

---

# **Yubico Authenticator User Guide**

**Yubico**

**Jun 17, 2024**



# CONTENTS

<b>1</b>	<b>Yubico Authenticator Overview</b>	<b>1</b>
1.1	Highlighted features . . . . .	1
1.2	Advantages . . . . .	2
1.3	Command line interface (CLI) tool . . . . .	3
<b>2</b>	<b>Platforms and Requirements</b>	<b>5</b>
2.1	Compatible YubiKeys . . . . .	5
2.2	Supported platforms . . . . .	5
2.3	WebAuthn Browser Support . . . . .	6
<b>3</b>	<b>Download the App</b>	<b>7</b>
3.1	Previous releases . . . . .	8
3.2	Developers . . . . .	8
<b>4</b>	<b>Install the App</b>	<b>9</b>
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
<b>5</b>	<b>Home and Settings</b>	<b>17</b>
5.1	The Home page: YubiKey at a glance . . . . .	17
5.2	Switching between keys . . . . .	18
5.3	Change a YubiKey’s label and color . . . . .	19
5.4	Toggle YubiKey applications on/off . . . . .	20
5.5	Change the Authenticator theme . . . . .	21
5.6	Android settings . . . . .	22
5.7	iOS/iPadOS settings . . . . .	24
<b>6</b>	<b>Accounts: OATH</b>	<b>31</b>
6.1	What is OATH authentication? . . . . .	31
6.2	Adding a new account . . . . .	32
6.3	Authenticating with OATH and Yubico Authenticator . . . . .	37
6.4	Password protection . . . . .	39
6.5	Pinning an account . . . . .	45
6.6	Renaming an account . . . . .	47
6.7	Deleting an account . . . . .	48
6.8	Custom icons . . . . .	48

<b>7</b>	<b>Passkeys: FIDO2</b>	<b>51</b>
7.1	Creating and managing the FIDO2 PIN . . . . .	51
7.2	Viewing and deleting passkeys . . . . .	54
<b>8</b>	<b>Fingerprints: FIDO2</b>	<b>57</b>
8.1	Creating and managing the FIDO2 PIN . . . . .	57
8.2	Registering and managing fingerprints . . . . .	60
<b>9</b>	<b>Certificates: PIV</b>	<b>65</b>
9.1	Add and manage certificates . . . . .	65
9.2	Manage the PIN, PUK, and Management Key . . . . .	66
<b>10</b>	<b>Slots: Yubico OTP Application</b>	<b>67</b>
10.1	Yubico OTPs . . . . .	67
10.2	Static passwords . . . . .	70
10.3	Challenge-response . . . . .	71
10.4	OATH HOTPs . . . . .	72
10.5	Managing slots . . . . .	74
<b>11</b>	<b>Factory Reset</b>	<b>77</b>
11.1	What happens during a reset? . . . . .	77
11.2	How does a reset affect my accounts? . . . . .	77
11.3	Recommended preparation . . . . .	78
11.4	Performing a reset on desktop and Android . . . . .	78
11.5	Performing a reset on iOS/iPadOS . . . . .	79
<b>12</b>	<b>Tips</b>	<b>81</b>
12.1	Resizing the app window . . . . .	81
12.2	Register a spare YubiKey . . . . .	84
12.3	Start Yubico Authenticator with the app window hidden . . . . .	86
12.4	Generate OATH OTPs from pinned accounts via the menu bar or system tray . . . . .	87
12.5	Set an OATH application password . . . . .	88
12.6	Works with YubiKey Catalog . . . . .	88
<b>13</b>	<b>Troubleshooting and Support</b>	<b>91</b>
13.1	OATH accounts . . . . .	91
13.2	Yubico OTP Slots . . . . .	91
13.3	Android . . . . .	92
13.4	Reporting issues and submitting feature requests . . . . .	93
13.5	Getting additional help . . . . .	93
13.6	Generating and collecting diagnostic data and logs . . . . .	93
<b>14</b>	<b>Azure MFA with Yubico Authenticator</b>	<b>97</b>
14.1	Self registration (recommended method) . . . . .	97
14.2	Administrator registration (alternative method) . . . . .	101
14.3	Use a YubiKey to sign in . . . . .	105
14.4	Troubleshooting . . . . .	105
14.5	Additional information . . . . .	106
<b>15</b>	<b>Smart Card on iOS</b>	<b>107</b>
15.1	X.509 Certificates . . . . .	108
15.2	Prerequisites . . . . .	108
15.3	Overview: Setup Process . . . . .	108
15.4	Troubleshooting . . . . .	111

<b>16 Import Smart Card Certificates onto your YubiKey</b>	<b>113</b>
16.1 YubiKey Manager GUI . . . . .	113
16.2 YubiKey Manager CLI . . . . .	117
16.3 Next Steps . . . . .	118
<b>17 Smart Card Certificate Provisioning</b>	<b>119</b>
17.1 Provision Your Public Certificate . . . . .	119
17.2 Next Steps . . . . .	121
<b>18 Authenticating with Smart Card on iOS</b>	<b>123</b>
18.1 Authenticate to a Website on Safari . . . . .	123
<b>19 Smart Card on iOS Troubleshooting</b>	<b>127</b>
19.1 Web Browser Does Not Trigger the Yubico Authenticator Application . . . . .	127
<b>20 Release Notes</b>	<b>131</b>
20.1 Desktop and Android 7.0.0 (6 May 2024) . . . . .	131
<b>21 Copyright</b>	<b>133</b>
21.1 Trademarks . . . . .	133
21.2 Disclaimer . . . . .	133
21.3 Contact Information . . . . .	133
21.4 Document Updated . . . . .	134



## 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 OATH OTP codes for two-factor authentication (2FA) to supported accounts.
- 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 supported across Windows, macOS, Linux, Android, and iOS/iPadOS devices and works over USB, Lightning, and wireless NFC connections.

---

**Note:** Connection type compatibility is dependent on your specific device and YubiKey model.

---

### 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 one of the following credential types: Yubico OTP, challenge-response, OATH HOTP, or static password.*
- *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, this means that 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](#).



## PLATFORMS AND REQUIREMENTS

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

---

**Note:** Compatibility between YubiKey interface and desktop/mobile platform is device-dependent. For example, USB-C is currently not supported on iOS/iPadOS, and not all mobile devices have a built-in NFC reader.

---

### 2.1 Compatible YubiKeys

YubiKeys from the following series are compatible with Yubico Authenticator:

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

### 2.2 Supported platforms

Fully Supported - these are the platforms 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 version 17763.0 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 users to have 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](#).

## 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](#)

## INSTALL THE APP

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

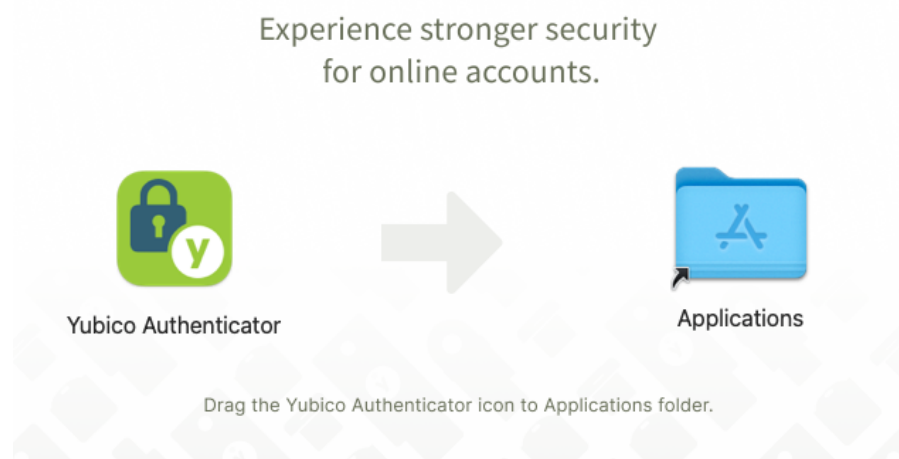
### 4.1 macOS

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.

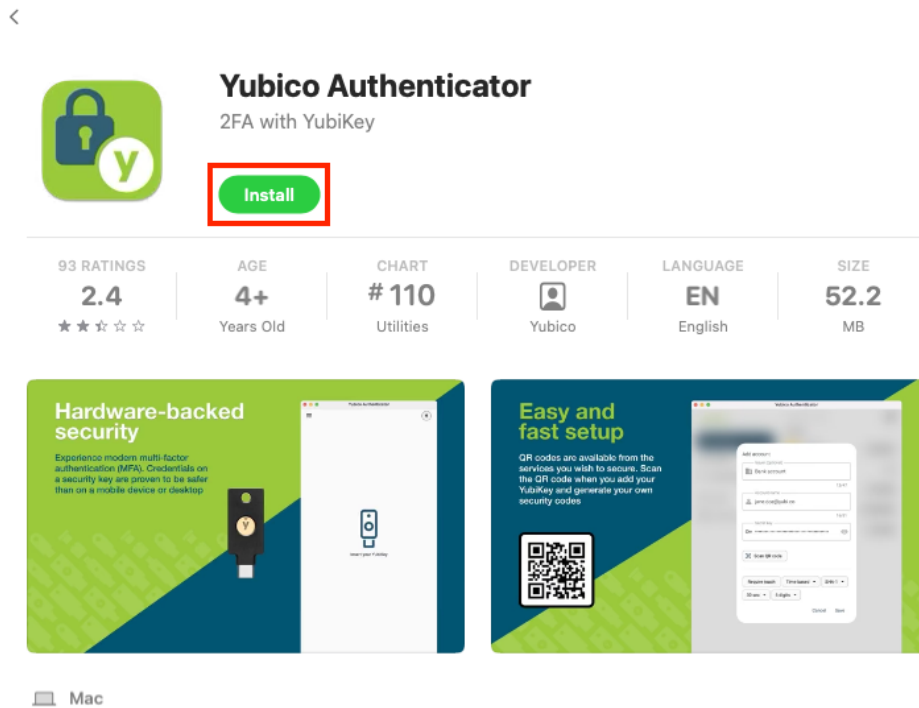


3. *Enable input monitoring and screen recording.*

### 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.



3. *Enable input monitoring and screen recording*

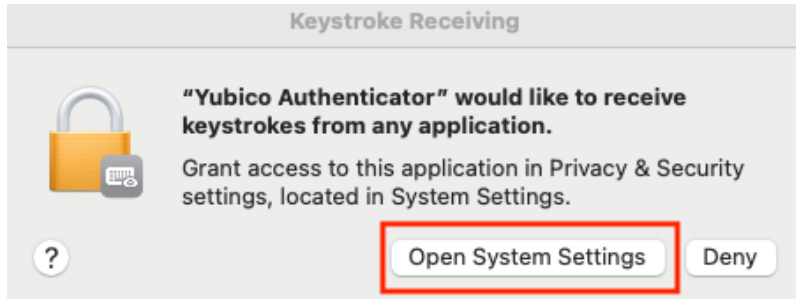
### 4.1.3 Enable input monitoring

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.

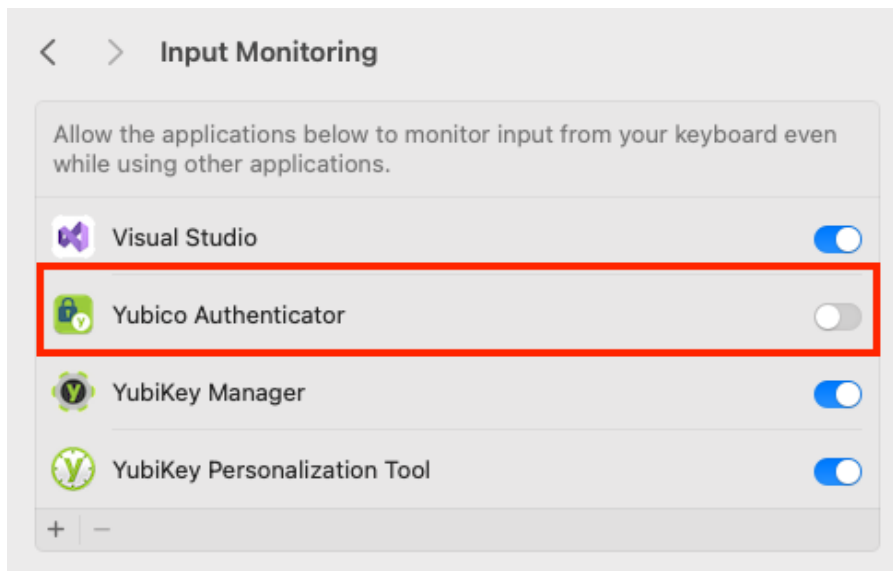
To enable input monitoring, do the following:

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**.

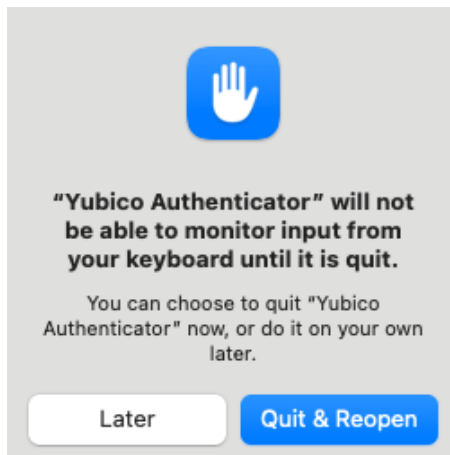




- This will take you to your **Input Monitoring** settings. Flip the toggle next to **Yubico Authenticator** to the “on” position.



- 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**.



---

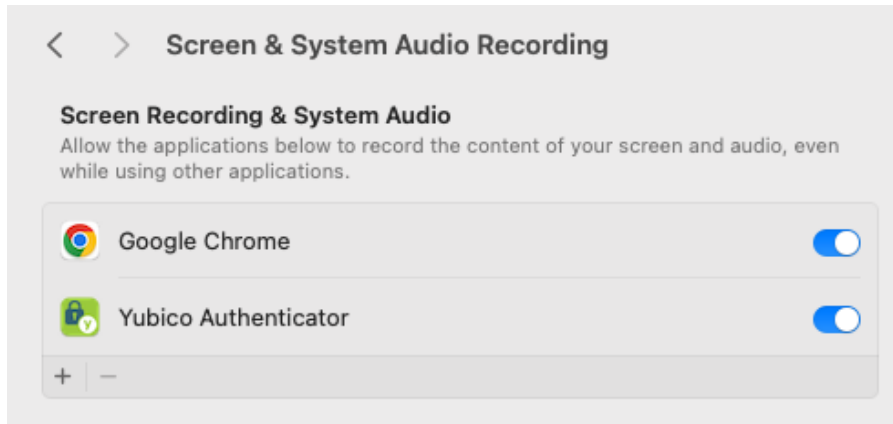
**Note:** If you are not automatically prompted to change your input monitoring settings when opening the app for the first time, you can still do this manually by going to **System Settings > Privacy & Security > Input Monitoring**. Click the + icon, select the Yubico Authenticator app in the window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



## 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 pcsd

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

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

```
sudo systemctl enable --now pcsd
```

To check if pcsd is running, enter:

```
systemctl status pcsd
```

To check if pcsd is enabled, enter:

```
systemctl is-enabled pcsd
```

### 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`.

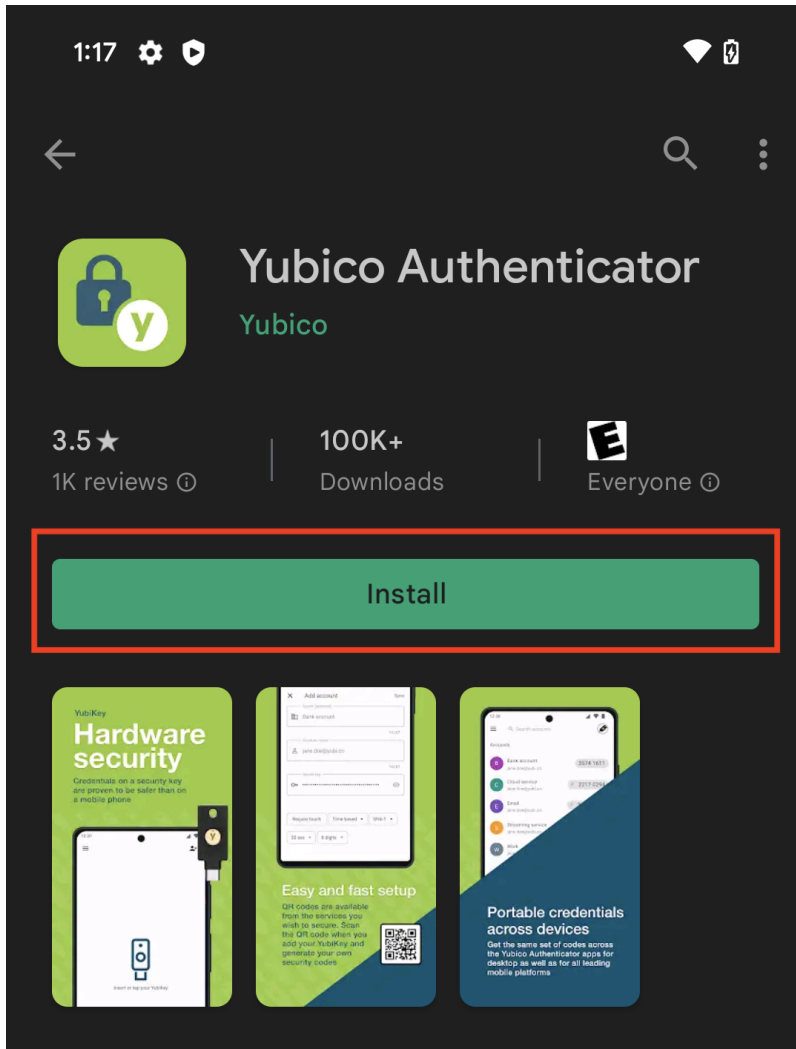
Alternatively, you can create a shortcut for Yubico Authenticator in the app launcher by running the [desktop\\_integration.sh](#) script, which is included in the tarball.

### 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](#).

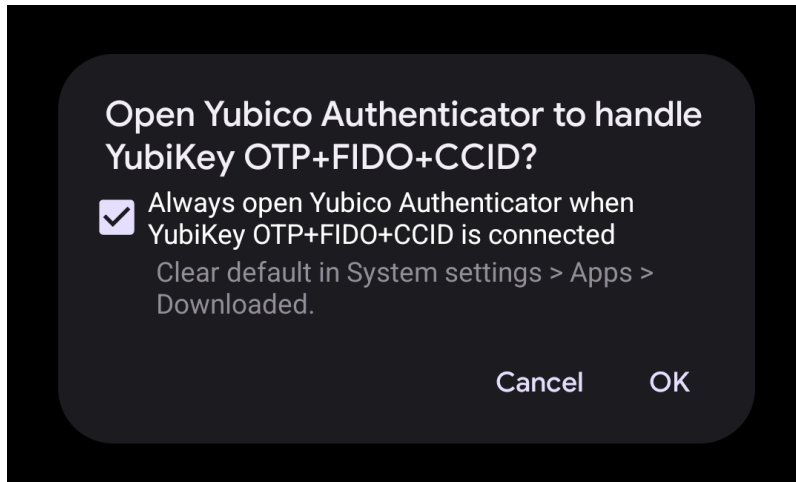
## 4.4 Android

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



#### 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**.

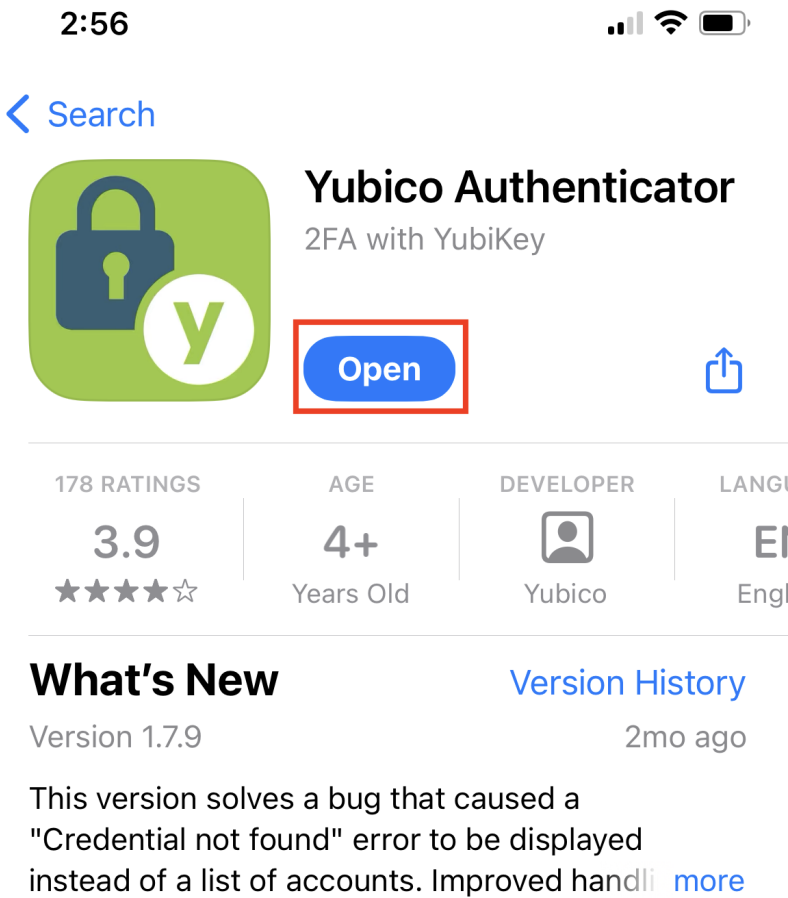


#### 4.4.2 Installation via direct download

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.



## 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](#)

## 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 (desktop only)*
- *changing the app theme*
- *toggling between multiple connected keys (desktop only)*
- *performing a factory reset of a YubiKey application*

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.

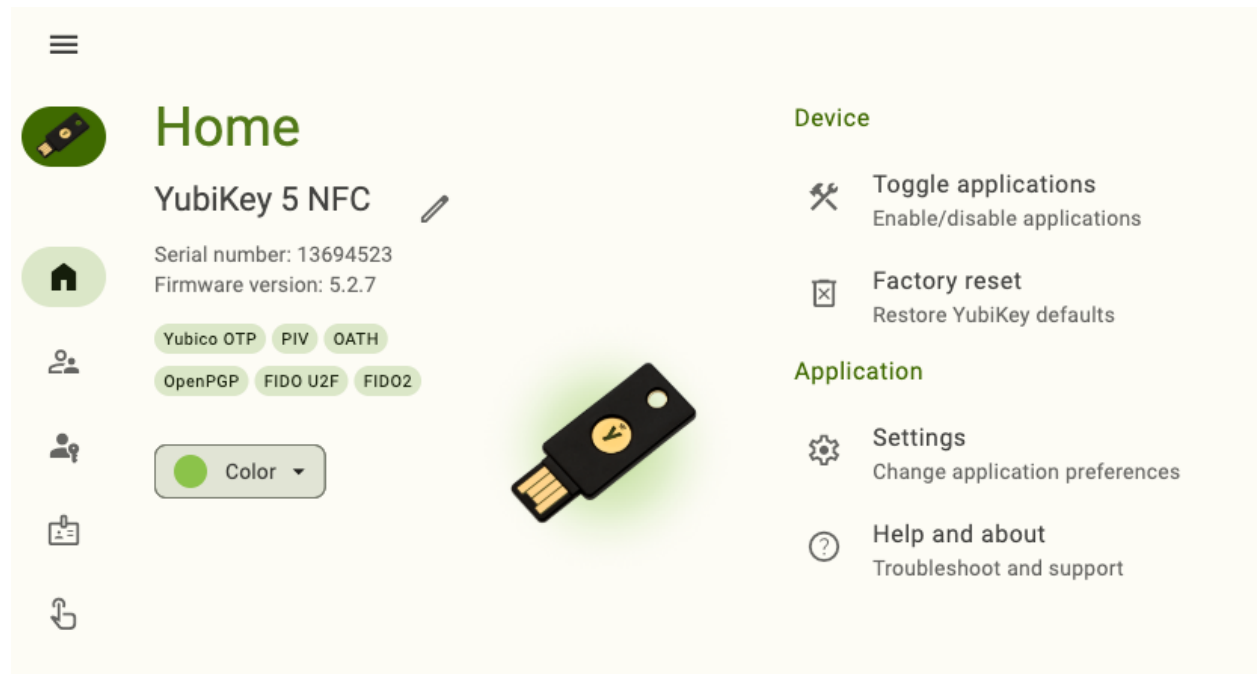
---

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.
- Enabled applications for current connection type (USB or NFC). Applications include Yubico OTP, PIV, OATH, OpenPGP, FIDO U2F, and FIDO2, depending on your YubiKey.

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.



## 5.2 Switching between keys

---

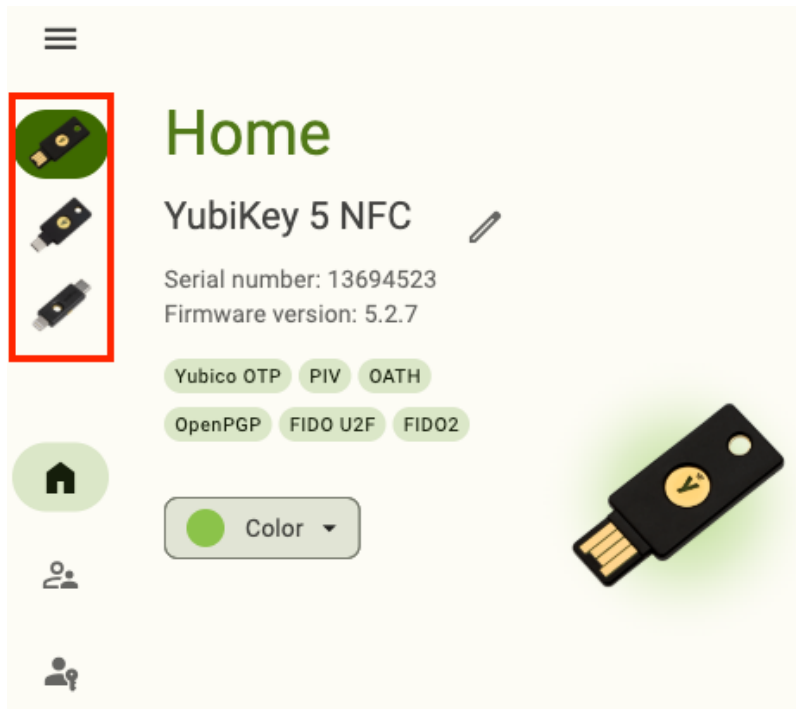
**Note:** Toggling between multiple connected YubiKeys is available on Yubico Authenticator for Desktop only.

---

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.





### 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.

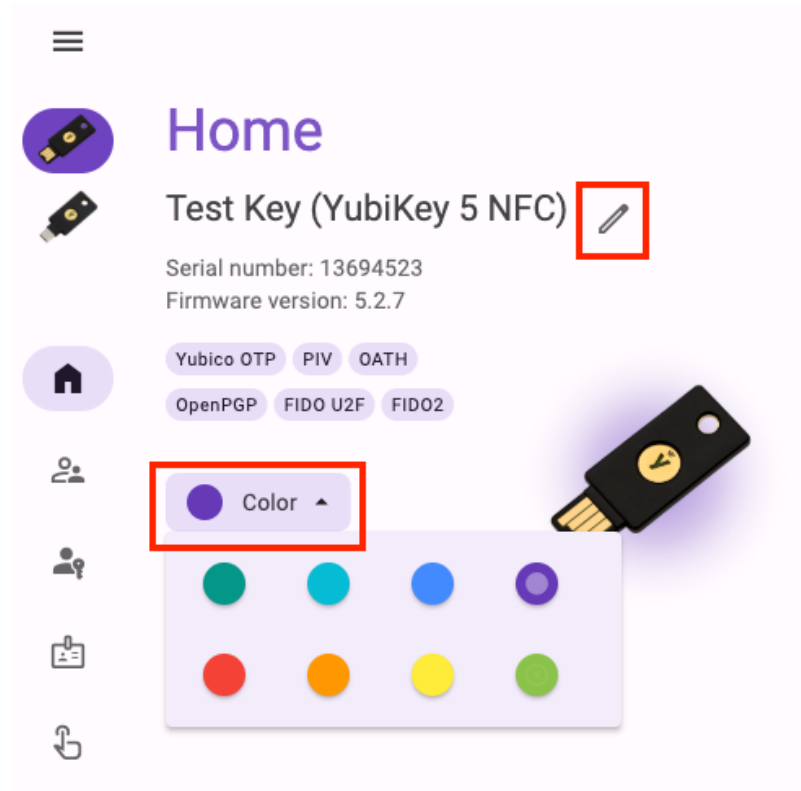
By default, connected YubiKeys are labeled with their model name on the **Home** page and the left menu bar. They also have a default color scheme within the app (green on desktop, purple on Android).

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 **Color** drop-down menu 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**.



### 5.4 Toggle YubiKey applications on/off

---

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

---

The YubiKey applications, which include Yubico OTP, PIV, OATH, OpenPGP, FIDO U2F, 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.

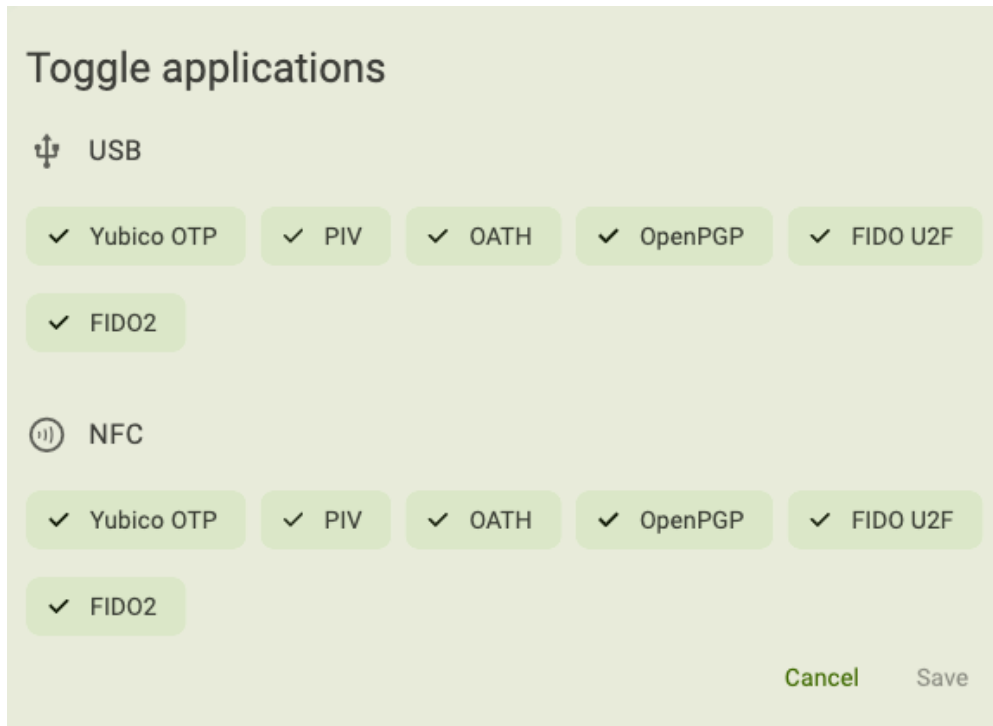
---

**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.
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**.



## 5.5 Change the Authenticator theme

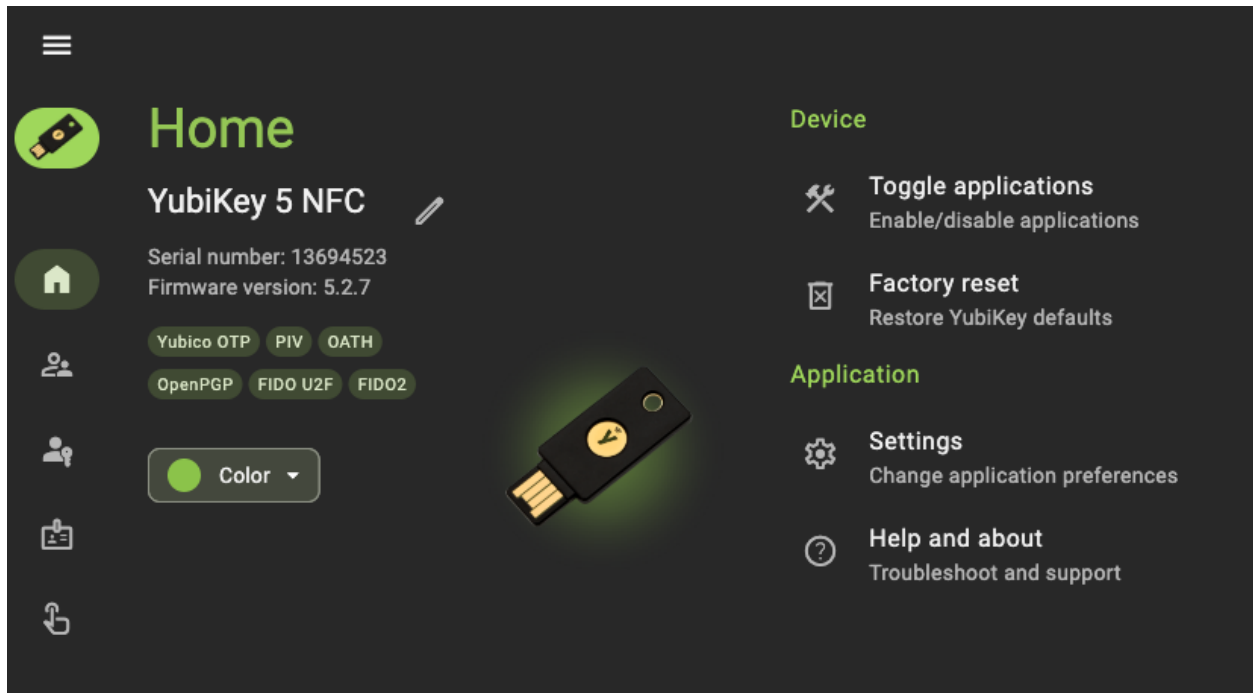
**Note:** The app theme can be changed on Yubico Authenticator for Desktop and Android only.

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.



## 5.6 Android settings

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

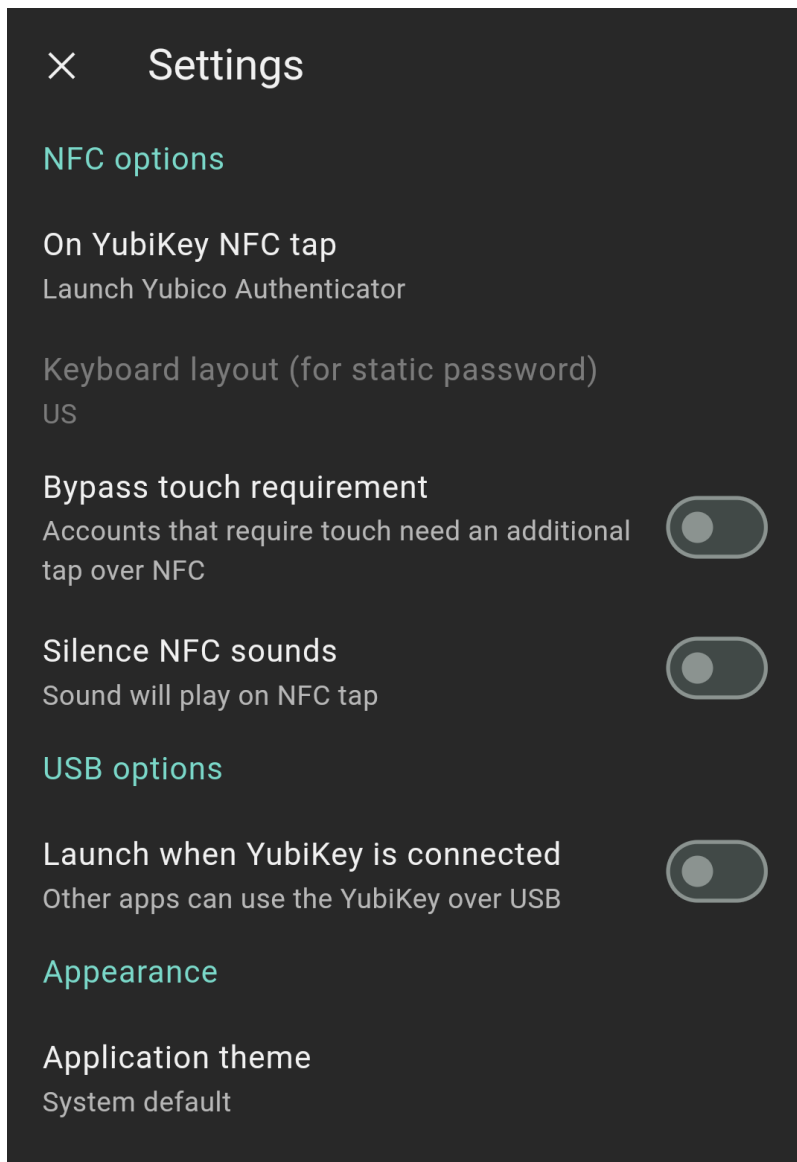
- NFC tap behavior
- Touch requirement with NFC
- NFC sounds
- USB connectivity

---

**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**.



### 5.6.1 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**.

### 5.6.2 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**.

### 5.6.3 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**.

### 5.6.4 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.

## 5.7 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

### 5.7.1 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



## INFORMATION

Device type

YubiKey 5Ci

Firmware

5.2.7

Serial number

15213076

## CONFIGURATION

Toggle One-Time Password >

Passwords and reset >

NFC settings >

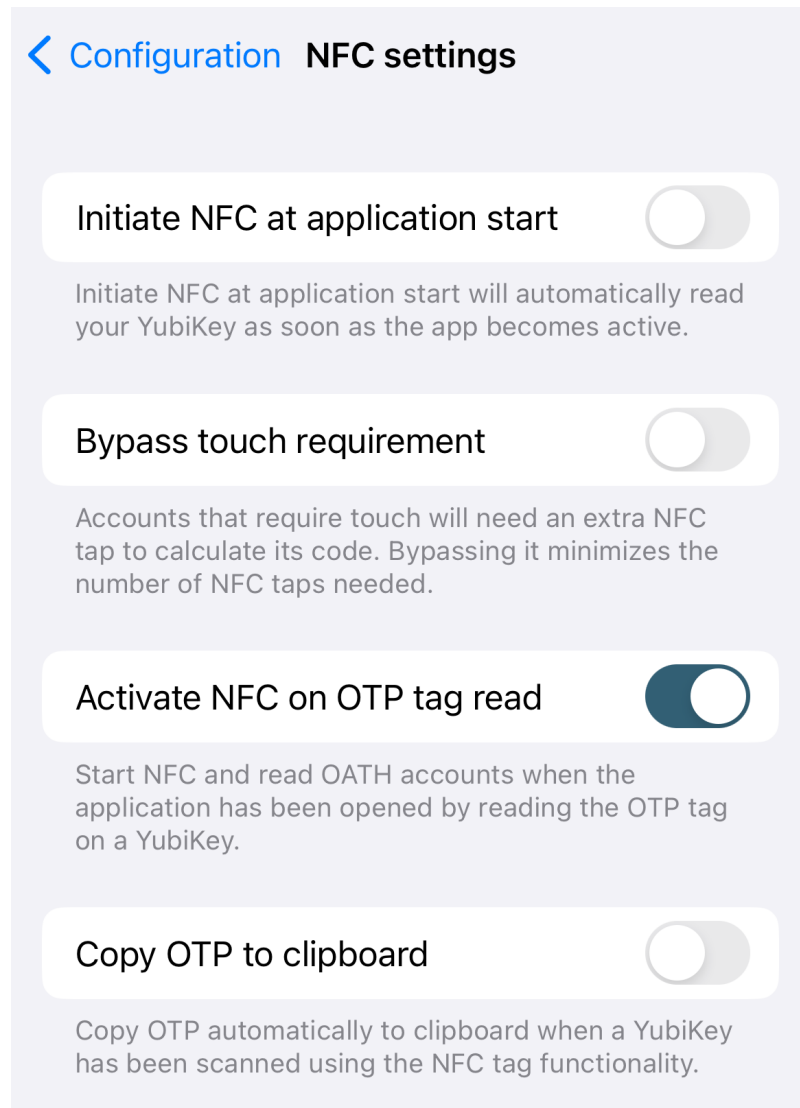
Smart card extension

Enabled >

## 5.7.2 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**.





### 5.7.3 Touch requirement

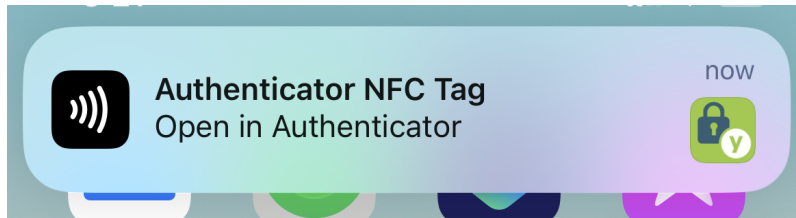
When an *OATH account* is added to a YubiKey, it can be configured to “require touch” in order to generate an OTP. For NFC connections, this means tapping the YubiKey against the device’s NFC reader at least twice: once to display the OATH accounts and again to generate and display the OTP for a particular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

### 5.7.4 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.



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**.

### 5.7.5 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

## Yubico OTP



ccccccuivgdghkfunlruuclgdgdlguvehneviirklcu

## 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**.

### 5.7.6 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 Lightning 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.

---



## 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.

---

The Accounts feature of Yubico Authenticator allows you to:

- *Configure a YubiKey with OATH credentials linked to a specific account.*
- *Generate and display OTPs for two-factor authentication using those OATH credentials.*
- *Protect the OATH application of a YubiKey with a password.*
- *Pin OATH accounts to the top of the Accounts screen 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.

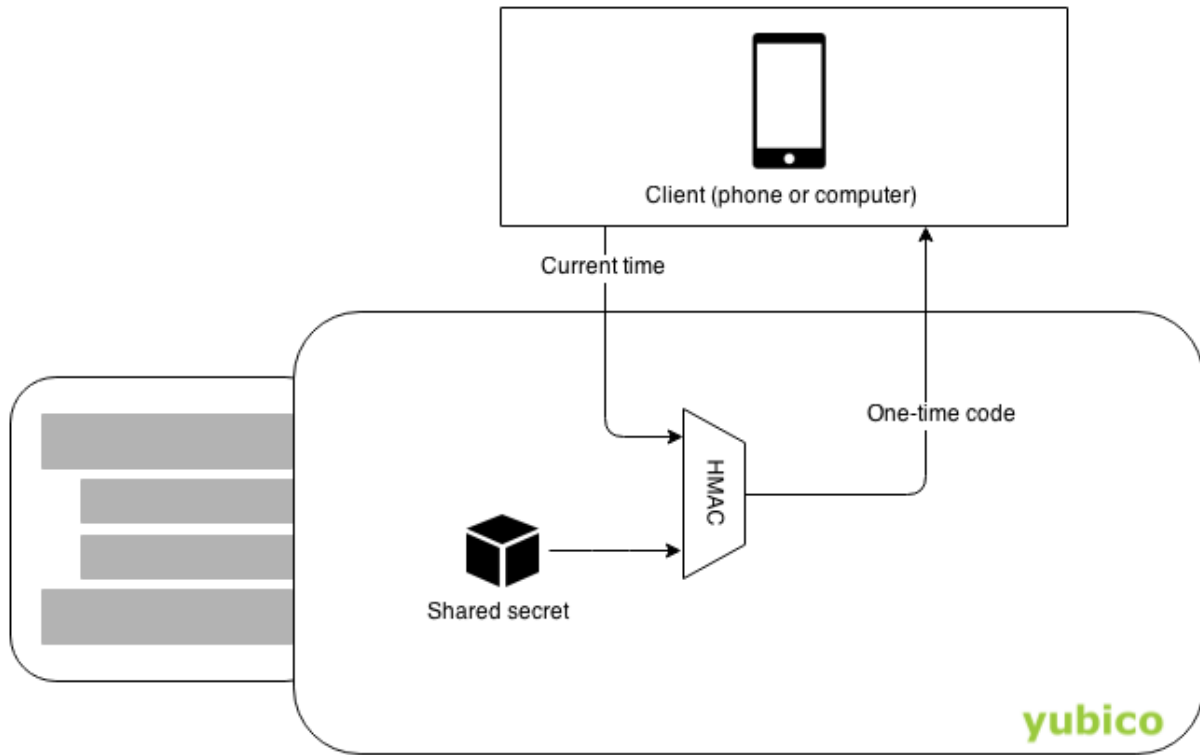
HOTPs are generated by hashing a secret key, counter, and length (6 or 8 digits) with a hashing algorithm (such as SHA-1). TOTPs are generated by hashing a secret key, current time, period, and length (6 or 8 digits) with a hashing algorithm. The resulting HOTPs and TOTPs are codes of 6 or 8 digits in 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/service 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 (including the secret key) are stored in the OATH application in the key’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 secrets 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*.
- **Accessibility:** Once a YubiKey is configured with an OATH account, OTPs can be generated by Yubico Authenticator on *any* device. For example, if your phone dies, you could still generate OTPs 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 and services typically describe OATH authentication as “two-factor authentication using an authenticator app”.

---

During registration, the YubiKey stores the secret key and associated account information. For information on how to access the secret key credentials with a particular site/account/service, see the [Works with YubiKey catalog](#).

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 still generate OTPs with that key on your desktop and vice versa.

With Yubico Authenticator, OATH accounts can be added via QR code or by entering the secret key (among other fields) manually. Both methods give you the option to “require touch” as a means of user verification. If you do not enable the touch requirement, the YubiKey will begin generating TOTP 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.

If you require touch, you must manually initiate the OTP calculation in Yubico Authenticator for each OTP you wish to generate.

---

**Note:** HOTP generation must be initiated manually regardless of whether touch is required.

---

To add an account, do the following:

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

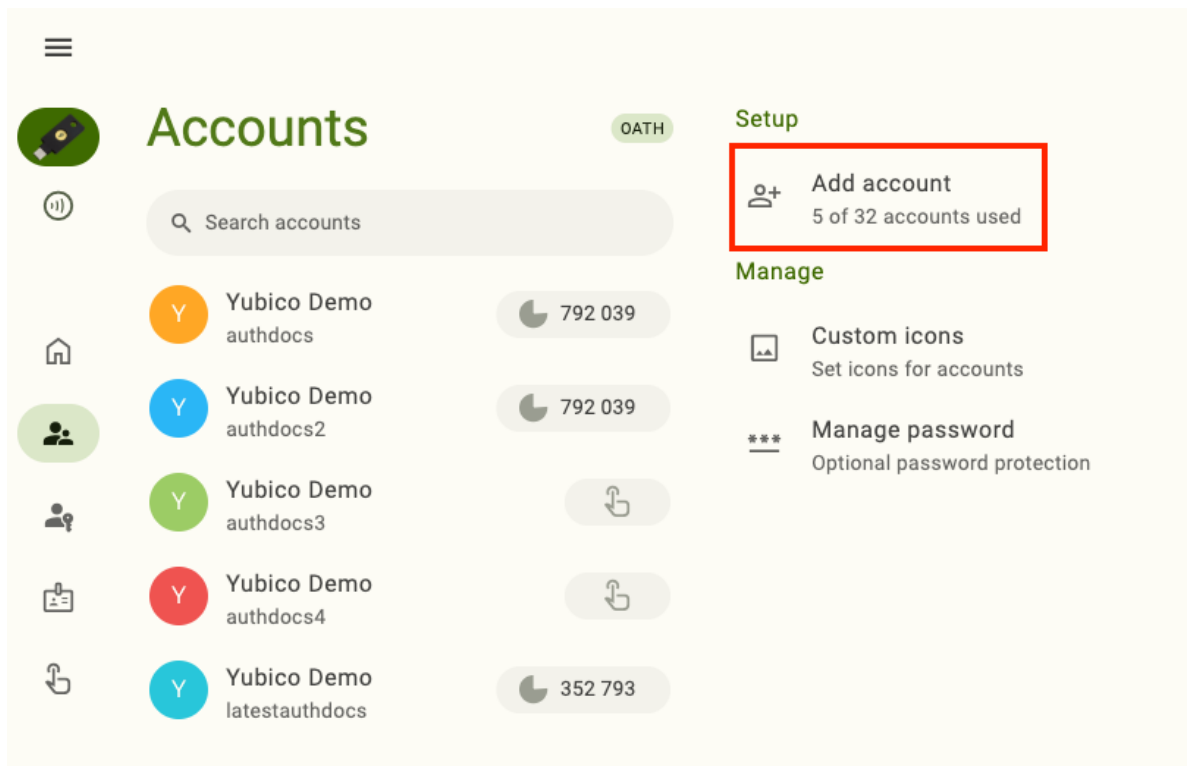
To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

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

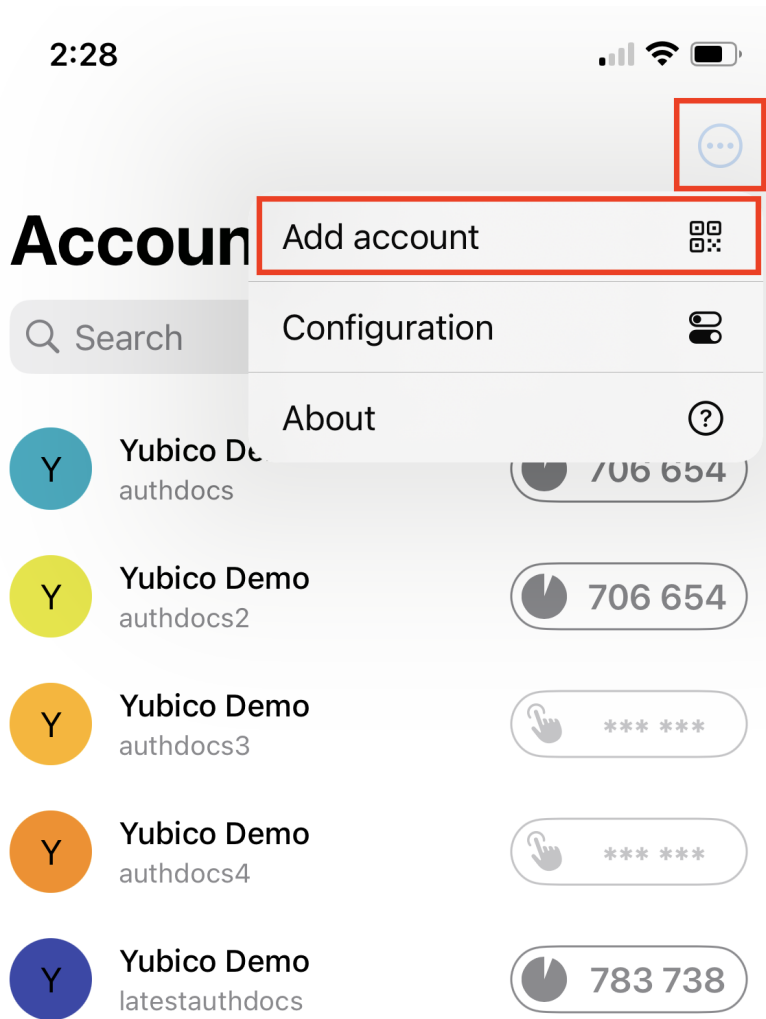
To connect via NFC on iOS/iPadOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.

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/iPadOS, 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 on a particular site you wish to register with.



# 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?

NEXT

---

**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 (provided by the site/account/service 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) and/or **Account name** (your username) if needed, click **Require touch** (optional), and then click **Save**. For NFC connections on Android and iOS/iPadOS, 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, click **Add manually** (desktop and Android) or **Enter manually** (iOS/iPadOS).

On the **Add account** screen, enter an **Issuer** (the site/service), **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/account/service**. 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** (optional) and then **Save**. For NFC connections on Android and iOS/iPadOS, tap your key to complete the operation.

The screenshot shows the 'Add account' screen with the following details:

- Issuer (optional):** Yubico Demo (11/55 characters)
- Account name:** authdemo (8/52 characters)
- Secret key:** [Redacted]
- Options:** Require touch (checked), Time based, SHA-1, 30 sec, 6 digits
- Buttons:** Cancel, Save

7. The account or service 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 was TOTP, enter the OTP listed next to the account in Yubico Authenticator. If you did require touch or the OTP type was 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/secret key and a different account name (for example, “account-name-backup”).

## 6.3 Authenticating with OATH and Yubico Authenticator

Once an OATH account has been *registered* with a YubiKey, that key in conjunction with Yubico Authenticator can be used to log in to that account.

To log into an account 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, plug your YubiKey into your device, click the menu icon in the upper left corner of the app (desktop and Android only), and select **Accounts**.

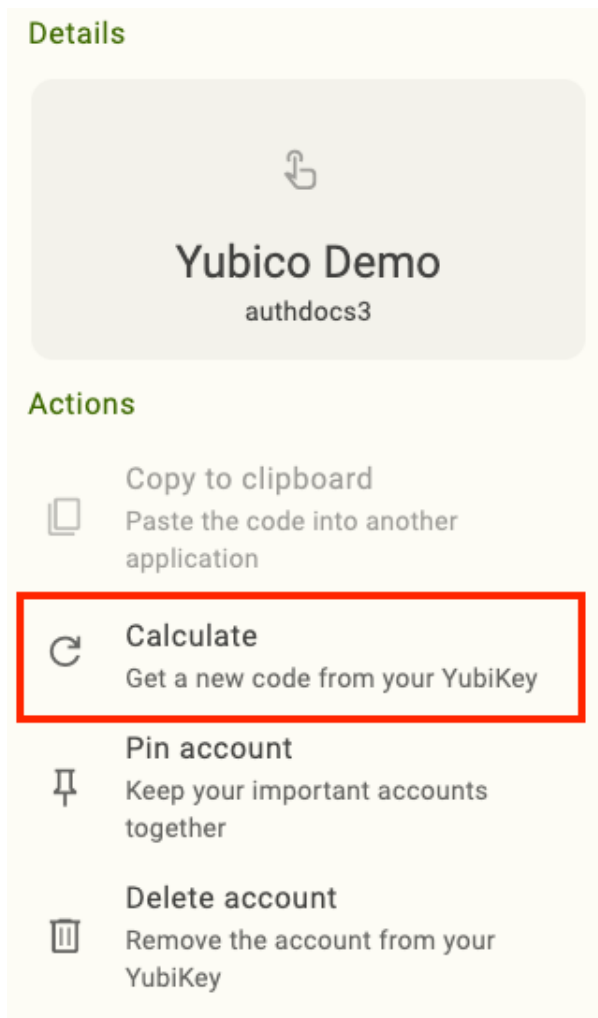
To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

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

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

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/iPadOS, 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.



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

To further enhance the security of your YubiKey, a password can be created for its OATH application so that none of the **Accounts** features can be accessed (on any device) until the password is entered correctly. This means that OTP codes cannot be viewed or calculated and accounts cannot be viewed, pinned, or deleted prior to password submission.

Once created, the password can be:

- remembered/forgotten on a particular 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 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.

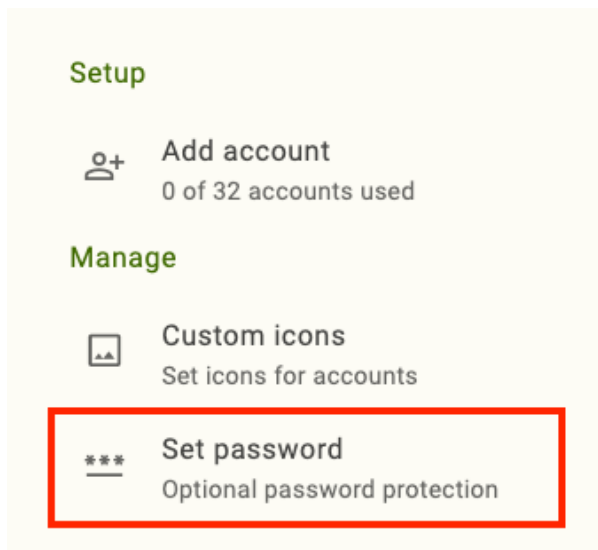
---

### 6.4.1 Desktop and Android

#### Create an OATH password

To create 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 **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**.

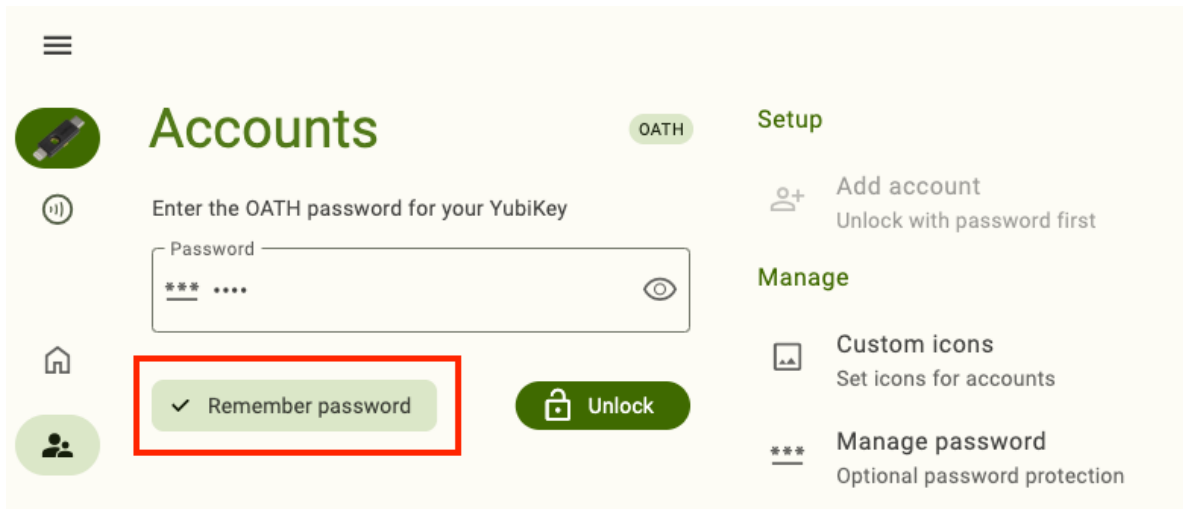
For NFC connections on Android, tap your key to complete the operation.

### 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 elect to remember the password on a particular device you trust to bypass this requirement. And once remembered, a password can also be forgotten (cleared from memory) at any time.

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.



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 password

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**

Enter your current password. If you don't know your password, you'll need to reset the YubiKey.

Current password

**Remove password** **Clear saved password**

Enter your new password. A password may contain letters, numbers and special characters.

New password

Confirm password

**Cancel** **Save**

## 6.4.2 iOS/iPadOS

### Create an OATH password

To create an OATH password, do the following:

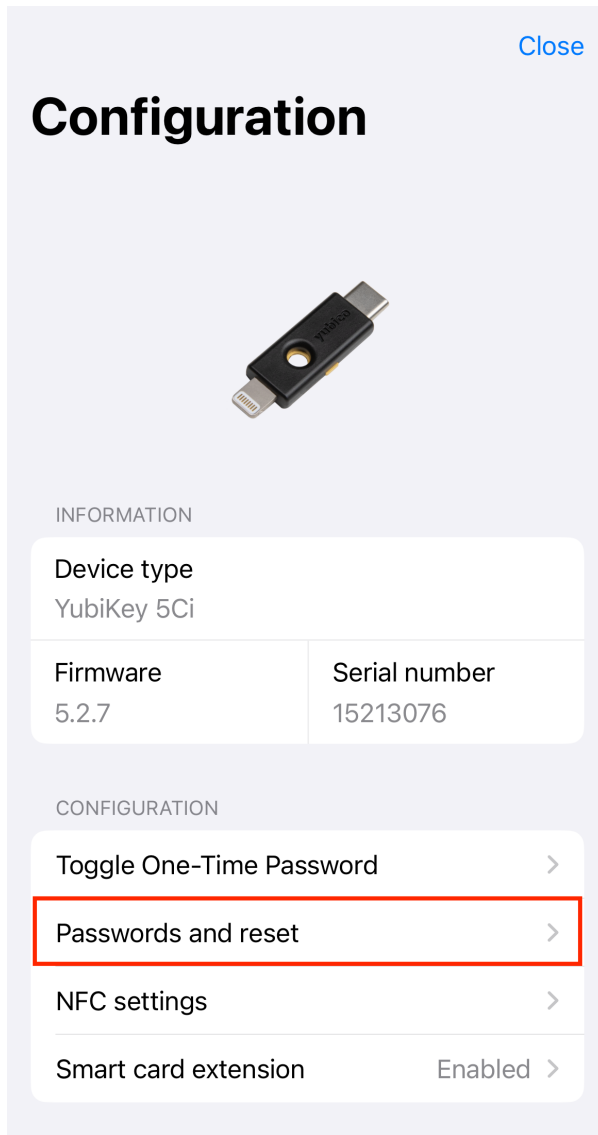
1. Plug your YubiKey into your device and select **Accounts**.

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



2. Click the three dots in the upper right corner of the app and select **Configuration**.
3. On the **Configuration** screen, select **Passwords and reset**.





4. Click **Set password**, 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, 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 elect to remember the password on a particular device you trust to bypass this requirement. And once remembered, a password can also be forgotten (cleared from memory) at any time.

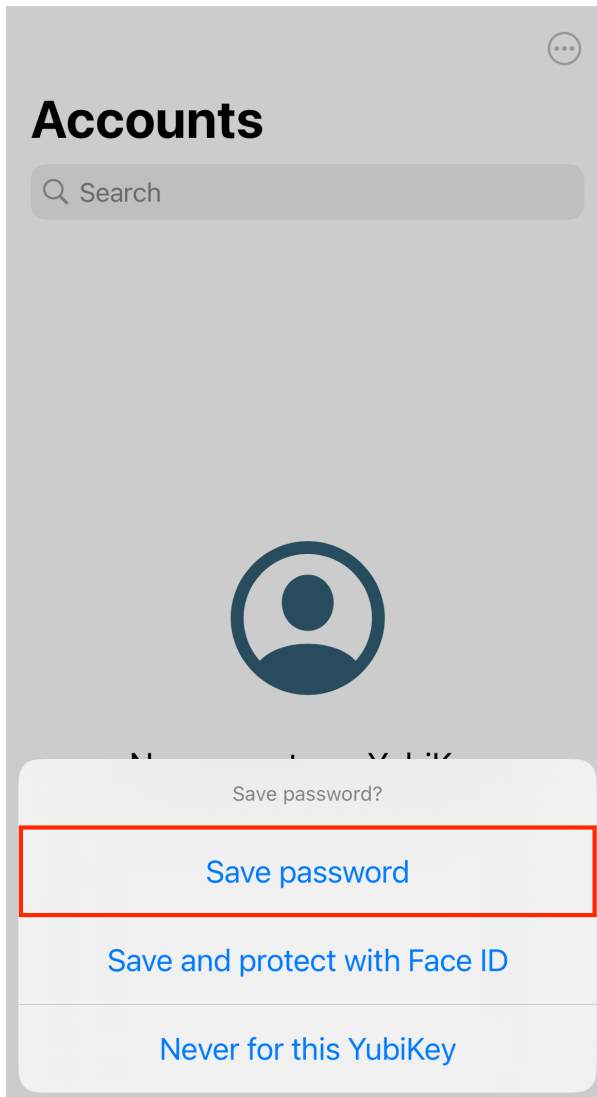
To remember or forget an OATH password on a particular device, do the following:

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

To connect via NFC on iOS/iPadOS, swipe down on the screen and 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, 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.

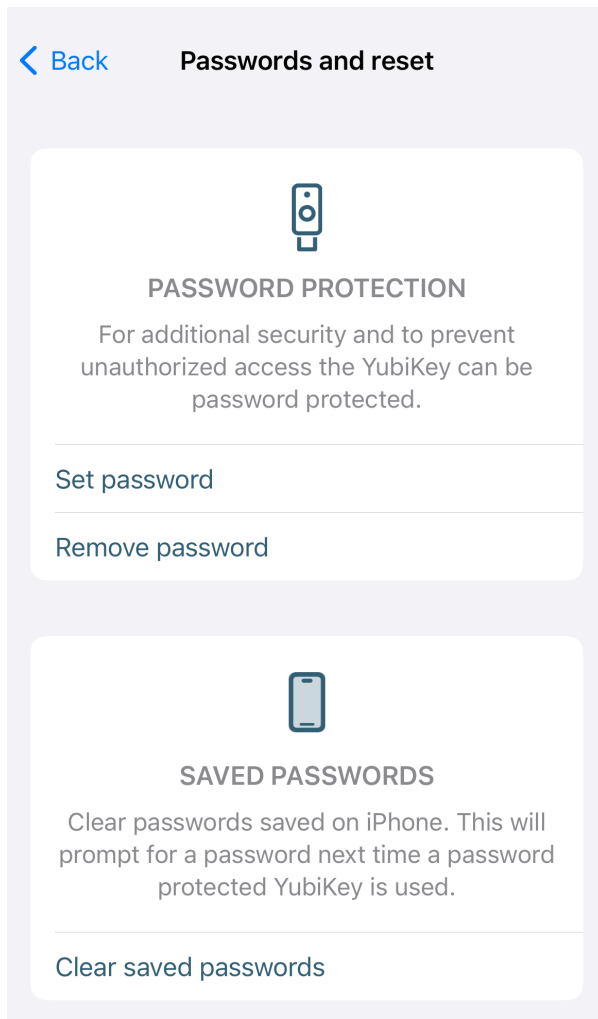


3. To forget a remembered password, click the three dots in the upper right corner of the app and select **Configuration**. Select **Passwords and reset** and then **Clear saved password**. Click **Clear** to confirm the operation. The next time you connect your YubiKey to your device, you will be prompted 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/iPadOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.
2. Click the three dots in the upper right corner of the app and select **Configuration**. Select **Passwords and reset**
3. To remove the password, click **Remove password** and enter your current password when prompted. For NFC connections, tap your key to complete the operation. Once removed, a new password can be set at any time.



4. To change a password, click **Set password** and enter the new password. Enter the new password again to confirm, click **Save**, and provide your current password when prompted. For NFC connections, tap your key to complete the operation.

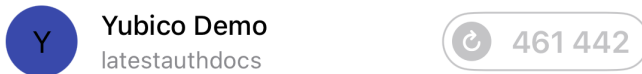
## 6.5 Pinning an account

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. Once several accounts have been registered, not all of them will be visible without scrolling in the app window. 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).



## Pinned

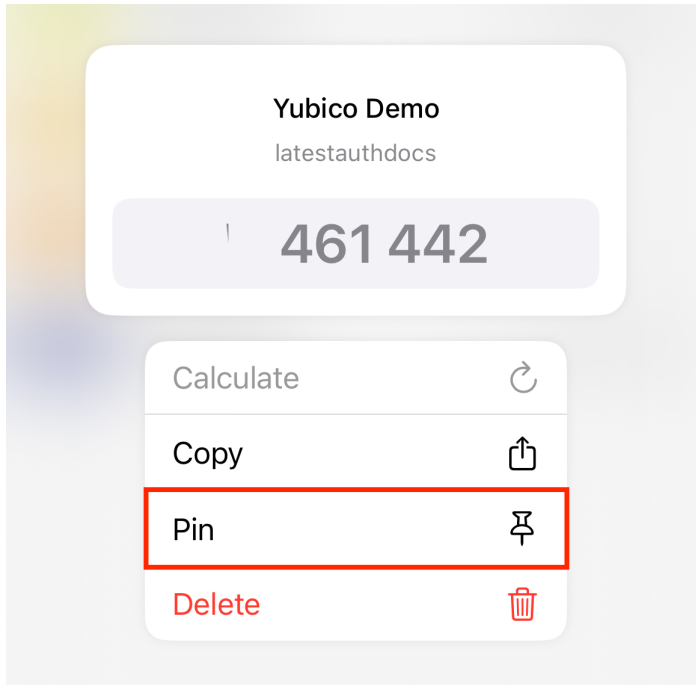


## Other



To pin an account, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app (desktop and Android only), 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/iPadOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.
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/iPadOS, 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 registered with 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, click the menu icon in the upper left corner of the app (desktop and Android only), 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/iPadOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.

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/iPadOS, 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/iPadOS, tap your key to complete the operation.

### 6.7 Deleting an account

OATH accounts can be deleted from your YubiKey. Before deleting an account from a YubiKey, make sure you have either disabled two-factor authentication within your account *or* registered a backup YubiKey with the same account to maintain access.

To delete an account, do the following:

1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app (desktop and Android only), 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/iPadOS, swipe down on the screen and tap your YubiKey on the back of your device to scan.

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/iPadOS, 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/iPadOS, 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.

To make accounts 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.

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 a custom 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 **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.

3. Select **Custom icons** under **Manage**.

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





## PASSKEYS: FIDO2

---

**Important:** The **Passkeys** feature is only available for Yubico Authenticator for Desktop and Android and FIDO2-certified YubiKeys. This includes YubiKey 5 Series (standard, FIPS, and CSPN), YubiKey Bio Series, and Security Key Series.

---

**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.

---

**Note:** YubiKey Bio Series keys require at least one *fingerprint* to be enrolled with the key before passkeys can be stored on the device. Fingerprints can be *enrolled and managed* via Yubico Authenticator.

---

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.*

### 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.

**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

To create a FIDO2 PIN, do the following:

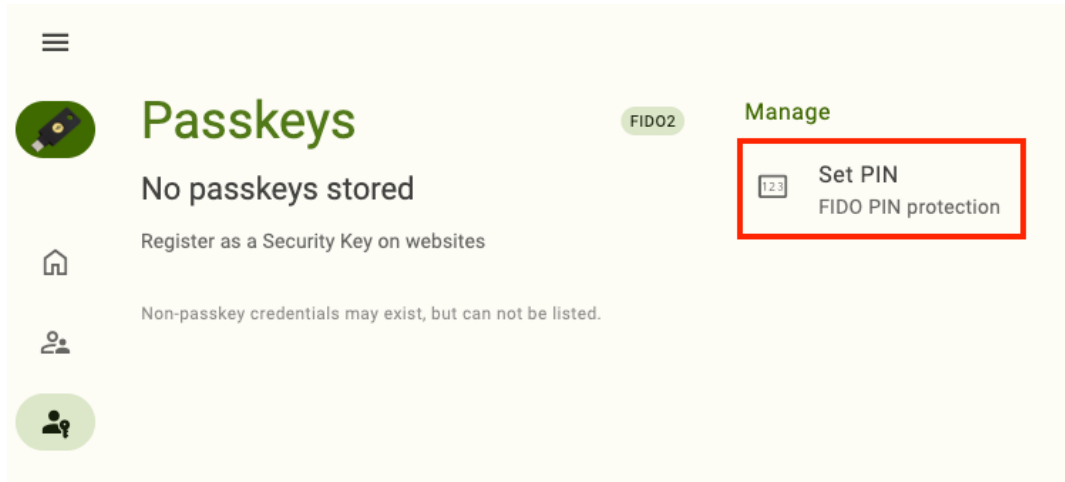
1. Plug your YubiKey into your device, click the menu icon in the upper left corner of the app, and select **Passkeys**.

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.

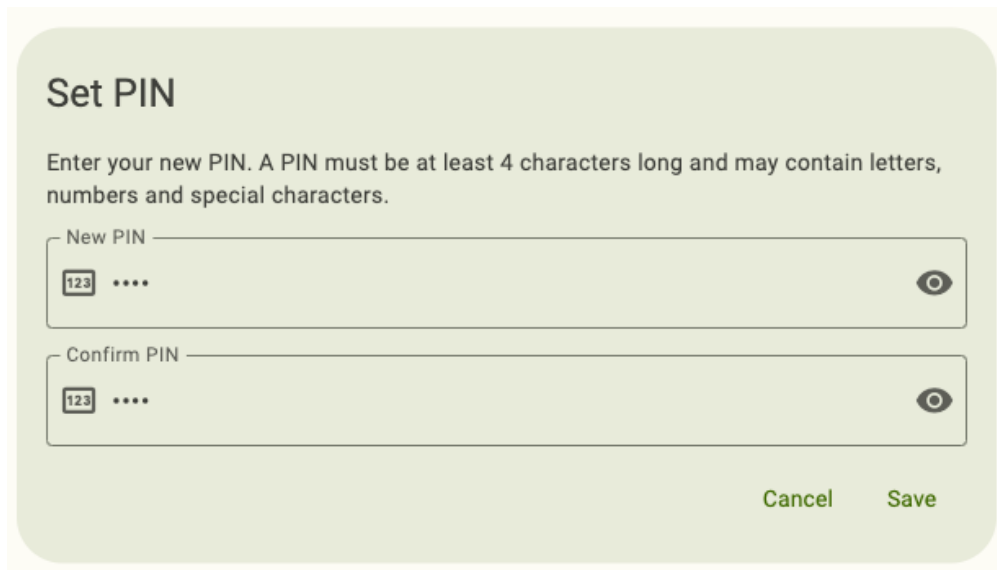
To connect via NFC on Android, tap your YubiKey on the back of your device to scan.

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.



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



## 7.1.2 Changing the FIDO2 PIN

To change the FIDO2 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 **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.
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**

Enter your current PIN. If you don't know your PIN, you'll need to reset the YubiKey.

Current PIN

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

New PIN

Confirm PIN

Cancel Save

## 7.2 Viewing and deleting passkeys

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**.

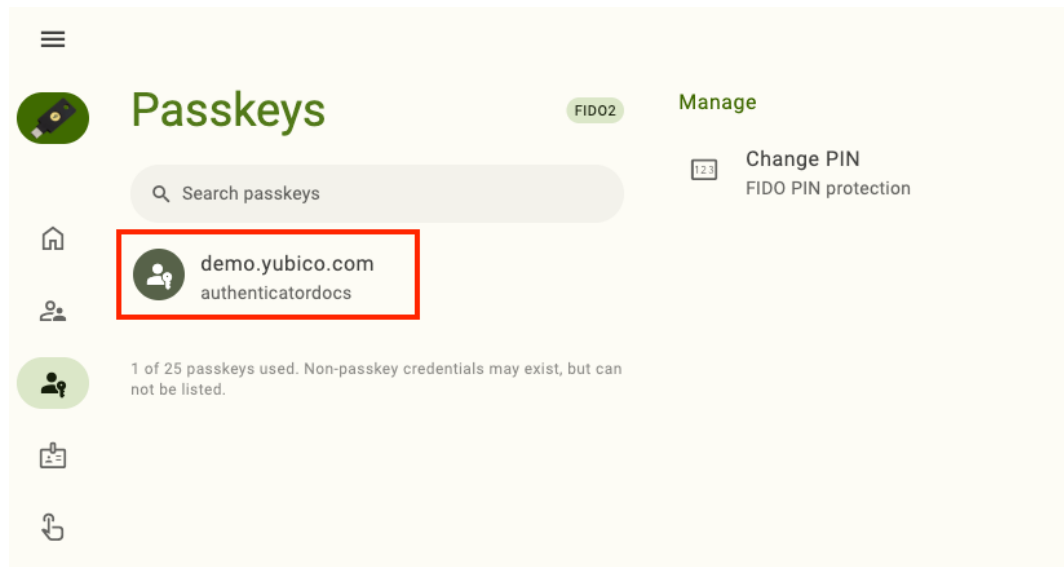
To connect via NFC on desktop, click the NFC icon in Yubico Authenticator and place your YubiKey on top of a desktop NFC reader. The key must maintain constant contact with the reader throughout the operation.

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.

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



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 e15f68a7dd9c6c4f171c23

### Actions



#### Delete passkey

Remove the passkey from the YubiKey

### Manage



#### Change PIN

FIDO PIN protection



## FINGERPRINTS: FIDO2

---

**Important:** The **Fingerprints** feature is only available for Yubico Authenticator for Desktop and Android and the YubiKey Bio Series.

---

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 the key before *passkeys* can be stored on the device.

---

**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* with 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.

**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.

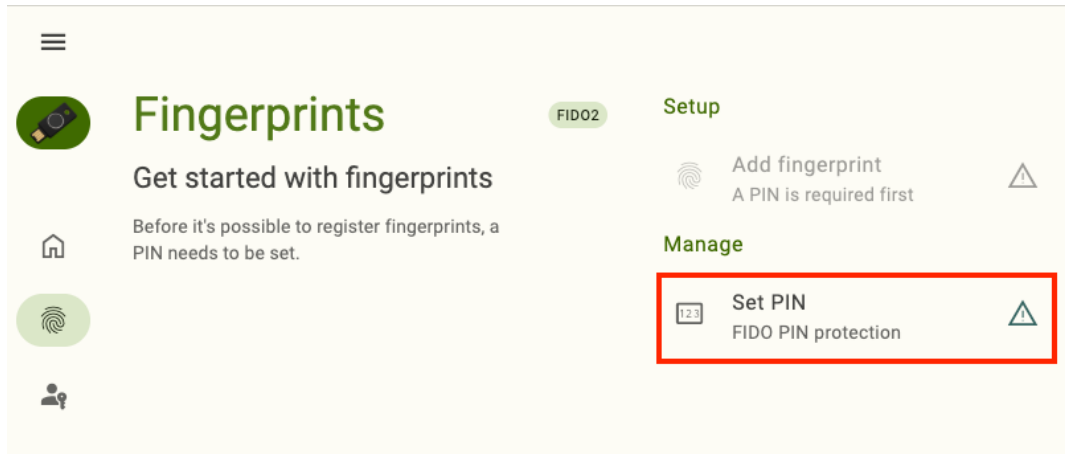
The same FIDO2 PIN is used for *passkeys*; if you have already created a FIDO2 PIN via the **Passkeys** feature, you do not need to create a new one for **Fingerprints**.

### 8.1.1 Creating a FIDO2 PIN

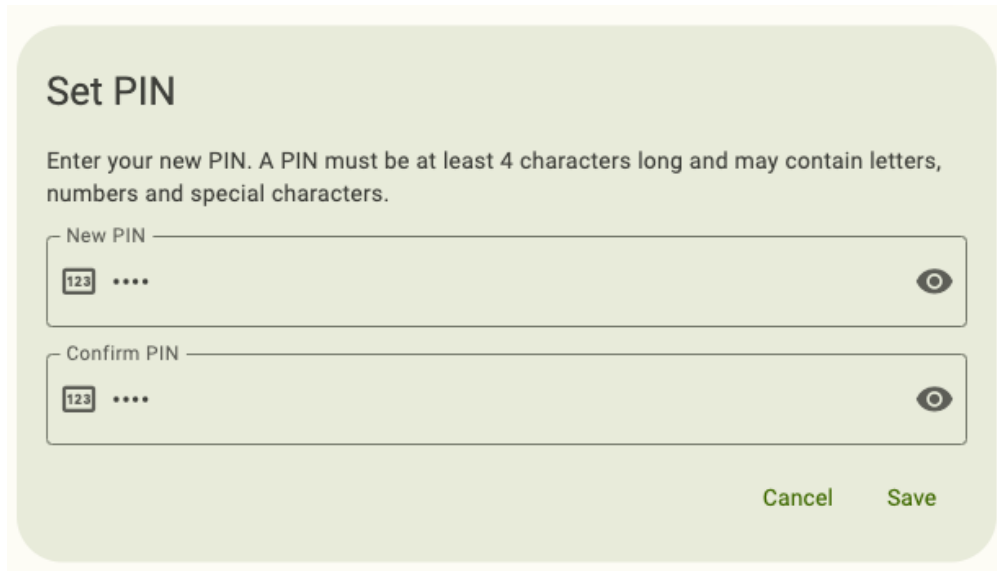
To create a FIDO2 PIN, do the following:

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.



3. In the **Set PIN** window, enter your new PIN. For most keys, it must be at least 4 characters long and may contain letters, numbers, and special characters.
4. Enter the new PIN again to confirm and click **Save**.





## 8.1.2 Changing the FIDO2 PIN

To change the FIDO2 PIN, do the following:

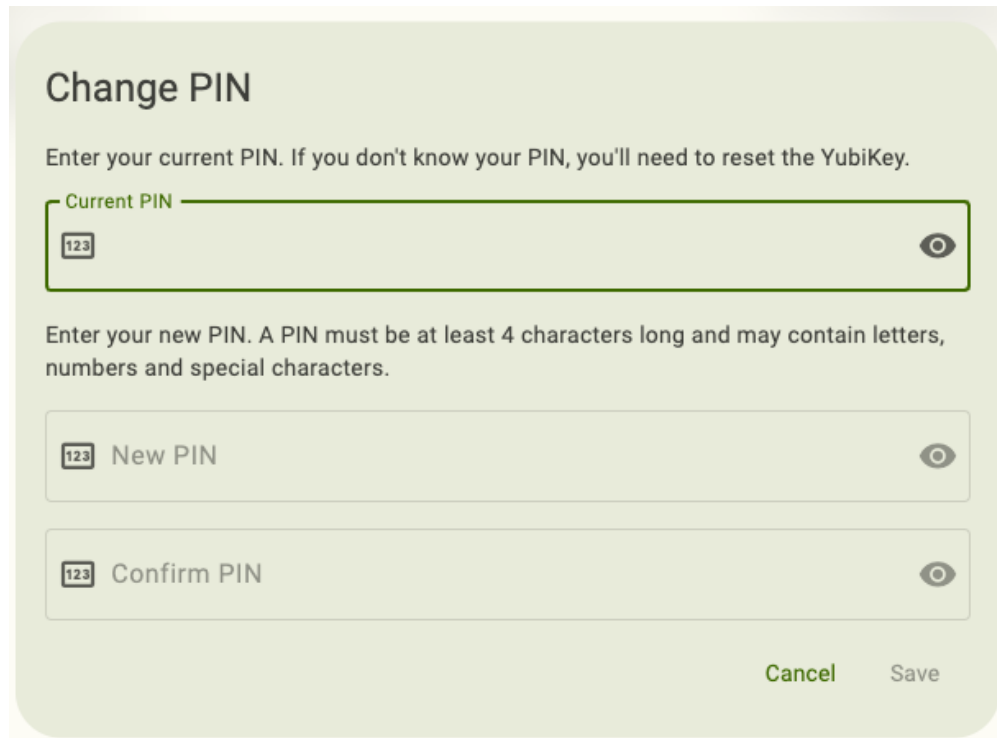
1. Plug your YubiKey Bio into your device, click the menu icon in the upper left corner of the app, and select **Fingerprints**.
2. Click **Change PIN** under **Manage**.

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; for most keys, it must be at least 4 characters long and may contain letters, numbers, and special characters.
5. Enter the new PIN again to confirm and click **Save**.



The screenshot shows a 'Change PIN' dialog box with a light green background. At the top, the title 'Change PIN' is displayed. Below the title, there is a subtitle: 'Enter your current PIN. If you don't know your PIN, you'll need to reset the YubiKey.' The first input field is labeled 'Current PIN' and contains the text '123'. To the right of this field is an eye icon. Below this field, there is a subtitle: 'Enter your new PIN. A PIN must be at least 4 characters long and may contain letters, numbers and special characters.' There are two more input fields: 'New PIN' and 'Confirm PIN', both containing '123'. Each of these fields also has an eye icon to its right. At the bottom right of the dialog, there are two buttons: 'Cancel' and 'Save'.

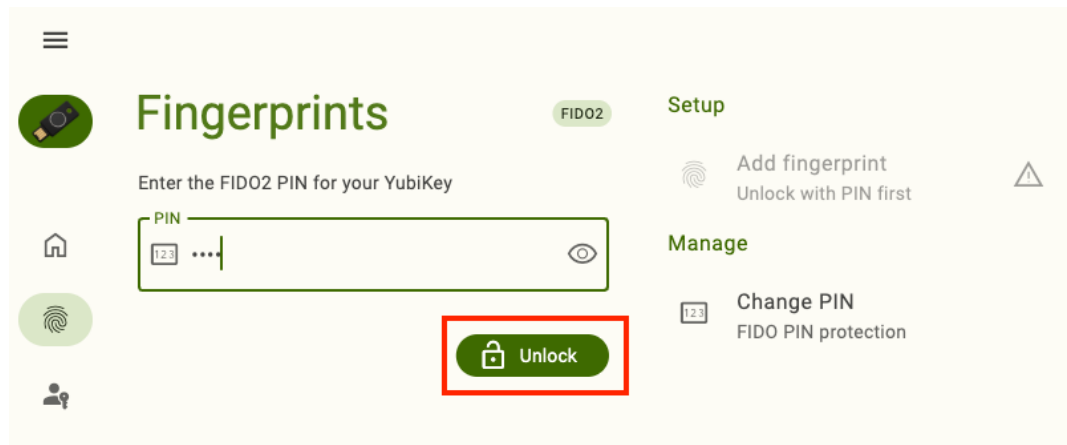
## 8.2 Registering and managing fingerprints

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.

### 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*.

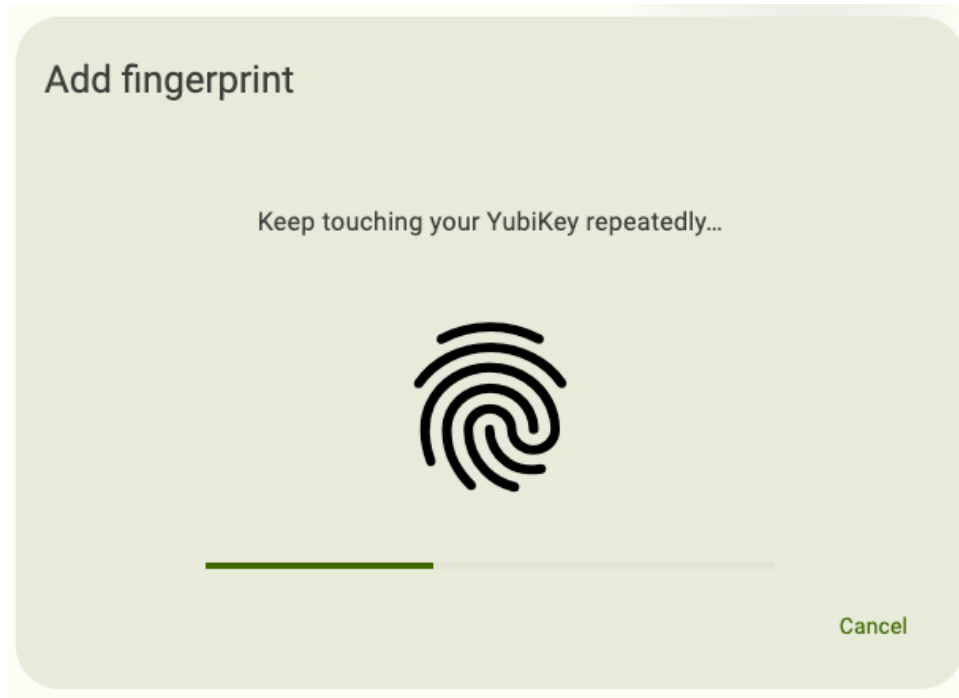


3. Click **Add fingerprint** under **Setup**.

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

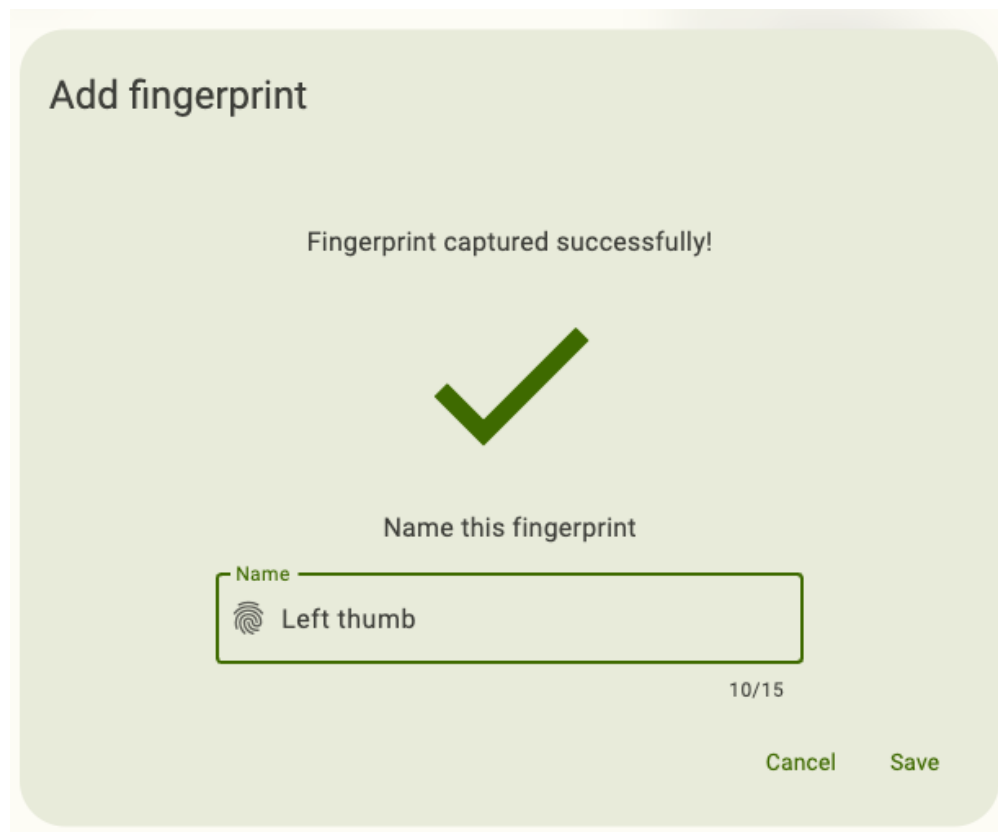
4. In the **Add fingerprint** window, press a finger against the biometric sensor of your key. When the window prompts you to “keep touching your key”, remove your finger and place it back on the sensor. Repeat this until the progress bar reaches 100% completion.

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](#).



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**.

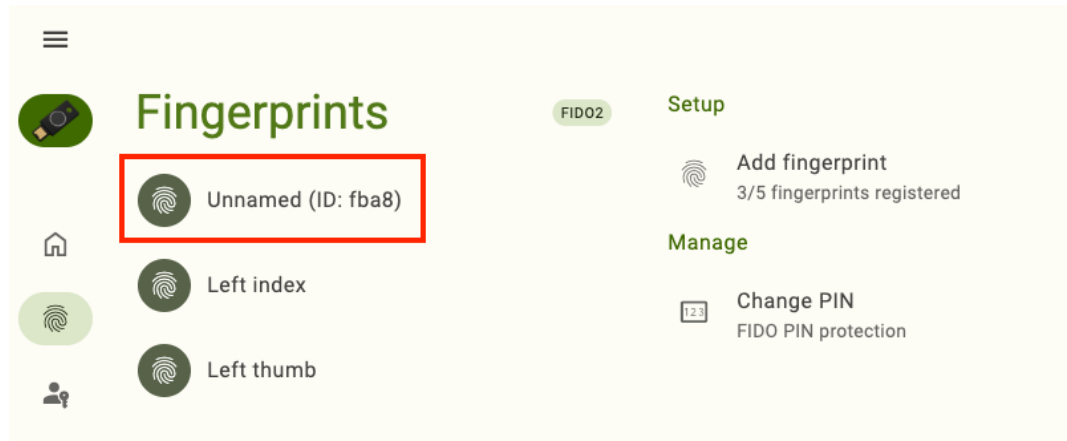
If you click cancel, the fingerprint will still be saved, but it will be given a name of the form **Unnamed (ID: XXXX)**. If you made a mistake, you can always *rename or delete* the fingerprint.



### 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



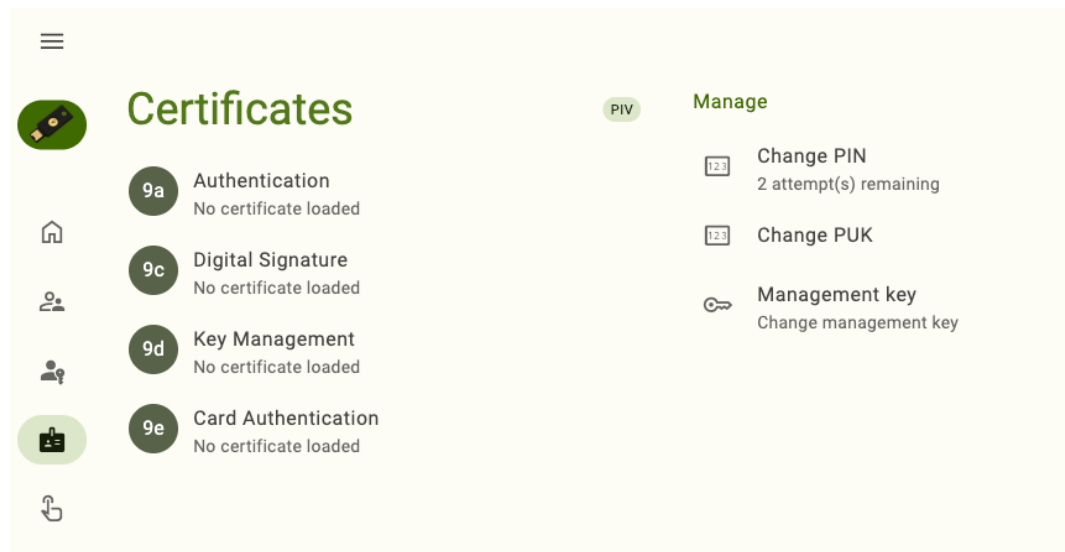
## CERTIFICATES: PIV

### 9.1 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.



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).

## 9.2 Manage the PIN, PUK, and Management Key

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.
4. Enter a new PIN (6-8 characters).
5. Enter the new PIN again to confirm and click **Save**.


**Change PIN**

Enter your current PIN. If you don't know your PIN, you'll need to unblock it with the PUK or reset the YubiKey.

Current PIN   0/8

Enter a new PIN to set. Must be 6-8 characters.

New PIN  0/8

Confirm PIN  0/8

Cancel Save



## 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.

---

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 slot can be configured for one of the following types of authentication:

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

Slot configurations can also be *swapped or deleted*.

---

**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 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 device fields. Yubico OTPs look similar to the following: cccccjlkjlevtdernkbbnrrvhcvdbljgchbgdbvgk.

Yubico OTPs can be used for both single-factor and two-factor authentication. 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](#).

## 10.1.1 Configuration

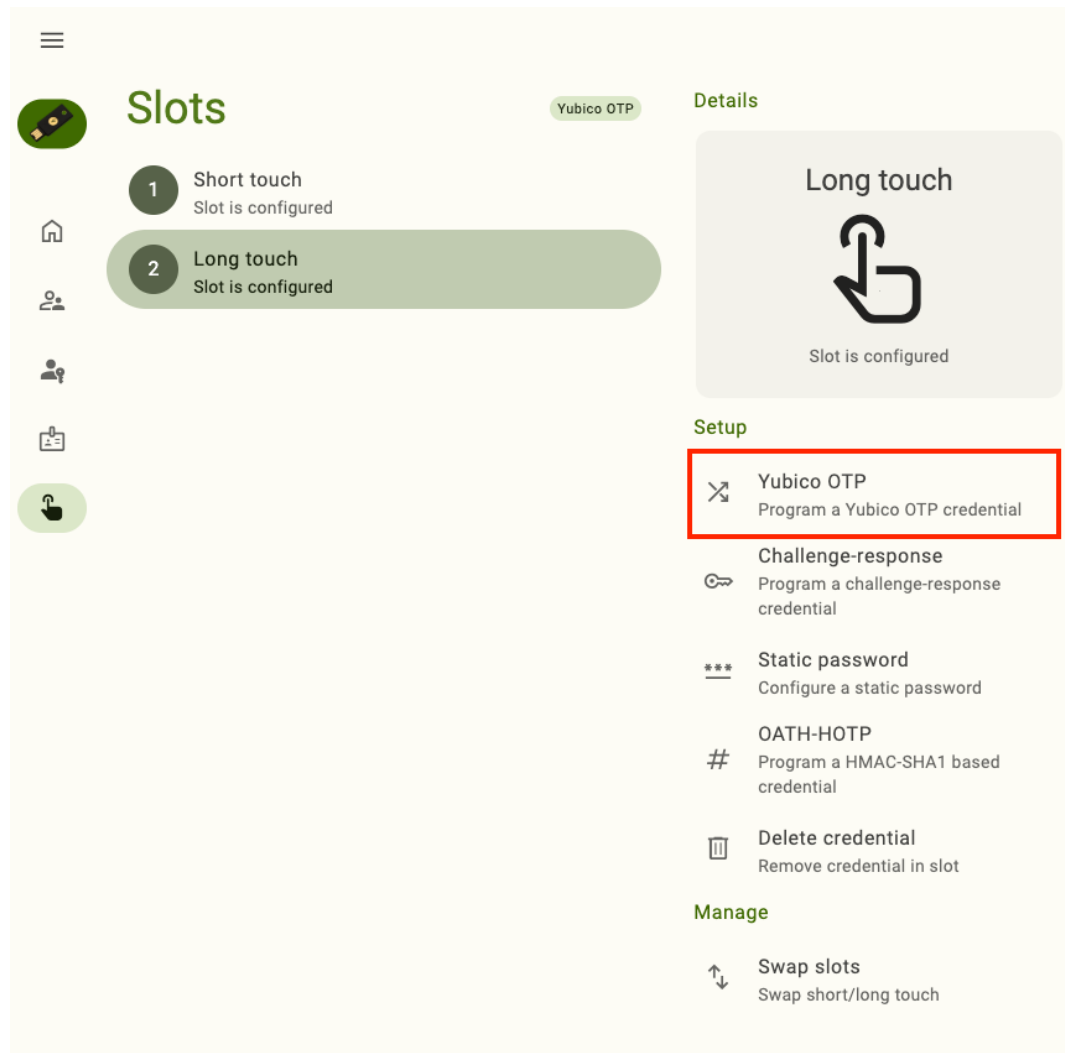
To configure an OTP application slot with a Yubico OTP, do the following:

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 (bcdefghijklnrtv) 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, 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 Enter keystroke, 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.

The screenshot displays the Yubico OTP configuration screen. It features three input fields:
 

- Public ID:** Contains the text 'vvcccctcvhen' and a '12/12' character count indicator.
- Private ID:** Contains the text '87eb04f8cd03' and a '12/12' character count indicator.
- Secret key:** Contains the text '8877f688b88c8ac5e35e320eff73d588' and a '32/32' character count indicator.

 At the bottom, there is a 'Append' button with a checkmark and a left arrow. To its right is a dropdown menu for 'Exported credentials to' with 'No export file' selected. Below the dropdown are 'Select file' and 'No export file' options. At the bottom right are 'Cancel' and 'Save' buttons. A URL 'upload.yubico.com' is visible in the background.

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.

### 10.1.2 Authentication

To generate and submit a Yubico OTP from a configured slot during an authentication attempt, simply place your cursor in the appropriate text field and tap the YubiKey to activate the short press slot or touch and hold the YubiKey for a few seconds to activate the long press slot. The key will generate the Yubico OTP using the slot's credential and type it into the text field.

## 10.2 Static passwords

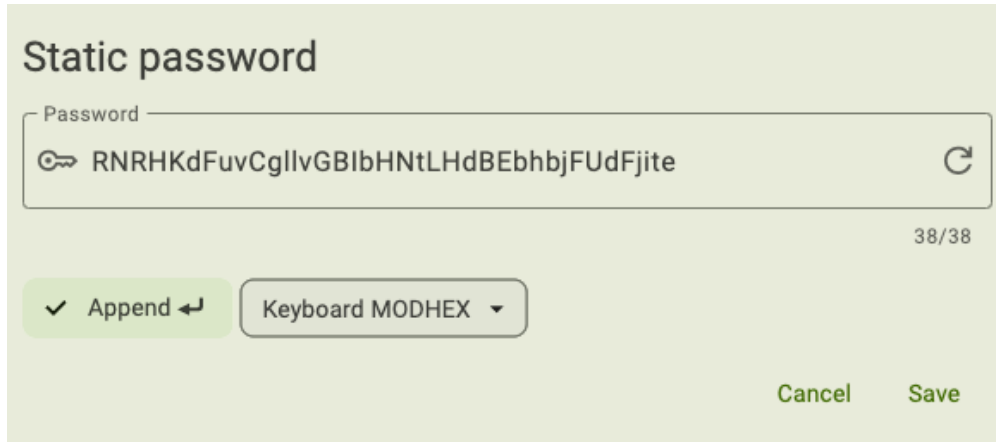
A static password, as the name implies, is a string of characters that never changes. It is no different from a password that you would create for any standard account. The advantage of programming a slot with one is that you can have a long, complicated password for an account that you can store in a secure location and not have to worry about remembering it.

Static passwords can be communicated over physical 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, 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 Enter keystroke, 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: bcd efghijkl nrtuv.
6. Click **Save** to complete the configuration. If the slot is already configured with a credential, click **Overwrite** when prompted.



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.

## 10.2.2 Authentication

To submit a static password from a configured slot, simply place your cursor in a text field and tap the YubiKey to activate the short press slot or touch and hold the YubiKey for a few seconds to activate 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" to your YubiKey. The YubiKey receives the challenge and "responds" by hashing the challenge with a stored secret key and sending the response code back to the host for authentication.

To find a list of sites and services that use challenge-response authentication, see the [Works with YubiKey Catalog](#).

For in-depth information on challenge-response authentication, see the [.NET SDK manual](#).

---

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

---

### 10.3.1 Configuration

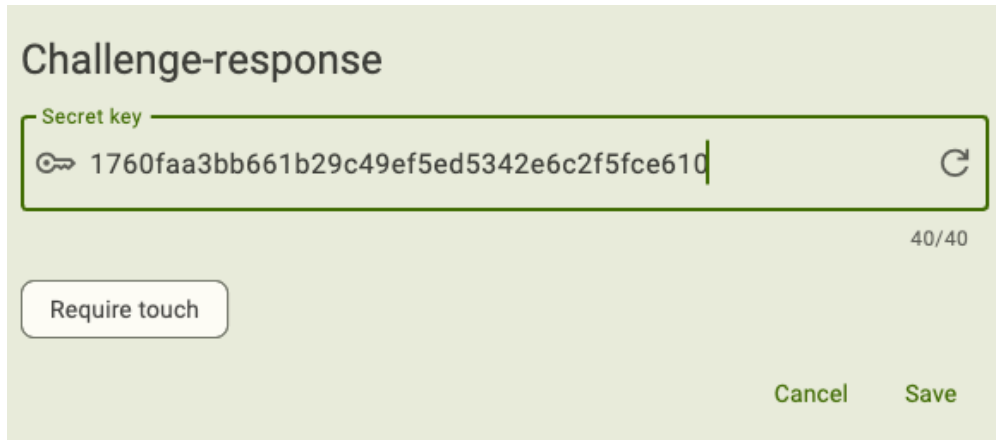
To configure an OTP application slot with a challenge-response credential, do the following:

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 validation server 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.



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.

### 10.3.2 Authentication

Unlike the other slot configuration types, challenge-response is initiated via an API call from the site/service/application you are attempting to authenticate to. This API call sends a challenge to the YubiKey, and 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/service/application for validation.

## 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, and the Authenticator application can display these OTPs.

For in-depth information on OATH HOTPs and how they work within 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, 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 Enter keystroke, 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.

## 10.4.2 Authentication

To generate and submit an OATH HOTP from a configured slot during an authentication attempt, simply place your cursor in the appropriate text field and tap the YubiKey to activate the short press slot or touch and hold the YubiKey for a few seconds to activate the long press slot. The key will generate the HOTP using the slot's credential and type it into the text field.

## 10.5 Managing slots

There are only two options for managing Yubico OTP application slots: the slot configurations can be swapped or deleted.

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.

### 10.5.1 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.



## 10.5.2 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.



## 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. If one application is reset, the others are not affected.

### 11.1 What happens during a reset?

When the FIDO2 application is reset, 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.

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

### 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.

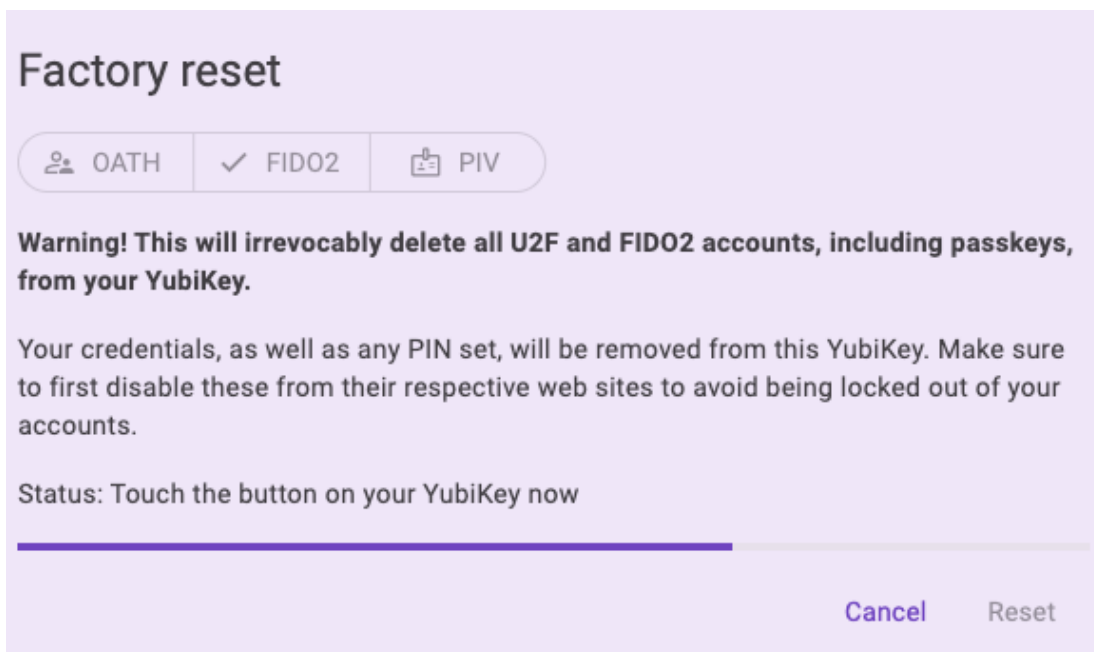
For passkey and OATH credentials, you can view a list of registered accounts in Yubico Authenticator by going to the **Passkey** and **Accounts** screens, respectively.

## 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**.
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**.



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**.

---

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

---

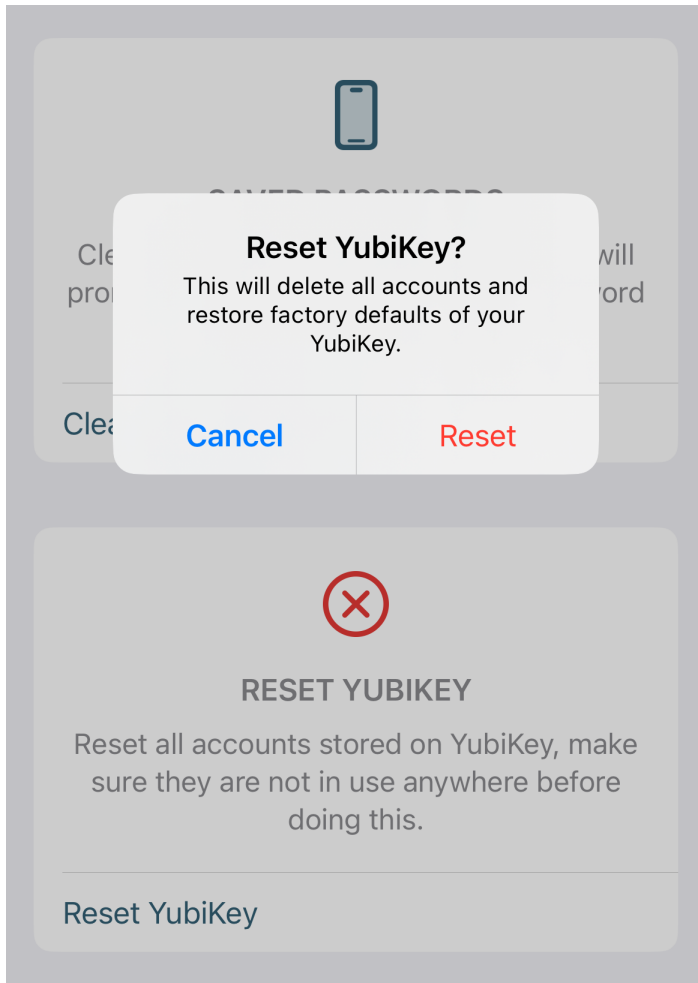
## 11.5 Performing a reset on iOS/iPadOS

For Yubico Authenticator for iOS/iPadOS, only the OATH application can be reset. To perform a reset for this application on your iOS/iPadOS device, do the following:

1. Open the Yubico Authenticator app. For Lightning 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.
2. Click the three dots in the upper right corner of the app and select **Configuration**.
3. On the **Configuration** screen, select **Passwords and reset**.
4. At the bottom of the screen, click **Reset YubiKey**. In the **Reset YubiKey?** window, click **Reset** again to confirm.

For NFC connections, scan your key when prompted.

For Lightning connections, click **OK** to close the window once the operation is complete.



---

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

---

## 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.*
- *Check out the Works with YubiKey Catalog for compatibility information (by YubiKey model, security protocol, and site/service/account) and account setup information.*

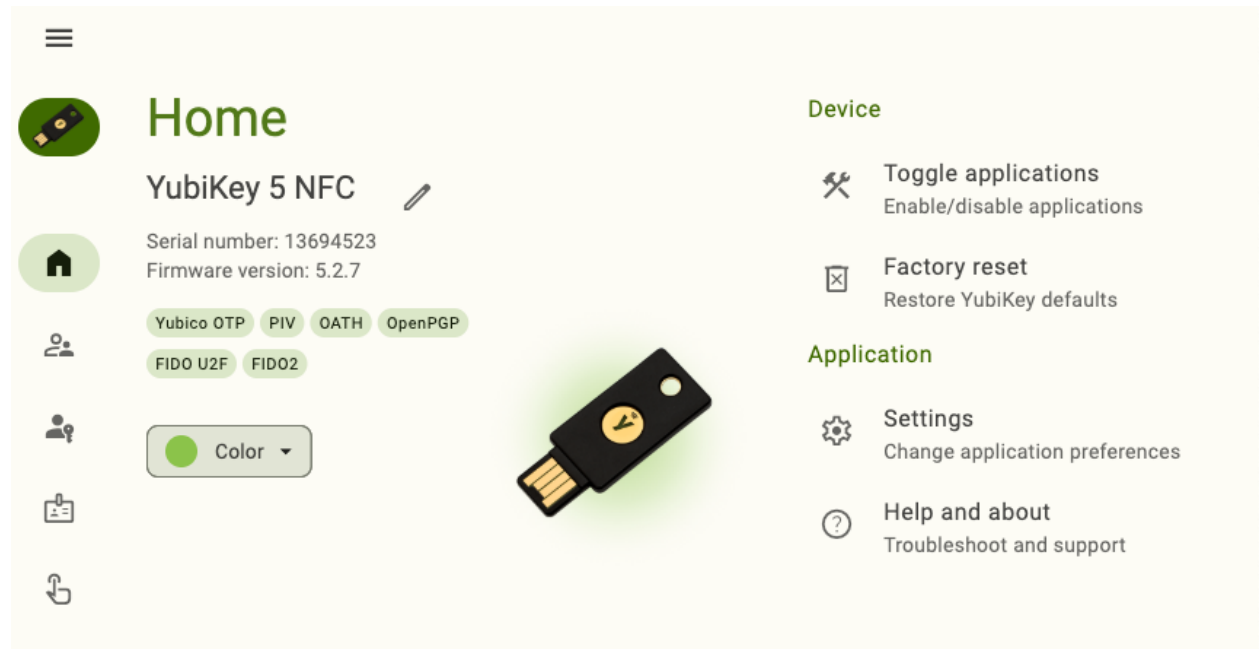
### 12.1 Resizing the app window

---

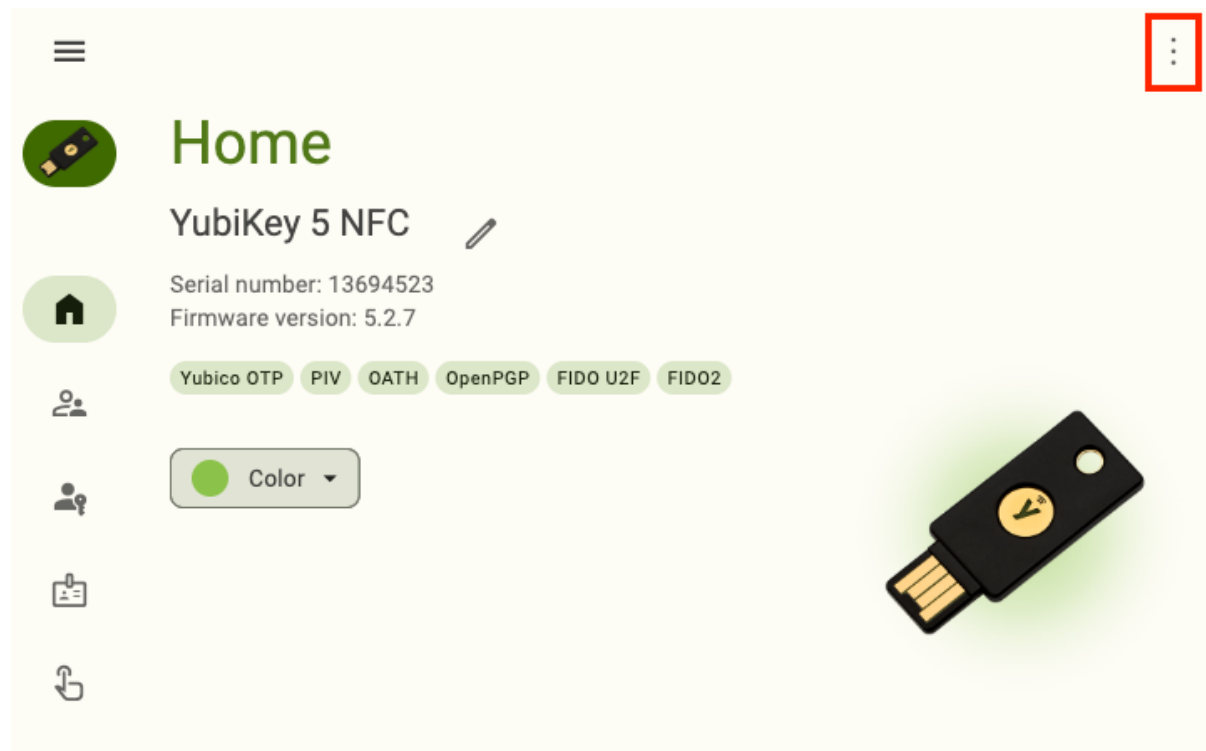
**Note:** The app window size can only be changed on desktop and Android tablet devices.

---

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

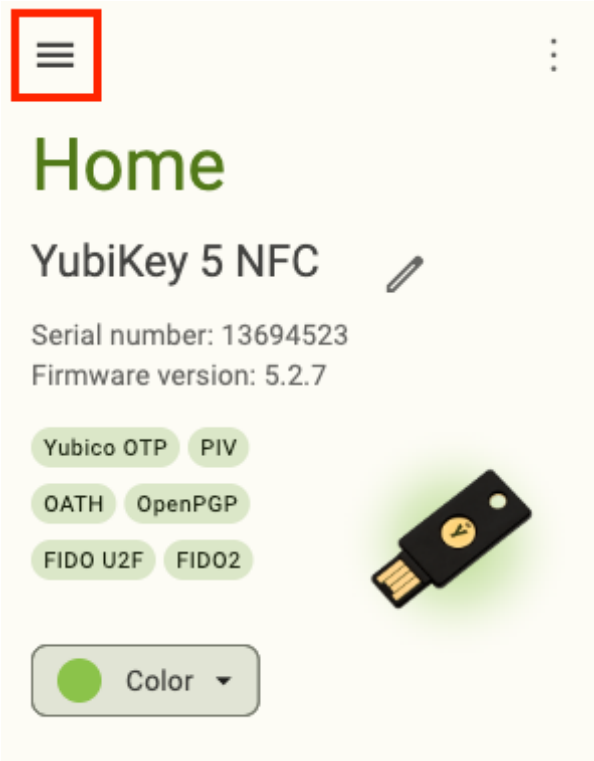


When the window is narrowed sufficiently, the righthand menu becomes hidden. However, these menu options can still be accessed by clicking the three dots in the upper right corner of the app:

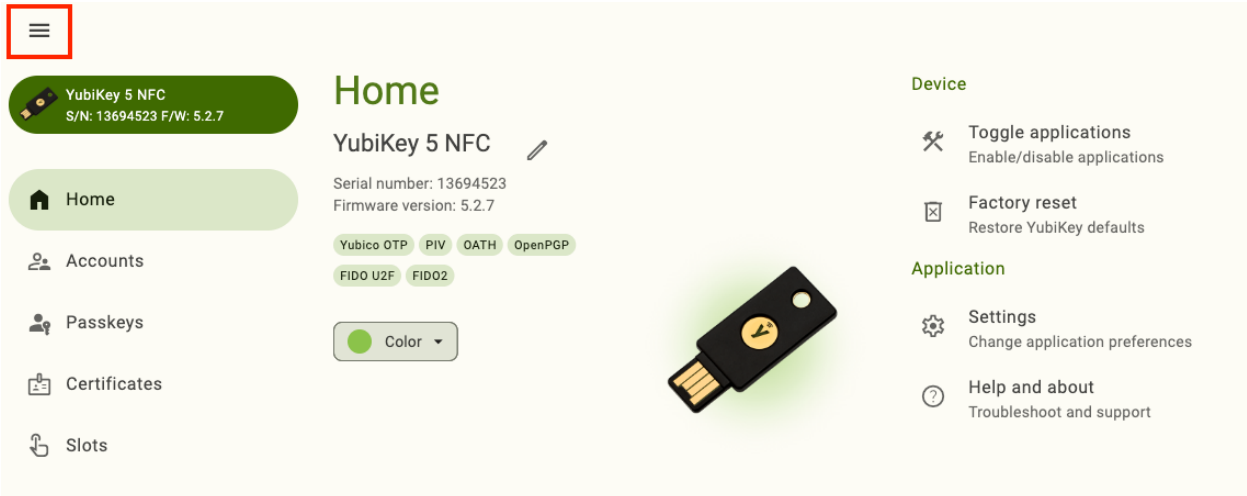


Further narrowing the width makes all page icons disappear. However, these pages can still be accessed by clicking the three lines in the upper left corner:





When the window is widened sufficiently, the page names are expanded. To collapse these names again, click the three lines in the upper left corner:



## 12.2 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.

### 12.2.1 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.

### 12.2.2 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.

### 12.2.3 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 activate 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 activate 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 activate 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.

## 12.3 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
```

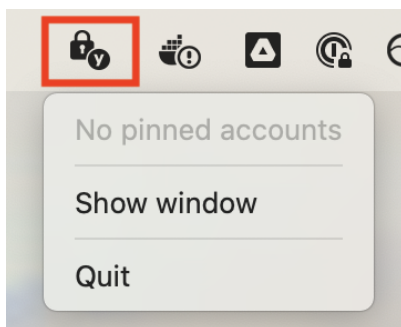
#### Windows:

```
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**.



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

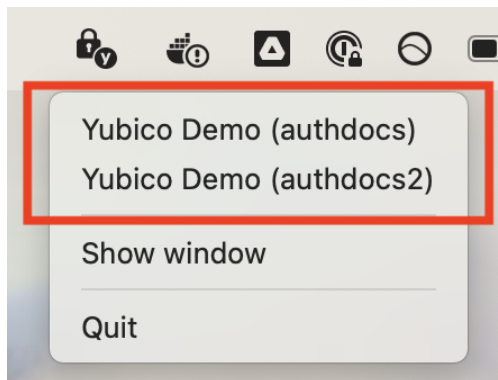
---

**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`.

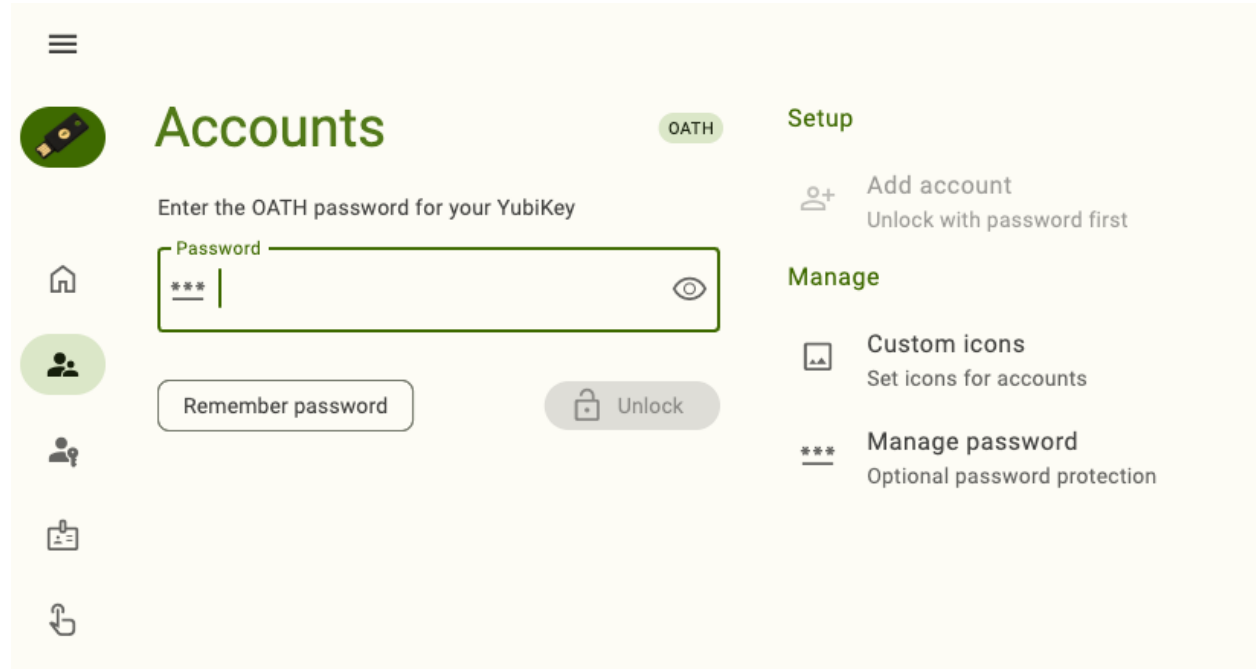
**Only use a trusted binary.** OTPs will be sent to it when copied to the clipboard from the system tray.

---

## 12.5 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.



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

## 12.6 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

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 →](#)





## 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 OATH accounts

#### 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

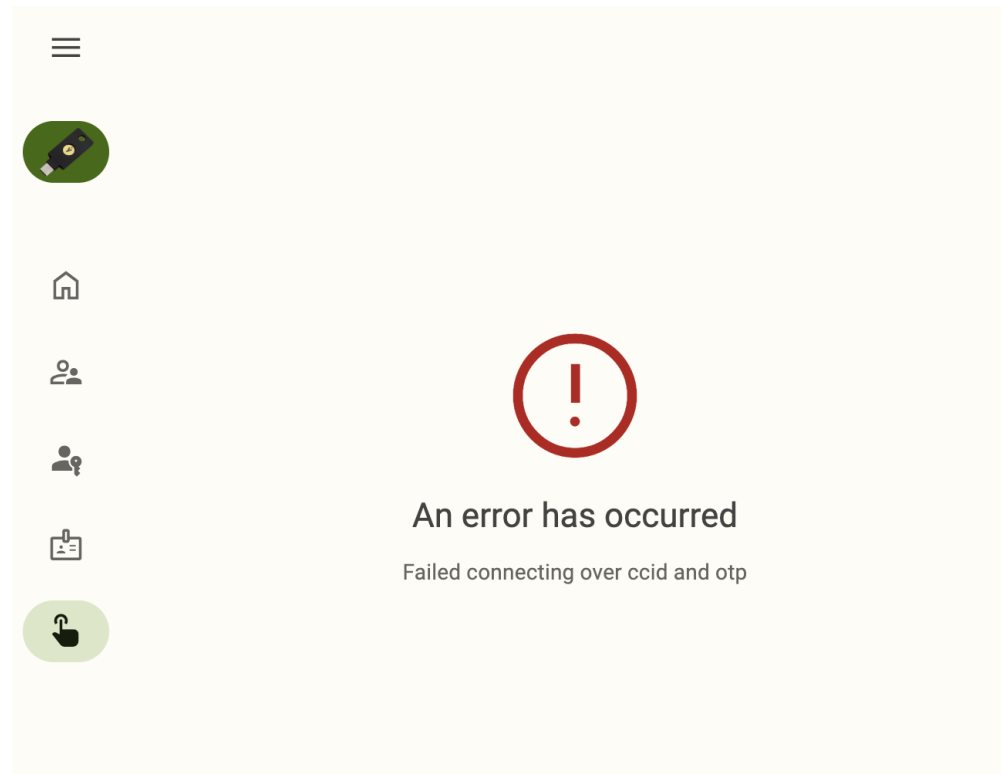
If an OATH account's TOTP codes are getting rejected as invalid during an authentication attempt and they have not expired at the time of submission, the clock on your device may be out of sync with the relying party (your account/service provider).

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](#).

### 13.2 Yubico OTP Slots

#### 13.2.1 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:



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.

## 13.3 Android

### 13.3.1 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**.

## 13.4 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.

## 13.5 Getting additional help

Can't find a solution to your issue? [Submit a help request](#) to Yubico's Customer Support team.

## 13.6 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.

### 13.6.1 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.

### 13.6.2 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.



### 13.6.3 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`.



## 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

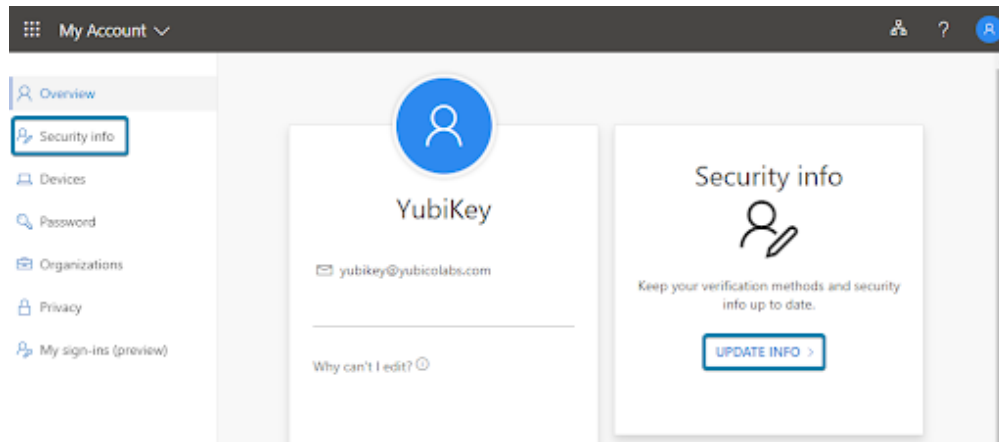
- Your user account must be in Azure Active Directory (AD)
- Have a compatible YubiKey.
- Install [Yubico Authenticator](#) on your mobile device and/or workstation. Since the YubiKey does not contain a battery, it cannot track time. Yubico Authenticator is required to generate and display OATH-TOTP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

#### 14.1.2 Register a YubiKey

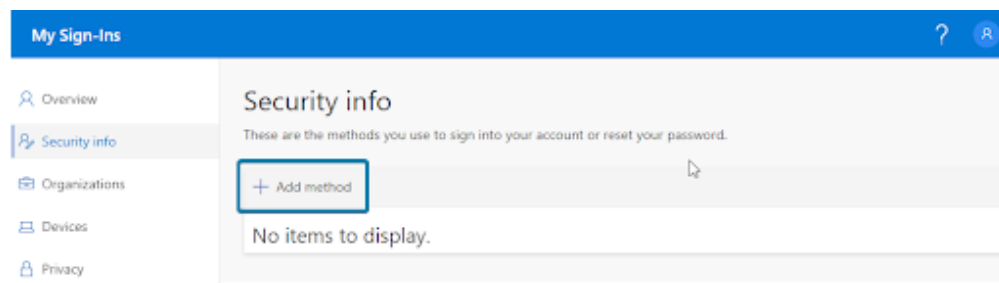
**Step 1:** Open a browser window and navigate to <https://myprofile.microsoft.com>.

**Step 2:** Sign in to your account.

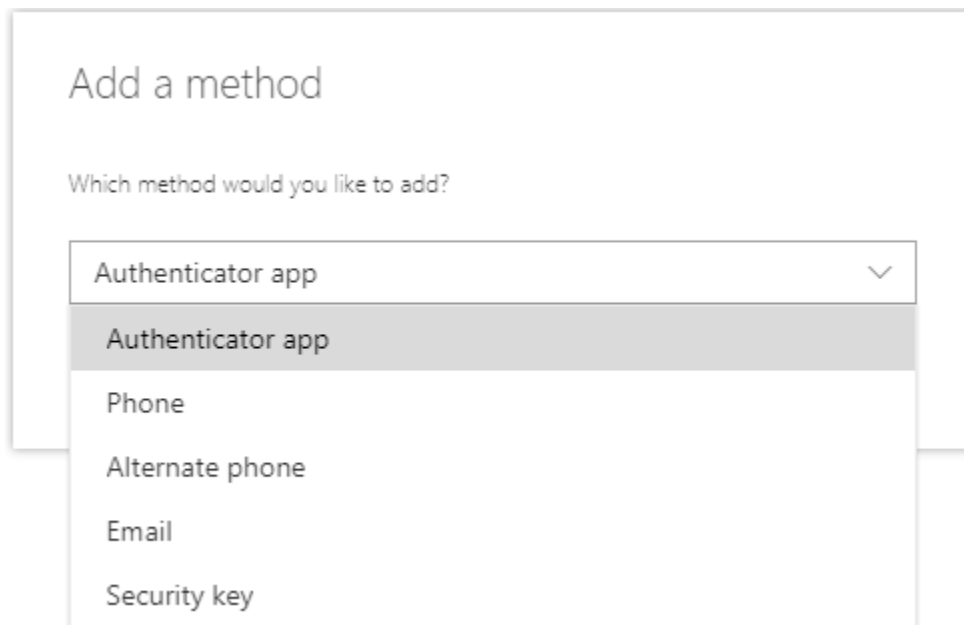
**Step 3:** Select **Security Info** in the left navigation or **Update Info** in the Security Info tile.



**Step 4: Select Add Method.**

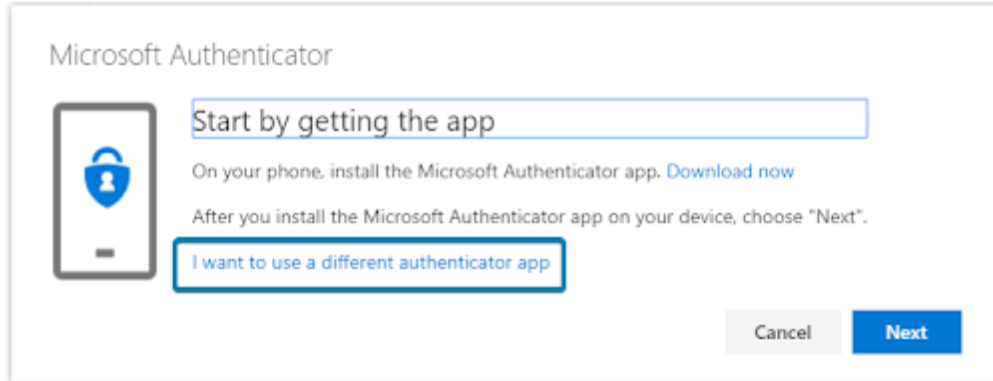


**Step 5: Select Authenticator app.**



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

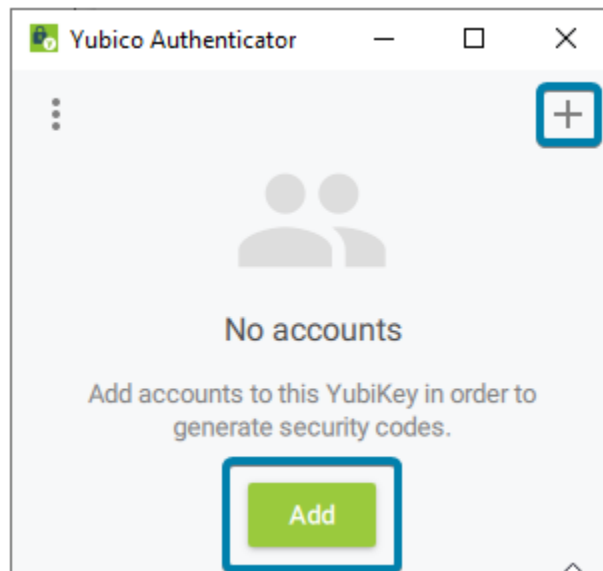




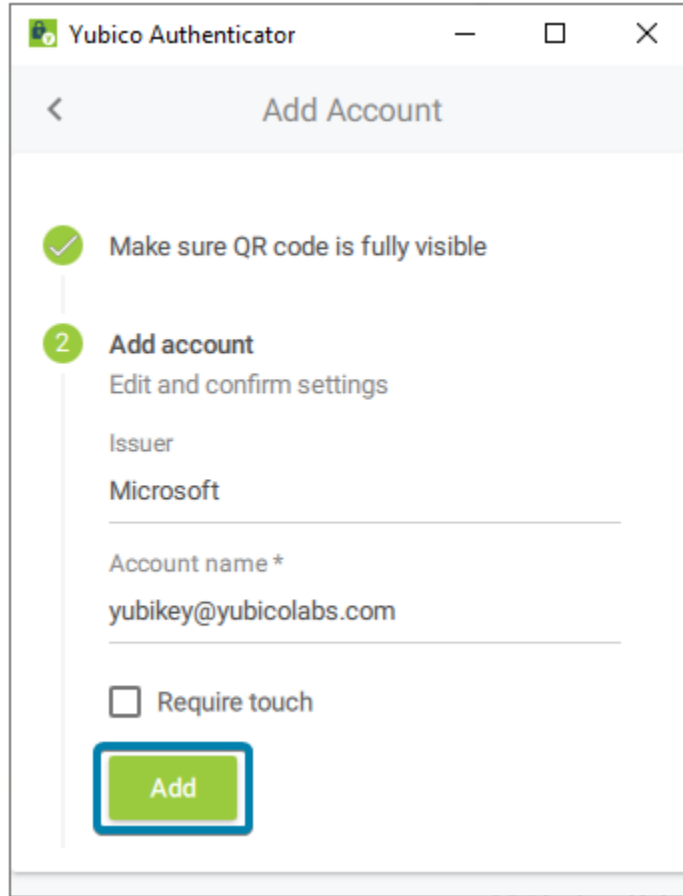
**Step 7:** Select **Next**.

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.



**Step 9:** Select **Add**.

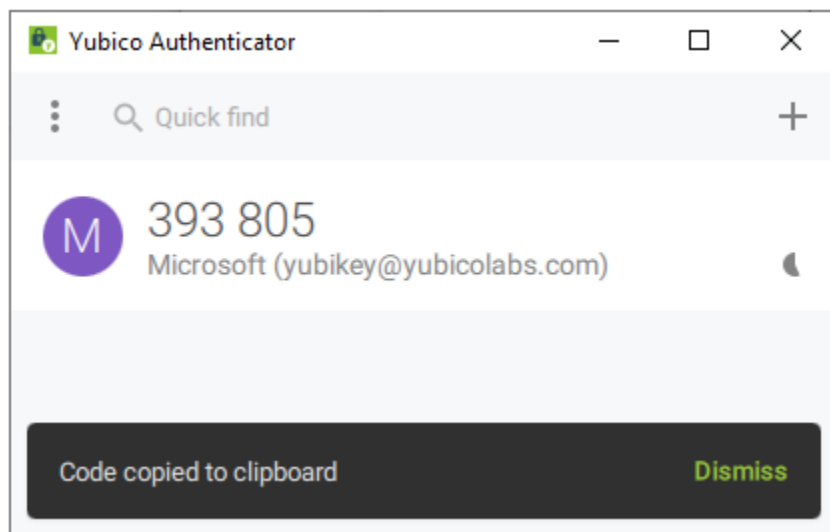


**Step 10:** Double-click the Microsoft entry to copy the code to your clipboard. If successful, the message displays **Code copied to clipboard**.

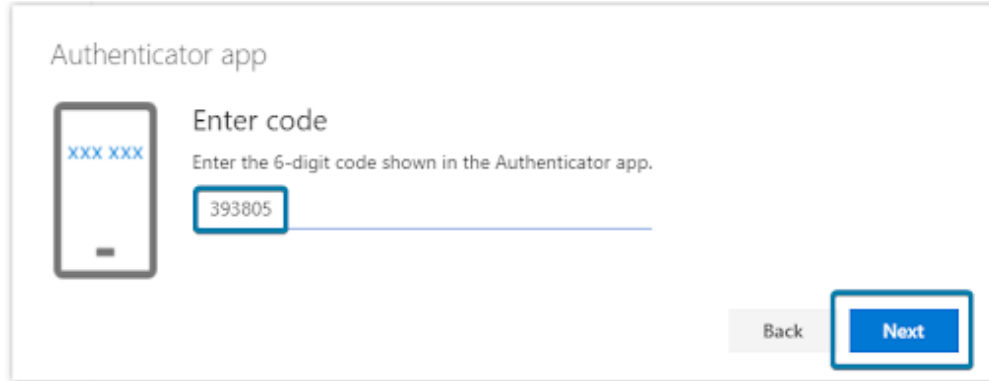
---

**Note:** if you selected Require Touch in the previous step you must touch your YubiKey to copy the code.

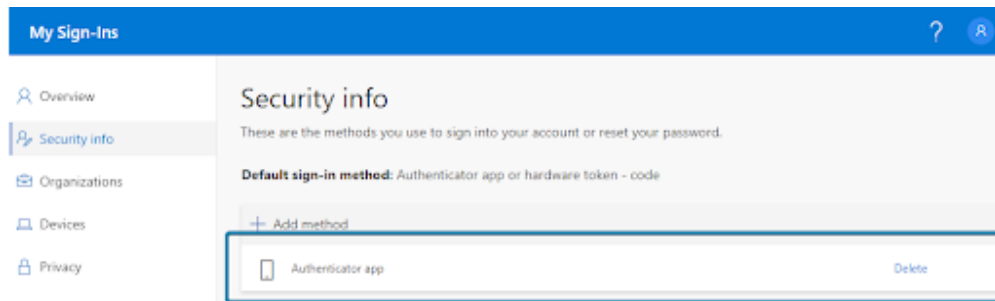
---



**Step 11:** Back in your internet browser window paste the code in the box and click **Next**.



**Step 12:** Select **Done**.



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

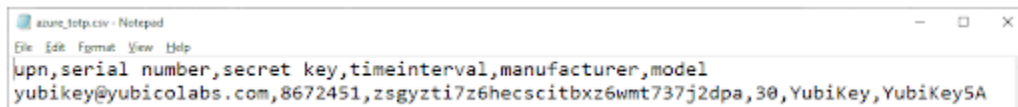
**Step 5:** Use 30 for the time interval.

**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.



```
azure_totp.csv - Notepad
File Edit Format View Help
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).

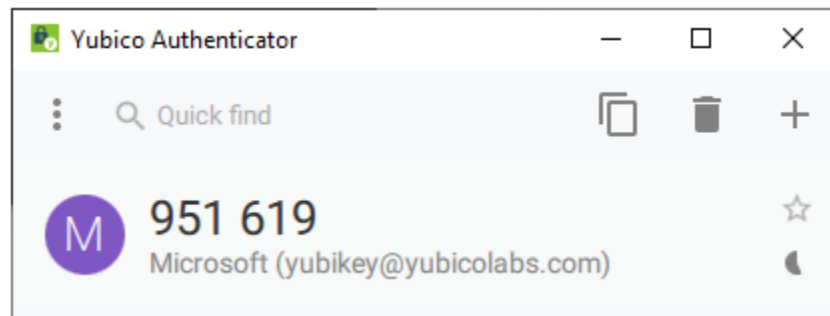
**Step 3:** Run the ykman command to program the YubiKey with the appropriate account name and secret from the CSV file created in the previous section.

```
ykman oath add -i Microsoft <accountname> <secret>
```

For example:

```
ykman oath add -i Microsoft test1@yubicolabs.com
zsgyzt17z6hecscitbzx6wmt737j2dpa
```

**Step 4:** Open Yubico Authenticator to verify the creation of the TOTP token on the YubiKey while the YubiKey is still inserted.



To see all the configuration options, consult the [YubiKey Manager CLI \(ykman\) User Manual](#).

### 14.2.4 Upload TOTP secrets and activate the YubiKey

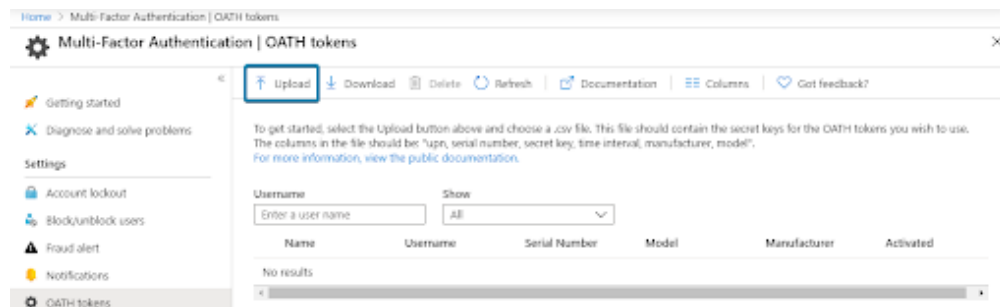
The file generated with the account and secret information needs to be uploaded to Azure AD MFA.

**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.



**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.

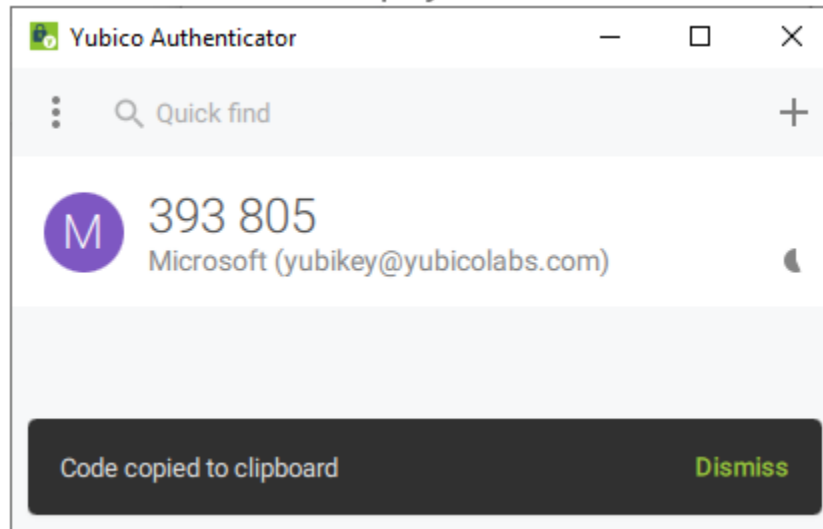
**Step 6:** Select **Activate** for a user.

Name	Username	Serial Number	Model	Manufacturer	Activated
<input type="checkbox"/> YubiKey	yubikey@yubicolabs...	8672451	YubiKey5A	YubiKey	<input type="button" value="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.



**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
<input type="checkbox"/> YubiKey	yubikey@yubicolabs...	8672451	YubiKey5A	YubiKey	<input checked="" type="checkbox"/>

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

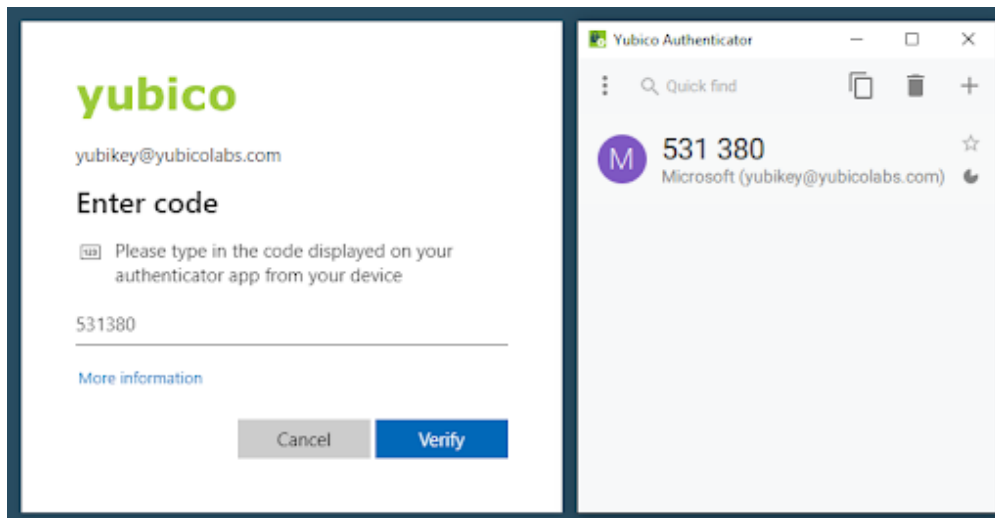
**Step 1:** Open the Yubico Authenticator application.

**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.



**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
<input type="checkbox"/> YubiKey	yubikey@yubicolabs...	8672451	YubiKey5A	YubiKey	<input checked="" type="checkbox"/>

### **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?](#)



## 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.

YubiKey Manager

YubiKey 5Ci [Help](#) [About](#)

**yubico** [Home](#) [Applications](#) [Interfaces](#)

---

## Certificates

[Home](#) / [PIV](#) / [Certificates](#)

[Authentication](#) [Digital Signature](#) [Key Management](#) [Card Authentication](#)

**Authentication (Slot 9a)**

**Issuer:** BadSSL Client Root Certificate Authority

**Subject name:** BadSSL Client Certificate

**Expiration date:** 2021-11-26

[Delete](#) [Export](#)

[Generate](#) [Import](#)

[Back](#)

2. *Provision the public certificate to your iOS Keychain* through the Yubico Authenticator application on your iOS device.



## 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](#).



## 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.

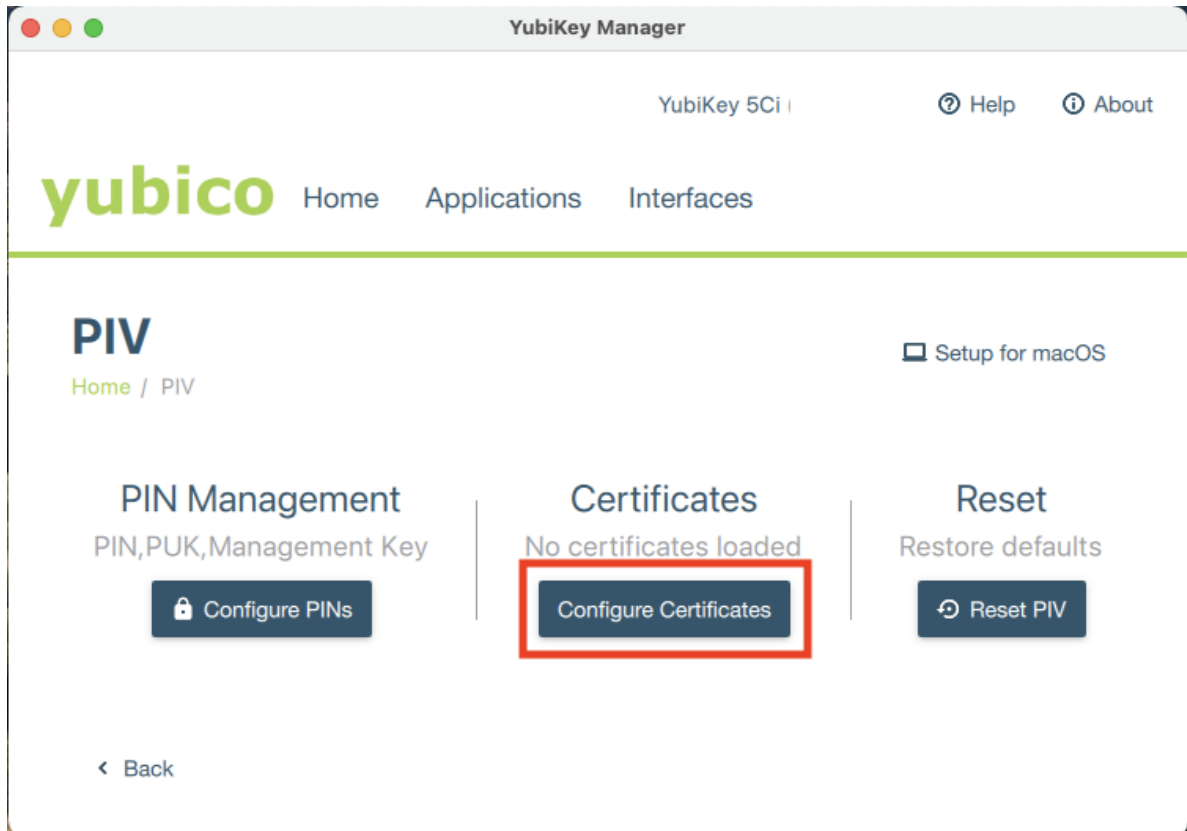
Follow the steps detailed below to import your smart card certificates onto your YubiKey using your preferred version of YubiKey Manager.

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:

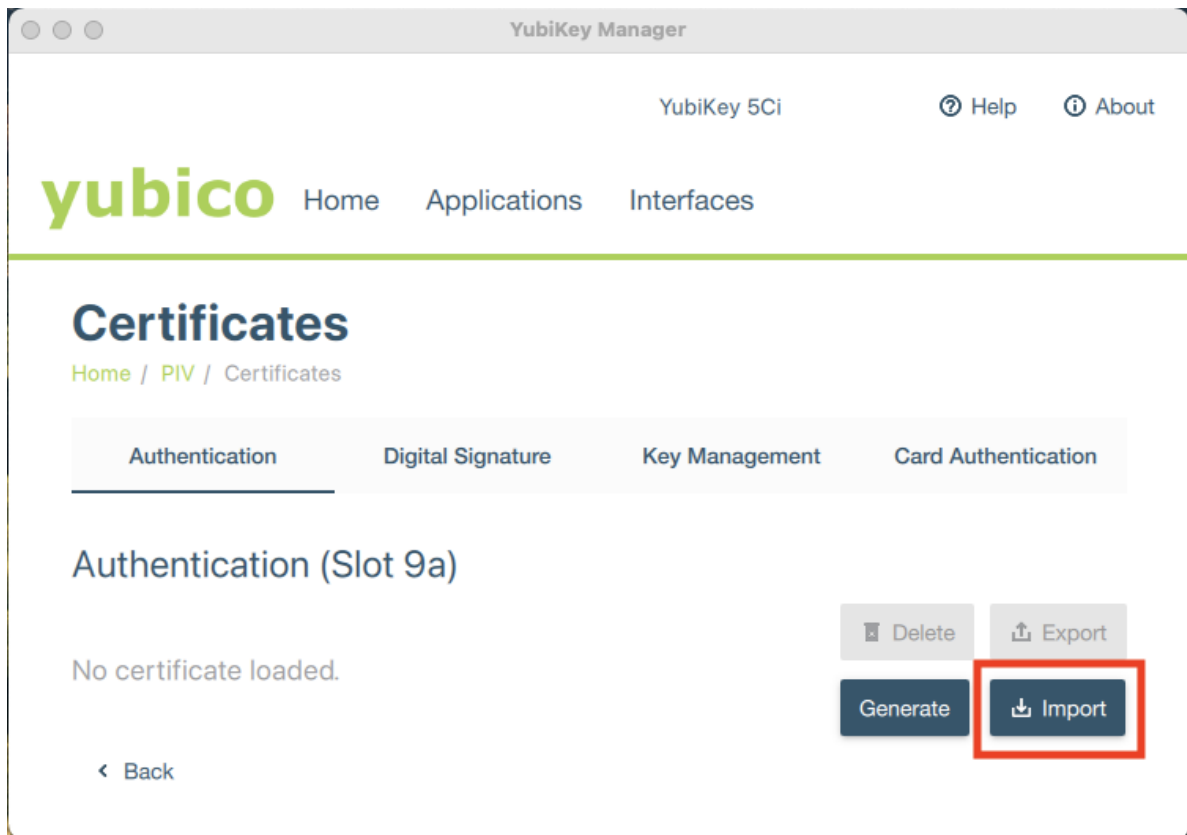
1. If you haven't already, download the appropriate version of the [YubiKey Manager GUI tool](#) onto your host computer. Click on the downloaded file and follow the prompts to complete the installation.
2. Open the YubiKey Manager GUI tool and plug your YubiKey into your computer.
3. On the homepage 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**.





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.

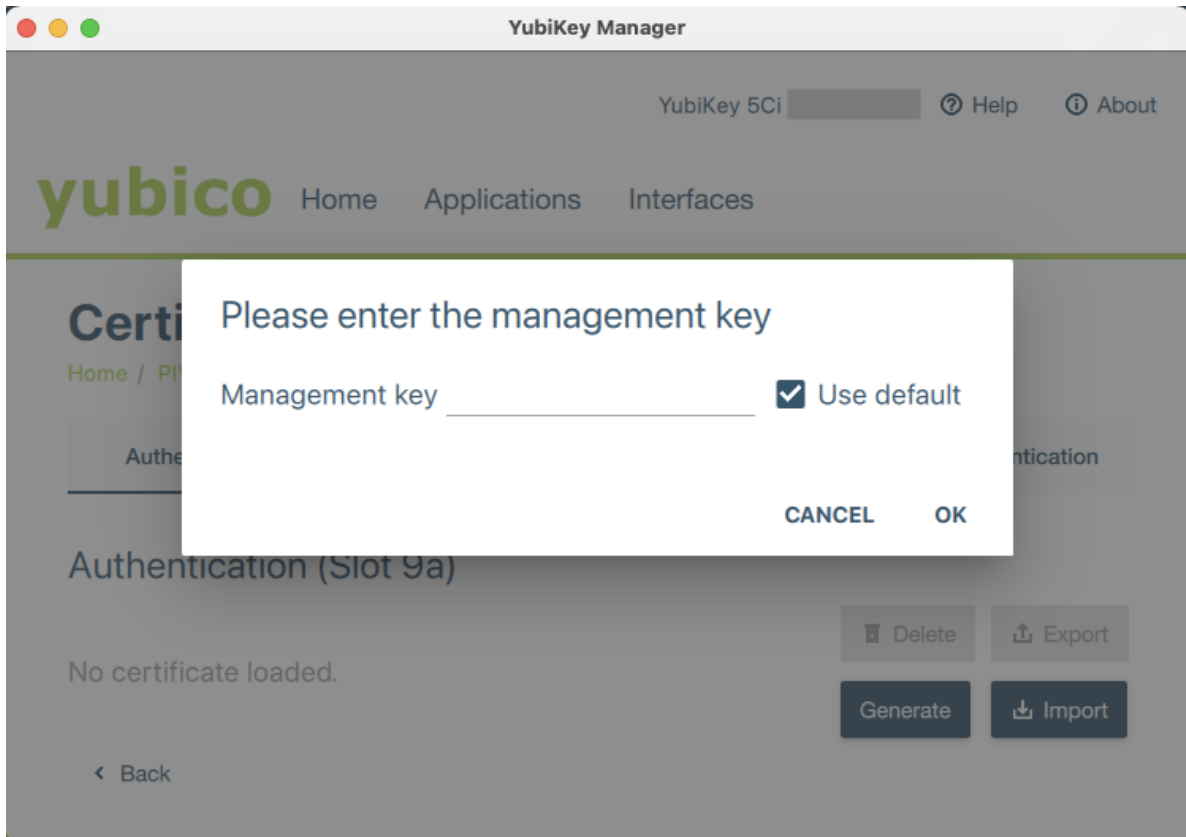
---

8. Next, enter the PIV application management key and click **OK**.

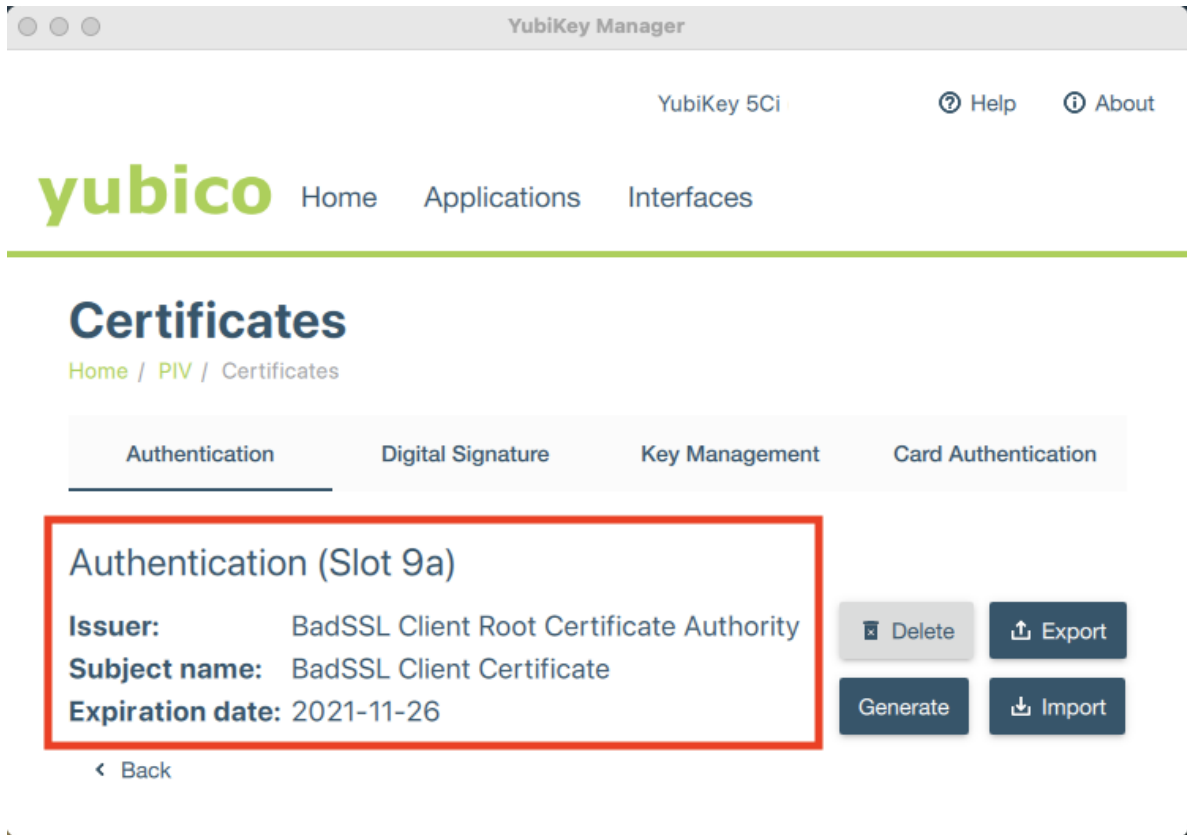
---

**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.

---



9. If the import was successful, the slot will display the issuer, subject name, and expiration date of the imported certificate.



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.

---

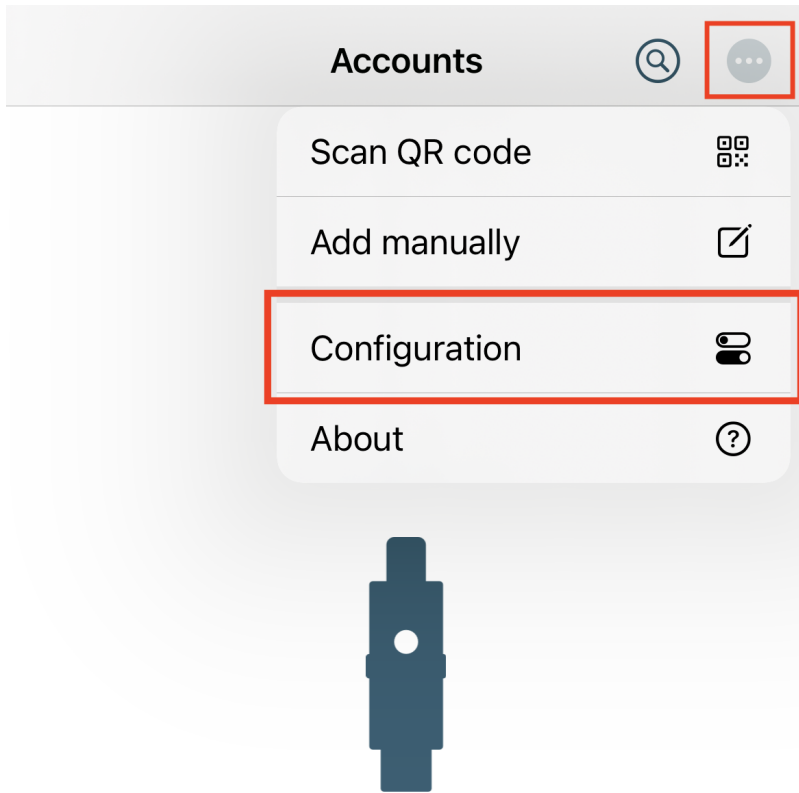
To file a support ticket with Yubico, click [Support](#).

## 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

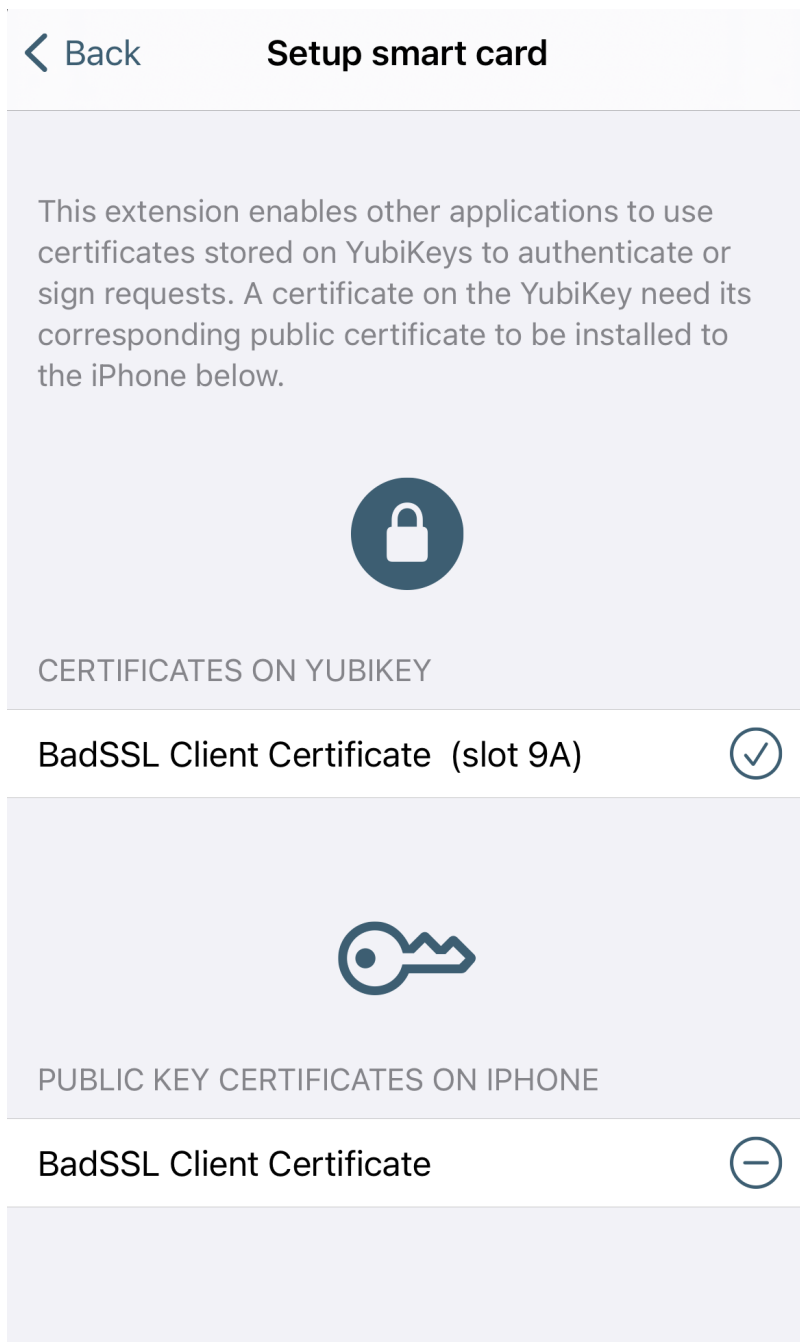
1. If you haven't already, [download and install the Yubico Authenticator application \(v.1.6 or newer\)](#) onto your iOS device.
2. Open Yubico Authenticator.
3. On the home screen of Yubico Authenticator, click on the three dots (...) in the upper right corner of the screen and select **Configuration**.



Insert your YubiKey

Pull down to refresh or activate NFC

4. On the **Configuration** screen, select **Setup smart card (PIV)**.
5. Insert your YubiKey into your device. If you are using a YubiKey with NFC capabilities, scan your key.
6. Once your YubiKey has been detected by the app, all certificates stored on your YubiKey will appear under **CERTIFICATES ON YUBIKEY**. To provision the public certificate from one of your PIV application slots to your iOS Keychain, click the appropriate (+) icon.
7. If the provisioning was successful, the name of your certificate will appear under **PUBLIC KEY CERTIFICATES ON IPHONE**. You may remove certificates from your iOS Keychain at any time by clicking the (-) icon next to the certificate name.



## 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](#).





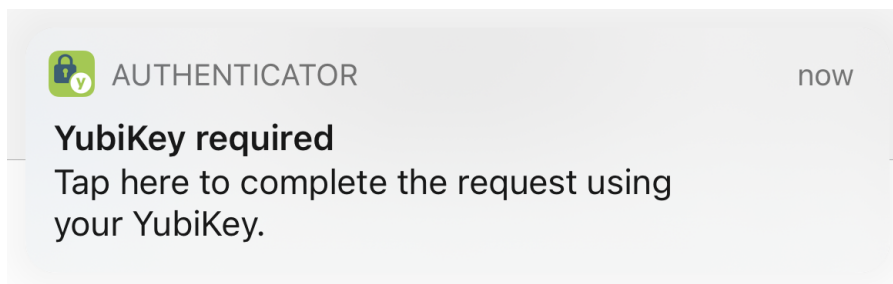
## AUTHENTICATING WITH SMART CARD ON IOS

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.



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.

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](#).



## 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:

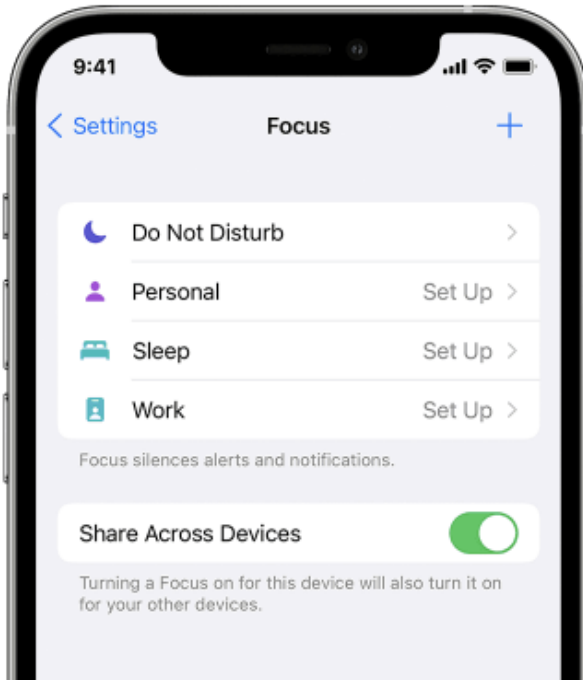
1. Open your [Control Center](#).
2. Select the Focus icon and toggle all modes to the off position.



### 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.



---

To file a support ticket with Yubico, click [Support](#).





## RELEASE NOTES

Updates to the desktop (Windows, Linux, macOS) and Android versions of the Yubico Authenticator app are released together and share a version number. The iOS/iPadOS app is released separately and has its own version number.

### 20.1 Desktop and Android 7.0.0 (6 May 2024)

#### 20.1.1 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 *toggle*d 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.



© 2022-2024 Yubico AB. All rights reserved.

## 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  
Kungsgatan 44  
111 35 Stockholm  
Sweden

---

More options for getting touch with us are available on the [Contact page](#) of Yubico's website.

## 21.4 Document Updated

2024-06-17 17:27:01 UTC