# YubiKey with Password Safe

**Author: Felicia King**

## Authentication concepts

### Single-factor authentication

Single-factor authentication is inherently flawed. Hackers and criminals install keystroke loggers, screen capture devices, and remote access Trojans as part of their standard operating procedure. Therefore, anything that can be input through normal computer input which is on the compromised endpoint is also compromised.

So imagine you are using a password storage application like Password Safe. If you have only your one password required to open the Password Safe, and your endpoint is compromised, then the hacker can download your Password Safe file and open your file. Then they have access to all of your passwords. Therefore, it would be prudent to have a second factor of authentication required to open your Password Safe.

### Two-factor authentication

The best two-factor authentication is one that involves a physical piece of hardware that is not connected to the endpoint (your computer) or is read only. Since the YubiKey is easily removable, you can and should remove the device from your computer when you are not using it. Take it with you or lock it up elsewhere. This prevents the YubiKey being stolen or compromised if your computer is subjected to unauthorized physical access.

YubiKeys are accessible and understandable to the average user, especially when combined with PasswordSafe and my common-sense recommendations in this document.

## YubiKey concepts

### Size

YubiKey comes in a standard size and a nano size. The standard size is like a really tiny USB flash drive, and the nano doesn't hardly stick out of a USB port but a couple of millimeters. Both have a small metal plate that is responsive to human finger touch. It is not a fingerprint reader, but does require human finger. It cannot be activated with a pen, pencil, or similar non-electroconductive items. The nano device might be a good choice for laptops so that very little is sticking out of the USB port.

### Programmability

YubiKeys have two digital slots. That means that a single YubiKey could provide you with two unique types of authentication. Slot 1 is generally reserved for integration with YubiCloud-integrated apps like websites. Slot 1 comes pre-programmed from Yubico. Slot 2 is easily programmable by the end user to supply a variety of types of two-factor authentication. The software to install custom programming into slot 2 is freely downloadable from Yubico's site, but is not necessary for using YubiKey with Password Safe.

### Procurement

Purchase YubiKeys directly from Yubico.com.

## Password Safe with YubiKey

### Authentication method

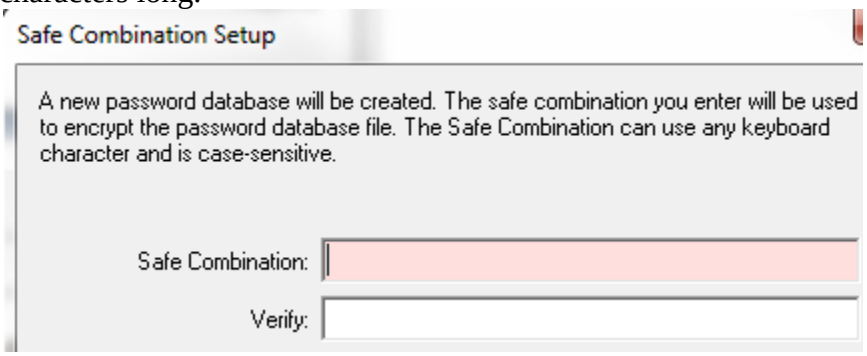
Password Safe normally uses a single, long, complex password to open the Password Safe. As a result, it is VERY important to choose an unlock password that is at least 15 characters long and contains significant complexity. Password Safe can be integrated with YubiKey such that both the standard unlock password AND the challenge-response method password from the YubiKey must both be entered in order to unlock the Password Safe. You can see how this would substantially increase the security around the Password Safe contents.

### Setup

1. If you don't already have Password Safe, download it from Sourceforge. http://passwordsafe.sourceforge.net/
2. Since you are not browsing the internet and doing your normal activities as an administrator account, you will need to log off the computer and log onto it as an administrator level account.
3. Install Password Safe.
4. Savvy individuals will notice that Password Safe desktop icon and Start Menu options install into the user's profile. This is a problem because then it is not accessible to all users. Therefore, you will need to COPY (not move) the desktop icon from C:\Users\YourAdmin to C:\Users\Public\Desktop. Finally, delete the desktop icon in the YourAdmin profile so that you do not have a duplicate on the desktop.
   The reason you must COPY and not move is because of permissions.
5. Then COPY (not move) the Password Safe folder from C:\Users\YourAdmin\AppData\Roaming\Microsoft\Windows\Start

Menu\Programs to C:\ProgramData\Microsoft\Windows\StartMenu\Programs. Finally, delete the Password Safe folder in the YourAdmin profile so you do not have a duplicate.

6. Now you can log off and then log back into the computer as your regular user account and begin to use Password Safe.
7. Open Password Safe and create a new Password Safe. During the setup process you will be required to supply two VERY IMPORTANT pieces of information.
8. Specify for the psafe3 file to be stored into a location where those data files are backed up on a daily basis. Perhaps that is the Documents folder in your profile.
9. Specify a very complex unlock password that is at least 15 characters long.

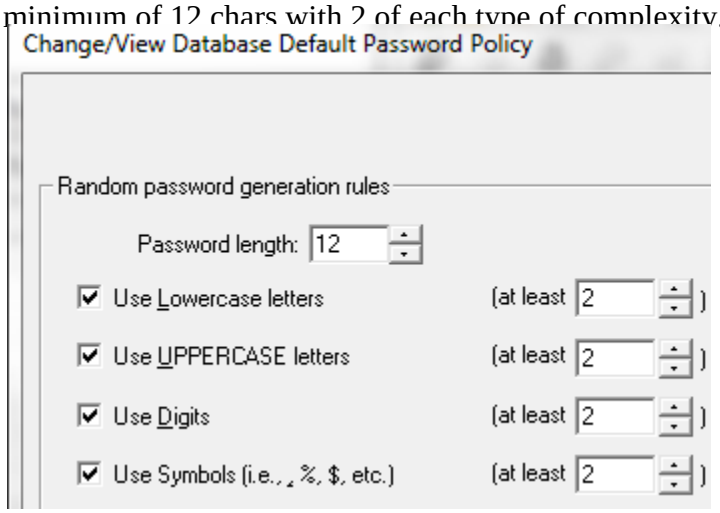



Make sure your Password Safe file is backed up to external media daily!

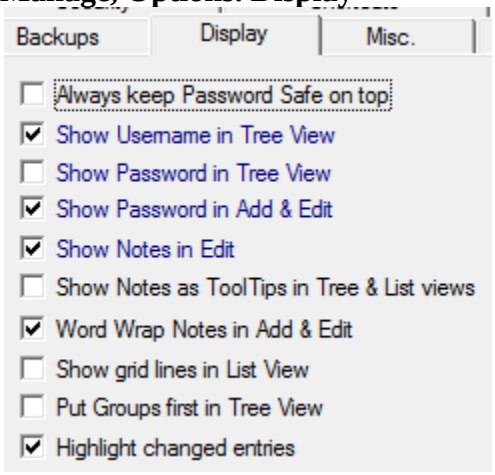
## General configuration recommendations

Now that your Password Safe file is created, I suggest the following configuration settings be used.

- In **Manage, Password Policies**, specify an appropriate password policy such as minimum of 12 chars with 2 of each type of complexity.




- **Manage, Options. Display**




- **Manage, Options, Security**: Specify an idle time you want.

## How many YubiKeys do I need to configure?

This is probably the most important part of this document. Realize that if you lose your YubiKey, and you have no backup copy of it, you will never get into your Password Safe again. Therefore, I highly recommend you have at least three YubiKeys that are programmed to open your Password Safe. I suggest three because you likely need to use your Password Safe on your PC and laptop, and then you need one to be protected against loss due to fire.

- One for your main PC
- One for your laptop
- One for storage inside a fire safe

## Configure Password Safe with YubiKey

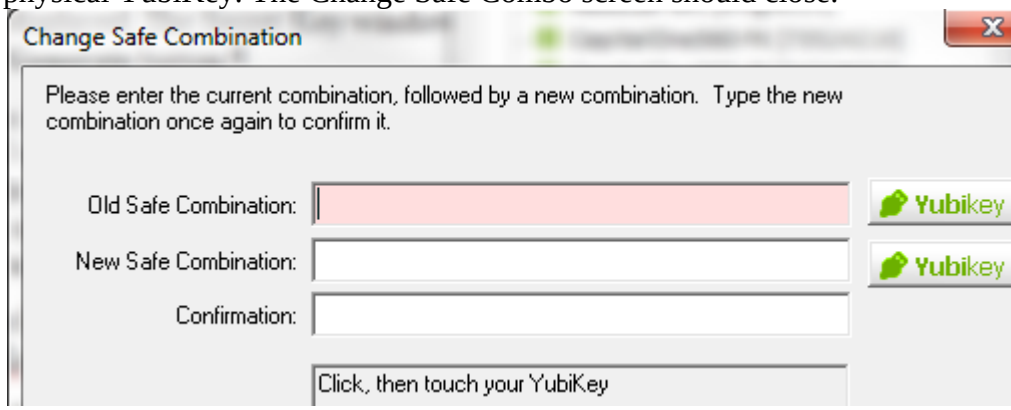
Now that your Password Safe file is created and the master unlock password has been set, you can enable YubiKey as the challenge-response password second factor of authentication for your safe.

### *NOTE:*

If you are working with a pre-existing Password Safe database that has content, I HIGHLY recommend you make a backup copy of the database before you attempt these changes. In that way, if anything goes wrong, you can roll back to using the unmodified psafe3 file. This procedure is provided to you for informational purposes. This procedure assumes that you have the skill to back up and restore your own files.

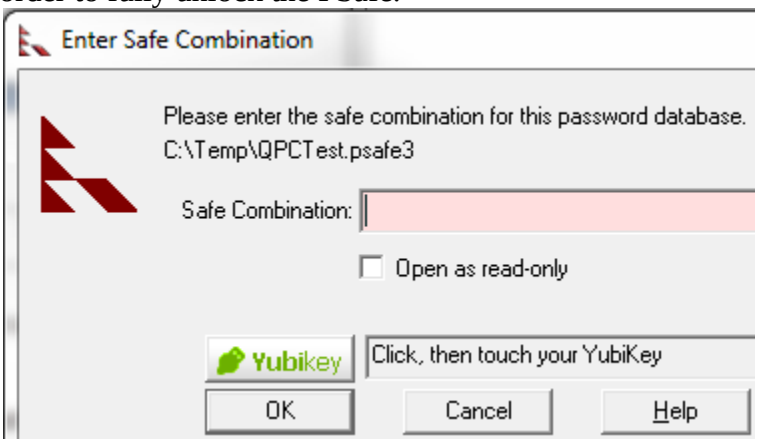
1. Insert YubiKey #1 into a USB port on your computer and wait for the driver to load. When the driver has finished loading, you will see the message that says that the device has installed. No special software is required.
2. In Password Safe, click on **Manage, YubiKey**.
3. In the YubiKey Configuration window, you will see the serial number for your YubiKey displayed. The Secret Key window should be blank. Click the **Generate** button.
4. As an added safeguard, you can optionally choose to copy the secret key into a notepad file and then print it. Note that I am not suggesting that you store the file on your computer. Perhaps it would be a better choice to store the printout of the Secret Key with YubiKey 3 in the fire safe.
5. Now that you have a Secret Key, click the button to program digital slot 2 in your YubiKey #1. Press the **Set YubiKey** button.
6. At this point, the Password Safe database psafe3 file is not yet configured to work with YubiKey. You must go through a password change process on the psafe3 file in order to fully integrate it.
7. In Password Safe, click on **Manage, Change Safe Combination**.
8. You must enter the existing unlock password, then enter the same password in the new combination boxes as well. Note that we are not really changing the password here, but really telling Password Safe to use YubiKey. After you have your unlock password entered into all three input boxes, click on the green Yubikey button on the screen. You will notice a countdown bar in the fourth box. Before the progress bar finishes, press the button on the

physical YubiKey. The Change Safe Combo screen should close.




9. After this is complete, close the Password Safe and reopen it with both the unlock password and the challenge-response from the YubiKey.
   IMPORTANT!!! It is critical that you test to make sure you have actually enabled YubiKey on your Password Safe by attempting to unlock it only with the unlock password. If the PSafe is correctly configured with YubiKey, it will not unlock the safe without the challenge-response.

10. You should have to click the YubiKey button on the screen and then touch the metal contact on the YubiKey with your finger in order to fully unlock the PSafe.




   Note that when you press the YubiKey button on the Safe Combination screen, that is the challenge. When you press the metal contact on the YubiKey, that is the response. That's why it's called challenge-response.

11. If you have successfully configured your Password Safe, remove YubiKey #1, then insert YubiKey #2 into the USB port.

12. Go back into **Manage, YubiKey**, but this time DO NOT click Generate. Instead, just click **Set YubiKey** to program YubiKey #2.

13. Repeat steps 7 and 8 for YubiKey #3.

14. Finally, I suggest you label your YubiKeys, test all three of them, and then put them where they belong. That means at least one of them goes into a fire safe with your paper printout that shows the Secret Key.

# Limitations

## Remote Desktop

YubiKey cannot function in the challenge-response mechanism over Remote Desktop.

## Network and multi-user

YubiKey works great in a multi-user environment that is connected via a LAN as long as all individuals with a YubiKey have the same slot 2 configuration to open the same Password Safe. This is often done in departments of individuals that have to share passwords because it is inappropriate to just put all the departmental passwords into some Word document that everyone can freely read, including unauthorized parties.