Yubico Authenticator User Guide

Yubico

Jun 11, 2025

CONTENTS

1 Yubico Authenticator Overview **1**

1.1 Highlighted features . . . 1

1.2 Advantages . . . 2

1.3 Command line interface (CLI) tool . . . 3

2 Platforms and Requirements **5**

2.1 YubiKey compatibility . . . 5

2.2 Supported platforms . . . 6

2.3 WebAuthn browser support . . . 6

3 Download the App **7**

3.1 Previous releases . . . 8

3.2 Developers . . . 8

4 Install the App **9**

4.1 macOS . . . 9

4.2 Windows . . . 12

4.3 Linux . . . 12

4.4 Android . . . 13

4.5 iOS and iPadOS . . . 15

4.6 Developers . . . 16

5 Home and Settings **17**

5.1 The Home page: YubiKey at a glance . . . 17

5.2 Switching between keys . . . 20

5.3 Change a YubiKey's label and color . . . 21

5.4 Toggle YubiKey applications on/off . . . 22

5.5 Change the Authenticator theme . . . 23

5.6 Load a custom icon pack . . . 24

5.7 Change the application language . . . 25

5.8 Show/hide NFC smart card readers . . . 25

5.9 Android settings . . . 27

5.10 iOS/iPadOS settings . . . 29

6 Accounts: OATH **35**

6.1 What is OATH authentication? . . . 35

6.2 Adding a new account . . . 36

6.3 Authenticating with OATH and Yubico Authenticator . . . 42

6.4 Password protection . . . 44

6.5 Pinning an account . . . 51

6.6 Renaming an account . . . 52

6.7 Deleting an account . . . 53
6.8 Custom icons . . . 54

7 Passkeys: FIDO2 55
7.1 Creating and managing the FIDO2 PIN . . . 55
7.2 Viewing and deleting passkeys . . . 61
7.3 Enterprise Attestation . . . 63
7.4 Custom icons . . . 64

8 Fingerprints: FIDO2 65
8.1 Creating and managing the FIDO2 PIN . . . 65
8.2 Registering and managing fingerprints . . . 68

9 Certificates: PIV 73
9.1 Managing the PIN, PUK, and Management Key . . . 73
9.2 Add and manage certificates . . . 80

10 Slots: Yubico OTP Application 83
10.1 Yubico OTPs . . . 83
10.2 Static passwords . . . 86
10.3 Challenge-response . . . 87
10.4 OATH HOTPs . . . 88
10.5 Performing authentication with OTP application slot credentials . . . 89
10.6 Managing slots . . . 94

11 Factory Reset 97
11.1 What happens during a reset? . . . 97
11.2 How does a reset affect my accounts? . . . 97
11.3 Recommended preparation . . . 98
11.4 Performing a reset on desktop and Android . . . 98
11.5 Performing a reset on iOS/iPadOS . . . 99

12 Tips 101
12.1 Resize the app window . . . 101
12.2 Change the Accounts and Passkeys screen layouts . . . 104
12.3 Register a spare YubiKey . . . 107
12.4 Start Yubico Authenticator with the app window hidden . . . 110
12.5 Generate OATH OTPs from pinned accounts via the menu bar or system tray . . . 110
12.6 Set an OATH application password . . . 111
12.7 Keyboard shortcuts . . . 112
12.8 Works with YubiKey Catalog . . . 113

13 Troubleshooting and Support 115
13.1 Accounts: OATH . . . 115
13.2 Certificates: PIV . . . 116
13.3 Slots: Yubico OTP . . . 117
13.4 Android . . . 117
13.5 NFC wireless connections . . . 118
13.6 Reporting issues and submitting feature requests . . . 119
13.7 Getting additional help . . . 119
13.8 Generating and collecting diagnostic data and logs . . . 119

14 Azure MFA with Yubico Authenticator 123
14.1 Self registration (recommended method) . . . 123
14.2 Administrator registration (alternative method) . . . 127

14.3 Use a YubiKey to sign in . . . 131
14.4 Troubleshooting . . . 131
14.5 Additional information . . . 132

15 Smart Card on iOS 133
15.1 X.509 Certificates . . . 134
15.2 Prerequisites . . . 134
15.3 Overview: Setup Process . . . 134
15.4 Troubleshooting . . . 137

16 Import Smart Card Certificates onto your YubiKey 139
16.1 YubiKey Manager GUI . . . 139
16.2 YubiKey Manager CLI . . . 143
16.3 Next Steps . . . 144

17 Smart Card Certificate Provisioning 145
17.1 Provision Your Public Certificate . . . 145
17.2 Next Steps . . . 148

18 Authenticating with Smart Card on iOS 149
18.1 Authenticate to a Website on Safari . . . 149

19 Smart Card on iOS Troubleshooting 153
19.1 Web Browser Does Not Trigger the Yubico Authenticator Application . . . 153

20 Release Notes 157
20.1 2025 . . . 157
20.2 2024 . . . 160

21 Copyright 165
21.1 Trademarks . . . 165
21.2 Disclaimer . . . 165
21.3 Contact Information . . . 165
21.4 Document Updated . . . 166

CHAPTER

ONE

YUBICO AUTHENTICATOR OVERVIEW

Yubico Authenticator is a software application that allows you to get the most out of your YubiKeys and their hardware-backed security capabilities. At a high level, the app provides an intuitive and easy-to-use interface for interacting with your keys, enabling you to:

- Generate codes for two-factor authentication (OATH TOTP/HOTP).
- Manage credentials and accounts across several YubiKey applications and security protocols, including FIDO2 passkeys, PIV certificates, OATH accounts, and Yubico OTPs.
- Authenticate to websites using smart card TLS in the Safari browser (iOS/iPadOS only).

Yubico Authenticator is broadly supported across Windows, macOS, Linux, Android, and iOS/iPadOS devices and works over USB, Lightning, and wireless NFC connections.

Note: For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

1.1 Highlighted features

OATH

- *Add OATH account credentials to your YubiKey via QR code or manual entry*.
- *Generate and display OATH OTPs from accounts on your YubiKey*.
- *Protect the OATH application with a password*.
- *Rename and delete OATH accounts*.

FIDO2

- *Manage passkeys stored on your YubiKeys*.
- *Create and manage a FIDO2 pin*.
- *Register and manage fingerprints on YubiKey Bio Series keys for biometric authentication*.

PIV

- *Load PIV certificates onto your YubiKeys*.
- *Change the PIV application PIN, PUK, and Management Key*.
- *Authenticate to websites with the Smart Card on iOS feature*.

Yubico OTP

- *Configure a Yubico OTP application slot with a Yubico OTP, challenge-response, OATH HOTP, or static password credential*.
- *Delete or swap slot configurations*.

Miscellaneous

- *Toggle individual YubiKey applications on/off over physical and NFC connections*.
- *Perform a factory reset of an individual YubiKey application*.
- *Change a YubiKey's label and color in the app*.
- *Toggle between multiple connected keys in the app*.
- *Change the app's theme*.

1.2 Advantages

With other authenticator apps, credentials (the secret keys associated with your accounts) are often stored in the app, phone, or computer. However, desktop and mobile devices can be compromised, stolen, or lost, which puts the security of your accounts at risk.

With Yubico Authenticator, credentials are stored in the secure element of the YubiKey; once stored, they cannot be extracted.

In addition to improving account security, if you lose or change your device, you will not be locked out of your accounts. Simply download Yubico Authenticator onto a new device and connect your YubiKey; OTP codes can be generated and credentials can be managed just as before.

Stronger hardware-backed security

Storing your credentials on a hardware security key is safer than storing them on a mobile phone. Your credentials cannot be extracted from the secure element of the YubiKey.

Portable credentials across devices

Once credentials have been configured on a YubiKey, you can use your key with any device running the Yubico Authenticator app, no additional setup required.

Cross-platform coverage

The Yubico Authenticator app works across Windows, macOS, Linux, iOS/iPadOS, and Android devices.

Self-service reduces IT costs

With other authenticator apps, when a user has a new phone or OS upgrade, IT often needs to help reset the enrollment flow, and support calls rack up costs. Yubico Authenticator allows users to self-enroll, making this a secure, efficient solution at scale.

1.3 Command line interface (CLI) tool

Looking for a CLI tool with similar capabilities? Check out the YubiKey Manager CLI tool.

CHAPTER

TWO

PLATFORMS AND REQUIREMENTS

Yubico Authenticator is developed for both desktop and mobile platforms and designed to work with USB, Lightning, and NFC-enabled YubiKeys.

However, not every Authenticator feature is supported on every platform. Similarly, not every Authenticator feature is supported for every YubiKey model. For example, the iOS/iPadOS versions of the app only support some FIDO2 features (regardless of YubiKey used), and Bio Series YubiKeys do not support any OATH features (regardless of app platform).

Compatibility between YubiKey interface (USB, NFC, Lightning) and platform is also device-dependent. For example, USB-C is currently not supported on iOS/iPadOS, and not all Android devices have a built-in NFC reader.

For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

2.1 YubiKey compatibility

Broadly speaking, YubiKeys from the following series are compatible with Yubico Authenticator:

- YubiKey Bio Series FIDO Edition
- YubiKey Bio Series Multi-protocol Edition
- YubiKey 5 Series
- YubiKey 5 FIPS Series
- YubiKey 5 CSPN Series
- Security Key Series
- YubiKey 4 Series
- YubiKey NEO

Note: For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

2.2 Supported platforms

Fully Supported - the platform versions that Yubico builds and tests on and commits to supporting.

Best Effort - the app is expected to work, but development is supported through community testing and full functionality cannot be guaranteed.

Platform	Fully Supported	Best Effort
Windows	Windows 10 or later	Windows 10 or later
macOS	macOS 11 or later	macOS 10.15 or later
Linux	Ubuntu 22.04 or later	Ubuntu 20.04 or later (or equivalent)
Android	Android 11 or later	Android 5.0 or later
iOS	iOS 15.0 or later	iOS 15.0 or later
iPadOS	iPadOS 15.0 or later	iPadOS 15.0 or later

2.3 WebAuthn browser support

The Web Authentication API (also known as WebAuthn) is a specification that enables FIDO-based authentication to websites.

WebAuthn support is not uniform across browsers. This does NOT affect your ability to manage FIDO credentials (*passkeys* and *fingerprints*) within the Yubico Authenticator app, but your ability to use your YubiKey's FIDO credentials for authentication will be dependent on your specific browser and device.

For a complete list of browser support for various authentication features across desktop and mobile platforms, please see the WebAuthn Compatibility page.

CHAPTER

THREE

DOWNLOAD THE APP

The latest versions of the Yubico Authenticator app are available to download directly from Yubico and/or via a platform store:

macOS

Yubico Authenticator for macOS direct download

Yubico Authenticator for macOS on the Mac App Store

Windows

Yubico Authenticator for Windows direct download

Yubico Authenticator for Windows on the Microsoft Apps Store

Linux

Yubico Authenticator for Linux direct download

Note: Yubico Authenticator for Linux is only available to download directly from Yubico as a tar.gz file. Do NOT download the app from the Snap Store; the latest versions of Yubico Authenticator are no longer available as a Snap download.

Android

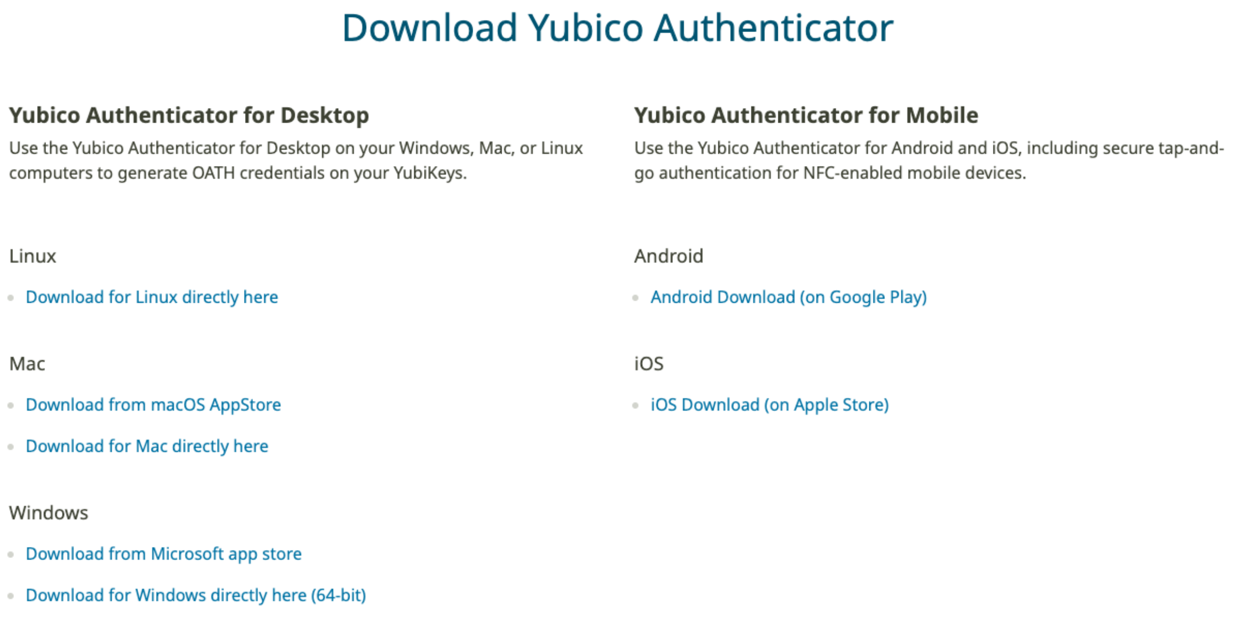
Yubico Authenticator for Android on the Google Play store

Yubico Authenticator for Android direct download

iOS and iPadOS

Yubico Authenticator for iPhone and iPad on the App Store

These download links can also be found on the Authenticator page on the Yubico Website.



Download Yubico Authenticator

Yubico Authenticator for Desktop

Use the Yubico Authenticator for Desktop on your Windows, Mac, or Linux computers to generate OATH credentials on your YubiKeys.

Linux

- Download for Linux directly here

Mac

- Download from macOS AppStore
- Download for Mac directly here

Windows

- Download from Microsoft app store
- Download for Windows directly here (64-bit)

Yubico Authenticator for Mobile

Use the Yubico Authenticator for Android and iOS, including secure tap-and-go authentication for NFC-enabled mobile devices.

Android

- Android Download (on Google Play)

iOS

- iOS Download (on Apple Store)

3.1 Previous releases

Previous versions of Yubico Authenticator (for Windows, Mac, Linux, and Android) can be downloaded from the Releases page.

3.2 Developers

For developers wishing to download the source files for Yubico Authenticator, please see the GitHub repos for your desired platform:

- Desktop and Android
- iOS/iPadOS

CHAPTER

FOUR

INSTALL THE APP

Once you have *downloaded* the Yubico Authenticator app, follow the installation instructions listed here for your chosen platform.

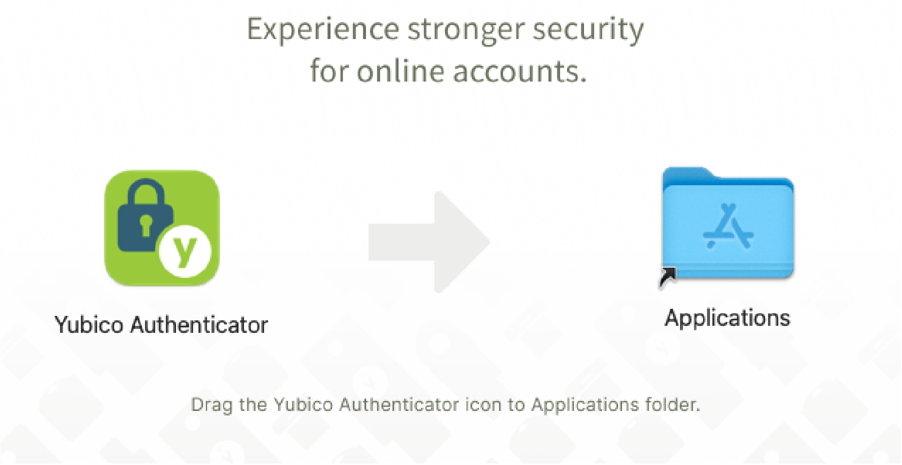
4.1 macOS

Yubico Authenticator installation on macOS is slightly different for *direct downloads* vs. *Mac App Store*. However, both methods require you to *enable input monitoring* and *screen recording* after installation.

4.1.1 Installation via direct download

If you *downloaded the .dmg file from the Yubico website*, do the following:

1. Double-click on the *yubico-authenticator-<version>.dmg* file.
2. Drag the Yubico Authenticator icon to the Applications folder when prompted.

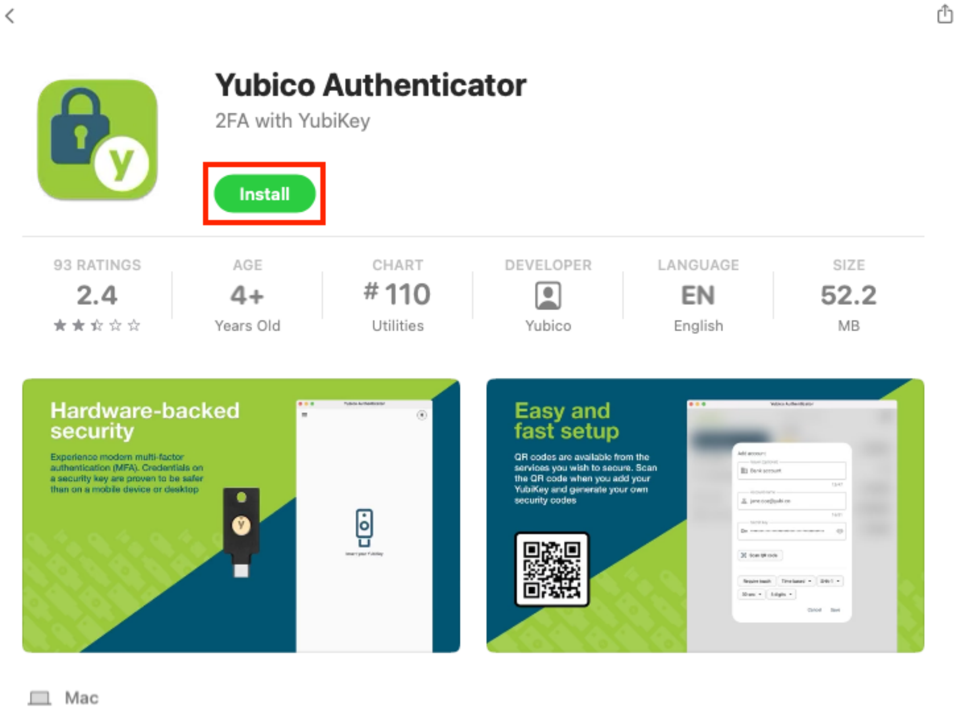

Experience stronger security
for online accounts.
Yubico Authenticator
Applications
Drag the Yubico Authenticator icon to Applications folder.

3. *Enable input monitoring* and *screen recording*.

4.1.2 Installation via the Mac App Store

If you want to *install the app via the Mac App Store*, do the following:

1. On the Yubico Authenticator page in the Mac App Store, click **Get**. Once the app has been downloaded, the blue **Get** button will change to a green **Install** button.
2. Click the **Install** button. Enter your Apple ID and password when prompted.



93 RATINGS	AGE	CHART	DEVELOPER	LANGUAGE	SIZE
2.4	4+	# 110		EN	52.2
★★⯪☆☆	Years Old	Utilities	Yubico	English	MB

Experience modern multi-factor authentication (MFA). Credentials on a security key are proven to be safer than on a mobile device or desktop

QR codes are available from the services you wish to secure. Scan the QR code when you add your YubiKey and generate your own security codes

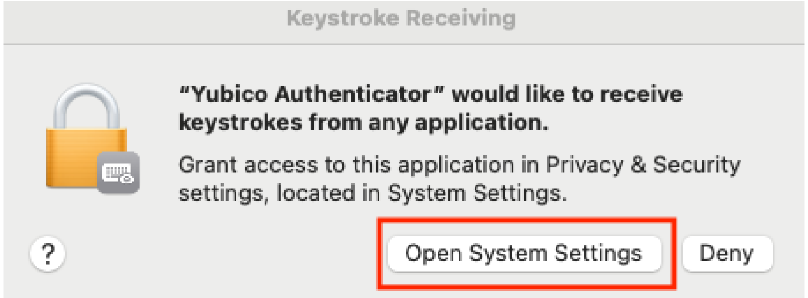
3. *Enable input monitoring* and *screen recording*

4.1.3 Enable input monitoring

Before you can use the *Slots* feature of Yubico Authenticator, you must enable input monitoring. These special permissions are required because the YubiKey's Yubico OTP application, which you interact with via **Slots**, communicates with your Mac as if it were an external keyboard.

To enable input monitoring, do the following:

1. Open the Yubico Authenticator app and insert a YubiKey into your Mac.
2. Click on **Slots**.
3. A **Keystroke Receiving** window should pop up. Click on **Open System Settings**.

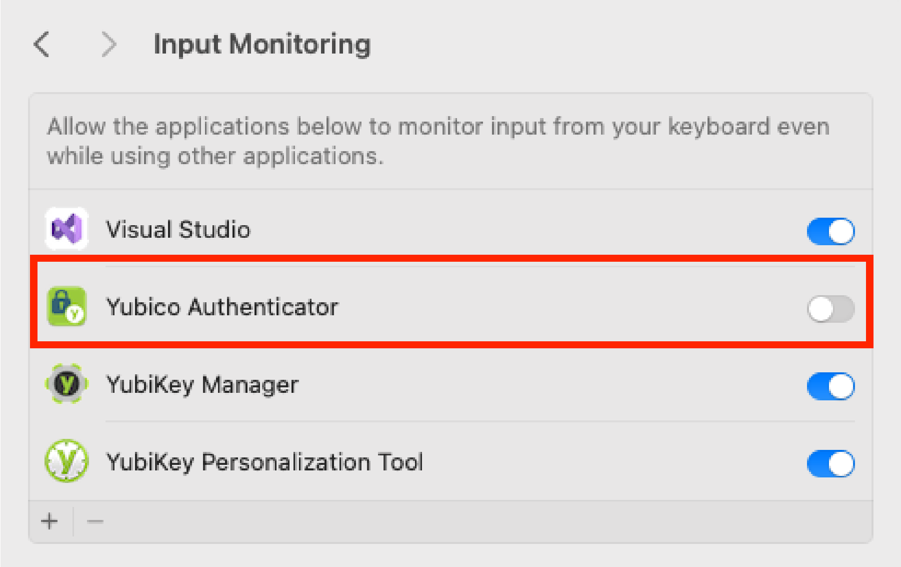


Keystroke Receiving

“Yubico Authenticator” would like to receive keystrokes from any application.

Grant access to this application in Privacy & Security settings, located in System Settings.

4. This will take you to your **Input Monitoring** settings. Flip the toggle next to **Yubico Authenticator** to the “on” position.



Input Monitoring

Allow the applications below to monitor input from your keyboard even while using other applications.

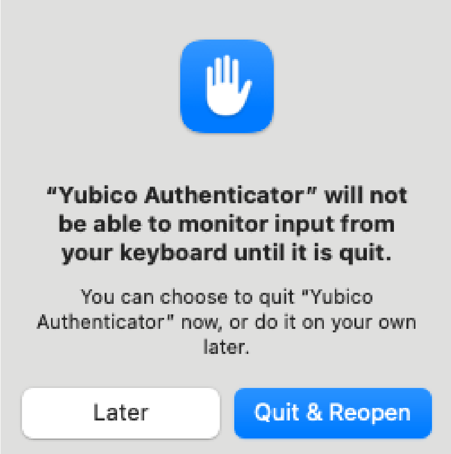
Visual Studio ●

Yubico Authenticator ○

YubiKey Manager ●

YubiKey Personalization Tool ●

5. If the Yubico Authenticator app is still open, another window will pop up prompting you to restart the app to apply the new settings. Click **Quit & Reopen**.



“Yubico Authenticator” will not be able to monitor input from your keyboard until it is quit.

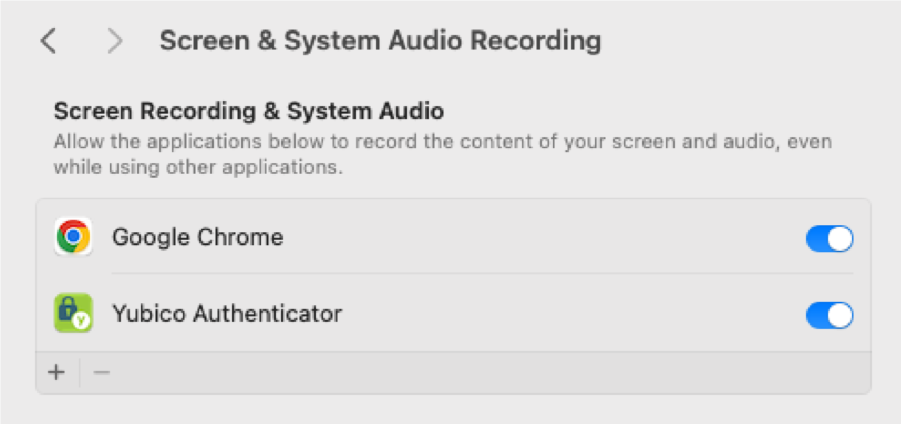
You can choose to quit "Yubico Authenticator" now, or do it on your own later.

Note: If you are not automatically prompted to change your input monitoring settings when opening the app for the first time, you can still do this manually by going to **System Settings** > **Privacy & Security** > **Input Monitoring**. Click the + icon, select the Yubico Authenticator app in the window that appears, and click **Open**.

4.1.4 Enable screen recording

Before you can add new *OATH accounts* via QR code, you must enable screen recording. You will be prompted to do this the first time you attempt a QR scan, but you can also set these permissions manually by doing the following:

1. On your macOS device, go to **System Settings** > **Privacy & Security** > **Screen & System Audio Recording**.
2. If you do not see Yubico Authenticator on the list yet, add it by clicking the plus symbol, selecting the app, and clicking **Open**.
3. Set the toggle next to Yubico Authenticator to the "on" position.



Screen & System Audio Recording

Screen Recording & System Audio

Allow the applications below to record the content of your screen and audio, even while using other applications.

4.2 Windows

If you *downloaded the .msi file from the Yubico website*, double-click the *yubico-authenticator-<version>-win64.msi* file and follow the prompts to complete installation.

Alternatively, you can install Yubico Authenticator for Windows via the *Microsoft Apps Store*.

4.3 Linux

Once you have *downloaded the tar.gz file from the Yubico website*, extract the folder where the app has permissions to run.

4.3.1 Enable pcscd

Before you can use the *Accounts* (OATH) and *Certificates* (PIV) features of Yubico Authenticator, you must enable pcscd, which allows communication over the CCID interface.

To enable and start pcscd on most Linux systems, run:

```
sudo systemctl enable --now pcscd
```

To check if pcscd is running, enter:

```
systemctl status pcscd
```

To check if pcscd is enabled, enter:

```
systemctl is-enabled pcscd
```

4.3.2 QR scanning

For Linux machines running the Wayland graphical environment, the QR scanning feature (used when adding a new *OATH account*) requires either the gnome-screenshot tool (when running the Gnome desktop environment) or the Spectacle tool (when running the KDE desktop environment).

4.3.3 Running the app

To run the Yubico Authenticator for Linux app, change your path to wherever the executable is located and enter `./authenticator`.

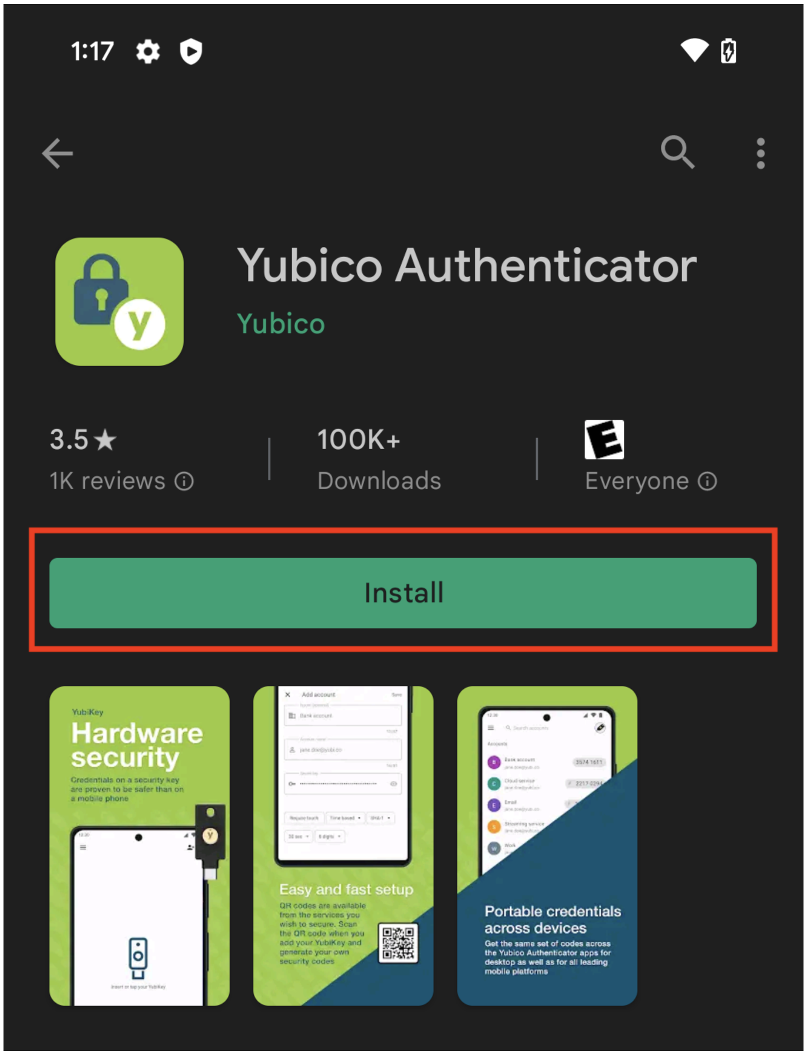
Alternatively, you can create a shortcut for Yubico Authenticator in the app launcher by running the desktop_integration.sh script, which is included in the tarball.

4.3.4 Installing older versions of Yubico Authenticator for Linux

To install an older version of Yubico Authenticator for Linux (5.1 and previous), follow the instructions on the Support site.

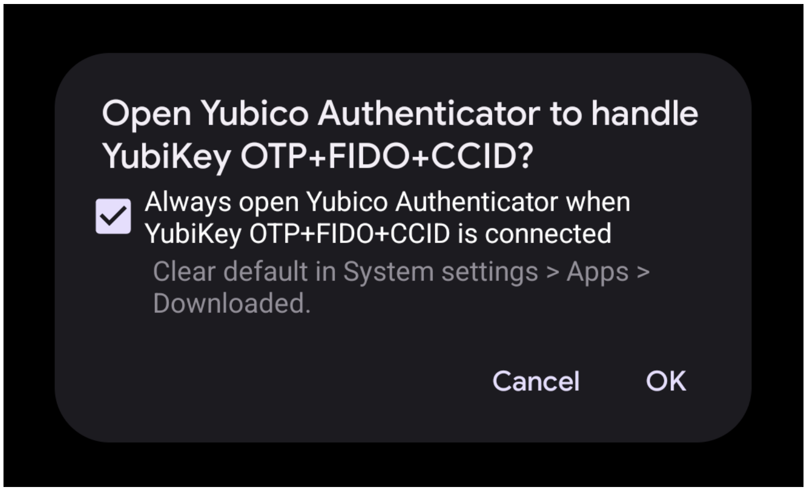
4.4 Android

To install Yubico Authenticator for Android, go to the Yubico Authenticator page in the *Google Play Store* and click **Install**.


1:17
Yubico Authenticator
Yubico
3.5★
1K reviews ⓘ
100K+
Downloads
E
Everyone ⓘ
Install
YubiKey
Hardware security
Credentials on a security key are proven to be safer than on a mobile phone
Easy and fast setup
QR codes are available from the services you wish to secure. Scan the QR code when you add your YubiKey and generate your own security codes
Portable credentials across devices
Get the same set of codes across the Yubico Authenticator apps for desktop as well as for all leading mobile platforms

4.4.1 USB permissions

When you open the app and connect a new YubiKey to your Android device over USB, you may be prompted to allow the app to communicate with the key over the USB interface. The USB device name for the key is often listed as “YubiKey OTP+FIDO+CCID”. Click **OK**.



Open Yubico Authenticator to handle YubiKey OTP+FIDO+CCID?

☑ Always open Yubico Authenticator when YubiKey OTP+FIDO+CCID is connected

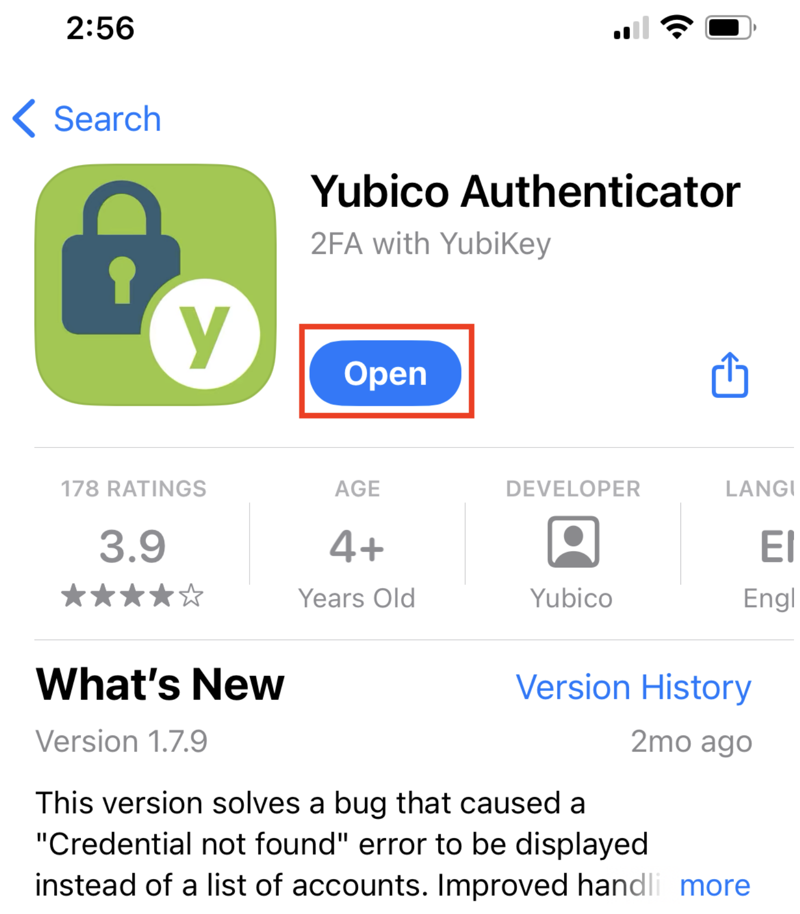
Clear default in System settings > Apps > Downloaded.

4.4.2 Installation via direct download

You may also *download the .apk file directly*. To install, click on the .apk file and follow the prompts. Your device may request permission to install apps downloaded from your browser.

4.5 iOS and iPadOS

To install Yubico Authenticator for iOS/iPadOS, go to the Yubico Authenticator page in the *App Store* and click **Get**. Authenticate with your Apple account information when prompted. Once downloaded, click **Open** to open the Yubico Authenticator app.



This version solves a bug that caused a "Credential not found" error to be displayed instead of a list of accounts. Improved handli

4.6 Developers

For developers wishing to build and package the Yubico Authenticator app from source, please see the GitHub documentation for your desired platform:

- Desktop and Android
- iOS/iPadOS

CHAPTER

FIVE

HOME AND SETTINGS

For desktop and Android devices, general app and key settings are managed primarily through the *Home page*. Features include:

- *changing a YubiKey's label and color in the app*
- *toggling YubiKey applications on/off*
- *changing the app theme*
- *toggling between multiple connected keys*
- *performing a factory reset of a YubiKey application*
- *loading an icon pack with custom OATH account and Passkey icons*
- *changing the application language*
- *showing/hiding NFC smart card readers*

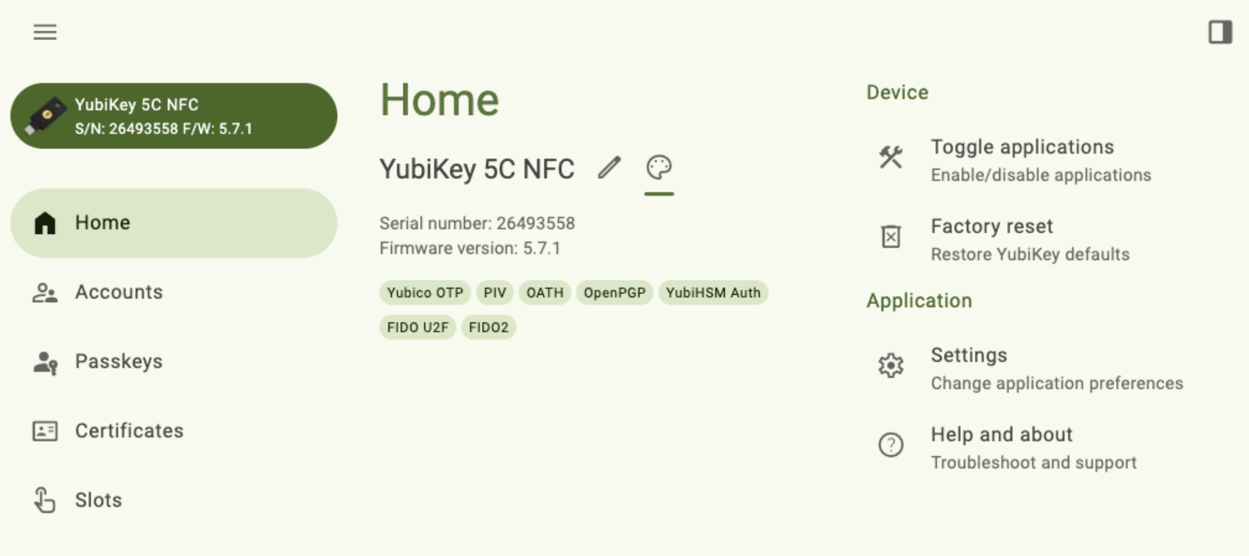
There are also mobile-specific settings for both *Android* and *iOS/iPadOS*.

5.1 The Home page: YubiKey at a glance

Note: The **Home** feature is available for Yubico Authenticator for Desktop and Android only.

The **Home** page displays a wealth of important information about the connected YubiKey, including:

- YubiKey model (e.g. YubiKey 5 NFC).
- Custom label (if one was created).
- Serial number.
- Firmware version.
- *PIN complexity status* (available for YubiKeys with the PIN complexity feature only).
- Enabled applications for current connection type (USB or NFC). Applications include Yubico OTP, PIV, OATH, OpenPGP, FIDO U2F, FIDO2, and YubiHSM Auth, depending on your YubiKey.
- *FIPS status* (available for YubiKey 5 FIPS Series keys with firmware 5.7 or later).



Serial number: 26493558
Firmware version: 5.7.1

5.1.1 Navigating to the Home page

To view the **Home** page, plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Home**.

To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation. To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

5.1.2 PIN complexity status

PIN complexity is a new feature offered with firmware version 5.7. If PIN complexity is enabled, the YubiKey will block the usage of trivial PINs, such as “11111111”, “password”, or “12345678”.

If the feature is enabled on your key, you will see the PIN complexity status (“PIN complexity enforced”) on the **Home** screen, which is underneath the firmware version. PIN complexity enablement occurs during YubiKey manufacturing and cannot be modified (disabled or re-enabled) via Yubico Authenticator.

PIN complexity is enabled by default on select YubiKey series and available as an optional add-on for some custom-configured YubiKeys. For more information on the PIN complexity feature and the full PIN blocklist, see the YubiKey Technical Manual. To verify PIN complexity support for various the YubiKey series, see the Firmware 5.7 Capabilities table.

Note: Yubico offers custom configuration options to personalize YubiKeys during production. For more details, visit Yubico’s Customization guide.

5.1.3 FIPS status

The FIPS status, which is available for YubiKey 5 FIPS Series keys with firmware 5.7 or later, has two components: FIPS capable and FIPS approved.

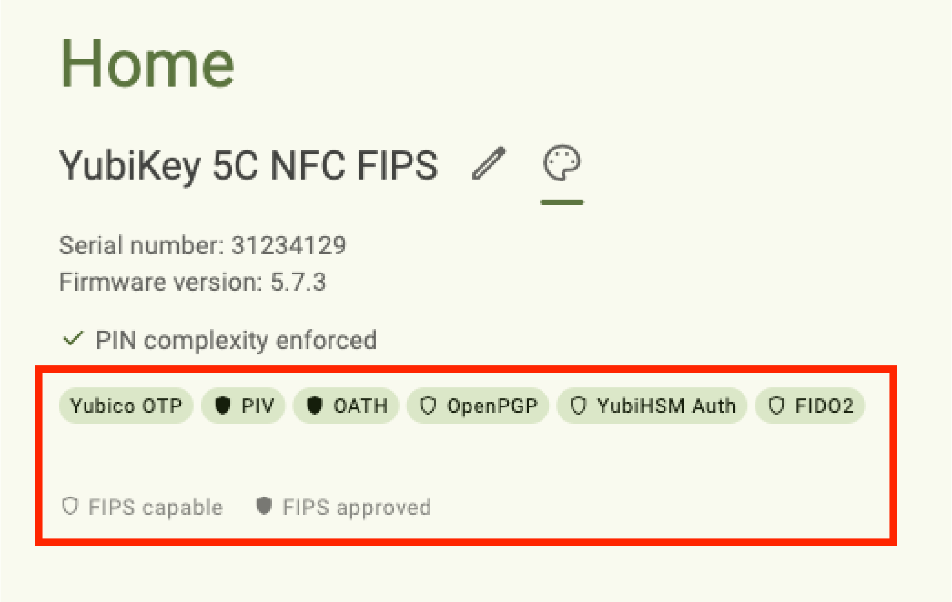
"FIPS approved" refers to YubiKey applications that are in compliance with the FIPS 140-3 standard. "FIPS capable" refers to YubiKey applications that are capable of complying with FIPS 140-3 but haven't yet been *configured* to achieve that status.

Note: For a complete list of the YubiKey requirements for FIPS 140-3, see the YubiKey Technical Manual.

The following YubiKey applications are capable of FIPS 140-3 compliance:

- PIV
- FIDO2
- OATH
- OpenPGP
- YubiHSM Auth

To check a key's FIPS status, look for the FIPS shield icon next to the application name on the **Home** screen. If an application has been disabled, you must *re-enable* it to check its FIPS status.



Home

YubiKey 5C NFC FIPS

Serial number: 31234129
Firmware version: 5.7.3

✓ PIN complexity enforced

Yubico Authenticator will not allow you to create credentials for applications in the FIPS capable state. This includes OATH accounts, FIDO2 passkeys, and PIV keys and certificates. The Yubico OTP application, which cannot be in the FIPS capable or FIPS approved states, is unaffected.

Once an application transitions to the FIPS approved state, the only way to return to the FIPS capable state is by performing a *factory reset* of that application.

Note: Yubico Authenticator for desktop and Android support Secure Channel Protocol 11b (SCP11b). This ensures that NFC connections between the app and YubiKey 5 FIPS Series keys are FIPS-compliant as long as the device running Yubico Authenticator also supports AES-CMAC (native support for AES-CMAC on Android is version-dependent).

Putting an application in FIPS approved mode

The PIV, FIDO2, and OATH applications can be put into the FIPS approved state using Yubico Authenticator. Once an application is in the FIPS approved state, you will have full access to the application's functionality.

Do the following for each application:

- **OATH**
    - Set an *OATH application password*.
- **FIDO2**
    - Set a *FIDO2 PIN*. The PIN must be at least 8 characters and adhere to the key's *PIN complexity* requirements.
- **PIV**
    - Change the *PIV PIN and PUK*. They must be at least 8 characters and adhere to the key's *PIN complexity* requirements.
    - Change the *Management Key*. You must use an AES key algorithm, which will be automatically enforced by Yubico Authenticator.

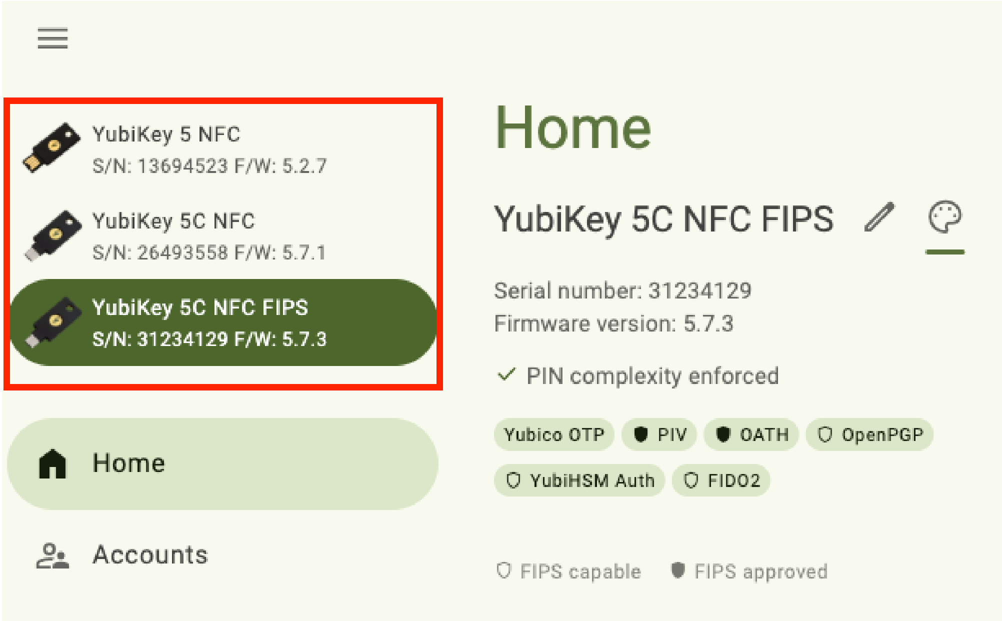
Note: The YubiHSM Auth and OpenPGP applications cannot be put into FIPS approved mode with Yubico Authenticator. (In fact, the only YubiHSM Auth and OpenPGP functionality the Authenticator offers is the ability to *toggle* those applications on/off.) To interact with these applications, use the ykman CLI tool. For more information on the requirements that must be met for the YubiHSM Auth and OpenPGP applications to achieve FIPS approved status, see the YubiKey Technical Manual.

5.2 Switching between keys

Note: Toggling between multiple connected YubiKeys is available on Yubico Authenticator for Desktop only.

Yubico Authenticator for Desktop allows you to interact with multiple connected YubiKeys (only one key can be connected over NFC, but USB connections are not limited). When performing operations in Yubico Authenticator, changes can only be applied to one key at a time.

If you have more than one YubiKey connected to your desktop device, you can toggle between them by selecting a key underneath the menu icon in the upper left corner of the app. Any YubiKey changes made via the **Home**, **Accounts**, **Passkeys**, **Fingerprints**, **Certificates**, and **Slots** pages will apply to the selected key only.



Serial number: 31234129
Firmware version: 5.7.3

✓ PIN complexity enforced

5.3 Change a YubiKey's label and color

Note: YubiKey labels and colors can be changed on Yubico Authenticator for Desktop and Android only.

By default, connected YubiKeys are labeled with their model name on the **Home** page and the left menu bar. They also have a default color scheme within the app (green on desktop, purple on Android).

To assist with managing multiple keys, key labels and colors can be customized. When a custom label is created, the key's model name is moved into parentheses after the custom text. These changes persist on the device they are initiated on; if a key is unplugged and then reconnected, the label and color will reflect whatever was previously configured. If multiple keys with different colors are connected to your desktop device, *switching between them* will change the app's color scheme.

The label and color information is stored in the app itself, not on the YubiKey. If you toggle these settings for a key on Device A and then connect the key to Device B, you will not see the label/color changes in the app on Device B.

To change a label or color for a particular YubiKey, do the following:

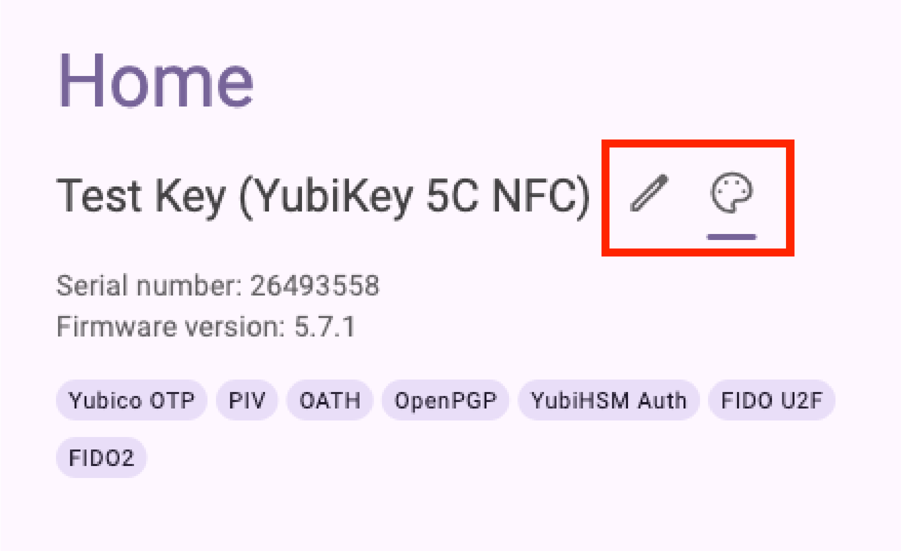
1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Home**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

2. To change the color, click the palette icon and select a new color.

3. To change the label, click the pencil icon next to the key's model name. Enter a new name for your key and click **Save**.



Home

Test Key (YubiKey 5C NFC)

Serial number: 26493558
Firmware version: 5.7.1

5.4 Toggle YubiKey applications on/off

Note: The **Toggle applications** feature is available on Yubico Authenticator for Desktop and Android only.

The YubiKey applications, which include Yubico OTP, PIV, OATH, OpenPGP, FIDO U2F, YubiHSM Auth, and FIDO2, can be enabled or disabled for both USB and NFC connections. If an application is disabled, that application will no longer interact with connected devices over the indicated connection type.

For example, if the Yubico OTP application is disabled over USB, the key will no longer emit a Yubico OTP (if a slot is configured with one) when the key is connected to a device over USB and touched. If the Yubico OTP application is disabled over NFC, it is not possible to start Yubico Authenticator for Android on an *NFC tap*.

A caveat: you cannot disable all applications over USB. Additionally, on Android, the OTP application cannot be the only application enabled over USB (the YubiKey would become impossible to detect on Android otherwise).

For YubiKey Bio Multi-protocol Edition keys, once the key is considered “in use”, applications cannot be toggled on/off until a factory *reset* is performed. “In use” means that the key has been configured in some way: a PIN has been set, the PIV management key has been changed, a certificate has been loaded into one of the PIV application slots, etc.

Note: Enabling/disabling an application does not reset the application; all credentials and settings are preserved.

To enable/disable an application, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Home**.

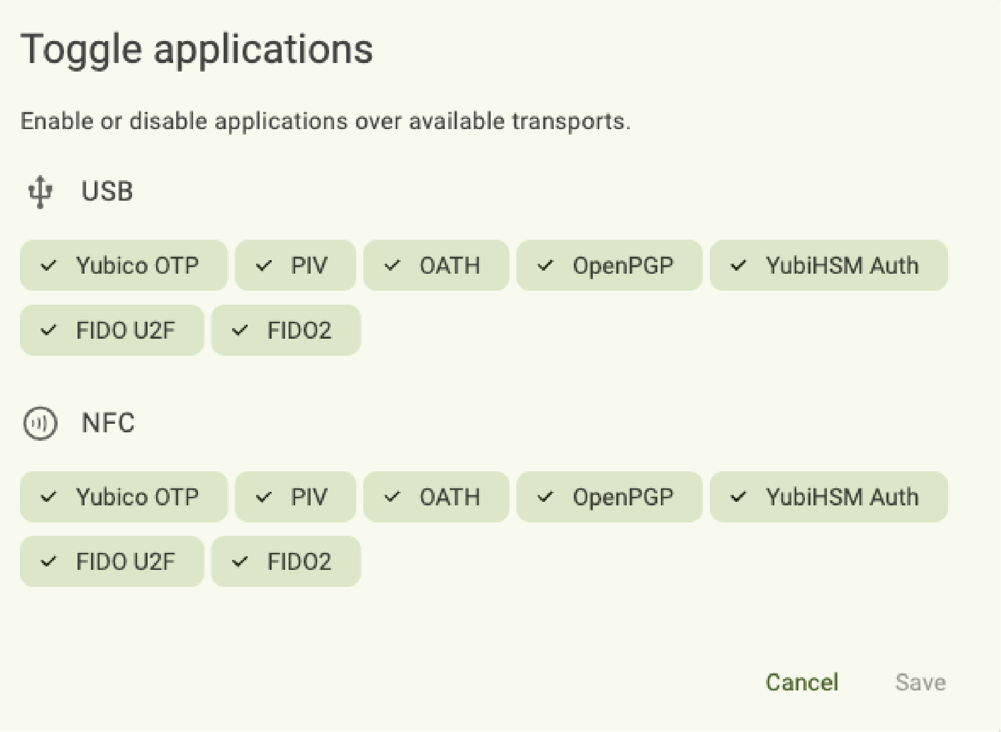
   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

2. Click **Toggle applications** under **Device**. To find the **Device** menu in a narrow app window, click the three dots in the upper right corner.

3. To enable an application, click on it until it shows a check mark. To disable an application, click on it until the check mark disappears. When you are done, click **Save**.

For NFC connections on Android, scan your key when prompted to confirm the operation.



Toggle applications

Enable or disable applications over available transports.

USB

✓ Yubico OTP ✓ PIV ✓ OATH ✓ OpenPGP ✓ YubiHSM Auth ✓ FIDO U2F ✓ FIDO2

NFC

✓ Yubico OTP ✓ PIV ✓ OATH ✓ OpenPGP ✓ YubiHSM Auth ✓ FIDO U2F ✓ FIDO2

5.5 Change the Authenticator theme

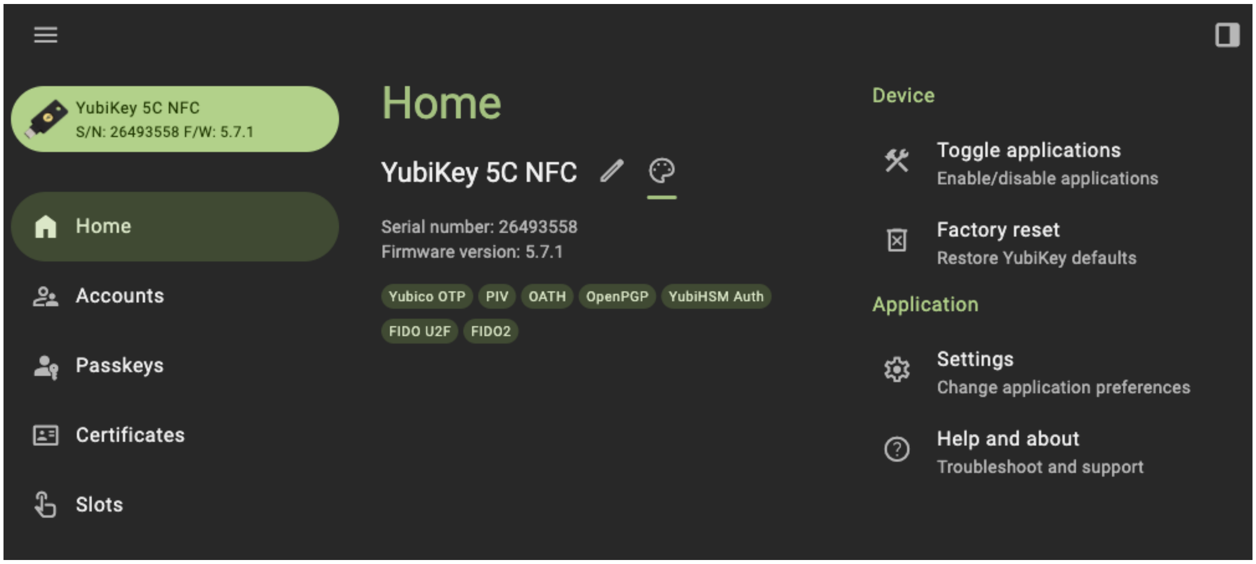
Note: The app theme can be changed on Yubico Authenticator for Desktop and Android only.

Yubico Authenticator for Desktop and Android have three themes available: default, light, and dark. The color of the default theme is dependent on your system settings.

To change the theme, do the following:

1. Open Yubico Authenticator, click the menu icon in the upper left corner of the app, and select **Home**.
2. Click **Settings** under **Application**. In the **Settings** window, click **Application theme** and select a new theme.

   To find the **Application** menu in a narrow app window, click the three dots in the upper right corner of the app.



Serial number: 26493558
Firmware version: 5.7.1

5.6 Load a custom icon pack

Note: Custom icons are only available for Yubico Authenticator for Desktop and Android.

When viewing *OATH accounts* on a YubiKey within Yubico Authenticator, each account is listed with a colored icon that contains the first letter of the issuer by default. Similarly, *Passkeys* are listed with a default Passkey icon.

To make OATH accounts and Passkeys more easily distinguishable from one another, custom icons can be uploaded and used in Yubico Authenticator. For example, with custom icons, instead of seeing the default “D” icon next to an OATH account for Docker, an icon containing the Docker logo and colors would be shown. For a Microsoft Passkey, an icon with the Microsoft logo and colors would be shown in place of the default Passkey icon.

Icon packs must be in the Aegis Icon Pack format. Feel free to use a pre-built icon pack from Aegis or create your own.

To upload an icon pack to Yubico Authenticator on desktop or Android, do the following:

1. Download a pre-built icon pack from Aegis or create your own.
2. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Home**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.
3. Select **Settings** under **Application**. On the **Settings** screen, click **Custom icons**.

   In a narrow app window, click the three dots in the upper right corner of the app to find the **Application** menu.
4. In the **Custom icons** window, click **Load icon pack**. Select the file containing the icons (for example, aegis-icons.zip).
5. Once loaded, any OATH account or Passkey with an issuer that is supported by the icon pack will display the custom icon. To delete the icon pack, click the trash can icon in the **Custom icons** window. Similarly, to update the icon pack, click **Replace icon pack** and select the new file.

5.7 Change the application language

Note: The app language can be changed on Yubico Authenticator for Desktop and Android only.

Yubico Authenticator supports multiple languages. The default language the application uses depends on your device's system settings, but it is also possible to manually select the app language. Supported languages include:

- English
- German
- Spanish
- French
- Polish
- Slovak
- Vietnamese
- Japanese
- Czech
- Swedish
- Turkish
- Chinese (Simplified and Traditional)

To change the app language, do the following:

1. Open Yubico Authenticator, click the menu icon in the upper left corner of the app, and select **Home**.
2. Click **Settings** under **Application**. In the **Settings** window, click **Language** and select your preferred language.

   To find the **Application** menu in a narrow app window, click the three dots in the upper right corner of the app.

5.8 Show/hide NFC smart card readers

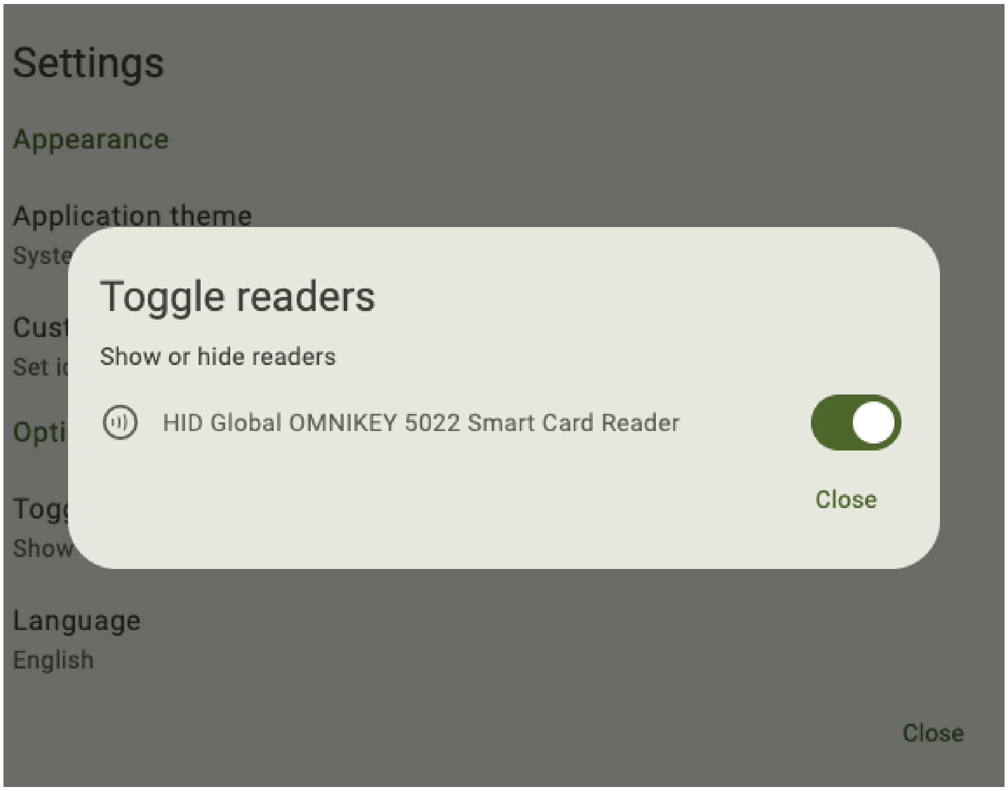
Note: The **Toggle readers** feature is only available on Yubico Authenticator for Desktop.

By default, any NFC smart card reader connected to a desktop device will be shown in Yubico Authenticator (regardless of whether a YubiKey is on the reader). **Settings** includes a toggle that allows you to show/hide connected readers. If a reader is hidden, you will not be able to interact with an NFC-enabled YubiKey in contact with the reader from within Yubico Authenticator.

To show/hide an NFC smart card reader, do the following:

1. Open Yubico Authenticator, click the menu icon in the upper left corner of the app, and select **Home**.
2. Click **Settings** under **Application**. In the **Settings** window, click **Toggle readers**.

   To find the **Application** menu in a narrow app window, click the three dots in the upper right corner of the app.
3. To show/hide a reader, click the toggle to the on/off position.



Settings

Appearance

Application theme

Syste

Cust

Set ic

Opti

Togg

Show

Toggle readers

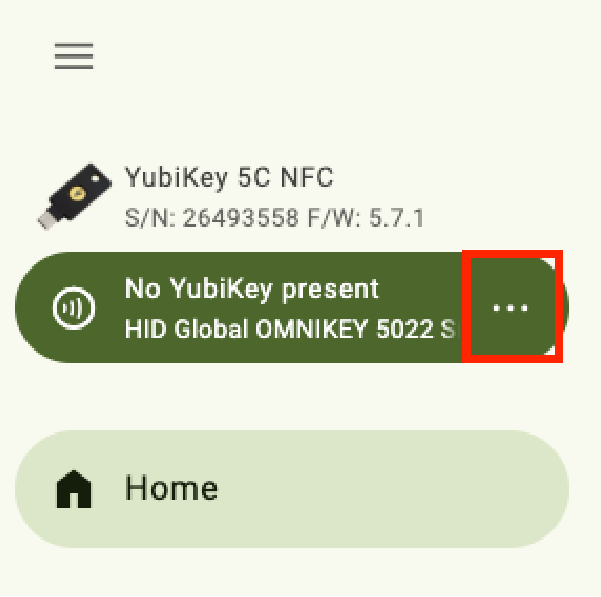
Show or hide readers

HID Global OMNIKEY 5022 Smart Card Reader

Language

English

Note: Readers can also be toggled off by clicking the three dots next to the reader name (or right-clicking on the NFC icon in a narrow app window) and selecting **Hide reader**.



YubiKey 5C NFC

S/N: 26493558 F/W: 5.7.1

No YubiKey present

HID Global OMNIKEY 5022 S

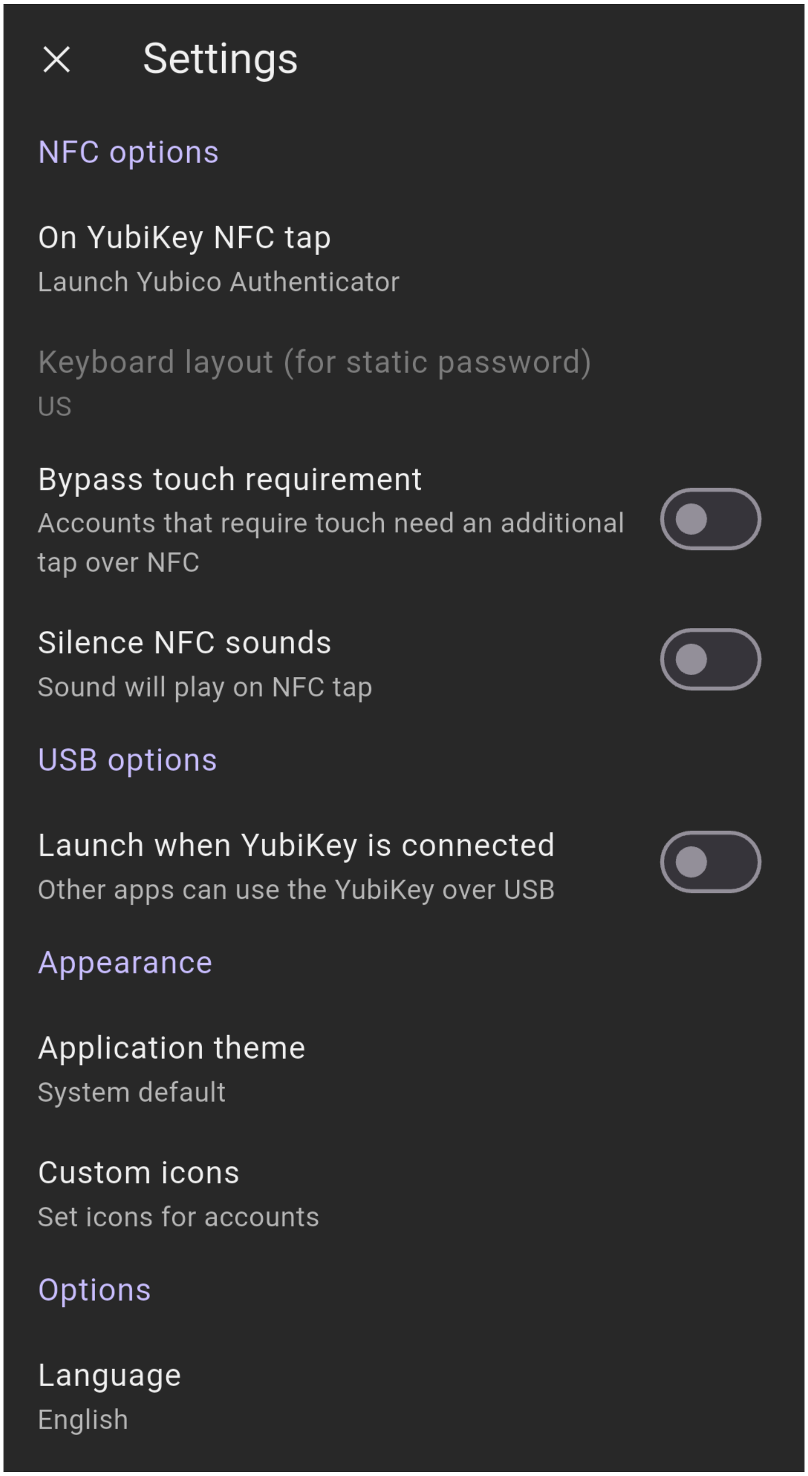
5.9 Android settings

There are several settings that are unique to Yubico Authenticator for Android. These include:

- NFC tap behavior
- Touch requirement with NFC
- NFC sounds
- USB connectivity

Note: Android NFC settings are only visible in the Yubico Authenticator app on devices that support NFC.

To toggle these settings, open Yubico Authenticator, click the menu icon in the upper left corner of the app, and select **Home**. Click the three dots in the upper right corner of the app and select **Settings** under **Application**.



Settings

NFC options

On YubiKey NFC tap
Launch Yubico Authenticator

Keyboard layout (for static password)
US

Bypass touch requirement
Accounts that require touch need an additional tap over NFC

Silence NFC sounds
Sound will play on NFC tap

USB options

Launch when YubiKey is connected
Other apps can use the YubiKey over USB

Appearance

Application theme
System default

Custom icons
Set icons for accounts

Options

Language
English

5.9.1 NFC tap behavior

Yubico Authenticator can be configured to do one of the following when a YubiKey is tapped against the Android device's NFC reader:

- Launch Yubico Authenticator
- Generate a *Yubico OTP* and copy it to clipboard
- Launch Yubico Authenticator, generate a Yubico OTP, and copy it to clipboard
- Nothing

By default, **Launch Yubico Authenticator** is selected. To toggle this setting, click **On YubiKey NFC tap** under **NFC options**.

5.9.2 Touch requirement with NFC

When an *OATH account* is added to a YubiKey, it can be configured to "require touch" in order to generate an OTP. For NFC connections, this means tapping the YubiKey against the device's NFC reader at least twice: once to display the OATH accounts and again to generate and display the OTP for a particular account.

However, on Android, this touch requirement can be bypassed so that OTPs are generated and displayed for all TOTP OATH accounts on the initial NFC tap. To do so, toggle on **Bypass touch requirement** under **NFC options**.

5.9.3 NFC sounds

By default, Android devices with volume on will emit a sound whenever a YubiKey is scanned by the NFC reader. To turn this sound off, click the toggle next to **Silence NFC sounds**.

5.9.4 USB connectivity

By default, Yubico Authenticator does not automatically launch when a YubiKey is connected to an Android device over USB.

To change this so that Yubico Authenticator launches automatically, toggle on **Launch when YubiKey is connected** under **USB options**. Note that this prevents other apps from using the YubiKey when connected over USB.

5.10 iOS/iPadOS settings

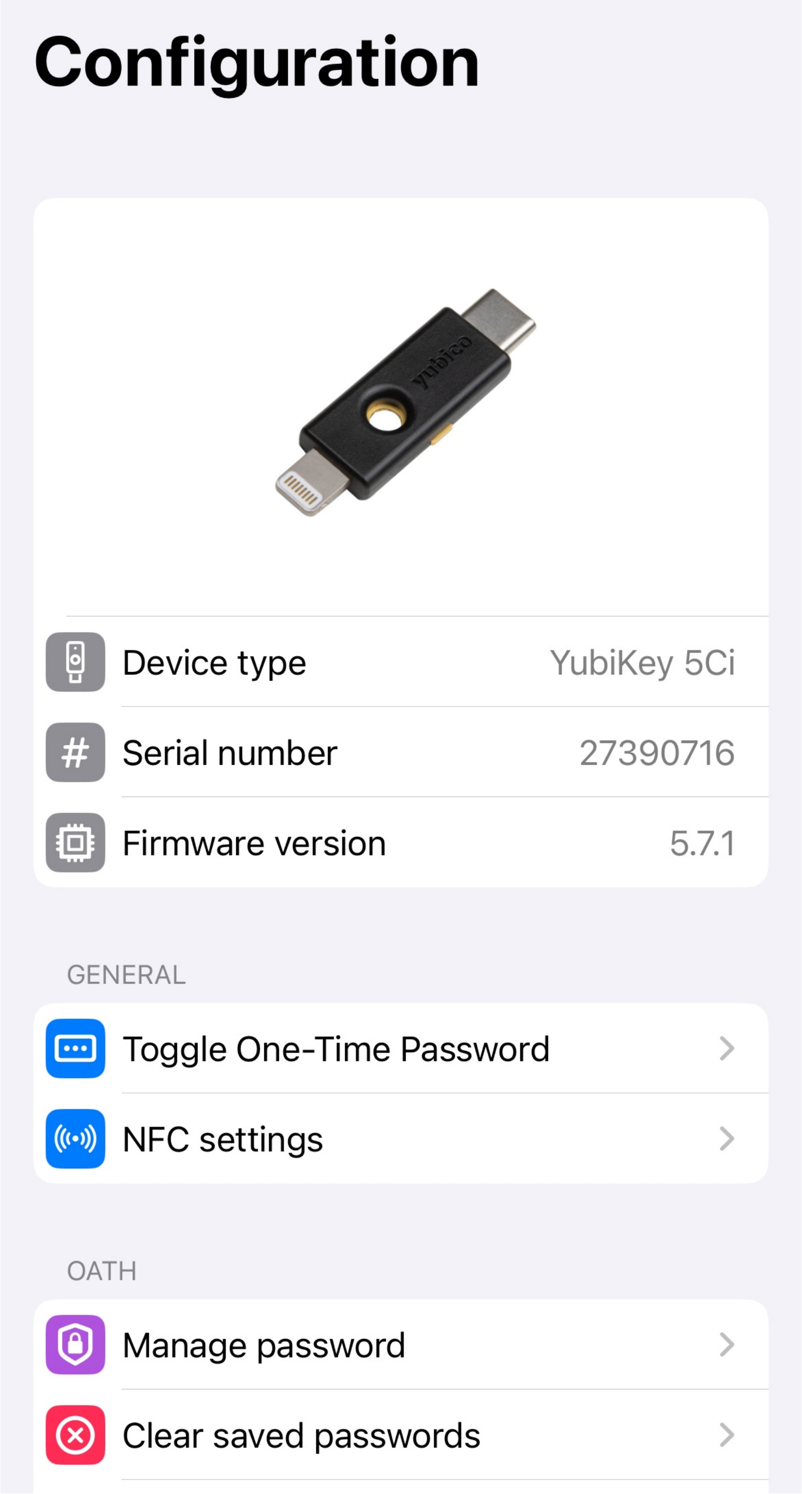
There are several settings that are unique to Yubico Authenticator for iOS/iPadOS. These include:

- NFC reader initiation after opening the app
- Touch requirement with NFC
- Clipboard settings for copying Yubico OTPs
- NFC reader initiation after generating a Yubico OTP
- Yubico OTP generation

5.10.1 YubiKey overview

To get an overview of a YubiKey connected to an iOS/iPadOS device, click the three dots in the upper right corner and select **Configuration**.

The **Configuration** screen displays the key's model name, firmware version, and serial number.



Configuration

Device type	YubiKey 5Ci
Serial number	27390716
Firmware version	5.7.1

GENERAL

Toggle One-Time Password >

NFC settings >

OATH

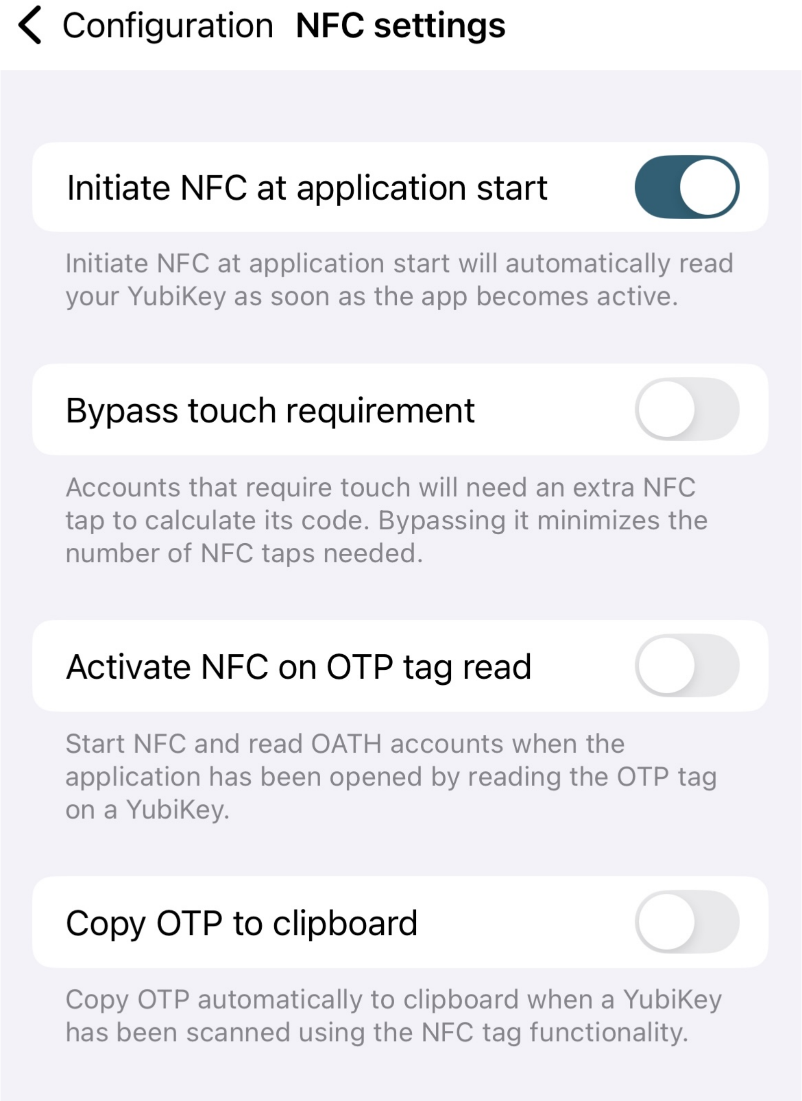
Manage password >

Clear saved passwords >

5.10.2 Initiate NFC at application start

By default, to connect to a YubiKey over NFC on iOS/iPadOS, you must swipe down on the screen to initiate the NFC reader prior to scanning the key. To automatically trigger the NFC reader when the application is launched (as in, the app will prompt you to scan your key without having to swipe down on the screen first), do the following:

1. Click the three dots in the upper right corner and select **Configuration**.
2. Click **NFC settings**.
3. On the **NFC settings** page, toggle on **Initiate NFC at application start**.



< Configuration **NFC settings**

Initiate NFC at application start ●

Initiate NFC at application start will automatically read your YubiKey as soon as the app becomes active.

Bypass touch requirement ○

Accounts that require touch will need an extra NFC tap to calculate its code. Bypassing it minimizes the number of NFC taps needed.

Activate NFC on OTP tag read ○

Start NFC and read OATH accounts when the application has been opened by reading the OTP tag on a YubiKey.

Copy OTP to clipboard ○

Copy OTP automatically to clipboard when a YubiKey has been scanned using the NFC tag functionality.

5.10.3 Touch requirement

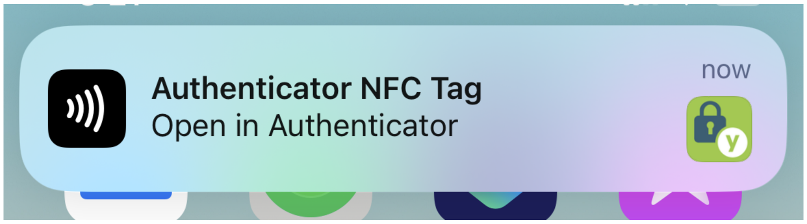
When an *OATH account* is added to a YubiKey, it can be configured to "require touch" in order to generate an OTP. For NFC connections, this means tapping the YubiKey against the device's NFC reader at least twice: once to display the OATH accounts and again to generate and display the OTP for a particular account.

However, on iOS/iPadOS, this touch requirement can be bypassed so that OTPs are generated and displayed for all TOTP OATH accounts on the initial NFC tap. To do so, do the following:

1. Click the three dots in the upper right corner and select **Configuration**.
2. Click **NFC settings**.
3. On the **NFC settings** page, toggle on **Bypass touch requirement**.

5.10.4 Copy Yubico OTP to clipboard

When a YubiKey is held next to an iOS/iPadOS device's NFC reader (whether the Authenticator app is open or not), the key will generate a *Yubico OTP* (if a slot is configured), and the device will prompt you to open Yubico Authenticator, where the OTP will be displayed. Clicking on the OTP will copy it to the clipboard.



Authenticator NFC Tag

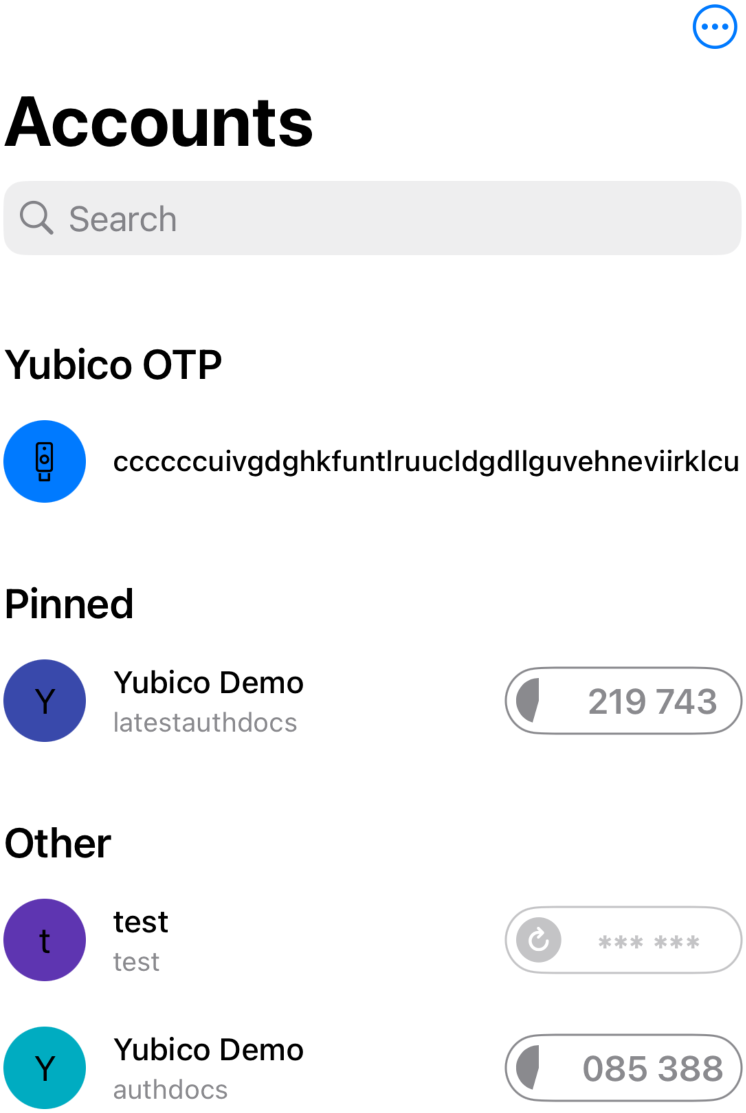
Open in Authenticator

To copy the OTP to the clipboard automatically after opening Yubico Authenticator, do the following:

1. Click the three dots in the upper right corner and select **Configuration**.
2. Click **NFC settings**.
3. On the **NFC settings** page, toggle on **Copy OTP to clipboard**.

5.10.5 Activate NFC on OTP tag read

When a YubiKey is held next to an iOS/iPadOS device's NFC reader (whether the Authenticator app is open or not), the key will generate a *Yubico OTP* (if a slot is configured), and the device will prompt you to open Yubico Authenticator, where the OTP will be displayed. The app can also be configured to launch the NFC reader once the app is opened in this scenario. Once the key is scanned, the OATH accounts are displayed along with the Yubico OTP.



Accounts

Search

Yubico OTP

ccccccuivgdghkfuntlruucldgdllguvehneviirklcu

Pinned

Yubico Demo
latestauthdocs
219 743

Other

test
test
*** ***

Yubico Demo
authdocs
085 388

This is set to “On” by default. To toggle this setting off, do the following:

1. Click the three dots in the upper right corner and select **Configuration**.
2. Click **NFC settings**.
3. On the **NFC settings** page, toggle off **Activate NFC on OTP tag read**.

5.10.6 Toggle Yubico OTPs

By default, YubiKeys will generate a *Yubico OTP* (if a slot is configured) when the key is touched or scanned with an NFC reader. To turn off this setting, do the following:

1. Click the three dots in the upper right corner and select **Configuration**.
2. On the **Configuration** page, select **Toggle One-Time Password**.
3. If connecting over NFC, scan your key when prompted. Otherwise, plug in your key.

4. Click the toggle next to **One-Time Password**. If connecting over NFC, scan your key when prompted to complete the operation.

Important: This toggle changes a setting on the YubiKey itself, not the app. If you toggle this setting off, the YubiKey will not emit an OTP when touched or scanned on ANY device. Also, if you toggle this setting off while connected over NFC, it will only prevent OTPs from being generated and submitted over NFC; touching the key when connected over USB or Lighting will still generate an OTP. Similarly, if you toggle this setting off when the key is plugged into your device, it will only prevent OTPs from being generated and submitted over USB/Lighting; scanning the key with an NFC reader will still generate an OTP.

CHAPTER

SIX

ACCOUNTS: OATH

Important: The **Accounts** feature is available for Yubico Authenticator for Desktop and Mobile (all platforms) and OATH-compatible YubiKeys. This includes the YubiKey 5 Series (standard, FIPS, and CSPN), YubiKey 4 Series, and YubiKey NEO. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

The Accounts feature of Yubico Authenticator allows you to:

- *Configure a YubiKey with OATH account credentials*.
- *Generate and display OATH account OTPs for two-factor authentication*.
- *Protect the OATH application of a YubiKey with a password*.
- *Pin OATH accounts to the top of the Accounts screen in Yubico Authenticator for easier access*.
- *Rename OATH accounts on a YubiKey*.
- *Delete OATH account credentials from a YubiKey*.
- *Configure the Yubico Authenticator application with custom OATH account icons*.

6.1 What is OATH authentication?

OATH (Initiative for Open Authentication) is an organization that specifies two open authentication standards: time-based one-time passwords (TOTPs) and HMAC-based one-time passwords (HOTPs). The term "OTP" encompasses both TOTPs and HOTPs.

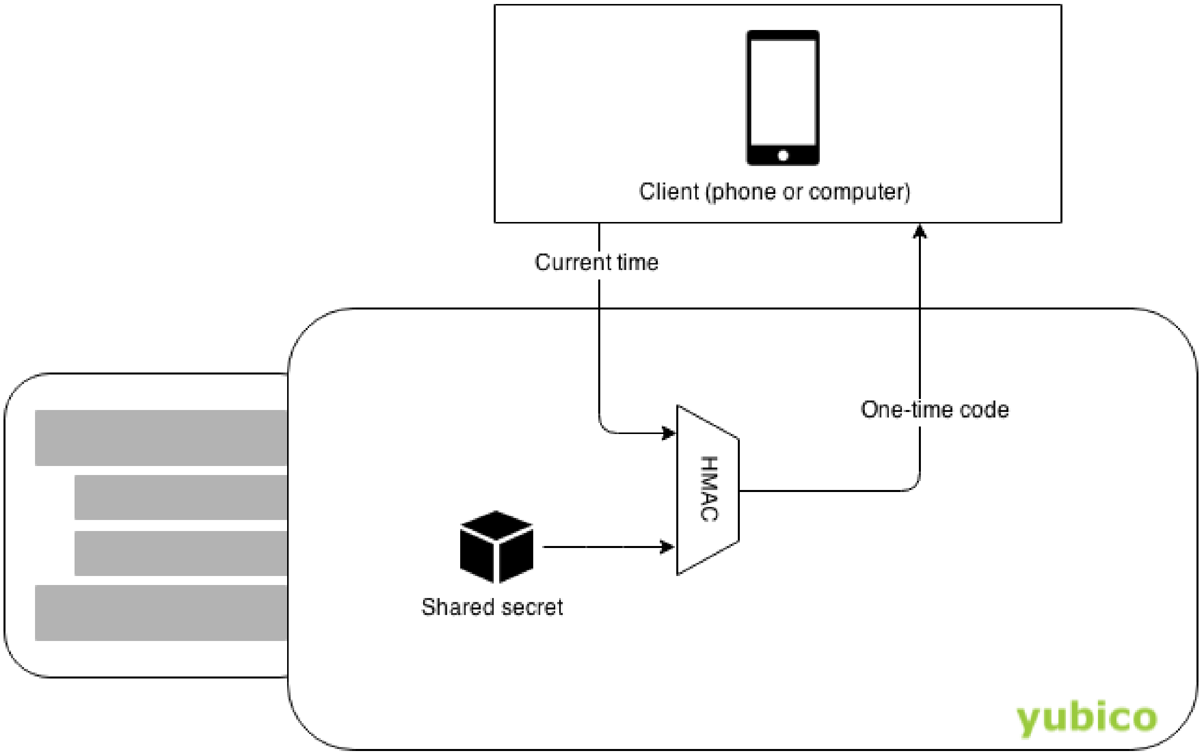
HOTPs are generated by hashing a secret key, counter, and length value with a hashing algorithm (such as SHA-1). TOTPs are generated by hashing a secret key, current time, period, and length value with a hashing algorithm. The resulting HOTPs and TOTPs are codes of 6 or 8 digits in length, such as 076 838.

Once generated, HOTPs are valid until an HOTP generated with a subsequent counter is used for authentication. TOTPs are only valid for the length of the period, which is often 30 seconds.

HOTPs and TOTPs cannot be decrypted. Therefore, OATH authentication works by comparing the OTP generated and submitted by a user with the OTP generated by the relying party (the site/application you are authenticating to) using the same credentials. If the OTPs match, the user is authenticated.

When using OATH for two-factor authentication with a YubiKey and Yubico Authenticator, the OATH credentials are stored in the OATH application in the YubiKey's secure element. During authentication, Yubico Authenticator is used to trigger OTP generation within the YubiKey and to display the OTP code. This OTP can then be copied and pasted onto a login screen. This has two major advantages over storing secrets on a phone:

- Security: The OATH secrets (account credentials) always stay within the YubiKey. A phone can get stolen, sold, infected by malware, have its storage read by a connected computer, etc. Furthermore, the OATH application itself can be protected by a *password*, which ensures that OATH account details cannot be easily accessed in the event of a lost or stolen YubiKey.
- Accessibility: Once a YubiKey is configured with an OATH account, OTPs can be generated by that key and Yubico Authenticator on *any* device. For example, if your phone dies, you could still generate OTPs with your YubiKey via Yubico Authenticator on a friend's phone.



6.2 Adding a new account

Adding a new account for OATH authentication requires a YubiKey, Yubico Authenticator, and the secret key information provided by the site/account/service you are registering the YubiKey with.

Note: Sites, services, and applications typically describe OATH authentication as "two-factor authentication using an authenticator app". They may also refer to authentication with a One-Time Password (OTP).

During registration, the YubiKey stores the secret key and associated account information. With Yubico Authenticator, OATH accounts can be added via QR code or by entering the secret key and other fields manually.

Once an account is registered with a YubiKey, the OTPs for that account can be generated via Yubico Authenticator on ANY device. For example, suppose you have Yubico Authenticator on both your desktop and mobile devices. If you register an account with a YubiKey on your mobile device, you can generate OTPs with that key on your desktop and vice versa.

When adding a new OATH account to a YubiKey, you are given the option to "require touch" as a means of user presence. With the touch requirement enabled, you must manually initiate the OTP calculation in Yubico Authenticator and touch (or scan) your YubiKey for each OTP you wish to generate. If you do not enable the touch requirement, the

YubiKey will begin generating TOTPs once it is connected to your device, and these TOTPs will be visible next to the account name in Yubico Authenticator. Counter-based HOTPs must be generated manually regardless of the touch requirement.

To add an account, do the following:

1. Plug your YubiKey into your device. On desktop and Android devices, click the menu icon in the upper left corner of the app and select **Accounts**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

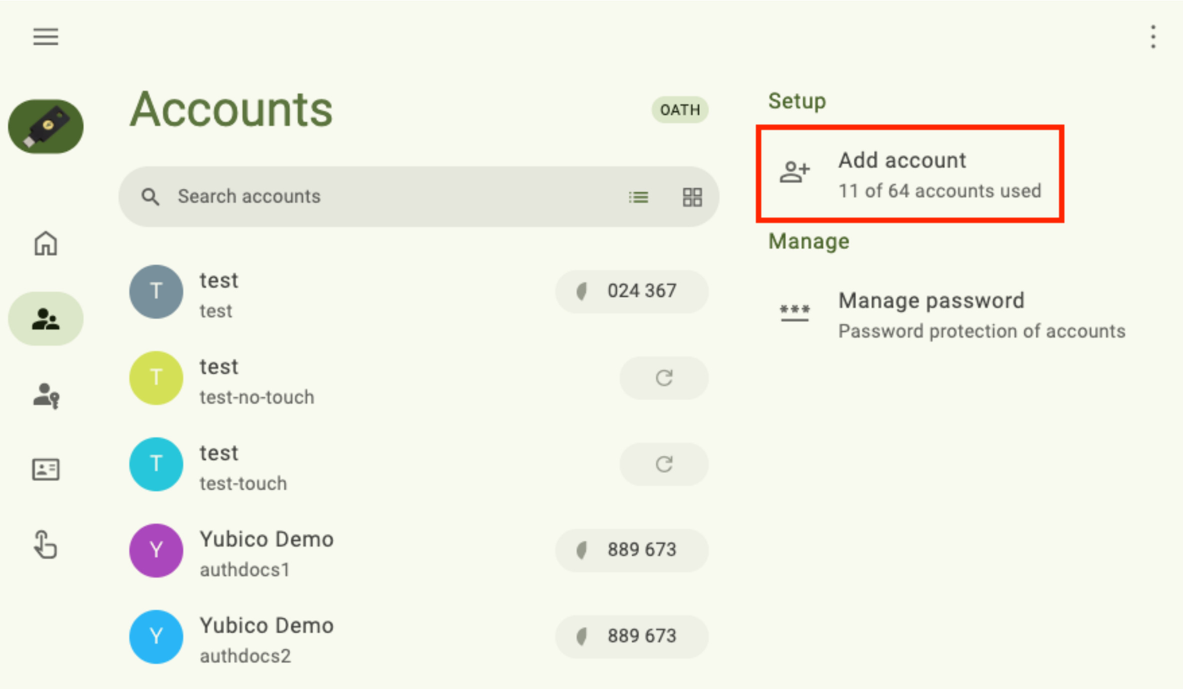
   To connect via NFC on iOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.

   Note: Lightning is currently the only supported *physical* connection type for iOS and iPadOS devices. NFC wireless connections are supported on iOS but not on iPadOS. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

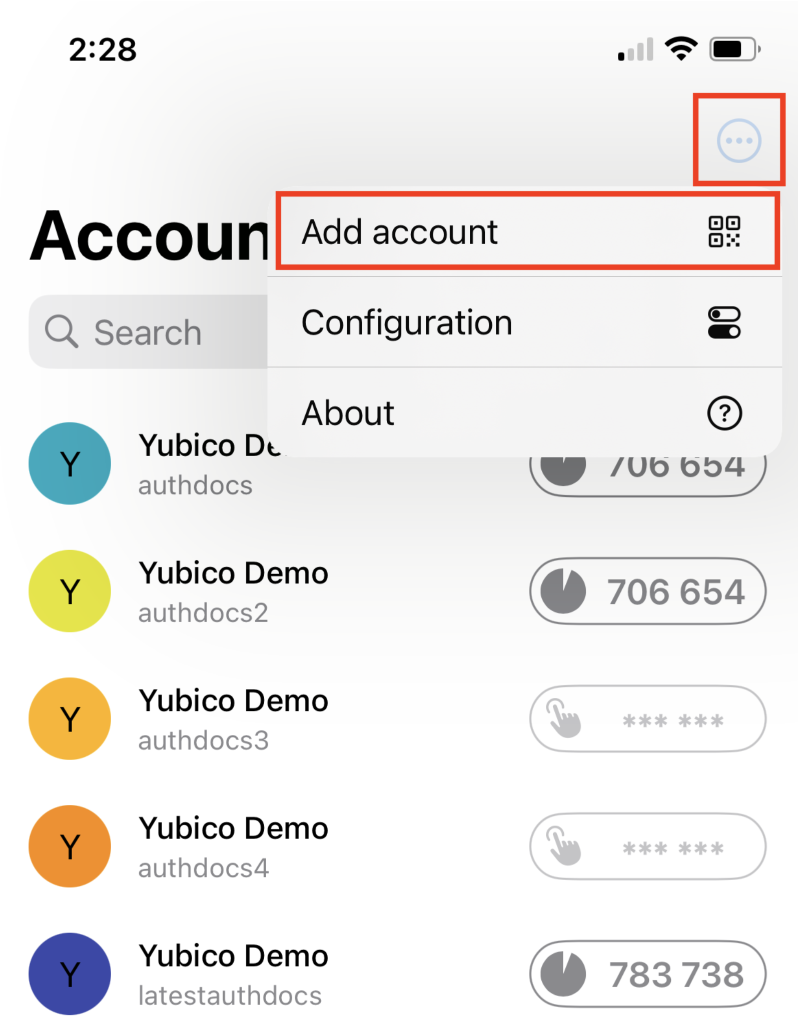
2. Enter your *OATH password* if prompted and click **Unlock** (on desktop and Android) or **Ok** (on iOS/iPadOS). For NFC connections on Android or iOS, scan your YubiKey again when prompted.

3. Click **Add account**.

   On desktop and Android, this is located under **Setup**. To find the **Setup** menu in a narrow app window, click the three dots in the upper right corner of the app.

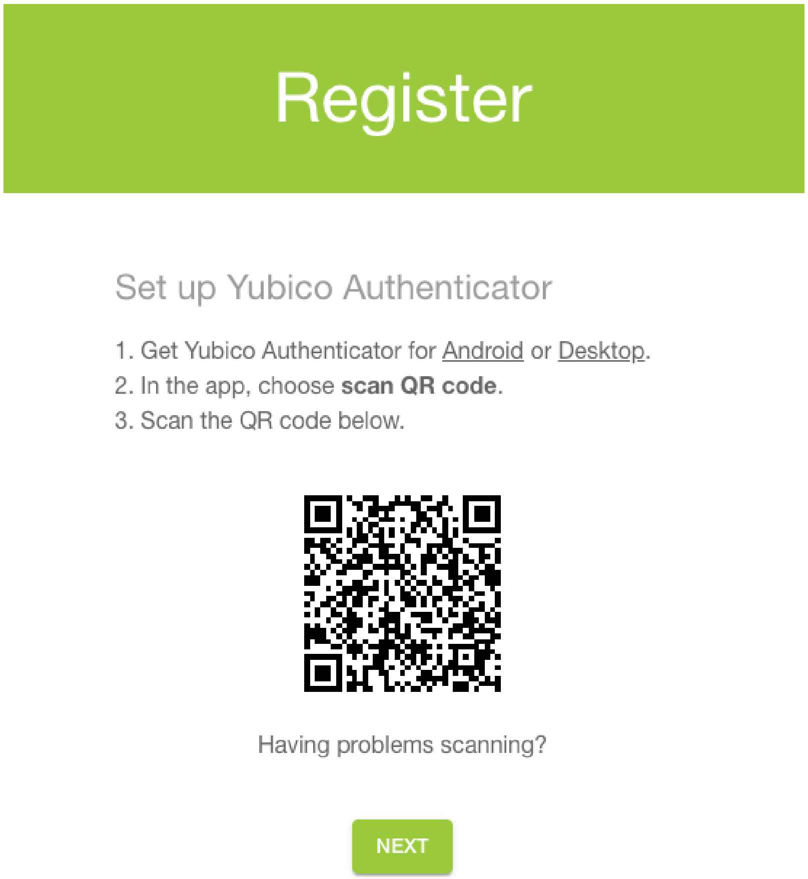


   On iOS/iPadOS, click the three dots in the upper right corner of the app to find **Add account**.



4. Locate the QR code or secret key information in the site/account/service you wish to register with.

   This typically requires logging into your account and going to “settings” or “security” > “two-factor authentication” or “two-step verification” > “register an authenticator application” (or similar). See the Works with YubiKey catalog for information on where to find these settings for your particular site/service/application.



Register

Set up Yubico Authenticator

1. Get Yubico Authenticator for Android or Desktop.
2. In the app, choose **scan QR code**.
3. Scan the QR code below.

Having problems scanning?

Important: Yubico recommends registering at least one backup key for each account to preserve access in the event of a loss of your primary YubiKey. Make a copy of the QR code or secret key information; you will need it when registering a second YubiKey.

5. To add an account via QR code on desktop, ensure the QR code, which is provided by the site/service/application you are registering with, is completely visible on your screen (no obstructions) and click **Scan QR code**.

   For Android and iOS/iPadOS, point your camera at the QR code to scan (if the QR code is on a separate screen/device). Alternatively, on Android, take a screenshot of the QR code on your Android device, click **Read from file**, and select the screenshot.

On the **Add account** screen, make edits to the **Issuer** (site/service/application) and/or **Account name** (your username) if needed, click **Require touch** to enable the *touch requirement* (optional), and then click **Save**. For NFC connections on Android and iOS, tap your key to complete the operation.

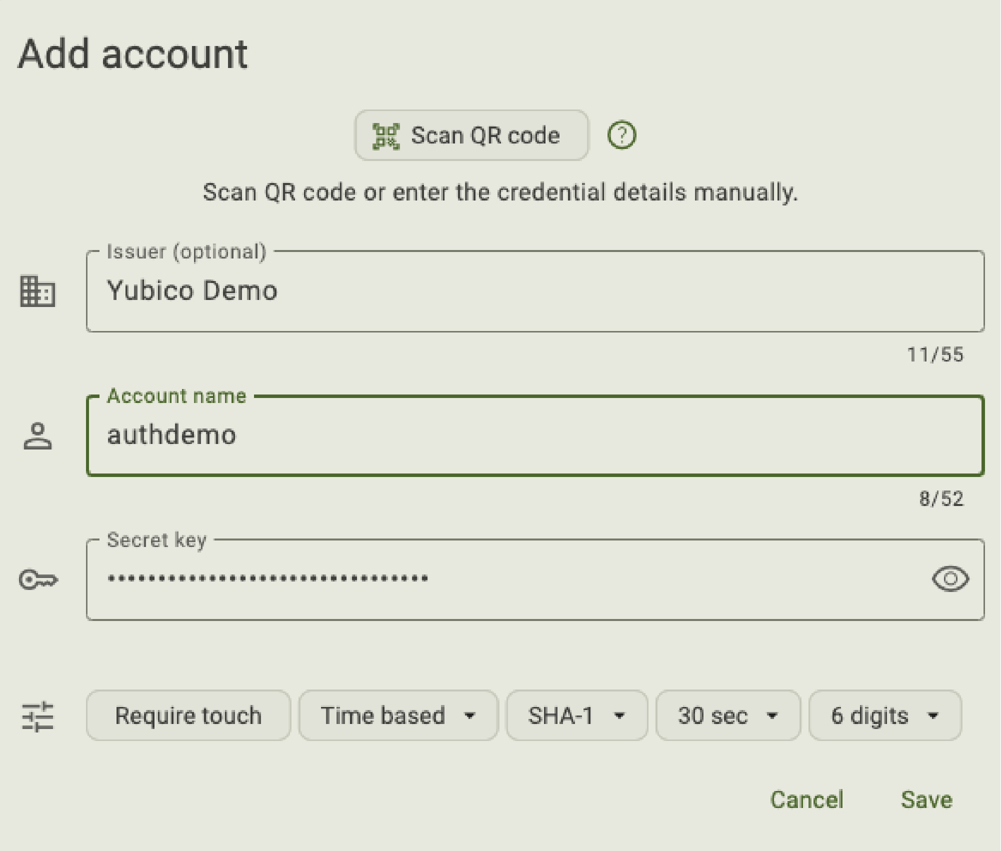
Note: macOS requires permission to record your screen in order to scan the QR code. You will likely be prompted to set up these permissions the first time you attempt the QR scan, but you can also *toggle them in System Settings* at any time.

---

6. To add an account manually, proceed to entering the account details (desktop and Android). On iOS/iPadOS, click **Enter manually** first to reach the **Add account** screen.

   On the **Add account** screen, enter an **Issuer** (the site/service/application), **Account name** (your username), and **Secret key**. Underneath these fields, select the appropriate OATH options for type of OTP, algorithm, period, and OTP length. **These settings must match those specified by the site/service/application**. If they do not, authentication will fail because the OTPs generated by the YubiKey will not match those generated by the relying party.

   Click or toggle **Require touch** to enable the *touch requirement* (optional) and then **Save**. For NFC connections on Android and iOS, tap your key to complete the operation.



Add account

Scan QR code or enter the credential details manually.

Issuer (optional): Yubico Demo
11/55

Account name: authdemo
8/52

Secret key: ••••••••••••••••••••••••••••••••

7. The site/service/application you are registering the YubiKey with will likely ask for an OTP code to complete the registration. If you did not check “require touch” during setup and the OTP type is TOTP, enter the OTP listed next to the account in Yubico Authenticator. If you enabled the touch requirement or the OTP type is HOTP, click on the account name (on desktop and Android, this opens the **Actions** section), select **Calculate**, and touch or scan the YubiKey when prompted. Enter the OTP that is generated.

8. Your YubiKey is now registered for OATH authentication. To register a backup YubiKey with your account,

repeat this process using the **same** QR code/account information.

For TOTPs, the primary YubiKey and backup YubiKey will always generate the same OTPs, which allows you to use the keys interchangeably.

HOTPs are more complicated. Given that HOTPs use a counter that is incremented with each OTP generated, the primary and backup YubiKeys will become out of sync unless OTPs are generated on both keys at the same time.

Tip: *Pin* frequently used OATH accounts to the top of the screen for easier access. Desktop and Android tablet devices can also use their wider screens to display more OATH accounts by changing the *screen layout*.

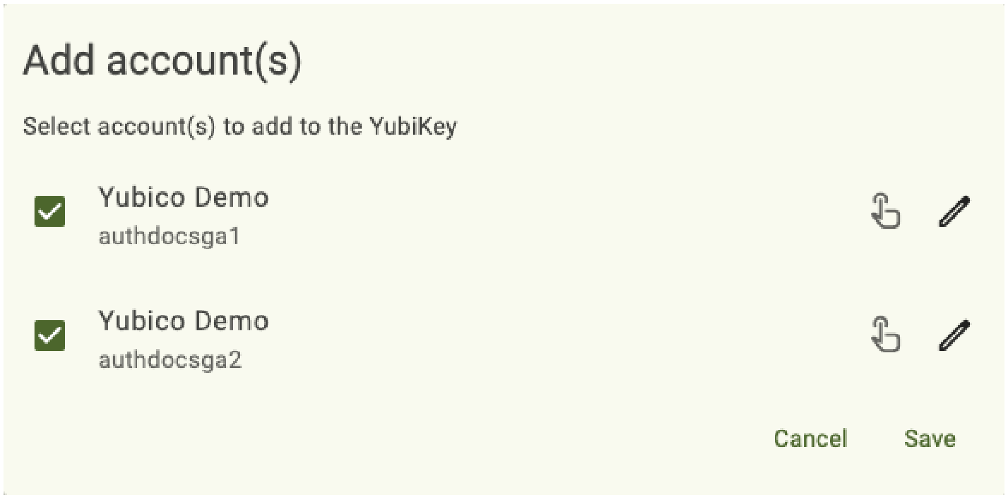
9. Bonus step: Yubico highly recommends setting an *OATH application password* if you haven't already done so. An OATH password improves the security of your YubiKey in that it blocks access to your YubiKey's OATH functionality until the correct password is entered. In the event that your YubiKey is lost or stolen, anyone in possession of your key could not generate OATH OTP codes or see any OATH account details in Yubico Authenticator without entering your OATH password.

6.2.1 Importing OATH account credentials from Google Authenticator

If you'd like to transfer existing OATH two-factor authentication accounts from Google Authenticator to a YubiKey for use in Yubico Authenticator, you can do so via the "Export accounts" feature in Google Authenticator.

To get started, follow the instructions in the Google Help docs to create a QR code containing your account credentials through **Transfer accounts** -> **Export accounts**. If you have more than one account in Google Authenticator, you'll be able to select which ones you'd like to transfer.

Once you have generated the QR code, follow the instructions in *Adding a new account* to connect your YubiKey to your device and scan the QR code in Yubico Authenticator. After scanning, Yubico Authenticator will allow you to rename the accounts and set their touch policy. Also note that QR codes from Google Authenticator are only compatible with the desktop and Android versions of Yubico Authenticator–if you try to scan the QR code with Yubico Authenticator for iOS/iPadOS, the operation will fail. However, once the accounts have been transferred to a YubiKey from Google Authenticator, you will be able to generate and display OATH two-factor authentication codes in Yubico Authenticator on any device, iOS/iPadOS included.



Add account(s)

Select account(s) to add to the YubiKey

☑ Yubico Demo
authdocsga1

☑ Yubico Demo
authdocsga2

6.3 Authenticating with OATH and Yubico Authenticator

Once an OATH account has been *added* to a YubiKey, that key can be used with Yubico Authenticator to generate OTP codes for two-factor authentication.

To authenticate with OATH, do the following:

1. Begin the login process for your account. This typically requires entering a username and password.
2. Launch Yubico Authenticator and plug your YubiKey into your device. On desktop and Android, click the menu icon in the upper left corner of the app and select **Accounts**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

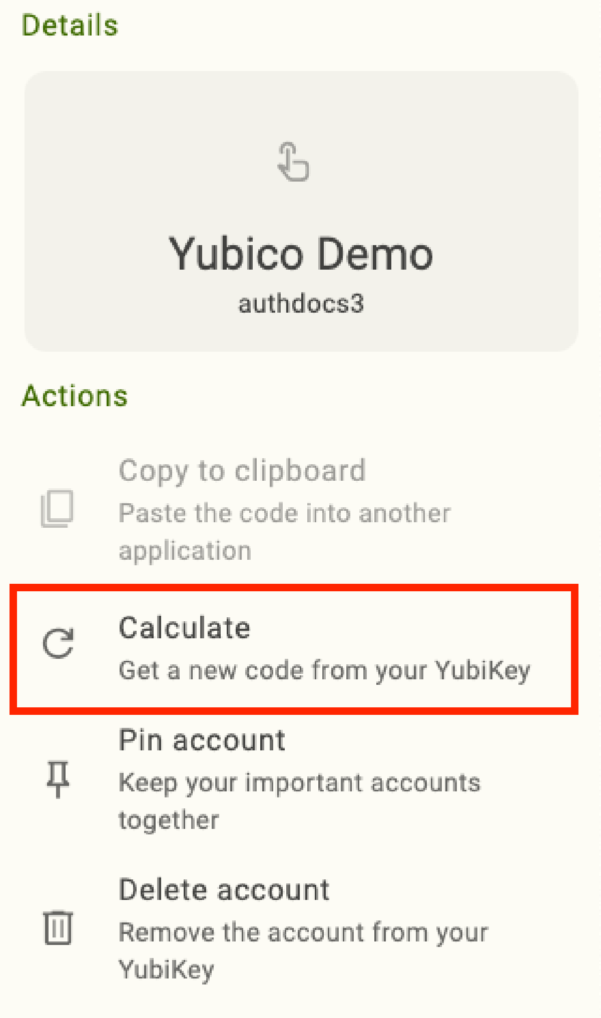
   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

   To connect via NFC on iOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.

   Note: Lightning is currently the only supported *physical* connection type for iOS and iPadOS devices. NFC wireless connections are supported on iOS but not on iPadOS. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

3. Enter your *OATH password* if prompted and click **Unlock** (on desktop and Android) or **Ok** (on iOS/iPadOS). For NFC connections on Android or iOS, scan your YubiKey again when prompted.
4. Locate your account on the **Accounts** screen. Next to the account name, you will see either an OTP code or a touch icon.

   If the touch icon is present, click on the account name, select **Calculate**, and touch or scan the YubiKey when prompted to generate the OTP code. Time-based OTPs are only valid for a short period of time (often 30 seconds). Once this period has lapsed (in other words, the OTP has expired), the OTP code becomes greyed out. To perform authentication again, you will need to repeat this process to generate a new code.



Details

Yubico Demo

authdocs3

Actions

Copy to clipboard
Paste the code into another application

Calculate
Get a new code from your YubiKey

Pin account
Keep your important accounts together

Delete account
Remove the account from your YubiKey

Next, click on the account in Yubico Authenticator and select **Copy to clipboard** (desktop and Android) or **Copy** (iOS/iPadOS).

Note: On desktop devices, you can speed up this process by double-clicking or long-clicking on the account name (to perform a long click, press and hold the mouse button for a couple of seconds). For accounts whose OTPs do not require user-initiated calculation, this action copies the OTP to the clipboard. For accounts whose OTPs *do* require user-initiated calculation, the double/long click will perform the calculation *and* the copy action. If touch is required, you will be prompted by Yubico Authenticator after clicking. You can also perform the same operation by selecting the account and typing command+C (macOS) or Ctrl+C (Windows/Linux).

On iOS/iPadOS devices, touch and hold (long-click) the account name to copy the OTP to clipboard (and perform the calculation if applicable). On Android devices, touch and hold the account name to copy the OTP to clipboard. If user-initiated OTP generation is required, you will have to perform the long click operation twice: first to perform the calculation and again to copy the OTP to clipboard.

5. Your account will prompt you for a code from your authenticator app. Paste (or type) the OTP from Yubico Authenticator and click **Sign In** (or similar).

6.4 Password protection

Yubico highly recommends setting an OATH application password. An OATH password improves the security of your YubiKey in that it blocks access to your key's OATH functionality until the correct password is entered. In the event that your YubiKey is lost or stolen, anyone in possession of your key could not generate OATH OTP codes or see any OATH account details in Yubico Authenticator without first entering your OATH password.

Once created, the OATH password can be:

- remembered/forgotten on a trusted device
- changed
- removed

Important: If you have forgotten your OATH password, the only way to change it is to *reset* the OATH application of your YubiKey to factory default settings, which will remove the password. Note that this will delete **ALL** OATH account credentials stored on the YubiKey, and you will no longer be able to generate OATH OTPs for those accounts with that key (we recommend registering at least one *backup YubiKey* with each account/service to maintain access for this reason). Once the OATH application has been reset, you can always add the accounts to your YubiKey again.

6.4.1 Desktop and Android

Create an OATH password

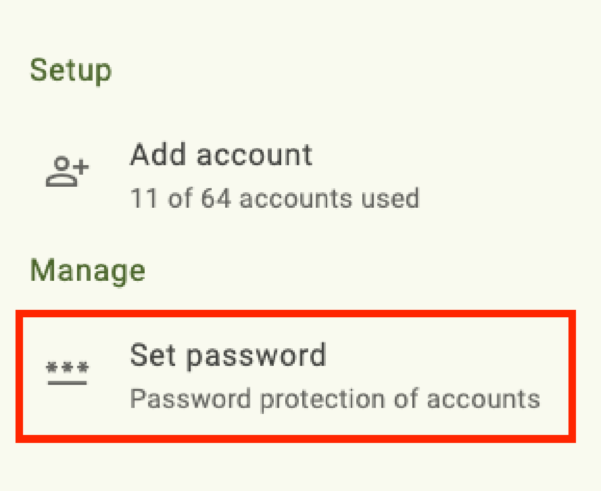
To create an OATH password for your YubiKey's OATH application, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Accounts**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

2. Click **Set password** under **Manage**.

   In a narrow app window, click the three dots in the upper right corner of the app to find the **Manage** menu.

3. In the **Set password** window, enter your new password. The password may contain letters, numbers, and special characters. Enter your password again to confirm and click **Save**.

For NFC connections on Android, tap your key to complete the operation.

Remember or forget an OATH password

Once the password has been created, you must enter it every time you want to access the **Accounts** features in Yubico Authenticator. However, you can bypass this requirement on trusted devices by enabling the "remember password" feature. This setting allows the Yubico Authenticator app to store your OATH password and automatically submit it to your YubiKey whenever you open the **Accounts** page. As this feature affects the app itself and not your YubiKey, you will need to enable it in the app on each device you wish to use it with.

Once a password is "remembered", it can also be "forgotten" (cleared from application memory) at any time. Updating or reinstalling the app will clear the remembered password from memory as well.

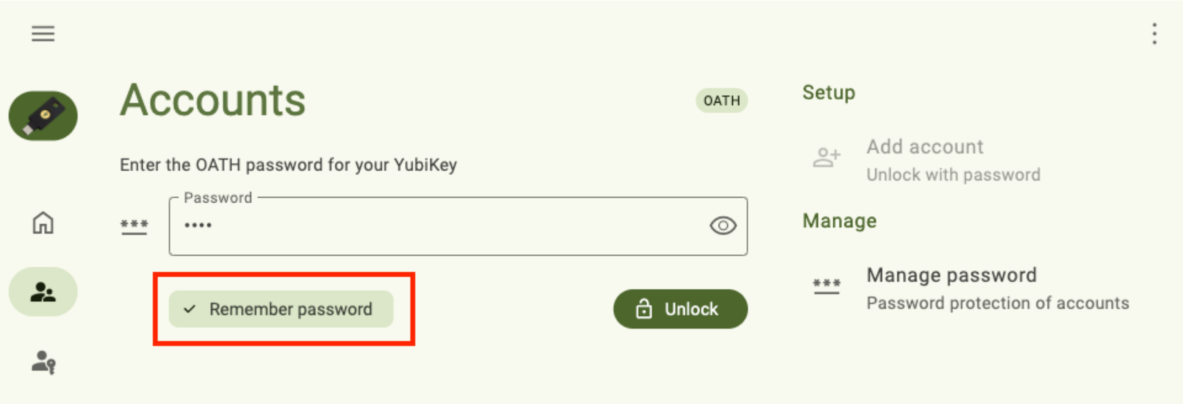
To remember or forget an OATH password on a particular device, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Accounts**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

2. To remember the password on your device, enter your OATH password when prompted, click **Remember password**, and then click **Unlock**. For NFC connections on Android, tap your key to complete the operation. The next time you connect your YubiKey to your device, you will not be prompted to enter the OATH password to view and manage OATH accounts.

   Enter the OATH password for your YubiKey

   Password: ••••

3. To forget a remembered password, click **Manage password** under **Manage**. In the **Manage password** window, enter your current password and click **Clear saved password**. For NFC connections on Android, scan your YubiKey again when prompted. The next time you connect your YubiKey to your device, you will be prompted to enter the OATH password to view and manage OATH accounts.

   In a narrow app window, click the three dots in the upper right corner of the app to find the **Manage** menu.

Change or remove an OATH pasword

To change or remove an OATH password, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Accounts**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

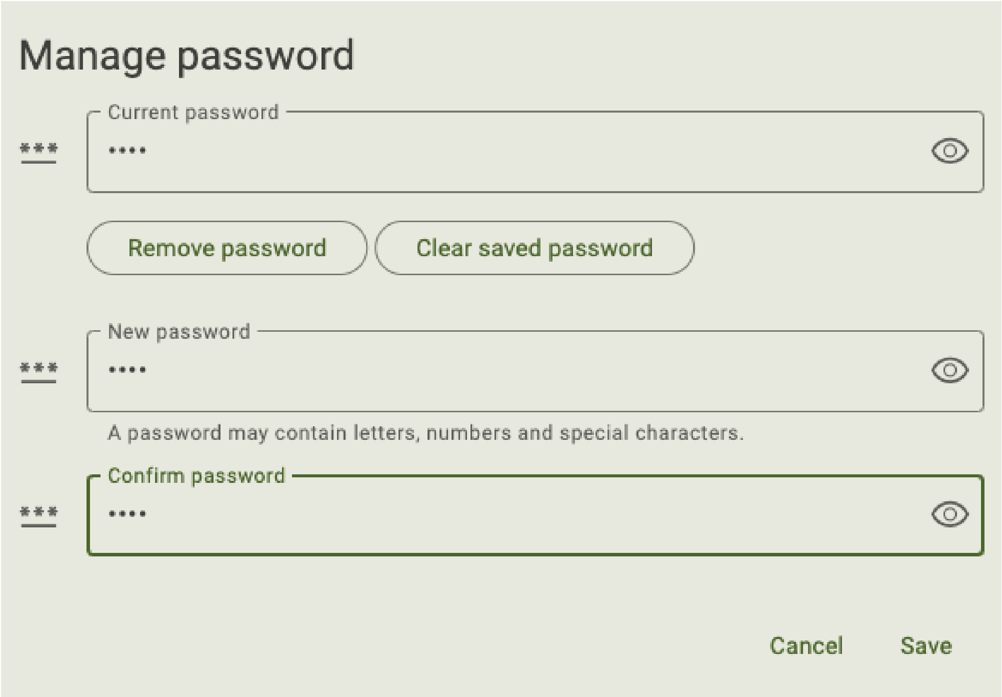
2. Click **Manage password** under **Manage**.

   In a narrow app window, click the three dots in the upper right corner of the app to find the **Manage** menu.

3. In the **Manage password** window, enter your current password.

4. To remove the password, click **Remove password**. For NFC connections on Android, tap your key to complete the operation. Once removed, a new password can be set at any time.

5. To change a password, enter a new password in the box provided. Enter the new password again to confirm and click **Save**. For NFC connections on Android, tap your key to complete the operation.



Manage password

Current password: ••••

New password: ••••

A password may contain letters, numbers and special characters.

Confirm password: ••••

6.4.2 iOS/iPadOS

Create an OATH password

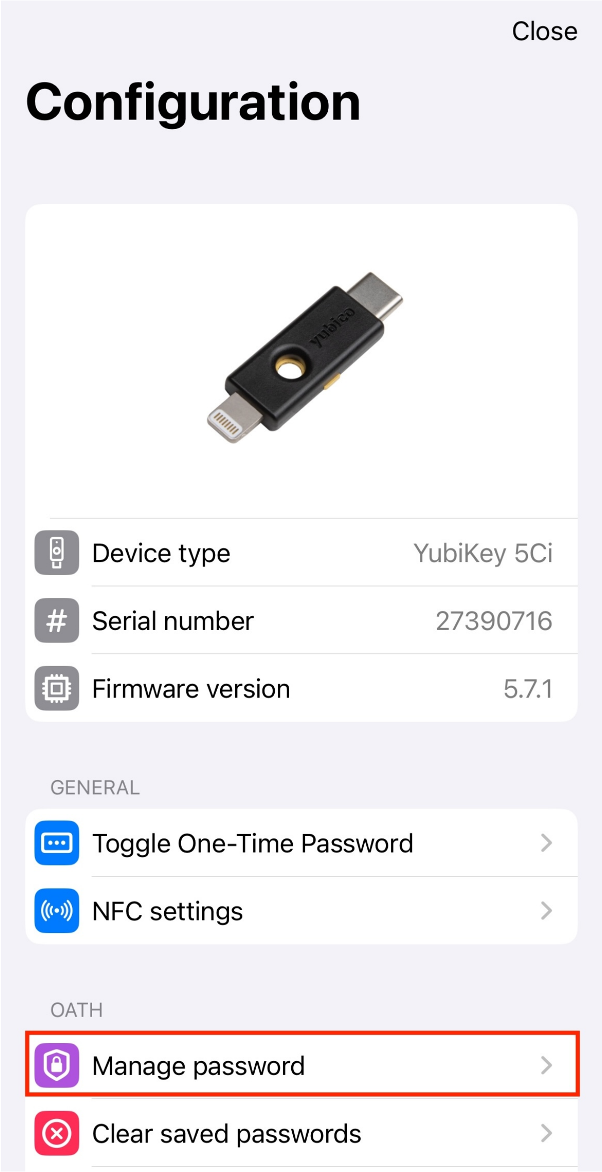
To create an OATH password, do the following:

1. Plug your YubiKey into your device and select **Accounts**.

   To connect via NFC on iOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.

Note: Lightning is currently the only supported *physical* connection type for iOS and iPadOS devices. NFC wireless connections are supported on iOS but not on iPadOS. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

2. Click the three dots in the upper right corner of the app and select **Configuration**.
3. On the **Configuration** screen, select **Manage password** under the **OATH** section.



Close

Configuration

Device type YubiKey 5Ci

Serial number 27390716

Firmware version 5.7.1

GENERAL

Toggle One-Time Password

NFC settings

OATH

Manage password

Clear saved passwords

4. Click **Set password** and enter your new password. The password may contain letters, numbers, and special characters. Enter your password again to confirm and click **Set**.

   For NFC connections, tap your key to complete the operation.

Remember or forget an OATH password

Once the password has been created, you must enter it every time you want to access the **Accounts** features in Yubico Authenticator. However, you can bypass this requirement on trusted devices by enabling the "remember password" feature. This setting allows the Yubico Authenticator app to store your OATH password and automatically submit it to your YubiKey whenever you open the **Accounts** page. As this feature affects the app itself and not your YubiKey, you will need to enable it in the app on each device you wish to use it with.

Once a password is "remembered", it can also be "forgotten" (cleared from application memory) at any time. Updating or reinstalling the app will clear the remembered password from memory as well.

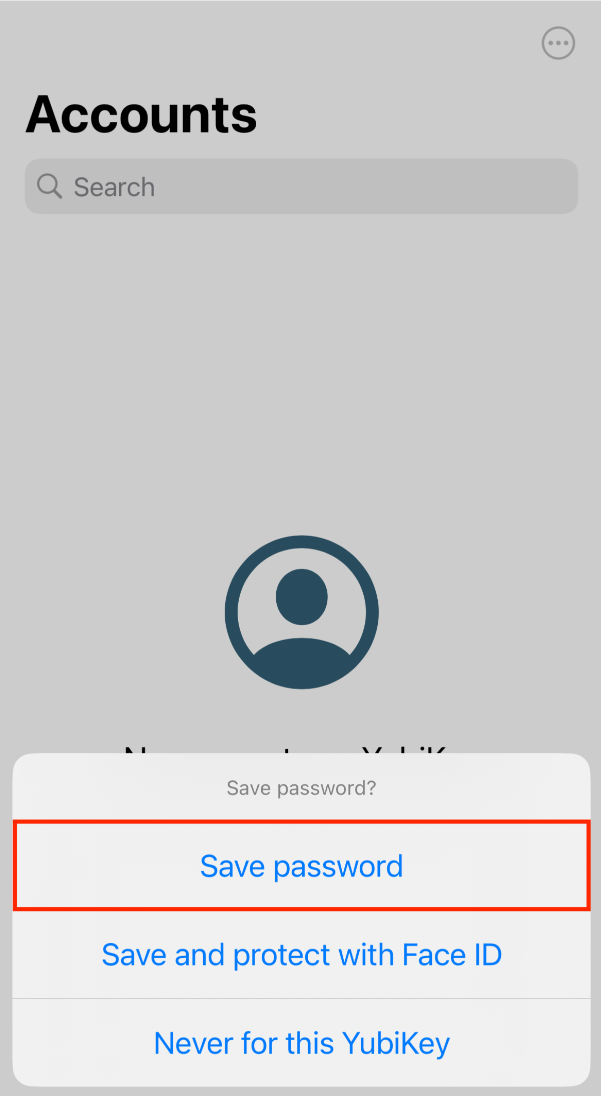
To remember or forget an OATH password on a particular device, do the following:

1. Plug your YubiKey into your device and select **Accounts**.

   To connect via NFC on iOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.

   Note: Lightning is currently the only supported *physical* connection type for iOS and iPadOS devices. NFC wireless connections are supported on iOS but not on iPadOS. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

2. To remember the password on your device, enter your OATH password when prompted, scan the key again if connected via NFC, and click **Save password**. The next time you connect your YubiKey to your device, you will not be prompted to enter the OATH password to view and manage OATH accounts.



3. To forget a remembered password, click the three dots in the upper right corner of the app and select **Configuration**. Select **Clear saved passwords** under the **OATH** section. Click **Clear saved passwords** again and then **OK** to confirm the operation. The next time you connect your YubiKey to your device, you will be prompted to enter the OATH password to view and manage OATH accounts.

Change or remove an OATH password

To change or remove an OATH password, do the following:

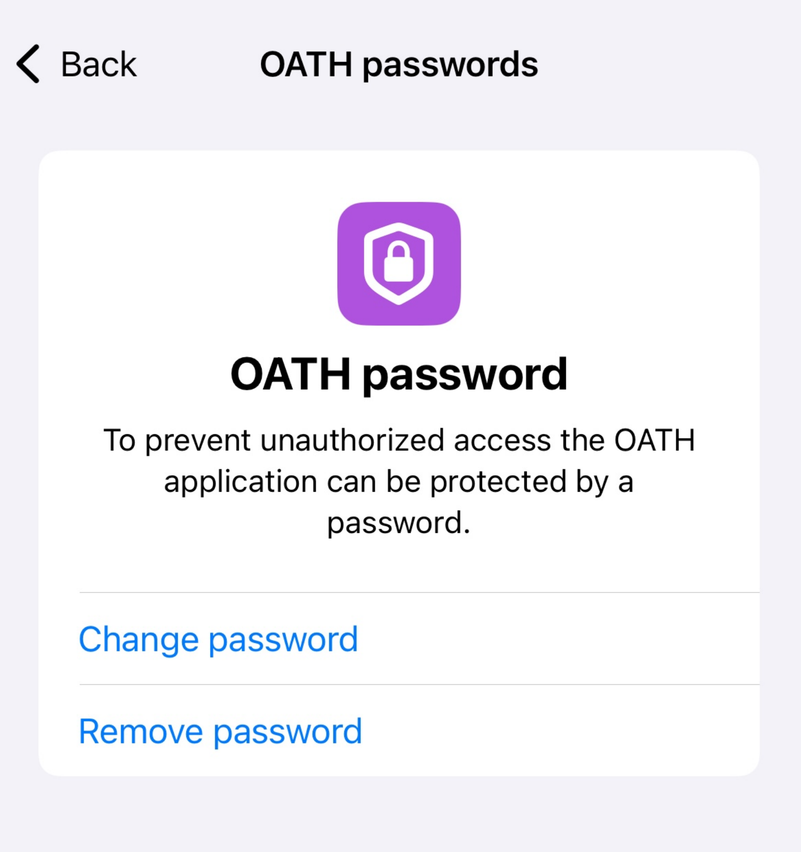
1. Plug your YubiKey into your device and select **Accounts**.

   To connect via NFC on iOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.

   Note: Lightning is currently the only supported *physical* connection type for iOS and iPadOS devices. NFC wireless connections are supported on iOS but not on iPadOS. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

2. Click the three dots in the upper right corner of the app and select **Configuration**. Select **Manage password** under the **OATH** section.

3. To remove the password, click **Remove password**. Enter your current password and click **Remove**. For NFC connections, tap your key to complete the operation. Once removed, a new password can be set at any time.



OATH password

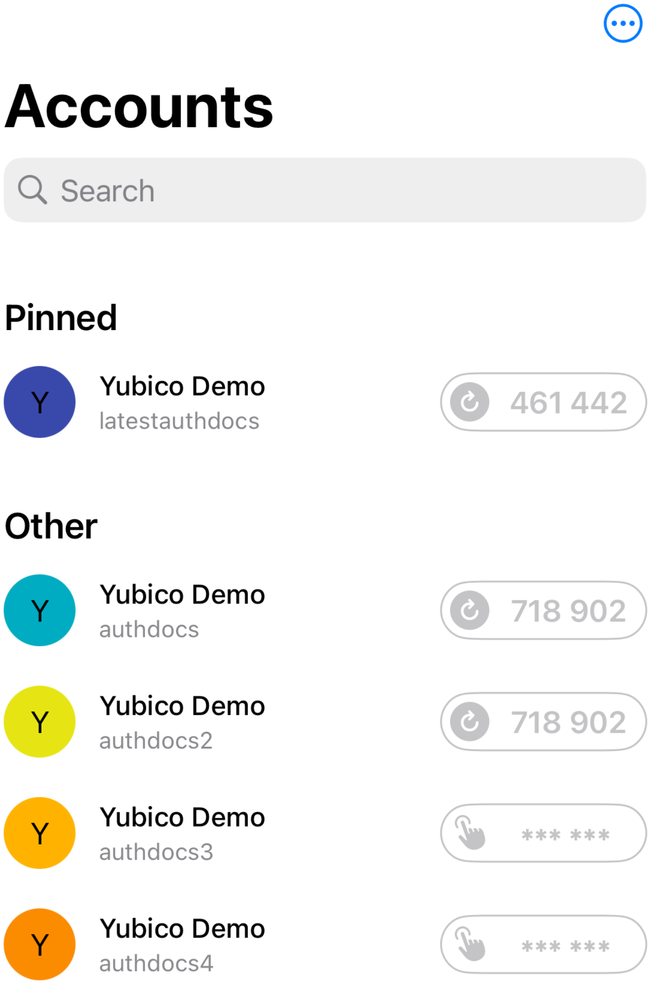
To prevent unauthorized access the OATH application can be protected by a password.

4. To change a password, click **Change password**. Enter your current password and the new password. Enter the new password again to confirm and click **Change**. For NFC connections, tap your key to complete the operation.

6.5 Pinning an account

Once an OATH account has been created, it will be listed on the **Accounts** screen in Yubico Authenticator whenever the YubiKey is connected to the device. If several accounts have been registered, not all of them will be visible in the app window at the same time, and you will need to scroll down the page to view the accounts at the bottom of the list. If some accounts are accessed more often than others, you may wish to pin them.

Pinning an account ensures that it remains at the top of the **Accounts** screen. If you have more than one account pinned, they will be ordered alphabetically (first by issuer, then by account name).



Accounts

Search

Pinned

Y Yubico Demo latestauthdocs 461 442

Other

Y Yubico Demo authdocs 718 902

Y Yubico Demo authdocs2 718 902

Y Yubico Demo authdocs3 *** ***

Y Yubico Demo authdocs4 *** ***

Tip: Desktop and Android tablet devices can also use their wider screens to display more OATH accounts by changing the *screen layout*.

To pin an account, do the following:

1. Plug your YubiKey into your device. On desktop and Android devices, click the menu icon in the upper left corner of the app and select **Accounts**.

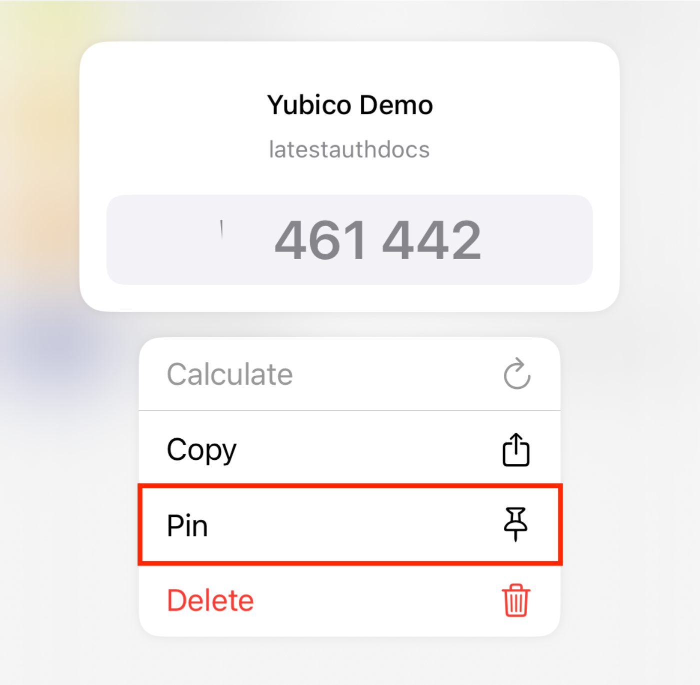
   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

To connect via NFC on iOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.

Note: Lightning is currently the only supported *physical* connection type for iOS and iPadOS devices. NFC wireless connections are supported on iOS but not on iPadOS. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

2. Enter your *OATH password* if prompted and click **Unlock** (on desktop and Android) or **Ok** (on iOS/iPadOS). For NFC connections on Android or iOS, scan your YubiKey again when prompted.
3. Select the account you wish to pin and click **Pin** (iOS/iPadOS) or **Pin account** (on desktop and Android, this is located under **Actions**). Once pinned, you can unpin the account at any time by clicking **Unpin** (iOS/iPadOS) or **Unpin account** (desktop and Android).



6.6 Renaming an account

Note: The OATH account renaming feature is only available for YubiKeys with firmware version 5.3.1 or later.

Once an OATH account has been added to your YubiKey, both the issuer and account name can be edited. To rename an OATH account, do the following:

1. Plug your YubiKey into your device. On desktop and Android, click the menu icon in the upper left corner of the app and select **Accounts**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

To connect via NFC on iOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.

Note: Lightning is currently the only supported *physical* connection type for iOS and iPadOS devices. NFC wireless connections are supported on iOS but not on iPadOS. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

2. Enter your *OATH password* if prompted and click **Unlock** (on desktop and Android) or **Ok** (on iOS/iPadOS). For NFC connections on Android or iOS, scan your YubiKey again when prompted.

3. Select the account you wish to rename and click **Rename** (iOS/iPadOS) or **Rename account** (on desktop and Android, this is located under **Actions**). Edit the **Issuer** and/or **Account name** as desired. Click **Save** to confirm the operation.

   For NFC connections on Android or iOS, tap your key to complete the operation.

6.7 Deleting an account

OATH accounts can be deleted from your YubiKey via Yubico Authenticator. Before deleting an account from a YubiKey, make sure you have either disabled two-factor authentication within your account settings with the site/service/application *or* added the account to a *backup YubiKey* to maintain access. (And make sure to test your backup key to verify it works.) This operation is not reversible–once an OATH account is deleted from your YubiKey, there is no way to recover the account credentials.

To delete an account, do the following:

1. Plug your YubiKey into your device. On desktop and Android, click the menu icon in the upper left corner of the app and select **Accounts**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

   To connect via NFC on iOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.

Note: Lightning is currently the only supported *physical* connection type for iOS and iPadOS devices. NFC wireless connections are supported on iOS but not on iPadOS. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

2. Enter your *OATH password* if prompted and click **Unlock** (on desktop and Android) or **Ok** (on iOS/iPadOS). For NFC connections on Android or iOS, scan your YubiKey again when prompted.

3. Select the account you wish to delete and click **Delete** (iOS/iPadOS) or **Delete account** (on desktop and Android, this is located under **Actions**). Click **Delete** to confirm the operation.

   For NFC connections on Android or iOS, tap your key to complete the operation.

6.8 Custom icons

Note: Custom icons are only available for Yubico Authenticator for Desktop and Android.

When viewing *OATH accounts* on a YubiKey within Yubico Authenticator, each account is listed with a colored icon that contains the first letter of the issuer by default. Similarly, *Passkeys* are listed with a default Passkey icon.

To make OATH accounts and Passkeys more easily distinguishable from one another, custom icons can be uploaded and used in Yubico Authenticator. For example, with custom icons, instead of seeing the default "D" icon next to an OATH account for Docker, an icon containing the Docker logo and colors would be shown. For a Microsoft Passkey, an icon with the Microsoft logo and colors would be shown in place of the default Passkey icon.

Icon packs must be in the Aegis Icon Pack format. Feel free to use a pre-built icon pack from Aegis or create your own.

To upload an icon pack to Yubico Authenticator on desktop or Android, do the following:

1. Download a pre-built icon pack from Aegis or create your own.
2. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Home**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.
3. Select **Settings** under **Application**. On the **Settings** screen, click **Custom icons**.

   In a narrow app window, click the three dots in the upper right corner of the app to find the **Application** menu.
4. In the **Custom icons** window, click **Load icon pack**. Select the file containing the icons (for example, aegis-icons.zip).
5. Once loaded, any OATH account or Passkey with an issuer that is supported by the icon pack will display the custom icon. To delete the icon pack, click the trash can icon in the **Custom icons** window. Similarly, to update the icon pack, click **Replace icon pack** and select the new file.

CHAPTER

SEVEN

PASSKEYS: FIDO2

Important: Yubico Authenticator's FIDO2 functionality is only available for FIDO2-certified YubiKeys. This includes YubiKey 5 Series (standard, FIPS, and CSPN), YubiKey Bio Series, and Security Key Series. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

Passkeys are credentials that allow you to perform passwordless authentication to accounts or services using the FIDO2 standard. Passkeys are created by relying parties (the sites and services that use them for authentication).

Passkeys can be stored on FIDO2-certified YubiKeys, and Yubico Authenticator helps you manage them. For more information on which services support FIDO2 authentication and an overview of their unique security key registration processes, see the Works with YubiKey catalog.

Non-passkey FIDO2 credentials can also be stored on YubiKeys, but they are not discoverable and cannot be listed and managed on the **Passkeys** page.

The Passkeys feature of Yubico Authenticator allows you to:

- *View and delete passkeys stored on a YubiKey*.
- *Create or change a YubiKey's FIDO2 PIN*.
- *Enable Enterprise Attestation (EA) and check a YubiKey's EA status*.

7.1 Creating and managing the FIDO2 PIN

Before you can register a YubiKey for passwordless FIDO2 authentication with an account or service (which means a passkey credential is created, linked to a specific account, and stored on the YubiKey), you must create a FIDO2 PIN.

If you have not created a PIN via Yubico Authenticator prior to your first registration attempt with an account/service, you will be prompted to do so during the registration process. Once the PIN is created, you will have to provide it during each subsequent registration with other accounts and services.

For YubiKey Bio Series Multi-protocol Edition keys, the FIDO2 application and the PIV application share a PIN. Therefore, performing the "Change PIN" action on the **Passkeys**, **Fingerprints**, or **Certificates** screen modifies the same PIN.

Warning: The YubiKey provides a total of eight (8) attempts to enter the correct current PIN during a PIN change attempt or registration attempt. After three (3) incorrect attempts in a row, that key must be removed and reinserted into your device. After 8 incorrect attempts, the FIDO2 application becomes blocked and must be *reset*. Entering the PIN correctly resets the PIN attempt counter back to 8.

For more information on the FIDO2 PIN, see Yubico's knowledge base article, Understanding YubiKey PINs.

7.1.1 Creating a FIDO2 PIN on desktop and Android

To create a FIDO2 PIN on desktop and Android devices, do the following:

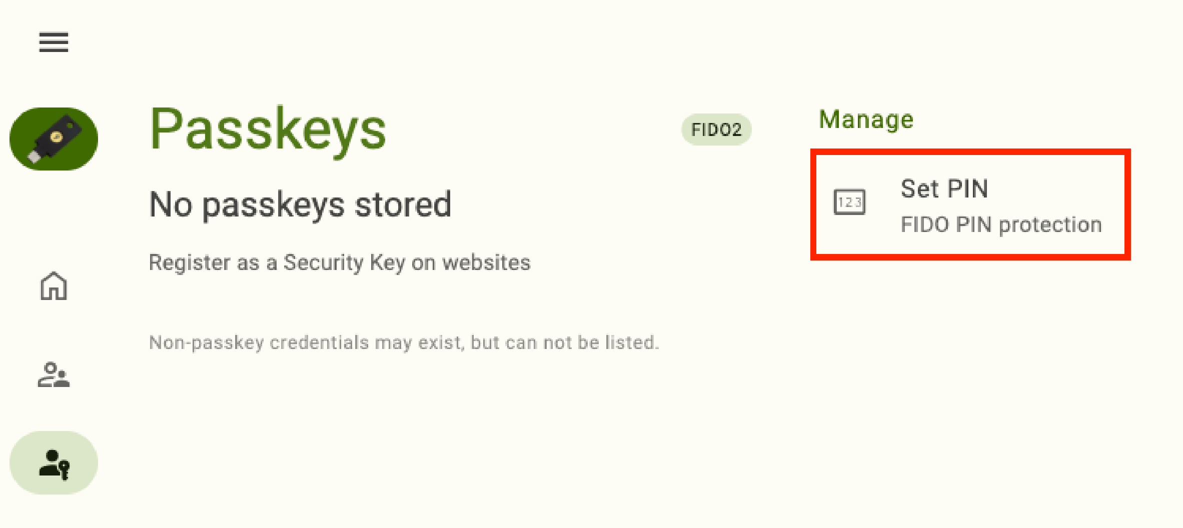
1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Passkeys**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

2. Click **Set PIN** under **Manage**.

   To find the **Manage** menu in a narrow app window, click the three dots in the upper right corner of the app.



Passkeys

No passkeys stored

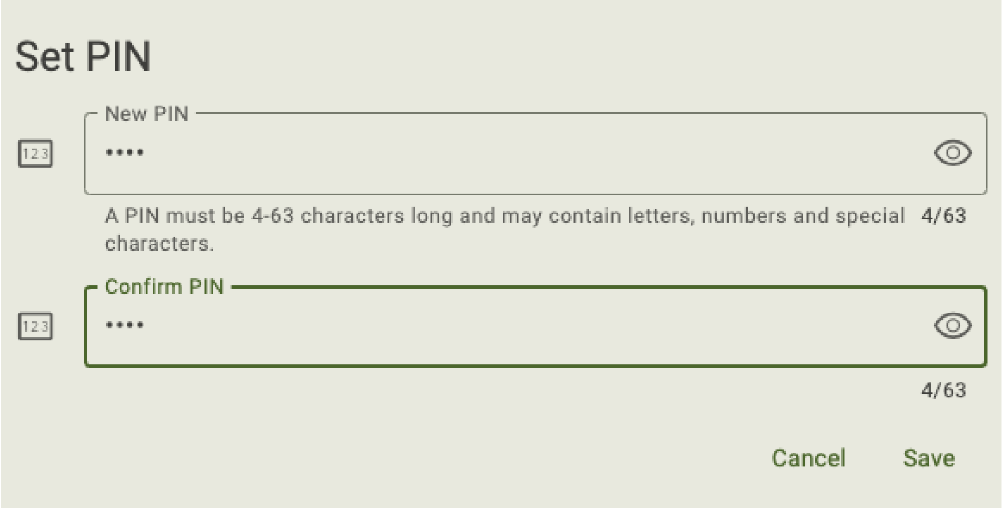
Register as a Security Key on websites

Non-passkey credentials may exist, but can not be listed.

3. In the **Set PIN** window, enter your new PIN.

Note: PIN requirements depend on your YubiKey's model, firmware version, and *PIN complexity* enforcement.

4. Enter the new PIN again to confirm and click **Save**. For NFC connections on Android, tap your key to complete the operation.



Set PIN

New PIN

••••

A PIN must be 4-63 characters long and may contain letters, numbers and special characters. 4/63

Confirm PIN

••••

4/63

7.1.2 Creating a FIDO2 PIN on iOS/iPadOS

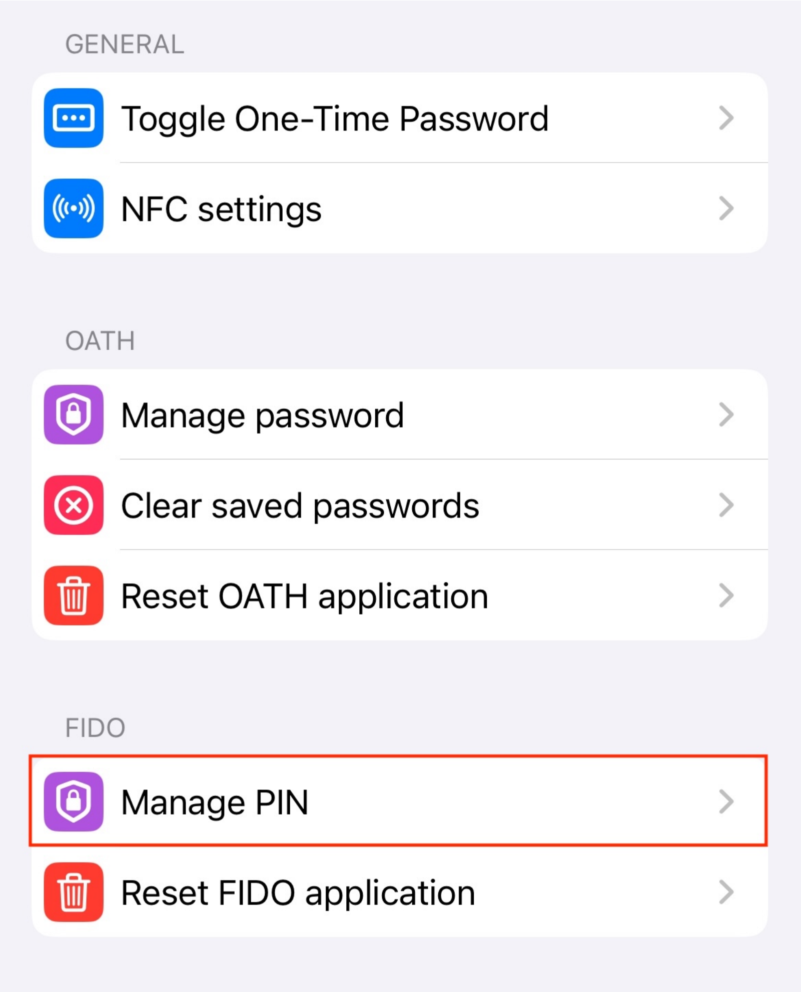
To create a FIDO2 PIN on iOS/iPadOS devices, do the following:

1. Plug your YubiKey into your device.

   To connect via NFC on iOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.

   Note: Lightning is currently the only supported *physical* connection type for iOS and iPadOS devices. NFC wireless connections are supported on iOS but not on iPadOS. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

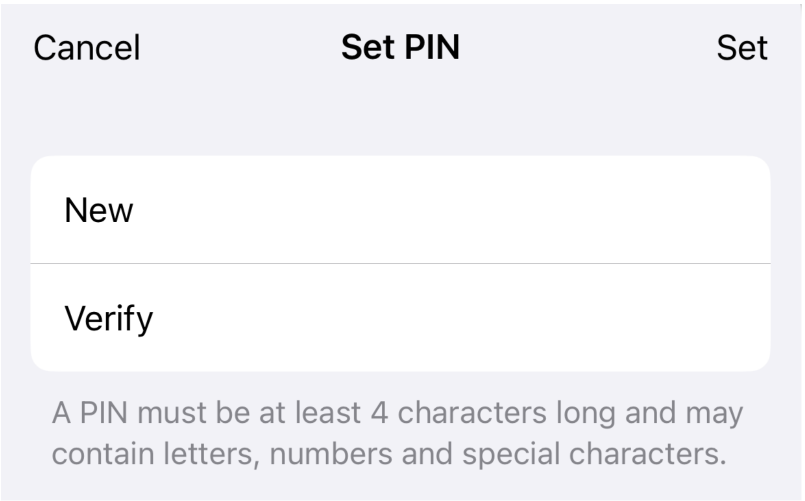
2. Click the three dots in the upper right corner of the app and select **Configuration**. Select **Manage PIN** under the **FIDO** section.



3. In the **FIDO PIN** window, click **Set PIN**. Enter your new PIN.

Note: PIN requirements depend on your YubiKey's model, firmware version, and *PIN complexity* enforcement.

4. Enter the new PIN again to confirm and click **Set**. For NFC connections on iOS, scan your key when prompted to complete the operation.



A PIN must be at least 4 characters long and may contain letters, numbers and special characters.

7.1.3 Changing the FIDO2 PIN on desktop and Android

To change the FIDO2 PIN on desktop and Android devices, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Passkeys**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

2. Enter your FIDO2 PIN and click **Unlock**. For NFC connections on Android, tap your key to complete the operation.

3. Click **Change PIN** under **Manage**.

   To find the **Manage** menu in a narrow app window, click the three dots in the upper right corner of the app.

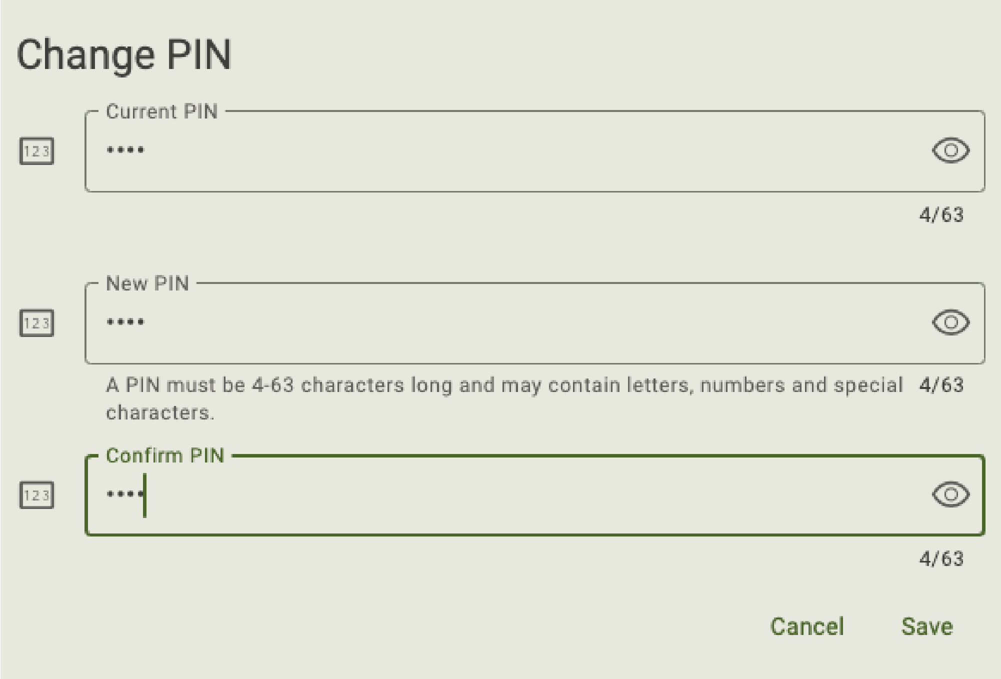
4. In the **Change PIN** window, enter your current PIN.

   If you have forgotten your current PIN, the only way to change it is to *reset* the FIDO2 application of your YubiKey to factory default settings (which will remove the PIN). Note that this will delete **ALL** *fingerprints* and passkeys stored on the YubiKey, and you will no longer be able to access those accounts with that key (we recommend registering at least one *backup YubiKey* with each account/service to maintain access). Once reset, you can always re-register your key with those same accounts and services.

5. Enter your new PIN.

   Note: PIN requirements depend on your YubiKey's model, firmware version, and *PIN complexity* enforcement.

6. Enter the new PIN again to confirm and click **Save**. For NFC connections on Android, tap your key to complete the operation.



Change PIN

Current PIN: ••••

4/63

New PIN: ••••

A PIN must be 4-63 characters long and may contain letters, numbers and special characters.

4/63

Confirm PIN: ••••

4/63

7.1.4 Changing the FIDO2 PIN on iOS/iPadOS

To change a FIDO2 PIN on iOS/iPadOS devices, do the following:

1. Plug your YubiKey into your device.

   To connect via NFC on iOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.

   Note: Lightning is currently the only supported *physical* connection type for iOS and iPadOS devices. NFC wireless connections are supported on iOS but not on iPadOS. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

2. Click the three dots in the upper right corner of the app and select **Configuration**. Select **Manage PIN** under the **FIDO** section.

3. In the **FIDO PIN** window, click **Change PIN**. Enter your current PIN followed by your new PIN.

   Note: PIN requirements depend on your YubiKey's model, firmware version, and *PIN complexity* enforcement.

4. Enter the new PIN again to confirm and click **Set**. For NFC connections on iOS, scan your key when prompted to complete the operation.

7.2 Viewing and deleting passkeys

Note: Passkeys can be managed on Yubico Authenticator for Desktop and Android only.

With Yubico Authenticator, you can view all passkeys stored on a YubiKey. Passkeys can only be deleted with the app; you cannot create or modify them with Yubico Authenticator.

Warning: Once a passkey is deleted, you cannot use the YubiKey to log into an account or service for which the passkey was registered. To re-register a YubiKey, you must be able to log into that account/service with an alternate credential (we recommend registering at least one *backup YubiKey* with each account/service for this reason).

To view and/or delete a passkey stored on your YubiKey, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Passkeys**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

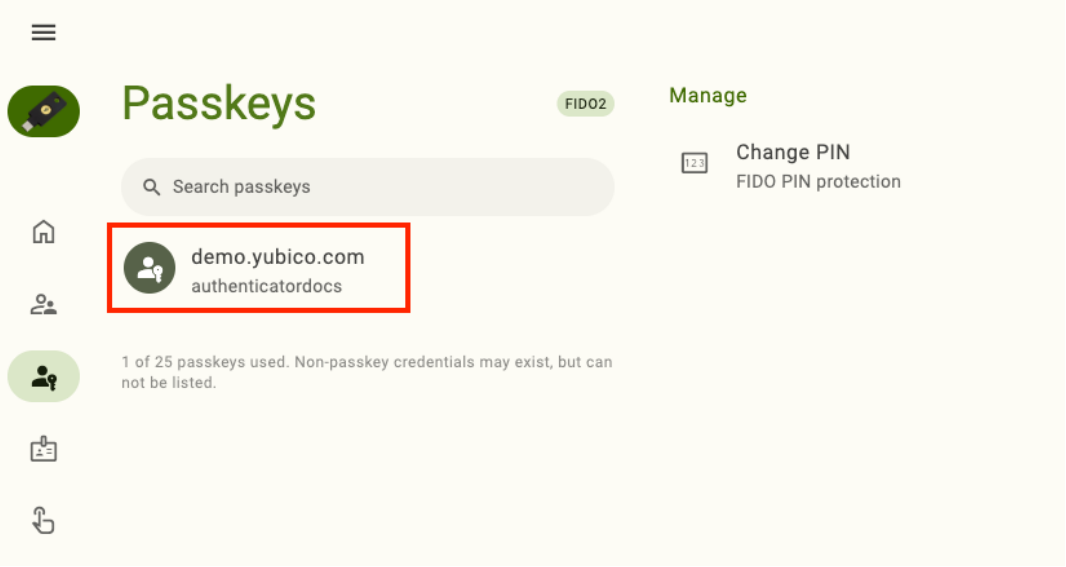
   To connect via NFC on Android, tap and hold your YubiKey on the back of your device to scan. Reading passkeys on a YubiKey is quite slow, and depending on how many are stored on your key, it could take up to several seconds for the NFC sensor to read the passkey information. You must maintain constant contact with the NFC sensor until all passkeys are read.

2. Enter your FIDO2 PIN and click **Unlock**. For NFC connections on Android, tap your key to complete the operation. All passkeys stored on your YubiKey will be listed under **Passkeys**.

   To view properties including RP ID, Display Name, User Name, User ID, and Credential ID for a specific passkey, click on it to open the **Details** section. To copy any of these properties to the clipboard, double-click on it.

   Note: Does your YubiKey have so many passkeys that you must scroll down the screen to find the one you're looking for? If you have a desktop or Android tablet device, you can take advantage of their wider screens by changing the *screen layout*.

3. To delete a passkey, click on it to open its **Details** tab.



Passkeys

FIDO2

Search passkeys

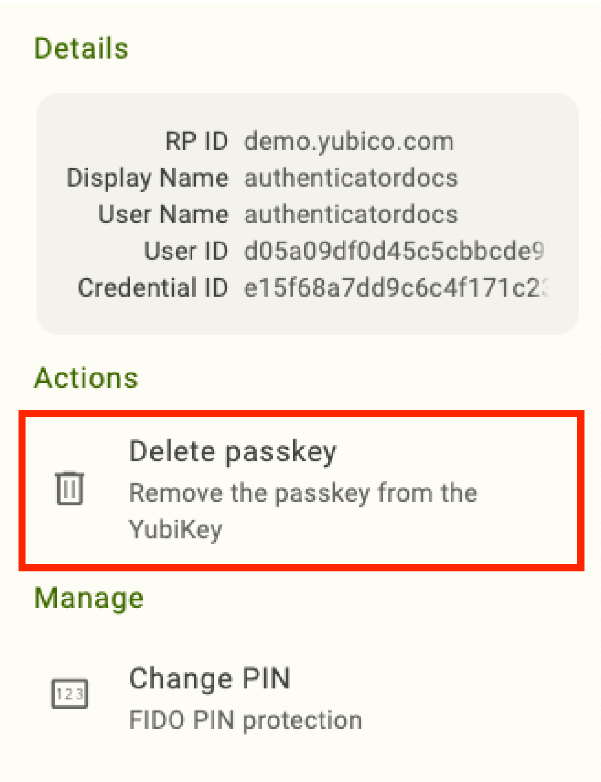
demo.yubico.com
authenticatordocs

1 of 25 passkeys used. Non-passkey credentials may exist, but can not be listed.

Manage

Change PIN
FIDO PIN protection

4. Click **Delete passkey** under **Actions**. To confirm the operation, click **Delete**. For NFC connections on Android, tap your key.



Details

RP ID	demo.yubico.com
Display Name	authenticatordocs
User Name	authenticatordocs
User ID	d05a09df0d45c5cbbcde9
Credential ID	e15f68a7dd9c6c4f171c2

Actions

Delete passkey
Remove the passkey from the YubiKey

Manage

Change PIN
FIDO PIN protection

7.3 Enterprise Attestation

Note: Enterprise Attestation can be managed on Yubico Authenticator for Desktop and Android only.

Enterprise Attestation (EA) is a feature available for custom-configured YubiKeys with firmware version 5.7 or later. EA enables Identity Providers (IdPs) to read the serial number (or other unique identifier specific to the organization) during FIDO2 registration. For more information on Enterprise Attestation, see the YubiKey Technical Manual

The **Passkeys** screen in Yubico Authenticator allows you to easily check your key's EA status and enable the feature (if available for your key).

7.3.1 Check status and enable Enterprise Attestation

To check your key's EA status and enable the feature, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Passkeys**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

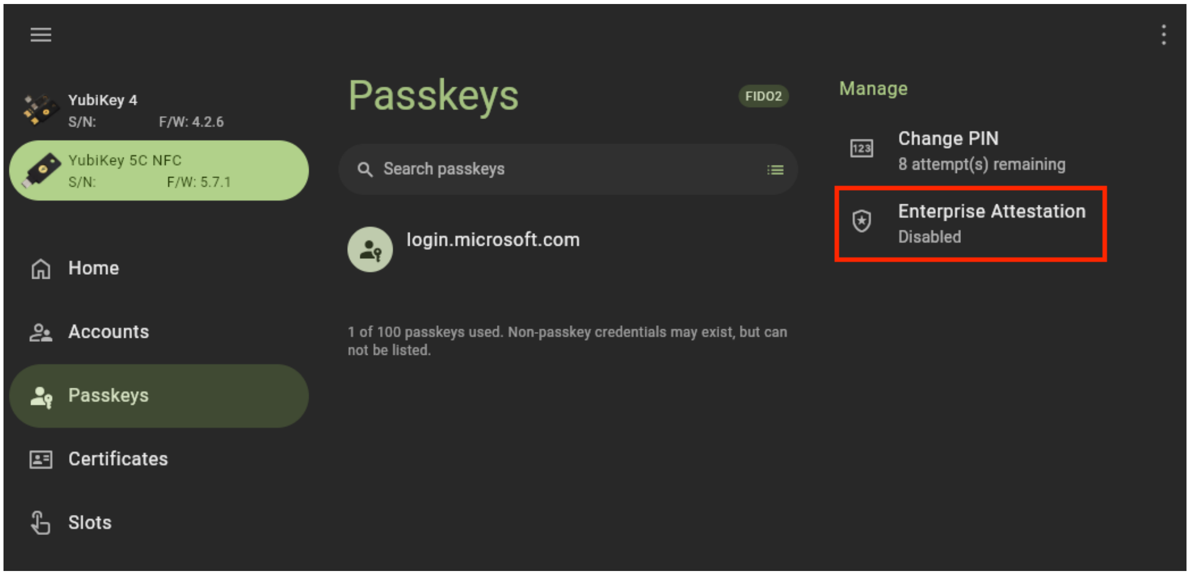
   To connect via NFC on Android, tap and hold your YubiKey on the back of your device to scan. Reading passkeys on a YubiKey is quite slow, and depending on how many are stored on your key, it could take up to several seconds for the NFC sensor to read the passkey information. You must maintain constant contact with the NFC sensor until all passkeys are read.

2. Enter your FIDO2 PIN if prompted and click **Unlock**. For NFC connections on Android, tap your key to complete the operation.

3. To check your key's EA status, find **Enterprise Attestation** under **Manage**.

   To find the **Manage** menu in a narrow app window, click the three dots in the upper right corner of the app.

4. To enable EA, click on **Enterprise Attestation**. In the **Enable Enterprise Attestation** window, select **Enable** to confirm the operation.



Change PIN
8 attempt(s) remaining

Enterprise Attestation
Disabled

1 of 100 passkeys used. Non-passkey credentials may exist, but can not be listed.

7.3.2 Disable Enterprise Attestation

Once Enterprise Attestation is enabled, it can only be disabled by performing a FIDO2 application factory *reset*. Note that a reset will also remove all fingerprints, passkeys, and non-passkey FIDO2 credentials from your YubiKey.

7.4 Custom icons

Note: Custom icons are only available for Yubico Authenticator for Desktop and Android.

When viewing *OATH accounts* on a YubiKey within Yubico Authenticator, each account is listed with a colored icon that contains the first letter of the issuer by default. Similarly, *Passkeys* are listed with a default Passkey icon.

To make OATH accounts and Passkeys more easily distinguishable from one another, custom icons can be uploaded and used in Yubico Authenticator. For example, with custom icons, instead of seeing the default "D" icon next to an OATH account for Docker, an icon containing the Docker logo and colors would be shown. For a Microsoft Passkey, an icon with the Microsoft logo and colors would be shown in place of the default Passkey icon.

Icon packs must be in the Aegis Icon Pack format. Feel free to use a pre-built icon pack from Aegis or create your own.

To upload an icon pack to Yubico Authenticator on desktop or Android, do the following:

1. Download a pre-built icon pack from Aegis or create your own.
2. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Home**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.
3. Select **Settings** under **Application**. On the **Settings** screen, click **Custom icons**.

   In a narrow app window, click the three dots in the upper right corner of the app to find the **Application** menu.
4. In the **Custom icons** window, click **Load icon pack**. Select the file containing the icons (for example, aegis-icons.zip).
5. Once loaded, any OATH account or Passkey with an issuer that is supported by the icon pack will display the custom icon. To delete the icon pack, click the trash can icon in the **Custom icons** window. Similarly, to update the icon pack, click **Replace icon pack** and select the new file.

CHAPTER

EIGHT

FINGERPRINTS: FIDO2

Important: The **Fingerprints** feature is only available for Yubico Authenticator for Desktop and Android and the YubiKey Bio Series. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

YubiKey Bio Series keys have a biometric sensor that allows you to use a fingerprint to authenticate to registered accounts/services via the *FIDO2* or FIDO U2F protocols. At least one *fingerprint* must be enrolled with a key to enable biometric functionality. And before you can enroll a fingerprint, you must first set the the key's *FIDO2 PIN*.

Note: See the YubiKey Bio Series documentation for more information on the key itself. For a list of products, services, and applications that are compatible with the YubiKey Bio and an overview of their unique security key registration processes, see the Works with YubiKey catalog.

The Fingerprints feature of Yubico Authenticator allows you to:

- *Enroll up to five (5) fingerprints on a YubiKey Bio Series key*.
- *Rename or delete saved fingerprints*.
- *Create or change the key's FIDO2 PIN*.

8.1 Creating and managing the FIDO2 PIN

Before you can *register and manage fingerprints* or add *FIDO2 passkeys* to a YubiKey Bio Series key, you must create a FIDO2 PIN. This PIN is also used by the YubiKey as a fallback; if the key doesn't recognize your fingerprint during a FIDO2 authentication attempt, the PIN can be used to bypass the fingerprint verification and complete authentication.

For YubiKey Bio Series Multi-protocol Edition keys, the FIDO2 application and the PIV application share a PIN. Therefore, performing the "Change PIN" action on the **Passkeys**, **Fingerprints**, or **Certificates** screen modifies the same credential.

Warning: The YubiKey provides a total of eight (8) attempts to enter the correct current PIN during a PIN change attempt, registration attempt, or authentication attempt. After three (3) incorrect attempts in a row, that key must be removed and reinserted into your device. After 8 incorrect attempts, the FIDO2 application becomes blocked and must be *reset*. Entering the PIN correctly resets the PIN attempt counter back to 8.

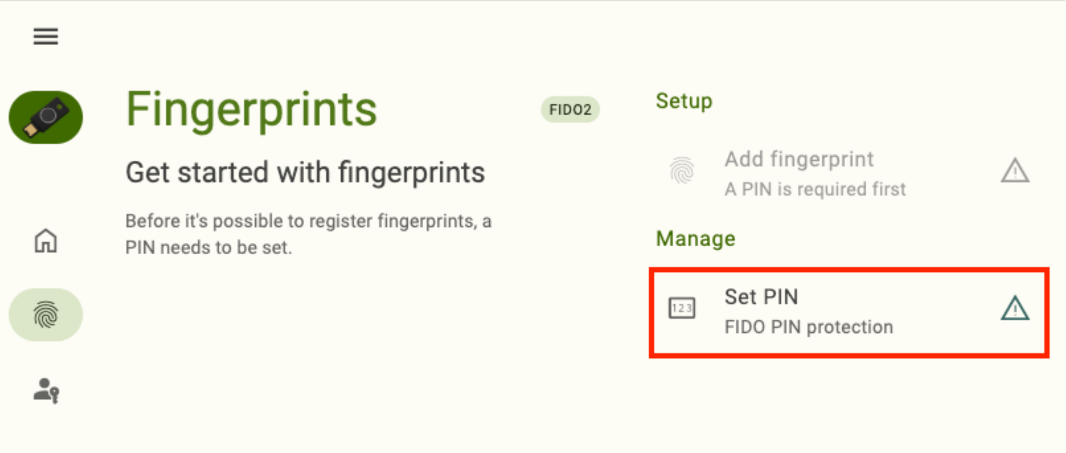
The same FIDO2 PIN is used for *passkeys*; if you have already created a FIDO2 PIN via the **Passkeys** feature, you do not need to create a new one for **Fingerprints**.

8.1.1 Creating a FIDO2 PIN

To create a FIDO2 PIN, do the following:

1. Plug your YubiKey Bio into your device, click the menu icon in the upper left corner of the app, and select **Fingerprints**.
2. Click **Set PIN** under **Manage**.

   In a narrow app window, click the three dots in the upper right corner of the app to find the **Manage** menu.



Fingerprints

FIDO2

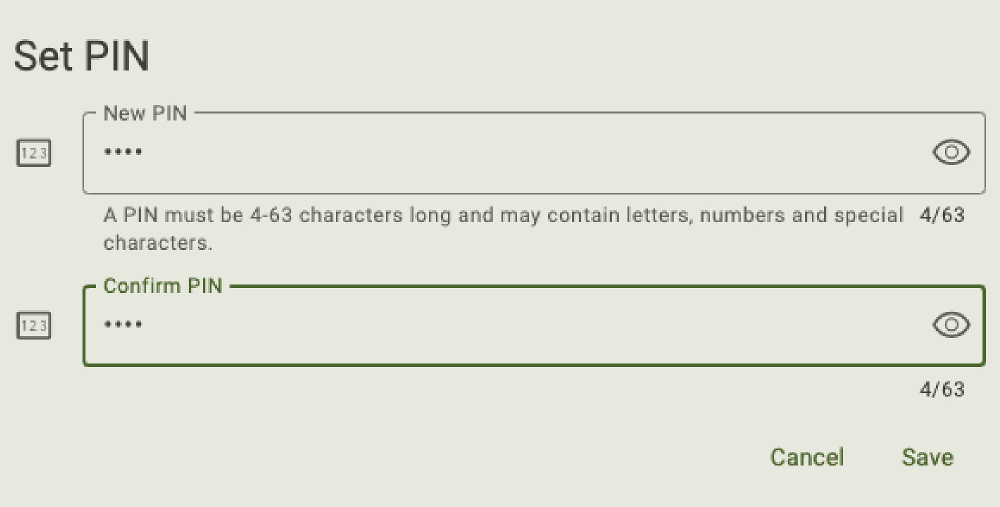
Get started with fingerprints

Before it's possible to register fingerprints, a PIN needs to be set.

3. In the **Set PIN** window, enter your new PIN.

Note: PIN requirements depend on your YubiKey’s model, firmware version, and *PIN complexity* enforcement.

4. Enter the new PIN again to confirm and click **Save**.



Set PIN

New PIN: ••••

A PIN must be 4-63 characters long and may contain letters, numbers and special characters. 4/63

Confirm PIN: ••••

4/63

8.1.2 Changing the FIDO2 PIN

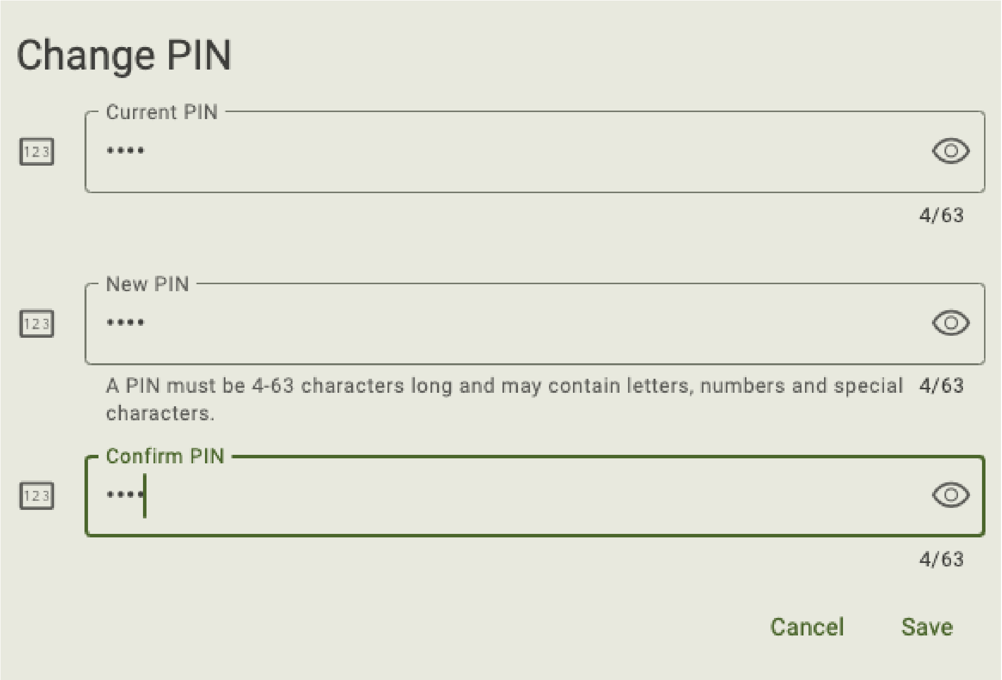
To change the FIDO2 PIN, do the following:

1. Plug your YubiKey Bio into your device, click the menu icon in the upper left corner of the app, and select **Fingerprints**.
2. Click **Change PIN** under **Manage**.

   In a narrow app window, click the three dots in the upper right corner of the app to find the **Manage** menu.
3. In the **Change PIN** window, enter your current PIN.

   If you have forgotten your current PIN, the only way to change it is to *reset* the FIDO2 application of your YubiKey to factory default settings (which will remove the PIN). Note that this will delete **ALL** fingerprints and *passkeys* stored on the YubiKey, and you will no longer be able to access those accounts with that key (we recommend registering at least one *backup YubiKey* with each account/service to maintain access). Once reset, you can always re-register your key with those same accounts and services.
4. Enter your new PIN.

   Note: PIN requirements depend on your YubiKey's model, firmware version, and *PIN complexity* enforcement.
5. Enter the new PIN again to confirm and click **Save**.


Change PIN
Current PIN
123
••••
4/63
New PIN
123
••••
A PIN must be 4-63 characters long and may contain letters, numbers and special characters.
4/63
Confirm PIN
123
••••
4/63
Cancel
Save

8.2 Registering and managing fingerprints

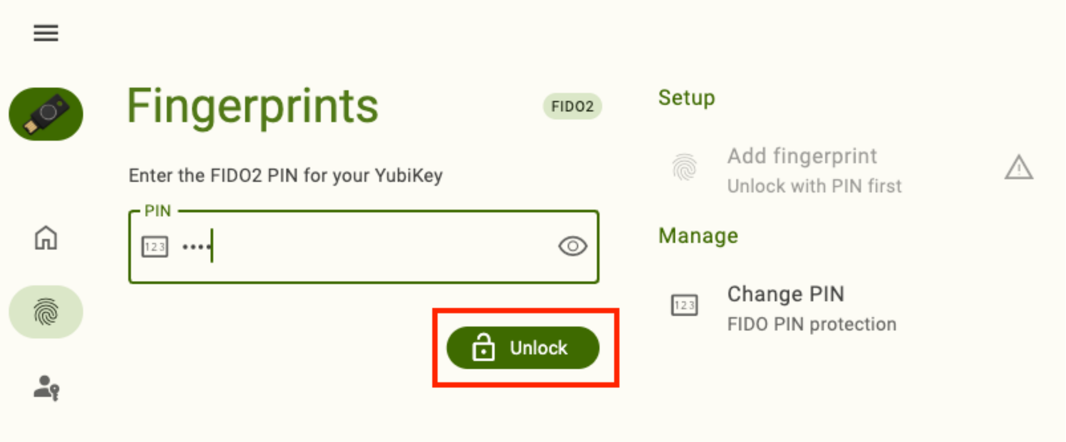
You can enroll up to five (5) fingerprints on a YubiKey Bio Series key. Once your key is registered for passwordless FIDO2 or FIDO U2F authentication with an account/service, you can perform authentication by touching the key with any of the fingers that match an enrolled fingerprint.

Note: If the key doesn't recognize your fingerprint during a FIDO2 authentication attempt, the FIDO2 PIN can be used to complete the authentication.

8.2.1 Enroll a fingerprint

To enroll a fingerprint, do the following:

1. Plug your YubiKey Bio into your device, click the menu icon in the upper left corner of the app, and select **Fingerprints**.
2. Enter your FIDO2 PIN and click **Unlock**. If you don't have a PIN yet, *create one*.



Enter the FIDO2 PIN for your YubiKey

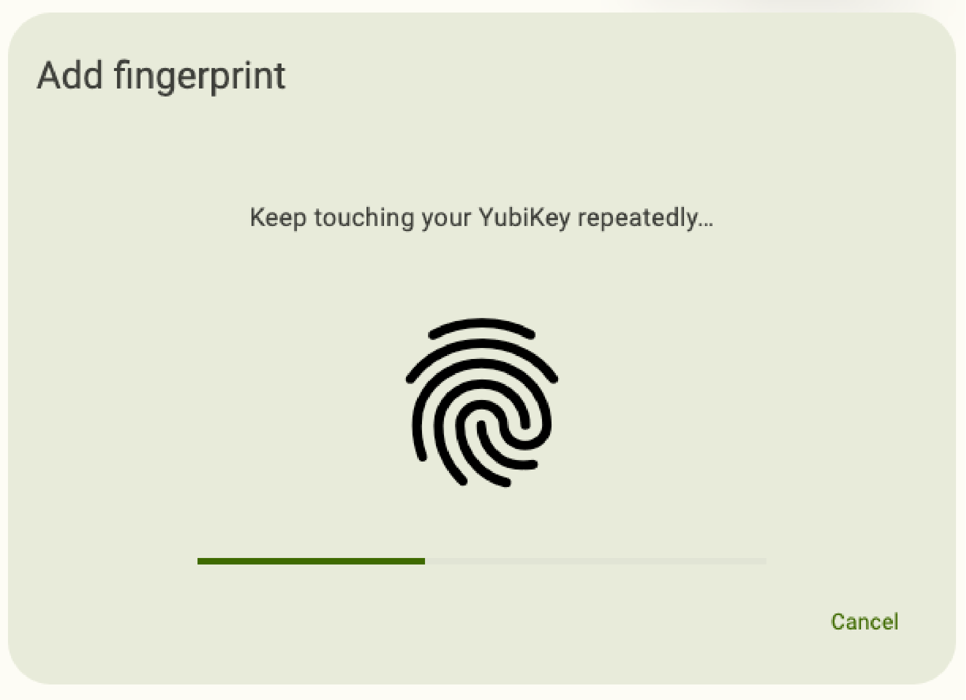
PIN: ••••

3. Click **Add fingerprint** under **Setup**.

   In a narrow app window, click the three dots in the upper right corner of the app to find the **Setup** menu.

4. In the **Add fingerprint** window, press a finger against the biometric sensor of your key. When the window prompts you to "keep touching your key", remove your finger and place it back on the sensor. Repeat this until the progress bar reaches 100% completion.

   > Make sure to touch both the sensor and bezel and adjust your finger pressure so that as much of your print is in contact with the sensor as possible; this will improve the quality of the reading. For additional tips on enrolling fingerprints, see the YubiKey Bio documentation.

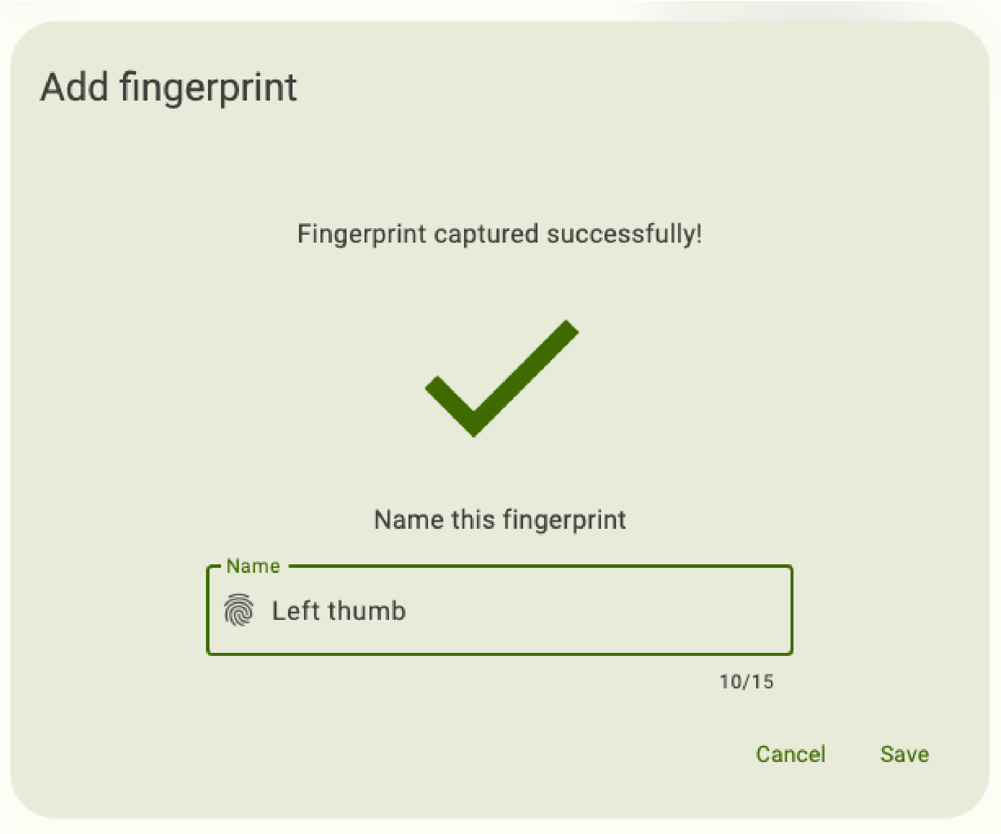


Add fingerprint

Keep touching your YubiKey repeatedly...

5. Once the fingerprint is captured successfully, enter a **Name** for the fingerprint and click **Save**. You will now see your new fingerprint listed under **Fingerprints**.

   If you click cancel, the fingerprint will still be saved, but it will be given a name of the form **Unnamed (ID: XXXX)**. If you made a mistake, you can always *rename or delete* the fingerprint.



Add fingerprint

Fingerprint captured successfully!

Name this fingerprint

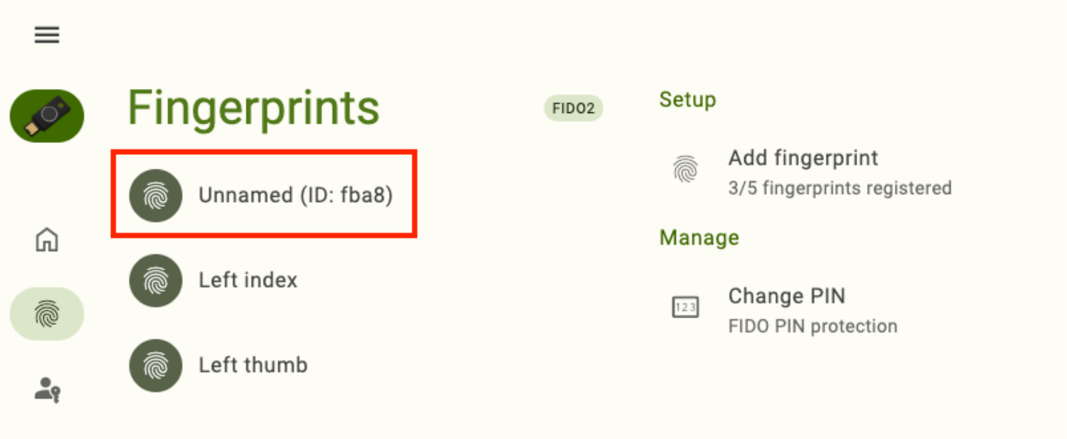
Name: Left thumb

10/15

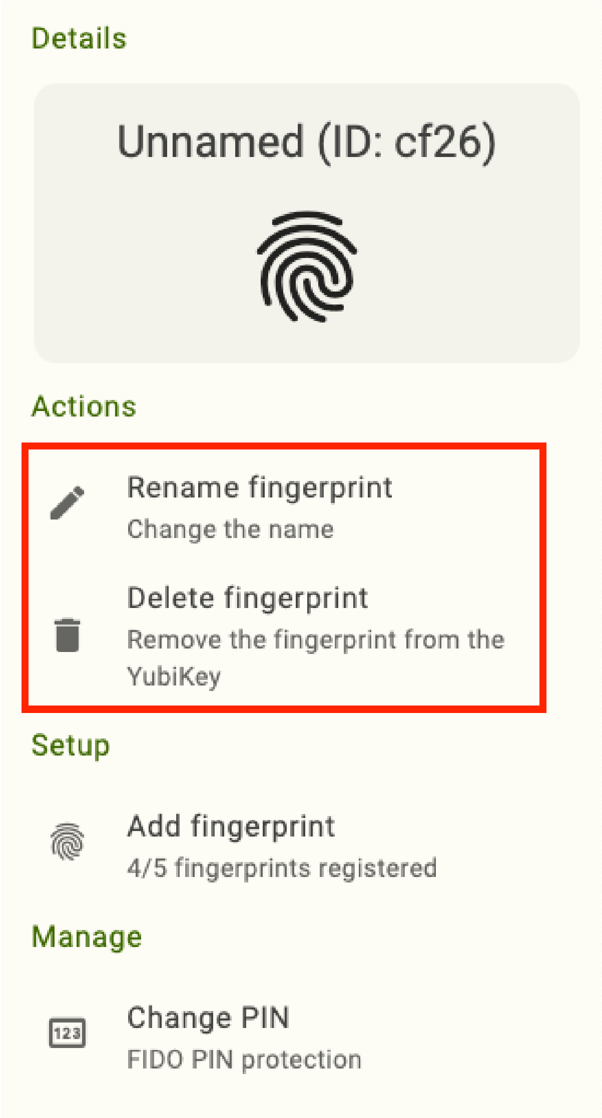
8.2.2 Rename or delete a fingerprint

To rename or delete an existing fingerprint, do the following:

1. Plug your YubiKey Bio into your device, click the menu icon in the upper left corner of the app, and select **Fingerprints**.
2. Enter your FIDO2 PIN and click **Unlock**.
3. Click on the fingerprint you would like to manage.



4. To rename the fingerprint, click **Rename fingerprint** under **Details**. Enter a new **Name** and click **Save**.
5. To delete a fingerprint, click **Delete fingerprint** under **Details**. To confirm the operation, click **Delete**.



Details

Unnamed (ID: cf26)

Actions

Rename fingerprint
Change the name

Delete fingerprint
Remove the fingerprint from the YubiKey

Setup

Add fingerprint
4/5 fingerprints registered

Manage

Change PIN
FIDO PIN protection

CHAPTER

NINE

CERTIFICATES: PIV

9.1 Managing the PIN, PUK, and Management Key

The PIN, PUK, and Management Key are essential to the functionality of the YubiKey's PIV application.

The PIN is a 6-8 character value (default: 123456) that protects the YubiKey's PIV slot credentials. It is required when performing operations such as authentication, encryption/decryption, and digital signature creation.

The PUK, or PIN Unblocking Key, is a 6-8 character value (default: 12345678) that is used, as the name implies, to *unblock* a blocked PIN. The PIN has a set *retry count*. Once the PIN has been entered incorrectly too many times in a row and the retries have been exhausted, the PIN becomes blocked and all PIV operations that require the PIN cannot be performed. The PUK, along with Yubico Authenticator, can be used to unblock (change) the PIN and reset the PIN's retry count without needing to perform a factory reset of the entire PIV application.

The Management Key (default: 010203040506070801020304050607080102030405060708) is required when performing certain operations with the YubiKey's PIV application slots, including the *generation, importation, and deletion of keys and certificates*. For YubiKeys with firmware version 5.7, the default Management Key is an AES-192 key. For YubiKeys with firmware versions prior to 5.7, the default Management Key is a Triple DES (TDES) key. Depending on your YubiKey, you may be able to select a different algorithm (TDES, AES-128, AES-192, or AES-256) when changing the Management Key. Management Key length is also dependent on the algorithm: 32 characters for AES-128, 48 characters for TDES and AES-192, and 64 characters for AES-256. Yubico Authenticator also provides the ability to toggle on the "Protect with PIN" feature, which allows you to use the PIN in place of the Management Key when performing operations that require Management Key verification.

To improve the security of your YubiKey, Yubico recommends changing the *PIN*, *PUK*, and *Management Key* from their default values before use. For YubiKey 5 FIPS Series keys with firmware 5.7 or later, these changes are required to enter *FIPS approved mode*.

9.1.1 Changing the PIN

Note: For YubiKey Bio Series Multi-protocol Edition keys, the FIDO2 application and the PIV application share a PIN. Therefore, performing the "Change PIN" action on the **Passkeys**, **Fingerprints**, or **Certificates** screen modifies the same credential.

To change the PIN, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Certificates**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

2. Select **Change PIN** under **Manage**.

   To find the **Manage** menu in a narrow app window, click the three dots in the upper right corner of the app.

3. Enter your current PIN.

   For YubiKeys with firmware version 5.4.x and later, if the current PIN is the default PIN (123456), this value will be prepopulated in the **Current PIN** box.

4. Enter a new PIN.

   In general, the PIN must be 6 to 8 characters long and can contain any ASCII character, which includes letters (uppercase and lowercase), numbers, and special characters (such as +, &, #). However, there may be additional PIN requirements depending on your YubiKey's model, firmware version, and *PIN complexity* enforcement. These requirements will be noted in the **Change PIN** window.

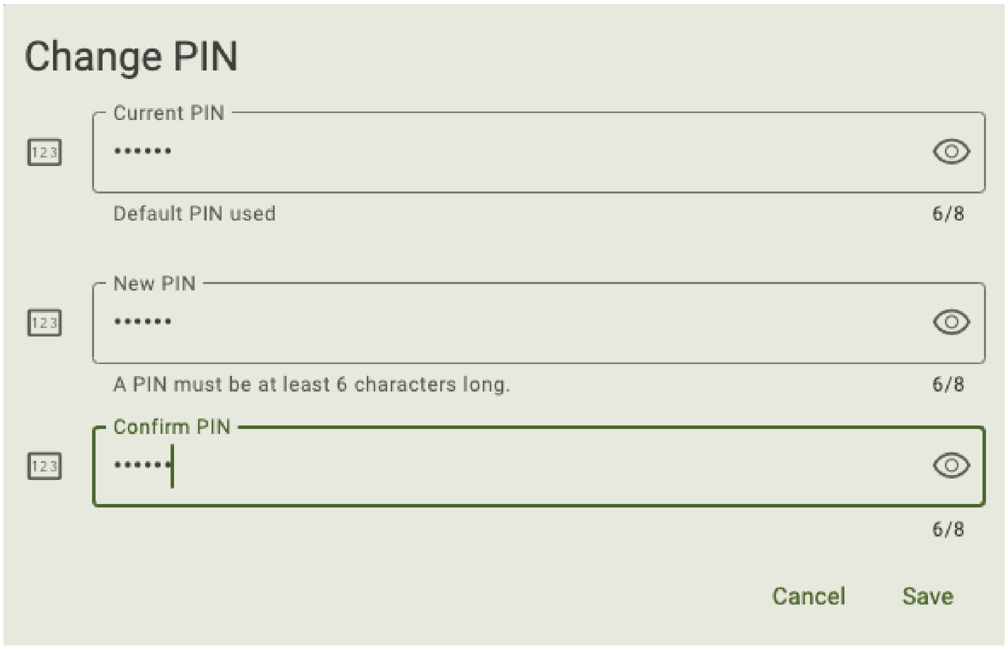
   Yubico Authenticator uses UTF-8 to encode the PIN and allows you to enter up to 8 *bytes* worth of (printable) UTF-8 encoded characters. The UTF-8 byte count is shown underneath the **New PIN** window. This is important because ASCII codes 0-127 (letters, numbers, and special characters found on a US keyboard) are one byte in length when encoded in UTF-8, but ASCII codes 128-255, which include less common symbols such as the degree sign (°), copyright sign (©), and the Pound sign (£), are more than one byte in length. So for example, if you enter `123456` as the PIN, the byte count in the Authenticator will show 6/8. However, if you enter `££££` for your new PIN, the byte count will show 8/8.

   For YubiKeys with firmware versions prior to 5.7, the YubiKey will accept the PIN as long as the UTF-8 byte count as shown in the Authenticator is 6-8. For YubiKeys with firmware version 5.7 and later, the YubiKey will only accept the PIN if it contains 6-8 individual characters. To reuse the previous example, a PIN of four £ sign characters would be rejected by a YubiKey with firmware version 5.7 for being too short (less than 6 characters) even though the Authenticator app shows the byte count as 8.

   Note: YubiKeys with firmware version 5.7 and later require PINs to be 6-8 unicode code points in length instead of 6-8 bytes. Each ASCII character is represented by a single code point, which means that PINs must include 6-8 individual characters.

   Yubico recommends creating a PIN that is easy to type–entering the PIN incorrectly too many times will result in the PIN becoming *blocked*. Also note that other PIV clients and applications that you interact with may not support all ASCII characters or may use a different encoding scheme for the PIN.

5. Enter the new PIN again to confirm and click **Save**.



Change PIN

Current PIN: ••••••

Default PIN used 6/8

New PIN: ••••••

A PIN must be at least 6 characters long. 6/8

Confirm PIN: ••••••

6/8

9.1.2 Changing the PUK

Note: YubiKey Bio Series Multi-protocol Edition keys do not have a PUK.

To change the PUK, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Certificates**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

2. Select **Change PUK** under **Manage**.

   To find the **Manage** menu in a narrow app window, click the three dots in the upper right corner of the app.

3. Enter your current PUK.

   For YubiKeys with firmware version 5.4.x and later, if the current PUK is the default PUK (12345678), this value will be prepopulated in the **Current PUK** box.

4. Enter a new PUK.

   In general, the PUK must be 6 to 8 characters long and can contain any ASCII character, which includes letters (uppercase and lowercase), numbers, and special characters (such as +, &, #). However, there may be additional PUK requirements depending on your YubiKey's model, firmware version, and *PIN complexity* enforcement. These requirements will be noted in the **Change PUK** window.

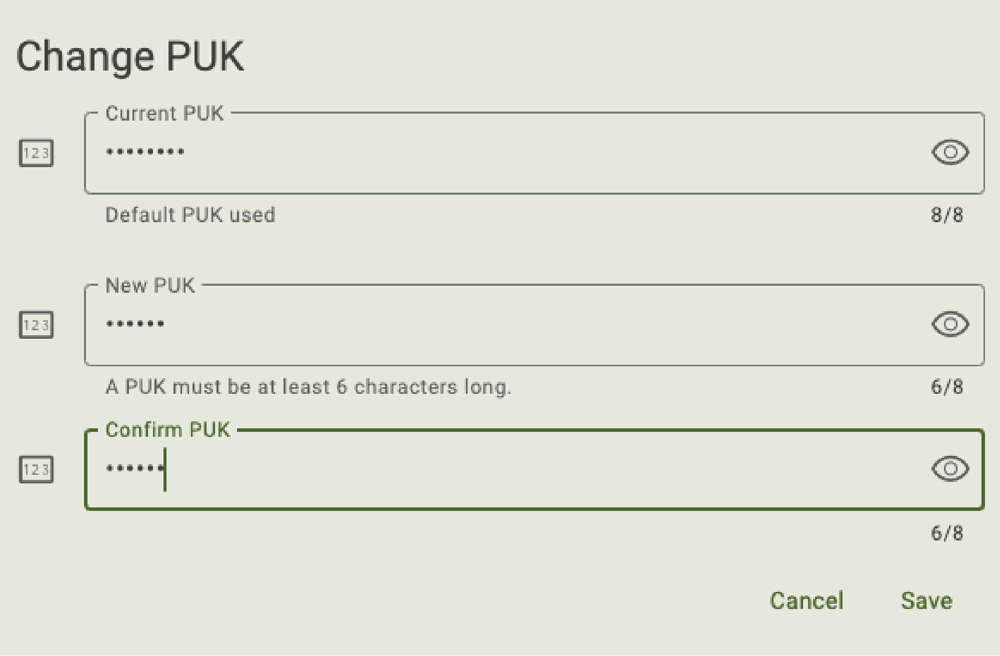
   Yubico Authenticator uses UTF-8 to encode the PUK and allows you to enter up to 8 *bytes* worth of (printable) UTF-8 encoded characters. The UTF-8 byte count is shown underneath the **New PUK** window. This is important because ASCII codes 0-127 (letters, numbers, and special characters found on a US keyboard) are one byte in length when encoded in UTF-8, but ASCII codes 128-255, which include less common symbols such as the degree sign (°), copyright sign (©), and the Pound sign (£), are more than one byte in length. So for example, if you enter `123456` as the PUK, the byte count in the Authenticator will show 6/8. However, if you enter `££££` for your new PUK, the byte count will show 8/8.

For YubiKeys with firmware versions prior to 5.7, the YubiKey will accept the PUK as long as the UTF-8 byte count as shown in the Authenticator is 6-8. For YubiKeys with firmware version 5.7 and later, the YubiKey will only accept the PUK if it contains 6-8 individual characters. To reuse the previous example, a PUK of four £ sign characters would be rejected by a YubiKey with firmware version 5.7 for being too short (less than 6 characters) even though the Authenticator app shows the byte count as 8.

Note: YubiKeys with firmware version 5.7 and later require PUKs to be 6-8 unicode code points in length instead of 6-8 bytes. Each ASCII character is represented by a single code point, which means that PUKs must include 6-8 individual characters.

Yubico recommends creating a PUK that is easy to type–entering the PUK incorrectly too many times will result in the PUK becoming *blocked*, and you will need to perform a factory reset of the PIV application in order to reset it. Also note that other PIV clients and applications that you interact with may not support all ASCII characters or may use a different encoding scheme for the PUK.

5. Enter the new PUK again to confirm and click **Save**.



Change PUK

Current PUK: ••••••••

Default PUK used 8/8

New PUK: ••••••

A PUK must be at least 6 characters long. 6/8

Confirm PUK: ••••••

6/8

9.1.3 Changing the Management Key

To change the Management Key, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Certificates**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

2. Select **Management key** under **Manage**.

   To find the **Manage** menu in a narrow app window, click the three dots in the upper right corner of the app.

3. Enter your current Management Key.

Depending on your key's firmware version, if your current Management Key is the default value (010203040506070801020304050607080102030405060708), you will either see this value prepopulated in the **Current management key** box or you will be able to insert the value by clicking the star icon.

If you enabled the "Protect with PIN" setting when you created the current Management Key, you will be prompted to enter the PIN instead.

4. Select an algorithm if the option is available. This is the algorithm that the YubiKey and the Authenticator will use during Management Key authentication to perform an authentication handshake.

   For YubiKeys with firmware version 5.3.x and earlier, Triple DES (TDES) is the default and only Management Key algorithm.

   For YubiKeys with firmware 5.4.x through 5.6.x, TDES is the default algorithm, but AES-128, AES-192, and AES-256 are supported as options and can be selected from the drop-down menu.

   Standard YubiKey 5 Series keys with firmware 5.7.x and later use AES-192 by default. TDES, along with AES-128 and AES-256, are supported as options. YubiKey 5 FIPS Series keys with firmware 5.7.x and later allow AES keys only, with AES-192 as the default.

5. Enter a new Management Key. The length requirement is determined by the algorithm you selected in the previous step and will be displayed underneath the **New management key** box (32 characters for AES-128, 48 characters for TDES and AES-192, and 64 characters for AES-256). To generate one randomly, click the arrow icon inside the **New management key** box. The following characters are allowed: abcdef0123456789.

   Store your new Management Key in a secure location. If you forget the Management Key, there is no way to recover it, and you will need to perform a *factory reset* of the PIV application to reset the Management Key to its default value.

6. To use the PIN in place of the Management Key during operations that require Management Key authentication, select **Protect with PIN** (optional).

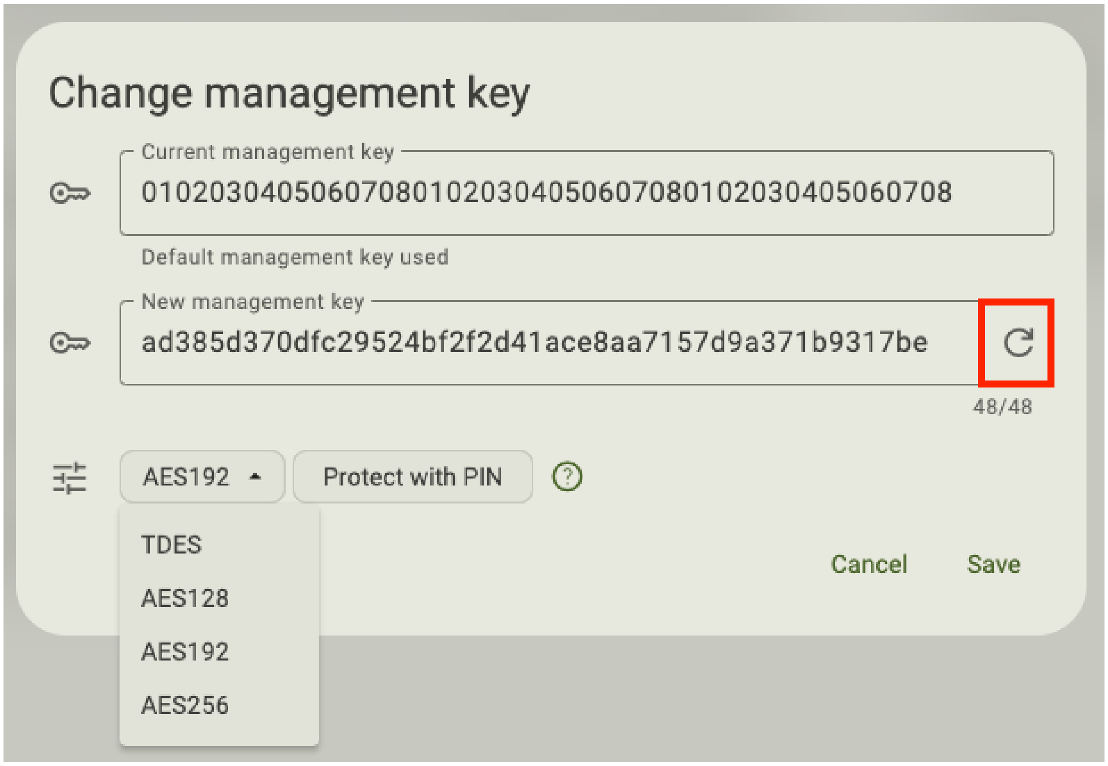
   Note: The "Protect with PIN" feature is available for all PIV-capable YubiKeys. However, YubiKey 5 FIPS Series keys with firmware version 5.7 or later must enter *FIPS approved* mode before the feature can be enabled.

   Operations that require Management Key authentication include the *generation, importation, or deletion of certificates*. If this setting is enabled, you will be prompted to enter the PIN when initiating these operations.

   Note that this setting does not remove the Management Key. The Authenticator will still perform Management Key authentication during an applicable operation, but only the PIN is required from the user.

   If this setting is enabled and the PIN becomes blocked, any operation requiring Management Key authentication *or* PIN authentication will not be possible until the PIN is unblocked with the PUK.

7. Click **Save**.



Change management key

Current management key: 010203040506070801020304050607080102030405060708

Default management key used

New management key: ad385d370dfc29524bf2f2d41ace8aa7157d9a371b9317be

48/48

AES192

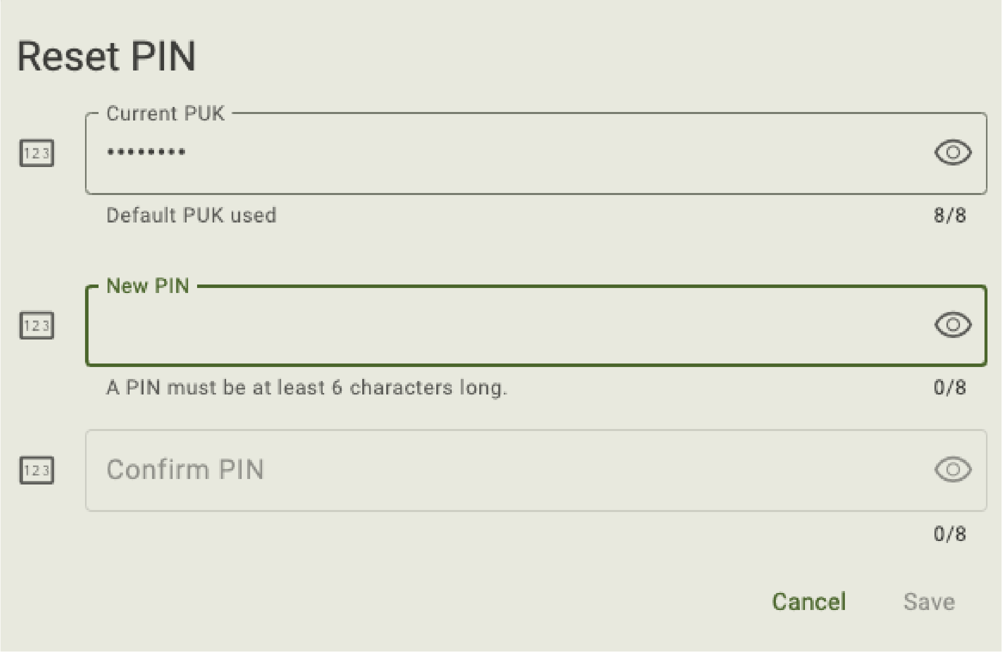
9.1.4 Unblocking the PIN

When you enter the PIN incorrectly too many times in a row, the PIN becomes blocked. The point at which this occurs is determined by your key's retry count, which is 8 by default for the YubiKey Bio Series Multi-protocol Edition and 3 by default for all other PIV-compatible YubiKeys.

Note: The retry count can be reconfigured to any value from 1 to 255 with the YubiKey Manager CLI tool.

Once the PIN in blocked, you will not be able to perform any PIV actions that require the PIN. However, you can unblock the PIN using the PUK (for all YubiKeys except for the YubiKey Bio Series Multi-protocol Edition), which will allow you to change the PIN and reset the number of PIN attempts back to the full retry count value.

To unblock the PIN on an eligible key, follow the *Changing the PIN* instructions. Instead of entering the current PIN, you will be prompted to enter the PUK. For YubiKeys with firmware version 5.4 and later, if the current PUK is the default PUK (12345678), this value will be prepopulated in the **Current PUK** box.



Reset PIN

Current PUK

••••••••

Default PUK used 8/8

New PIN

A PIN must be at least 6 characters long. 0/8

Confirm PIN

0/8

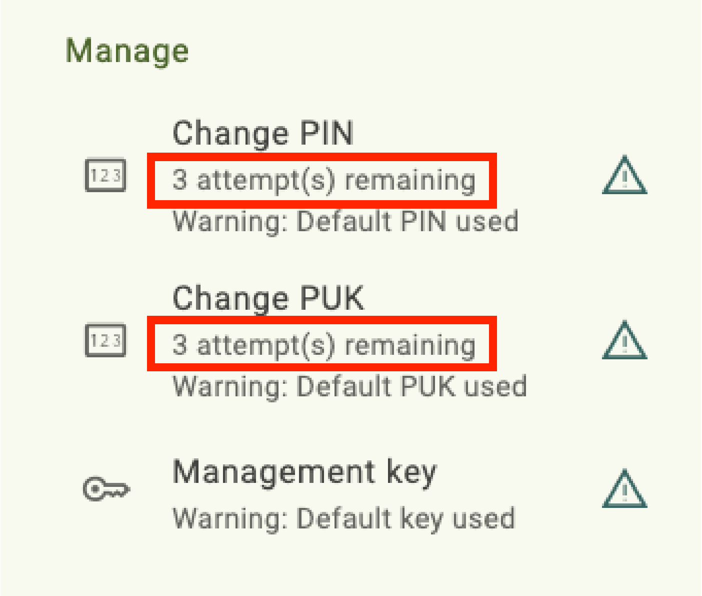
Because YubiKey Bio Series Multi-protocol Edition keys do not have a PUK, you cannot unblock the PIN using the method described above. The only way to change a blocked PIN on these keys is to perform a *factory reset* of the PIV application. This will remove all private keys and certificates from the YubiKey, and the PIN and Management Key will be reset to their factory default values.

9.1.5 Recovering from a blocked or forgotten PUK or Management Key

If you forgot your PUK or Management Key or the PUK has become blocked, the only way to recover them is to perform a *factory reset* of the PIV application. This will remove all private keys and certificates from the YubiKey, and the PIN, PUK, and Management Key will be reset to their factory default values.

9.1.6 PIN and PUK attempts remaining and total retry count

The **Certificates** screen in Yubico Authenticator displays the attempts remaining for both the PIN (all YubiKeys) and the PUK (for YubiKeys with firmware version 5.4 and above) under **Manage**. To find the **Manage** menu in a narrow app window, click the three dots in the upper right corner of the app.



Manage

Change PIN
3 attempt(s) remaining
Warning: Default PIN used

Change PUK
3 attempt(s) remaining
Warning: Default PUK used

Management key
Warning: Default key used

Both the PIN and PUK have a total retry count of 3 by default for all YubiKeys except for the YubiKey Bio Series Multi-protocol Edition, which has a PIN retry count of 8 by default. However, the retry count for the PIN and PUK can be reconfigured to any value from 1 to 255 with the YubiKey Manager CLI tool.

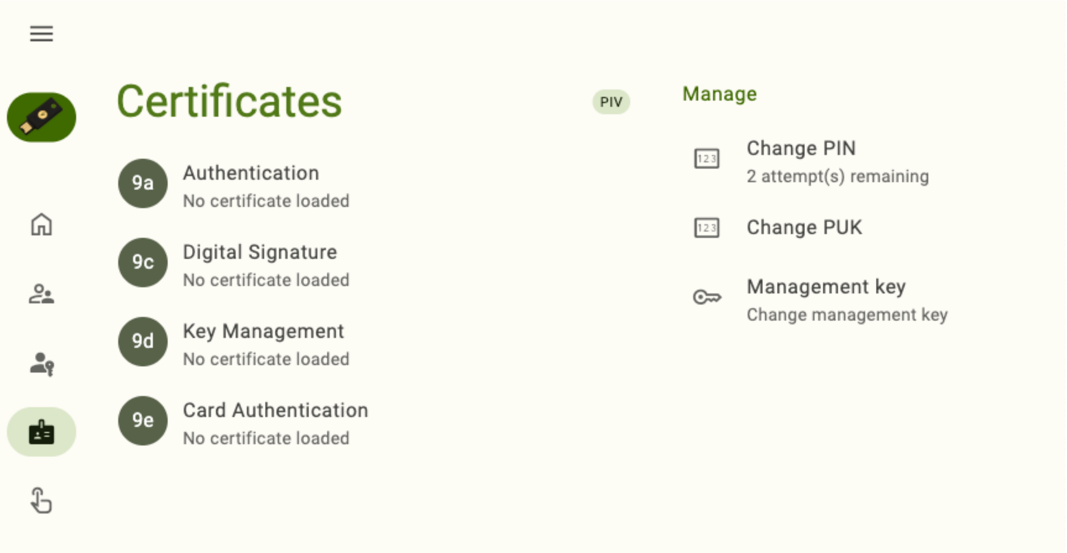
There is no direct way to verify the total retry count for a particular YubiKey in Yubico Authenticator. However, the retry count is reset whenever the PIN/PUK is entered correctly, so the retries remaining will reflect the total retry count at that moment. Alternatively, you can use the `ykman piv info` command with the YubiKey Manager CLI tool to display both total and remaining retries for the PIN and PUK.

9.2 Add and manage certificates

To add a certificate to one of the PIV application slots, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Certificates**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.



Certificates

PIV

9a Authentication
No certificate loaded

9c Digital Signature
No certificate loaded

9d Key Management
No certificate loaded

9e Card Authentication
No certificate loaded

Manage

Change PIN
2 attempt(s) remaining

Change PUK

Management key
Change management key

2. Select a slot and click **Import file** under **Actions**.

   To find the **Actions** menu in a narrow app window, click the three dots in the upper right corner of the app.

3. Enter the PIV management key when prompted and click **Unlock**.
4. Select the certificate file on your device and click **Choose** (or similar).

CHAPTER

TEN

SLOTS: YUBICO OTP APPLICATION

Important: The **Slots** feature is only available for Yubico Authenticator for Desktop and Yubico OTP-compatible YubiKeys. This includes the YubiKey 5 Series (standard, FIPS, and CSPN), YubiKey 4 Series, and YubiKey NEO. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

The **Slots** feature of Yubico Authenticator allows you to manipulate both the short press (or short touch) slot and the long press (long touch) slot of the YubiKey's Yubico OTP application. Each OTP application slot can be configured with one of the following types of credentials:

- *Yubico OTP*
- *Static password*
- *Challenge-response*
- *OATH HOTP*

Once a slot has been configured with a credential, that credential can be used during *authentication* to a compatible site, service, or application. See the Works with YubiKey Catalog for credential compatibility information.

Slot configurations can also be *swapped or deleted*.

10.1 Yubico OTPs

A Yubico OTP (one-time password) is a unique 44-character string that is generated by the YubiKey using a secret key and other YubiKey device fields. Yubico OTPs look similar to the following: ccccccjlkgjlevtdernkbbnrrvhcvdbljgchbgbdbvgk.

Once an OTP application slot has been configured with a Yubico OTP credential, "activation" of that slot triggers the generation of a new Yubico OTP. For more information on authenticating with Yubico OTPs, see *Performing authentication with OTP application slot credentials*.

To find a list of sites and services that use Yubico OTPs, see the Works with YubiKey Catalog. For in-depth information on the Yubico OTP and how they work, see the .NET SDK manual.

Note: Standard YubiKeys are preconfigured with a Yubico OTP in the short press slot. This credential is also preregistered with YubiCloud for out-of-the-box validation.

10.1.1 Configuration

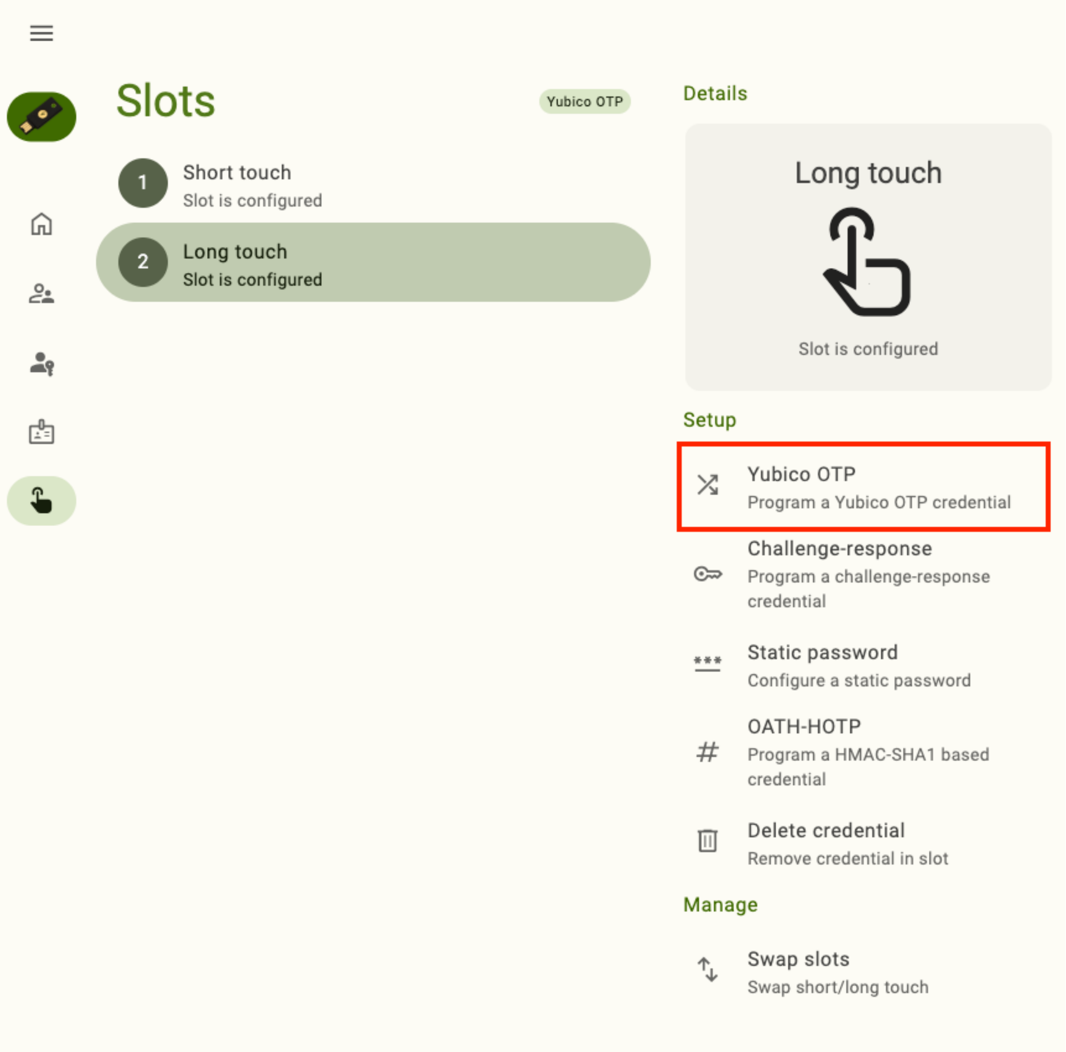
To configure an OTP application slot with a Yubico OTP, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Slots**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

2. Click on the slot you would like to configure and select **Yubico OTP** under **Setup**.

   To find the **Setup** menu in a narrow app window, click the three dots in the upper right corner of the app.



3. Enter a 12-digit **Public ID**. You can either type in your own or use a ModHex representation of your YubiKey's serial number. If using your own ID, only ModHex characters (bcdefghijklnrtuv) are allowed. To use the serial number, click the star icon in the **Public ID** box.

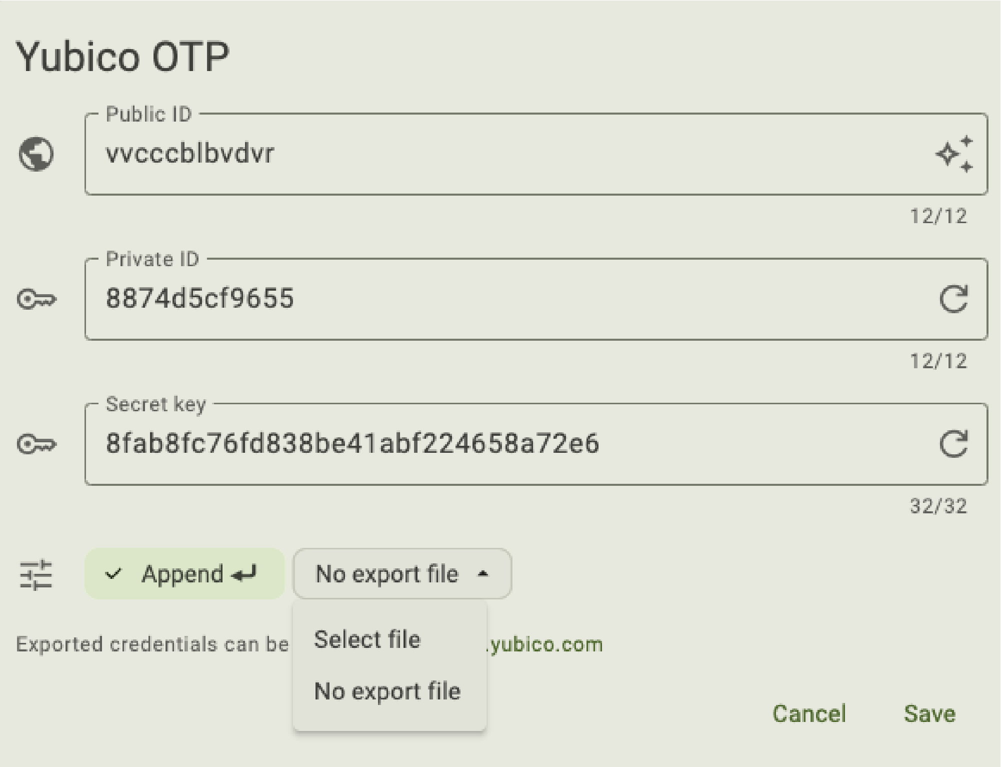
4. Enter a 12-digit **Private ID**. You can either type in your own or generate one randomly. If using your own ID, only the following characters are allowed: abcdef0123456789. To generate a random 12-digit ID, click the arrow icon in the **Private ID** box.

5. Enter a 32-digit **Secret key**. You can either type in your own or generate one randomly. If using your own key, only the following characters are allowed: abcdef0123456789. To generate a random 32-digit secret key, click the arrow icon in the **Secret key** box.

6. By default, a carriage return (an **Enter** keystroke) will be applied to the end of the OTP. This means that when the OTP is generated and typed into a field on a login screen, you won't have to click another button to start the validation process. To remove the carriage return, click **Append** until the check mark disappears.

7. To export the credential to a file, click on the export file drop-down menu and click **Select file**. Enter a name for the file, select a location, and click **Save**. You should now see the name of your file in the drop-down. This step isn't required, but keep in mind that these fields will need to be shared with the validation server for every site or service you wish to authenticate to with this Yubico OTP configuration, so they will need to be saved somewhere (at least temporarily).

   If you elect to save the credential fields to a text file, they will be in a comma-separated list in the following order: YubiKey serial number, Public ID, Private ID, Secret key, date and time the configuration was created.

   Yubico OTP

   Public ID: vvcccblbvdvr (12/12)

   Private ID: 8874d5cf9655 (12/12)

   Secret key: 8fab8fc76fd838be41abf224658a72e6 (32/32)

   ✓ Append ↵

   No export file

   Exported credentials can be .yubico.com

8. Click **Save** to complete the configuration. If the slot is already configured with a credential, click **Overwrite** when prompted.

9. Once configured, share the credential fields with the validation server for every site and service you wish to authenticate to with this Yubico OTP configuration. Remember, during Yubico OTP authentication, the validation server must decrypt the OTP with the secret key in order to determine validity. If the server does not have this information, it cannot validate *any* OTPs generated with your new configuration for any account.

   If a site/service uses the YubiCloud validation service, these fields can be uploaded at https://upload.yubico.com/. If a site/service uses an alternative validation server, refer to their setup instructions.

10. After the credential has been added to the appropriate validation servers, you must register your key with your accounts. See the Works with YubiKey Catalog for setup instructions for your particular sites/services.

    This step links the Public ID for the credential with your account; if the Public ID of an OTP submitted for validation does not match the Public ID linked to your account, the OTP will be rejected.

10.2 Static passwords

A static password, as the name implies, is a string of characters that never changes. It is no different from a password that you would create for any standard account.

Once an OTP application slot is configured with a static password, that password will be typed into a text field by the YubiKey whenever the slot is "activated" (provided that your device's cursor has been placed into the text field). Slot activation occurs when a YubiKey is connected to a desktop or mobile device and its gold contacts are touched. For more information on authenticating with static passwords and the OTP application, see *Performing authentication with OTP application slot credentials*.

Think of the OTP application's static password functionality as akin to a physical password manager. You can set up an account with a long, complicated, and difficult-to-guess password, and instead of trying to remember that password or writing it down in an insecure location, it can be stored safely in the YubiKey.

Static passwords can be communicated over USB connections only.

10.2.1 Configuration

To configure an OTP application slot with a static password, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Slots**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

2. Click on the slot you would like to configure and select **Static password** under **Setup**.

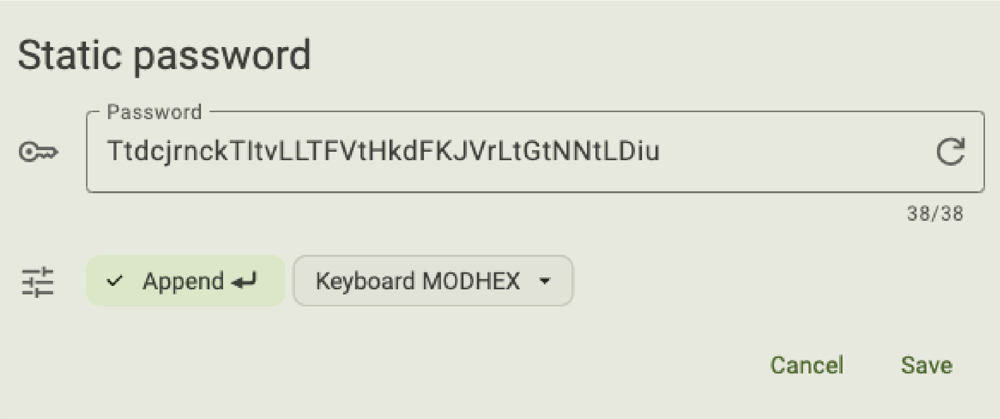
   To find the **Setup** menu in a narrow app window, click the three dots in the upper right corner of the app.

3. Enter a **Password** up to 38 characters in length. If you'd prefer to generate a 32-character password randomly, click the arrow icon in the **Password** box.

4. By default, a carriage return (an **Enter** keystroke) will be applied to the end of the static password. This means that when the password is typed into a field on a login screen, you won't have to click another button to continue the login process. To remove the carriage return, click **Append** until the check mark disappears.

5. Select a **Keyboard** layout from the drop-down menu. Choose the layout that matches the keyboard configuration on the devices you will use your YubiKey with. If you use devices with more than one configuration or you aren't sure what they are, pick ModHex. With ModHex characters, the password will be communicated to a host device correctly, regardless of its keyboard layout setting. Note that if you select ModHex, your password may only contain the following characters: bcdefghijklnrtuv.

6. Click **Save** to complete the configuration. If the slot is already configured with a credential, click **Overwrite** when prompted.



Static password

Password: TtdcjrnckTltvLLTFVtHkdFKJVrLtGtNNtLDiu

38/38

✓ Append ↵

Keyboard MODHEX ▾

7. If you haven't already, register the static password with your accounts. This can be accomplished by the standard "create a new password" or "change your password" flows. If you've forgotten the static password you configured the slot with, simply place your cursor into any text field and activate the slot (tap the key for the short press slot or touch and hold for a few seconds for the long press slot). The static password will be typed into the text field.

10.3 Challenge-response

Challenge-response is a type of authentication where a host (the site, service, or application you are trying to log in to) sends a "challenge" in the form of a byte array to your YubiKey. The YubiKey receives the challenge and "responds" by hashing the challenge with a secret key and the HMAC-SHA1 algorithm. This operation produces a response code in the form of an HOTP, which is sent back to the host for authentication.

When configuring a Yubico OTP slot with a challenge-response credential, a secret key (even-numbered, 2-40 characters in length) must be provided. An optional touch requirement can also be set.

To find a list of sites and services that use challenge-response authentication, see the Works with YubiKey Catalog. For in-depth information on how challenge-response works with the Yubico OTP application, see the .NET SDK manual.

Note: Challenge-response authentication with the Yubico OTP application works over USB connections only.

10.3.1 Configuration

To configure an OTP application slot with a challenge-response credential, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Slots**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

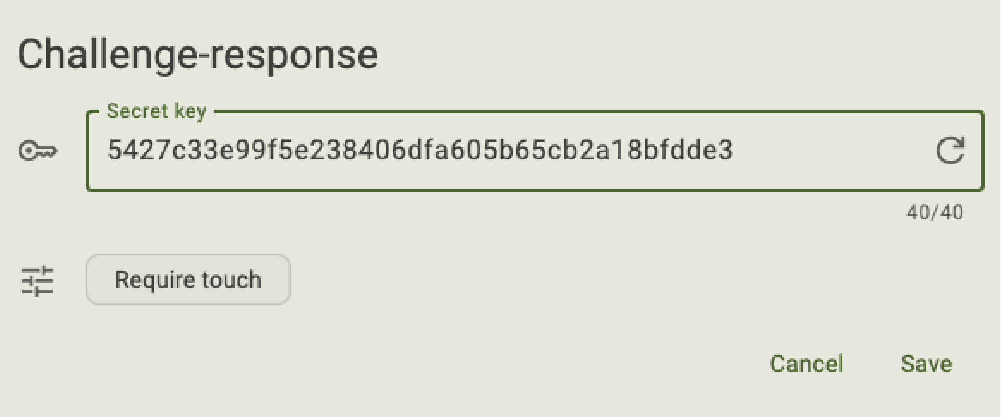
2. Click on the slot you would like to configure and select **Challenge-response** under **Setup**.

   To find the **Setup** menu in a narrow app window, click the three dots in the upper right corner of the app.

3. Enter an even-numbered **Secret key** up to 40 digits in length. You can either type in your own or generate one randomly. If using your own key, only the following characters are allowed: abcdef0123456789. To generate a random 40-digit secret key, click the arrow icon in the **Secret key** box.

   Be sure to **make a copy of your secret key**; you will need to share it with the site/application for each of your accounts during registration process.

4. Optionally, toggle on **Require touch**. This setting requires the user to touch the YubiKey before the key will process the challenge and communicate the response to the host device.
5. Click **Save** to complete the configuration. If the slot is already configured with a credential, click **Overwrite** when prompted.



Challenge-response

Secret key: 5427c33e99f5e238406dfa605b65cb2a18bfdde3

6. After the credential has been added to the appropriate validation servers, you must register your key with your accounts. See the Works with YubiKey Catalog for setup instructions for your particular sites/services.

10.4 OATH HOTPs

OATH HOTPs (Initiative for Open Authentication HMAC-based one-time passwords) are 6 or 8 digit unique passcodes that are used as the second factor during two-factor authentication. An HOTP looks like the following: 154916.

Generally, we recommend using the YubiKey's *OATH application* for HOTP and TOTP authentication. With the OATH application, you can add OATH credentials for numerous accounts, there are more configuration options (including algorithm, touch requirement, account name, etc.), OTP generation is triggered via the Authenticator application, and the app itself can display the resulting OTPs on all platforms.

With the Yubico OTP application, only counter-based HOTPs generated via the HMAC-SHA1 algorithm are supported. Configuration options are limited to the secret key, OTP size (6 or 8 digits), and an optional carriage return appendage (an **Enter** keystroke).

Once an OTP application slot is configured with an HOTP credential, an HOTP can be generated by "activating" the slot via touch (if the key is connected over USB) or an NFC scan. See *Performing authentication with OTP application slot credentials* for more information.

Note: For additional information on OATH HOTPs and the Yubico OTP application, see the .NET SDK manual.

10.4.1 Configuration

To configure an OTP application slot with an OATH HOTP credential with the HMAC-SHA1 algorithm, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Slots**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

2. Click on the slot you would like to configure and select **OATH-HOTP** under **Setup**.

   To find the **Setup** menu in a narrow app window, click the three dots in the upper right corner of the app.

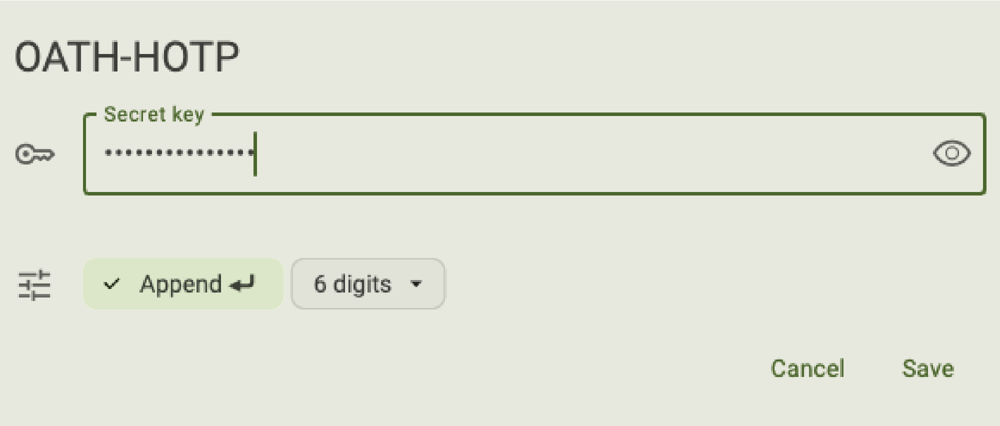
3. Enter an even-numbered **Secret key** up to 40 digits in length. Only the following characters are allowed: letters a through z and numbers 2 through 7.

   Be sure to **make a copy of your secret key**; you will need to share it with the validation server for each of your accounts during registration process.

4. By default, a carriage return (an **Enter** keystroke) will be applied to the end of the OTP. This means that when the password is typed into a field on a login screen, you won't have to click another button to continue the login process. To remove the carriage return, click **Append** until the check mark disappears.

5. Select an OTP length (6 or 8 digits).

6. Click **Save** to complete the configuration. If the slot is already configured with a credential, click **Overwrite** when prompted.

7. After the credential has been added to the appropriate validation servers, you must register your key with your accounts. See the Works with YubiKey Catalog for setup instructions for your particular sites/services.

10.5 Performing authentication with OTP application slot credentials

Once an OTP application slot has been configured with a credential, and that credential has been registered with a compatible site, service, or application, follow the steps detailed here to perform authentication via your designated device and connection type.

10.5.1 Yubico OTP, static password, and HOTP authentication on desktop and Android devices via USB

To generate and submit a Yubico OTP, static password, or HOTP from an OTP application slot for authentication on a desktop or Android device over USB, do the following:

1. Connect your YubiKey to your device over USB.
2. Begin the sign-in process for an account with which your slot credential has been registered.
3. Place your cursor in the OTP code/password text field on the account login screen.
4. Tap the YubiKey's gold contact(s) to activate the credential in the short press slot or touch and hold the YubiKey for a few seconds to activate the credential in the long press slot.
5. The YubiKey will type the Yubico OTP, static password, or HOTP into the text field. If you did not configure the slot to append an Enter keystroke following the OTP/password, click **Submit** (or similar) to complete the login process.

10.5.2 Yubico OTP and HOTP authentication on Android and iOS devices via NFC

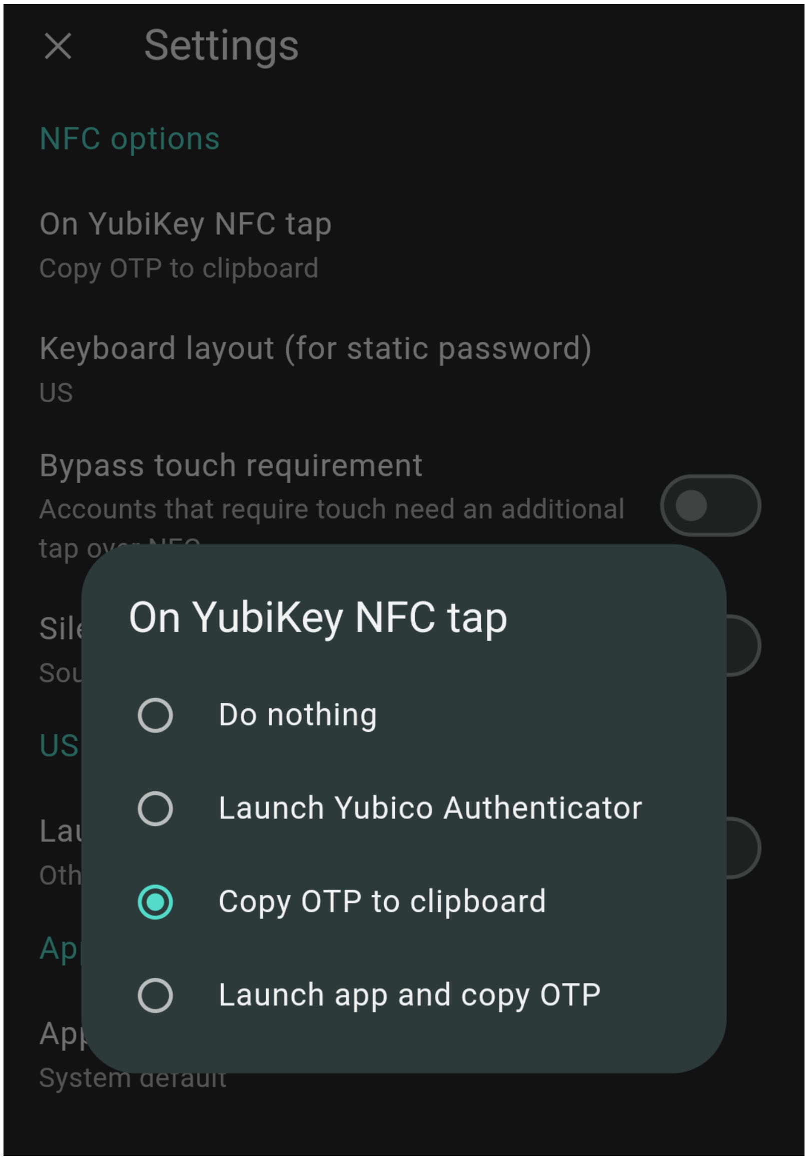
Yubico Authenticator for Android and iOS both support Yubico OTP and HOTP generation via NFC. On iOS devices, the OTP is displayed in the app itself, while on Android devices, the OTP is copied to the clipboard.

Only one slot can be activated over NFC. By default, this is the short press slot. If the slot credential you wish to use over NFC was configured in the long press slot, we recommend *swapping slot configurations*.

Note: Alternatively, the YubiKey can be configured to activate the long press slot over NFC by manipulating the YubiKey's NDEF tag with the YubiKey Manager CLI tool. When calling `ykman otp ndef`, you must use a URI payload with the value `https://my.yubico.com/yk/#`. If a different URI or text payload is used, the Authenticator app will not receive the OTP from the YubiKey.

To get started, do the following:

1. Yubico Authenticator for Android and iOS will not generate OTPs via NFC by default. To enable this feature on Android, *go to Settings*, click **On YubiKey NFC tap**, and select either **Copy OTP to clipboard** or **Launch app and copy OTP**.



Settings

NFC options

On YubiKey NFC tap
Copy OTP to clipboard

Keyboard layout (for static password)
US

Bypass touch requirement
Accounts that require touch need an additional tap ov

Sile
Sou

US

Lau
Oth

Ap

App
System default

On YubiKey NFC tap

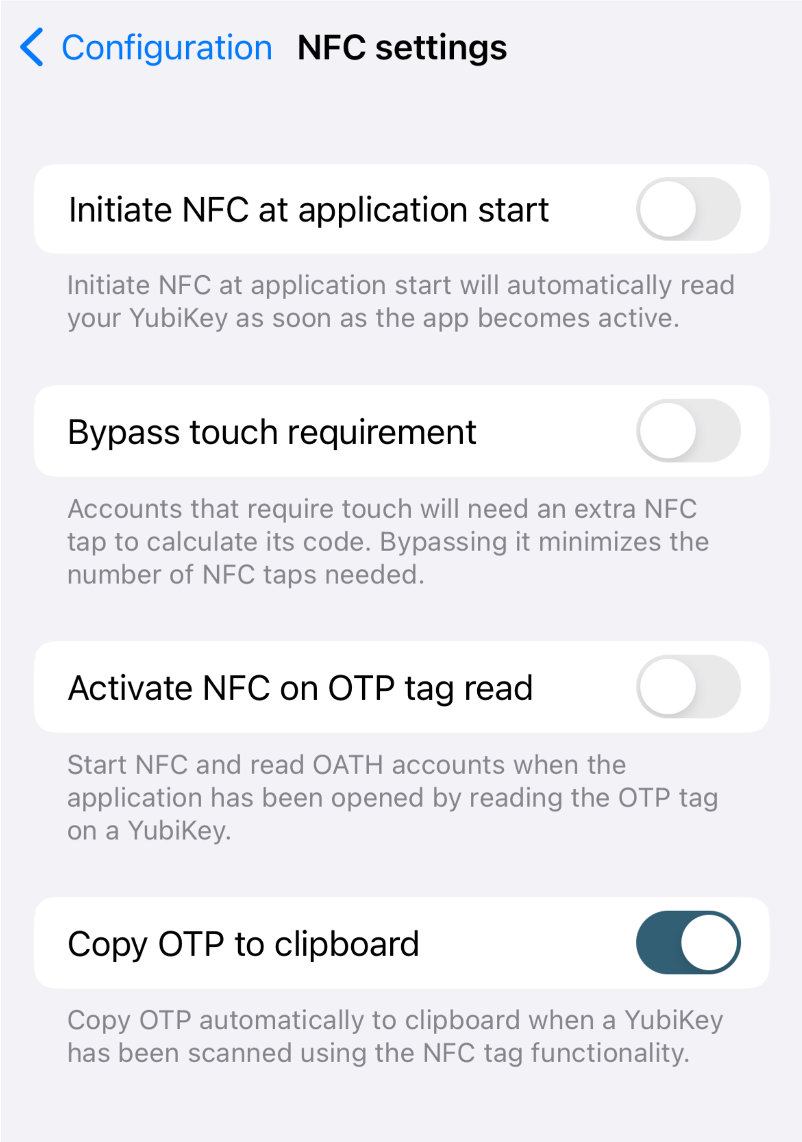
○ Do nothing

○ Launch Yubico Authenticator

● Copy OTP to clipboard

○ Launch app and copy OTP

To enable this feature on iOS, *go to Configuration*, click **NFC settings**, and select **Copy OTP to clipboard**.



Initiate NFC at application start

Initiate NFC at application start will automatically read your YubiKey as soon as the app becomes active.

Bypass touch requirement

Accounts that require touch will need an extra NFC tap to calculate its code. Bypassing it minimizes the number of NFC taps needed.

Activate NFC on OTP tag read

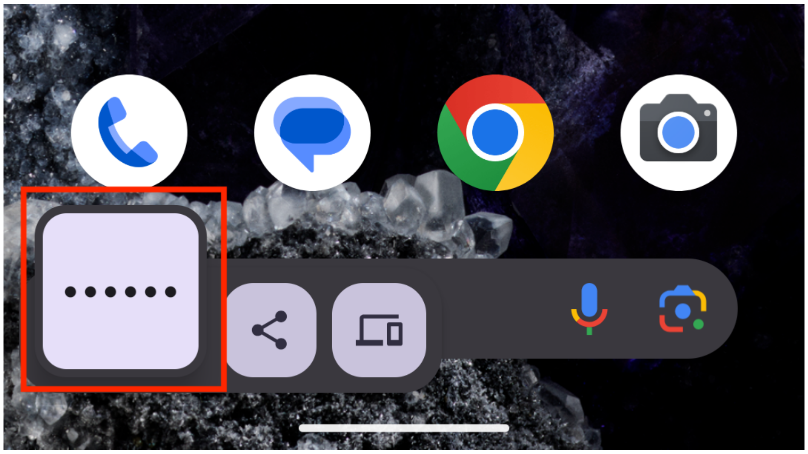
Start NFC and read OATH accounts when the application has been opened by reading the OTP tag on a YubiKey.

Copy OTP to clipboard

Copy OTP automatically to clipboard when a YubiKey has been scanned using the NFC tag functionality.

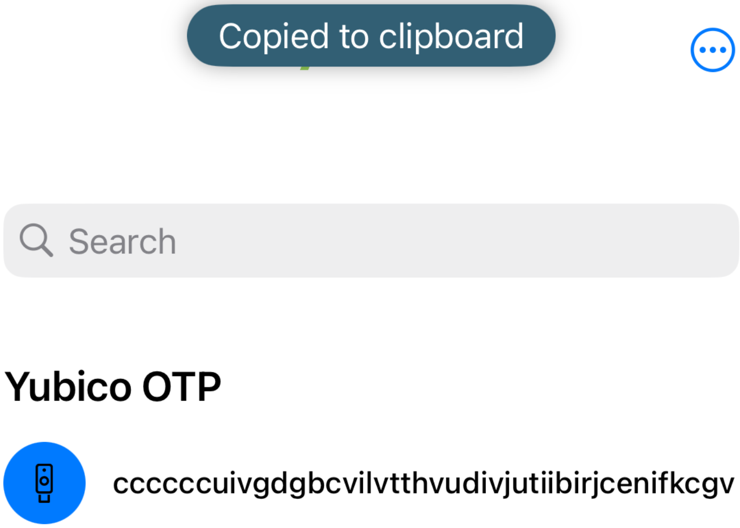
2. Begin the sign-in process for an account with which your OTP credential has been registered.

3. To generate the OTP on Android, start by closing or hiding the Authenticator app. If the app is open on screen, a new OTP will not be generated. Next, hold the YubiKey up to the device's NFC reader. Once the key is scanned, you will see the clipboard preview icon (for Android 13 devices and newer) or a message confirming receipt of the OTP (for Android 12 devices and older) at the bottom of the screen.



Now that the clipboard contains the OTP, paste it into the login screen to complete authentication.

To generate the OTP on iOS, hold the YubiKey up to the device's NFC reader (the Authenticator app can be open, closed, or hidden). Click on the notification that appears at the top of the screen prompting you to open the NFC tag in Authenticator. The OTP will be displayed in the app and copied automatically to the clipboard. Paste the OTP into the login screen to complete authentication.


Copied to clipboard

Yubico OTP

cccccuivgdgbcvilvtthvudivjutiibirjcenifkcgv

10.5.3 Challenge-response authentication

Unlike the other slot configuration types, challenge-response is initiated via an API call from the site or application you are attempting to authenticate to. This API call sends a challenge to the YubiKey, which must be physically connected to your device. The YubiKey takes the challenge (after the user touches the key, if touch is required) and hashes it using the secret key the slot was configured with. The key then sends the response back to the site or application for validation.

See the Works with YubiKey Catalog for more specific authentication instructions for your particular site or application.

10.6 Managing slots

There are only two options for managing Yubico OTP application slots: swap or delete.

Swapping slots means moving the configuration in the short press slot to the long press slot and vice versa. This could be useful when the credential you use most often is in the long press slot; by moving that credential to the short press slot, activation only requires tapping the key briefly instead of touching and holding for a few seconds.

Deleting a slot's configuration is an irreversible operation, so exercise caution. We recommend registering at least one *spare key* with your accounts in order to maintain account access prior to deleting a configuration.

10.6.1 Swap slots

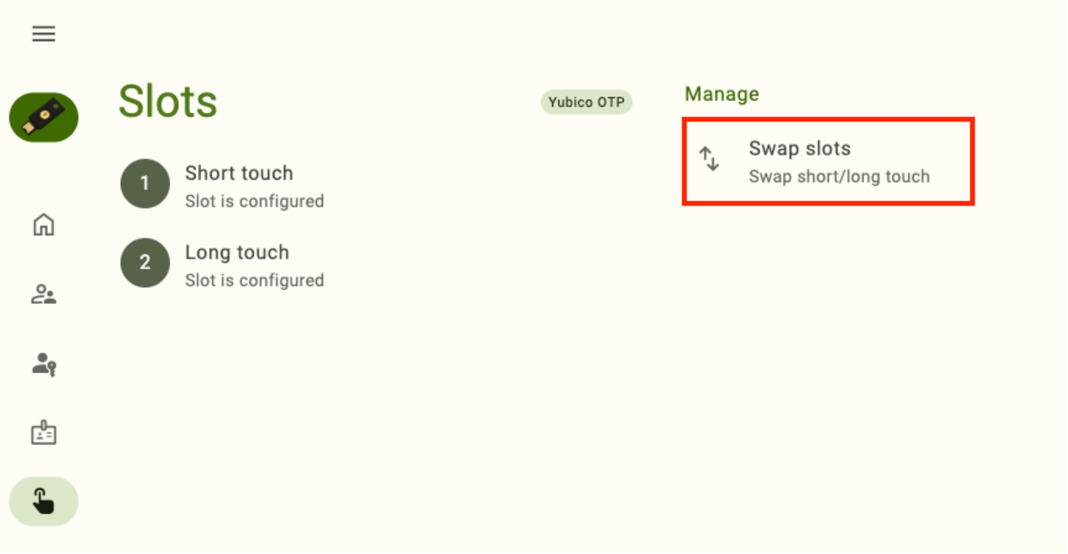
To swap the slot configurations, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Slots**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

2. Select **Swap slots** under **Manage**.

   To find the **Manage** menu in a narrow app window, click the three dots in the upper right corner of the app.



3. Click **Swap** to confirm the operation. The configuration that was previously in the short touch slot is now in the long touch slot and vice versa.

10.6.2 Delete a slot's configuration

To delete a slot's configuration, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Slots**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

2. Click on the slot whose configuration you would like to delete and select **Delete credential** under **Setup**.

   To find the **Setup** menu in a narrow app window, click the three dots in the upper right corner of the app.

3. Click **Delete** to confirm the operation.

CHAPTER

ELEVEN

FACTORY RESET

With the help of Yubico Authenticator, the YubiKey can be reset to factory default settings *by application*.

Depending on the YubiKey model and platform, this can include the *FIDO2*, *OATH*, and *PIV* applications. For all YubiKey models except for the YubiKey Bio Series Multi-protocol Edition (MPE), if one application is reset, the others are not affected.

Note: YubiKey Bio Series Multi-protocol Edition (MPE) keys share a PIN between the PIV and FIDO2 applications. Therefore, a reset affects **both** applications.

Once an application is reset, the operation **cannot be undone**.

11.1 What happens during a reset?

When the FIDO2 application is reset, *Enterprise Attestation* (available with custom-configured keys only) is disabled, and the FIDO2 PIN and all *fingerprints*, *passkeys*, and non-passkey FIDO2 credentials are removed from the YubiKey. Similarly, when the OATH application is reset, all OATH account credentials plus the OATH application password are removed.

When the PIV application is reset, all private keys and certificates are removed from the YubiKey, and the PIN, PUK, and management key are reset to their factory default values.

The Yubico OTP application itself can't be reset, but the configuration of each slot can be deleted. See *Slots: Yubico OTP Application* for instructions on how to perform this operation.

Note: For YubiKey 5 FIPS Series keys with firmware version 5.7 or later, a reset will return all "FIPS approved" applications back to the "FIPS capable" *state*.

11.2 How does a reset affect my accounts?

While a reset removes credentials from the YubiKey, it does not affect the accounts and services that those credentials are registered with.

For example, suppose you registered a YubiKey for OATH authentication with your GitHub account. If you reset the OATH application on your key, the OATH credentials linked to your GitHub account will be removed from the key, but if you log into your GitHub account, you'll still see the key registered for two-factor authentication in your settings. However, you will not be able to authenticate to your account using that key because it no longer has the corresponding OATH credentials. To use the key with that account again, you will have to reregister it.

11.3 Recommended preparation

Prior to performing a reset, we recommend that you either *register a backup YubiKey* *or* temporarily disable two-factor authentication with each account that will be affected by the reset. This ensures that you will still be able to access those accounts once your key is reset.

For passkey and OATH credentials, you can view a list of registered accounts in Yubico Authenticator by going to the **Passkey** and **Accounts** screens, respectively.

11.4 Performing a reset on desktop and Android

To reset an application, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Home**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

2. Select **Factory reset** under **Device**.

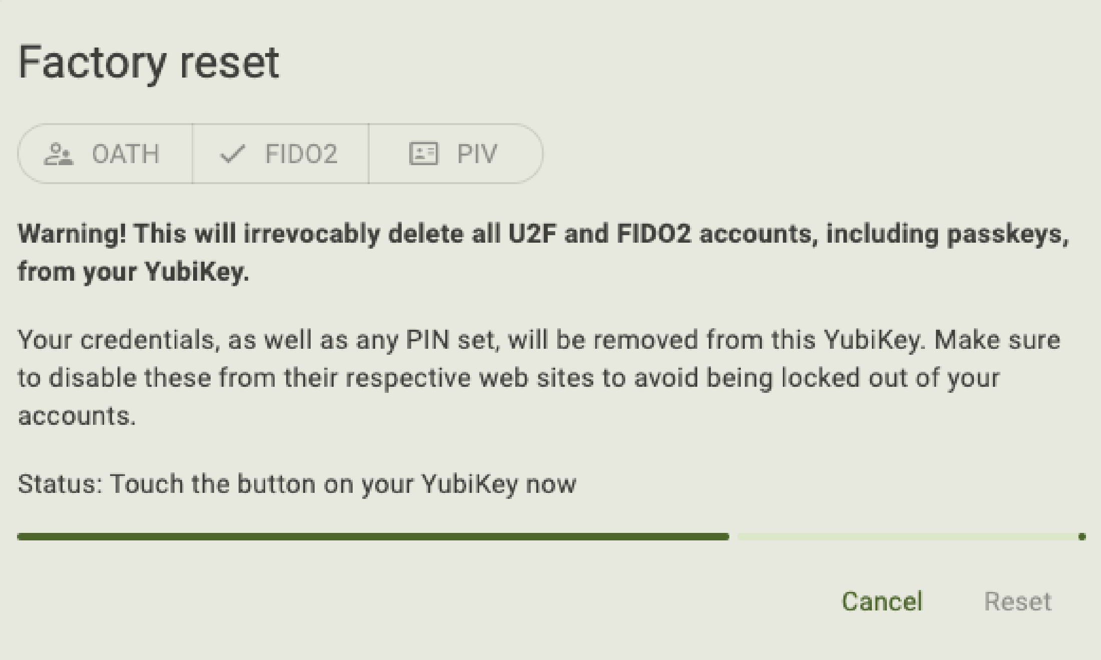
   To find the **Device** menu in a narrow app window, click the three dots in the upper right corner of the app.

3. In the **Factory reset** window, select the application you'd like to reset and click **Reset**.

   YubiKey Bio Series Multi-protocol Edition (MPE) keys share a PIN between the PIV and FIDO2 applications. Therefore, a reset affects **both** applications. You cannot select an application to reset individually for Bio Series MPE keys.

4. If you selected the OATH application and are connected via NFC on Android, tap your key against the NFC reader when prompted. No other steps are required to perform the reset for OATH and PIV.

   For the FIDO2 application with USB connections, unplug your YubiKey, reinsert your key into your device, and touch your key when prompted (for YubiKey Bio Series keys, touch the fingerprint sensor; for all other keys, touch the gold contact). Once the status reads "FIDO application reset", click **Close** on desktop or the **X** on Android to return to **Home**.



Factory reset

Warning! This will irrevocably delete all U2F and FIDO2 accounts, including passkeys, from your YubiKey.

Your credentials, as well as any PIN set, will be removed from this YubiKey. Make sure to disable these from their respective web sites to avoid being locked out of your accounts.

Status: Touch the button on your YubiKey now

For the FIDO2 application with desktop NFC connections, remove your key from the NFC reader and place it back on the NFC reader when prompted. Once the status reads “FIDO application reset”, click **Close**.

For the FIDO2 application with NFC connections on Android, tap your key against the NFC reader when prompted. Once the operation is complete, click the **X** to return to **Home**.

Once the key has been reset, you must reregister it with your accounts to continue using it for authentication with those sites and services.

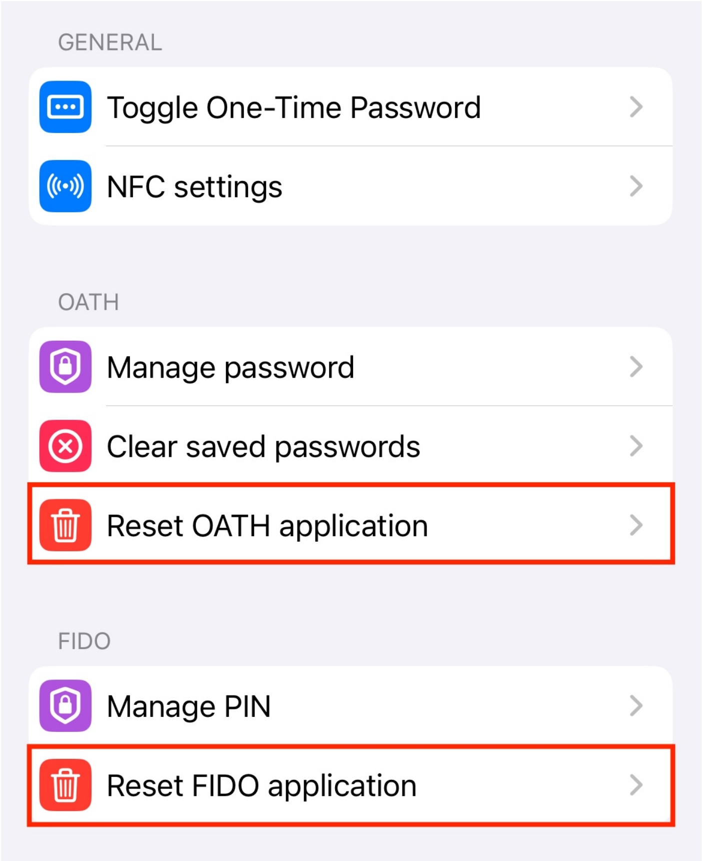
11.5 Performing a reset on iOS/iPadOS

For Yubico Authenticator for iOS, only the OATH and FIDO2 applications can be reset. In addition, **FIDO2 reset on iOS is limited to NFC connections for YubiKeys with a firmware version prior to 5.7.4**. iPads do not have built-in NFC readers, therefore, only OATH reset is supported on iPadOS at this time. To perform a reset for one of these applications on your iOS/iPadOS device, do the following:

1. Open the Yubico Authenticator app. For Lighting connections, plug in your YubiKey. For NFC connections, swipe down on the screen and tap your YubiKey on the back of your device to scan.

Note: Lightning is currently the only supported *physical* connection type for iOS and iPadOS devices. NFC wireless connections are supported on iOS but not on iPadOS. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

2. Click the three dots in the upper right corner of the app and select **Configuration**.
3. To reset the OATH application, select **Reset OATH application** under the **OATH** section. Click **Reset OATH** followed by **Reset** to confirm the operation. For NFC connections, scan your key when prompted.
4. To reset the FIDO2 application on iOS (NFC connections only for YubiKeys with a firmware version prior to 5.7.4), select **Reset FIDO application** under the **FIDO** section. Click **Reset FIDO** followed by **Reset** to confirm the operation. Scan your key when prompted.



Once the key has been reset, you must reregister it with your accounts to continue using it for authentication with those sites and services.

CHAPTER

TWELVE

TIPS

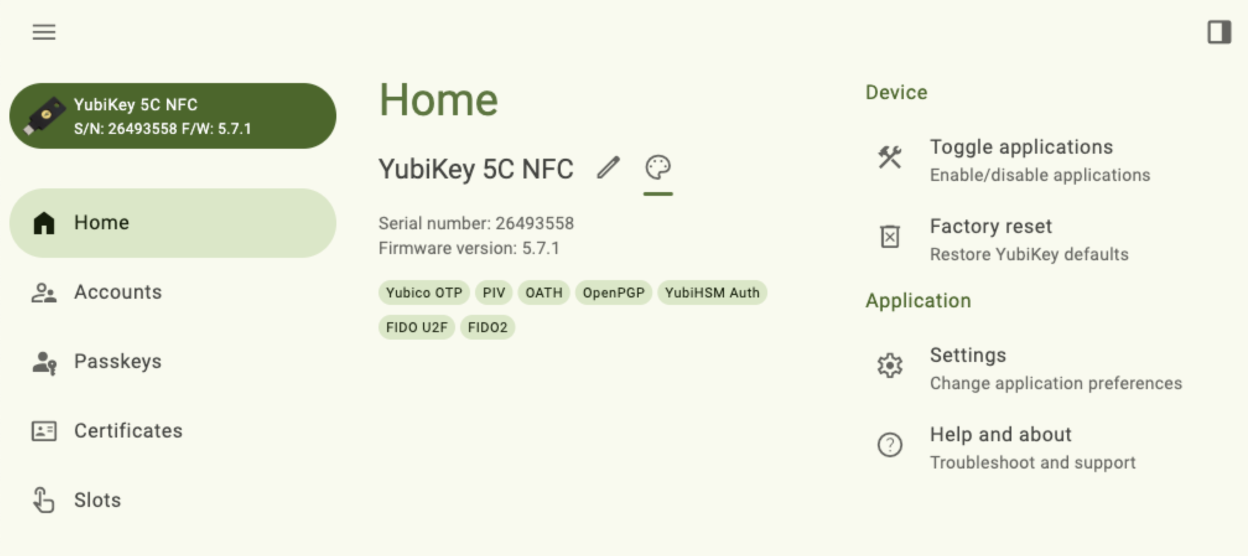
The following tips and tricks can help you take full advantage of the Yubico Authenticator application's functionality:

- *Resize the app window on desktop and Android tablets to your preferred size.*
- *Register spare YubiKeys with your accounts to maintain access in the event of a loss of your primary YubiKey.*
- *Start Yubico Authenticator with the app window hidden to reduce desktop clutter.*
- *As a convenient shortcut, generate OATH OTPs from pinned accounts via the menu bar or system tray on desktop devices.*
- *Set an OATH application password to add an additional layer of security.*
- *Speed up Yubico Authenticator operations with the help of keyboard shortcuts*
- *Check out the Works with YubiKey Catalog for compatibility information (by YubiKey model, security protocol, and site/service/account) and account setup information.*

12.1 Resize the app window

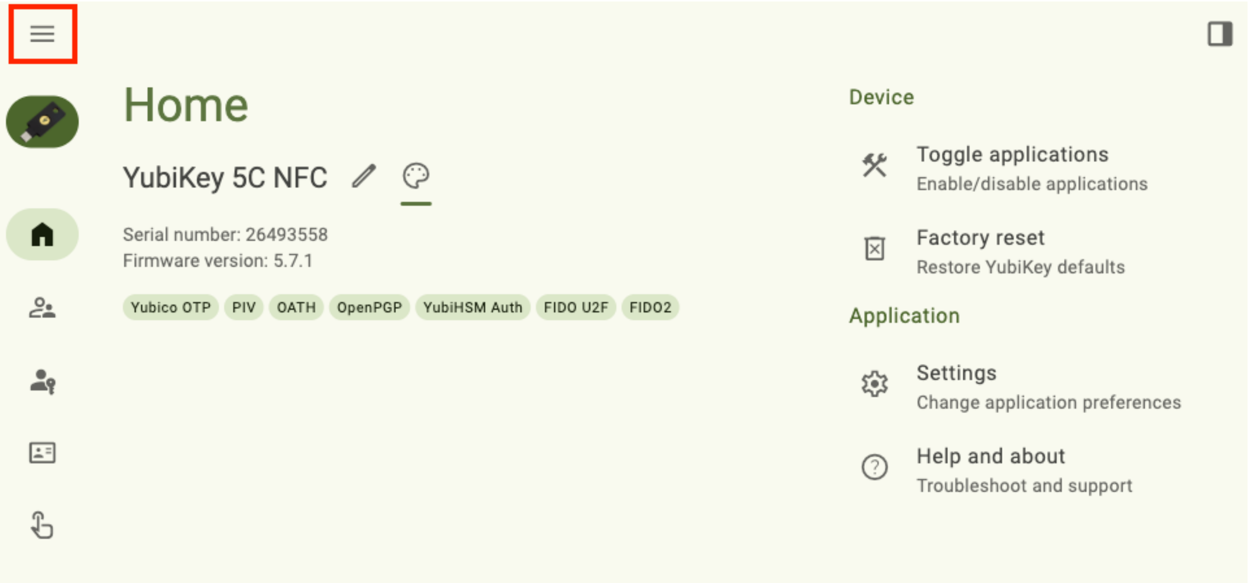
Note: The app window size can only be changed on desktop and Android tablet devices.

The Yubico Authenticator app window can be resized by both height and width. The default window width on most desktop devices shows the following:



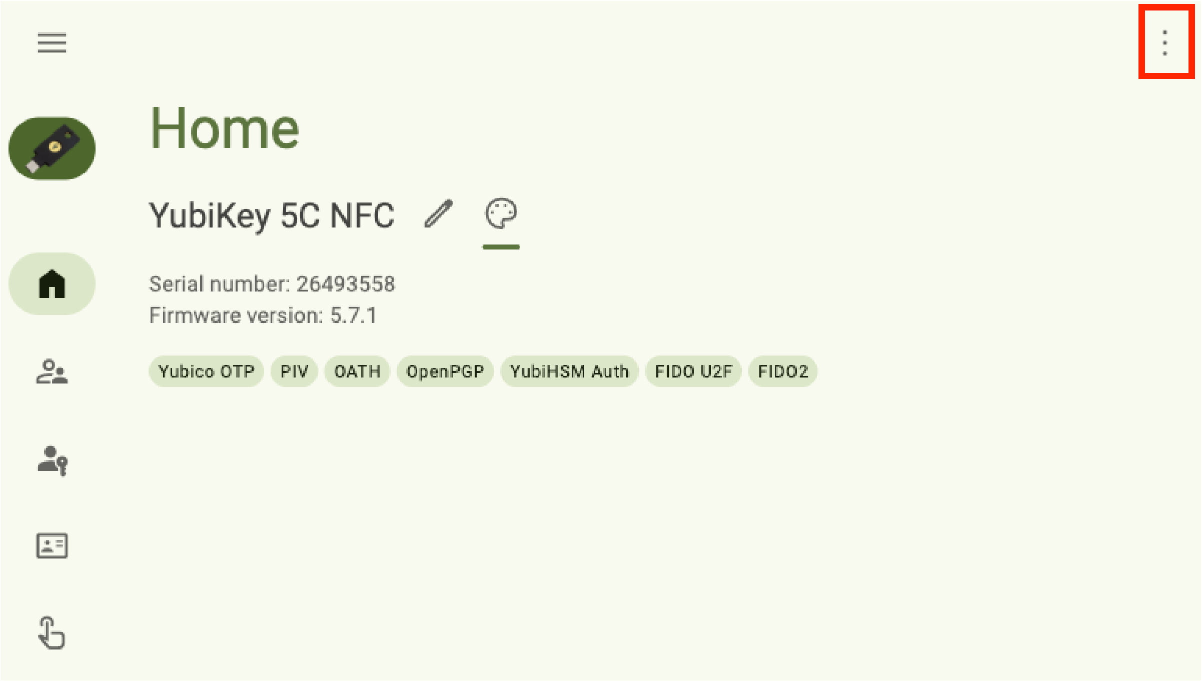
Serial number: 26493558
Firmware version: 5.7.1

When the window is narrowed sufficiently, only the icons for the left-hand menu items are shown. To view the full icon text (page titles and YubiKey information), click the three lines in the upper left corner of the app:



Serial number: 26493558
Firmware version: 5.7.1

Narrowing the window again hides the right-hand menu. However, these menu options can still be accessed by clicking the three dots in the upper right corner of the app:

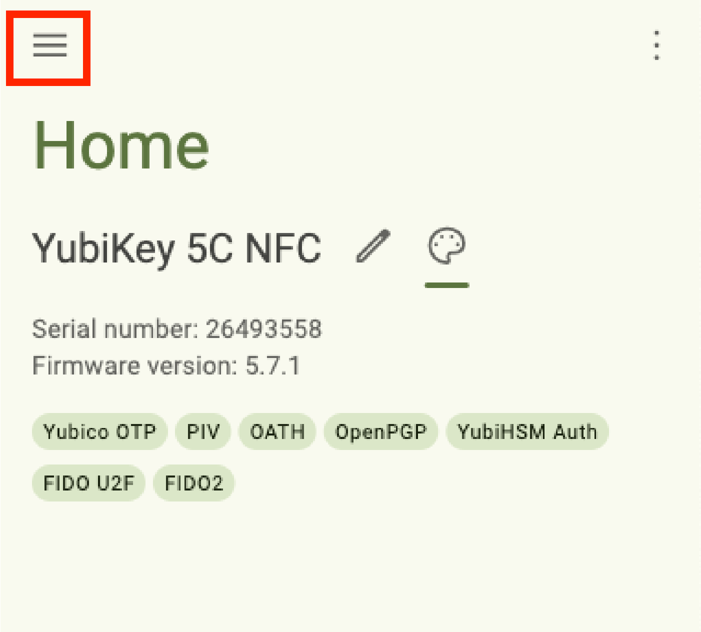


Home

YubiKey 5C NFC

Serial number: 26493558
Firmware version: 5.7.1

Further narrowing the width makes all page icons disappear. However, these pages can still be accessed by clicking the three lines in the upper left corner:

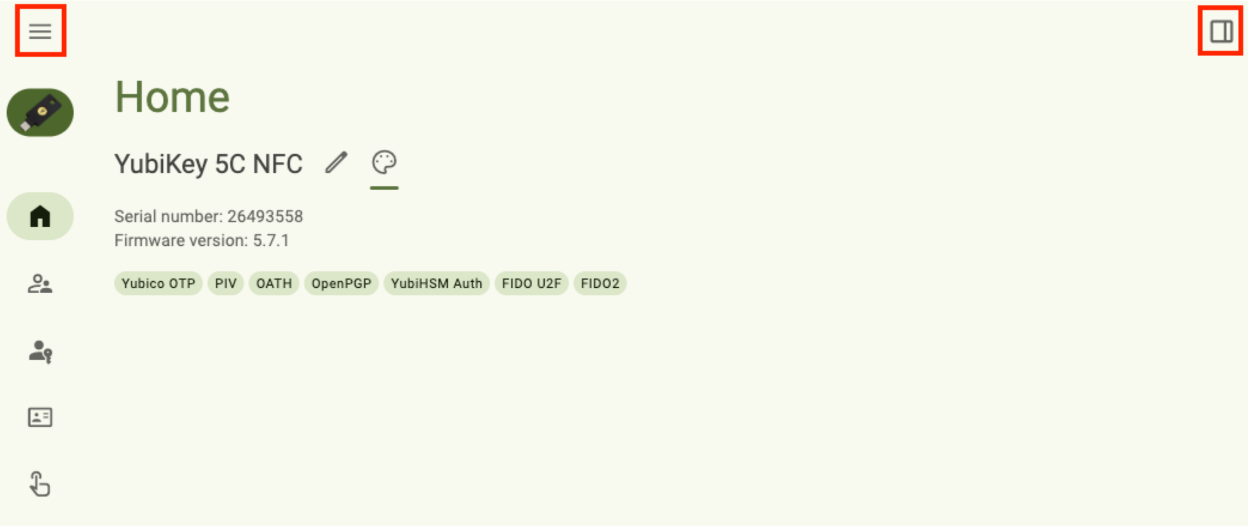


Home

YubiKey 5C NFC

Serial number: 26493558
Firmware version: 5.7.1

When the window is fully widened, all menu items are expanded. To collapse the left-hand menu items, click the three lines in the upper left corner. To collapse the right-hand menu items, click the page icon in the upper right corner. Click the icons again to re-expand.



Home

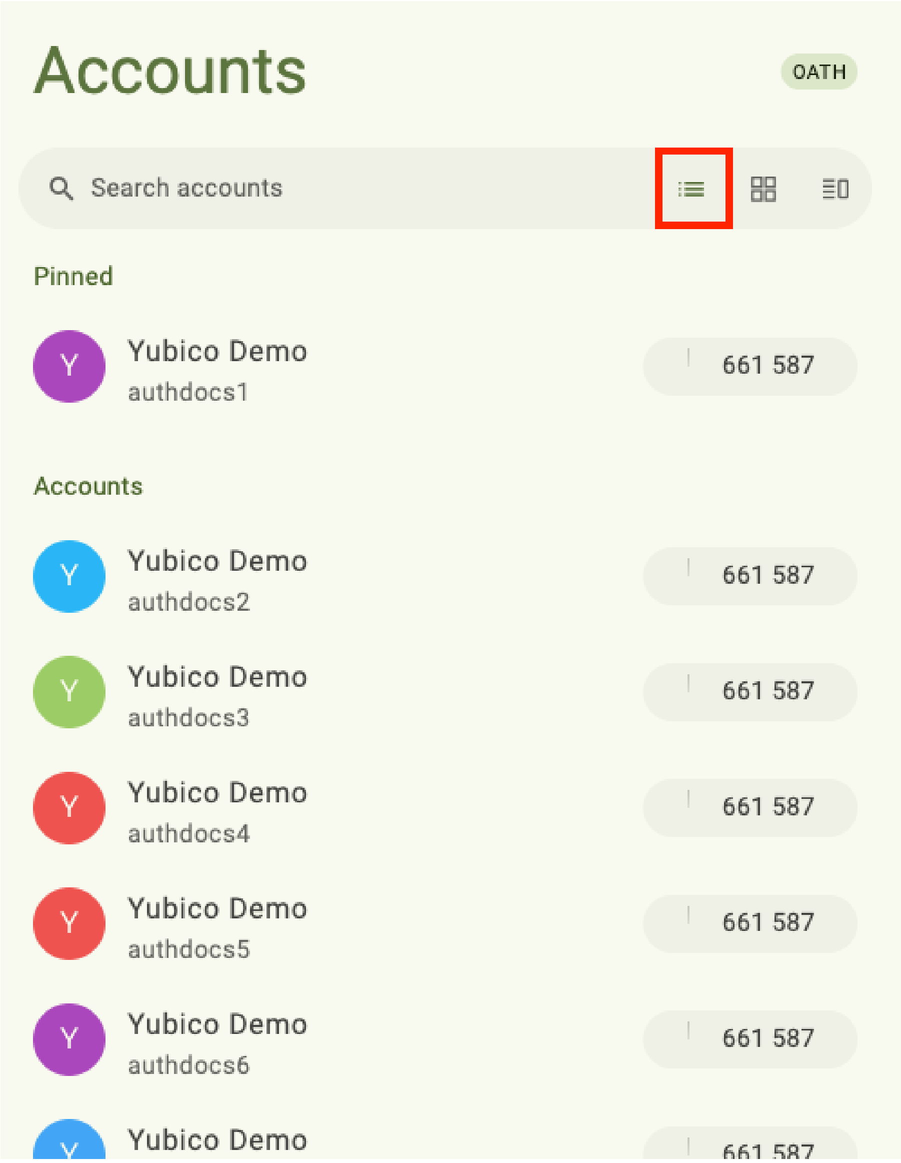
YubiKey 5C NFC

Serial number: 26493558
Firmware version: 5.7.1

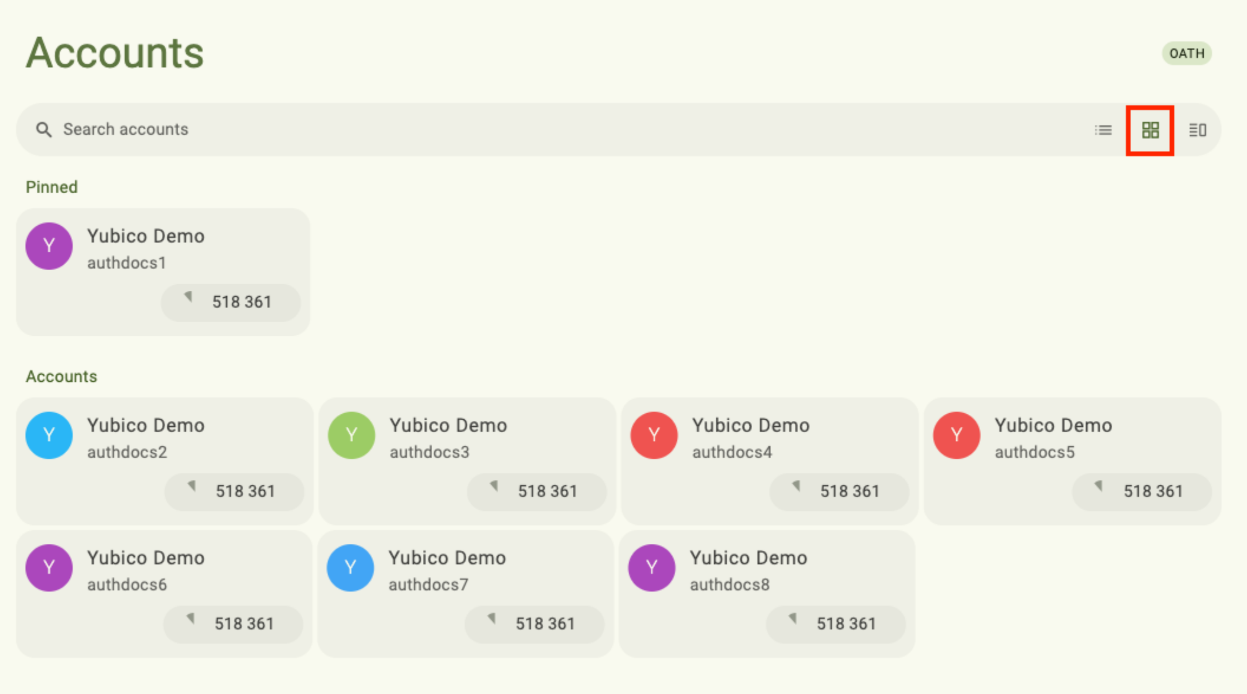
12.2 Change the Accounts and Passkeys screen layouts

Note: The Passkeys and Accounts screen layouts can only be changed on desktop and Android devices.

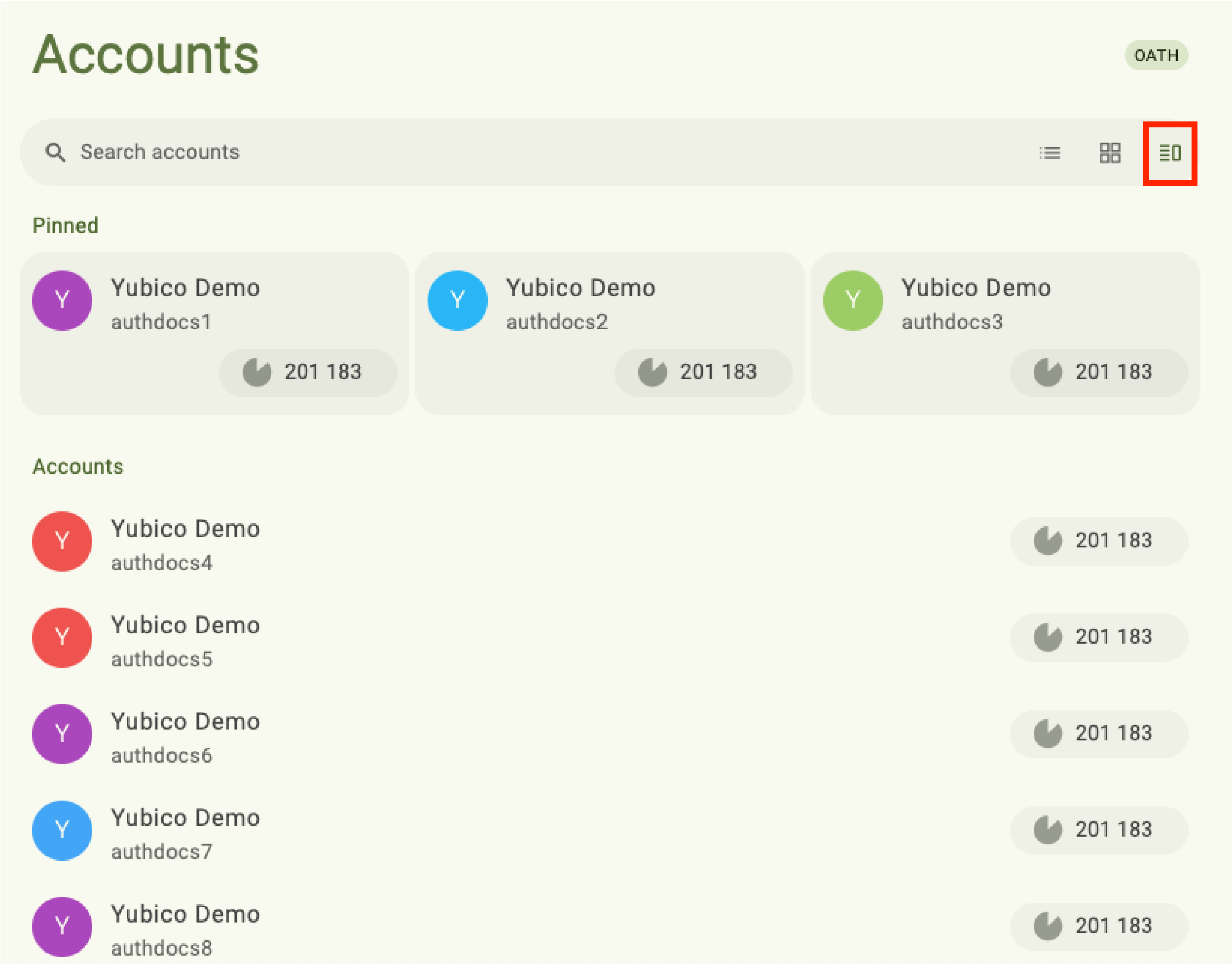
If you have a lot of passkeys or OATH accounts on your YubiKey, it may not be possible to see them all in Yubico Authenticator without scrolling when using the default **List layout**:



However, desktop and Android tablet devices can take advantage of a wider screen by using the **Grid layout**:



Or for the best of both worlds, try the **Mixed layout** (available for the Accounts screen only and requires that at least one account be *pinned*):



Accounts

OATH

Search accounts

Pinned

Yubico Demo
authdocs1
201 183

Yubico Demo
authdocs2
201 183

Yubico Demo
authdocs3
201 183

Accounts

Yubico Demo
authdocs4
201 183

Yubico Demo
authdocs5
201 183

Yubico Demo
authdocs6
201 183

Yubico Demo
authdocs7
201 183

Yubico Demo
authdocs8
201 183

Toggle between the layout options on the Accounts and Passkeys screens by selecting the desired layout icon in the search bar.

12.3 Register a spare YubiKey

We highly recommended registering at least one backup YubiKey with each account you have. In the event that you lose your primary YubiKey, you will still be able to access your accounts with your spare key.

The registration process for the spare key depends on the type of authentication and the specific site/service. Refer to the following sections.

12.3.1 OATH accounts

To register a spare YubiKey for *OATH authentication*, the OATH account must be *added* to the spare key using the **same** QR code and credentials as your primary key. This means that the primary key and spare key will generate the same TOTP codes in Yubico Authenticator on any device.

For many sites and services, OATH authentication is often referred to as “registering an authenticator app” in your account settings. Generally, these sites/services allow you to register only one application, meaning that only one set of OATH credentials can be associated with your account at a time. So to be able to use more than one YubiKey to generate TOTP codes in Yubico Authenticator for a single account, each of those keys must have the same credentials so that they can generate the same TOTPs.

If you do not have a copy of the QR code or OATH credentials used to register your primary key, you will have to remove your primary key from your account and reregister the primary key along with the spare key. To do so, perform the following:

1. Locate the OATH authentication settings within your account. For guidance on how to find this with your particular site/service, see the Works with YubiKey catalog.
2. Remove the registered key/app and generate a new QR code or OATH credentials. Take a screenshot of the QR code or copy the OATH credentials.
3. Perform the full *registration process* for the primary key.
4. Register the account with the spare key in Yubico Authenticator using the screenshot of the QR code or copy of the OATH credentials. You do not need to provide another TOTP to the site/service in order to complete the registration process; once your primary key has been successfully registered, spare keys need only to be configured in the Yubico Authenticator app.
5. Once completed, you should see the keys generate the same TOTP codes in the Yubico Authenticator app. As a security best practice, delete the QR code screenshot or copy of the OATH credentials once all spare keys have been registered.

12.3.2 Passkeys

To register a spare YubiKey for use as a *passkey* with an existing account or service, follow the same steps you performed when registering your primary key. See the Works with YubiKey catalog for more information on your account’s specific registration process.

12.3.3 Yubico OTP application credentials

Spare YubiKeys can be configured for all Yubico OTP application configuration types:

- Yubico OTP
- Challenge-response
- Static password
- OATH HOTP

Yubico OTPs

For sites and services that use Yubico OTP authentication, *register* a spare key the same way that you registered the primary key. See the Works with YubiKey catalog for more information on your account's specific registration process.

An important caveat: if the site/service in question uses the YubiCloud validation service and the Yubico OTP credential on your spare key has not been registered with YubiCloud, you will need to do that prior to registering the key with the site/service. To register a Yubico OTP credential with YubiCloud, upload the required information via the Yubico OTP key upload form. You will need the key's serial number, public ID, private ID, and secret key.

How do you know if your Yubico OTP credential is registered with YubiCloud? Generate and submit a Yubico OTP with your key for validation on the Yubico demo site. As a reminder, tap the key briefly to active the short press slot or touch and hold the key to activate the long press slot.

Note: Standard YubiKeys are preconfigured with a Yubico OTP in the short press slot. This credential is also preregistered with YubiCloud for out-of-the-box validation.

If the site/service uses a non-YubiCloud validation server, the OTP credential information (serial number, public ID, private ID, and secret key) will need to be shared with the server during the registration process.

Challenge-response credentials

To register a spare YubiKey for challenge-response authentication, you must *configure* a slot of the spare YubiKey with the same challenge-response secret key as your primary key.

If you do not have a copy of the secret key that the primary key was configured with, you will have to reconfigure and reregister the primary key in addition to configuring the spare key.

Static passwords

To register a spare YubiKey for static password authentication, you must *configure* a slot of the spare YubiKey with the same static password and keyboard layout as your primary key.

If you do not remember your static password, open a text editor and activate the slot on your primary key that is configured with the static password (tap the key briefly to active the short press slot or touch and hold the key to activate the long press slot). The static password will be typed into the text editor.

If you do not remember the keyboard layout the primary key was configured with, you will have to reconfigure and reregister the primary key in addition to configuring the spare key.

OATH HOTP

To register a spare YubiKey for OATH HOTP authentication, you must *configure* a slot of the spare YubiKey with the same OATH HOTP secret key and OTP length as your primary key.

If you do not have a copy of the secret key that the primary key was configured with, you will have to reconfigure and reregister the primary key in addition to configuring the spare key.

If you do not remember the OTP length that the primary key was configured with, open a text editor and activate the slot on your primary key that is configured with the OATH HOTP credential (tap the key briefly to active the short press slot or touch and hold the key to activate the long press slot). The HOTP will be typed into the text editor. Count the number of digits present; this is the OTP length.

12.4 Start Yubico Authenticator with the app window hidden

Note: Yubico Authenticator can only be started in the "hidden" state on desktop devices.

To reduce desktop clutter, Yubico Authenticator can be started in the "hidden" state; the app runs in the background, but the app window will not be shown until requested.

OATH OTPs can still be *generated for pinned accounts from the menu bar/system tray* while the app window is hidden.

To start the app with the window hidden, start a terminal and pass the `--hidden` argument when opening the app. The full command depends on your OS:

macOS:

```
open -a "Yubico Authenticator" --args --hidden
```

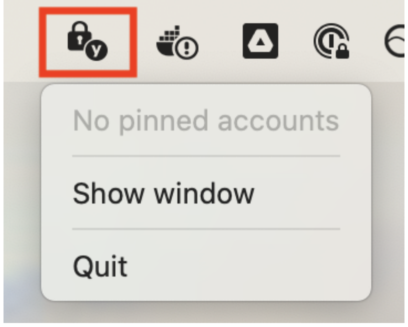
Windows:

```
C:\Program Files\Yubico\Yubico Authenticator\authenticator.exe --hidden
```

Linux:

```
/path/to/authenticator --hidden
```

Once the app has been started, you will see the Yubico Authenticator icon in the menu bar (macOS) or system tray (Windows, Linux). To show the app window, click on this icon and select **Show window**. To hide the window again, click on the icon and select **Hide window**.



12.5 Generate OATH OTPs from pinned accounts via the menu bar or system tray

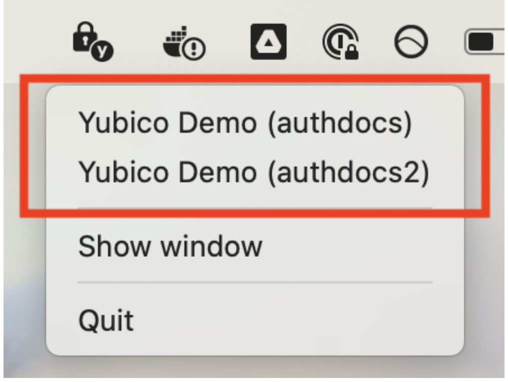
Note: OATH OTPs can only be generated from the menu bar or system tray on desktop devices.

When Yubico Authenticator is running (with the app window shown *or hidden*), OTPs can be generated for *pinned* accounts from the menu bar (macOS) or system tray (Windows, Linux) instead of within the app window itself. To do so, perform the following:

1. Plug your YubiKey into your device.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader.

2. If the OATH application of your YubiKey is protected with a *password*, enter that password on the **Accounts** screen in Yubico Authenticator and click **Unlock**. If you remove your key from your device and reconnect it at any point, you will need to enter your OATH password again.
3. Click on the Yubico Authenticator icon in the menu bar (macOS) or system tray (Windows, Linux). Select the OATH account for which you would like to generate an OTP.



4. If touching the key is not required to generate the OTP, the YubiKey will light up and remain illuminated for several seconds. This means the key generated the OTP and copied it to the clipboard automatically. Paste the OTP into the desired window.

   If touching the key *is* required, the YubiKey will flash until you touch the gold contact. Once touched, the key will generate the OTP and copy it to the clipboard.

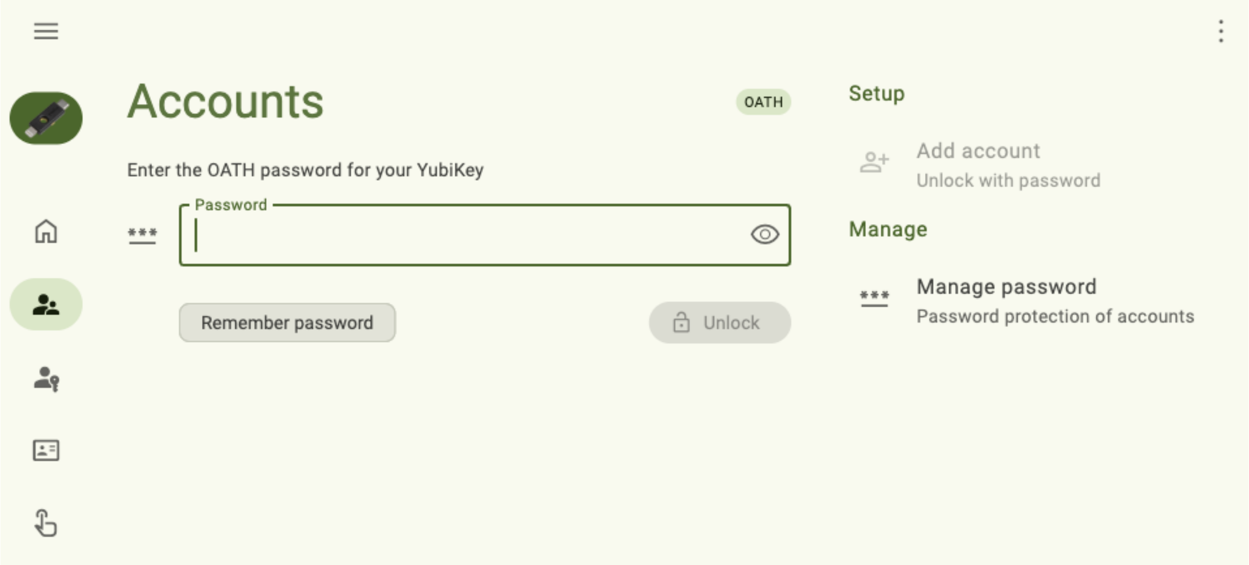
Important: For some Linux configurations running Wayland, copying an OTP to the clipboard only works when the app has focus (as in, you've clicked on the Yubico Authenticator app window). If you are unable to reliably copy to the clipboard from the system tray icon, you can use a separate binary which takes the payload to stdin by defining the environment variable `_YA_TRAY_CLIPBOARD`. This must be an absolute path to a binary owned by root:root and should not be world-writable. For example: `_YA_TRAY_CLIPBOARD=/usr/bin/wl-copy`.

Only use a trusted binary. OTPs will be sent to it when copied to the clipboard from the system tray.

12.6 Set an OATH application password

Note: OATH-compatible YubiKeys include the YubiKey 5 Series (standard, FIPS, and CSPN), YubiKey 4 Series, and YubiKey NEO.

To further enhance the security of your YubiKey, create a password for its OATH application. Once the OATH application has password protection, the key's OATH accounts and their OTPs cannot be viewed or generated until the correct password is entered in the Yubico Authenticator app.



Enter the OATH password for your YubiKey

To create and manage an OATH password, see the *OATH Accounts chapter*.

12.7 Keyboard shortcuts

Note: Keyboard shortcuts are fully supported on Yubico Authenticator for Desktop only.

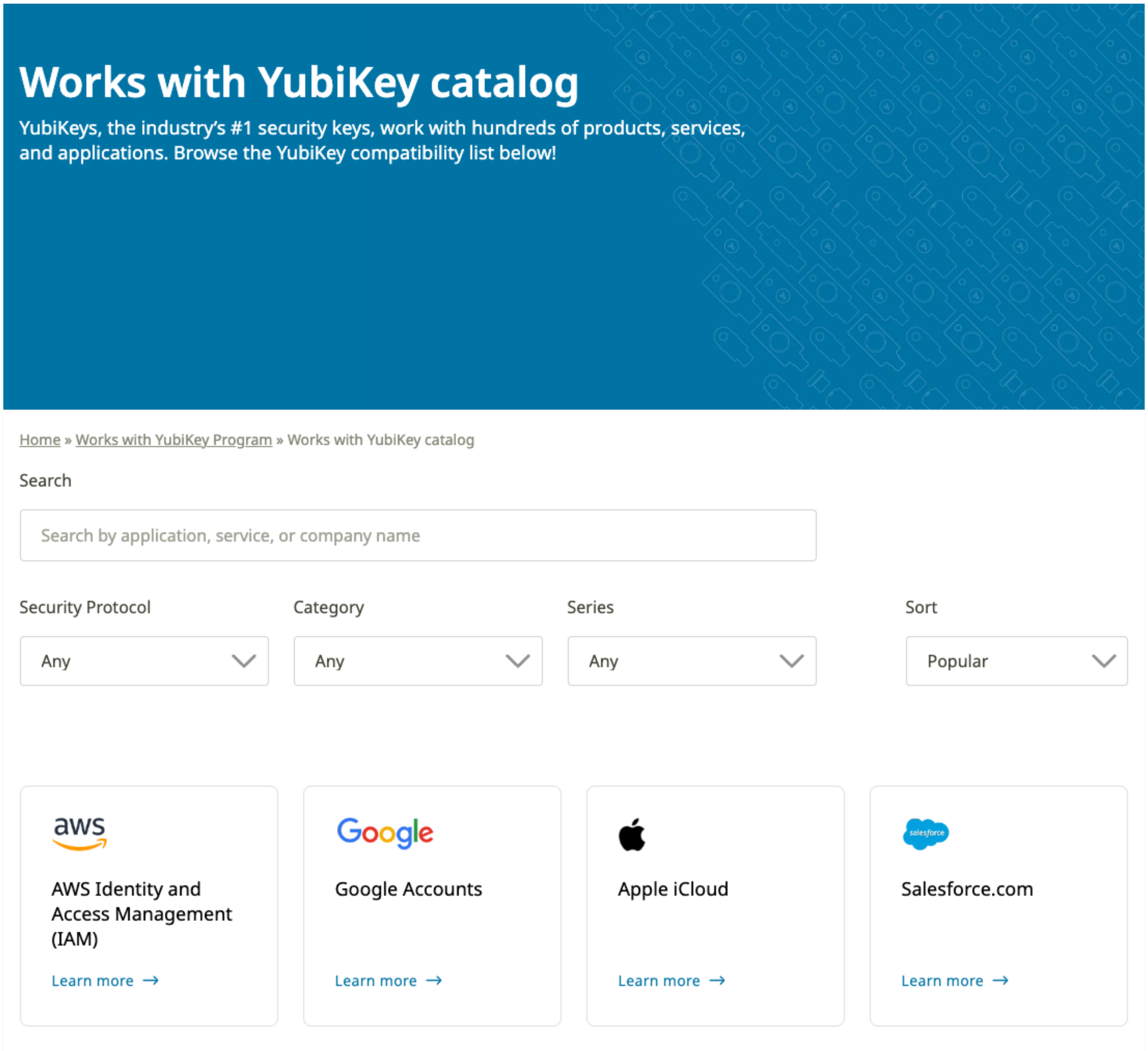
Take advantage of the available keyboard shortcuts to speed up operations such as calculating OATH codes, toggling through connected YubiKeys and menu items, and hiding the app.

Top view the full list of keyboard shortcuts within Yubico Authenticator, go to the **Home** screen, select **Help and about**, and click on **Shortcuts** under the **Help and feedback** section.

Operation	Shortcut (macOS)	Shortcut (Windows)
Open **Keyboard shortcuts** help screen	Cmd + /	Ctrl + /
Expand/collapse left menu	Cmd + B	Ctrl + B
Expand/collapse right menu	Option + Cmd + B	Alt + Ctrl + B
Open Search (if available)	Cmd + F	Ctrl + F
Dismiss/close	Escape	Escape
Next YubiKey	Ctrl + Tab	Ctrl + Tab
Previous YubiKey	Ctrl + Shift + Tab	Ctrl + Shift + Tab
Open **Help and about**	F1	F1
Hide Yubico Authenticator	Cmd + W	Ctrl + W
Quit Yubico Authenticator	Cmd + Q	Not supported
Open **Settings**	Cmd + ,	Not supported
Calculate OATH code	Cmd + R	Ctrl + R
Copy OATH code to clipboard	Cmd + C	Ctrl + C
Navigate within Yubico Authenticator	Arrow keys	Arrow keys
Open item details	Return or Space	Enter or Space
Delete item	Delete	Delete

12.8 Works with YubiKey Catalog

Not sure if a particular site or service supports a specific security protocol or YubiKey model? Check out the Works with YubiKey Catalog to quickly and easily find compatibility information.



Works with YubiKey catalog

YubiKeys, the industry's #1 security keys, work with hundreds of products, services, and applications. Browse the YubiKey compatibility list below!

Home » Works with YubiKey Program » Works with YubiKey catalog

Search

Search by application, service, or company name

Security Protocol: Any

Category: Any

Series: Any

Sort: Popular

AWS Identity and Access Management (IAM)
Learn more →

Google Accounts
Learn more →

Apple iCloud
Learn more →

Salesforce.com
Learn more →

CHAPTER

THIRTEEN

TROUBLESHOOTING AND SUPPORT

Running into problems with Yubico Authenticator? Check the guidance in this chapter for information on solving common issues and how to get additional support.

13.1 Accounts: OATH

13.1.1 OATH account renaming and/or deletion doesn't work over NFC on iOS/iPadOS

When attempting to edit an OATH account name or delete an OATH account on iOS/iPadOS over an NFC connection, the name changes don't save or the account isn't successfully deleted despite following the correct steps. The app never prompts you to scan your key to complete the operation.

To solve this issue, close the app, reopen it, and try the operation again.

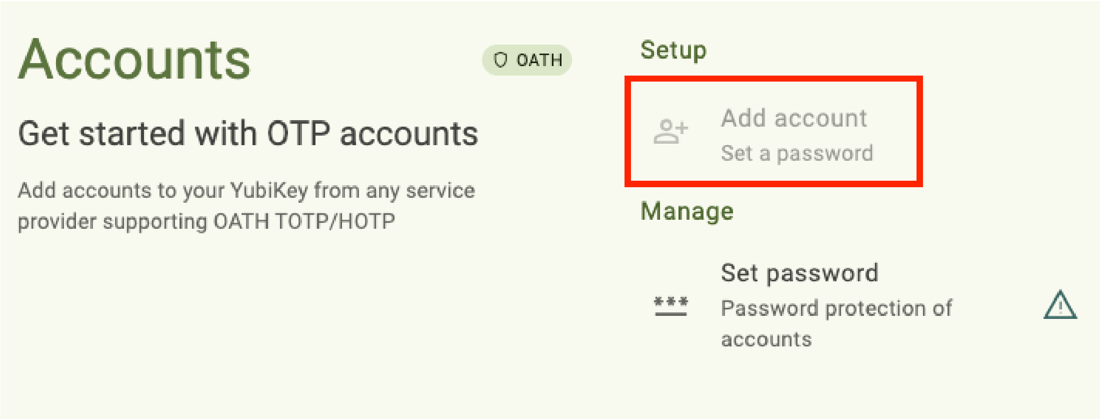
13.1.2 OTP authentication fails due to incorrect TOTP codes

If an OATH account's TOTP codes are getting rejected as invalid during an authentication attempt and they have not expired at the time of submission, the clock on your device may be out of sync with the relying party (your account/service provider).

Reset the clock by following the instructions for your operating system or device. For example, Dell laptop users can reset the Real-Time Clock (RTC) by following the Dell knowledge base article instructions.

13.1.3 Cannot add OATH account

When attempting to add an OATH account to your YubiKey, the operation is greyed-out in Yubico Authenticator:



Accounts

OATH

Get started with OTP accounts

Add accounts to your YubiKey from any service provider supporting OATH TOTP/HOTP

Setup

Add account
Set a password

Manage

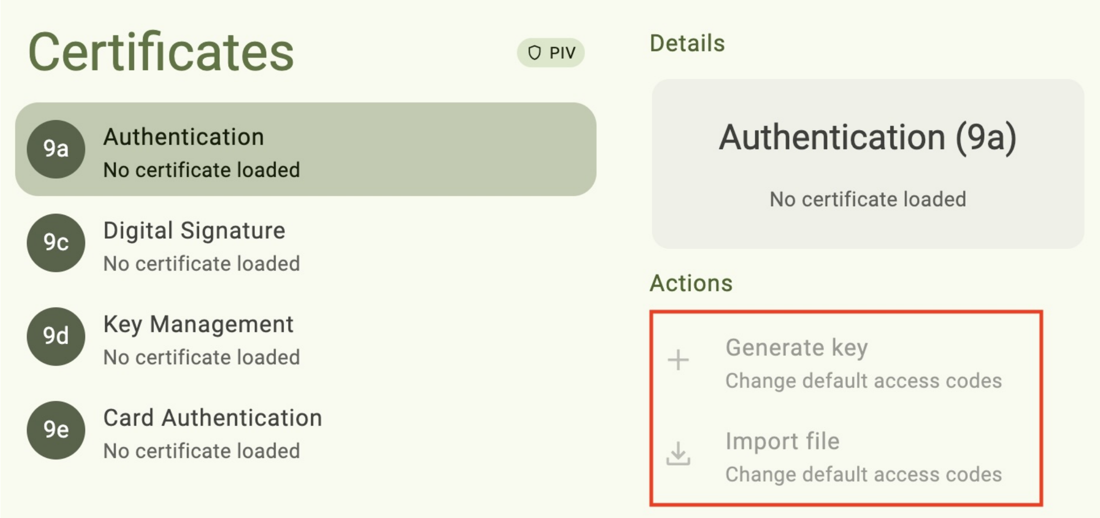
Set password
Password protection of accounts

If you have a YubiKey 5 FIPS Series key with firmware version 5.7 or later, you will not be able to add OATH accounts to your YubiKey until the OATH application is in the *FIPS approved state*. Perform the *operations* required to achieve FIPS approved status, then try adding an account again.

13.2 Certificates: PIV

13.2.1 Cannot import or generate PIV keys or certificates

When attempting to import or generate a PIV key/certificate, the operations are greyed-out in Yubico Authenticator:



Certificates

PIV

9a Authentication
No certificate loaded

9c Digital Signature
No certificate loaded

9d Key Management
No certificate loaded

9e Card Authentication
No certificate loaded

Details

Authentication (9a)

No certificate loaded

Actions

Generate key
Change default access codes

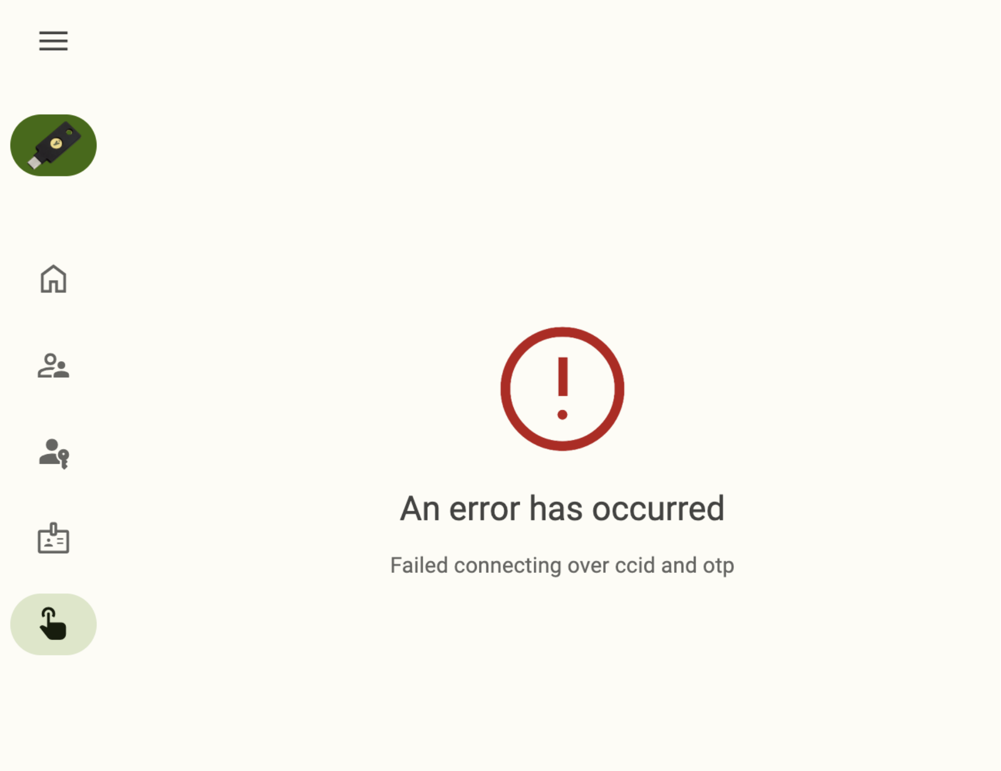
Import file
Change default access codes

If you have a YubiKey 5 FIPS Series key with firmware version 5.7 or later, you will not be able to add PIV credentials to your YubiKey until the PIV application is in the *FIPS approved state*. Perform the *operations* required to achieve FIPS approved status, then try importing/generating PIV credentials again.

13.3 Slots: Yubico OTP

13.3.1 An error occurs when trying to open the Slots screen on macOS

When trying to open the *Slots* screen on macOS, the following error message is seen:



An error has occurred

Failed connecting over ccid and otp

If you receive this error, it likely means that input monitoring has not been enabled on your device. *Toggle that setting*, close and reopen the app, and try again.

13.4 Android

13.4.1 Unable to take screenshots of the app on Android

When attempting to capture a screenshot of the Yubico Authenticator app on an Android device, only a blank screen is saved.

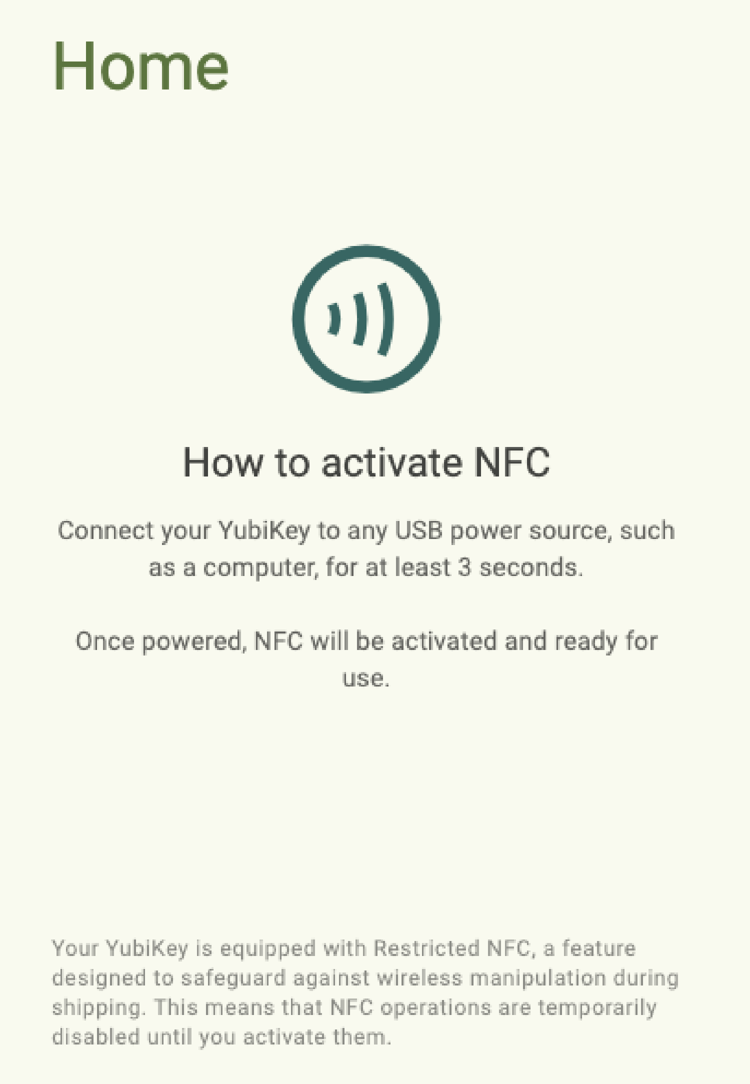
By default, screenshots are disabled on Yubico Authenticator for Android. To enable screenshots, do the following:

1. Click the menu icon in the upper left corner of the app and select **Home**.
2. Click **Help and about** under **Application**. To find the **Application** menu in a narrow app window, click the three dots in the upper right corner.
3. Under **Troubleshooting**, click **Allow screenshots**.

13.5 NFC wireless connections

13.5.1 NFC activation required

When attempting to use a brand new YubiKey with Yubico Authenticator over NFC, a message appears in the app that says NFC activation is required:



Home

How to activate NFC

Connect your YubiKey to any USB power source, such as a computer, for at least 3 seconds.

Once powered, NFC will be activated and ready for use.

Your YubiKey is equipped with Restricted NFC, a feature designed to safeguard against wireless manipulation during shipping. This means that NFC operations are temporarily disabled until you activate them.

This message indicates that the key has the Restricted NFC feature enabled. Restricted NFC is a standard feature for all NFC-capable YubiKeys with firmware version 5.7 and later. Like the message indicates, this feature is intended to prevent wireless manipulation of your YubiKey during shipment.

Once the feature is disabled, you may use your YubiKey via NFC freely. To do so, connect your YubiKey to any powered USB port for at least 3 seconds.

Restricted NFC may be re-enabled at any time via the YubiKey Manager CLI tool.

13.6 Reporting issues and submitting feature requests

Found a bug? Want to request a new feature? Submit an Issue on GitHub.

For Yubico Authenticator for Desktop and Android, submit an Issue in the yubioath-flutter repository.

For Yubico Authenticator for iOS/iPadOS, submit an Issue in the yubioath-ios repository.

13.7 Getting additional help

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

13.8 Generating and collecting diagnostic data and logs

Note: Logs and diagnostic data can be collected on Yubico Authenticator for Desktop and Android only.

While troubleshooting an issue with Yubico's support or development teams, you may be asked to collect and submit app logs and diagnostic data.

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 or to a log file via the command line. There is a fixed size buffer for the **Copy log** button in the app, so if the log is longer than 1000 lines, only the latest 1000 will be included. There is no such limit when outputting logs to a file.

The diagnostics data is useful for making sure the YubiKey is correctly detected and to get information about the key itself and its configuration. The log data is more useful when trying to figure out why a specific action in the app is failing.

13.8.1 Log levels

The log levels (log types) include ERROR, WARNING, INFO, DEBUG, and TRAFFIC, in order of increasing verbosity. The default level is INFO. In general, the following information is collected:

- ERROR - Any error that occurs, which is often an action that cannot be performed.
- WARNING - Something failed, but the app is able to recover and complete the action, or the failure doesn't impact the action.
- INFO - What the app is doing without specific details. For example, a credential was added/removed/renamed, etc.
- DEBUG - More detailed information about actions performed. This can include things like the name of an added account and the method with which the account was added. Some info at this level might be considered sensitive identifiable data (usernames, YubiKey serial numbers, etc).
- TRAFFIC - Even more detailed than DEBUG and INFO. It includes ALL raw traffic to/from the YubiKey. This includes the actual secrets when adding a credential, PIN codes that are being set, etc.

The DEBUG and TRAFFIC levels will show a red warning in the app when active. You should be very cautious when sharing logs of DEBUG and TRAFFIC data with others given that they may contain sensitive information.

13.8.2 Generating logs and diagnostic data within the app

To generate this data, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Home**.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

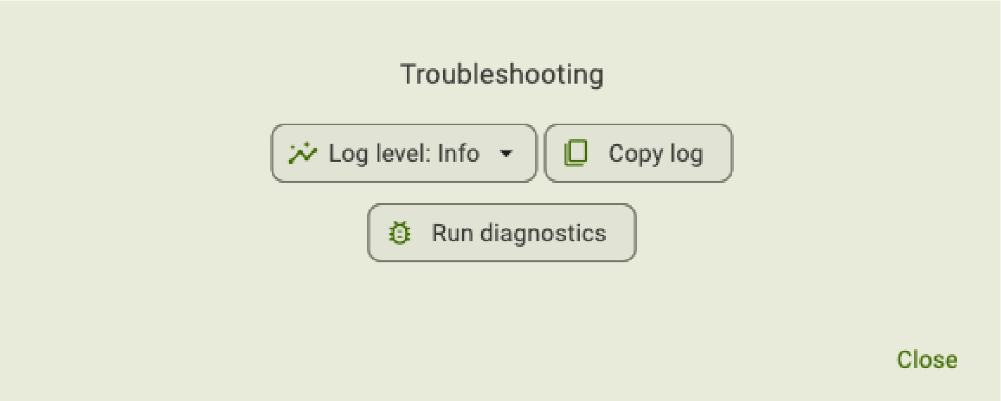
   To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

2. Click **Help and about** under **Application**. To find the **Application** menu in a narrow app window, click the three dots in the upper right corner.

3. Under **Troubleshooting**, select the relevant log type from the **Log level** drop-down menu.

4. If there is a particular operation you want to collect logs on, perform that operation. Now go back to **Troubleshooting** and click **Copy log**. This copies the log information to the clipboard. Paste the log information into a text file (or other document) and save it.

   To generate diagnostic data (desktop only), click **Run diagnostics**. When the operation has completed, it will copy the data to the clipboard automatically. Paste this data into a text file (or other document) and save it.



13.8.3 Generating logs at the command line

To generate logs at the command line, do the following:

1. Open a terminal.

2. Plug your YubiKey into your device.

   To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

3. Start the app and set your desired log level with the `--log-level LEVEL` argument, where `LEVEL` should be one of `error`, `warning`, `info`, `debug`, or `traffic`:

   macOS:

   ```
   open -a "Yubico Authenticator" --args --log-level LEVEL
   ```

   Windows:

   ```
   \Program Files\Yubico\Yubico Authenticator\authenticator.exe --log-level LEVEL
   ```

   Linux:

```
/path/to/authenticator --log-level LEVEL
```

4. If there is a particular operation you want to collect logs on, perform that operation.
5. Copy the logs to a file by passing the `--log-file` argument along with the filename (`myfile.log` in this example):

   macOS:

   ```
   open -a "Yubico Authenticator" --args --log-file myfile.log
   ```

   Windows:

   ```
   C:\Program Files\Yubico\Yubico Authenticator\authenticator.exe --log-file myfile.log
   ```

   Linux:

   ```
   /path/to/authenticator --log-file myfile.log
   ```

   On macOS, the log file will be created at `~/Library/Containers/com.yubico.yubioath/Data/mylogfile.log`. Due to sandboxing on macOS, an alternate file path cannot be provided when calling `--log-file`.

CHAPTER

FOURTEEN

AZURE MFA WITH YUBICO AUTHENTICATOR

These instructions show how to use YubiKeys with Azure Multi-Factor Authentication (Azure MFA). This document focuses on cloud-based Azure MFA implementations and not on the on-premises Azure MFA Server. For an overview of Azure MFA see Microsoft's How it works: Azure Multi-Factor Authentication.

There are two methods to use a YubiKey with Azure MFA as an OATH-TOTP token. Both are described below. The recommended method is to have users self register their YubiKey to their account. The second method is for an Azure AD administrator to register a YubiKey on behalf of the user.

Objectives:

- Register a YubiKey to a user account in Azure AD as an OATH-TOTP token.
- Authenticate using a YubiKey as an OATH-TOTP token.

14.1 Self registration (recommended method)

A user can self register a YubiKey with their Azure AD Account. This is the recommended method for registering a YubiKey as an OATH-TOTP token.

14.1.1 Before you begin

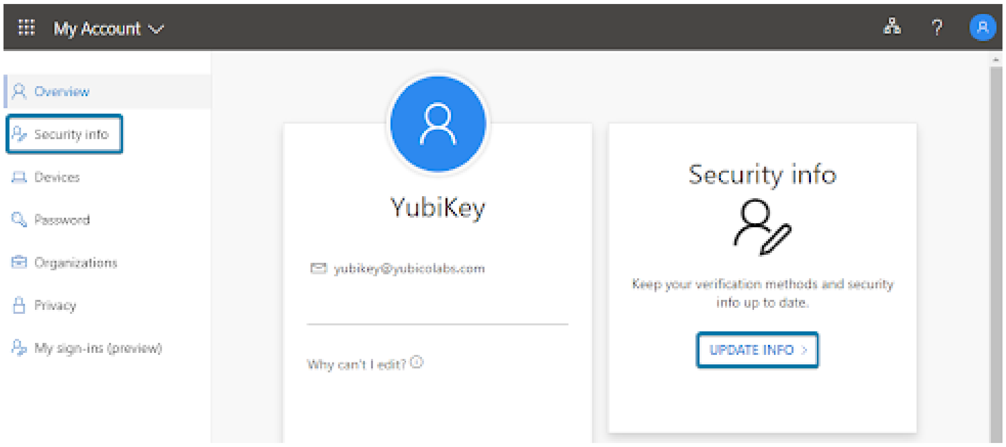
- Your user account must be in Azure Active Directory (AD)
- Have a compatible YubiKey.
- Install Yubico Authenticator on your mobile device and/or workstation. Since the YubiKey does not contain a battery, it cannot track time. Yubico Authenticator is required to generate and display OATH-TOTP codes.

14.1.2 Register a YubiKey

Step 1: Open a browser window and navigate to https://myprofile.microsoft.com.

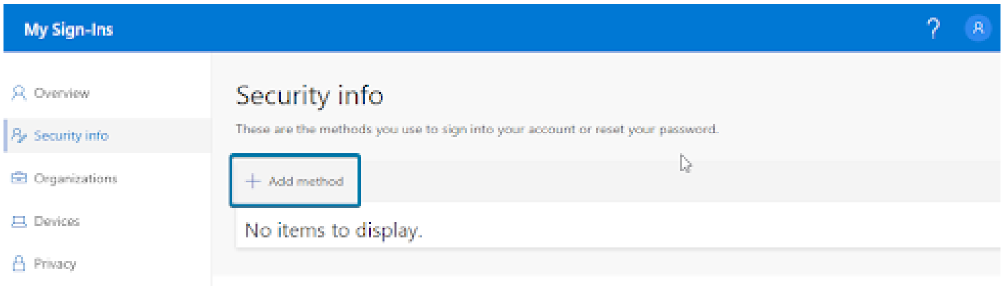
Step 2: Sign in to your account.

Step 3: Select **Security Info** in the left navigation or **Update Info** in the Security Info tile.



Keep your verification methods and security info up to date.

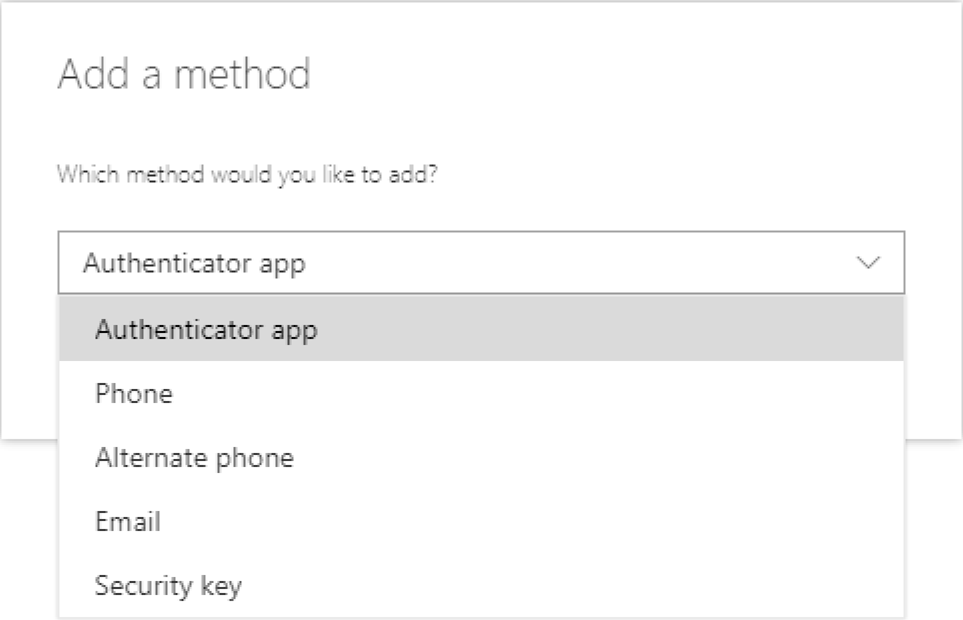
Step 4: Select **Add Method**.



These are the methods you use to sign into your account or reset your password.

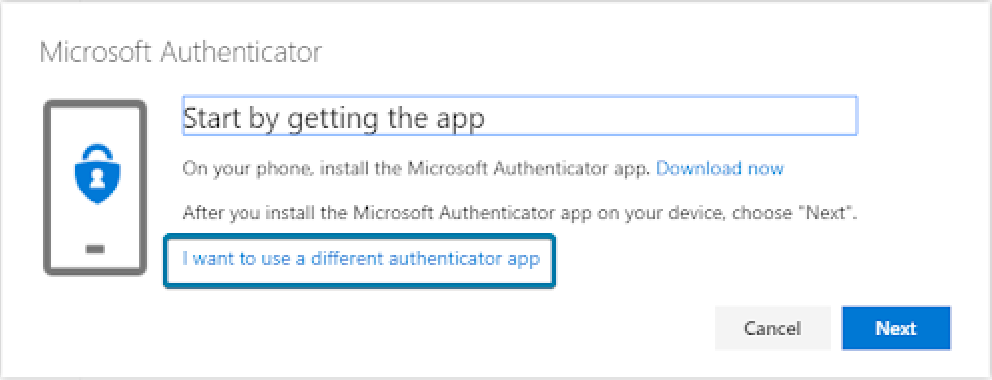
No items to display.

Step 5: Select **Authenticator app**.



Which method would you like to add?

Step 6: Select **I want to use a different authenticator app**.



Microsoft Authenticator

Start by getting the app

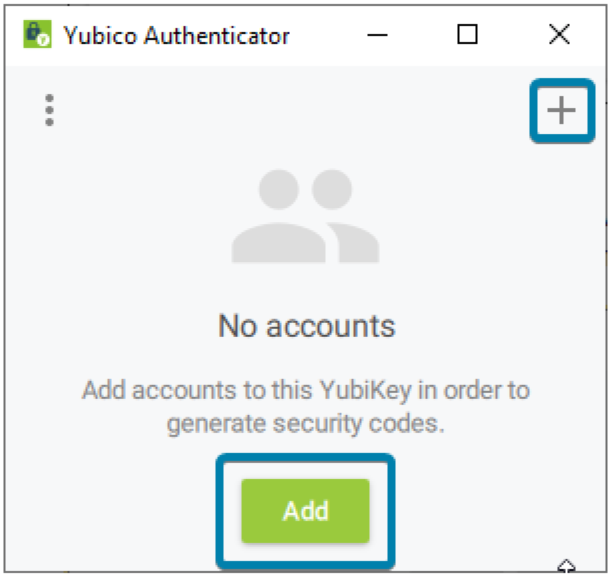
On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

Step 7: Select **Next**.

A QR code is displayed on the screen.

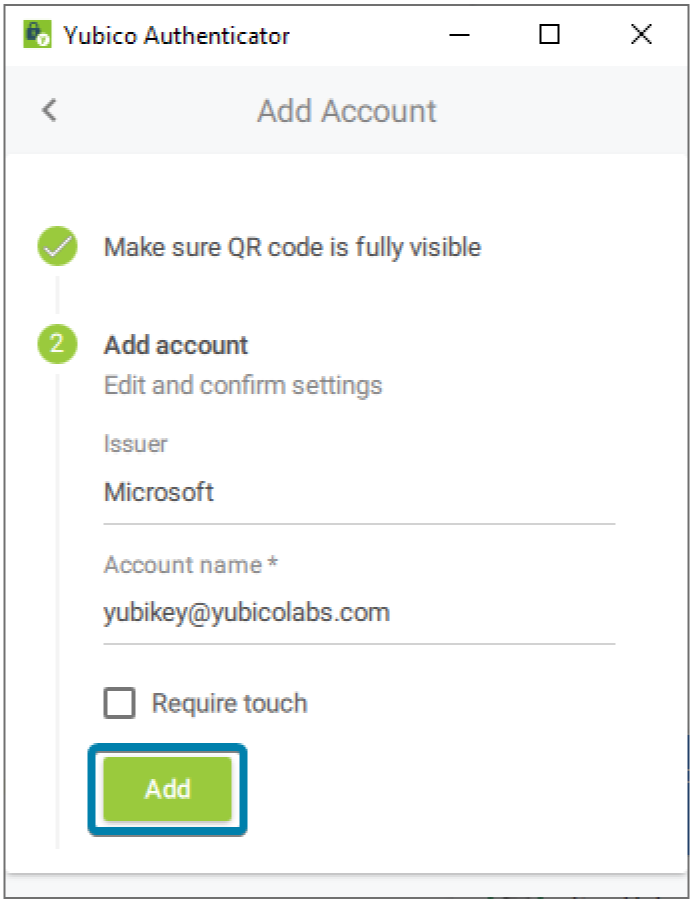
Step 8: Insert your YubiKey and open Yubico Authenticator. Select **Add** or **+**. If the QR Code is visible, it automatically fills in the fields required.



No accounts

Add accounts to this YubiKey in order to generate security codes.

Step 9: Select **Add**.



Make sure QR code is fully visible

2 Add account

Edit and confirm settings

Issuer

Microsoft

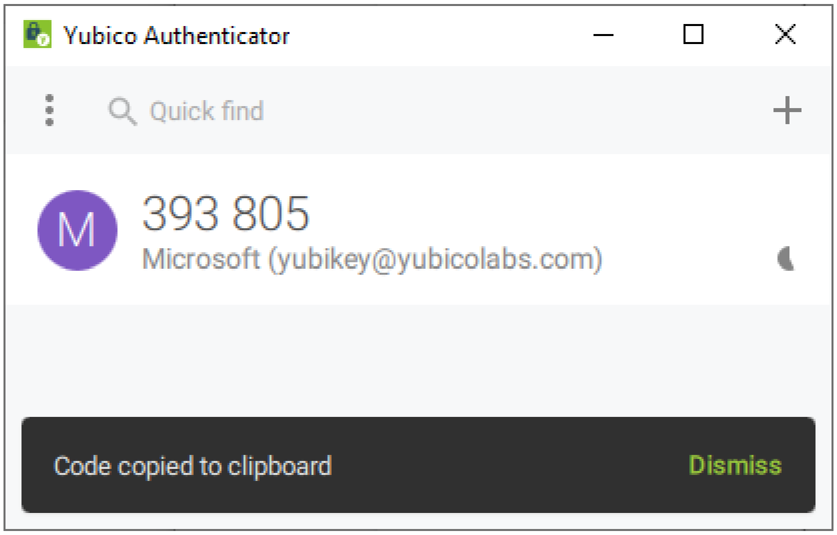
Account name *

yubikey@yubicolabs.com

□ Require touch

Step 10: Double-click the Microsoft entry to copy the code to your clipboard. If successful, the message displays **Code copied to clipboard**.

Note: if you selected Require Touch in the previous step you must touch your YubiKey to copy the code.

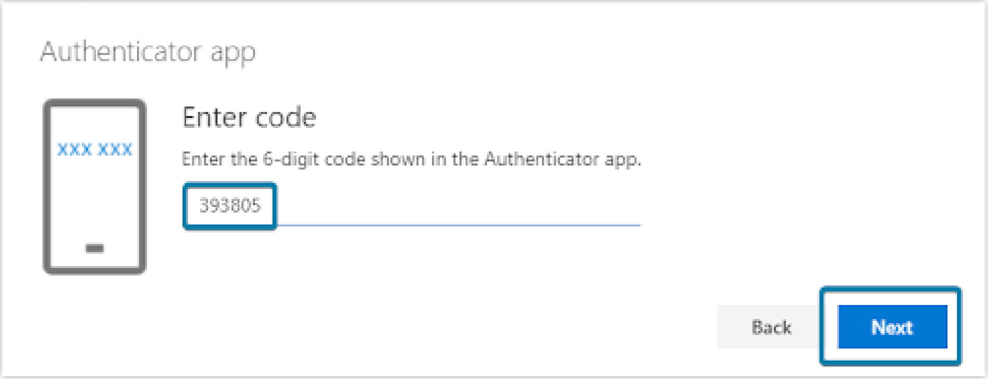


393 805

Microsoft (yubikey@yubicolabs.com)

Code copied to clipboard

Step 11: Back in your internet browser window paste the code in the box and click **Next**.



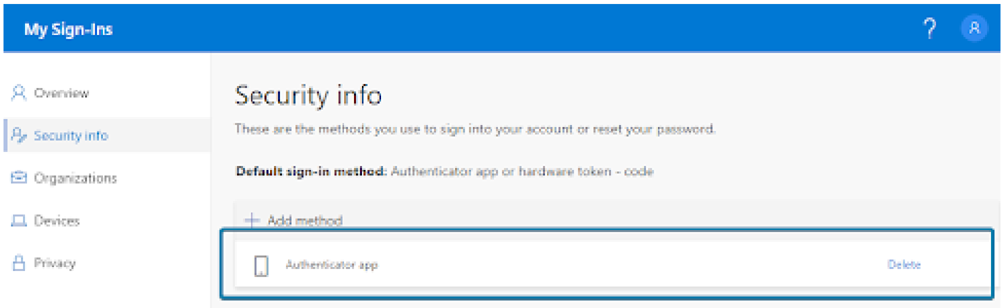
Authenticator app

Enter code

Enter the 6-digit code shown in the Authenticator app.

393805

Step 12: Select **Done**.



Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Authenticator app or hardware token - code

You have now successfully registered your YubiKey to your account!

14.2 Administrator registration (alternative method)

An Azure AD administrator can register and assign a YubiKey to users' accounts. This is an alternative method for registering a YubiKey as an OATH-TOTP token and requires the YubiKey to be registered and activated by an Azure AD Administrator then distributed to a user before use.

There are several steps for the Azure AD Administrator to follow outlined below. The high level process is outlined in Microsoft article, What authentication and verification methods are available in Azure Active Directory.

Note: Yubico can generate the TOTP secrets and program them onto YubiKeys before they are shipped to you. There is a minimum order requirement. Please contact your Yubico sales representative or request someone to contact you.

14.2.1 Before you begin

- The user account must be in Azure AD.
- Have a compatible YubiKey.
- Install Yubico Authenticator.

Since the YubiKey does not contain a battery it cannot track time and will require software to generate OATH-TOTP codes. Yubico provides Yubico Authenticator for all major platforms (Windows, MacOS, Android, and iOS) to display the one time passcodes generated on the YubiKey.

- Install the latest version of YubiKey Manager.

- Ensure users that will be assigned a YubiKey have been assigned an Azure AD Premium license, this may also be included in an Office 365 license.

14.2.2 Generate TOTP secrets

The secrets that are stored on the YubiKey need to be generated. A comma separated value (CSV) text file will be used to track the secrets and associate them to a YubiKey. This file should be considered extremely sensitive and should be protected at all times.

For simplicity the example will only use one account in the file, but Azure supports multiple accounts to be added in one file.

Step 1: Create a text file beginning with **upn, serial number, secret key, time interval, manufacturer, model** (see screenshot below). The meaning of each of these are as follows.

- **upn:** Each user's User Principal Name from Azure AD
- **serial number:** A unique identifier, recommend using the serial number of the YubiKey
- **secret key:** A randomly generated OTP secret. Limited to 128 characters. The secret key can only contain the characters a-z or A-Z and digits 1-7
- **timeinterval:** The time interval for generating new a OTP
- **manufacturer:** Any text used to identify the hardware token, recommend using YubiKey
- **model:** Any text used to identify the model of hardware token, recommend using the YubiKey model

Step 2: Add the UPN of the account to register.

Example: `yubikey@yubicolabs.com`

Step 3: Add the YubiKey serial number that will be assigned to each user.

Example: `8672451`

Step 4: Generate and add a Base32 string that will be used as the secret (see Generating Base32 string examples for examples of how to generate a random Base32 string).

Example: `zsgyzti7z6hecscitbxz6wmt737j2dpa`

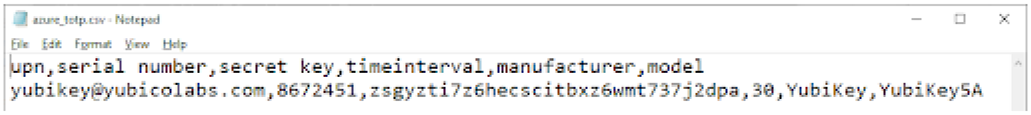
Step 5: Use 30 for the time interval.

Step 6: Use YubiKey for the manufacturer.

Step 7: Add the model of the YubiKey that will be registered.

Example: `YubiKey5NFC`

Step 8: Save and close the file.



```
upn,serial number,secret key,timeinterval,manufacturer,model
yubikey@yubicolabs.com,8672451,zsgyzti7z6hecscitbxz6wmt737j2dpa,30,YubiKey,YubiKey5A
```

14.2.3 Program a YubiKey with a generated secret

The TOTP secrets generated in the previous step now need to be programmed onto the associated YubiKey using YubiKey Manager.

Step 1: Open a terminal window and change the directory to the ykman.exe install directory.

Step 2: Insert the YubiKey associated with the secret (if you are using YubiKey serial numbers).

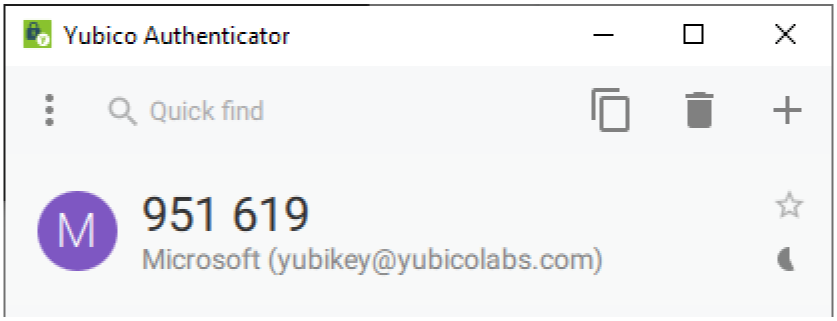
Step 3: Run the ykman command to program the YubiKey with the appropriate account name and secret from the CSV file created in the previous section.

```
ykman oath add -i Microsoft <accountname> <secret>
```

For example:

```
ykman oath add -i Microsoft test1@yubicolabs.com
zsgyzti7z6hecscitbxz6wmt737j2dpa
```

Step 4: Open Yubico Authenticator to verify the creation of the TOTP token on the YubiKey while the YubiKey is still inserted.



951 619
Microsoft (yubikey@yubicolabs.com)

To see all the configuration options, consult the YubiKey Manager CLI (ykman) User Manual.

14.2.4 Upload TOTP secrets and activate the YubiKey

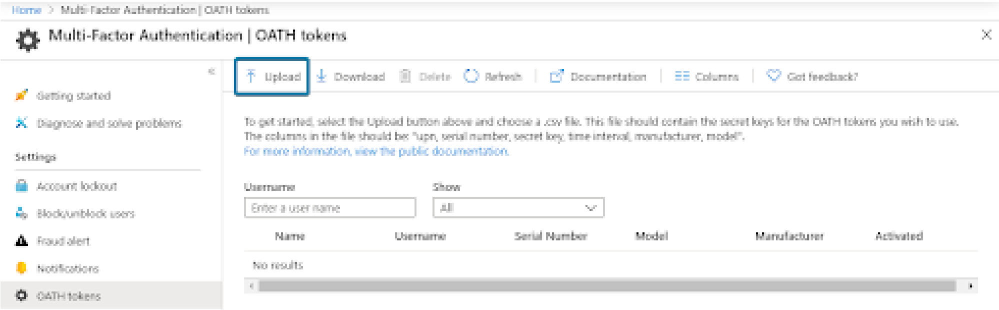
The file generated with the account and secret information needs to be uploaded to Azure AD MFA.

Step 1: Open a browser window and navigate to https://portal.azure.com.

Step 2: Sign in with a Global Administrator account.

Step 3: Select **Active Directory**, then **Security**, then **MFA**, then **OATH tokens**.

Step 4: Select **Upload** and select the generated CSV file.



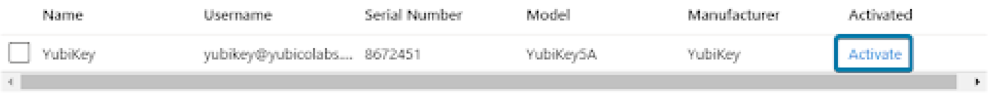
To get started, select the Upload button above and choose a .csv file. This file should contain the secret keys for the OATH tokens you wish to use. The columns in the file should be: "upn, serial number, secret key, time interval, manufacturer, model".
For more information, view the public documentation.

Username: Enter a user name
Show: All

Name	Username	Serial Number	Model	Manufacturer	Activated
No results					

Step 5: Select **Refresh** to see the accounts in the file are listed. It may take several minutes for the file to process and display the user accounts.

Step 6: Select **Activate** for a user.

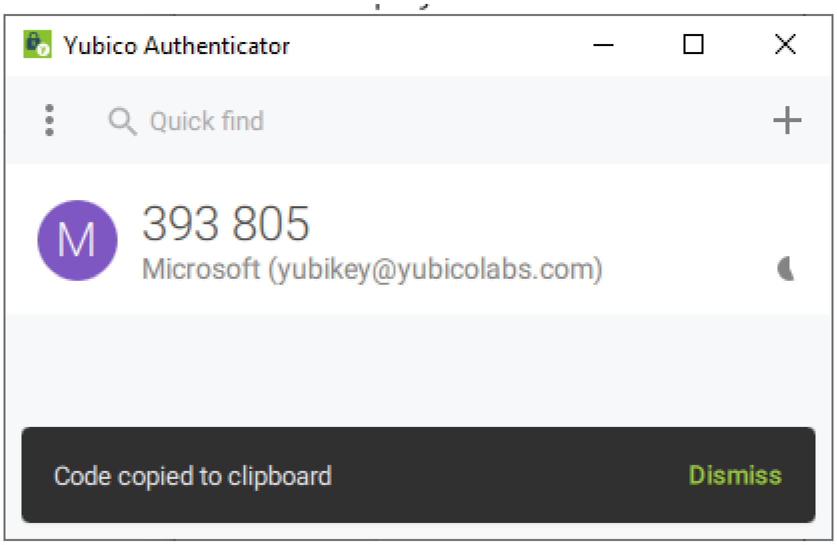


	Name	Username	Serial Number	Model	Manufacturer	Activated
□	YubiKey	yubikey@yubicolabs....	8672451	YubiKey5A	YubiKey	Activate

Step 7: Open Yubico Authenticator.

Step 8: Insert the YubiKey associated with the user.

Step 9: Double click the code displayed in Yubico Authenticator.

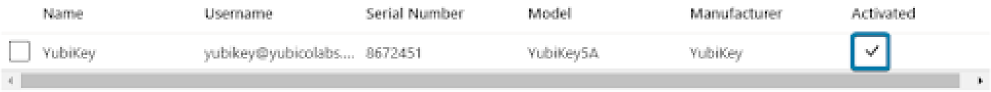


393 805
Microsoft (yubikey@yubicolabs.com)

Code copied to clipboard

Step 10: Paste the code into the web browser window and select **Ok**.

Step 11: Verify the user was successfully activated by looking for a check mark.



	Name	Username	Serial Number	Model	Manufacturer	Activated
□	YubiKey	yubikey@yubicolabs....	8672451	YubiKey5A	YubiKey	✓

The YubiKey can now be distributed to the associated person for use.

14.3 Use a YubiKey to sign in

It is simple to use your YubiKey as an OATH token to sign in to a Microsoft site, or site that has been federated to Azure AD. Generating the YubiKey OTP code to sign in can be done on any device where the Yubico Authenticator is installed (Linux, MacOS, Microsoft Windows, Android, and iOS).

14.3.1 Before you begin

- Your YubiKey will need to be registered to your Azure AD account.
- Install Yubico Authenticator.

14.3.2 Website sign in

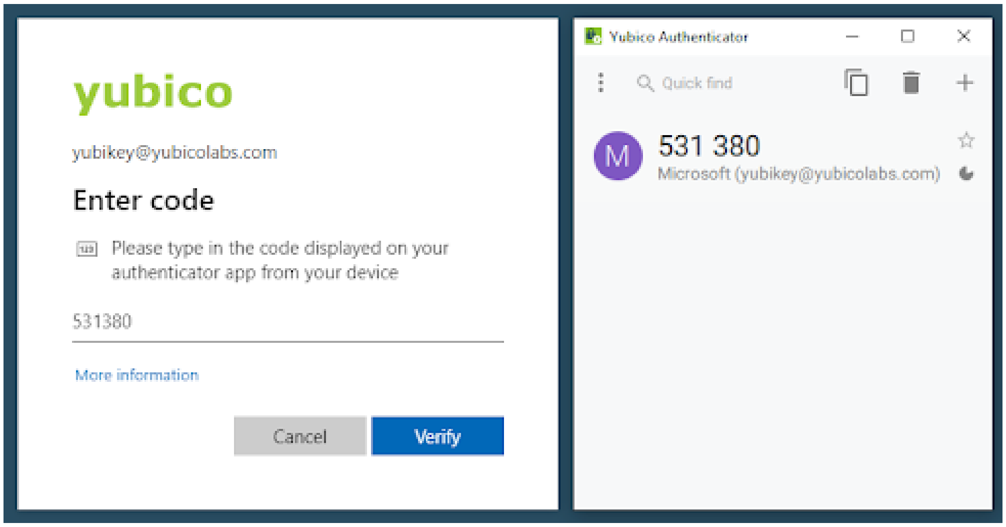
Step 1: Open the Yubico Authenticator application.

Step 2: Insert the YubiKey into the device.

Step 3: Sign into a Microsoft site with a username and password.

Step 4: Double click the code in Yubico Authenticator application to copy the OTP code.

Step 5: Paste the code into the prompt.



yubico

yubikey@yubicolabs.com

Enter code

Please type in the code displayed on your authenticator app from your device

531380

531 380

Microsoft (yubikey@yubicolabs.com)

Step 6: Select **Verify** to complete the sign in.

14.4 Troubleshooting

Listed below are some common troubleshooting tips. In addition, you can visit Microsoft's "Troubleshooting Azure Multi-factor Authentication issues" site.

(Self-service) QR code not recognized by Yubico Authenticator

If one does not click **I want to use a different authenticator app** when setting up TOTP MFA via self-service, the QR code produced will only be readable by Microsoft Authenticator. When trying to scan such a QR code, Yubico Authenticator for desktop will indicate that no QR code is visible on screen (*No QR code found on screen*), Yubico

Authenticator for iOS version will produce the error *Error occurred - Invalid URI format*, and Yubico Authenticator for Android, *The scanned barcode is invalid*.

Azure AD Admin cannot access the MFA section in Azure AD.

The Azure AD MFA feature to manage OATH-TOTP tokens requires an Azure AD Premium license, this may also be included in an Office 365 subscription.

CSV file (OATH script) will not load.

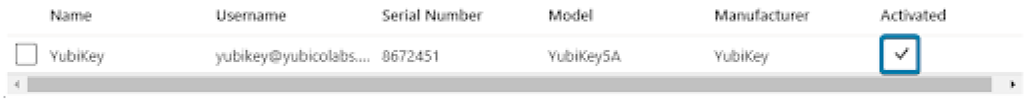
The most common reasons for failure to upload are:

- The file is improperly formatted
- The header row is not included in the file
- here are duplicate entries in the file

Be sure to check the current status of the upload by clicking on the refresh button. If an error message appears, click on the Details link and download the file that had failures. The downloaded file will have a Status column that will include information on the failure.

YubiKey is not working after an Administrator enrolled on behalf of the user.

Verify that the OATH token is activated in the Azure MFA portal.



	Name	Username	Serial Number	Model	Manufacturer	Activated
□	YubiKey	yubikey@yubicolabs....	8672451	YubiKey5A	YubiKey	☑

Another OATH token cannot be added.

Microsoft specifies in the article, What authentication and verification methods are available in Azure Active Directory? that up to five MFA tokens can be associated with one account. The limit applies to hardware and software OATH-TOTP implementation including Microsoft Authenticator apps. For example, you can associate three YubiKeys, one Microsoft Authenticator app, and a phone number to an individual account if no other OATH token is being used.

14.5 Additional information

- Azure Multi-Factor Authentication documentation
- What is OATH?

CHAPTER

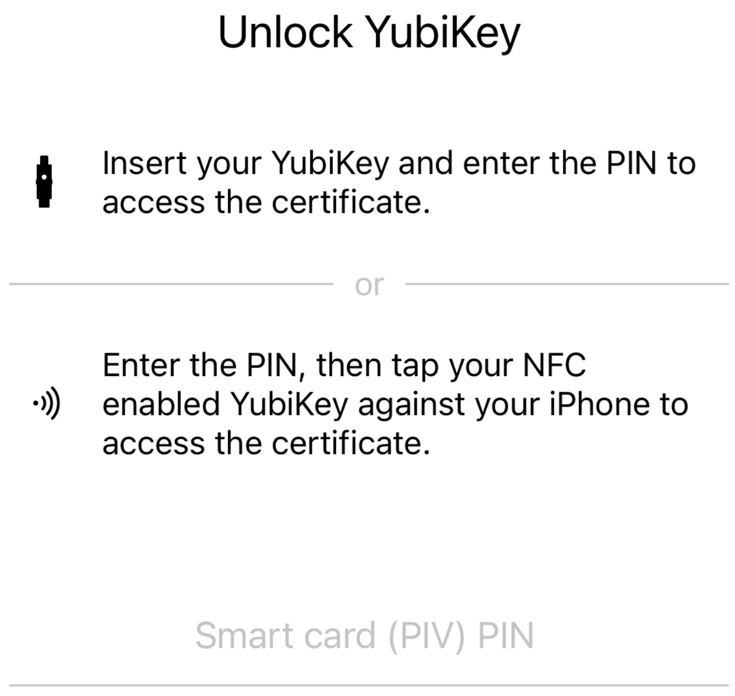
FIFTEEN

SMART CARD ON IOS

The Smart Card on iOS feature within Yubico Authenticator facilitates smart card Transport Layer Security (TLS) authentication to websites from within the Safari browser. This feature is currently supported for iPhones/iPads with iOS/iPadOS 14.2 or later.

Smart Card on iOS allows you to easily provision the public portion of any smart card certificate stored on your YubiKey to the iOS Keychain on your iOS device. The private key of your smart card certificate remains on your YubiKey, from which it cannot be extracted.

During TLS authentication to a website, the public certificate is accessible to Safari via iOS Keychain, and Yubico Authenticator facilitates signing with the private key stored on your YubiKey. In order to complete authentication with Yubico Authenticator, you must plug your YubiKey into your iPhone/iPad (or scan if using an NFC-enabled YubiKey) and enter your smart card certificate PIN when prompted.



Unlock YubiKey

Insert your YubiKey and enter the PIN to access the certificate.

or

Enter the PIN, then tap your NFC enabled YubiKey against your iPhone to access the certificate.

Smart card (PIV) PIN

The Smart Card on iOS feature can also be used for signing emails and decrypting messages/documents. Please note that this guide focuses only on certificate-based authentication. Likewise, the feature also supports certificate-based authentication with third-party iOS applications, but the walkthrough included herein only covers the Safari browser usage.

15.1 X.509 Certificates

Both the iOS Keychain and the YubiKey can hold X.509 smart card certificates. Certificates are stored in the PIV application on the YubiKey, which contains 24 “slots” (for YubiKey 5 Series keys), four of which are easily accessible via the YubiKey Manager tool.

To enable the Smart Card on iOS functionality, both the public certificate and the private key need to be imported onto the YubiKey.

The YubiKey Manager tool supports importing of X.509 certificates and keys in the PEM, DER, and PKCS12 formats. For Smart Card on iOS, we recommend using certificates in the PKCS12 format (which have the .p12 and .pfx file extensions) as both the public certificate and private key are stored in the same file.

15.2 Prerequisites

To use the Smart Card on iOS feature, you must have the following:

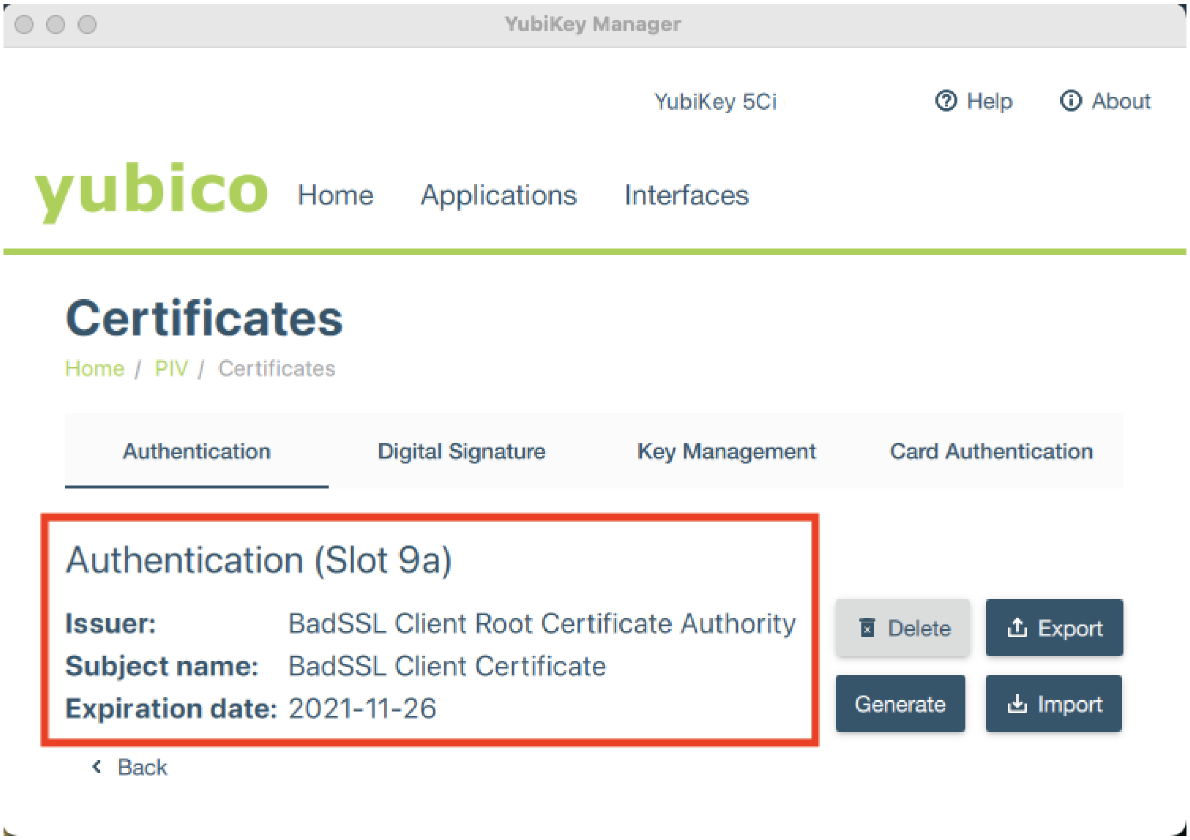
- Apple iPhone/iPad with iOS/iPadOS 14.2 or later.
- YubiKey 5 series key (5 NFC, 5C NFC, or 5Ci).
- Yubico Authenticator iOS application (v.1.6 or newer).
- Host computer.
- YubiKey Manager tool (available for Windows, Linux, and macOS).
- X.509 smart card certificate from a website you’d like to authenticate to. We recommend using the .p12 or .pfx file types if available. Download this file directly to your computer.

Note: If your YubiKey already has a smart card certificate stored in its PIV application, you only need an iPhone, your YubiKey, and Yubico Authenticator.

15.3 Overview: Setup Process

After satisfying the prerequisites listed above, do the following to set up and use the Smart Card on iOS feature (we use the BadSSL site for the example screenshots):

1. *Import your smart card certificate onto your YubiKey using YubiKey Manager.* If your YubiKey already has a certificate stored in its PIV application, skip to the next step.



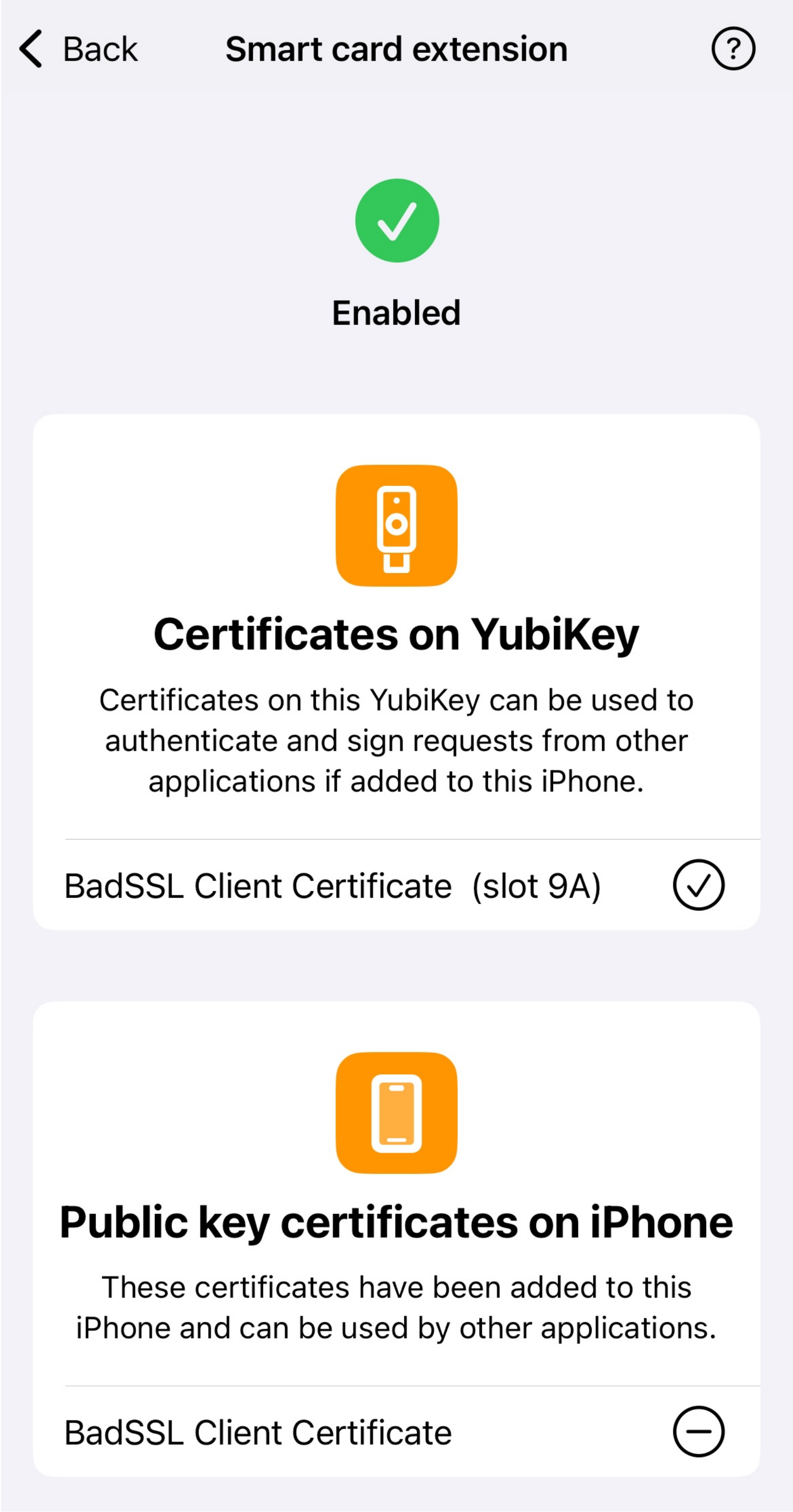
Authentication (Slot 9a)

Issuer: BadSSL Client Root Certificate Authority

Subject name: BadSSL Client Certificate

Expiration date: 2021-11-26

2. *Provision the public certificate to your iOS Keychain* through the Yubico Authenticator application on your iOS device.



Enabled

Certificates on YubiKey

Certificates on this YubiKey can be used to authenticate and sign requests from other applications if added to this iPhone.

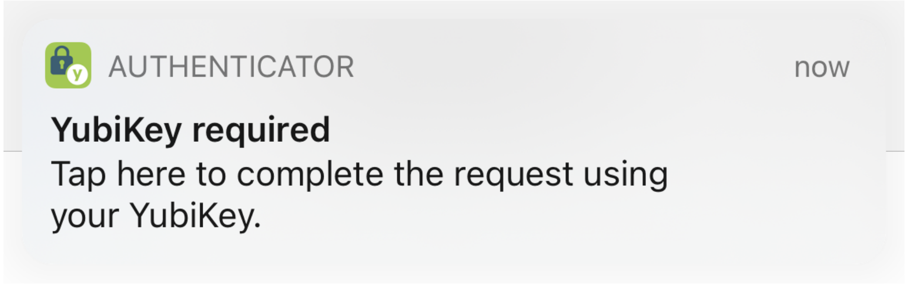
BadSSL Client Certificate (slot 9A) ✓

Public key certificates on iPhone

These certificates have been added to this iPhone and can be used by other applications.

BadSSL Client Certificate ⊖

3. *Authenticate to the website that requires your smart card certificate on the Safari browser.*



AUTHENTICATOR now

YubiKey required
Tap here to complete the request using your YubiKey.

15.4 Troubleshooting

If you run into issues using the Smart Card on iOS feature, check out the *Smart Card on iOS Troubleshooting* chapter for possible solutions.

To file a support ticket with Yubico, click Support.

CHAPTER

SIXTEEN

IMPORT SMART CARD CERTIFICATES ONTO YOUR YUBIKEY

Before your smart card certificates can be provisioned to your iOS Keychain with Yubico Authenticator, you must first import those certificates onto a YubiKey from your host computer. This can be done through either of the following tools:

- YubiKey Manager GUI
- YubiKey Manager CLI

The GUI (graphical user interface) tool allows you to configure PIV functionality by clicking through a series of screens, whereas the CLI (command line interface) tool allows you to configure the same functionality through commands in a terminal. Both versions of the tool are supported for Windows, Linux, and macOS.

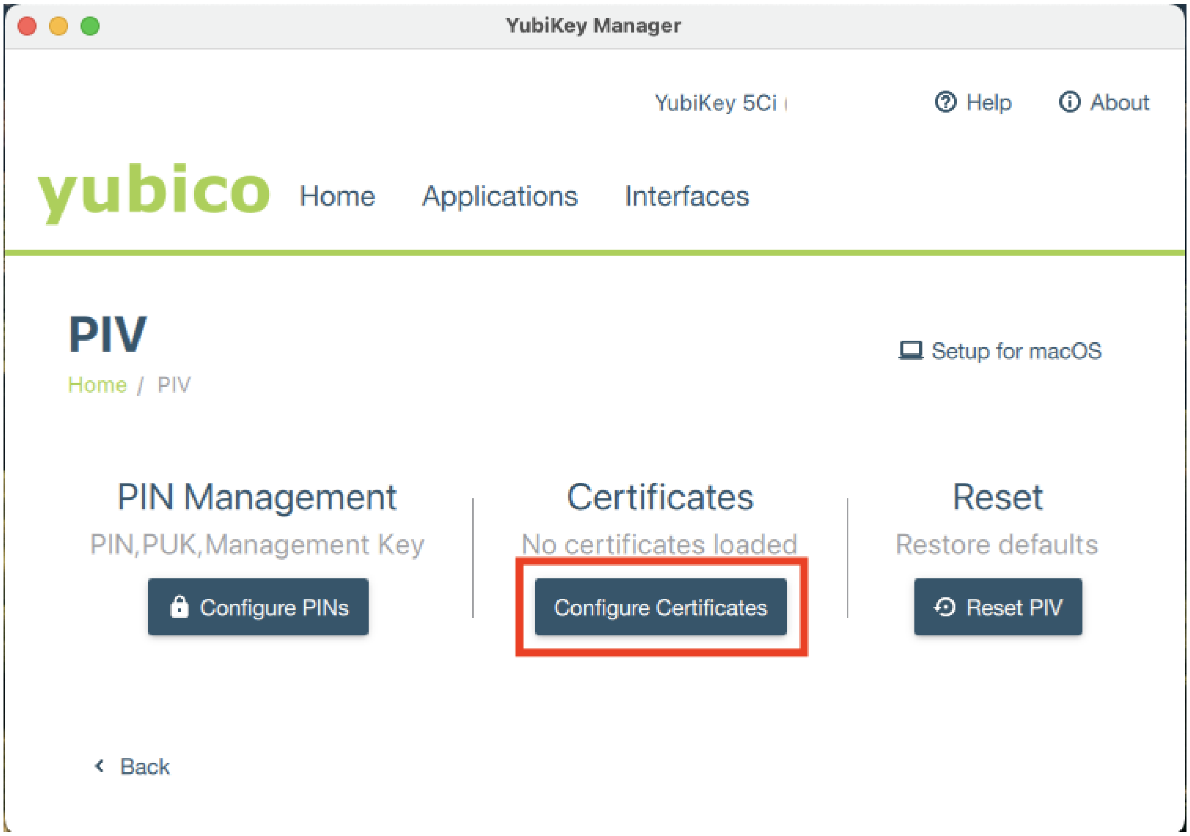
Follow the steps detailed below to import your smart card certificates onto your YubiKey using your preferred version of YubiKey Manager.

If you already have your smart card certificate stored on your YubiKey, skip to the next section: *Smart Card Certificate Provisioning*.

16.1 YubiKey Manager GUI

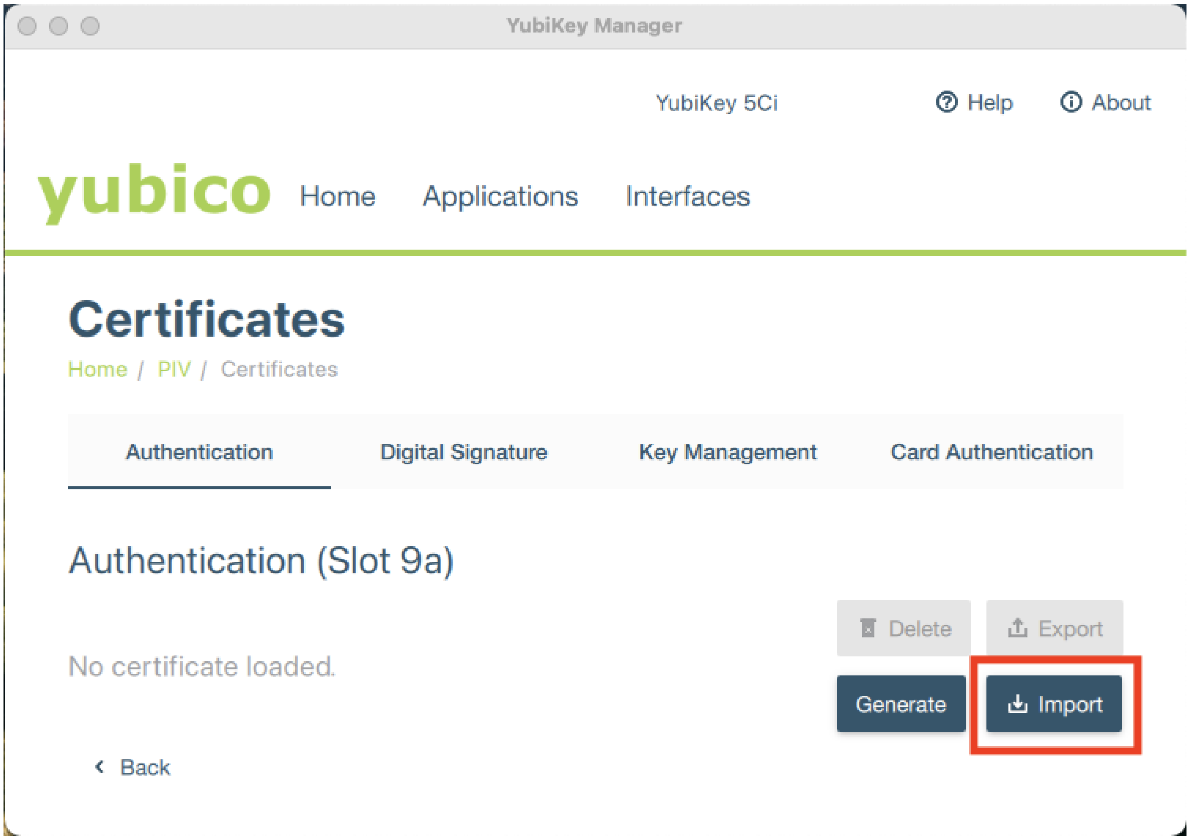
To use the GUI version of YubiKey Manager to import your certificate, follow the steps below:

1. If you haven't already, download the appropriate version of the YubiKey Manager GUI tool onto your host computer. Click on the downloaded file and follow the prompts to complete the installation.
2. Open the YubiKey Manager GUI tool and plug your YubiKey into your computer.
3. On the homepage of the YubiKey Manager, click on the **Applications** drop-down menu and select **PIV**.
4. Select **Configure Certificates** under the **Certificates** section.



5. The YubiKey has 24 total PIV slots, four of which are accessible via the YubiKey Manager tool (9a, 9c, 9d, and 9e). Technically, all of these accessible slots can be used to hold an X.509 certificate for authentication, but slot 9a is intended to be used for this purpose. For more information on PIV application slots, check out the slot documentation.

   Select an empty slot and click **Import**.



No certificate loaded.

6. Navigate to the certificate file on your computer and select it to begin the import process.

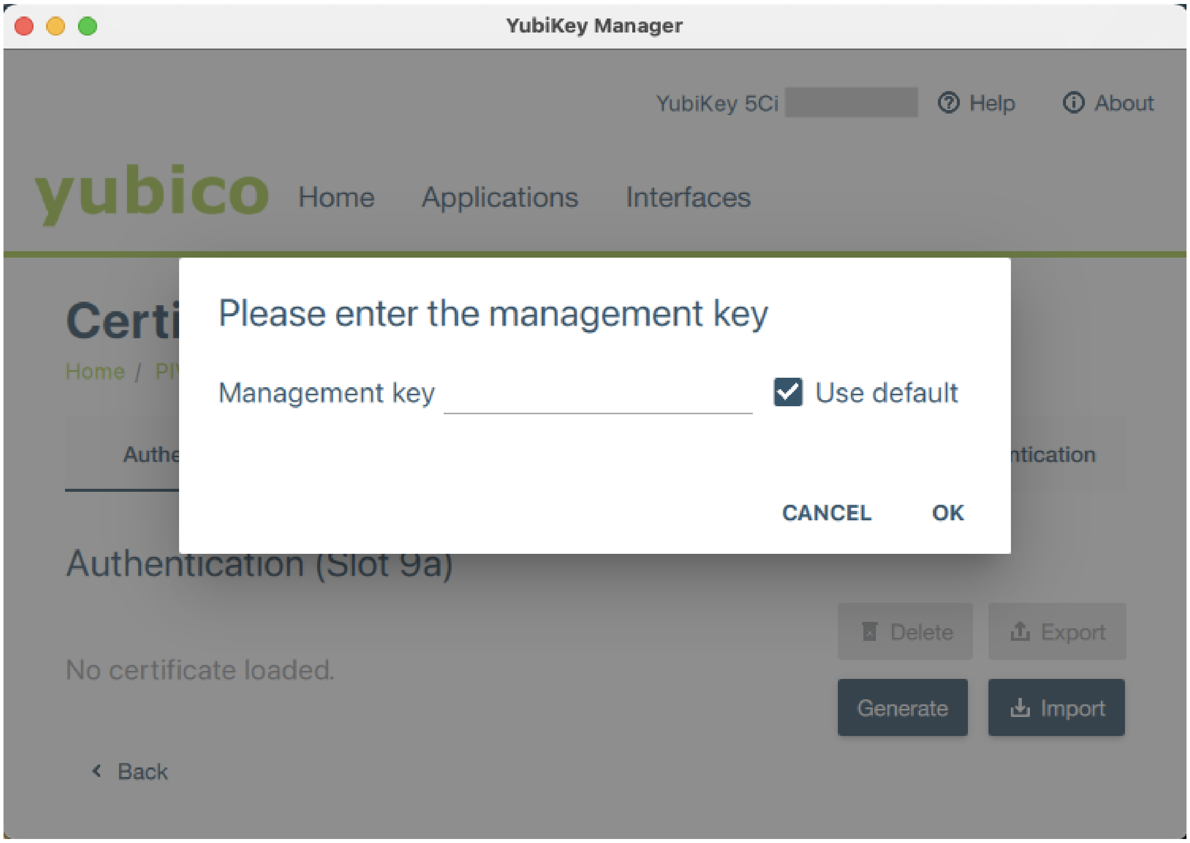
   Remember, the public certificate AND its private key must be imported onto your YubiKey. While the YubiKey can store any X.509 certificate of the PEM, DER, and PKCS12 format, we recommend using the PKCS12 file type (which have .pfx or .p12 file extensions) because the public certificate and private key are stored in a single file.

7. When prompted, enter the certificate's password and click **OK**.

   Note: If you do not know your certificate's password, check with your admin (if applicable) or the certificate provider.

8. Next, enter the PIV application management key and click **OK**.

   Note: If you have not changed the management key using YubiKey Manager, the default management key will be sufficient. If your YubiKey is managed by your organization, reach out to your admin for your management key.

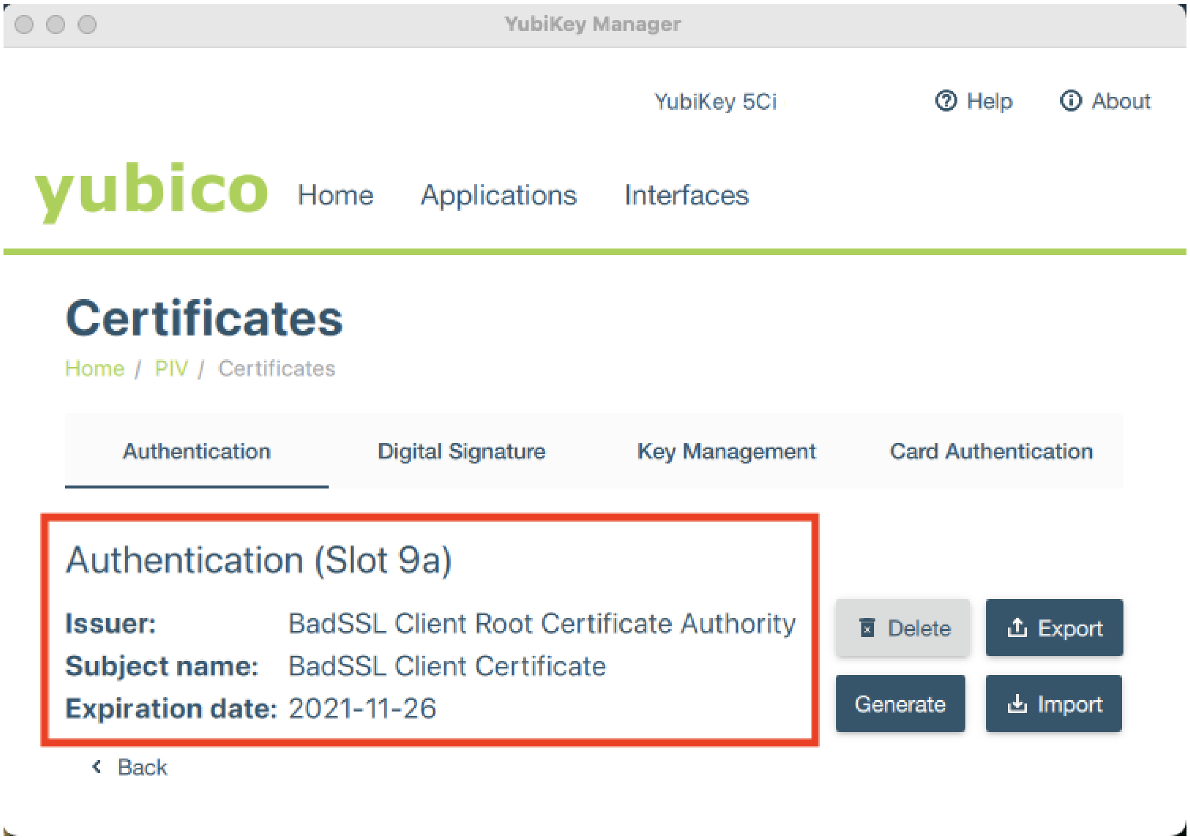


Please enter the management key

Management key ☑ Use default

CANCEL OK

9. If the import was successful, the slot will display the issuer, subject name, and expiration date of the imported certificate.



Authentication (Slot 9a)

Issuer: BadSSL Client Root Certificate Authority

Subject name: BadSSL Client Certificate

Expiration date: 2021-11-26

10. Repeat this process to import additional smart card certificates as needed.

16.2 YubiKey Manager CLI

If you prefer to use the command line version of the YubiKey Manager tool (ykman) to import your certificate, follow the steps below:

1. Install ykman onto your host computer.
2. ykman can be run within a command prompt, terminal, or PowerShell. Please see the ykman documentation for more information on configuring your system to do this.
3. Once your system has been configured, open a command prompt, terminal, or PowerShell.
4. Plug your YubiKey into your computer.
5. The YubiKey has 24 total PIV slots, four of which are accessible via the YubiKey Manager tool (9a, 9c, 9d, and 9e). Technically, all of these accessible slots can be used to hold an X.509 certificate for authentication, but slot 9a is intended to be used for this purpose. For more information on PIV application slots, check out the slot documentation.

   Enter `ykman piv info` to check if any slots on your YubiKey are already occupied.
6. Once you have identified an appropriate empty slot, navigate to the folder containing your smart card certificate.
7. Enter `ykman piv certificates import <slot> <filename>` to import your certificate onto your YubiKey. `<slot>` refers to the slot number (e.g. 9a), and `<filename>` refers to the name of your certificate file (e.g. certificate.p12).

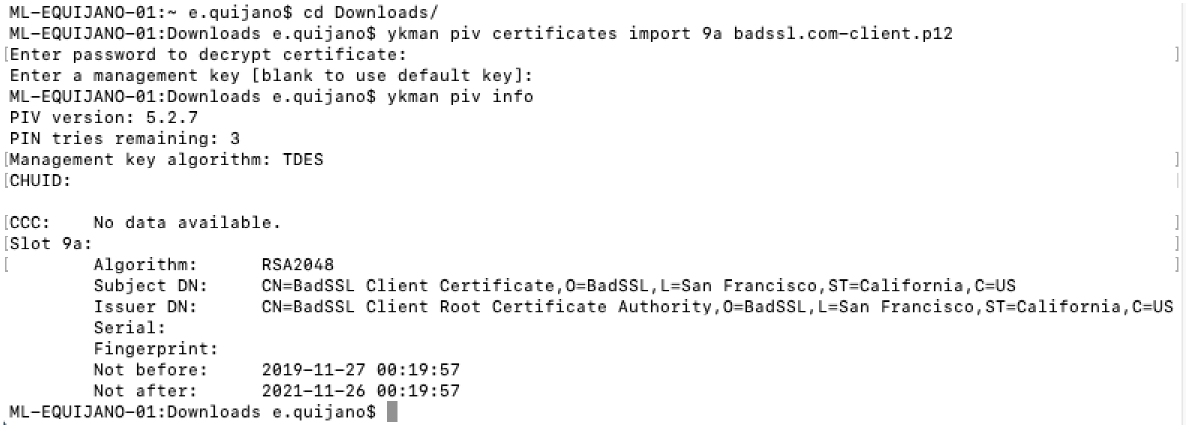
Remember, the public certificate AND its private key must be imported onto your YubiKey. While the YubiKey can store any X.509 certificate of the PEM, DER, and PKCS12 format, we recommend using the PKCS12 file type (which have .pfx or .p12 file extensions) because the public certificate and private key are stored in a single file.

8. When prompted, enter your certificate's password and your PIV application management key.

Note: If you do not know your certificate's password, check with your admin (if applicable) or the certificate provider. If you have not changed the management key using YubiKey Manager, the default management key will be sufficient. If your YubiKey is managed by your organization, reach out to your admin for your management key.

9. Enter `ykman piv info` again to verify that the certificate import was successful. You will see the slot number listed along with the certificate algorithm, subject DN, issuer DN, serial number, fingerprint, and the time period the certificate is valid for.

Note: For more information on ykman PIV commands, please see the ykman documentation.



```
ML-EQUIJANO-01:~ e.quijano$ cd Downloads/
ML-EQUIJANO-01:Downloads e.quijano$ ykman piv certificates import 9a badssl.com-client.p12
Enter password to decrypt certificate:
Enter a management key [blank to use default key]:
ML-EQUIJANO-01:Downloads e.quijano$ ykman piv info
PIV version: 5.2.7
PIN tries remaining: 3
Management key algorithm: TDES
CHUID:

CCC:    No data available.
Slot 9a:
        Algorithm:      RSA2048
        Subject DN:     CN=BadSSL Client Certificate,O=BadSSL,L=San Francisco,ST=California,C=US
        Issuer DN:      CN=BadSSL Client Root Certificate Authority,O=BadSSL,L=San Francisco,ST=California,C=US
        Serial:
        Fingerprint:
        Not before:     2019-11-27 00:19:57
        Not after:      2021-11-26 00:19:57
ML-EQUIJANO-01:Downloads e.quijano$ 
```

10. Repeat this process to import additional smart card certificates as needed.

16.3 Next Steps

Now that you have imported your smart card certificate onto your YubiKey, you may *provision the certificate to your iOS Keychain* through the Yubico Authenticator application on your iOS device.

To file a support ticket with Yubico, click Support.

CHAPTER

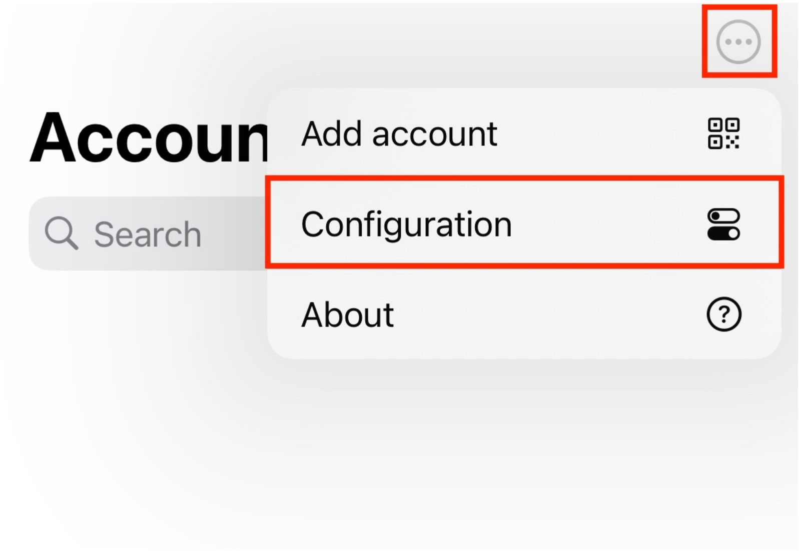
SEVENTEEN

SMART CARD CERTIFICATE PROVISIONING

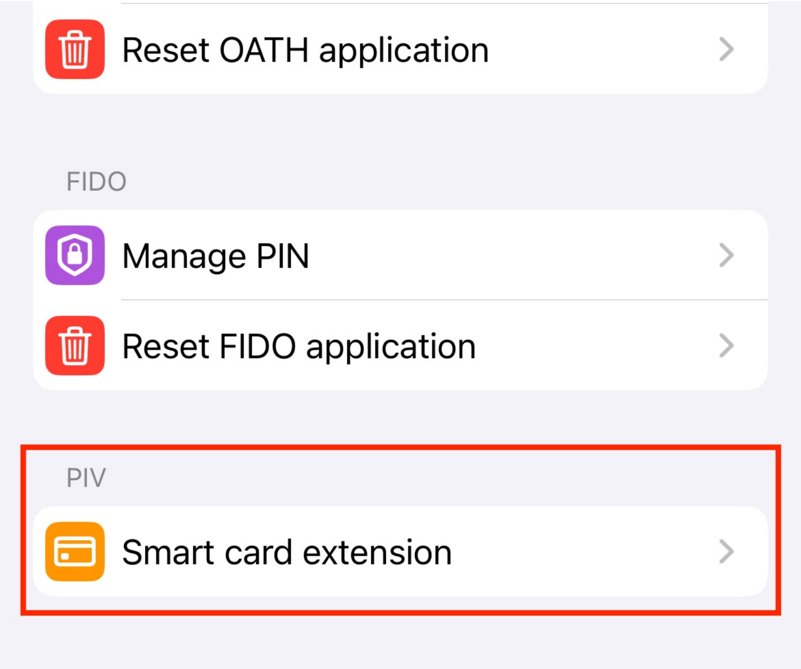
Now that your smart card certificates have been *imported onto your YubiKey*, you must provision the public portion of the certificates onto your iOS Keychain through Yubico Authenticator. After completing this step, you will be able to use the Smart Card on iOS feature to authenticate to the websites that require those smart card certificates on the Safari browser.

17.1 Provision Your Public Certificate

1. If you haven't already, download and install the Yubico Authenticator application (v.1.6 or newer) onto your iOS device.
2. Open Yubico Authenticator.
3. On the home screen of Yubico Authenticator, click on the three dots (. . .) in the upper right corner of the screen and select **Configuration**.



4. On the **Configuration** screen, select **Smart card extension** under the **PIV** section.



5. Insert your YubiKey into your device.

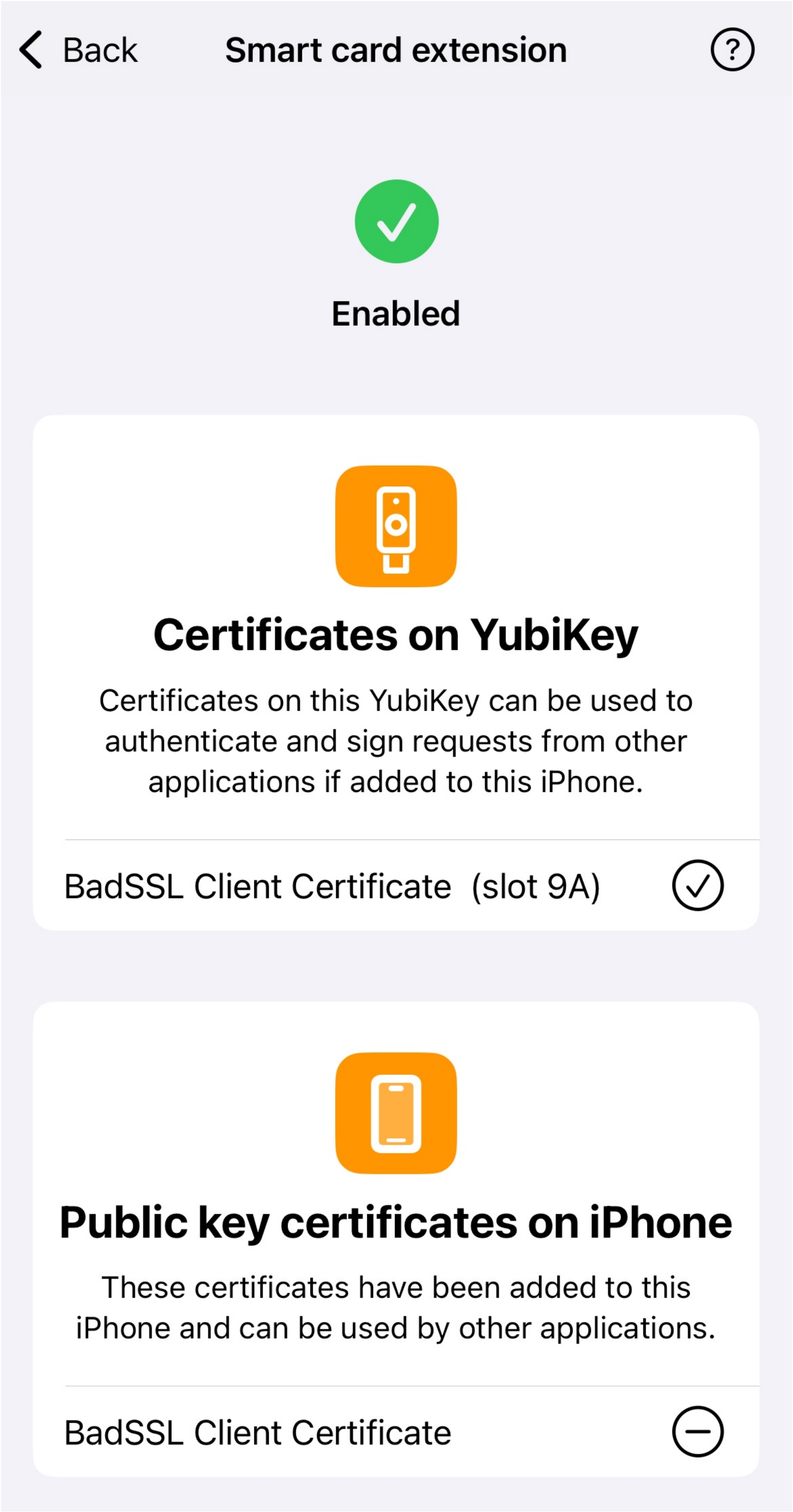
   To connect via NFC on iOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.

   Note: Lightning is currently the only supported *physical* connection type for iOS and iPadOS devices. NFC wireless connections are supported on iOS but not on iPadOS. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

   ---

6. Once your YubiKey has been detected by the app, all certificates stored on your YubiKey will appear under the **Certificates on YubiKey** section. To provision the public certificate from one of your PIV application slots to your iOS Keychain, click the (**+**) icon next to the certificate name.

7. If the provisioning was successful, the name of your certificate will appear under the **Public key certificates on iPhone** section. You may remove certificates from your iOS Keychain at any time by clicking the (**–**) icon next to the certificate name.



Smart card extension

✓

Enabled

Certificates on YubiKey

Certificates on this YubiKey can be used to authenticate and sign requests from other applications if added to this iPhone.

BadSSL Client Certificate (slot 9A) ✓

Public key certificates on iPhone

These certificates have been added to this iPhone and can be used by other applications.

BadSSL Client Certificate ⊖

17.2 Next Steps

Congratulations! Your public certificate has been provisioned to your iOS device, and you are now ready to authenticate to the website requiring that smart card certificate on Safari. See *Authenticating with Smart Card on iOS* for guidance.

To file a support ticket with Yubico, click Support.

CHAPTER

EIGHTEEN

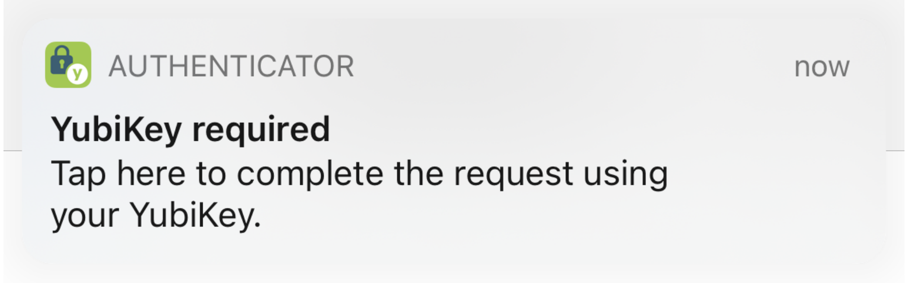
AUTHENTICATING WITH SMART CARD ON IOS

Now that you have *imported your smart card certificates onto your YubiKey* and *provisioned the public portions of the certificates to your iOS Keychain* through Yubico Authenticator, you are ready to use the Smart Card on iOS feature to authenticate to the websites corresponding to your provisioned certificates on Safari.

Follow the steps below for guidance on how to use the Smart Card on iOS feature.

18.1 Authenticate to a Website on Safari

1. Click the compass icon to open the Safari browser on your iOS device.
2. Enter the URL of the website you'd like to authenticate to. The website must correspond to a public certificate stored in your iOS Keychain.
3. If you have more than one certificate stored in your iOS Keychain, or if you are browsing in private mode on Safari, you will be asked to confirm which certificate you'd like to use for authentication. Follow the prompts as necessary.
4. A pop-up from Yubico Authenticator will appear at the top of the screen. Click on the pop-up to begin the authentication.



AUTHENTICATOR now

YubiKey required

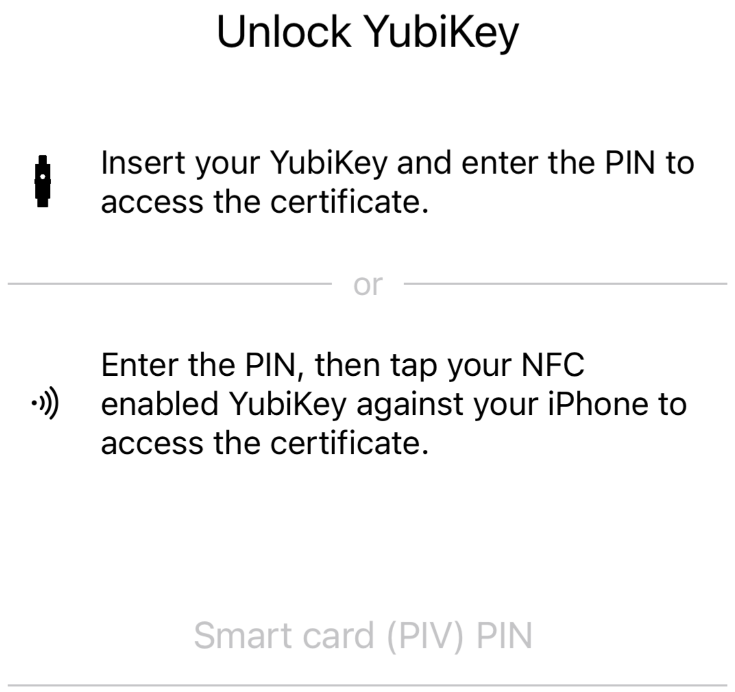
Tap here to complete the request using your YubiKey.

5. Insert your YubiKey into your iOS device, and type in your PIV application pin. If you are using an NFC-enabled YubiKey, enter your PIN first and then tap your key to scan.

Note: Lightning is currently the only supported *physical* connection type for iOS and iPadOS devices. NFC wireless connections are supported on iOS but not on iPadOS. For a complete breakdown of Yubico Authenticator functionality by platform and connection type for each YubiKey model, see the Yubico Authenticator Functionality table.

The default PIV application PIN is 123456. If you reset your PIN using YubiKey Manager, enter that number here. If your YubiKey is managed by your organization, reach out to your admin for your PIN.

Caution: You only have three attempts to enter the correct PIN before your YubiKey is locked.



Unlock YubiKey

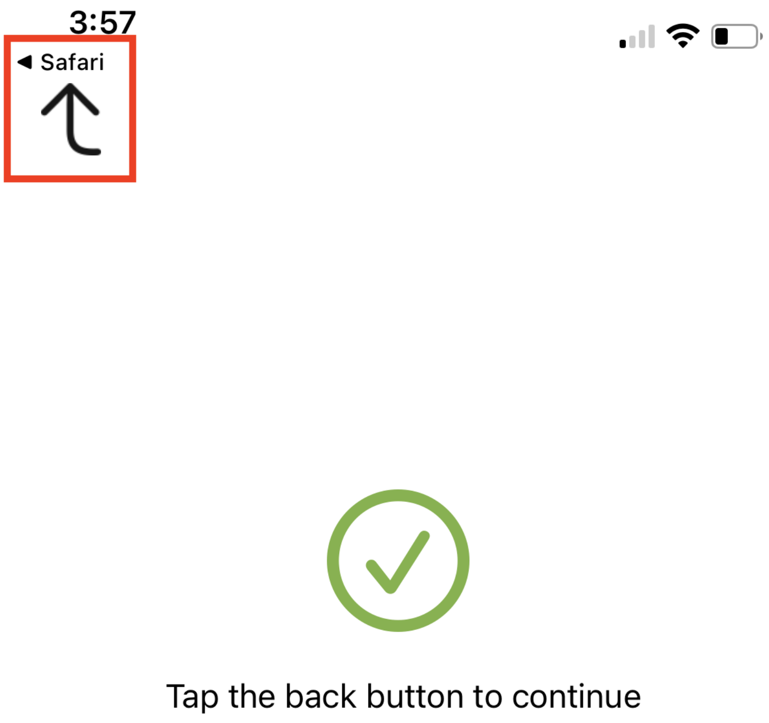
Insert your YubiKey and enter the PIN to access the certificate.

or

Enter the PIN, then tap your NFC enabled YubiKey against your iPhone to access the certificate.

Smart card (PIV) PIN

6. If you entered the correct PIN and authentication was successful, you will see a green check mark. Click on **Safari** in the upper left corner to return to your browser.



Tap the back button to continue

7. After returning to Safari, you will be logged into the website.

To file a support ticket with Yubico, click Support.

CHAPTER

NINETEEN

SMART CARD ON IOS TROUBLESHOOTING

Running into issues using the Smart Card on iOS feature? Check the guidance below for possible solutions.

19.1 Web Browser Does Not Trigger the Yubico Authenticator Application

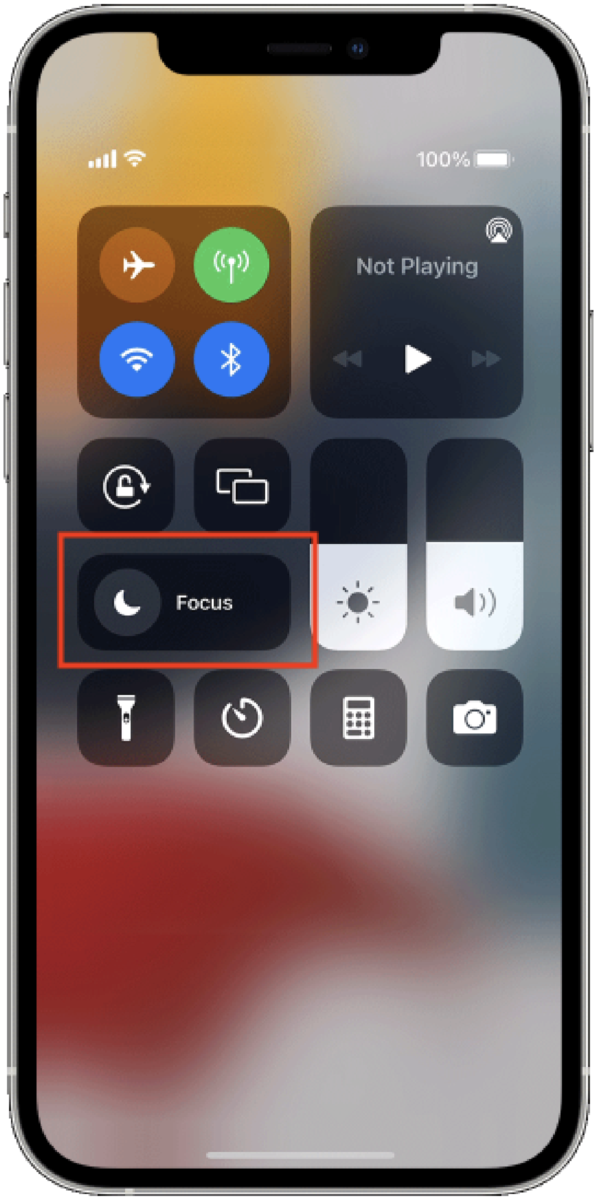
Problem: when trying to authenticate to a website, the browser does not trigger the Yubico Authenticator application, and the pop-up that allows you to complete your authentication request does not appear. You may have received a timeout error or a message about an inability to create a secure connection.

Solution: iOS Focus modes, such as Do Not Disturb, Sleep, Personal, and Work, suppress notifications, including the Yubico Authenticator pop-up. If you have a Focus mode turned on, you will see the mode's symbol on your lock screen (e.g. Do Not Disturb uses a moon symbol). To use the Smart Card on iOS feature with Yubico Authenticator, you must turn off all focus modes *or* add Yubico Authenticator as an Allowed Notification for each mode.

19.1.1 Toggle Focus Modes Off

To toggle your Focus modes off, do the following:

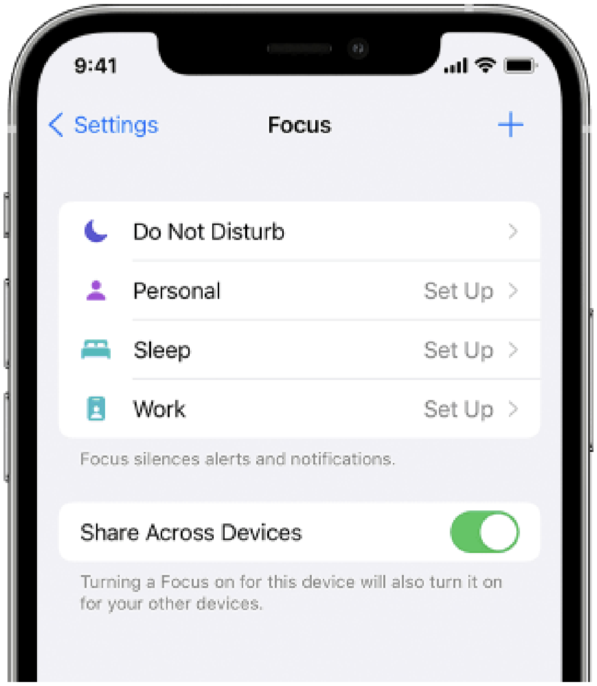
1. Open your Control Center.
2. Select the Focus icon and toggle all modes to the off position.



19.1.2 Add Yubico Authenticator as an Allowed Notification

If your device is running iOS/iPadOS 15 or higher, and you would like to keep your Focus modes on while using the Smart Card on iOS feature, you may instead add Yubico Authenticator as an Allowed Notification.

1. Go to **Settings** > **Focus**.
2. Click on each Focus mode (Do Not Disturb, Personal, Sleep, and Work), select **Allowed Notifications**, and choose the Yubico Authenticator application.



9:41

< Settings Focus +

Do Not Disturb >

Personal Set Up >

Sleep Set Up >

Work Set Up >

Focus silences alerts and notifications.

Share Across Devices ●

Turning a Focus on for this device will also turn it on for your other devices.

To file a support ticket with Yubico, click Support.

CHAPTER

TWENTY

RELEASE NOTES

Updates to the desktop (Windows, Linux, macOS) and Android versions of the Yubico Authenticator app are generally released together and share a version number. The iOS/iPadOS app is released separately and has its own version number. Release numbering follows the semantic versioning format: Major.Minor.Patch.

20.1 2025

20.1.1 Desktop and Android 7.2.3 (11 June 2025)

New features & enhancements

- Language support:
  - New languages are supported in the app, including Chinese (Simplified and Traditional), Czech, Spanish, Swedish, and Turkish.
  - On the **Choose language** selection screen, language names are now displayed in their corresponding language instead of the selected language. For example, if “English” is the selected language, “Deutsch” will be shown instead of “German”.
- Keyboard shortcuts and navigation:
  - A help dialog detailing all supported shortcuts has been added to the app under **Home** -> **Help and about** -> **Shortcuts**.
  - New *keyboard shortcuts* have been added, including ones for opening the application settings, opening the shortcuts help dialog, and navigating through app screens, keys, and menu items.

Resolved issues

- YubiKey Bio Multi-protocol Edition support:
  - References to the PIV PUK have been removed from the app when a YubiKey Bio Multi-protocol Edition key, which does not have a PUK, is connected.
  - Previously, when the PIN was blocked on a YubiKey Bio Multi-protocol Edition key, the **Certificates** screen help dialog contained a button for the wrong PIV application reset operation. This has been fixed so that the button executes the device-wide reset, which is compatible with the YubiKey Bio Multi-protocol Edition.
- Keyboard shortcuts and navigation:
  - Previously, pressing the Escape key three times incorrectly disabled keyboard navigation functionality. This has been fixed.

  - The Escape key now unfocuses from text fields as intended.

- An bug affecting NFC support for YubiKey NEO on Android has been fixed.
- Previously, if more than one YubiKey was connected to a device, the Yubico Authenticator app would prompt the user to enter the FIDO PIN for the active key whenever another YubiKey was disconnected from the device in the background. This has been fixed.
- Yubico Authenticator tray and application icons on Linux have been improved.

20.1.2 iOS and iPadOS 1.12.0 (28 May 2025)

Resolved issues

- FIPS keys are now correctly named within the app.
- TOTP codes now update correctly after scrolling out of view on the **Accounts** screen.

20.1.3 iOS and iPadOS 1.11.1 (16 April 2025)

Resolved issues

- Improved support for YubiKeys that do not have a management application (e.g. YubiKey NEO).

20.1.4 iOS and iPadOS 1.11.0 (9 April 2025)

New features & enhancements

- Added support for YubiKey FIPS Series keys over NFC.

20.1.5 Android 7.2.2 (27 March 2025)

Resolved issues

- A regression introduced in 7.2.1 involving FIDO PIN entry on Android has been fixed.

20.1.6 Android 7.2.1 (27 March 2025)

Resolved issues

- A crash that would occur when reopening the app after a longer period of inactivity has been fixed.
- The handling of invalid input when setting the FIDO PIN has been improved.

20.1.7 Desktop and Android 7.2.0 (26 March 2025)

New features & enhancements

- *Custom icons*, which are now available for both Passkeys and OATH accounts, are now managed under **Settings** on the **Home** page.
- The *Toggle applications* feature is now supported on Android.
- The *application language* can now be configured under **Settings**.
- A *Toggle readers* feature for showing/hiding NFC smart card readers within the Yubico Authenticator app has been added under **Settings**.
- When importing a signed certificate, Yubico Authenticator now automatically checks if the certificate's public key matches the PIV slot's private key (if present).
- The predictive back gesture is now supported on Android.
- Help text and popups have been added and improved.
- Android 15 is now fully supported.
- A PIN, PUK, and management key usage notification has been added to the **Certificates** page.

Resolved issues

- When configuring a slot with a new Yubico OTP credential, the export feature now creates a file with the correct file extension.
- On Android, the Submit button on the keyboard will only execute the **Unlock** operation for the FIDO2 PIN when the length of the entered PIN matches or exceeds the minimum PIN length requirement.
- When a FIDO reset operation is successfully completed on Android, the reset dialog is now closed automatically.
- Previously, some YubiKey serial numbers were displayed with a negative sign (-) in Android. This has been fixed.
- HIDE_OVERLAY_WINDOWS has been implemented in Android to block overlays from third-party apps, improving security in Yubico Authenticator.
- Previously, import of OATH QR codes containing the "=" padding character failed on desktop. This has been fixed.
- Previously, calculation of OATH credentials failed on Android for YubiKeys containing over 40 OATH accounts due to a timeout. This has been fixed.
- Yubico Authenticator for Android now supports devices with 16KB page sizes.
- When copying a Yubico OTP or static password to the clipboard on Android, the help text now uses the selected app language.
- Previously, a cryptic error message was displayed when removing a YubiKey while viewing the **Toggle applications** screen. This has been fixed.
- The "last selected" YubiKey is now updated correctly in the event of a disconnection of the current active key.

20.1.8 iOS and iPadOS 1.10.0 (30 January 2025)

New features & enhancements

- German and Slovak languages are now supported.

20.2 2024

20.2.1 iOS and iPadOS 1.9.1 (4 December 2024)

Resolved issues

- Previously, the app would crash during the OATH **Add account** flow whenever a user scanned a malformed QR code or removed a YubiKey from an iPad device prior to saving the new account credentials. This has been fixed.

20.2.2 iOS and iPadOS 1.9.0 (27 November 2024)

New features & enhancements

- The application's **About** page and its sub-elements (**How does it work** tutorial, **Version history**, and **Licensing**) have been refreshed with SwiftUI.

20.2.3 iOS and iPadOS 1.8.1 (20 November 2024)

Resolved issues

- Previously, the app would crash if a timeout occurred when reading a YubiKey over USB-C or NFC. This has been fixed.

20.2.4 iOS and iPadOS 1.8.0 (14 November 2024)

New features & enhancements

- FIDO2 functionality has been added to the app for compatible YubiKeys:
  - The FIDO2 PIN can now be managed (*set*, *changed*). The PIN format hint also reflects the YubiKey's PIN requirements.
  - The FIDO2 application can now be *reset*.
- The **Configuration** page UI has been refreshed with SwiftUI.
- The OATH password management and reset flows have been refreshed with SwiftUI.

Resolved issues

- Previously, when attempting to add an OATH credential to a YubiKey that did not have space for additional credentials, the error message displayed to the user did not clearly state the cause. This has been improved.

20.2.5 Desktop 7.1.1 (30 October 2024)

Resolved issues

- "Touch your YubiKey" messages in the app are now read correctly by screen readers.
- Previously, attempts to change the PIV PIN/PUK with the wrong PIN/PUK were not handled correctly, reducing the PIN/PUK retries count by two instead of one. This has been fixed.

20.2.6 iOS and iPadOS 1.7.11 (26 September 2024)

Resolved issues

- A crash that occurred in the NFC settings view has been fixed.

20.2.7 iOS and iPadOS 1.7.10 (25 September 2024)

New features & enhancements

- Japanese and French are now fully supported.

20.2.8 Desktop and Android 7.1.0 (25 September 2024)

New features & enhancements

- Additional support for YubiKey 5 FIPS Series keys:
  - The *FIPS status* of each application can now be viewed on the **Home** screen.
  - Help text has been added to assist with putting devices into the FIPS approved state.
  - Warnings have been added to alert users of data loss prior to entering the FIPS approved state.
  - The app now supports Secure Channel Protocol 11b (SCP11b), which ensures FIPS compliance when using FIPS Series YubiKeys with the Authenticator over NFC.
  - An error message is now shown in the app when SCP11b communication is attempted on Android devices that do not support AES-CMAC.
  - The app now prevents unapproved operations (such as adding an OATH account or generating a PIV key) for applications in the "FIPS capable" state on FIPS Series YubiKeys. Error messaging for this behavior has also been improved.
- Additional support for YubiKey Bio Series Multi-protocol Edition keys:
  - Fingerprint authentication is now supported as a configuration option when generating a new PIV key on a Multi-protocol Edition key.
  - *Toggling of applications* is now prohibited for Multi-protocol Edition keys that are "in use". Error messaging has also been improved.

  - Multi-protocol Edition keys are now handled properly on Windows when running Yubico Authenticator in a non-elevated state.
- The *Enterprise Attestation* feature can now be enabled for eligible custom-configured YubiKeys via the **Passkeys** screen.
- The **Home** screen now displays the *PIN complexity status* for YubiKey 5 FIPS Series keys, Security Key Series - Enterprise Edition keys, and eligible custom-configured YubiKeys with firmware version 5.7 or later.
- Instructions and error messaging have been improved in PIN set/change dialogs to account for YubiKey 5 FIPS Series PIN requirements, YubiKey Bio Series Multi-protocol Edition PIN requirements, and PIN complexity.
- Android 15 is now fully supported.
- Messaging has been added to support users in activating YubiKeys with the *Restricted NFC* feature enabled.
- Yubico Authenticator is now compatible with screen readers, which includes NVDA, JAWS, and Microsoft Narrator.
- UI colors have been updated to align with changes in the latest Flutter upgrade.
- A *grid layout* option has been added to the **Passkeys** and **Accounts** screens.
- App version is now recorded during *log collection*.
- The NFC dialogs on Android have been improved to better support the slower wireless communication of YubiKeys with firmware version 5.7.
- The following Android forms have been updated so that focus shifts automatically to the next text box when the Submit key is tapped:
  - Set OATH password
  - Manage OATH password
  - Set FIDO2 PIN
  - Change FIDO2 PIN

Resolved issues

- Previously, toggling YubiKey applications on/off over NFC on desktop did not update the application state until the YubiKey was removed from the NFC reader and reconnected. This has been fixed so that the application state updates with the key remaining connected.
- Previously, changing the OATH password via NFC resulted in an error even when all input fields were entered correctly. This has been fixed so that the operation completes as expected.
- Previously, when scrolling down the **Accounts** or **Passkeys** screens so that the search bar becomes hidden, using the Cmd/Ctrl + F shortcut did not show the search bar as expected. This has been fixed.

20.2.9 Android 7.0.1 (29 May 2024)

Resolved issues

- When starting the app via NFC, OATH accounts are now shown after a single NFC tap.
- Previously, fingerprints would be shown in a random order on the **Fingerprints** screen in the app whenever a YubiKey Bio Series key was connected to an Android device. This has been fixed so that fingerprints are shown in the order in which they were created.
- The dynamic color selection on the **Home** page has been improved.

- An issue affecting the use of USB-connected YubiKeys in the app while the Android device's NFC sensor is activated by a non-YubiKey NFC object has been fixed.

20.2.10 Desktop and Android 7.0.0 (6 May 2024)

New features & enhancements

- A *Home* screen has been added. **Home** features device information, customization options, and the factory reset functionality.
- A search bar has been added to the *Passkeys* screen. When a passkey is selected, additional passkey information is displayed.
- French and Japanese are now officially supported.
- Support for FIDO features (FIDO PIN, Passkeys, Fingerprints, and FIDO2 application factory reset) has been added to the Android app.
- Management features for retired PIV key slots has been added.
- Applications can now be *toggled on/off* when the Configuration Lock code is set. The Yubico Authenticator app does not let you set/unset the Configuration Lock Code itself, but it will prompt you for it if needed during an operation.
- Yubico OTP application slots can now be managed when an OTP Access Code is set. The Yubico Authenticator app does not let you set/unset the OTP Access Code itself, but it will prompt you for it if needed during an operation.
- An external program can be used on Linux to *copy OTPs to the clipboard from the system tray*.
- Additional features have been added to support YubiKeys with the new 5.7 firmware:
  - PIN complexity handling.
  - New PIV key algorithms: RSA3072, RSA4096, Ed25519, and X25519.
  - PIV keys can be moved and deleted.

CHAPTER

TWENTYONE

COPYRIGHT

21.1 Trademarks

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

21.2 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.

21.3 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.

21.4 Document Updated

2025-06-11 16:11:28 UTC