

Using a Yubikey Neo with Google & Gmail

This document explains how to use the Yubikey Neo. The Yubikey Neo is a hardware token, used for two-factor authentication, which is U2F compliant, so it can be used as a 2-factor device for your Gmail / Google account. ***Using a "Security Key" is only supported in Google Chrome.***

Google will require you to connect your phone by default. You can choose to just setup the Security Key, or also enable the authentication app. When you enable both, Google will first ask for your Security Key and offer the app as a back-up (E.G in other browsers)

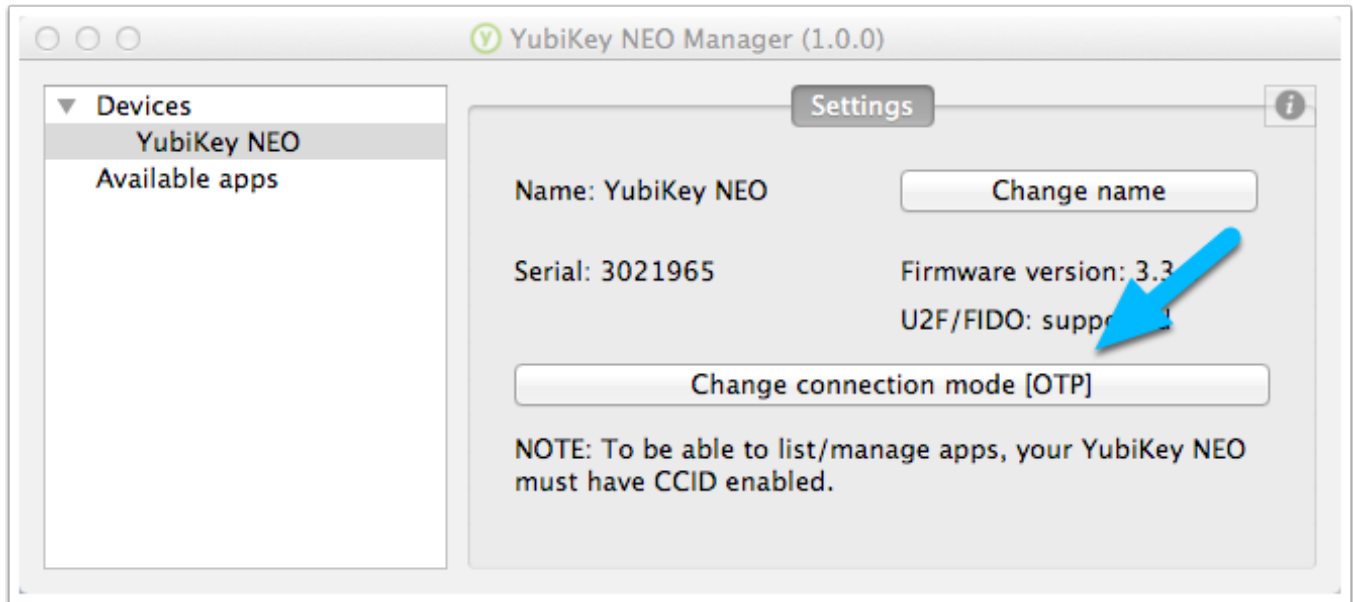
1. Requirements

- Two-factor authentication via your app must be enabled
- You must download and install the NEO Manager (which is a separate tool from the Yubikey Personalization tool)

You can download the NEO Manager here:

- NEO Manager for Windows: <http://yubi.co/NEOMgrWin>
- ? NEO Manager for OSX: <http://yubi.co/NEOMgrMac>
- ? NEO Manager for Linux: <http://yubi.co/NEOMrgLux>

2. Configure the NEO

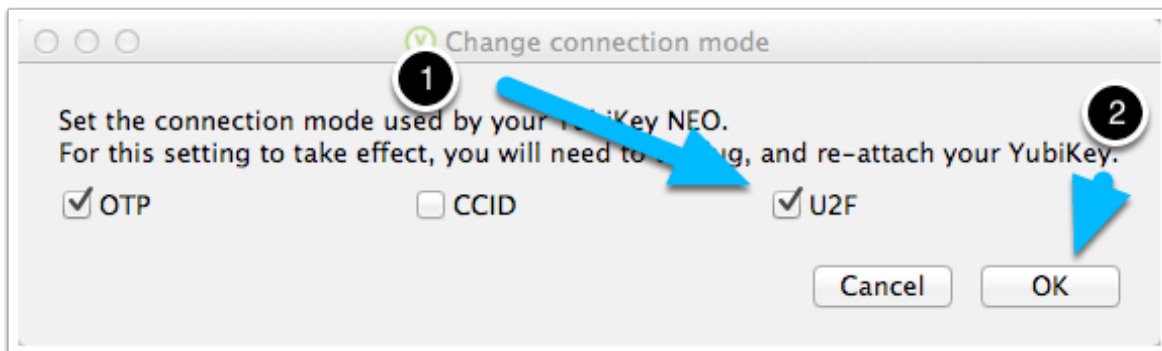


Once you've installed the NEO Manager, open the application.

To configure your NEO to support U2F (used by Google), click "Change connection mode (OTP)"

When you enable U2F you will still be able to use the OTP functionality of your NEO e.g for logging into your websites.

3.

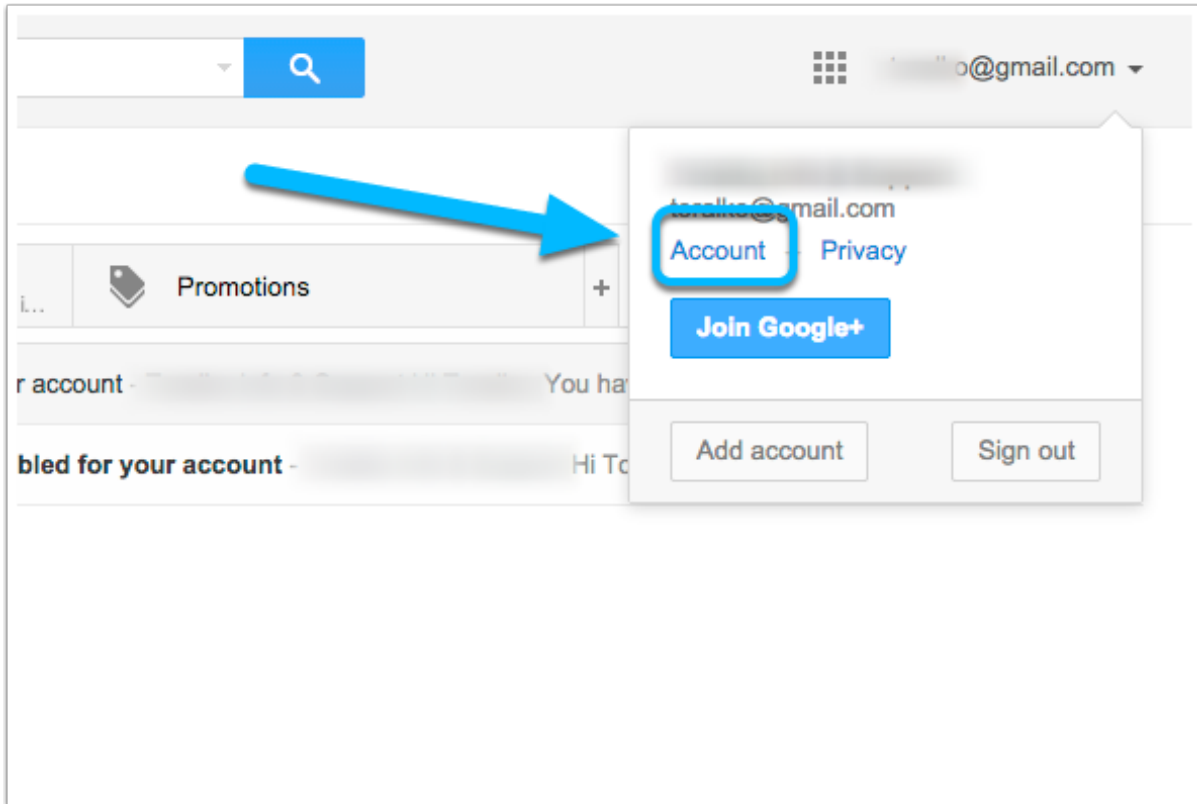


1. Check the U2F box.
2. Click "Ok"

Using a Yubikey Neo with Google & Gmail

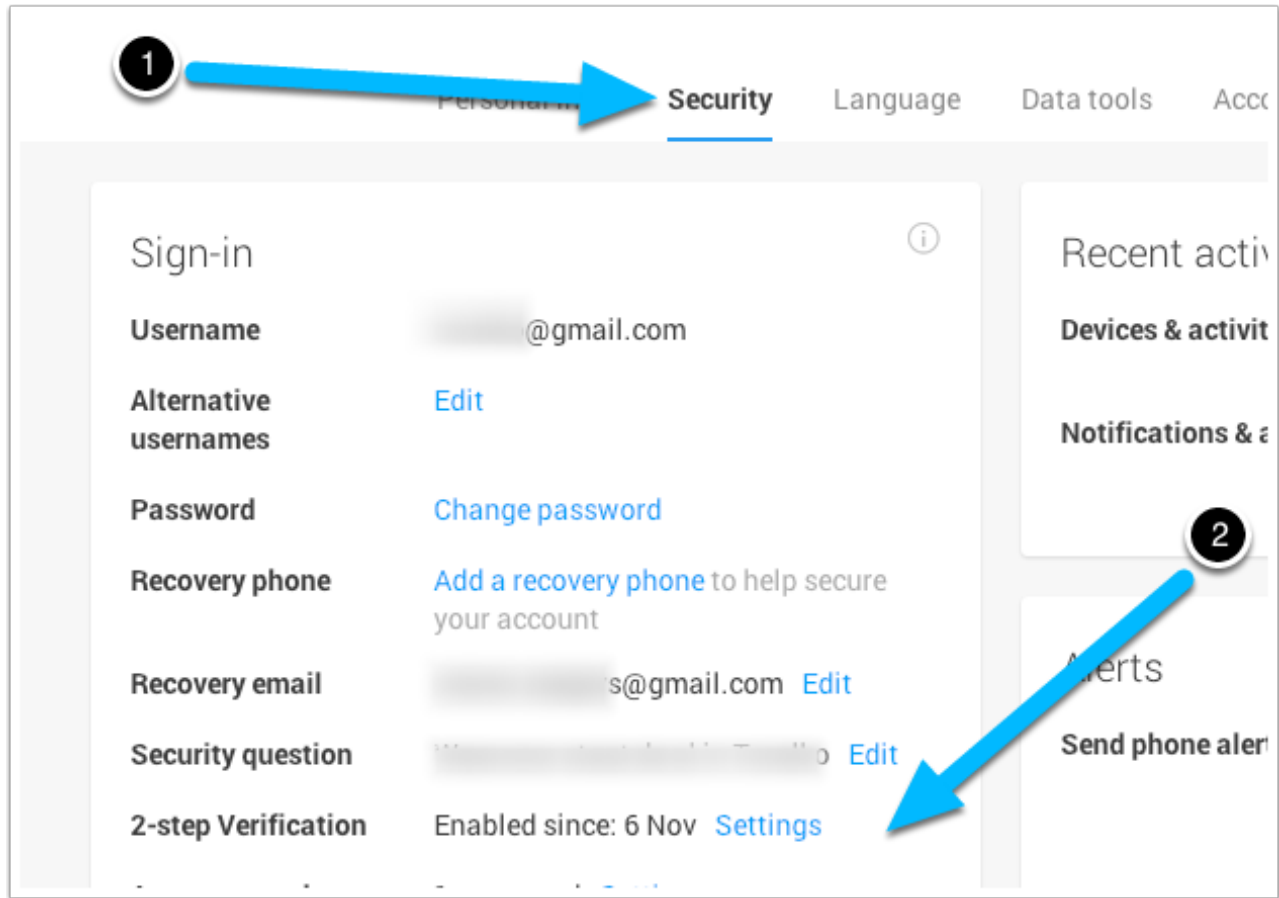
3. You will be prompted to remove your Yubikey NEO. Remove the Yubikey now.

4. Configure your account



Login to your Google account. Open your "profile" in the top right, and click "Account"

5. Enable the Security Key



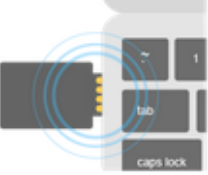
1. Go to the "Security" tab in your profile
2. Click "Settings" next to 2-step verification. *2-factor authentication needs to be enabled to be able to continue.*

6.

2-step Verification

Verification codes	App-specific passwords	Registered computers	Security Keys
--------------------	------------------------	----------------------	----------------------

SECURITY KEYS



A Security Key is a physical device that makes signing in to your Google Account more secure. After registering a Security Key, you can sign in by inserting the Security Key instead of typing a verification code.

You don't currently have any Security Keys registered.

[Add Security Key](#)


Note: A blue arrow points from the 'Registered computers' tab to the 'Security Keys' tab. Another blue arrow points from the 'Add Security Key' button to the right.

Open the "Security Keys" tab, and click "Add security key"

7. Adding the key

Add a Security Key

As a 2-Step Verification user, you can add a Security Key to your Google Account to make the sign-in process easier and more secure.



Here's how:

- 1** Make sure that you have a Security Key with you
Don't have one? [Learn more](#)
- 2** Remove your Security Key if already inserted
- 3** Click 'Register' and then insert your Security Key into a USB port
If your Security Key has a button or gold disc, tap it. [Having trouble?](#)

[Done](#) [Cancel](#) [Register](#)

- Make sure the Yubikey **isn't plugged in yet**.
- Click the register button, *then* plug in the Yubikey NEO.
- Touch the gold disk to send the code, until you get the "Registered" confirmation.
- Click "Done"

8. Using the key

When you try to access your Google account, Google might ask for your Security Key. Plug in the Yubikey Neo, and touch the gold disk to send the code, after which you will be logged in. You're now using 2-factor authentication!