
Yubico Authenticator User Guide

Yubico

Mar 01, 2023

CONTENTS

1	Introduction to Yubico Authenticator App	1
1.1	Yubico Authenticator for Desktop	1
1.2	Yubico Authenticator for Mobile	2
1.3	Managing Keys	2
1.4	Workflow Overview	2
1.5	How it works	2
1.5.1	Hardware-backed Security	3
1.5.2	Easy and fast setup	3
1.5.3	Secure multiple work and personal accounts	3
1.6	The YubiKey Advantage	3
1.6.1	Stronger hardware-backed security	3
1.6.2	Portable credentials across devices	4
1.6.3	Cross-platform coverage	4
1.6.4	Self-service reduces IT costs	4
1.7	Related Yubico Authenticator Links	4
2	Yubico Authenticator Platforms and Requirements	5
2.1	Supported Devices	5
2.2	Yubico Authenticator for Mobile Devices	5
2.3	Yubico Authenticator for Desktop	5
2.3.1	Desktop System Requirements	5
2.4	Online Accounts	6
2.5	GUI and CLI	6
3	Download the Yubico Authenticator App	7
3.1	Download Yubico Authenticator Options	7
3.2	Download and Install the Yubico Authenticator App for Mobile	7
3.3	Download Yubico Authenticator for Desktop	10
4	Install Yubico Authenticator on Desktop	11
4.1	Linux Installation Tips	11
5	Setup Yubico Authenticator Desktop on Windows	13
6	Setup Yubico Authenticator Desktop on macOS	15
7	Setup Yubico Authenticator Mobile on Android	17
7.1	Development	17
7.2	Issues	17
8	Setup Yubico Authenticator Mobile on iOS	19

8.1	Using your YubiKey 5Ci on iOS/iPadOS	20
8.1.1	Adding accounts on iOS/iPadOS	20
8.1.2	Generating codes on iOS/iPadOS	21
8.2	Using your YubiKey 5 NFC, YubiKey NEO	21
8.2.1	Adding accounts on YubiKey 5 NFC, YubiKey NEO	21
8.2.2	Generating codes on YubiKey 5 NFC, YubiKey NEO	22
9	Setup YubiKey with iPads	23
9.1	YubiKeys with iPads with lightning ports	23
9.2	YubiKeys with iPad Pros with USB-C ports	23
10	Use OATH with the YubiKey	25
11	WebAuthn Compatibility	27
11.1	WebAuthn Platform Compatibility	27
11.1.1	Features	27
11.1.2	Windows 10 21H1	27
11.1.3	MacOS 11.4	28
11.1.4	iOS 14	28
11.1.5	iPadOS 15.5	29
11.1.6	Android 11	30
12	Using MFA Authenticator Codes with your YubiKey on Desktops	31
12.1	Setup Your YubiKey with Yubico Authenticator for Desktop	31
12.1.1	Requirements	31
12.1.2	Instructions	31
13	Using MFA Authenticator Codes with your Yubikey on Mobile Devices	33
13.1	Setup Your NFC-enabled YubiKey with Yubico Authenticator for Android App	33
13.1.1	Requirements	33
13.1.2	Instructions	33
13.2	Setup Your YubiKey with Yubico Authenticator for iOS App	34
13.2.1	Requirements	34
13.2.2	Instructions	35
14	Using YubiKeys with Azure MFA OATH-TOTP	37
14.1	Objectives	37
14.2	Self registration (recommended method)	37
14.2.1	Before you begin	37
14.2.2	Register a YubiKey	38
14.3	Administrator registration (alternative method)	41
14.3.1	Before you begin	41
14.3.2	Generate TOTP secrets	42
14.3.3	Program a YubiKey with a generated secret	43
14.3.4	Upload TOTP secrets and activate the YubiKey	43
14.4	Use a YubiKey to sign in	45
14.4.1	Before you begin	45
14.4.2	Website sign in	45
14.5	Troubleshooting	45
14.6	References	46
15	Log on to your MFA Account with Yubico Authenticator	47
15.1	Logging on to Your Account, Service, or Website	47
16	OATH Functionality with Authenticator on Desktops	49

16.1	Protect the YubiKey’s OATH Application	49
16.2	Resetting the OATH Applet on a YubiKey	49
16.3	Steps to Reset OATH Applet	49
17	Short Cut to Authenticator Functionality	51
17.1	Integrating Authenticator Functionality	51
17.2	Short Cut to Controlling Authenticator	54
17.3	Configuring Favorites	54
17.4	Generating OTP Codes for Favorite Accounts	55
18	Register a Spare YubiKey	57
18.1	Identify your service security protocols	57
18.2	Generate the QR code for the YubiKey	57
18.3	Locate the QR code for your primary YubiKey	57
18.4	Link the primary YubiKey QR code with the spare YubiKey	58
18.5	Create a spare key for this account	58
18.6	Challenge-Response services backup process	58
18.7	Static password function backup process	59
19	Managing YubiKeys	61
19.1	Configuring WebAuthn/FIDO2 Capabilities	62
19.1.1	FIDO2 PIN	63
19.2	PIN Protection	65
19.2.1	Managing the FIDO2 PIN	65
19.2.1.1	Setting the PIN	65
19.2.1.2	Changing the PIN	65
19.3	Sign-in Data	69
19.3.1	Viewing, Labeling, and Deleting Individual Credentials	69
19.4	Fingerprints	69
19.4.1	Managing Fingerprint Templates	69
19.4.1.1	Enrolling Fingerprints	69
19.4.1.2	Labelling Templates	74
19.5	Reset Defaults	74
20	Yubico Authenticator Troubleshooting	77
20.1	Wrong/Incorrect Codes from Yubico Authenticator	78
20.2	Password-protecting the YubiKey’s OATH Application	79
20.3	Backing up Accounts	79
21	Yubico Authenticator with Smart Cards on iOS	81
21.1	X.509 Certificates	82
21.2	Prerequisites	82
21.3	Overview: Setup Process	82
21.4	Troubleshooting	85
22	Import Smart Card Certificates onto your YubiKey	87
22.1	YubiKey Manager GUI	87
22.2	YubiKey Manager CLI	91
22.3	Next Steps	92
23	Smart Card Certificate Provisioning with Yubico Authenticator	93
23.1	Provision Your Public Certificate	93
23.2	Next Steps	95
24	Authenticating with Smart Card on iOS	97

24.1	Authenticate to a Website on Safari	97
25	Yubico Authenticator Smart Card Troubleshooting	101
25.1	Web Browser Does Not Trigger the Yubico Authenticator Application	101
25.1.1	Toggle Focus Modes Off	101
25.1.2	Add Yubico Authenticator as an Allowed Notification	102
26	Copyright	105
26.1	Trademarks	105
26.1.1	Disclaimer	105
26.1.2	Contact Information	105
26.1.3	Document Updated Date	106

INTRODUCTION TO YUBICO AUTHENTICATOR APP

This document describes using Yubico Authenticator with the YubiKey 5 Series, the YubiKey Bio - FIDO Edition, the YubiKey 5 FIPS Series, and the Security Key Series.

Yubico Authenticator is a software-based authenticator by Yubico for authenticating users of software applications.

There are many differences between the Yubico Authenticator and other authenticators. This is because all the secrets (One-Time Passwords (OTPs) that are used to authenticate to your accounts) are stored on your YubiKey and not in the app. In most of the other authenticators the secrets are stored on your phone or computer, which can be compromised or stolen. Yubico Authenticator stores the credentials in the secure element of the YubiKey and cannot be extracted from the YubiKey.

That means that if you lose your phone, change your phone, or lose access to the Yubico Authenticator, you will not be locked out of your accounts. All you will need to do is download the app on a desktop or mobile device, plug in or scan your key, and you are able to access to all the codes on it.

The Yubico Authenticator adds a layer of security to your online accounts by generating 2-step verification codes on your mobile or desktop device. It uses the OATH-TOTP protocol to do this. [OATH Initiative for Open Authentication](#) is an industry-wide collaboration that has specified two open authentication standards: the Time-based One-time Password Algorithm (TOTP, see [RFC 6238](#)) and the HMAC-based One-time Password algorithm (HOTP, see [RFC 4226](#)).

To authenticate, the user enters a 6-8 digit code that changes with the Yubico Authenticator counter. The code is generated using HMAC (sharedSecret, and counter or timestamp). For HOTP, the counter is different with each login. For TOTP, the timestamp changes every 30 seconds.

The shared secret is often provisioned as a QR-code or preprogrammed into a hardware security key. The advantage of HOTP (HMAC-based One-time Password) is that passcodes require no clock. The Yubico Authenticator counter is encrypted and remains in sync with your YubiKey. The advantage of TOTP is that their passcodes are only available for a specific amount of time.

Since the YubiKey does not contain a battery it cannot track time and requires software to generate OATH codes. Yubico provides Yubico Authenticator for all major platforms (Windows, MacOS, Linux, Android, and iOS) to display the OTPs generated on the YubiKey.

1.1 Yubico Authenticator for Desktop

Use the Yubico Authenticator for Desktop on your Windows, Mac, or Linux computers to generate OATH credentials on your YubiKeys. In addition, the Yubico Authenticator for Desktop implements FIDO application management on YubiKeys, supporting the creation and management of FIDO2 PINs, management of existing discoverable credentials, resetting the FIDO application on the YubiKey, and on the YubiKey Bio managing fingerprint templates.

1.2 Yubico Authenticator for Mobile

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

1.3 Managing Keys

Use Yubico Authenticator to manage keys in the Yubikey 5 Series, the YubiKey Bio Series, and the Security Key Series. Management features include:

- Add, delete, and manage up to 5 fingerprints.
- Reset your YubiKey to factory defaults.
- Manage the YubiKey PIN.
- Troubleshoot common issues.

1.4 Workflow Overview

Yubico Authenticator supports iOS and Android for mobile, with a separate app for the three Desktop platforms. All platforms display similar instructions when you pull up Yubico Authenticator:

- Get a shared secret from any service you wish to secure, store it on the YubiKey and use it to generate your security codes. You will need a YubiKey 5Ci or a compatible YubiKey with NFC to get started.
 - If you have a YubiKey 5Ci, plug it in. Touch the contacts on the sides when prompted.” A green LED flashes on the right side of the key.
 - If you have a YubiKey with NFC, pull down the main view to activate NFC. Hold the key horizontally and tilt the iPhone towards the key. Touch the center of the key to the edge of the phone.
- QR codes are available from the services you wish to secure. Simply scan the QR code when you add your YubiKey and generate your own security codes.
- You can mark your credential as ‘Favorite’ and it will appear at the top of the list. Simply swipe all the way or swipe and tap the **Add to Favorites** button.

1.5 How it works

For maximum security we always recommend protecting your user accounts with the YubiKey. However where an authenticator app is preferred, the Yubico Authenticator app allows you to store your credentials on a YubiKey and not on your mobile phone, so that your secrets cannot be compromised. Yubico Authenticator requires a YubiKey 5 Series to generate OTP codes.

Use Yubico Authenticator to generate the 6-8 digit one-time code (also called *passcode* or *password*) that you need to enter (in addition to username and password) when you log on to sites that support Yubico Authenticator. By implementing two-step verification services, Yubico Authenticator enables you to safeguard access to your services and applications, protecting them from unauthorized access. Example sites where you can use codes to authenticate include Amazon, Dropbox (unless you are using U2F), Evernote, Facebook, and many others.

Yubico Authenticator generates Open Authentication (OATH) Time-based One-time Password (TOTP) and event-based HMAC-based One-Time Password (HOTP) codes.

1.5.1 Hardware-backed Security



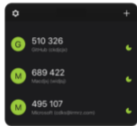
Add your credential to the YubiKey with touch or NFC-enabled tap. Hardware-backed strong two-factor authentication raises the bar for security while delivering the convenience of an authenticator app. Users can also experience greater convenience by unlocking their YubiKey with FaceID or TouchID.

1.5.2 Easy and fast setup



Generate your unique credential using QR codes available from the services you wish to protect with 2FA. Secures all the services currently compatible with other Authenticator apps. For example, Azure MFA supports TOTP authentication to secure Office 365.

1.5.3 Secure multiple work and personal accounts



Start protecting all of your accounts with stronger two-factor authentication. Easily generate new security codes that change periodically to add protection beyond passwords. And your secrets are never shared between services.

1.6 The YubiKey Advantage

1.6.1 Stronger hardware-backed security



Storing your credentials on a hardware key is safer than storing them on a mobile phone. Your credential stays safe in the secure element of the YubiKey and cannot be extracted.

1.6.2 Portable credentials across devices



Your credentials work seamlessly across multiple devices. With a portable hardware root of trust you do not lose your credentials when your phone is compromised or upgraded.

1.6.3 Cross-platform coverage



The Yubico Authenticator app works across Windows, macOS, Linux, iOS and Android. Get the same set of codes across all Yubico Authenticator apps for desktops as well as for all leading mobile platforms.

1.6.4 Self-service reduces IT costs



Users switch phones often. 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. The Yubico Authenticator app allows for user self-service to enroll multiple secrets across various services, making this a secure and efficient solution at scale.

1.7 Related Yubico Authenticator Links

- Download the Yubico Authenticator app [here](#).
- Quick-start guide to learn more about how to use the Yubico Authenticator with the services you want to secure, check out [this article](#).
- [Short video](#) showing overview of how the Yubico Authenticator works across your different devices.
- If you are planning on registering a spare key with your accounts, as we recommend, then it's important to save the QR code generated when initially setting up the service. You can read more about this in the OATH-TOTP protocol section of our [spare key registration guide](#).
- [YubiKey Mobile Concept descriptions](#).
- Quick reference to [protocols supported by the YubiKey 5 Series](#).

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

YUBICO AUTHENTICATOR PLATFORMS AND REQUIREMENTS

Yubico Authenticator app works with mobile and desktop platforms.

2.1 Supported Devices

Yubico Authenticator for Desktop supports YubiKeys from the following series:

- YubiKey Bio - FIDO Edition
- YubiKey 5 FIPS Series
- YubiKey 5 Series
- YubiKey 4 Series
- The NEO

OTP Codes

To generate OTP codes, the Yubico Authenticator requires a key from the YubiKey 5 Series.

2.2 Yubico Authenticator for Mobile Devices

This is an authenticator app compatible with the OATH standard for time and counter based numeric OTPs, as used by many online services.

To store these credentials and generate the codes, it uses a compatible YubiKey, connected either via NFC or USB (requires a USB On-the-go cable, or USB-C).

The USB functionality requires your mobile device to support USB Host mode, and for CCID to be enabled on your YubiKey.

2.3 Yubico Authenticator for Desktop

2.3.1 Desktop System Requirements

The following operating systems are supported. The application might run on other platforms too.

- Windows 8.1 or later
- macOS High Sierra 10.13 or later
- Ubuntu 16.04 LTS or later

Linux systems

Make sure the `pcscd` service is installed and running.

As a cross-platform application, Yubico Authenticator for Desktop runs on Window, Mac, and Linux.

Use of the Yubico Authenticator for Desktop requires a compatible YubiKey, i.e., one from the *Supported Devices* list.

Yubico Authenticator for Desktop can be provisioned using both slot-based credentials (compatible with any YubiKey that supports OTP) and the more powerful standalone OATH functionality.

Yubico Authenticator is a software authenticator. It provides the following features and capabilities:

- Generate two-step verification codes on a desktop to authenticate to online services and software applications
- Generate authenticator codes without having to open the app
- Manage YubiKeys: Manage fingerprint templates on the YubiKey Bio as well as the PIN and credentials stored on any YubiKey (e.g. 4 Series, 5 Series, FIPS, or CSPN)
- Keep your secret seeds safe by storing them on a YubiKey
- Set the YubiKey to require user presence (touch) to generate the code
- Protect your OATH credentials with a device password
- Connect an external smart card reader to use the YubiKey over NFC.

2.4 Online Accounts

Yubico Authenticator adds a layer of security for online accounts.



Generate 2-step verification codes on a mobile or desktop device and apply cross platform.



Experience stronger security for online accounts by adding a layer of security beyond passwords.



Secure all services currently compatible with other authenticator apps, including Google Authenticator.

2.5 GUI and CLI

Yubico Authenticator is a GUI application. If you prefer to use a CLI (command line interface), use the [YubiKey Manager CLI](#) with the `ykman fido` commands.

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

DOWNLOAD THE YUBICO AUTHENTICATOR APP

Yubico Authenticator adds a layer of security for online accounts.



Generate 2-step verification codes on a mobile or desktop device and apply cross platform.



Experience stronger security for online accounts by adding a layer of security beyond passwords.



Secure all services currently compatible with other authenticator apps, including Google Authenticator.

3.1 Download Yubico Authenticator Options

Download the latest versions from the Yubico Authenticator [download](#) page. Links are provided to download directly or by selecting the appropriate store. Or select the direct link listed here.

3.2 Download and Install the Yubico Authenticator App for Mobile

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

For mobile devices download and install are completed through the distribution method.

Android

[Download for Android from Google Play](#)

Install Yubico Authenticator from Google Play

iOS

[Download for iOS from Apple Store](#)

Get Yubico Authenticator from Apple App Store

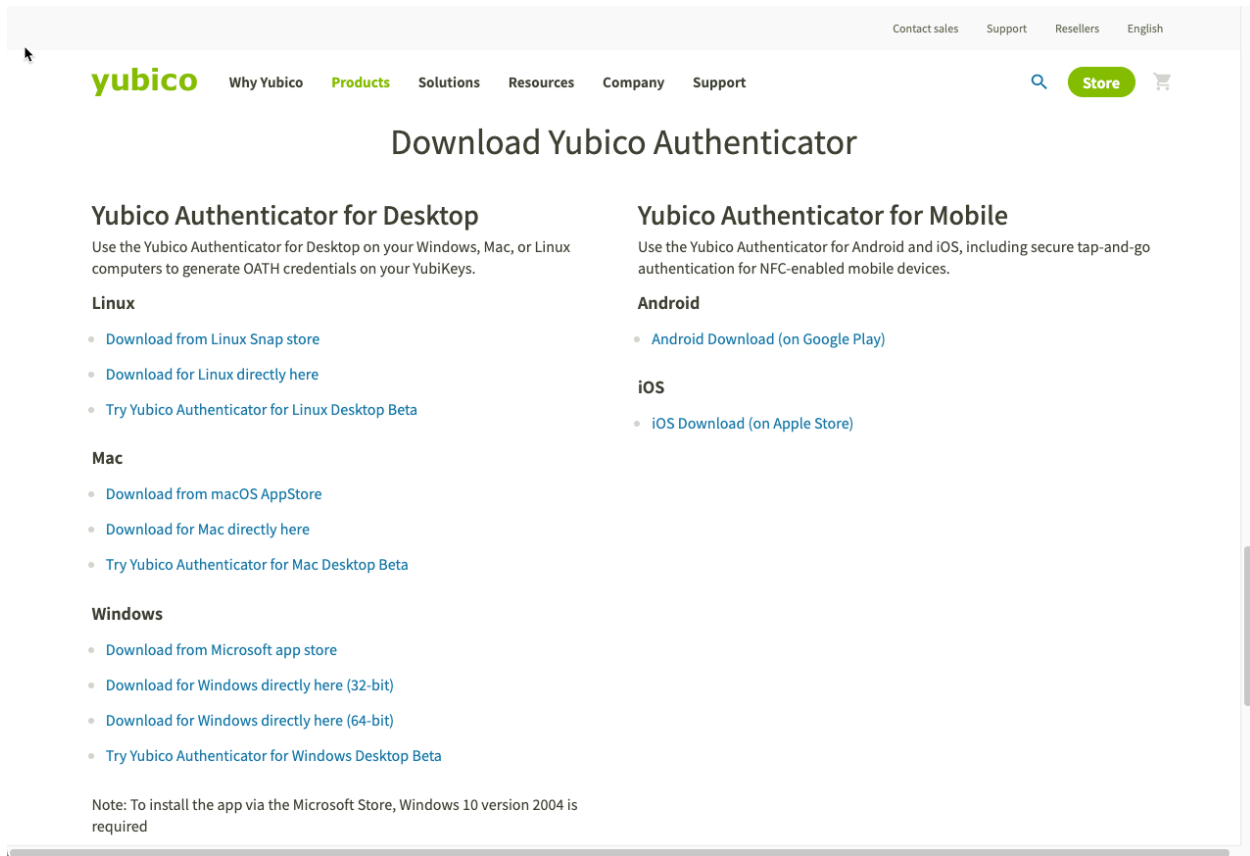


Fig. 1: Yubico Authenticator App Installer Downloads

Google Play Games Apps Movies & TV Books Kids

Yubico Authenticator
Yubico

3.5★
1.19K reviews

100K+
Downloads

Everyone

Install

Trailer

You don't have any devices

About this app →

Yubico Authenticator allows you to use a YubiKey to store OATH credentials (TOTP and HOTP supported, as used by Google, Microsoft, Dropbox, Amazon and many more) used for 2-factor authentication.

Storing the credentials on an OATH enabled YubiKey ensures that your credentials are safe, even if your phone is compromised.

It also makes it easy to move between multiple Android devices.

Yubico Authenticator
2FA with YubiKey
★★★★☆ 124

GET

Hardware security
Credentials on a security key are proven to be safer than on a mobile phone

Insert YubiKey or pull down to activate NFC

Ready to Scan
Scan your YubiKey

SUPPORT FOR NFC authentication
Activate NFC in the app before scanning your YubiKey

EASY SETUP WITH OATH
Secure services with QR codes — available from the service itself

3.3 Download Yubico Authenticator for Desktop

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

Download the Yubico Authenticator installer to your computer, then proceed to the desktop installation steps appropriate to your OS.

Linux

[Download from Linux Snap store](#)

[Download from Linux directly here](#)

Mac

[Download from macOS AppStore](#)

[Download for Mac directly here](#)

Windows

[Download from Microsoft app store](#)

[Download for Windows directly here4 \(32-bit\)](#)

[Download for Windows directly here \(64-bit\)](#)

Note: To install the app via the Microsoft Store, Windows 10 version 2004 is required.

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

INSTALL YUBICO AUTHENTICATOR ON DESKTOP

Step 1

Download Yubico Authenticator for your operating system.

See [Download the Yubico Authenticator App](#). Downloads for all supported operating systems are available on the [Yubico Authenticator release](#) page.

Step 2

Start the installer.

- MacOS – Double-click the *yubico-authenticator-<version>.dmg*
- Windows – Double-click the *Yubico-desktop-<version>.msi*
- Linux – See [Linux Installation Tips](#).

Step 3

Follow the prompts as presented by each operating system.

When installation is complete, see [Setup Yubico Authenticator Desktop on Windows](#) and [Setup Yubico Authenticator Desktop on macOS](#) for additional setup steps for Windows and macOS.

4.1 Linux Installation Tips

Recommended

Install via [Snap Store](#), or use the AppImage available [here](#).

See [How to run an AppImage?](#) for instructions on how to use AppImages.

If you have trouble getting the AppImage to work, make sure your system has the **pcscd** package installed.

Alternatively

Install via your distribution's repositories, if possible. Since the exact steps for this vary from OS to OS, please refer to your distribution's documentation for more information.

For additional methods for installing Yubico software on Linux, see [Installing Yubico Software on Linux](#).

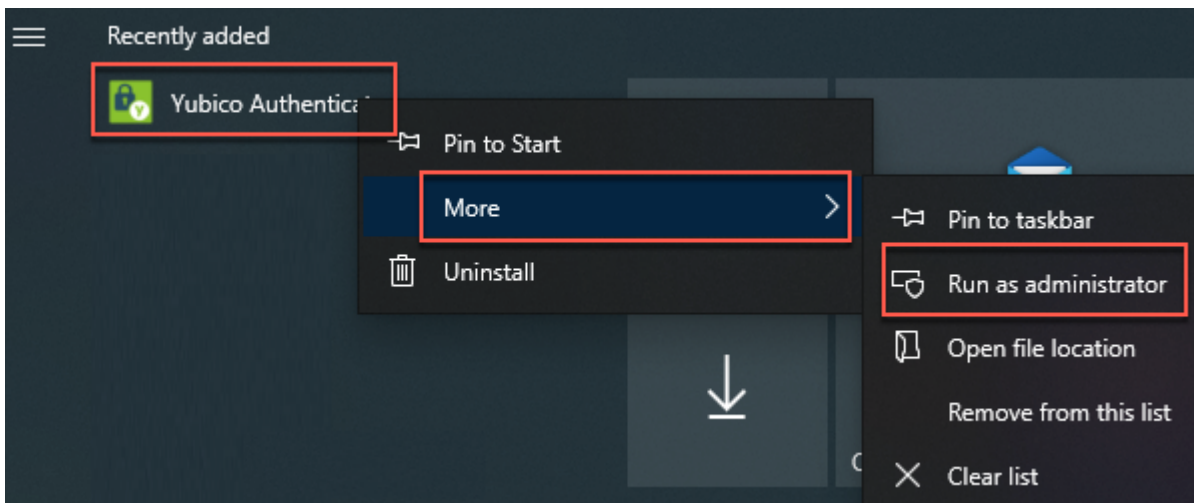
To file a support ticket with Yubico, click [Support](#).

SETUP YUBICO AUTHENTICATOR DESKTOP ON WINDOWS

On Windows, running Authenticator requires Administrator permissions.

Step 1

Select **Run as Administrator** when you start the Authenticator for the first time.



Step 2

Insert your YubiKey.

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

SETUP YUBICO AUTHENTICATOR DESKTOP ON MACOS

After installation, the Yubico Authenticator requires:

- Permission to receive keystrokes from other applications

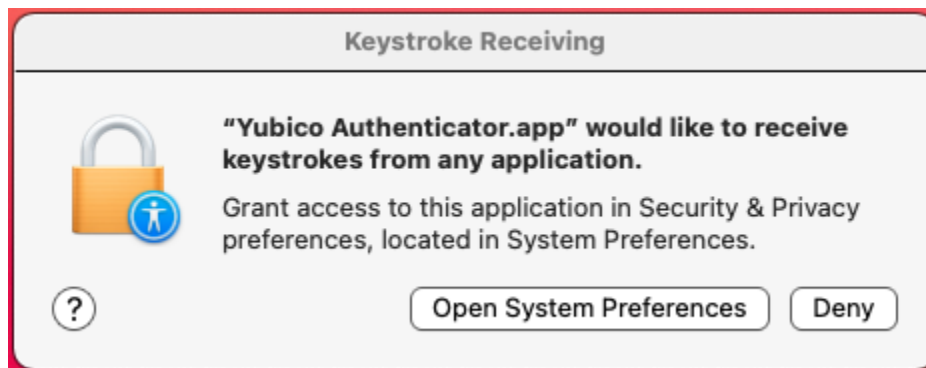


Fig. 1: MacOS: Give Permission to Receive Keystrokes

- Permission to record your computer's screen.

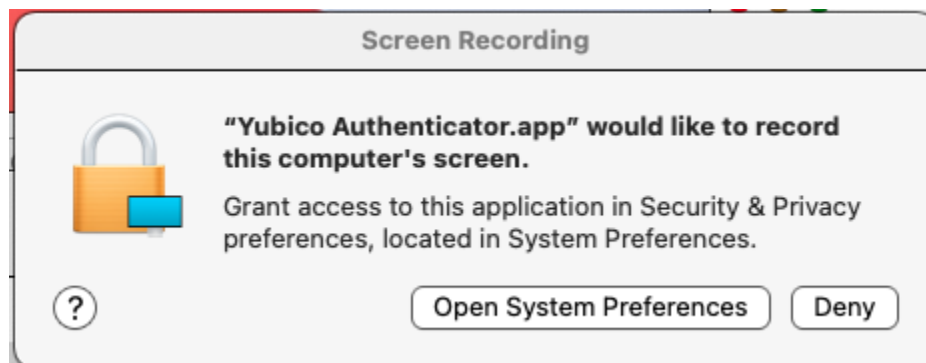


Fig. 2: MacOS: Give Permission to Record Screen

You can wait to do this until you need to use the Authenticator or apply these settings now.

Step 1

Grant Yubico Authenticator permissions in the settings for your operating system.

When you start the Authenticator, the permission request popups are displayed.

1. Click **Open System Preferences**.

2. Click to unlock settings.
3. Check the **Authenticator** box.
4. Close the settings.

Step 2

Apply the permissions, quit Yubico Authenticator application and restart it.

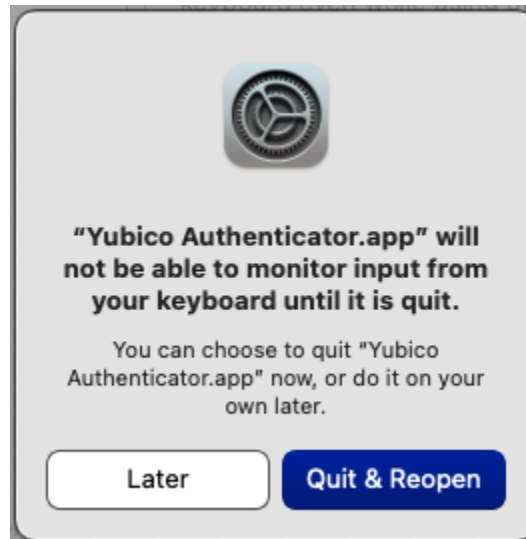


Fig. 3: MacOS: Apply Permission

Step 3

Insert your YubiKey, at the prompt when Authenticator restarts.

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

SETUP YUBICO AUTHENTICATOR MOBILE ON ANDROID

Yubico Authenticator for Android is hosted on [Google Play](#) as Yubico Authenticator.

See the file COPYING for copyright and license information.

Add credentials by tapping the + action button near the bottom right, and selecting either to add a credential by scanning a QR code, or by entering a Base32 encoded secret manually.

Once credentials have been added, simply tap or connect your YubiKey to display codes.

7.1 Development

This app is developed in Android Studio, using gradle for building. To build the APK from the command line, run:

```
`$ ./gradlew assemble
```

Once done the .apk file can be found in the app/build/outputs/apk/ directory.

7.2 Issues

Please report app issues in the [issue tracker on GitHub](#).

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

SETUP YUBICO AUTHENTICATOR MOBILE ON IOS

Note: This article covers basic YubiKey / Security Key use on iOS and iPadOS. For information such as **can I log into my service on iOS/iPadOS**, consult the [Works with YubiKey Catalog](#) or reach out to the service directly for more information. Yubico does not maintain setup documentation for third party products or services.

Depending on the iOS/iPadOS hardware as well as the YubiKey or Security Key model, there are three methods for using a YubiKey with iOS/iPadOS:

- The YubiKey 5Ci can connect directly to an iOS/iPadOS device via a Lightning connector.
- The YubiKey 5 NFC, YubiKey NEO, and Security Key NFC can be used over NFC on NFC-enabled iPhones.(1)
- Any YubiKey model can be plugged either directly into an iOS/iPadOS device or using a compatible adapter to take advantage of both the OTP functionality, as well as WebAuthn.(1)

Note: Yubico Authenticator does not support this option.(2)

NOTES:

- (1) iOS/iPadOS 13.3 and Safari are required to leverage native support for WebAuthn.
- (2) iOS/iPadOS is only able to communicate with the YubiKey's OATH application (required for Yubico Authenticator functionality) via NFC and Lightning.
 - Since the one-time passwords generated by Yubico Authenticator are time-based, and the YubiKey does not have the ability to track time (due to its lack of a battery), proper functionality requires iOS/iPadOS being able to both write to and read from the YubiKey (it sends the YubiKey the current time and receives the one-time password).
 - Read/write is possible over NFC due to [Apple's recent expansion](#), and via Lightning due to the YubiKey 5Ci's MFi certification, but not using other connection methods, namely USB-C, which has replaced the Lightning connector on third-generation and later iPad Pros. At this time, there is no way to use Yubico Authenticator on these iPads, as they do not support NFC.
- (3) For developers, the [Yubico Mobile iOS SDK](#) (software development kit) can be integrated into your apps to enable the YubiKey 5Ci and NFC-enabled YubiKeys to interact with iOS apps beyond the basic functionality covered in this document (e.g. OpenPGP, PIV, Challenge-Response, etc.).
- (4) **Important:** Depending on the service you're attempting to use, as well as the model and method of connecting your YubiKey to iOS/iPadOS, your desired use case may not be supported.
 - The [Works With YubiKey Catalog](#) is intended to list all known YubiKey integrations, including what devices the integration is supported on.

- Instructions for how to add and use the YubiKey with the service is also linked from every integration in the [Works With YubiKey Catalog](#). Please consult this list to determine if your use case is supported on iOS/iPadOS.
- If you discover that a service supports the YubiKey but isn't located in the catalog, reach out either by opening a support case (via <https://yubi.co/support>).

(5) For information about iOS using protocols other than OATH, see [Getting Started with iOS](#).

8.1 Using your YubiKey 5Ci on iOS/iPadOS

Yubico Authenticator for iOS can be used to store TOTP and HOTP accounts, as well as to generate codes to authenticate to services that support “authenticator apps.” Basic account adding and code generation is covered below.

Note: Once an HOTP/TOTP account is stored on the YubiKey, it can be accessed on any version of Yubico Authenticator where the YubiKey is plugged in. For example, you can store an account using Yubico Authenticator for iOS and then access the accounts code on an Android phone using Yubico Authenticator for Android, or on a Windows/MacOS/Linux desktop or laptop running Yubico Authenticator for Desktop.

Since the secret is stored on the YubiKey, generating a code requires both the YubiKey and the Yubico Authenticator. Since the secret cannot be extracted once it is added to a YubiKey, it is important to consider account recovery and backups before you add an account to the YubiKey. Backups **cannot** be made after the Authenticator app setup for any given service is completed without going through the setup process again.

8.1.1 Adding accounts on iOS/iPadOS

To add accounts to your YubiKey using Yubico Authenticator for iOS, complete the steps:

Step 1: Download and install Yubico Authenticator for iOS, available in the App Store for any iPhone/iPad with a Lightning port.

iPads with USB-C ports are **not** supported.

Step 2: Open Yubico Authenticator for iOS.

Step 3: Plug in a YubiKey 5Ci.

Step 4: On another device:

1. Set up the service you are trying to secure with the Authenticator app.
2. Continue until the service provides a QR code.

If you need assistance with the Authenticator app setup process for a service, please refer to the service's setup instructions.

Step 5: In Yubico Authenticator for iOS, tap the + button at the top right.

Step 6: Tap **Scan QR code**. If a pop-up appears requesting permission to access the camera, tap **Allow**.

Step 7: Point the iPhone/iPad's camera at the QR code on the other device until the QR code is read.

The iPhone/iPad should vibrate and a **New Account** screen should appear.

Step 8: Tap **Save**.

At this point, if you wish to store the same account on a second YubiKey in your possession, simply repeat steps 3-7 for each YubiKey.

Alternatively, if you wish to add this account to another YubiKey but don't have one currently, you can save a copy of the QR code (or secret key) in a safe place to scan and add later.

Step 9: Use the current code displayed in Yubico Authenticator for iOS for this account to complete setup of the account on the other device.

8.1.2 Generating codes on iOS/iPadOS

To generate codes for accounts stored on your YubiKey using Yubico Authenticator for iOS, follow the process below:

Step 1: Open Yubico Authenticator for iOS.

Step 2: Plug in a YubiKey 5Ci.

All current TOTP codes should be displayed.

If an account you added uses HOTP, or if you set the TOTP account to **require touch**, you will first have to display the current code:

1. Tap the credential.
2. Tap the gold YubiKey contact, if prompted.

8.2 Using your YubiKey 5 NFC, YubiKey NEO

Yubico Authenticator for iOS can be used to store TOTP and HOTP accounts, as well as to generate codes to authenticate to services that support "authenticator apps." Basic account adding and code generation is covered below.

Note: Once an HOTP/TOTP account is stored on the YubiKey, it can be accessed on any version of Yubico Authenticator where the YubiKey is plugged in. For example, you can store an account using Yubico Authenticator for iOS and then access the accounts code on an Android phone using Yubico Authenticator for Android, or on a Windows/MacOS/Linux desktop or laptop running Yubico Authenticator for Desktop.

Since the secret is stored on the YubiKey, generating a code requires both the YubiKey and the Yubico Authenticator. Since the secret cannot be extracted once it is added to a YubiKey, it is important to consider account recovery and backups before you add an account to the YubiKey. Backups **cannot** be made after the Authenticator app setup for any given service is completed without going through the setup process again.

8.2.1 Adding accounts on YubiKey 5 NFC, YubiKey NEO

To add accounts to your YubiKey using Yubico Authenticator for iOS, follow the process below

Step 1: Download and install Yubico Authenticator for iOS, available in the App Store for any iPhone/iPad with a Lightning port

iPads with USB-C ports are **not** supported.

Step 2: Open Yubico Authenticator for iOS.

Step 3: On another device:

1. Set up the service you are trying to secure with the Authenticator app.

2. Continue until the service provides a QR code.

If you need assistance with the Authenticator app setup process for a service, please refer to the service's setup instructions.

Step 4: In Yubico Authenticator for iOS, tap the + button at the top right.

Step 5: Tap **Scan QR code**. If a pop-up appears requesting permission to access the camera, tap **Allow**.

Step 6: Point the iPhone/iPad's camera at the QR code on the other device until the QR code is read.

The iPhone/iPad should vibrate and a **New Account** screen should appear.

Step 7: Tap **Save**.

A **Ready to Scan** pop-up should appear.

Step 8: Tap and hold your NFC-capable YubiKey to your phone's NFC antenna (typically at the top-rear of the phone).

A checkmark will appear if the account is securely added to the YubiKey.

At this point, if you wish to store the same account on a second YubiKey in your possession, simply repeat steps 4-8 for each YubiKey.

Alternatively, if you wish to add this account to another YubiKey but don't have one currently, you can save a copy of the QR code (or secret key) in a safe place to scan and add later.

Step 9: Use the current code displayed in Yubico Authenticator for iOS for this account to complete setup of the account on the other device.

With an NFC capable YubiKey, only one set of codes will be generated each time you tap the YubiKey to your phone.

If the service doesn't accepted the current code, try swiping down from the top of the Yubico Authenticator application which will prompt you to rescan your YubiKey (and provide a new code).

8.2.2 Generating codes on YubiKey 5 NFC, YubiKey NEO

To generate codes for accounts stored on your YubiKey using Yubico Authenticator for iOS, follow the process below:

Step 1: Open Yubico Authenticator for iOS.

Step 2: Pull down from below the **Quick Find** search box (as if you are trying to "refresh").

This initiates the prompt to scan an NFC-capable YubiKey. All current TOTP codes should be displayed.

If an account you added uses HOTP, or if you set the TOTP account to **require touch**, you will first have to display the current code:

1. Tap the credential.
2. Scan your YubiKey again to generate the code.

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

SETUP YUBIKEY WITH IPADS

There are some caveats with using your iPad with your various services you want to secure. Generally, it will depend on if your iPad has a lightning or USB-C connection, and which security protocols the service you are using supports. We'll dive into more details below!

9.1 YubiKeys with iPads with lightning ports

For iPads with a lightning port, the [YubiKey 5Ci](#) works with everything the iPhone does. The YubiKey 5Ci works with the **Yubico Authenticator** app. This is our only key with a direct lightning connection.

Please keep in mind that you cannot use a lightning adapter as the lightning is MFi (made for iPhone) and therefore it may not work. Adapters should work with OTP and FIDO U2F security protocols, however we don't recommend it.

9.2 YubiKeys with iPad Pros with USB-C ports

When connecting a YubiKey to your iPad Pro over USB-C, the functions that work are button-press OTP (namely, [Yubico OTP](#) or `ccccccukedtgvcjbeblfjdeeneidnflbudkuhlerctnf`) and WebAuthn (which generally encompasses FIDO U2F and FIDO2).

Note: YubiKeys are not compatible with the [Yubico Authenticator app](#) (OATH security protocol) on iPad Pro, because the iPad Pro does not have lightning or NFC capabilities. This is due to Apple's restrictions on what is able to communicate with iPadOS over USB-C, combined with the fact that Apple's MFi program (which we use to enable this kind of communication over the lightning connector) does not apply to the USB-C connector.

In summary: **You should be able to use your key with any services that use Yubico OTP on an iPad over USB-C.** For services that use WebAuthn, FIDO U2F, and FIDO2, the capability is there in iPadOS if you use the Safari browser (this leverages iPadOS' native support for WebAuthn), but note that some services may simply not give you the option to use a YubiKey if they detect you are logging in from an iPad. This is outside of our control.

For services that support our products via authenticator apps, you should still be able to use Yubico Authenticator with a YubiKey to generate the one-time passwords, but you cannot do this on your iPad. You can however, generate the OTPs on another device, and then hand-copy them onto your iPad.

You can see which security protocols a service supports in our [Works with YubiKey Catalog](#).

Please see [Getting Started on iOS](#) for further information regarding use of YubiKeys with iPads.

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

USE OATH WITH THE YUBIKEY

OATH is an organization that specifies two open authentication standards: TOTP and HOTP.

When using OATH with a YubiKey on desktops or mobile devices, the shared secrets are stored and processed in the YubiKey's secure element. This has two advantages over storing secrets on a phone:

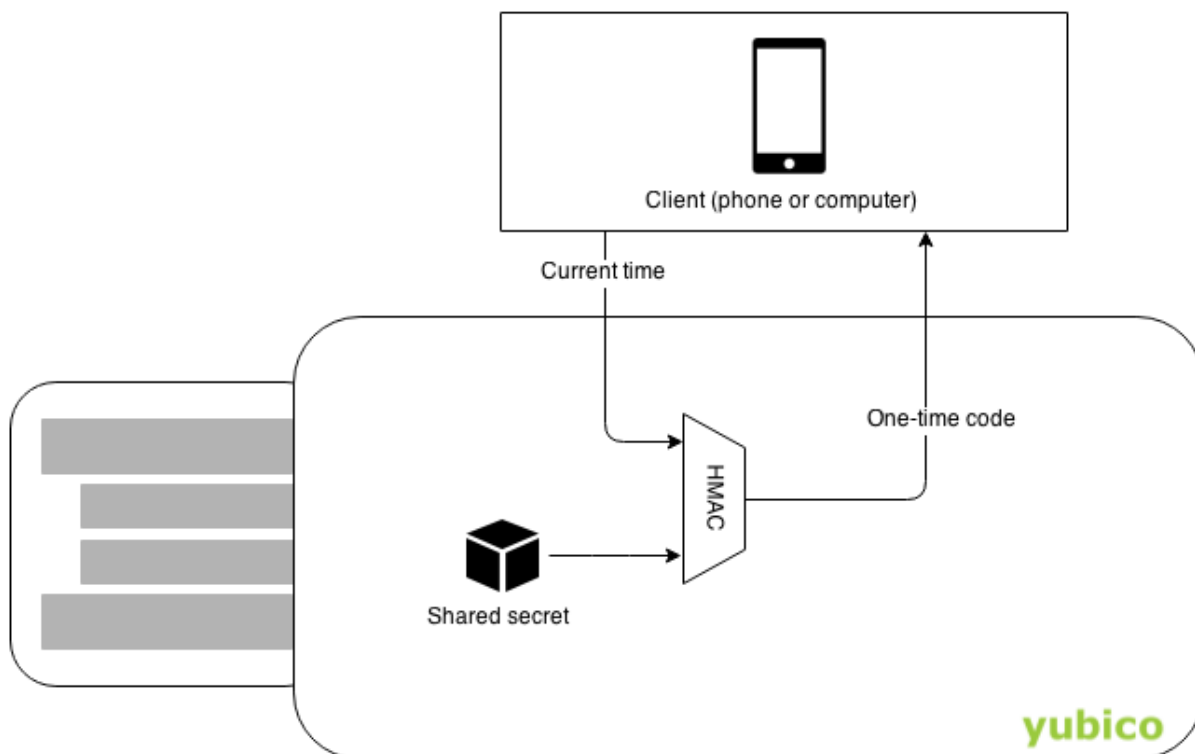
- *Security*

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.

- *Accessibility*

You can display OATH codes on more than one phone or computer. If your phone runs out of battery, you can get a code using a friend's phone or your computer.

A YubiKey can emit a HOTP code when its button is pressed. This is configured using [Yubikey Personalization GUI](#). For TOTP you need an [application that can read OATH codes from YubiKeys](#), since YubiKeys does not have an internal clock.



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

WEBAUTHN COMPATIBILITY

The Web Authentication API (also known as WebAuthn) is a specification written by the W3C and FIDO. This enables users to have FIDO-based authentication to websites.

This is underlying functionality that allows you to use your YubiKey with Yubico Authentication on supported browsers and platforms.

11.1 WebAuthn Platform Compatibility

WebAuthn support is not uniform across browsers. For services implementing WebAuthn, it is vital to note which user environments are supported, and have the appropriate error handling in the event of an unsupported browser.

11.1.1 Features

- User Presence - The browser supports a physical user interaction to establish an event is not being initiated by a remote attacker.
- Resident Key / Discoverable Credential - The browser supports WebAuthn credentials stored on the authenticator. These credentials can be read to identify the user account without the user manually providing them.
- User Verification (PIN / Biometric) - The browser supports an interface to allow a user to verify their identity via entering a WebAuthn PIN or Biometric.
- CTAP 1 / U2F Legacy Support - The browser has legacy support for authenticators only supporting U2F.

11.1.2 Windows 10 21H1

- Edge Chromium 91
 - User Presence (touch) : USB, NFC
 - Resident Key/Discoverable Credential : USB, NFC
 - User Verification (PIN/Biometric) : USB, NFC
 - CTAP 1/U2F Legacy Support : USB, NFC
- Chrome 91
 - User Presence (touch) : USB, NFC
 - Resident Key/Discoverable Credential : USB, NFC
 - User Verification (PIN/Biometric) : USB, NFC

CTAP 1/U2F Legacy Support :USB, NFC

- Firefox 89

User Presence (touch) : USB, NFC

Resident Key/Discoverable Credential : USB, NFC

User Verification (PIN/Biometric) : USB, NFC

CTAP 1/U2F Legacy Support : USB, NFC

Notes: Chrome differences from other browsers. When a request to create a credential with a resident key is made User Verification is enforced even if the request has UV = 0.

11.1.3 MacOS 11.4

NFC support has been excluded since NFC is not supported on macOS browsers.

- Safari 14.6 (note 1)

User Presence (touch) : USB

Resident Key/Discoverable Credential : USB

User Verification (PIN/Biometric) : USB

CTAP 1/U2F Legacy Support : USB

- Chrome 91

User Presence (touch) : USB

Resident Key/Discoverable Credential : USB

User Verification (PIN/Biometric) : USB

CTAP 1/U2F Legacy Support : USB

- Firefox 89 (note 2)

User Presence (touch) : none

Resident Key/Discoverable Credential : none

User Verification (PIN/Biometric) : none

CTAP 1/U2F Legacy Support : USB

Note 1: Safari will not allow users to set a PIN for User Verification if one is not already set.

Note 2: Bug for FIDO2 support on MacOS: https://bugzilla.mozilla.org/show_bug.cgi?id=1530370

11.1.4 iOS 14

Verified with iPhone 12, 11, XR, XS and iPhone 8.

Most browsers on Apple mobile devices use [Apple WebKit](#). As such, these browsers will have all the same functionality available.

- Safari 14.6 (note 1)

User Presence (touch) : Lightning, NFC
 Resident Key/Discoverable Credential : Lightning, NFC
 User Verification (PIN/Biometric) : Lightning, NFC
 CTAP 1/U2F Legacy Support : Lightning, NFC

- Chrome 91 (note 1)

User Presence (touch) : Lightning, NFC
 Resident Key/Discoverable Credential : Lightning, NFC
 User Verification (PIN/Biometric) : Lightning, NFC
 CTAP 1/U2F Legacy Support : Lightning, NFC

- Firefox 34.2 (note 1)

User Presence (touch) : Lightning, NFC
 Resident Key/Discoverable Credential : Lightning, NFC
 User Verification (PIN/Biometric) : Lightning, NFC
 CTAP 1/U2F Legacy Support : Lightning, NFC

Note 1: If a PIN is already set on the YubiKey, then a browser will display a PIN prompt only when creating a credential and when user verification has not been requested. Any request for user verification will fail if there is no PIN set on the YubiKey.

11.1.5 iPadOS 15.5

Verified with iPad 6th generation (Lightning), iPad Air (USB-C) 4th generation, and iPad Pro 2018 (USB-C).

Most browsers on Apple mobile devices use Apple WebKit. As such, these browsers will have all the same functionality available.

NFC tests have been excluded since NFC is not supported on iPadOS browsers. USB-C is only available on iPad Pro and 4th and 5th generation iPad Air models.

- Safari 14.6 (note 1)

User Presence (touch) : Lightning, USB-C
 Resident Key/Discoverable Credential : Lightning, USB-C
 User Verification (PIN/Biometric) : Lightning, USB-C
 CTAP 1/U2F Legacy Support : Lightning, USB-C

- Chrome 91 (note 1)

User Presence (touch) : Lightning
 Resident Key/Discoverable Credential : Lightning
 User Verification (PIN/Biometric) : Lightning
 CTAP 1/U2F Legacy Support : Lightning

- Firefox 34.2 (note 1)

User Presence (touch) : Lightning

Resident Key/Discoverable Credential : Lightning

User Verification (PIN/Biometric) : Lightning

CTAP 1/U2F Legacy Support : Lightning

Note 1: If a PIN is already set on the YubiKey, then a browser will display a PIN prompt only when creating a credential and when user verification has not been requested. Any request for user verification will fail if there is no PIN set on the YubiKey.

11.1.6 Android 11

Verified with Pixel 3a

Currently the Android platform only supports CTAP1 (U2F) authenticators. Android does support clients (browsers) making WebAuthn requests to a relying party.

- Chrome 91

User Presence (touch) : none

Resident Key/Discoverable Credential : none

User Verification (PIN/Biometric) : none

CTAP 1/U2F Legacy Support : USB, NFC

- Firefox 89.1

User Presence (touch) : none

Resident Key/Discoverable Credential : none

User Verification (PIN/Biometric) : none

CTAP 1/U2F Legacy Support : none

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

USING MFA AUTHENTICATOR CODES WITH YOUR YUBIKEY ON DESKTOPS

These instructions show you how to set up your YubiKey so that you can use two-factor authentication to sign in to any account that requires authenticator codes. Example sites where you can use codes to authenticate include Amazon, Dropbox (if you aren't using U2F), Evernote, Facebook, and many others. To use a code at one of these sites, you use an application, such as Google Authenticator, to generate the codes. The codes generated are OATH-TOTP codes, a type of one-time password, that are usually six-digits. You can use Yubico Authenticator, which is similar to Google Authenticator. We have created both a desktop and mobile version of this app for you to use so you can use it on a Windows, Mac, Linux, or Android.

To sign in to any account that requires authenticator codes, use Yubico Authenticator to *Setup Your YubiKey with Yubico Authenticator for Desktop*. Note that some services call two-factor authentication *two-step verification*.

If you save a service's QR code or secret key (referenced in step 2 below), you can program the credential into other YubiKeys. It is always recommended to have a [backup security key](#).

You can set Issuer, Account name Require touch (referenced in step 5 below) differently for each account.

12.1 Setup Your YubiKey with Yubico Authenticator for Desktop

These steps apply to Windows, macOS, and Linux systems. The Yubico Authenticator app for desktop uses the same interface.

12.1.1 Requirements

Yubico Authenticator

12.1.2 Instructions

Step 1

Enable two-factor authentication for the service. The details of the procedure may vary from service to service. Typically, you:

- a) Log in to the service
- b) Select **Settings** or **Security**
- c) Select the option **Enable two-factor authentication**.

Step 2

Select the option to use an authenticator. A QR code should appear. This code is sometimes referred to as the *secret key*.

- **If you are planning to register more than one YubiKey with this service, please save a copy of the QR code, or secret key as you will need it when registering more keys.**

Step 3

Open Yubico Authenticator for Desktop and plug in your YubiKey.

Step 4

Click the + button then click **Scan** to scan the QR code.

Making sure the QR code is not partially obscured by another window.

Step 5

Before adding the YubiKey as the credential, you can adjust the following settings on a per-credential basis; in other words, each credential can have these set differently. **These cannot be changed after you save the credential.**

- **Issuer** - Name of the service
- **Account name** - Name of the account holder
- **Require touch** - Toggles the requirement to touch the YubiKey (thus demonstrating user presence) in order to display the OATH or FIDO code. Checked = On, Unchecked = Off.

Step 6

When you are satisfied with the settings, to add the YubiKey as a credential, click **Add**.

Step 7

To add another YubiKey to the service, unplug the YubiKey that is currently plugged in, insert the next key, and carry out steps 4-6 again.

- It is recommended to save a copy of the QR code (or secret key) safe so you have the ability to program the credential into future backup YubiKeys.

Step 8

Complete the setup process on the website. This typically requires you to enter:

- a) One-time password generated by the Yubico Authenticator
- b) Your login password for a second time.

Your YubiKey is now configured for authenticator codes for this service.

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

USING MFA AUTHENTICATOR CODES WITH YOUR YUBIKEY ON MOBILE DEVICES

These instructions show you how to set up your YubiKey so that you can use two-factor authentication to sign in to any account that requires authenticator codes on iOS or Android mobile devices. Example sites where you can use codes to authenticate include Amazon, Dropbox (if you aren't using U2F), Evernote, Facebook, and many others. To use a code at one of these sites, you use an application, such as Google Authenticator, to generate the codes. The codes generated are OATH-TOTP codes, a type of one-time password, that are usually six-digits. You can use Yubico Authenticator, which is similar to Google Authenticator. We have created both a desktop and mobile version of this app for you to use so you can use it on a Windows, Mac, Linux, or Android.

To sign in to any account that requires authenticator codes, use Yubico Authenticator to *Setup Your YubiKey with Yubico Authenticator for Desktop*. Note that some services call two-factor authentication *two-step verification*.

Save a service's QR code or secret key, so you can program the credential into other YubiKeys. It is always recommended to have a [backup security key](#).

You can set Issuer, Account name Require touch differently for each account.

13.1 Setup Your NFC-enabled YubiKey with Yubico Authenticator for Android App

13.1.1 Requirements

- YubiKey 5 NFC, YubiKey 5C NFC, or YubiKey NEO
- [Yubico Authenticator for Android app](#) from the Google Play store
- An Android phone that supports NFC

13.1.2 Instructions

Step 1

Enable two-factor authentication for your service. Usually, you will do this by selecting **Settings** or **Security**, and then selecting the option to **Enable two-factor authentication**.

Tip: Some services call this *two-step verification*.

Step 2

Select the option to use a mobile app or Google Authenticator.

:Step 3: You will need to copy the text string as well as scan the QR code. Click **Enter your secret key manually** and copy the text of the code and paste it into a text file now.

- Be sure to save a copy of the secret key. You can use this to create a backup copy of your YubiKey configured to use authenticator codes. It is always best security practices to ensure you have a backup YubiKey.

Step 4

Open the Yubico Authenticator app on your Android device.

Step 5

Tap the control icon to open the menu.

Step 6

Select **Scan account QR-code**, and then scan the QR code from the web page.

- Be sure to save a copy of the QR code in a safe place. You can use this to create a backup YubiKey configured to use authenticator codes. It is always best security practices to ensure you have a backup YubiKey.

Note: To manually add the secret key, select **Add account manually**, then enter the credential name, and type the secret key that you previously saved as a backup.

Step 7

On the web page, click **Next**. You have successfully configured your YubiKey for authenticator codes!

Step 8

To view the credential, tap and hold your YubiKey on the back of your phone where the NFC antenna is located. Yubico Authenticator displays the six digit code associated with this credential. This is the code you need to enter to authenticate when using two-factor authentication.

13.2 Setup Your YubiKey with Yubico Authenticator for iOS App

13.2.1 Requirements

Note: Yubico Authenticator is not supported on iPads with USB-C ports due to limitations in the Apple ecosystem.

- YubiKey 5 NFC, YubiKey 5C NFC, YubiKey NEO, or YubiKey 5Ci
 - [Yubico Authenticator for iOS app](#) from the App Store
 - **For NFC** an iPhone 7 or newer, running iOS 13 or newer
 - **For Lightning connectivity** an iPhone, iPod Touch, or iPad with a Lightning connector, running iOS/iPadOS 11.2 or newer.
-

13.2.2 Instructions

Step 1

Download and install Yubico Authenticator for iOS, available in the App Store for any iPhone/iPad with a Lightning port.

Step 2

Open Yubico Authenticator for iOS.

Step 3

If you are using a YubiKey 5Ci over Lightning, plug it in.

Step 4

On another device (such as a laptop), launch the service you want to use with an authenticator app. Follow the on-screen prompts for securing the service with an authenticator app until the point when a QR code is displayed. (If you need assistance with the authenticator app setup process for a service, please refer to the service's setup instructions or contact their support team).

Step 5

In Yubico Authenticator for iOS on your iPhone/iPad, tap the + button at the top right.

Step 6

Tap Scan QR code. If a pop-up appears requesting permission to access the camera, tap **Allow**.

Step 7

Point the iPhone/iPad's camera at the QR code on the other device until the QR code is read. This is signaled by a **New Account** screen appearing in Yubico Authenticator for iOS.

Step 8

Before saving this credential, you have the option to adjust the following settings.

Note that these cannot be changed after saving the credential.

- **Issuer** - defines the service name
- **Account name** - Defines the account holder name
- **Require touch** - Toggles on or off the requirement to touch the YubiKey (or scan again in the case of NFC) in order to display the OATH code. Note that this is set on a per-credential basis. In other words, each credential can have this set differently.

Step 9

Tap **Save**. If you are using a YubiKey over NFC, when the **Ready to Scan** pop-up appears, bring your key next to your phone's NFC reader (typically located on the rear of the phone near the top) and hold it there until a checkmark appears on-screen, indicating the credential has been securely added to the YubiKey.

- At this point, if you wish to store the same account on a second YubiKey, simply repeat steps 3 and 5-9 for each additional YubiKey. Alternatively, if you wish to add this account to another YubiKey but don't have one currently, you can save a copy of the QR code (or secret key) in a safe place to scan and add later.

Step 10

Use the current code displayed in Yubico Authenticator for iOS for this account to complete setup of the account on the other device.

Your YubiKey is now configured for authenticator codes for this service.

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

USING YUBIKEYS WITH AZURE MFA OATH-TOTP

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.

14.1 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.

14.2 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.

14.2.1 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.

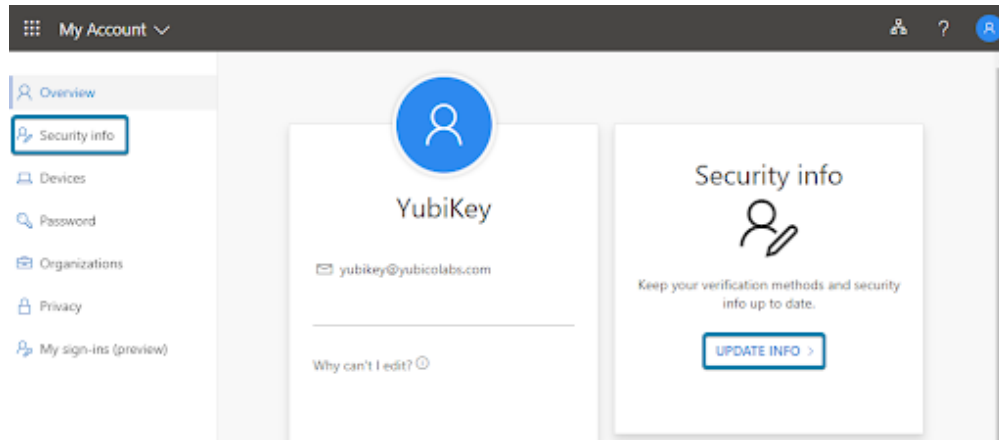
Since the YubiKey does not contain a battery it cannot track time and will require software to generate OATH-TOTP codes. Yubico provides Yubico Authenticator for all major platforms (Windows, MacOS, Android, and iOS) to display the one time passcodes generated on the YubiKey.

14.2.2 Register a YubiKey

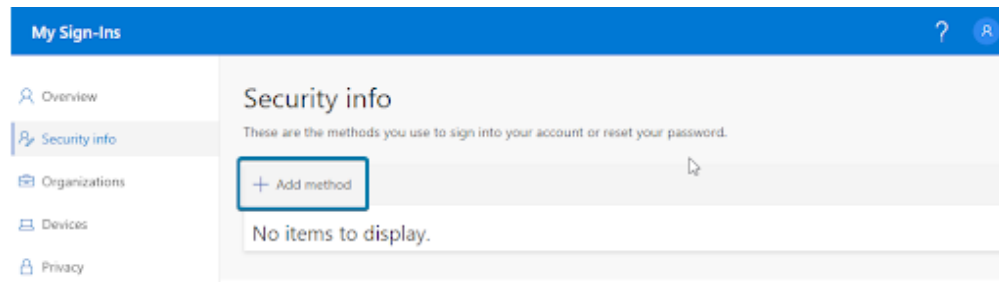
Step 1: Open a browser window and navigate to <https://myprofile.microsoft.com>.

Step 2: Sign in to your account.

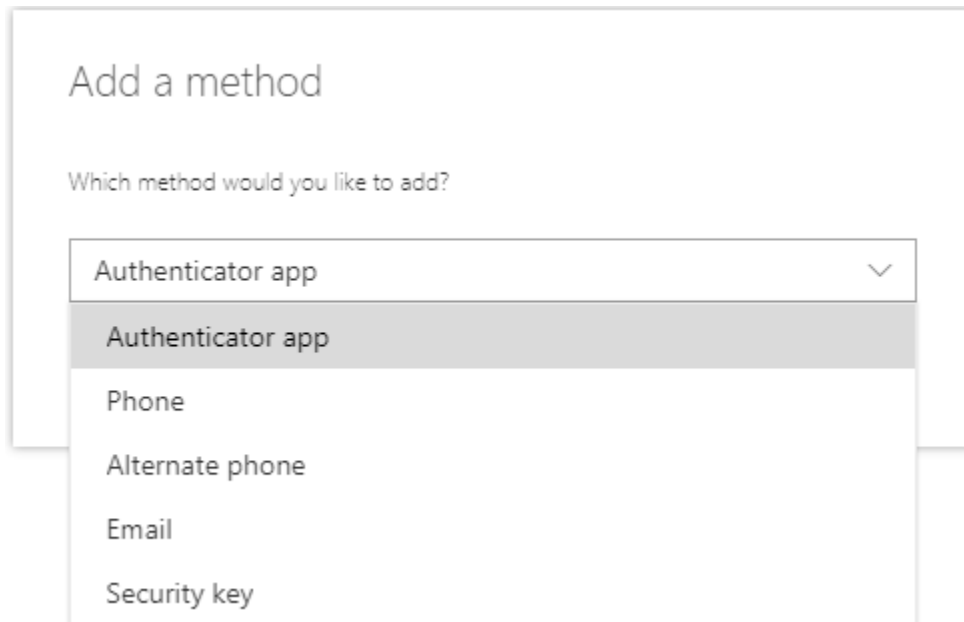
Step 3: Select **Security Info** in the left navigation or **Update Info** in the Security Info tile.



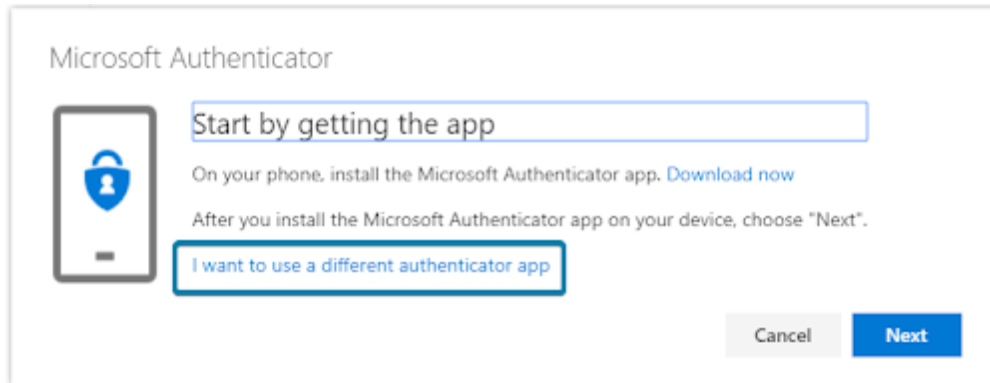
Step 4: Select **Add Method**.



Step 5: Select **Authenticator app**.



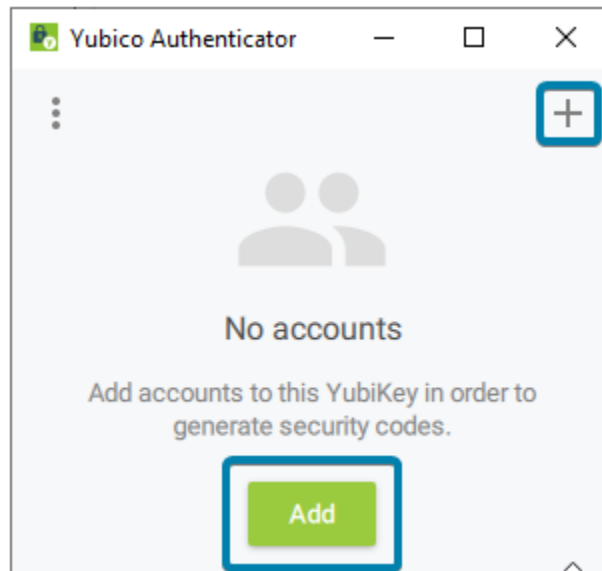
Step 6: Select **I want to use a different authenticator app**.



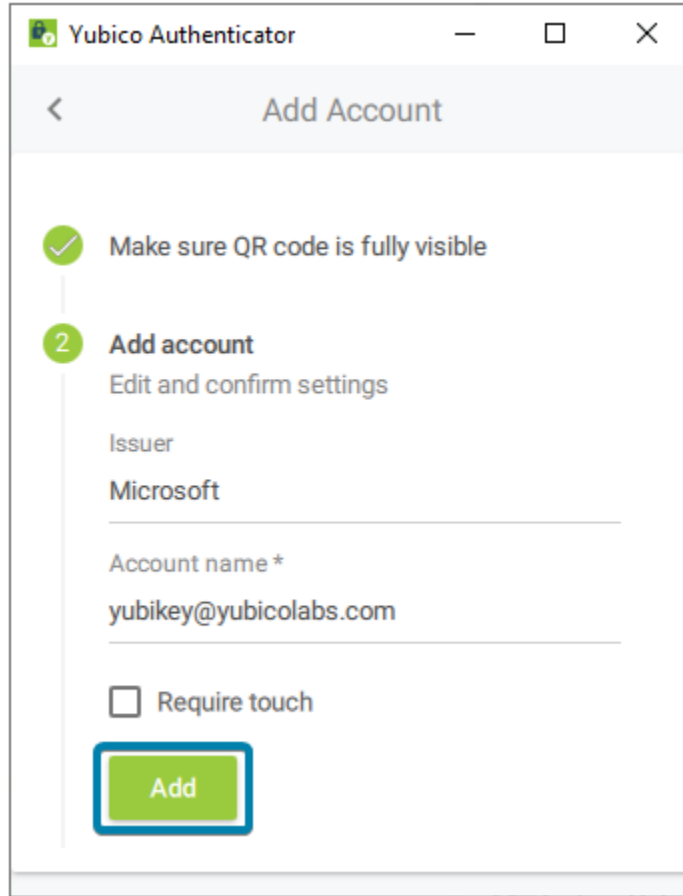
Step 7: Select **Next**.

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.

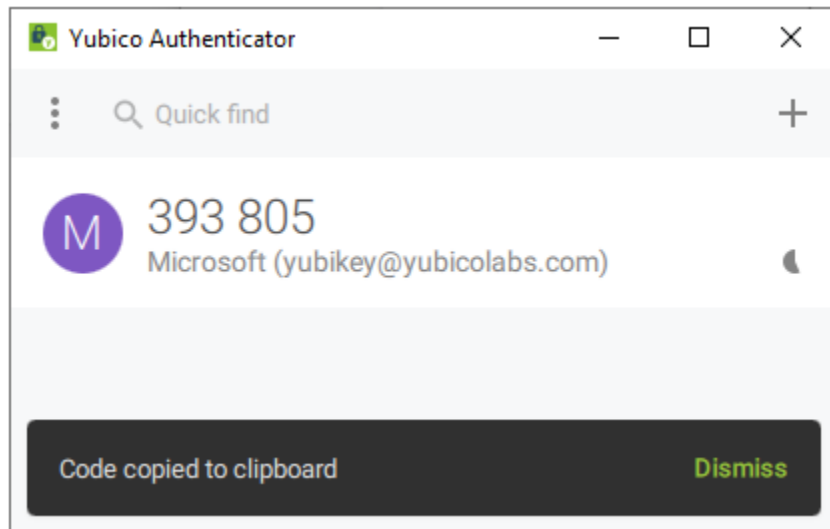


Step 9: Select **Add**.

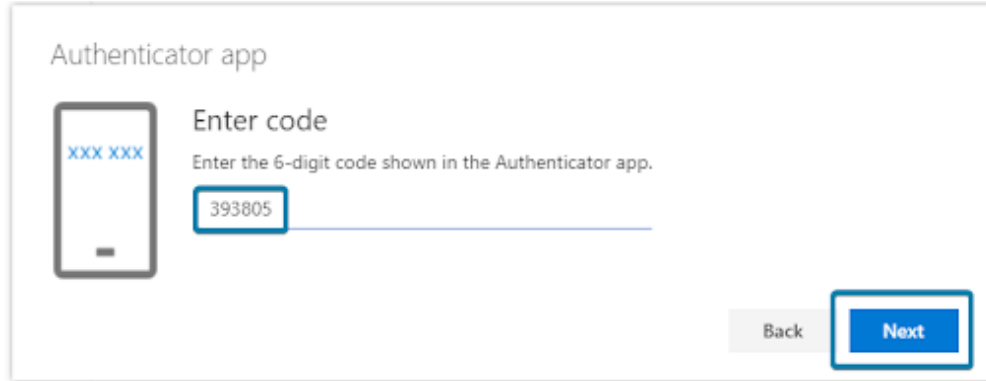


Step 10: Double-click the Microsoft entry to copy the code to your clipboard. If successful, the message displays **Code copied to clipboard**.

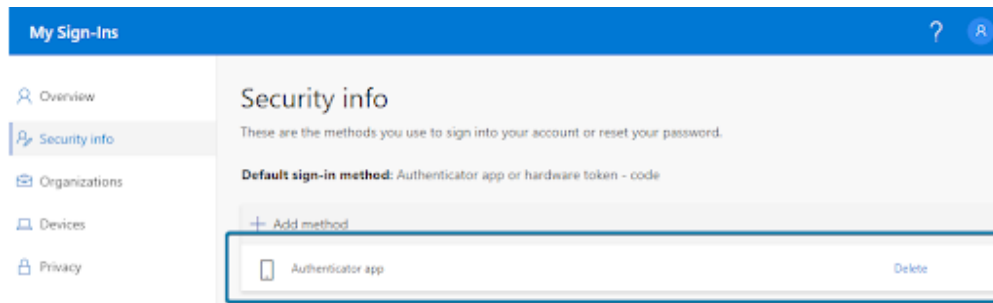
Note: if you selected Require Touch in the previous step you must touch your YubiKey to copy the code.



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!

14.3 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](#).

14.3.1 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.

14.3.2 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: zsgyzt i7z6hecscitbxz6wmt737j2dpa

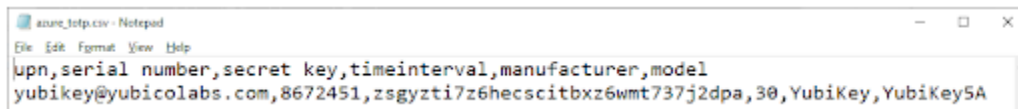
Step 5: Use 30 for the time interval.

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,zsgyzt i7z6hecscitbxz6wmt737j2dpa,30,YubiKey,YubiKey5A
```


14.3.3 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).

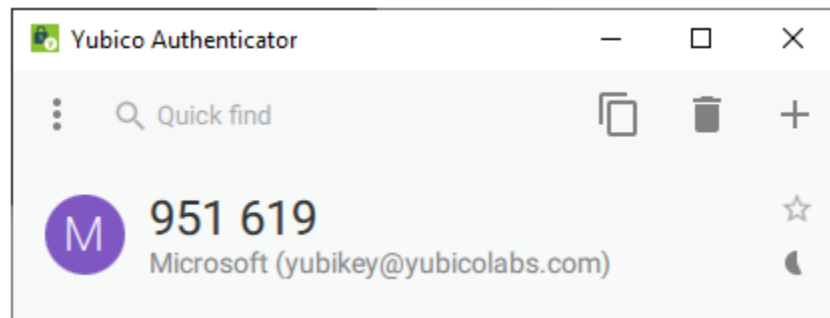
Step 3: Run the ykman command to program the YubiKey with the appropriate account name and secret from the CSV file created in the previous section.

```
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](#).

14.3.4 Upload TOTP secrets and activate the YubiKey

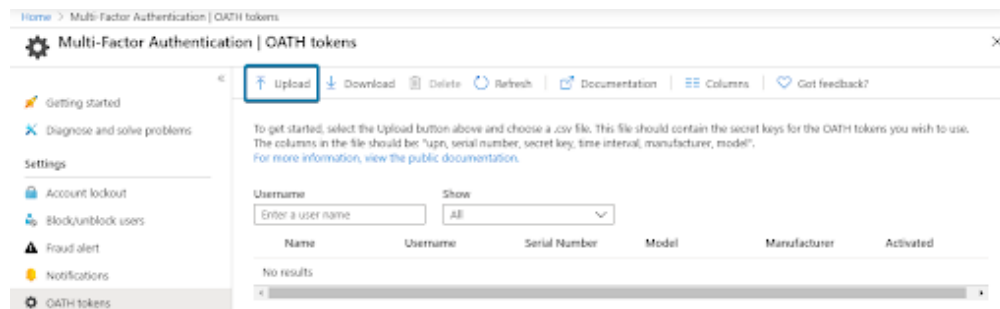
The file generated with the account and secret information needs to be uploaded to Azure AD MFA.

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.

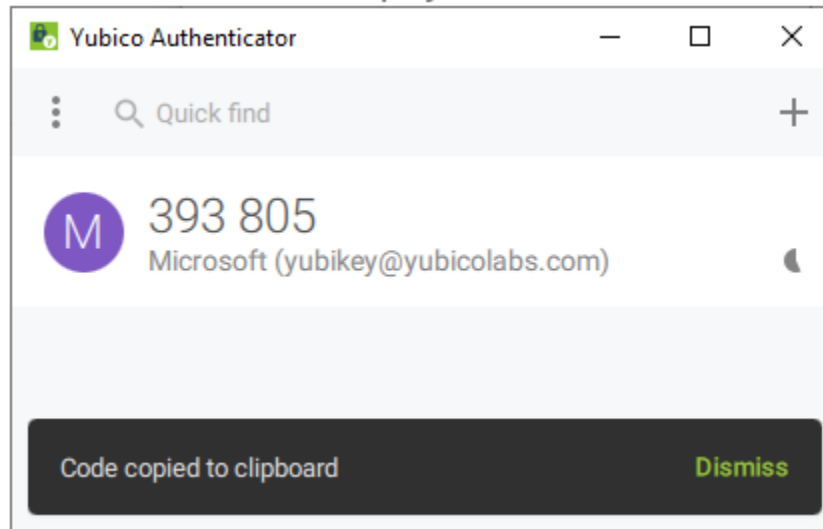
Step 6: Select **Activate** for a user.

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.

14.4 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).

14.4.1 Before you begin

- Your YubiKey will need to be registered to your Azure AD account.
- Install [Yubico Authenticator](#).

14.4.2 Website sign in

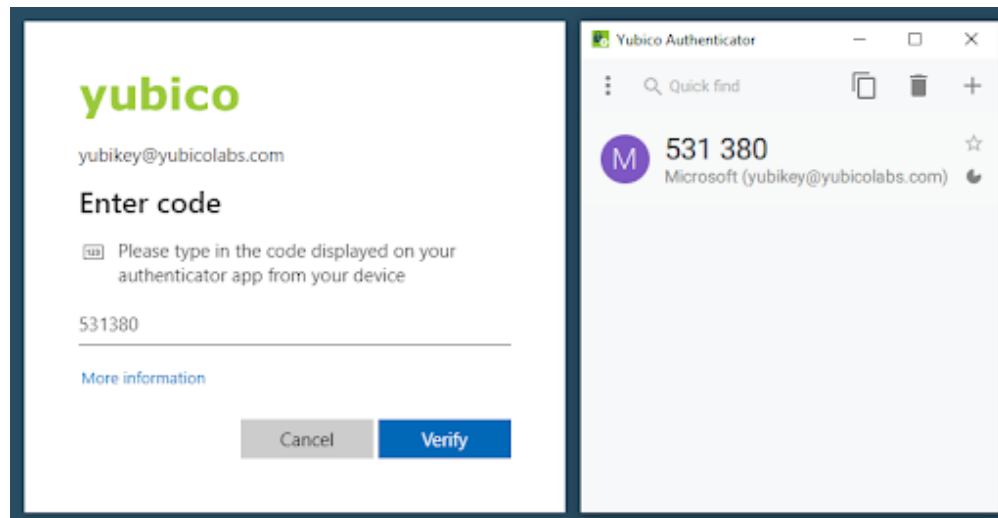
Step 1: Open the Yubico Authenticator application.

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.

14.5 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.

14.6 References

- [Azure Multi-Factor Authentication documentation](#)
- [Learn more about Yubico Authenticator](#)
- [What is OATH?](#)

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

LOG ON TO YOUR MFA ACCOUNT WITH YUBICO AUTHENTICATOR

Once you have configured your account with a service for authenticator app two-factor authentication, you must use a code generated by Yubico Authenticator when logging in to that service.

15.1 Logging on to Your Account, Service, or Website

After you have configured your account for two-factor authentication using the Yubico Authenticator, when logging in to that service you *must* use a code generated by the Yubico Authenticator.

Step 1

Launch Yubico Authenticator on your mobile device or computer.

Step 2

Log into your account or service website on the device (mobile or desktop). Enter your usual credentials: user name and password.

- You are then prompted for an authenticator code.

Step 3

Locate the authenticator code from your Yubico Authenticator.

- **Desktop:** Insert your YubiKey into your mobile device. The code is listed next to the service's identification, for example: **Issuer** (the name of the service). Double-click the authenticator code to copy it.

- **Mobile iOS Lightning port:**

- a) Insert your YubiKey 5Ci into your device's Lightning port.
- b) If the credential requires a touch verification, touch your YubiKey's sensor. For example with a YubiKey 5Ci. (See Note)

The code is listed next to the service's identification, for example: **Issuer** (the name of the service).

- **Mobile iOS NFC:**

- a) Place the Yubikey over the NFC area (pull down) to activate NFC.
- b) When prompted, scan your key.
- c) If the credential requires a touch verification, scan your YubiKey NFC again. (See Note)

The code is listed next to the service's identification, for example: **Issuer** (the name of the service).

- **Mobile Android:** Tap and hold your NFC-enabled YubiKey against the NFC antenna on the back of your phone. The code is shown next to the service's identification, for example: **Issuer** (the name of the service).
- **Note:** For generating codes set to require touch, tap the **refresh** icon next to the credential, then scan the YubiKey a second time when prompted. Touch credentials work this way over NFC because NFC does not provide enough power for the capacitive touch sensor on the YubiKey to function.

Step 4

Paste (desktop) or Enter (mobile) the code into the appropriate field on the service website or account and click **Sign In** (or similar).

TIP: In Yubico Authenticator for Desktop, you can double-click the code, and then paste it into the field for the authenticator code.

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

OATH FUNCTIONALITY WITH AUTHENTICATOR ON DESKTOPS

16.1 Protect the YubiKey's OATH Application

To further enhance the security of your YubiKey, consider adding a password to its OATH application so that no codes can be generated by the Yubico Authenticator unless that password is entered. To add a password to the OATH application, click the triple-dot icon to open the menu and expand the **Set password** section.

To use the standalone OATH functionality your YubiKey must have the CCID mode enabled, which can be done by using the [YubiKey Manager](#).

16.2 Resetting the OATH Applet on a YubiKey

Warning: Resetting the OATH Applet on a YubiKey deletes all of the OATH credentials stored on your YubiKey; this also includes Windows Hello registrations. If you are actively using these, be sure to disable the 2FA requirement for your accounts before performing these steps to ensure you do not lock yourself out of any accounts.

16.3 Steps to Reset OATH Applet

1. Download and install [Yubico Authenticator](#).
2. Insert your YubiKey to an available USB port on your computer.
3. Open Yubico Authenticator.
4. From the *File* menu, select *Reset...*
5. Click *OK* to confirm the reset.

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

SHORT CUT TO AUTHENTICATOR FUNCTIONALITY

You can generate and copy One Time Passwords (OTPs) directly from Windows' system tray or from the menu bar in MacOS. This saves you having to launch the Yubico Authenticator every time you want to use it. Just click on the Authenticator icon. The screenshots below show the icon (blown up) first as it appears when the app is inactive, and then when the app is running in the background:



Fig. 1: MacOS: Authenticator Icon Inactive



Fig. 2: MacOS: Authenticator Icon Active



Fig. 3: Windows Authenticator Icon

17.1 Integrating Authenticator Functionality

To insert **Yubico Authenticator** code generation function into a system tray (on Windows) or menu bar (in MacOS),

Step 1

Launch the **Yubico Authenticator** desktop application.

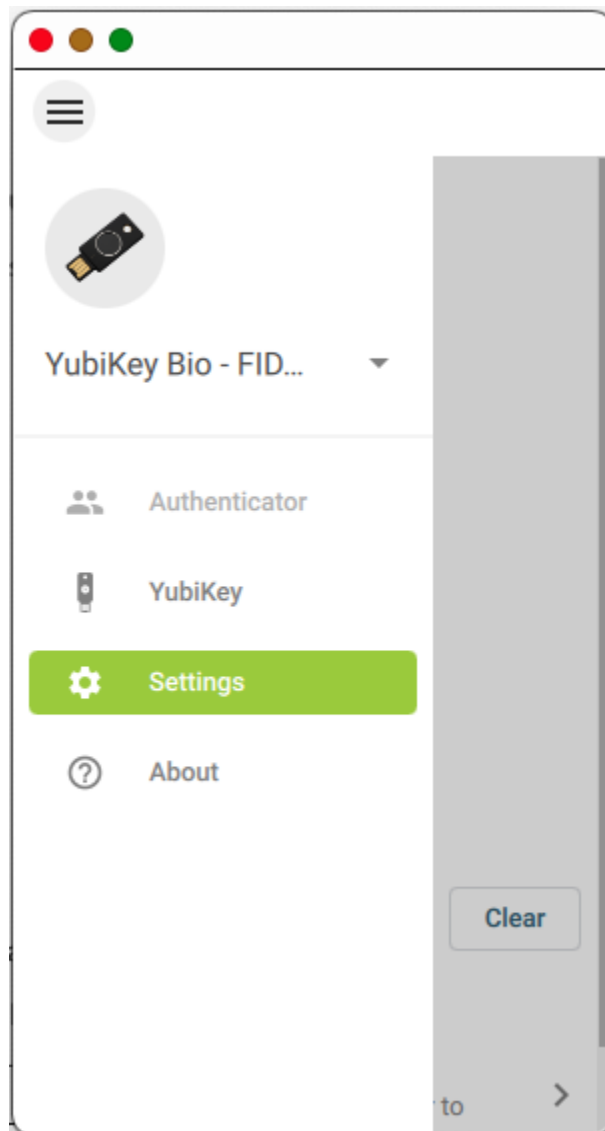
Step 2

If **Settings** is already selected, open it to the Settings window by clicking the three horizontal bars in the top left corner.

If **Settings** is not already selected, select it. The Settings window appears.

Step 3

Under **Application**, click the checkbox labeled **Show in system tray** (or **Show in menu Bar** for MacOS).



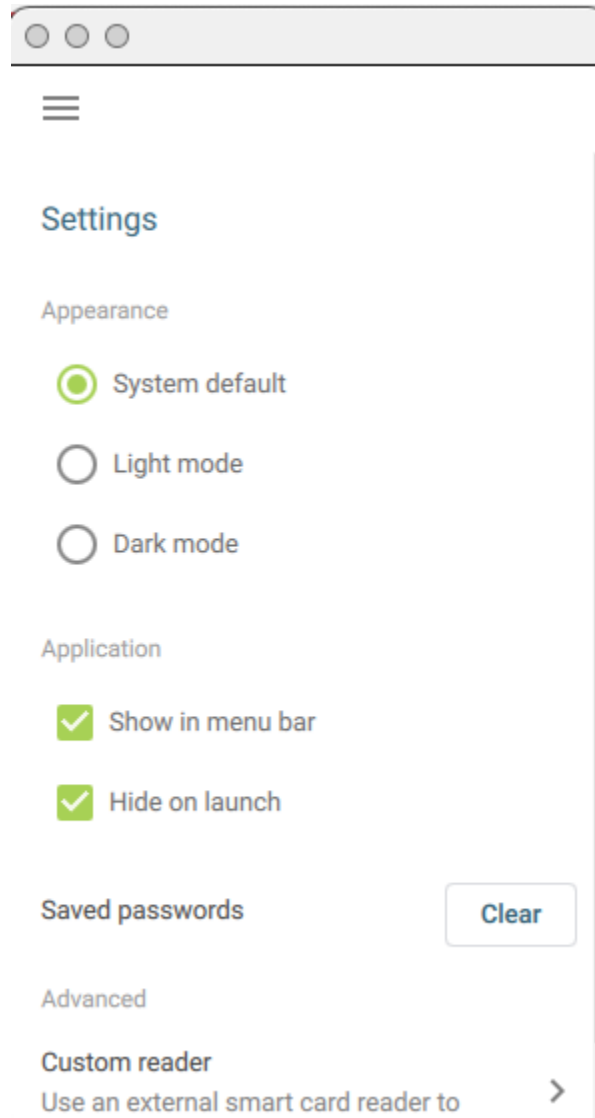


Fig. 4: MacOS: Show in Menu Bar

(Optional) The **Hide on launch** checkbox automatically minimizes Yubico Authenticator on launch, so that only the System tray or Menu bar (MacOS) icon is shown instead of the fully expanded application.

The Yubico Authenticator icon should now be displayed in the System tray (Windows) or Menu bar (MacOS).



Fig. 5: MacOS: Yubico Authenticator Icon in Menu Bar

17.2 Short Cut to Controlling Authenticator

To show the Authenticator GUI in the foreground or to close the app, right-click the Authenticator icon in the system tray or menu bar and select as desired from the menu, **Show Yubico Authenticator** or **Quit** :

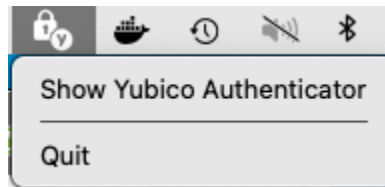


Fig. 6: MacOS: Icon Menu

17.3 Configuring Favorites

Multiple accounts can be favorited. In this example, an account has already been added to the YubiKey as described in *Setup Your YubiKey with Yubico Authenticator for Desktop*. Note that favorited accounts are *specific to the local device*. Accounts will need to be re-marked as a favorite for every instance of the **Yubico Authenticator** desktop application.

Step 1

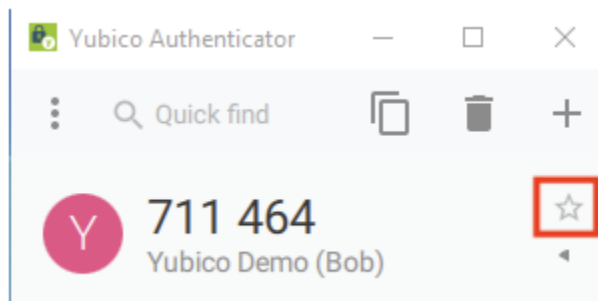
Launch the **Yubico Authenticator**.

Step 2

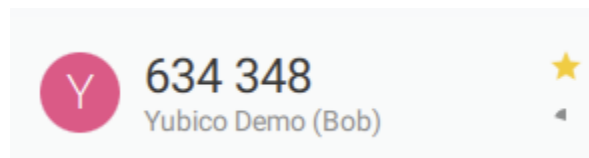
Insert the YubiKey.

Step 3

In the Yubico Authenticator GUI, mouse over the account to be favorited and click on the star outline in the top right corner.



Once an account has been set as a favorite, the star outline turns gold.



17.4 Generating OTP Codes for Favorite Accounts

The images shown below are from a sample authentication flow. Other services may have a different interface for accepting OTPs.

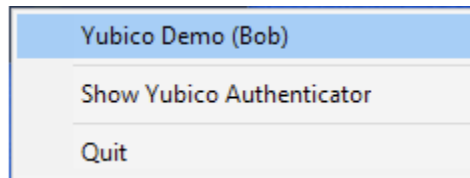
Step 1

in the System tray (Windows) or Menu bar (MacOS), right click the **Yubico Authenticator** icon.



Step 2

From the resulting pop-up, select the desired account.



Step 3

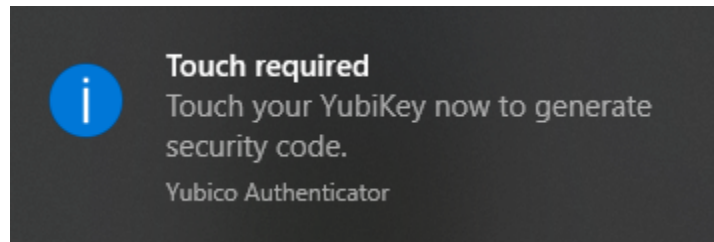
[*Optional*] The operating system prompts you to touch the YubiKey if **Require touch** was enabled during setup.

The operating system automatically copies the OTP to the clipboard.

Step 4

when prompted by the service of the favorited account, paste the copied OTP into the appropriate field on the website.

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



Get code from Authenticator

Enter code *

141873|

Tip: When storing TOTP secrets on a YubiKey the Authenticator can be used from both mobile (Android) and desktop.

NEXT

REGISTER A SPARE YUBIKEY

We at Yubico always recommend having more than one YubiKey. This way, one key can be used as a primary key, and the other can be used as a spare. There are a few ways to register a spare key, and the process is different depending on if the service supports Yubico OTP and FIDO security protocols, or OATH-TOTP protocol.

Important: Keys are not linked together in any way. Rather, both keys are registered separately to the account. That way either can be used for authentication.

18.1 Identify your service security protocols

Identify the security protocols the services you use support. Check our [Works with YubiKey Catalog](#).

18.2 Generate the QR code for the YubiKey

- If the service uses **Yubico OTP or FIDO security protocols**, register the second key exactly as you registered the first. Follow the same setup instructions listed in our [Works with YubiKey Catalog](#).
- If the service uses **OATH-TOTP protocol**, meaning you use the [Yubico Authenticator app](#) to generate codes to login, then the process is a bit different.

Important: Save this generated QR code!

Saving the QR code essential to creating a spare key for this particular account in the future. We recommend taking a picture of the QR code and storing it someplace safe.

18.3 Locate the QR code for your primary YubiKey

When registering your first YubiKey, you are given a secret from the service in the form of a QR code.

If you did not save the QR code generated the first time,

Step 1

Delete your primary key from the account.

Step 2

Restart the registration process again.

Step 3

Be sure to save the QR code generated!

See, *Using MFA Authenticator Codes with your Yubikey on Mobile Devices*. This article describes how to use your YubiKey with authenticator codes.

18.4 Link the primary YubiKey QR code with the spare YubiKey

Step 1

Use the Yubico Authenticator app, to scan the QR code from the first time you registered a YubiKey to this account.

Step 2

Scan your primary YubiKey.

This links the primary YubiKey QR code and the primary YubiKey to the account.

18.5 Create a spare key for this account

Step 1

Scan the same QR code generated from the initial registration (when you registered the primary YubiKey).

Step 2

Scan your spare YubiKey.

Now either key can be used to authenticate.

18.6 Challenge-Response services backup process

For services that use Challenge-Response, the backup process is similar to OATH-TOTP.

Step 1

Locate a backup of the secret that was programmed into your primary YubiKey.

This is required to program the same credential into your spare YubiKeys.

Step 2

If you do not have the Challenge-Response secret:

- Re-set up your primary YubiKey with the service(s) that use Challenge-Response.
- Save a copy of the secret key in the process.

Step 3

Program the same credential into your backup YubiKeys. For most configurations, you should be able to use the **Applications > OTP** menu in [YubiKey Manager](#) to accomplish this.

18.7 Static password function backup process

If you use the YubiKey's static password function, the backup process is similar to OATH-TOTP.

For static passwords, you likely do not need a backup of the original credential, but can use the YubiKey's output (the static password it "types") to program your backup key(s).

If you programmed a static password that is greater than 38 characters using the **Static Password > Advanced** menu in the [YubiKey Personalization Tool](#), in order to program it into another key you need:

- A copy of the parameters of your static password credential (public ID, private ID and secret key).
- To use the Personalization Tool.

If you do not have these parameters:

Step 1

Reconfigure your primary YubiKey and the services you use its static password with.

Step 2

Save a copy of the new parameters – if your **new** static password also exceeds 38 characters and was programmed using the **Static Password > Advanced** menu.

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

MANAGING YUBIKEYS

Yubico Authenticator provides all management capabilities for YubiKeys and Security Keys by Yubico. With the the **YubiKey Bio** in particular, you can use other methods of enrolling fingerprints and setting PINs, but only the Yubico Authenticator enables you to label your fingerprint templates and delete individual templates.

You can, of course, delete fingerprint templates by resetting the key, but that resets the key back to factory defaults, removing everything from it: all fingerprints, all credentials. To reset using a GUI, see [Resetting FIDO2 Function in the YubiKey Manager CLI and GUI Guide](#). To reset using the CLI, see [FIDO Commands](#) in the same guide.

Note: Do not click the **Clear** button visible on the main page of the Authenticator unless you mean to delete all your saved passwords.

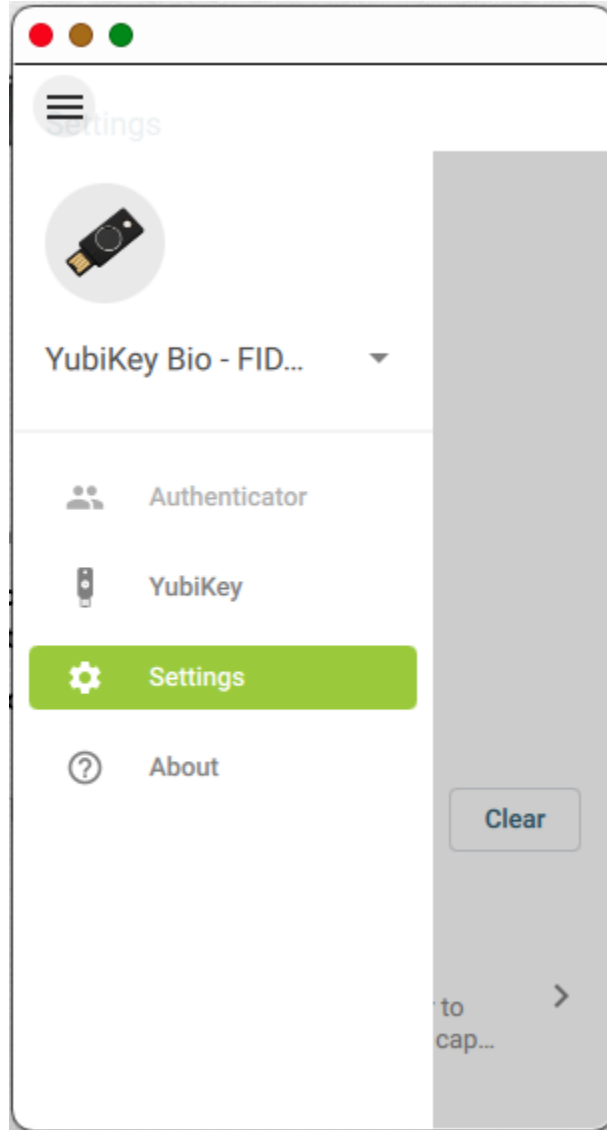


Fig. 1: Clear Button

19.1 Configuring WebAuthn/FIDO2 Capabilities

The **WebAuthn/FIDO2** screen enables you to control the way the YubiKey handles or behaves with certain aspects of this protocol and websites that implement WebAuthn.

19.1.1 FIDO2 PIN

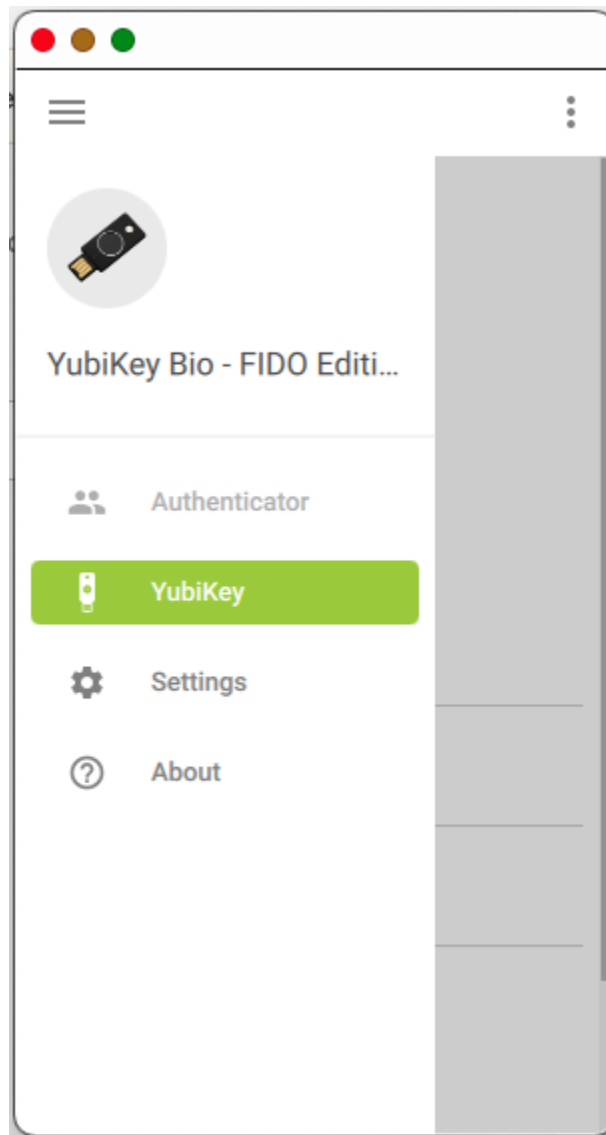
The FIDO2 PIN is the prerequisite for configuration: without a PIN, there is no management at all. For example, if a YubiKey Bio cannot read a fingerprint, entering the PIN is an easy workaround. It should be noted that PINs in general, and the FIDO2 PIN in particular are a topic unto themselves, and understanding some PIN basics will save you a lot of troubleshooting. For more details, see Yubico's knowledge base article [Understanding YubiKey PINs](#).

Deleting credentials can be important to ensure personal safety.

To set and manage the PIN, enroll fingerprints and manage stored credentials,

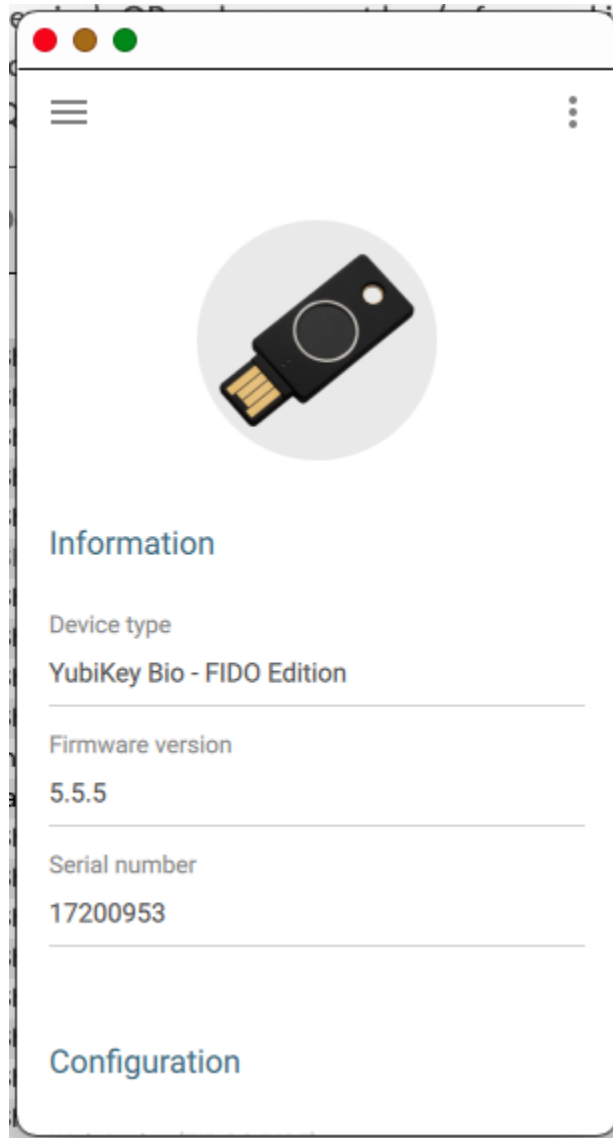
Step 1

Launch the Yubico Authenticator, and select the YubiKey menu option. The Information window appears.



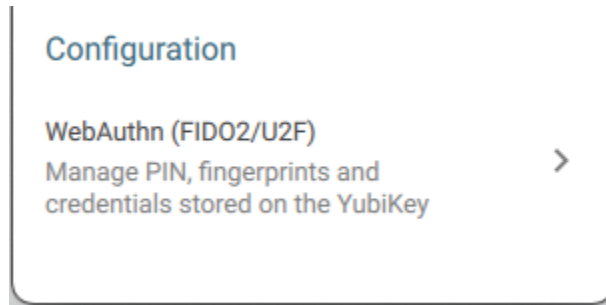
If the YubiKey menu option is already selected, click the three dots or the **X** on the upper right.

The Information window appears.



Step 2

Scroll down *past* the word **Configuration** to reveal the WebAuthn (FIDO2/U2F) option:

**Step 3**

Click the little caret to the right. The WebAuthn (FIDO2/U2F) screen appears.

19.2 PIN Protection

19.2.1 Managing the FIDO2 PIN

Because the PIN is the principal credential, it must be set at the start of configuration. The **PIN protection** menu option on the WebAuthn (FIDO2/U2F) screen enables you to set or change the PIN.

If you have previously set a PIN that you cannot remember, you have eight tries before the key locks up. Once the key is locked, your only option is to reset it. [Use the YubiKey Manager to reset the PIN.](#)

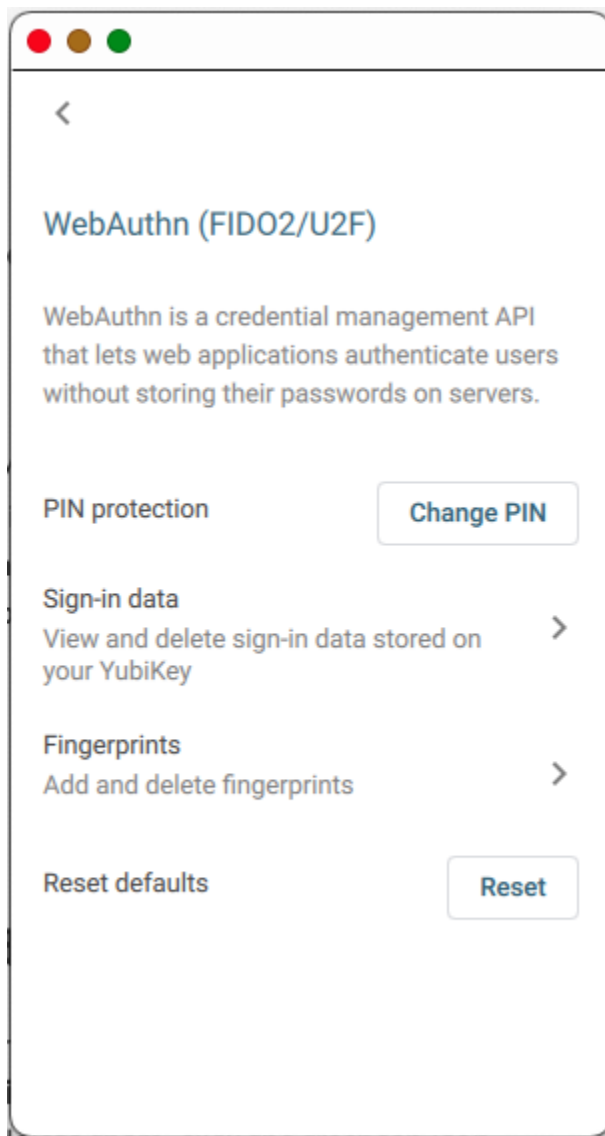
Note: For all the details on YubiKey PINs in general (not just FIDO2 PINs), see our comprehensive knowledge-base article, [Understanding YubiKey PINs](#).

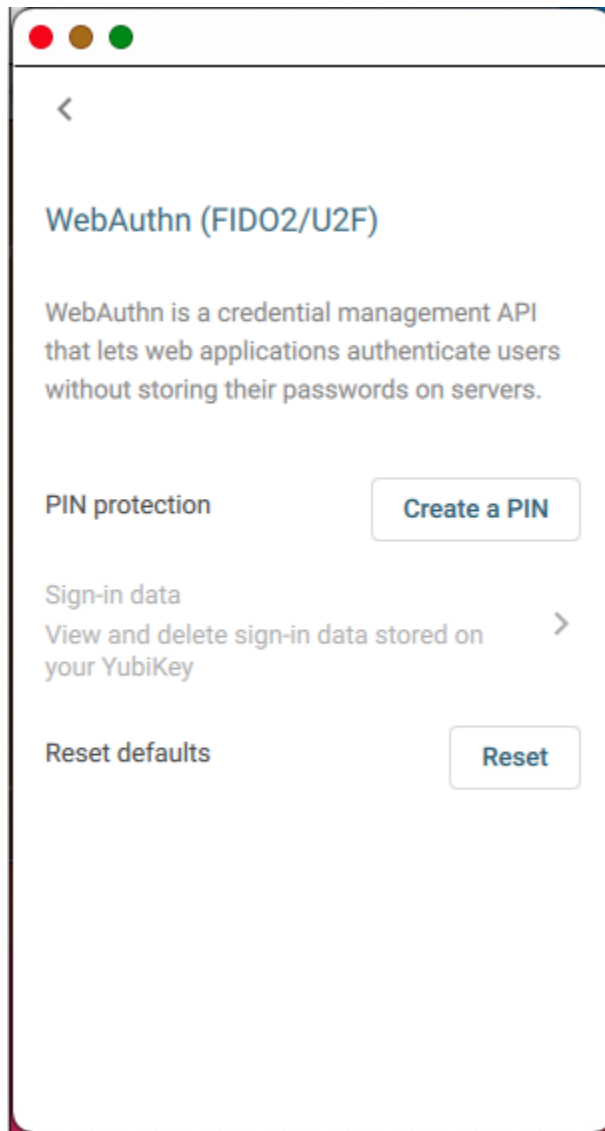
19.2.1.1 Setting the PIN

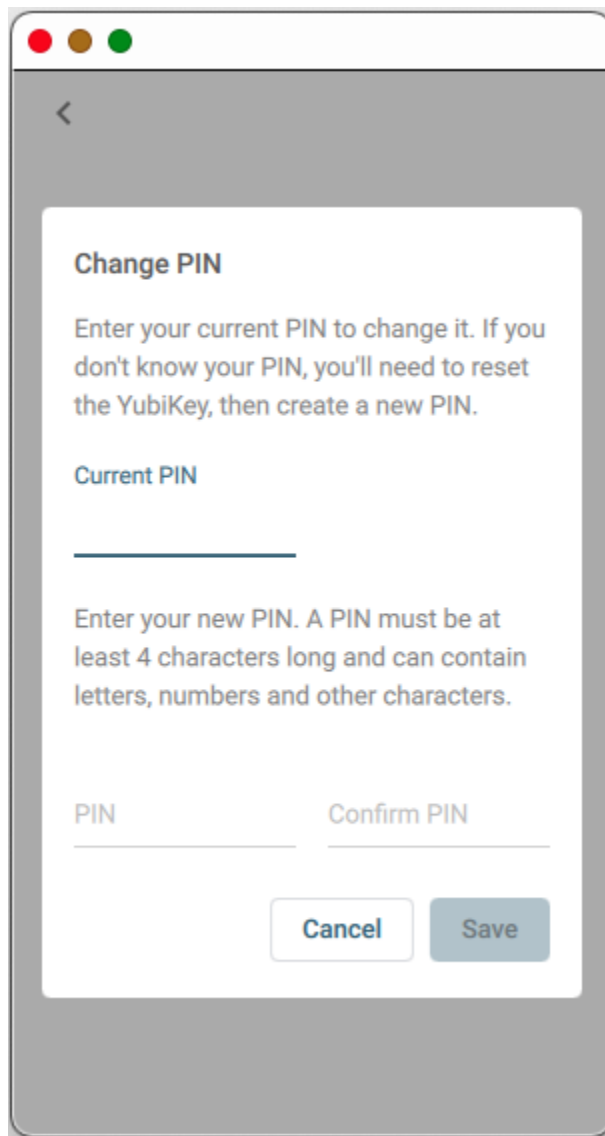
Select **YubiKey**, then the > to the right of **Configuration**, and finally, on the WebAuthn (FIDO2/U2F) screen, **Create a PIN**. You are prompted to enter and confirm a PIN with four alphanumeric characters at minimum.

19.2.1.2 Changing the PIN

Select **YubiKey**, then the > to the right of **Configuration**, and finally, on the WebAuthn (FIDO2/U2F) screen, **Change PIN**. You are prompted to enter the current PIN. If you do not know it, you must [reset the YubiKey](#) before you can change it.







19.3 Sign-in Data

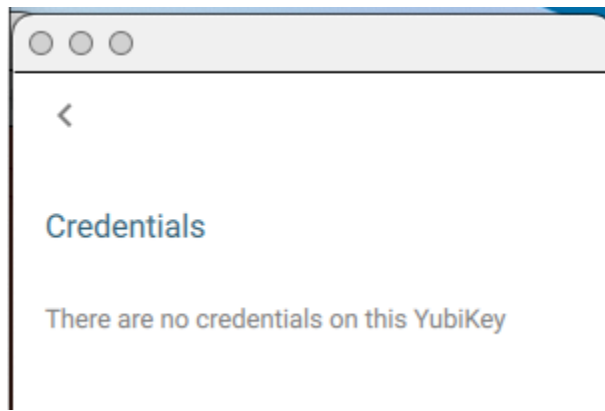
19.3.1 Viewing, Labeling, and Deleting Individual Credentials

Credentials include the sites with which the key is registered. Deleting the evidence that you have used sites or services can be essential in some situations.

To view any credentials stored on the key, to label fingerprint templates, and to delete individual credentials (including templates),

Select **YubiKey**, then the > to the right of **Configuration**, and finally, on the WebAuthn (FIDO2/U2F) screen, the > to the right of **Sign-in data**. On the **Credentials** screen,

If it is a new YubiKey, there will be no credentials listed.



If there are credentials of any sort stored on the key, you are prompted to enter the PIN before you can view them:

If it is a YubiKey Bio with fingerprints enrolled, the templates will be listed.

To label a fingerprint template, click the Edit icon.

19.4 Fingerprints

19.4.1 Managing Fingerprint Templates

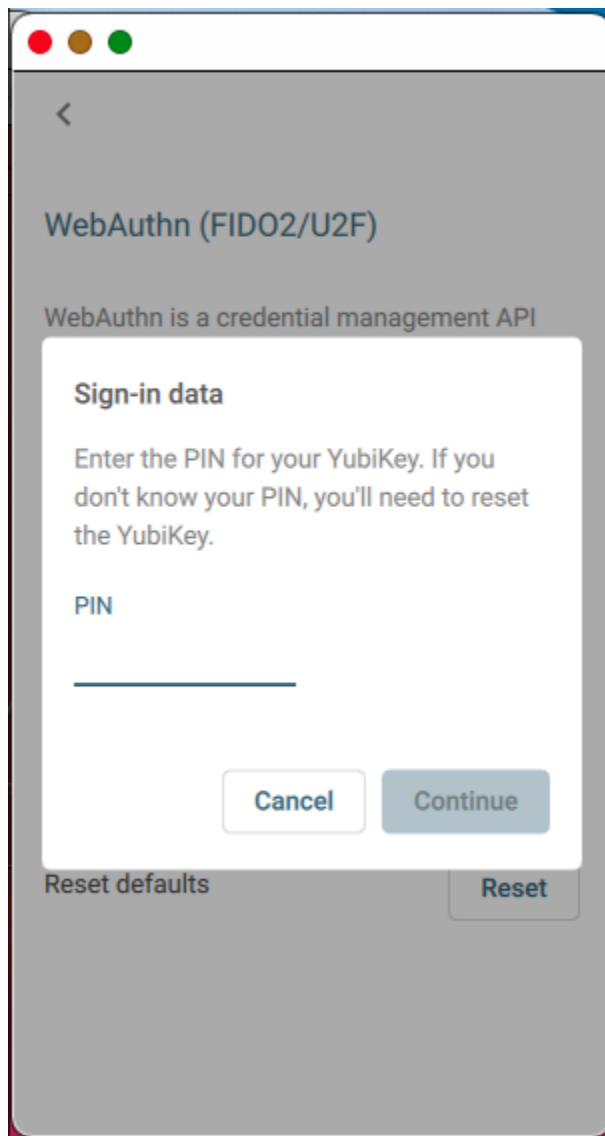
This section is relevant only to the YubiKey Bio. Before fingerprints can be used to authenticate to any site or service, they must be enrolled on the key, which records them as templates (for details, see the [Technical Manual](#) for the YubiKey Bio).

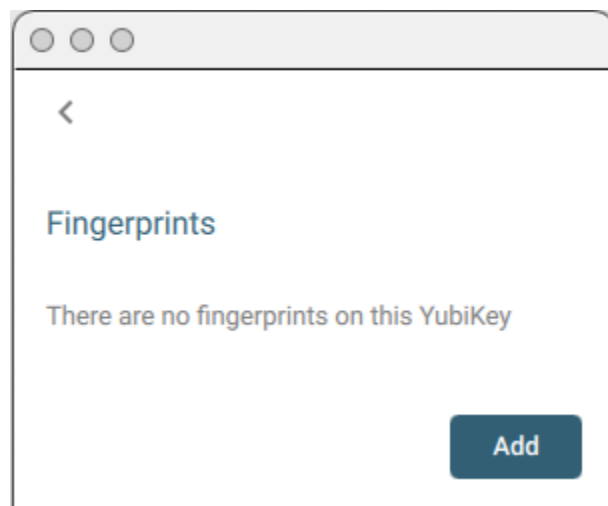
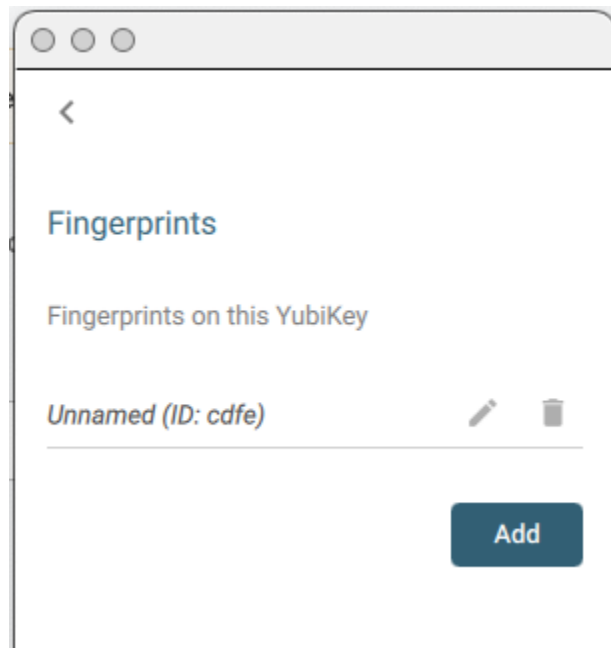
19.4.1.1 Enrolling Fingerprints

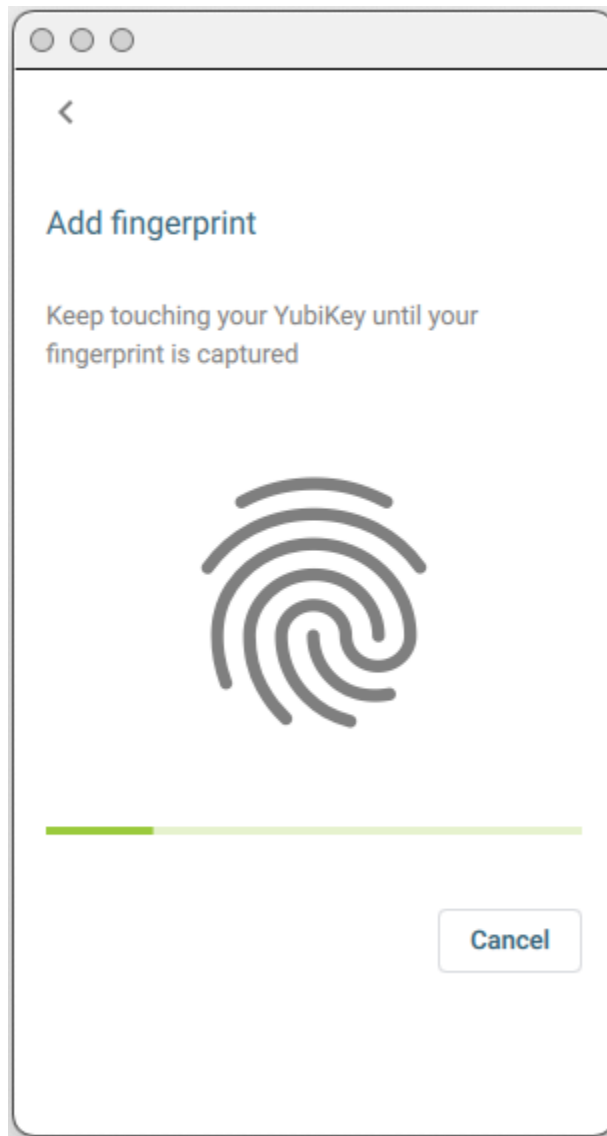
To enroll a fingerprint on the YubiKey Bio, select **YubiKey**, then the > to the right of **Configuration**, and finally, on the WebAuthn (FIDO2/U2F) screen, the > to the right of **Fingerprints**. The **Fingerprints** screen appears. Click **Add**.

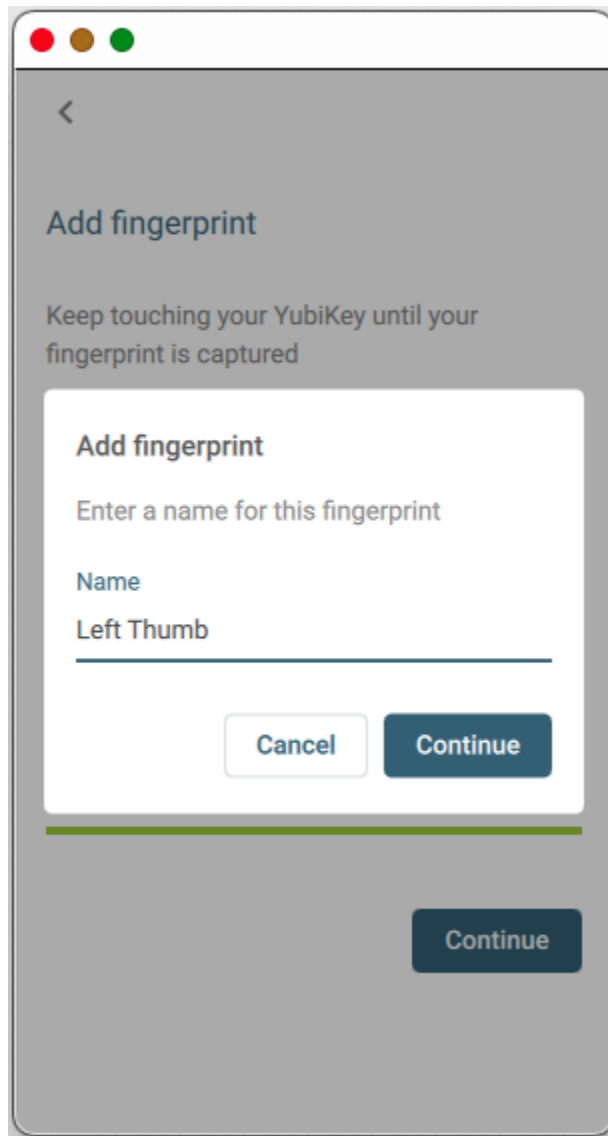
When the Add Fingerprint screen appears, apply your fingerprint to the sensor, touching the bezel ring as well. Lift and repeat, changing the angle of pressure slightly each time so that the key can read the full print. The progress bar below the fingerprint icon shows how much of your print has been read.

When the key has captured the full print, click **Continue**. You are prompted to label the template. It will not be saved unless you label it.





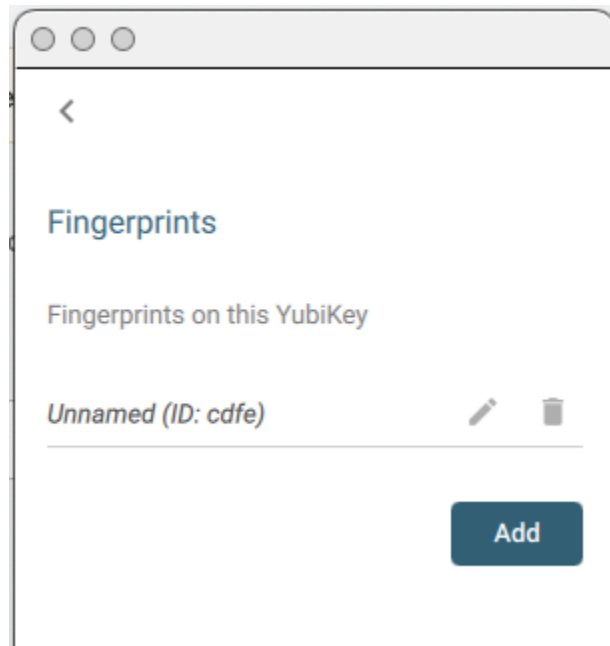




Add more fingerprint templates up to a total of five (5).

19.4.1.2 Labelling Templates

If you use the Yubico Authenticator to enroll fingerprints, you are obliged to label them. However, if you use other means, such as Yubico's [YubiKey Bio start page](#), the templates have automatically assigned IDs that are seldom intuitive:



To label such a template, on the **Fingerprints** screen, click the edit icon next to the unnamed template.

19.5 Reset Defaults

Completing this procedure involves several steps.

To return your YubiKey to its factory default condition, with no FIDO2/U2F sign-in data (credentials), no PIN and no fingerprints (if applicable), click **Reset**.

You are prompted to unplug your YubiKey.

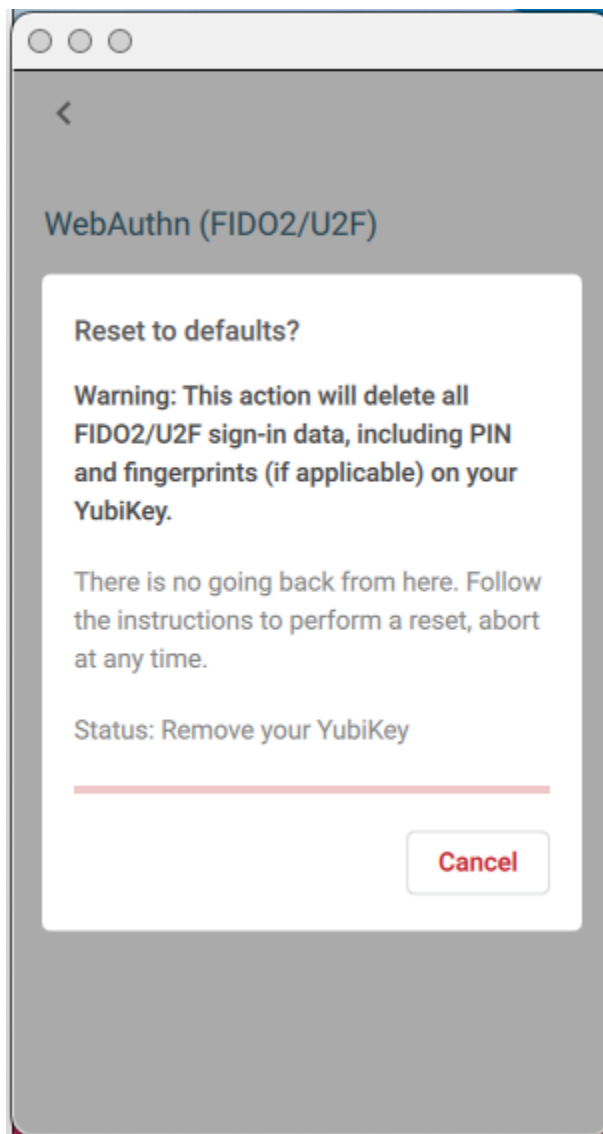
The status bar above the **Cancel** button shows the progress of the operation. The reset is not complete until the bar is entirely red, and the **Cancel** button turns into a **Continue** button.

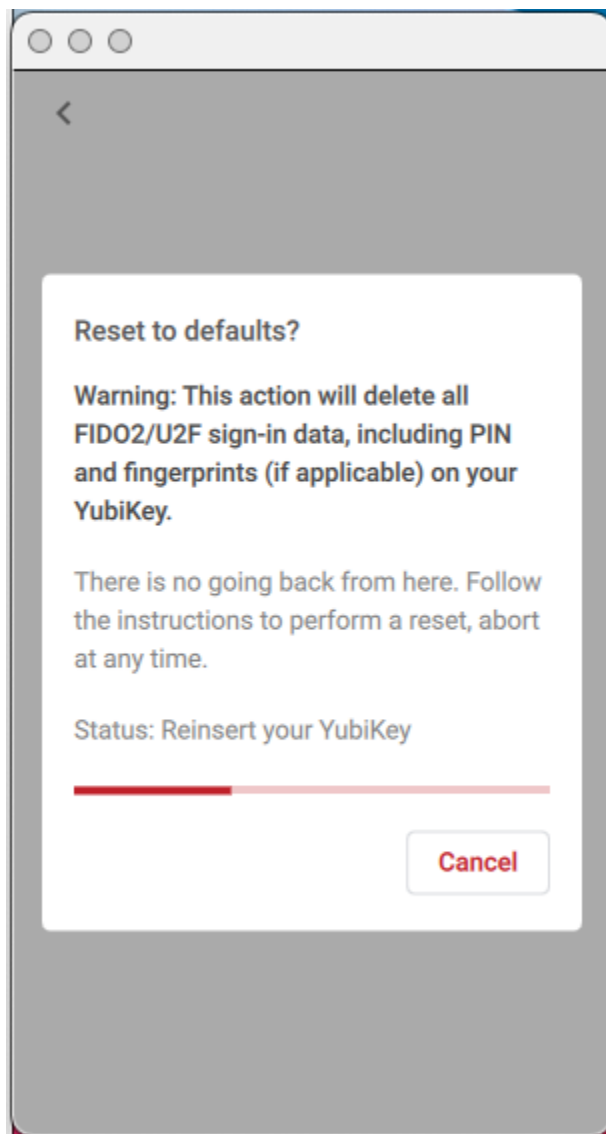
When prompted, reinsert your YubiKey.

When prompted, touch the YubiKey (on a YubiKey Bio, touch the sensor) to finish the reset.

Note: To authenticate with sites and services to which you have previously registered using this key, you will need to register the key again, because it will not be recognizable as the same key.

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





YUBICO AUTHENTICATOR TROUBLESHOOTING

Important: Do not click the **Clear** button visible on the main page of the Authenticator unless you mean to delete all your saved passwords.

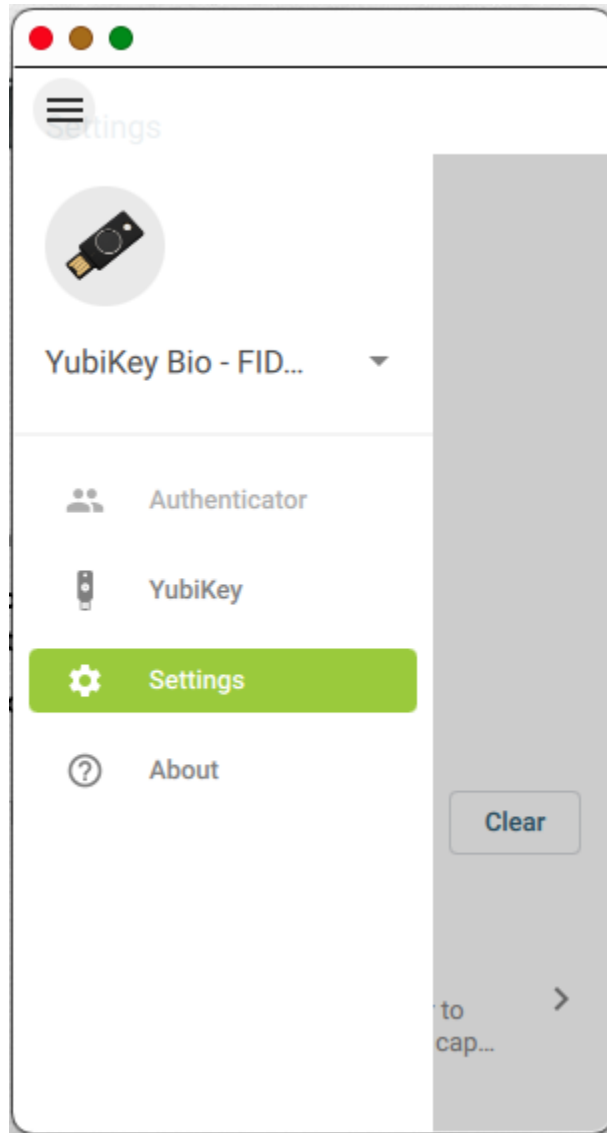


Fig. 1: Clear Button

20.1 Wrong/Incorrect Codes from Yubico Authenticator

Yubico Authenticator generates time-based one-time passwords (or passcodes or just codes) (TOTPs) as per the OATH-TOTP standard. If the codes being generated are being rejected as incorrect, it is probably because the clock is wrong on the device running Yubico Authenticator. Reset the clock by following the instructions for that operating system or device: for an example, see the [knowledge base article on this topic for a Dell computer](#).

20.2 Password-protecting the YubiKey's OATH Application

Note: OATH-related information is not relevant to the YubiKey Bio, which uses the FIDO protocol.

To further enhance the security of your YubiKey, consider adding a password to its OATH application. This will result in the password being required before codes can be generated with Yubico Authenticator. To add a password to the OATH application:

- In Yubico Authenticator for desktop:
 - Click the triple-dot button to open the menu and expand the section **Set password**.
- In Yubico Authenticator for iOS:
 - Tap the gear button to open the menu, and tap **Set password**.
- In Yubico Authenticator for Android:
 - Scan or insert your YubiKey, tap the triple-dot button, then tap **Change password**.

20.3 Backing up Accounts

While it isn't possible to back up accounts from the YubiKey itself, it is possible to back up the piece of information provided by each service provider, and then use that to program the same account (or credential) onto multiple YubiKeys.

To back up your access to your accounts:

1. When you first set up a service with Yubico Authenticator, take a screenshot of the QR code (or make a copy of the secret key) provided by the service. Do this for every service.
 2. Complete setting up your primary YubiKey using this QR code or secret key.
 3. Use that to program the same account or credential onto multiple YubiKeys. See *Setup Your YubiKey with Yubico Authenticator for Desktop*, step 5 in particular.
-

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

YUBICO AUTHENTICATOR WITH SMART CARDS 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.

21.1 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.

21.2 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.

21.3 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)

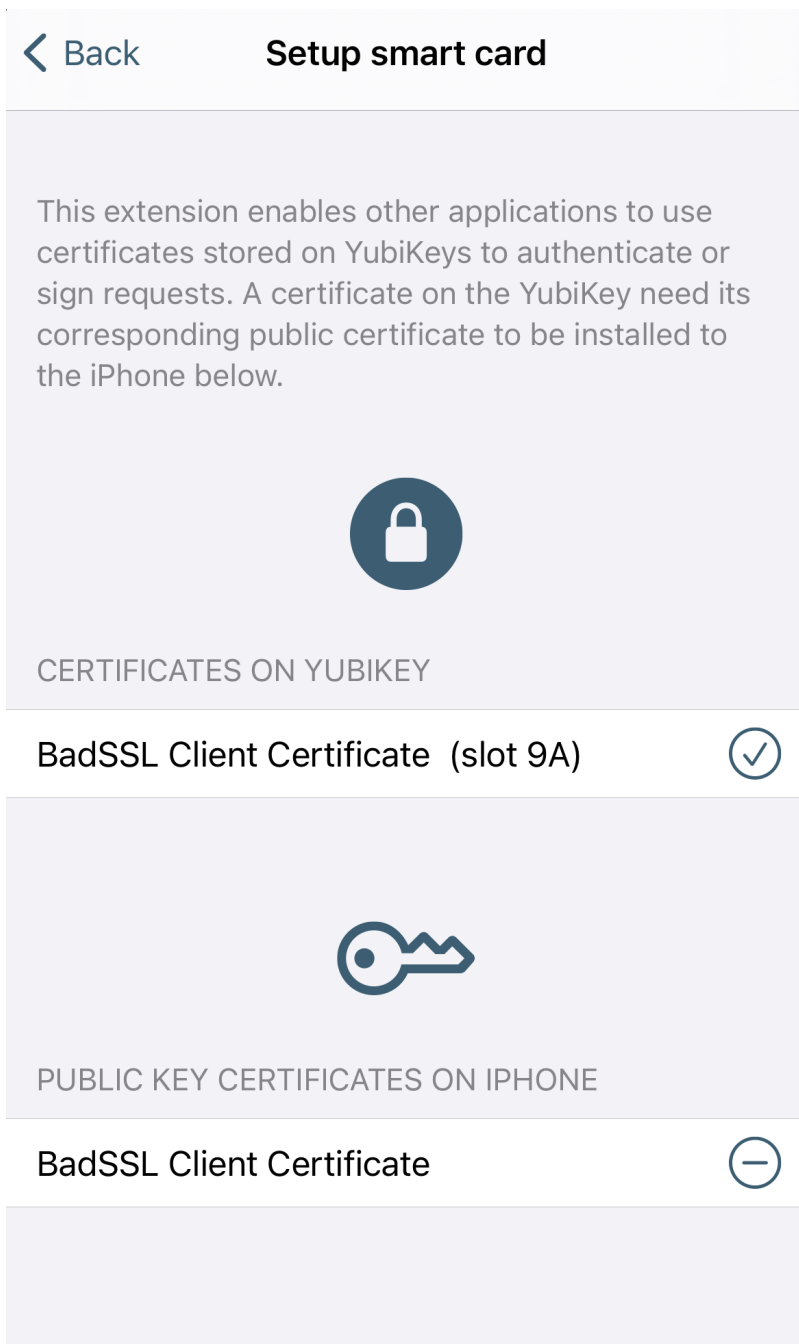
Issuer: BadSSL Client Root Certificate Authority [Delete](#) [Export](#)

Subject name: BadSSL Client Certificate [Generate](#) [Import](#)

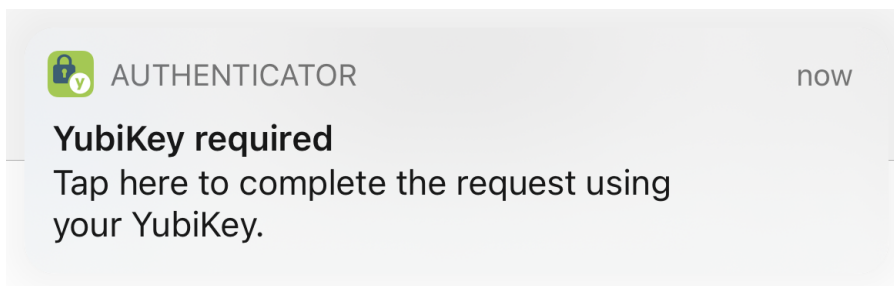
Expiration date: 2021-11-26

[Back](#)

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



3. *Authenticate to the website that requires your smart card certificate on the Safari browser.*



21.4 Troubleshooting

If you run into issues using the Smart Card on iOS feature, check out the *Yubico Authenticator Smart Card 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.

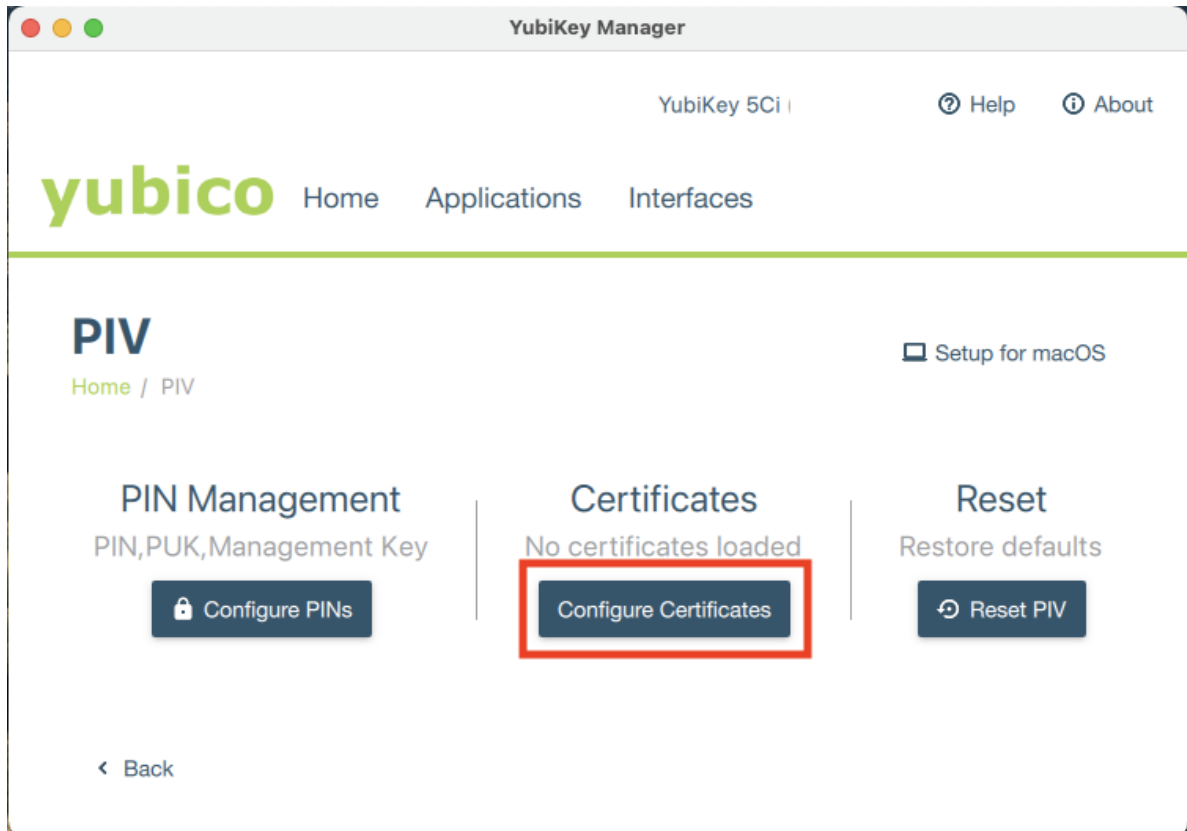
Follow the steps detailed below to import your smart card certificates onto your YubiKey using your preferred version of YubiKey Manager.

If you already have your smart card certificate stored on your YubiKey, skip to the next section: *Smart Card Certificate Provisioning with Yubico Authenticator*.

22.1 YubiKey Manager GUI

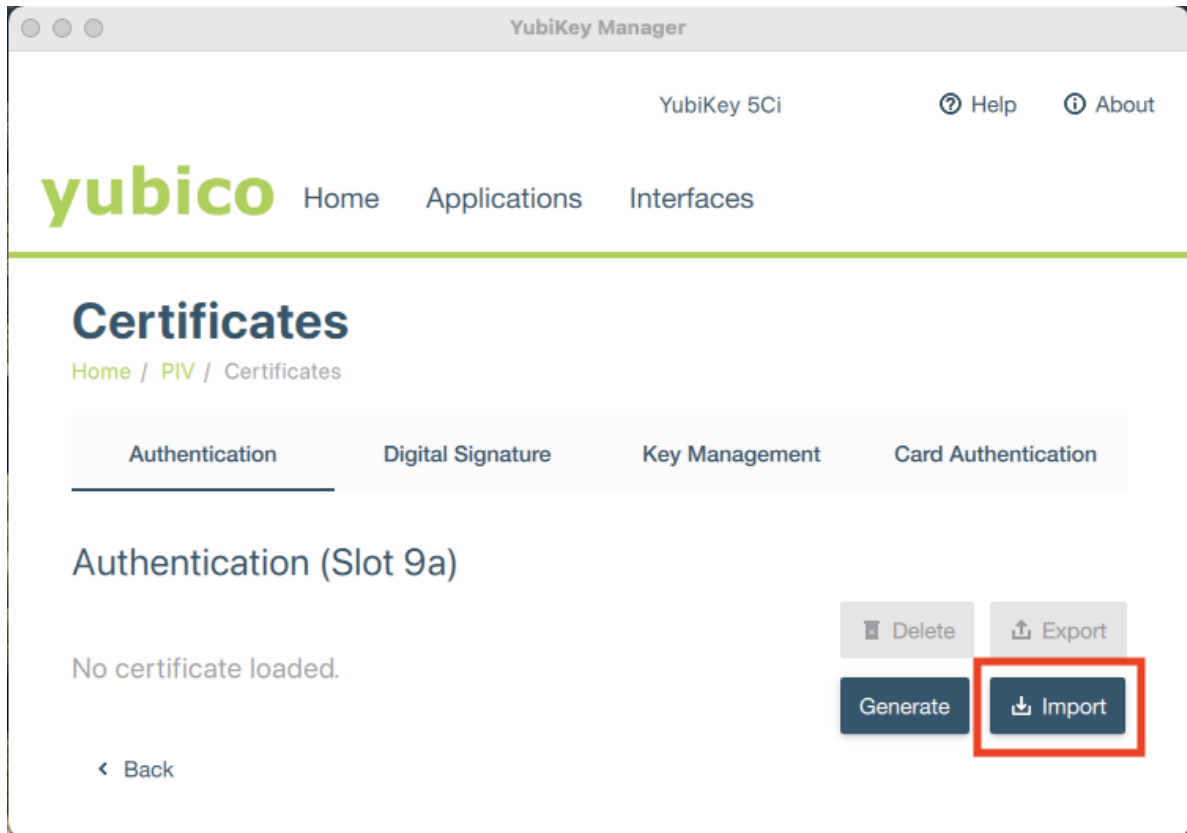
To use the GUI version of YubiKey Manager to import your certificate, follow the steps below:

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.

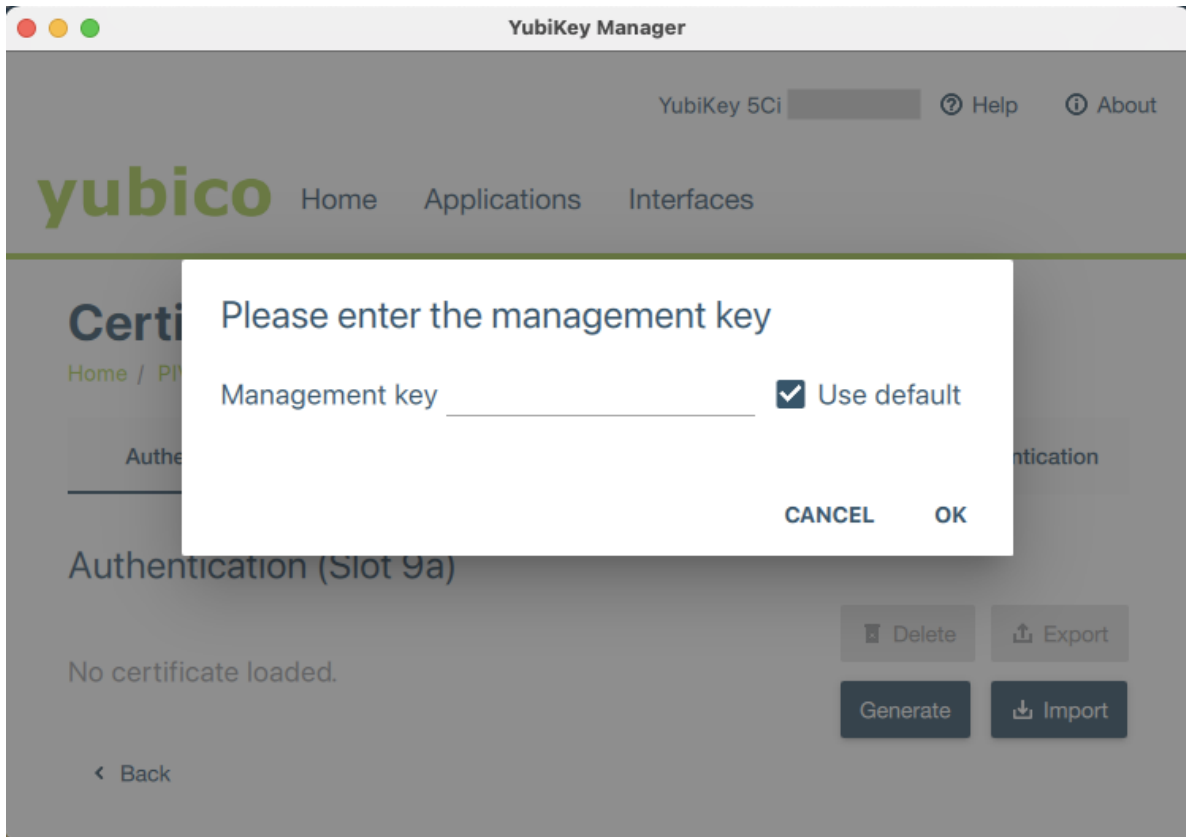
Remember, the public certificate AND its private key must be imported onto your YubiKey. While the YubiKey can store any X.509 certificate of the PEM, DER, and PKCS12 format, we recommend using the PKCS12 file type (which have .pfx or .p12 file extensions) because the public certificate and private key are stored in a single file.

7. When prompted, enter the certificate's password and click **OK**.

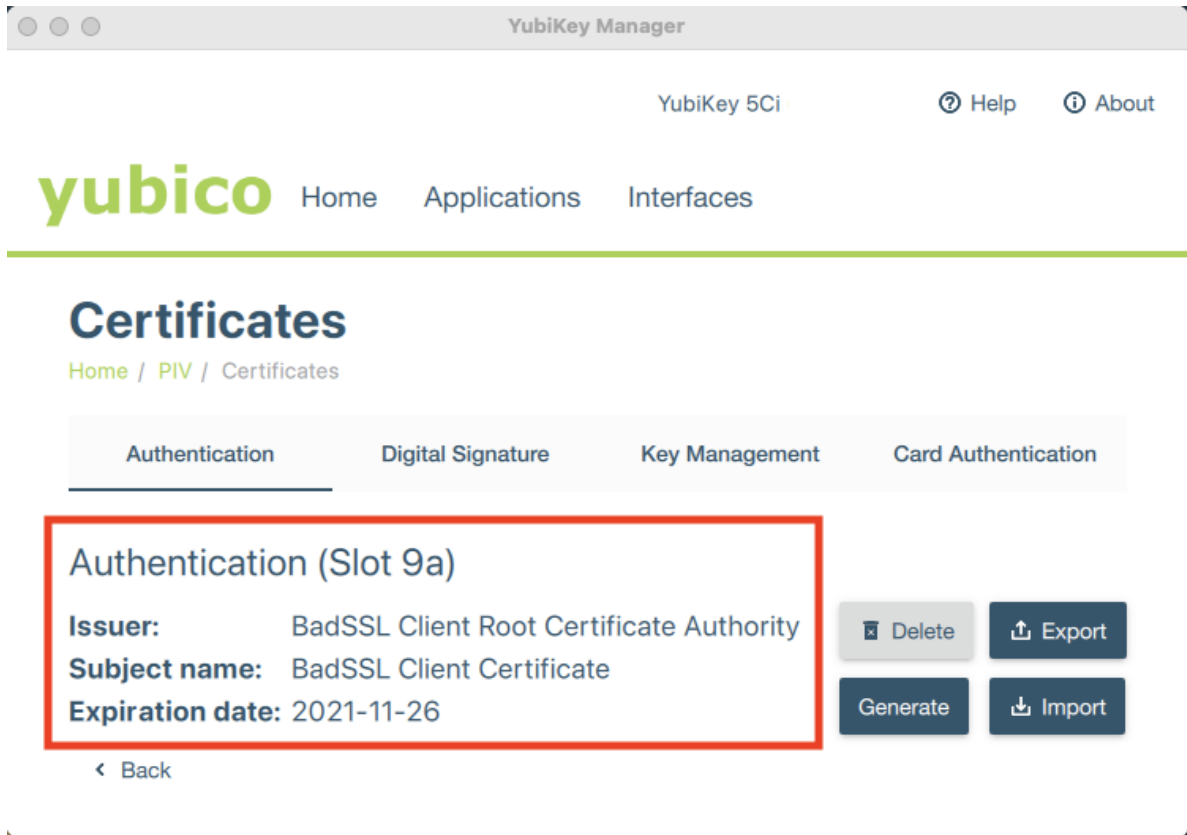
Note: If you do not know your certificate's password, check with your admin (if applicable) or the certificate provider.

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.

22.2 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.

22.3 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.

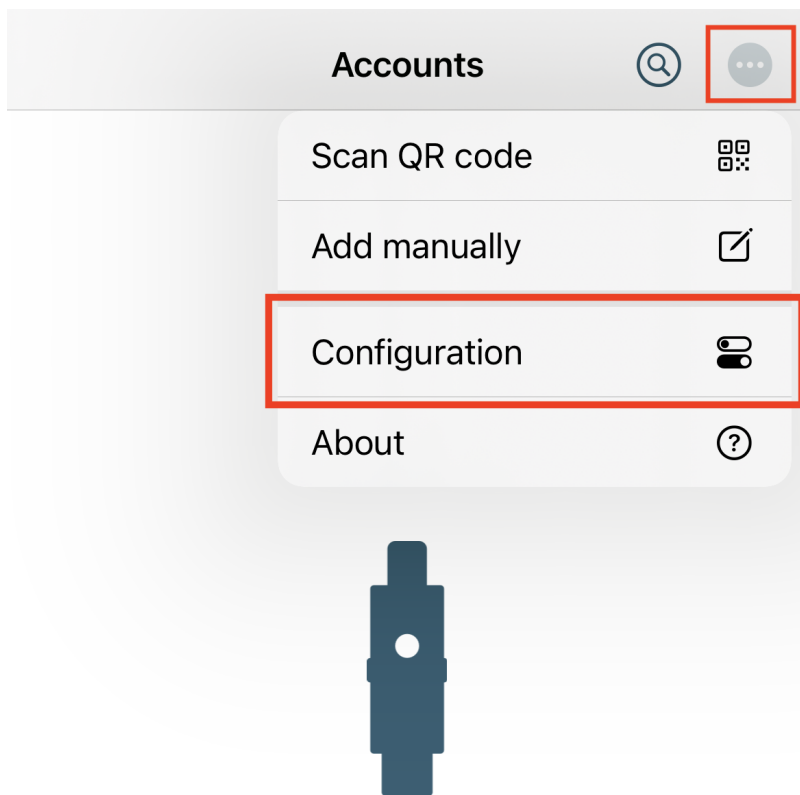
To file a support ticket with Yubico, click [Support](#).

SMART CARD CERTIFICATE PROVISIONING WITH YUBICO AUTHENTICATOR

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.

23.1 Provision Your Public Certificate

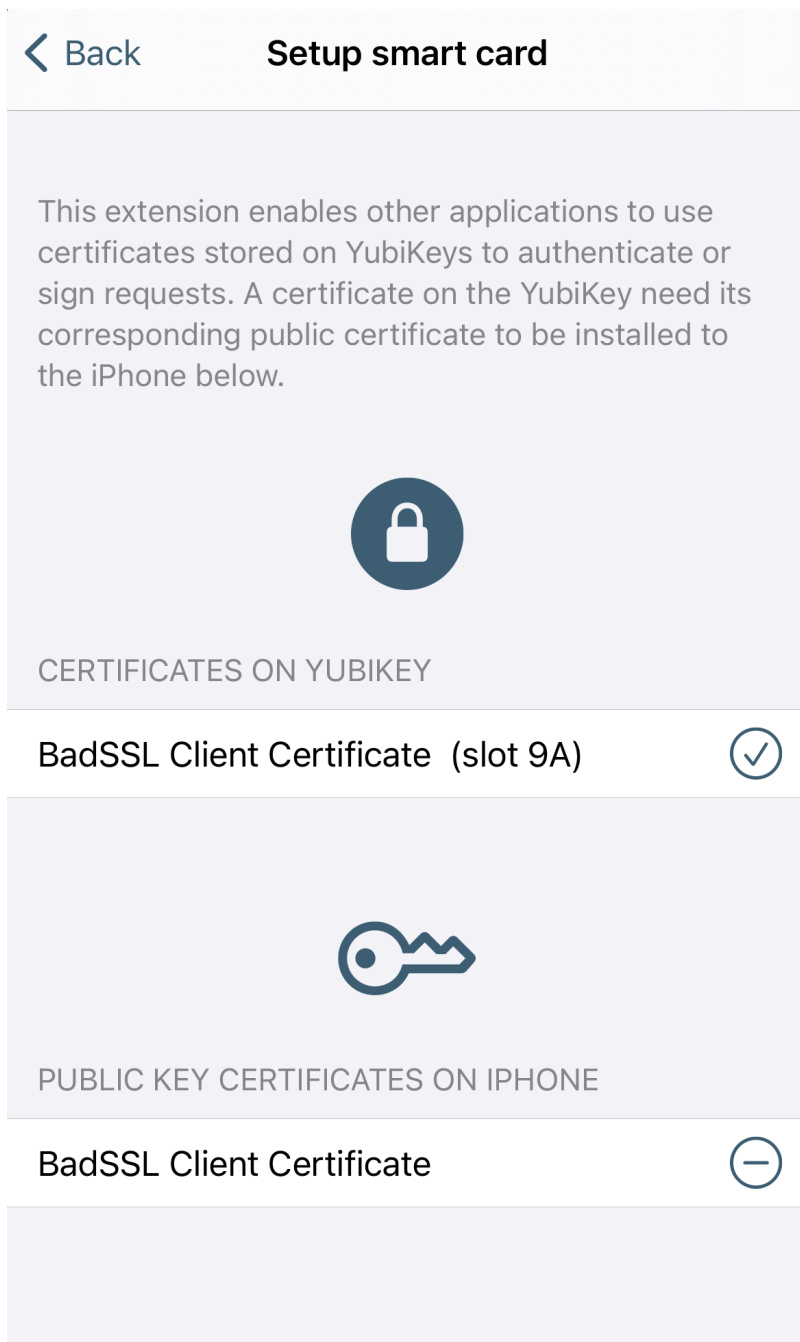
1. If you haven't already, [download and install the Yubico Authenticator application](#) (v.1.6 or newer) onto your iOS device.
2. Open Yubico Authenticator.
3. On the home screen of Yubico Authenticator, click on the three dots (...) in the upper right corner of the screen and select **Configuration**.



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.



23.2 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](#).

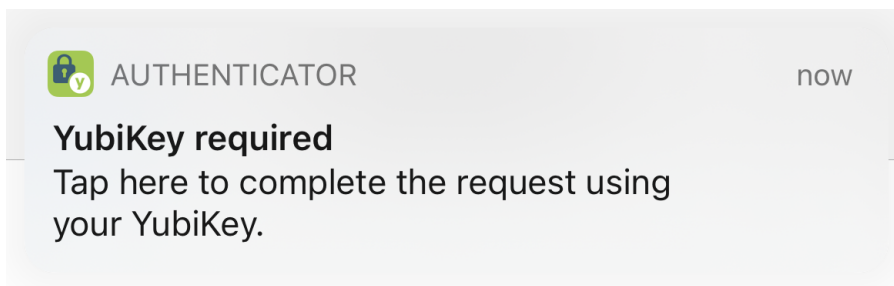
AUTHENTICATING WITH SMART CARD ON IOS

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.

24.1 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](#).

YUBICO AUTHENTICATOR SMART CARD TROUBLESHOOTING

Running into issues using the Smart Card on iOS feature? Check the guidance below for possible solutions.

25.1 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.

25.1.1 Toggle Focus Modes Off

To toggle your Focus modes off, do the following:

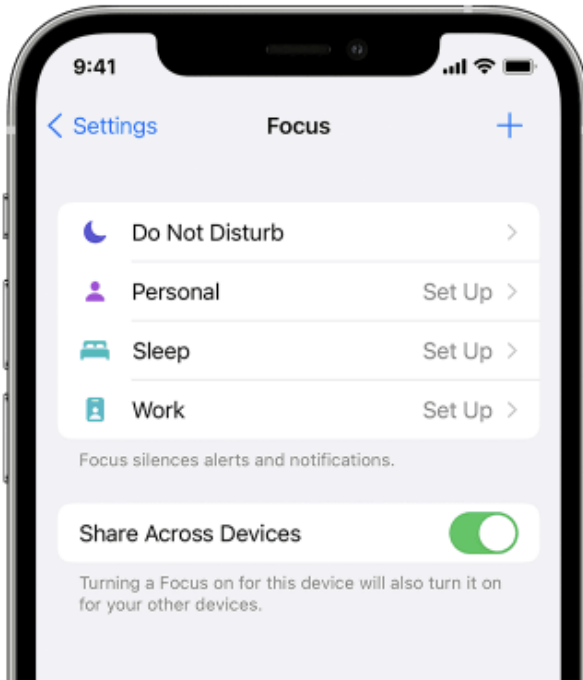
1. Open your [Control Center](#).
2. Select the Focus icon and toggle all modes to the off position.



25.1.2 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](#).

© 2023 Yubico AB. All rights reserved.

26.1 Trademarks

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

26.1.1 Disclaimer

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

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

26.1.2 Contact Information

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

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

26.1.3 Document Updated Date

2023-03-01 20:06:24 UTC