yubico

Reviewer's Guide: Security Key NFC

Security Key NFC by Yubico

Welcome to the Security Key NFC Reviewer's Guide!

Now that you are the proud owner of a Security Key NFC by Yubico, we've put together a quick-start guide to help you make the most of your key and take advantage of all its features. Please carefully review each section below and if you have any questions, please reach out to press@yubico.com for further assistance.

Step 1: Learn more about the Security Key NFC

Step 2: Confirm device and system requirements

Step 3: Set up your key for use via USB

Step 4: Set up your key for use with your mobile platform

Step 5: Login with peace of mind!

Step 1: Learn more about the Security Key NFC

The Security Key NFC retails for $27 and is available for purchase at Yubico.com or Amazon.com. At a low price point, this makes the Security Key NFC a cost-effective solution that will deliver seamless access to many of the most popular online accounts over both a USB and NFC connection.

The Security Key NFC is the perfect hardware authentication solution for consumers as well as enterprise users who are looking to add protection to their most popular online accounts.

The Security Key NFC supports two different authentication protocols to help eliminate account takeovers: FIDO U2F and FIDO2/WebAuthn. Authentication is available over both a standard USB-A connection as well as a near field communication (NFC) connection for a mobile tap-and-go experience. With the option of multiple communication methods, and with support for both FIDO U2F and FIDO2/WebAuthn, this one key is able to deliver a simple and seamless user experience across multiple devices for strong multi-factor, two-factor (2FA), and single-factor passwordless authentication.

The addition of NFC to the Security Key is critical to enable strong, yet simple, authentication for mobile users. With billions of stolen passwords and usernames available on the black market, and rampant phishing scams, secure logins are a must-have feature on mobile.

The Security Key NFC works out of the box with any service that supports the FIDO U2F or FIDO2/WebAuthn protocols including: Google, Microsoft accounts, Dropbox, Facebook, Twitter, GitHub, Dashlane, Keeper Security, and more. Refer to the Works with YubiKey catalog for a full list of services that support the YubiKey. Just register your key with the desired service, and from that point on you will be asked to present your key at the time of login.

It's important to note that while FIDO U2F and FIDO2/WebAuthn deliver the highest levels of security available to users, these open standards are not yet supported by all services. For cases when you may not be able to use the Security Key NFC, we recommend the YubiKey 5 Series. The YubiKey 5 Series is Yubico's set of multi-protocol security keys, which expands support from just FIDO U2F and FIDO2/WebAuthn to also include several other authentication protocols. As a result, this set of keys can more easily support a wide range of use cases and services such as email encryption, computer login, one-time password, smart card authentication, or code signing.

Step 2: Confirm device and system requirements

To find out whether your device is NFC-write-capable, do any of the following:

- Visit https://www.unitag.io/nfc/is-my-phone-compatible-with-nfc
- Use any search engine to do a search using the terms "NFC write-capable" and your "<device type model>"
- For Android power-users, consult NXP TagInfo: https://play.google.com/store/apps/details?id=com.nxp.taginfolite&hl=en_US).
- Contact your carrier.

The Security Key NFC works with supported web browsers across Linux, macOS, and Windows operating systems, but depending on what services you'd like to use the key with (FIDO U2F or FIDO2), and in what capacity (USB or NFC), there are additional system requirements to consider.

Browser Requirements

The following web browsers are compatible with the Security Key NFC: Chrome, Opera, Mozilla Firefox, Safari, and Brave. For setting up the suggested accounts referenced further in this document, we recommend using Google Chrome.

If you are using your key with Microsoft accounts, which supports FIDO2/WebAuthn with a passwordless experience, we recommend using Microsoft Edge. While Mozilla Firefox, Chrome, and Safari also support WebAuthn, they are not yet compatible with Microsoft accounts.

Device Requirements

USB-A

If you plan to use the Security Key NFC on a desktop or laptop machine, ensure that your device is equipped with a standard USB-A port. If your device is only equipped with USB-C ports, you may also choose to use an adapter. Alternatively, the YubiKey 5 Series includes USB-C specific devices.

USB-A USB-C

Near Field Communication (NFC)

For authentication with the Security Key NFC on mobile, the FIDO2 and the U2F protocols require that the operating system (OS) of your mobile device has both NFC-read and NFC-write capability, such as Android. If the OS supports NFC-write operations, then it will certainly have NFC-read capability, even if it needs add-ons to make use of that capability. For example, although the Security Key NFC will work with the Windows 10 Surface tablet via USB-A port, to access the NFC capability for wireless authentication, you need an external NFC card reader.

The method of determining whether your device's OS is NFC write-capable differs depending on the device and in some cases, on the carrier. Phone specifications can change without notice and they can also vary from region to region. Most Android phones support both NFC read and write, and recently, iOS devices can also support NFC read and write.

With these recent updates, iPhone users (running iOS 13+) can experience mobile NFC authentication with a Security Key NFC on apps and browsers that have added support. However, there are no apps and browsers that have added this support to date. Yubico continues to work closely with our partners, with the goal of YubiKey support being added to your favorite, day-to-day apps soon.

Step 3: Set up your key for use via USB

For added convenience when enrolling your key, we recommend that you first register your key with each account from a desktop or laptop machine.

Every online service provider implements the key enrollment/registration process differently, and therefore registration instructions vary depending on the service. Below you will find direct links to the appropriate procedures from a few of the most popular services. We recommend beginning the enrollment process with Gmail.

Google: Go to Google Account Help's Use a security key for 2-Step Verification.

Microsoft accounts: Go to Microsoft Windows Support's Sign in to your Microsoft account with Windows Hello or a security key.

GitHub: Go to GitHub Help's Configuring Two Factor Authentication.

Dropbox: Go to the Yubico tutorial.

Additional services that support the Security Key NFC include: Facebook, Go Daddy, GitLab, Dashlane, Keeper Security, Coinbase, Kraken, Salesforce, Twitter, and more, with others adding support. You can find set up instructions for other service providers by visiting our Works with YubiKey catalog and selecting the company of your choice.

Google

Microsoft

GitHub

Dropbox

Step 4: Set up your key to work with your mobile device for use via NFC

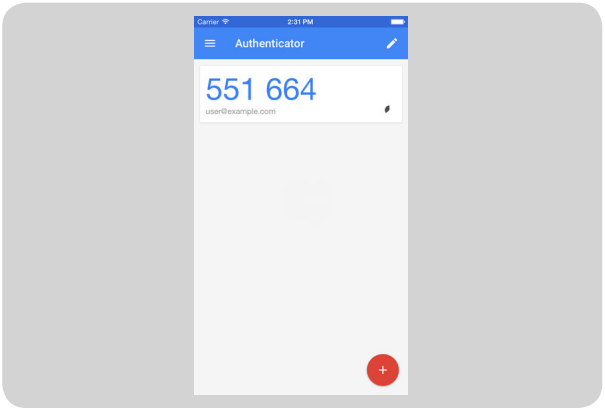
Once you've registered your security key with select accounts from a desktop or laptop machine, it can also be used to authenticate via NFC.

NFC via Mobile

To start authenticating over NFC on your mobile platform, complete the following:

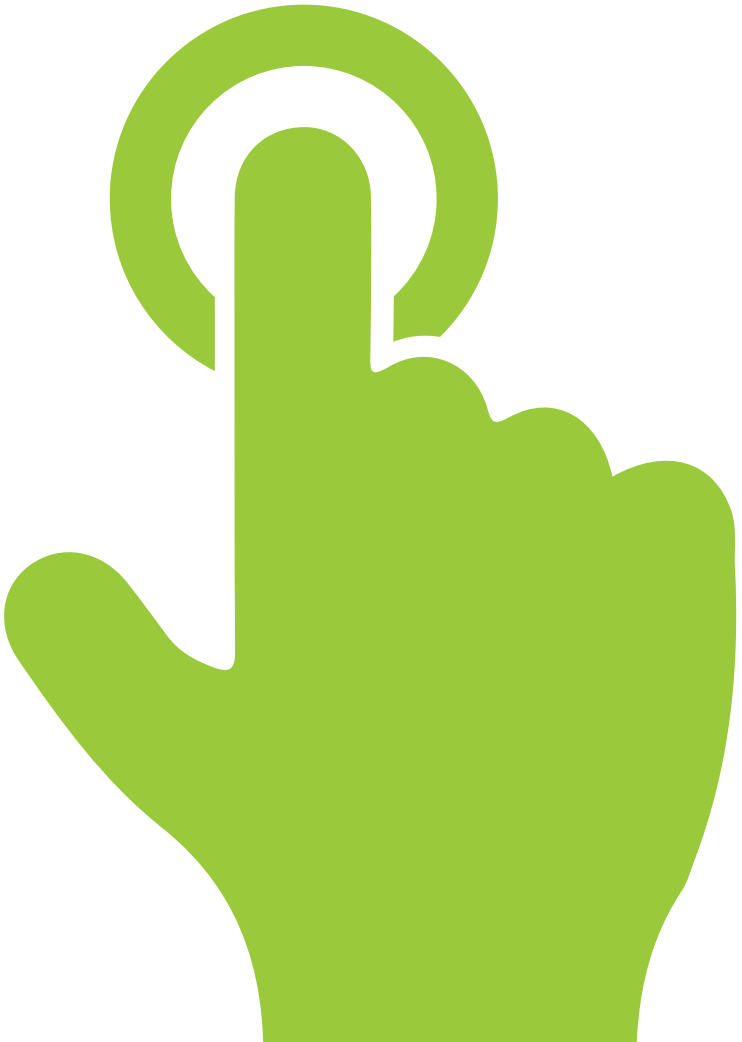
Step 1: Ensure that NFC is enabled on your device. To find out how to do this, either consult your device's manual or find a site such as this one, whose two subsections "Do You Have NFC" and "Activating NFC" provide very clear directions.

Step 2: Depending on your version of Android OS, you may need to install Google Authenticator on your device to help complete FIDO U2F transactions.



It's important to note that just because a service makes support for the YubiKey on desktop, it does not necessarily mean that it will also make support for the YubiKey within its mobile app. However, due to Android's native NFC, you are able to access some services through the Chrome mobile browser. We recommend logging into your Gmail account (which you should have already set up with your Security Key NFC) via the Chrome browser on your Android device.

Step 5: Login with peace of mind



Now that you've registered your Security Key NFC with your online accounts, you can rest assured that you have hardware-backed protection against phishing and man-in-the-middle attacks.

As a new YubiKey user, here are a few good habits that we recommend.

1. When possible, we always recommend registering a second YubiKey with all of your accounts, as it's important to always have a backup authentication method. That way, if you lose your YubiKey, forget it at work/home, or misplace it, you will still be able to access your accounts. Not every service allows users to register multiple YubiKeys. In this case, we recommend referencing their supported authentication factors to choose another option that suits you best.
2. If you register two or more YubiKeys with your account, we recommend that you keep one key in a secure location (a lock box at home or a locked desk drawer at work), and keep the other in a place where you are likely to always have access to it (on your keychain, in your wallet, with your corporate badge, etc.).
3. If you lose your key, revoke access for that specific YubiKey by going into your account settings and removing it. This must be done on an account-by-account basis. Once you revoke access for the device, it is no longer usable for logging into your accounts. In the event you find your lost YubiKey, it is possible to re-register the device with your account(s). If anyone else were to find your key, there is no way for them to identify who the key belongs to nor where the key has been used.
4. If there is a service or application that does not yet include YubiKey support, let the provider know that you want to use your YubiKey with their service or application. Yubico is regularly engaged with service providers to broaden the YubiKey ecosystem, but we often hear that it's the customer preference that is most influential. Most product features and roadmaps are prioritized based on popular customer demands.

www.yubico.com

yubico