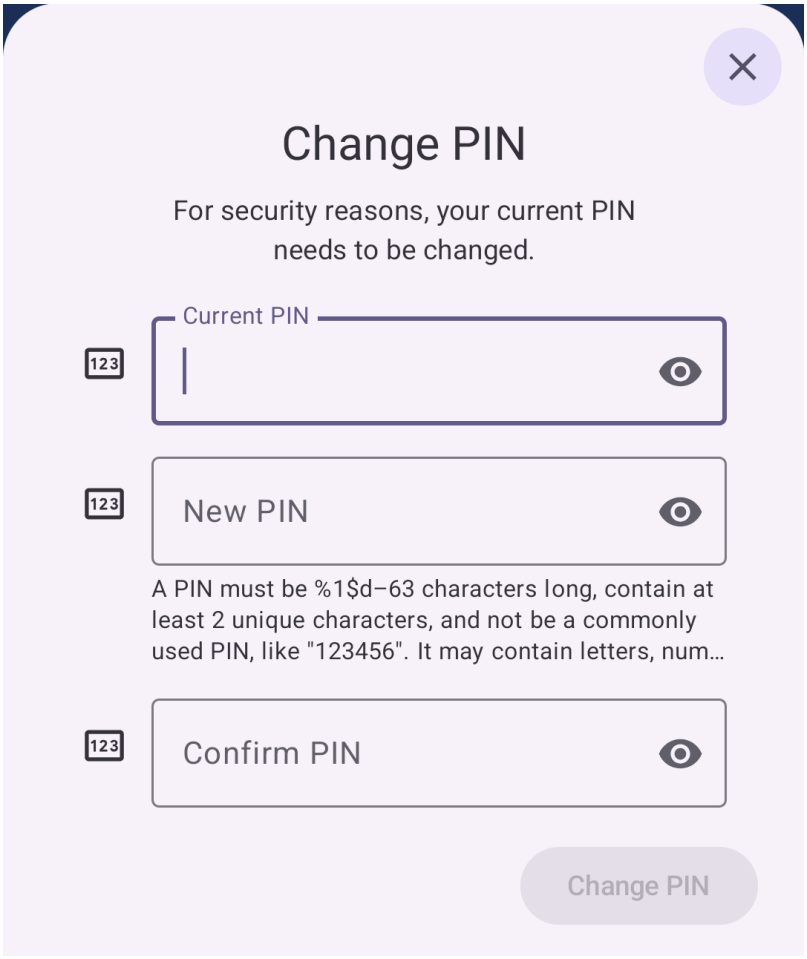
   Tip: PIN best practices:

   - When creating a new PIN, do not choose something that is easily forgotten. If you forget your PIN, the only way to change your PIN without needing to enter the current PIN is to reset your security key, which removes all passkey credentials.
   - To maintain the highest level of security for your accounts, do not share your PIN.



   b. If you already have a PIN, enter it when prompted and click **Confirm**.

c. If you already have a PIN but are being asked to set a new one, enter your current PIN followed by your new PIN and click **Change PIN**.



d. If you have a security key with fingerprint biometric capabilities and you have at least one fingerprint stored on your security key, use your fingerprint when prompted. If fingerprint entry fails, you will be asked to retry, and once your retries have been exhausted, you will be asked to enter your PIN as a fallback.

6. If you are registering the passkey via NFC, tap and hold your security key against your device again when prompted. If you are connected via USB, touch your security key if prompted. If the operation succeeds, passkey registration is complete.

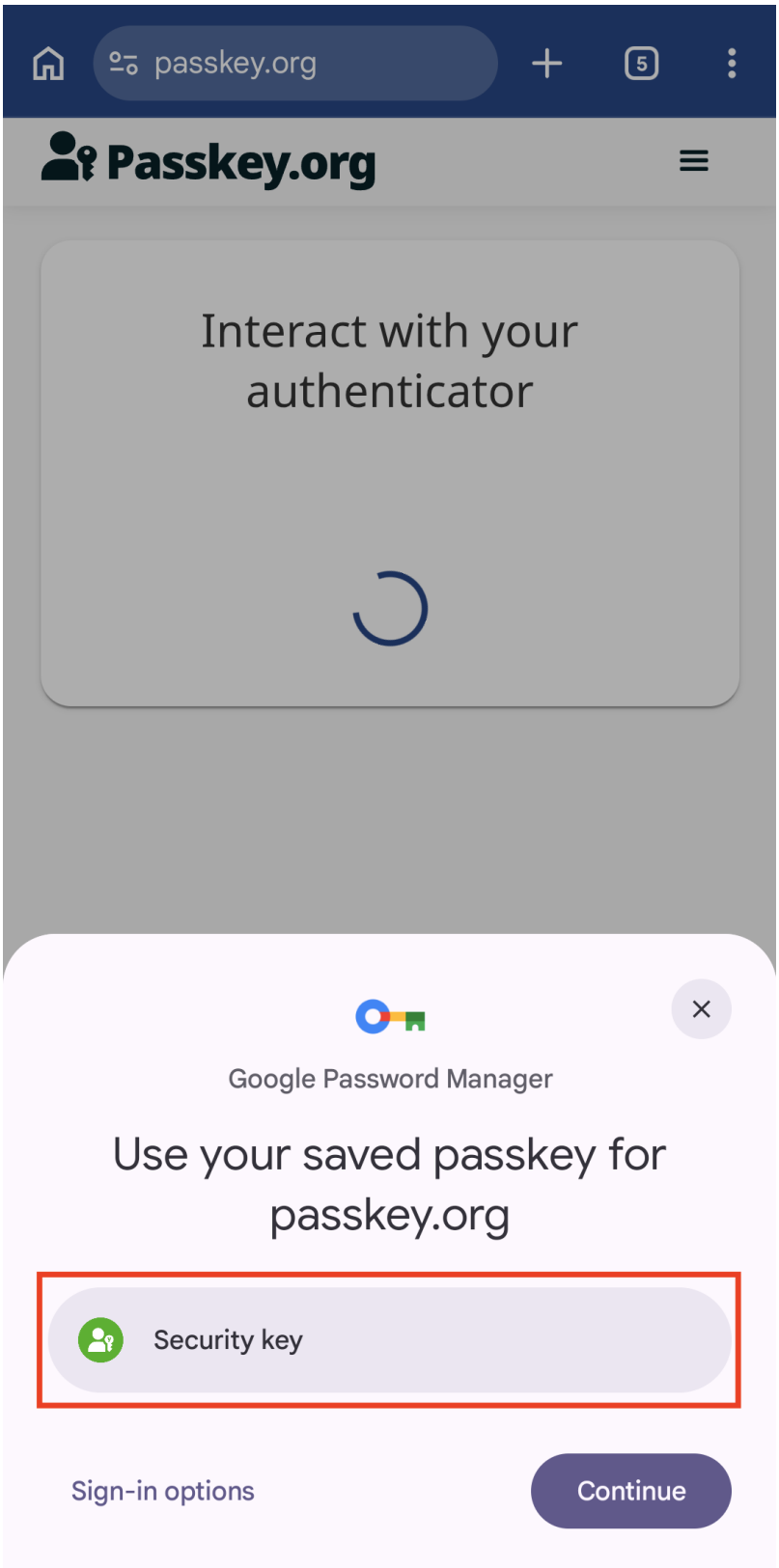
5.3 Using the YubiKey Passkey Enabler during a passkey authentication flow

To authenticate with a passkey stored on your security key with the YubiKey Passkey Enabler, do the following:

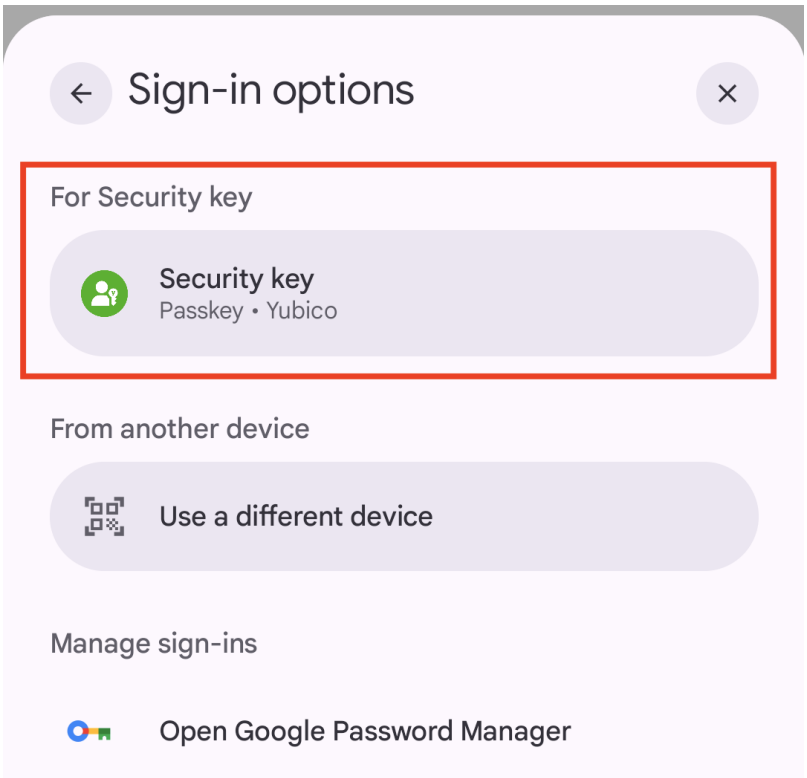
1. On your Android device, navigate to the WebAuthn-enabled site or app you wish to authenticate to. Make sure to use a *supported app or browser*.
2. Initiate the authentication process (i.e. log in to your account).
3. Once passkey authentication has been initiated, you will see a window appear with Android's Credential Manager at the bottom of your screen. From here, you will need to select the passkey you would like to use for authentica-

tion. To use a passkey stored on your security key, you will need to select the YubiKey Passkey Enabler as your passkey provider.

Depending on how you configured your *Android passkey provider settings*, the YubiKey Passkey Enabler (shown as **Yubico** and/or **Security key** with the app icon in the Credential Manager window) may be the default choice or it will need to be manually selected. If **Yubico / Security key** is the default option, select it to continue.



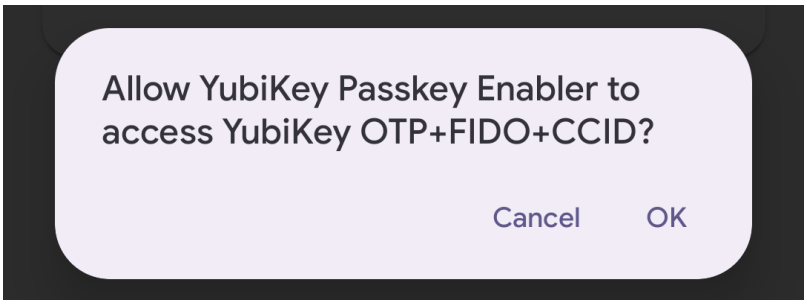
Otherwise, click **Sign-in options** and select **Yubico / Security key** from the list of passkey providers.



4. Next, you will be prompted to connect your security key. For USB connections, plug your security key into your Android device. For NFC connections, tap and hold your security key on the back of your device as close to the NFC antenna as possible.

   If your device provides information about its NFC components to the app, an icon will appear on screen indicating the location of your Android device's NFC antenna.

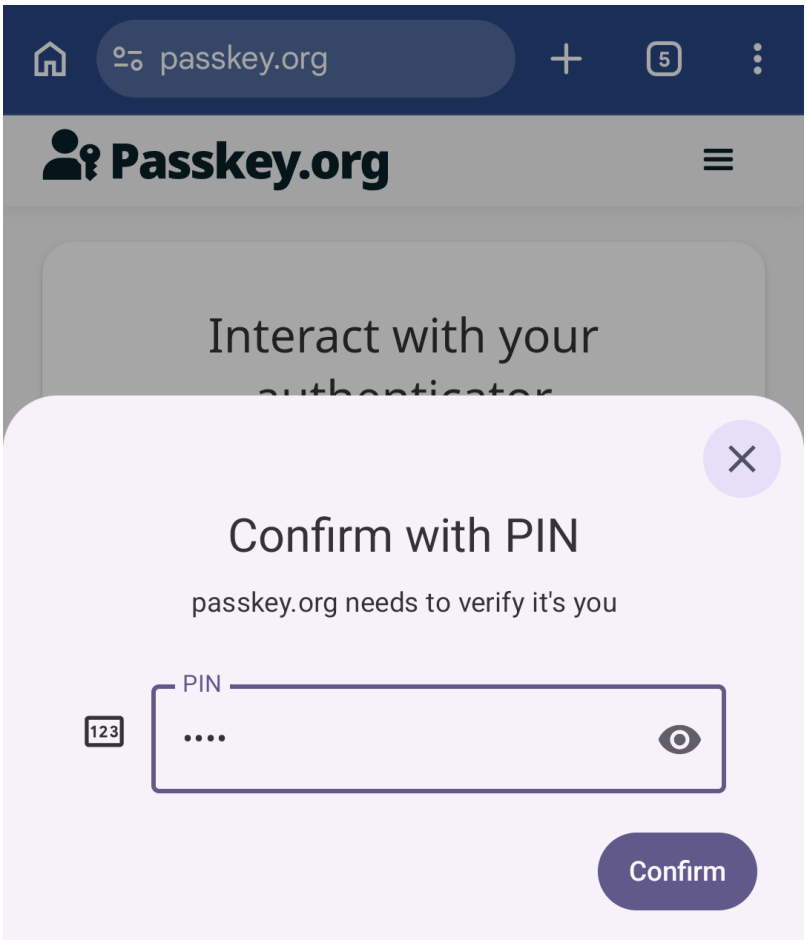
Note: When connecting a YubiKey via USB, you may be asked to allow the app to communicate with your key. Click **OK** to continue.



   If *Always ask for PIN* is enabled, the YubiKey Passkey Enabler app will prompt for the PIN prior to connecting your security key (see the next step).

5. Depending on the status of your FIDO2 PIN and the type of security key you have, do one of the following:

   a. If you have a PIN, enter it when prompted and click **Confirm**.



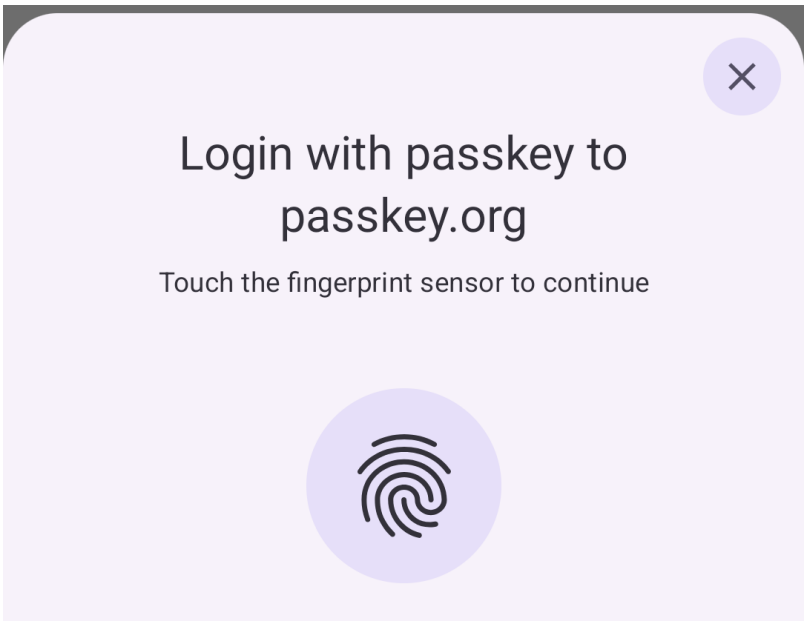
b. If you have a PIN but are being asked to set a new one, enter your current PIN followed by your new PIN and click **Change PIN**.

Tip: PIN best practices:

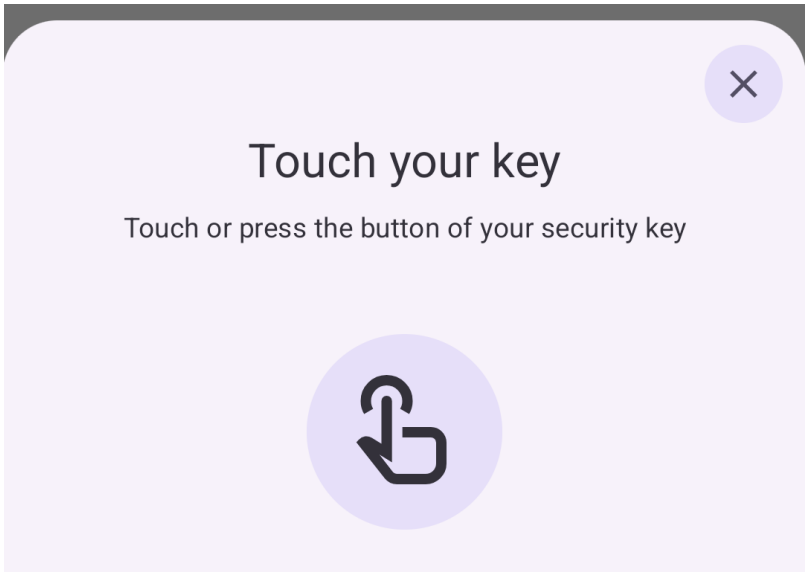
- When creating a new PIN, do not choose something that is easily forgotten. If you forget your PIN, the only way to change your PIN without needing to enter the current PIN is to reset your security key, which removes all passkey credentials.
- To maintain the highest level of security for your accounts, do not share your PIN.

---

c. If you have a security key with fingerprint biometric capabilities and you have at least one fingerprint stored on your security key, use your fingerprint when prompted. If fingerprint entry fails, you will be asked to retry, and once your retries have been exhausted, you will be asked to enter your PIN as a fallback.



6. If you are authenticating via NFC, tap and hold your security key against your device again when prompted. If you are connected via USB, touch your security key if prompted. If the operation succeeds, passkey authentication is complete.



CHAPTER

SIX

VIEWING DEVICE INFORMATION

In addition to assisting with passkey registration and authentication flows, the YubiKey Passkey Enabler app also has some helpful functionality on its home page for viewing *security key device information* and the location of your *Android device's NFC sensor*.

6.1 Viewing AAGUID, PIN status, and supported interfaces

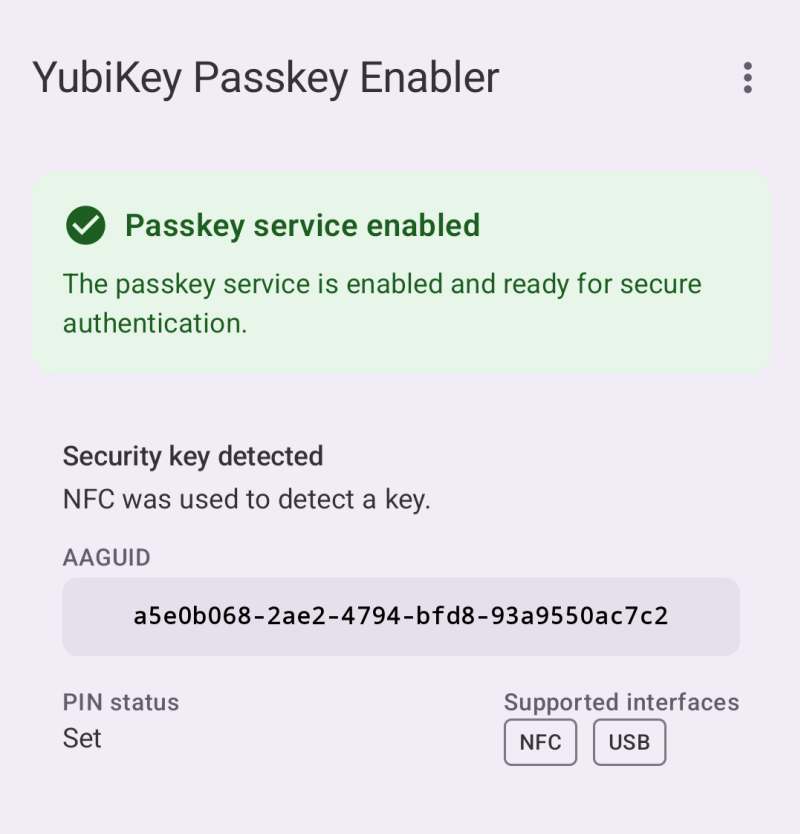
When you connect your security key via USB or scan via NFC, the home page of the YubiKey Passkey Enabler displays some helpful device information, including:

- AAGUID
- FIDO2 PIN status (Set, Not set)
- Supported interfaces (USB, NFC)

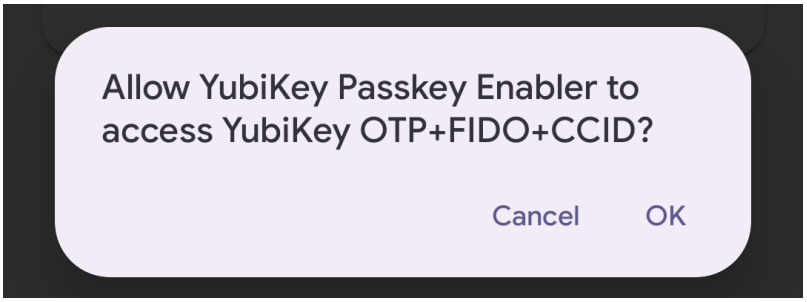
An AAGUID is a unique 128-bit identifier indicating your authenticator (security key) model. This information can be useful for debugging, as some relying parties restrict which authenticators can be used by AAGUID. For a list of YubiKey AAGUIDs and their corresponding models, see YubiKey hardware FIDO2 AAGUIDS.

If you do not have a FIDO2 PIN set on your security key yet, the YubiKey Passkey Enabler will guide you through the PIN creation process when registering your first passkey.

As for the interfaces information, this indicates which interfaces your security key is capable of communicating over, which is helpful for confirming that your security key is NFC-capable. Note that this does not indicate which interfaces are *enabled* on your security key. With the YubiKey, you can disable USB and/or NFC communication for the FIDO2 application. If you try to connect/scan your YubiKey over a disabled FIDO2 interface, you will not be able to view this device information in the YubiKey Passkey Enabler nor will you be able to perform any FIDO2 operations over that interface. Thankfully, enabling/disabling FIDO2 interfaces can be easily accomplished via the Yubico Authenticator app. See Toggle YubiKey applications on/off for more details.



Note: When connecting a YubiKey via USB, you may be asked to allow the app to communicate with your key. Click **OK** to continue.

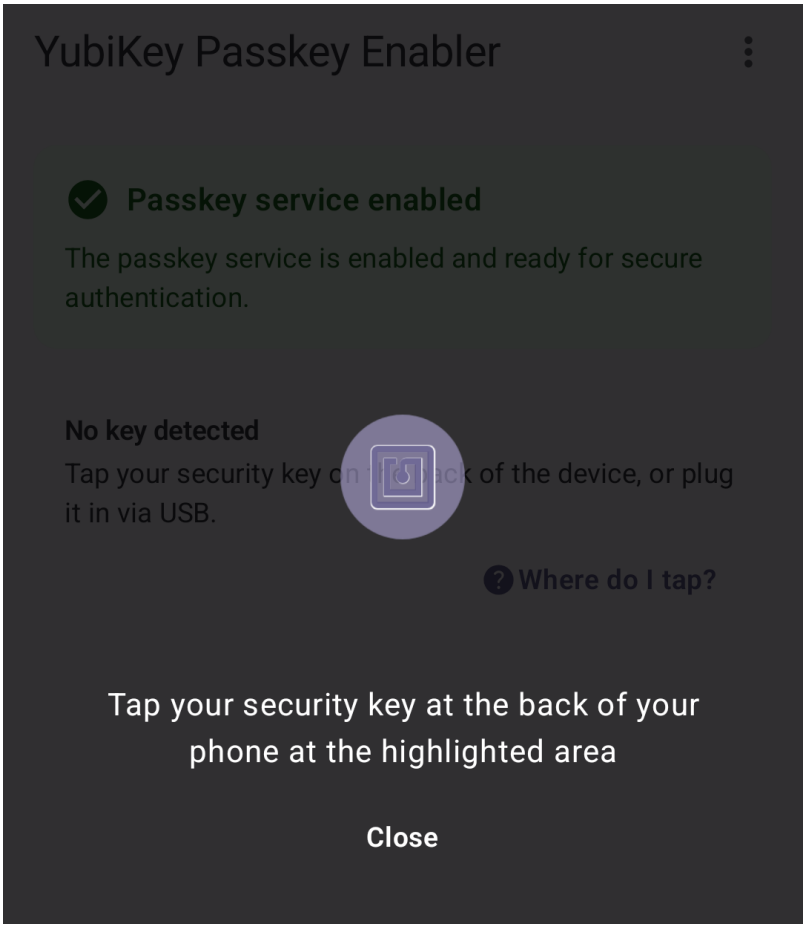


6.1.1 Yubico Authenticator

If you have a YubiKey and want to check additional device information, such as product name, serial number, firmware version, enabled/disabled interfaces, FIDO2 PIN retries remaining, and passkey credential details, we recommend using the Yubico Authenticator for Android application. You can download the app via the Google Play Store by following the link at the bottom of the YubiKey Passkey Enabler's home screen. For information on how to use Yubico Authenticator, see the Yubico Authenticator User Guide.

6.2 Locating your device's NFC sensor

Unsure of where to tap your security key on your Android device to scan via NFC? On the home screen of the YubiKey Passkey Enabler, click **Where do I tap?** If your Android device provides information about its NFC components to the app, an icon will appear on screen indicating the location of your device's NFC antenna. To effectively transfer data between your security key and your Android device during passkey registration and authentication, tap and hold your key as close to this location as possible.



If your Android device **does not** provide information about its NFC components to the app, you can still find the approximate location of the antenna during a FIDO2 operation by placing the security key against the back of the device and sliding it around until the app indicates that the operation has progressed to the next step.

CHAPTER

SEVEN

TROUBLESHOOTING

Running into issues with the YubiKey Passkey Enabler? Check this page for solutions to common problems.

7.1 FIDO2 registration or authentication fails

If passkey registration fails, it could be because you either have insufficient space on your security key, you already have a passkey for that account on your security key, or the relying party you are interacting with has restricted the use of your security key.

If you have a YubiKey, you can verify if storage space or an existing passkey is an issue by going to the **Passkeys** screen in the Yubico Authenticator for Android app. **Passkeys** allows you to view all passkeys on your YubiKey and check how much space remains for additional credentials. For information on downloading and installing Yubico Authenticator, see Download the App. For information on the **Passkeys** screen in Yubico Authenticator, see Viewing and deleting passkeys.

Note: YubiKeys with firmware version 5.7 and later can store up to 100 passkeys, but YubiKeys with firmware version 5.0 through 5.6 can only store up to 25 passkeys.

If the relying party, such as Microsoft Entra, has restricted the use of your security key (which is typically done via *AAGUID*), this may be indicated in the error message received when attempting passkey registration. The only workaround is to use a security key from the relying party's allow list.

If passkey authentication fails because you cannot get past the PIN entry screen despite entering the correct PIN, your PIN may be blocked. See *The PIN is blocked* for more information.

7.2 NFC scanning fails

If you are attempting to perform a FIDO2 operation via NFC, but the NFC scan won't initiate, it could be due to a few different issues:

- **Your security key is too far from the NFC antenna**

  The YubiKey Passkey Enabler will display a circular chip icon at the location of your device's NFC antenna. Touch your security key on the *back* of your device as close to this icon as possible.

- **NFC connectivity is disabled on your Android device or YubiKey**

  See *Toggle NFC connectivity* for information on how to check and turn on NFC connectivity on your Android device. To check if NFC is disabled for the FIDO2 application on your YubiKey and to re-enable it, you must use the Yubico Authenticator app. See Toggle YubiKey applications on/off for more details.

- **Your Android device and/or security key is not NFC-compatible**

  See *Platforms and Requirements* for more information on device and security key requirements.

If the NFC scan fails *after* initiation, you may be removing the security key from the sensor before the process has completed. Retry the operation and hold the key against your device until the YubiKey Passkey Enabler indicates that the operation is complete.

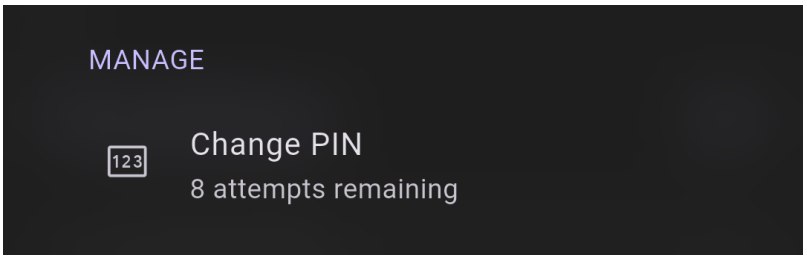
7.3 The PIN is blocked

With FIDO2-compatible YubiKeys, you have a total of 8 attempts to enter the PIN correctly during a FIDO2 operation. Once you have exhausted these attempts, the FIDO2 application on your YubiKey becomes blocked, and you will not be able to perform any FIDO2 operations until your YubiKey's FIDO2 application is reset.

A FIDO2 reset removes the PIN and all FIDO2 credentials on your YubiKey, meaning that you will no longer be able to authenticate to any website for which you had registered your YubiKey as a passkey. (For this reason, Yubico recommends registering a backup YubiKey to maintain account access.) Once your YubiKey is reset, you will be able to re-register it with your accounts (as long as you can access them via a backup YubiKey or other recovery method).

To reset the FIDO2 application on your YubiKey, we recommend using Yubico Authenticator for Android. For information on downloading and installing Yubico Authenticator, see Download the App. For instructions on performing a FIDO2 application reset with the Yubico Authenticator app, see Factory reset.

Note: Once the FIDO2 PIN is entered correctly during an operation, the PIN retry count resets to 8. You can check the number of PIN retries remaining on your YubiKey via Yubico Authenticator. To do so, open the app and navigate to the **Passkeys** or **Fingerprints** screens. You will find the retry count next to the **Change PIN** action under **MANAGE**, which can be navigated to via the menu icon in the upper right corner of the app.



7.4 I'm not getting prompted for biometrics (fingerprint) during authentication

If you are attempting to perform FIDO2 authentication with a YubiKey Bio Series key and you are not being prompted to use your fingerprint, this may be because you do not have any fingerprints stored on your YubiKey. While the YubiKey Passkey Enabler can facilitate biometric authentication, it cannot handle the process of adding new fingerprints to your YubiKey.

To add a fingerprint to your YubiKey, we recommend using Yubico Authenticator for Android. For information on downloading and installing Yubico Authenticator, see Download the App. For instructions on adding a fingerprint to your YubiKey with the Yubico Authenticator app, see Registering and managing fingerprints.

7.5 I do not see the option to select the YubiKey Passkey Enabler during a FIDO2 operation

If you do not see the YubiKey Passkey Enabler as a selectable option in the Android Credential Manager window during a FIDO2 operation (it will be listed as **Yubico**), you may not have enabled the app as a passkey provider service yet. See *Enable the app as a passkey provider service in your Android settings* for more information on what this setting is and how to configure it.

7.6 Getting additional help

Can't find a solution to your issue? Submit a help request to Yubico's Customer Support team.

7.7 Collecting application logs

While troubleshooting an issue with Yubico's support or development teams, you may be asked to collect and submit application logs. If an action within the app is failing, logs collected while performing that action can provide helpful diagnostic information.

Log collection begins as soon as the app is started. If the log level is changed while the app is running, the logs collected from that point onward will be at the new level.

Logs can be copied to the clipboard from within the app. There is a fixed size buffer for the "Copy to Clipboard" button in the app, so if the log is longer than 1000 lines, only the latest 1000 will be included.

7.7.1 Log levels

The log levels include ERROR, WARN, INFO, DEBUG, and TRACE, in order of increasing verbosity. The default level is INFO. In general, the following information is collected for each log level:

- ERROR - Any error that occurred, which is often an action that could not be performed.
- WARN - Something failed, but the app was able to recover and complete the action, or the failure didn't impact the action.
- INFO - What the app is doing without specific details. For example, a credential was added, etc.
- DEBUG - More detailed information about actions performed. This can include things like the name of an account and the method with which the account was added. Some information at this level might be considered sensitive identifiable data (usernames, YubiKey serial numbers, etc).
- TRACE - Even more detailed than DEBUG and INFO. It includes ALL raw traffic to/from the security key. This includes things like origin URLs and credential IDs.

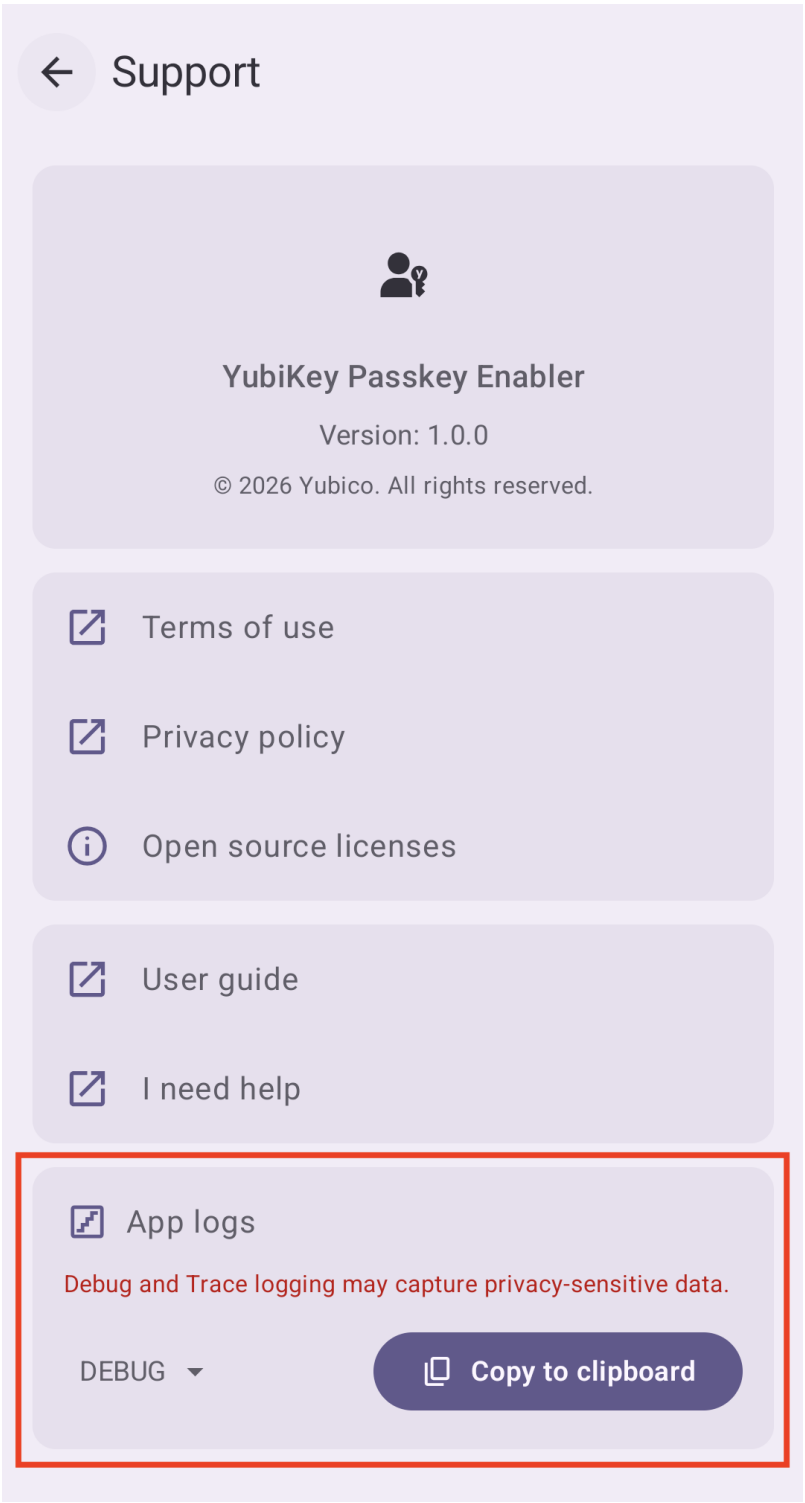
Be very cautious when sharing logs containing DEBUG and TRACE data given that they may contain sensitive information.

7.7.2 Generating logs within the app

To generate log data, do the following:

1. Open the YubiKey Passkey Enabler app, click on the menu icon in the upper right corner of the app, and select **Support**.
2. Select the appropriate log level from the drop-down menu in the **App logs** section.
3. If there is a particular operation you want to collect logs on, such as passkey authentication in a browser, perform that operation. Now go back to **Support** and click the **Copy to Clipboard** button. Paste the log information into a text file, email, or other relevant file/location and save it.

Important: Once you click **Copy to Clipboard**, the log buffer (which contains the logs you just copied) will be removed, and the log level will be reverted back to INFO. Make sure to save your logs before overwriting your clipboard.


Support
YubiKey Passkey Enabler
Version: 1.0.0
© 2026 Yubico. All rights reserved.
Terms of use
Privacy policy
Open source licenses
User guide
I need help
App logs
Debug and Trace logging may capture privacy-sensitive data.
DEBUG
Copy to clipboard

CHAPTER

EIGHT

RELEASE NOTES

8.1 2026

8.1.1 1.0.0 (22 June 2026)

YubiKey Passkey Enabler 1.0.0 is the application's initial release. It provides the following functionality:

- seamless integration with Android's Credential Manager as a passkey provider service
- communication with security keys over USB and NFC connections
- PIN creation, change, and entry during FIDO2 flows
- fingerprint biometric entry and PIN fallback during FIDO2 flows
- user interaction prompts (connecting, tapping, and touching the security key)
- device information on the app's home screen (including AAGUID, PIN status, and supported interfaces)
- on-screen icon showing the location of your Android device's NFC antenna

CHAPTER

NINE

COPYRIGHT

9.1 Trademarks

Yubico and YubiKey are registered trademarks of Yubico AB. All other trademarks are the property of their respective owners.

9.2 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.

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.

9.3 Contact Information

Yubico AB
Gävlegatan 22
113 30 Stockholm
Sweden

More options for getting touch with us are available on the Contact page of Yubico's website.

9.4 Document Updated

2026-06-22 16:12:18 UTC