# YubiKey OSX Login

## Via Yubico-PAM Challenge-Response

Version 1.6

**October 24, 2015**

## About Yubico

As the inventors of the YubiKey®, Yubico sets new world standards for secure login across the Internet. Our unique USB and NFC key offers one-touch strong authentication supporting multiple authentication protocols for all devices and platforms - with no driver or client software needed. With successful enterprise deployments in 140 countries, including 7 of the top 10 Internet companies, Yubico is adding the consumer market to its list of strong authentication converts. Founded in 2007, Yubico is privately held with offices in Palo Alto, Calif., Stockholm, and London. For more information visit yubico.com

## 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.

## Trademarks

Yubico and YubiKey are trademarks of Yubico Inc.

## Contact Information

**Yubico Inc**
459 Hamilton Avenue, Suite 304
Palo Alto, CA 94301
USA
yubi.co/contact

# Contents

# 1 Configuration of YubiKeys

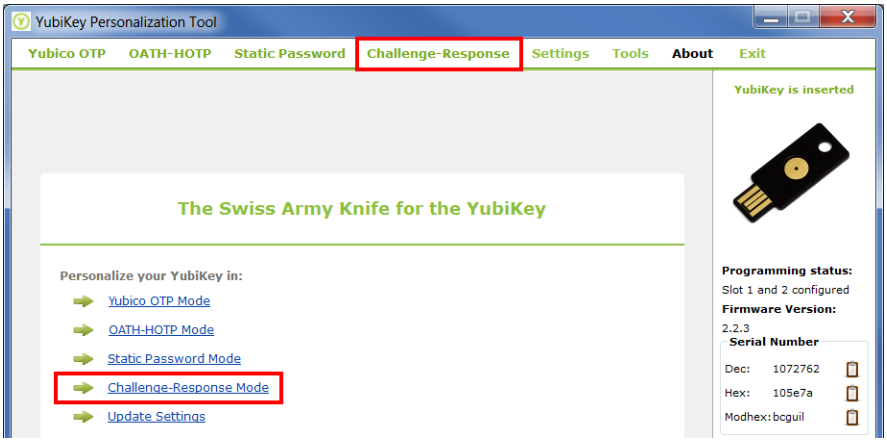
It is recommended to have YubiKeys pre-configured with the HMAC-SHA1 Challenge-Response configuration before setting up the OS X Login. The YubiKey configuration can easily be done ahead of time, or even by Yubico at the initial purchase (for orders larger than 500 YubiKeys).

For configuring YubiKeys in Challenge-Response mode personally, there are software applications provided by Yubico; the YubiKey Cross-Platform Personalization tool in both Graphical and Command Line interfaces.

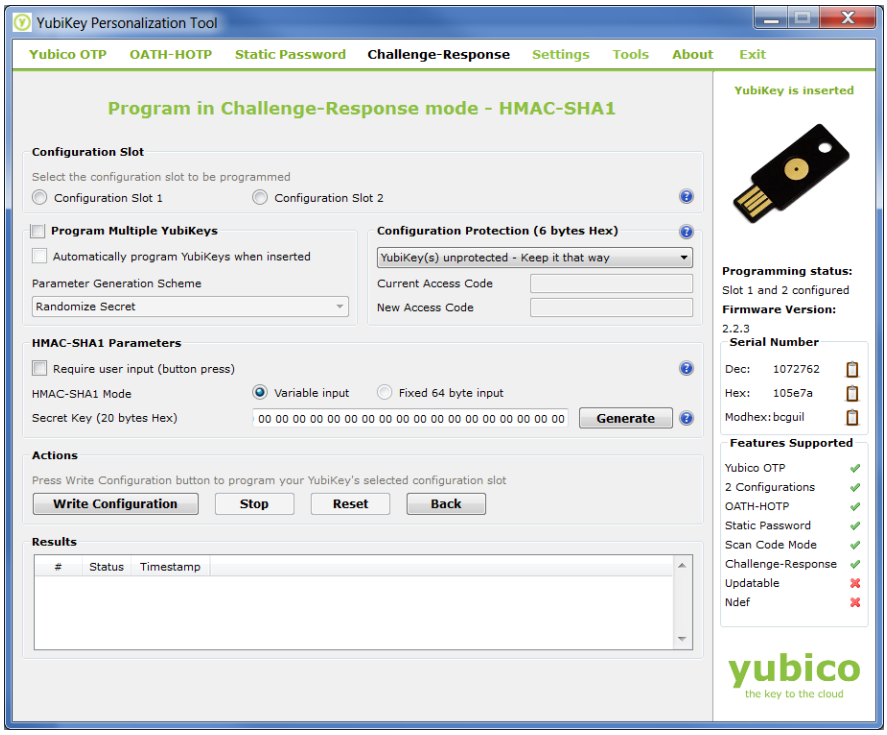
## 1.1 Personalization Tool (recommended)

The Personalization Tool is the simplest way to set up small numbers of YubiKeys (<500) with the Challenge-Response credential.

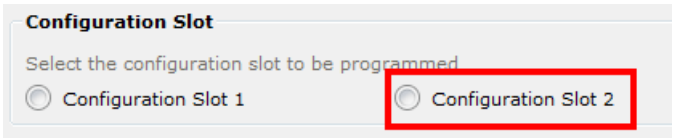
1) First, install the latest version of the YubiKey Personalization Tool from the App Store - https://itunes.apple.com/us/app/yubikey-personalization-tool/id638161122?mt=12.
2) Once the YubiKey Personalization Tool has been installed, insert a YubiKey in a USB port on your Mac and launch the YubiKey Personalization Tool.
3) Open the “Settings tab” at the top of the window, and ensure that the “Logging Settings” section has logging enabled, and the “Yubico Output” selected.
4) Open the “Challenge Response” tab at the top of the window:



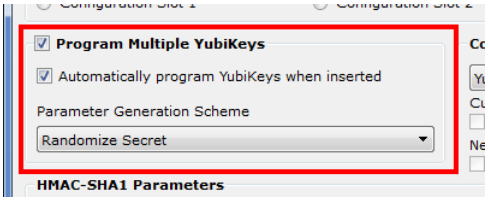

5) In the “Program in Challenge-Response mode” menu, click on “HMAC-SHA1”. You’ll then see the following window:



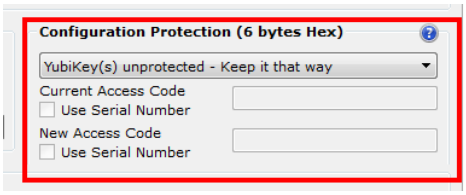

6) Locate the Configuration Slot section and select the “Configuration Slot 2” option




7) If you wish to program multiple YubiKeys, select the “Program Multiple YubiKeys” and “Automatically program YubiKeys when inserted” options. This will instruct the application to automatically program YubiKeys when they are plugged, one at a time, into the USB port of the host machine until the application is stopped.

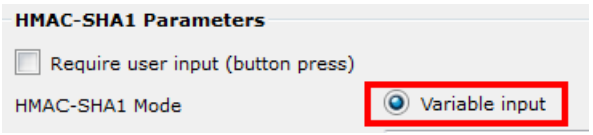



8) For added security, you may apply a Configuration Access Code – this locks down the configuration so it cannot be changed without supplying the code. In the Configuration Protection section, select “YubiKey(s) unprotected – enable protection” from the drop down menu, and either enter a 12 character hex access code, or select “Use Serial Number”.



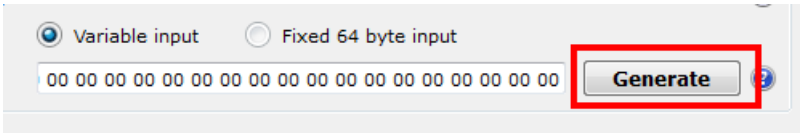
9) Locate the HMAC-SHA1 Section. In this section, ensure the checkbox “Require User input (button press)” is NOT selected.


10) In the HMAC-SHA1 section, for the HMAC-SHA1 Mode, select the “Variable input” option.

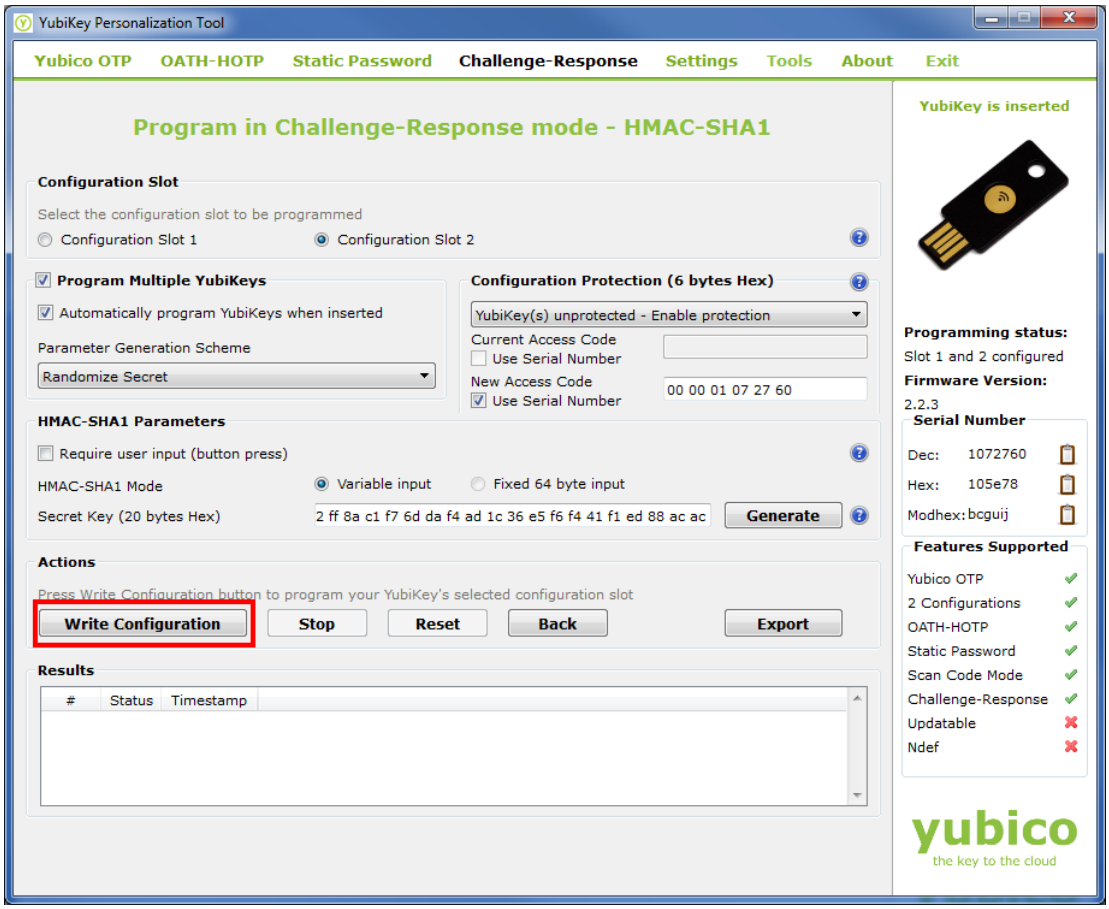



11) Click the “Generate” button in to the right of the field labelled “Secret Key (20 bytes Hex).

**Note:** This secret key is essential for making a backup to configured YubiKeys. This value will be included in the configuration log generated when the YubiKey is configured (as long as you have that option enabled). Store this value in a safe location for generating backup or secondary YubiKeys for the OS X Challenge-Response Login.




12) In the Actions Section, click the “Write Configuration” button. This will configure the YubiKey. If the “Program Multiple YubiKeys” option was enabled, the Tool will continue to configure new YubiKeys each time they are plugged in until the “Stop” button is clicked.




## 1.2 Command Line Tool (advanced users)

The Command Line Tool and library is useful for automating or integrating YubiKey Configuration. Integration of this library is outside the scope of this document, and focus will be on the command line interface.

1) First install the CLI (Command Line Interface) tool from the yubico developer's website at (https://developers.yubico.com/yubikey-personalization/Releases/). If building your own release, the yubico-c library is a pre-requisite (https://developers.yubico.com/yubico-c/)
2) Once installed, launch the Tool in the command line and plug in the YubiKey.
3) To configure the YubiKey correctly in Challenge-Response mode for OSX, use the following format:

```
ykpersonalize -2 -y -ochal-resp -ochal-hmac -o-chal-btn-trig -o-hmac
-lt64 -oallow-update -c<ACCESS CODE> -a<SECRET KEY>
```

# 2 Back up your Mac using Time Machine

Before continuing this process, it is important to back up your system with Time Machine. If mistakes are made, it is possible to get locked out of your system. The only way to recover from this is to restore from a Time Machine backup made prior to editing the *authorization* file (Section 7.4). *Yubico assumes no responsibility if you get locked out of your account(s).*

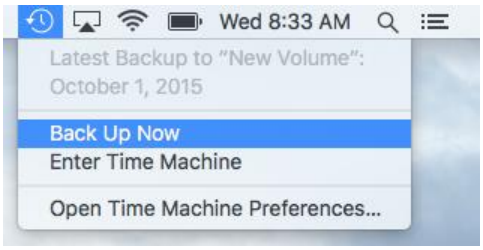
1) Make sure your external hard drive used for Time Machine backups is plugged into your computer.

   **Note:** If you see the Time Machine icon in the OS X menu bar ( ), skip to step 6.

2) Click on the Apple menu at the top left, and select **System Preferences…**


3) Click **Time Machine**


4) At the bottom, click the checkbox next to **Show Time Machine** in menu bar.
5) Close the Time Machine window.
6) Click on the Time Machine icon in the OS X menu bar and select **Back Up Now**.



# 3 Install Xcode Command Line Tools

1) Open a Terminal window and run the following command to install the Xcode Command Line Tools:

```
Xcode-select --install
```

You will be prompted that Xcode Command Line Tools need to be installed. Follow the prompts to complete the process.

# 4 Install Homebrew

1) Open a Terminal window and then run the following command to install Homebrew:

```
ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"
```

2) Press *Enter* when prompted.

3) Enter your sudo password, and press *Enter*. Several warning pop-ups will appear – these can be ignored.

4) With the Homebrew installation complete, enter the following command in Terminal to check for any issues from the installation, and then press *Enter*:

```
brew doctor
```

5) If no issues were found, you should see the following message:

```
Your system is ready to brew.
```

# 5 Install Yubico-PAM

Now that you have Xcode Command Line Tools and Homebrew installed, you need to install the Yubico-PAM module.

1) Open a Terminal window, and run the following command:

```
brew install yubico-pam
```

The Yubico-PAM module should now be installed on your Mac. If you have OS X version 10.11 (El Capitan), skip to Section 6. If you have OS X 10.10 (Yosemite) or 10.9 (Mavericks), continue to section 5.1.

## 5.1 Move the pam_yubico.so file (OS X 10.10 and earlier)

If you have OS X 10.10 (Yosemite) or earlier, run the following command in Terminal:

```
sudo cp /usr/local/Cellar/pam_yubico/2.20/lib/security/pam_yubico.so
/usr/lib/pam/pam_yubico.so
```

**NOTE:** The command above assumes you currently have pam_yubico version 2.20. If you get an error message using this command, you may need to confirm that a different version of PAM isn't installed.

To continue, skip to section 7.

# 6 Move pam_yubico.so to protected location (OS X 10.11 only)

Mac OS X 10.11 (El Capitan) introduced a new security feature, System Integrity Protection (AKA “rootless”). The feature protects certain directories from being modified. In order for the OS X login to function in version 10.11, a file required for the Yubico PAM module to function (`pam_yubico.so`) needs to be moved to a directory protected by System Integrity Protection. To resolve this issue, it is necessary to temporarily disable System Integrity Protection, move the file, and then enable System Integrity Protection

## 6.1 Disable System Integrity Protection (OS X 10.11 only)

1) Restart your system. Once the screen turns black, hold the *command* and *R* keys until the Apple icon appears. This will boot your system into Recovery Mode.
**Note:** The slower than normal boot time is expected behavior.

2) Click on the *Utilities* menu at the top of the screen, and then click *Terminal*:


3) Type the following into the Terminal window, and then press *Enter*:

```
csrutil disable
```

4) Type the following into the Terminal window to restart, and then press *Enter*:

```
reboot
```

## 6.2 Move directory (OS X 10.11 only)

If you have OS X 10.11, run the following command in Terminal:

```
sudo cp /usr/local/Cellar/pam_yubico/2.20/lib/security/pam_yubico.so
/usr/lib/pam/pam_yubico.so
```

**NOTE:** The command above assumes you currently have pam_yubico version 2.20. If you get an error message using this command, you may need to confirm that a different version of PAM isn't installed.

## 6.3 Enable System Integrity Protection (OS X 10.11 only)

1) Restart your system. Once the screen turns black, hold the *command* and *R* keys until the Apple icon appears. This will boot your system into Recovery Mode.

2) Click on the *Utilities* menu at the top of the screen, and then click *Terminal*:


3) Type the following into the Terminal window, and then press *Enter*:

```
csrutil enable
```

4) Type the following into the Terminal window to restart, and then press *Enter*:

```
reboot
```

# 7 Configure PAM

To this point, you have configured a YubiKey for Challenge Response and installed Xcode Command Line Tools, Homebrew, and the Yubico-PAM module. Next, you will configure the desired user account for YubiKey Authentication. You will have two different options – Screensaver (section 7.4) and User Account login (section 7.5).

## 7.1 Initial PAM setup

1) Log into the account you want to add YubiKey Logon to.
2) In Terminal, run the following command to create a needed directory on your Mac:

```
mkdir –m0700 –p ~/.yubico
```

3) Make sure your YubiKey is plugged into your system and configured for Challenge Response (covered in Section 1 of this document), and then run the following command (to create a directory to store the initial challenge and expected response):

```
ykpamcfg -2
```

At this point, please verify that ykpamcfg has stored the initial challenge and expected response. You should see a confirmation similar to this:

```
Stored initial challenge and expected response in '/Users/[USERNAME]
/.yubico/challenge-[YUBIKEY SERIAL NUMBER].
```

If the initial challenge is stored in */var/root/[USERNAME]/challenge-[YUBIKEY SERIAL NUMBER]*, enter the following command into Terminal (where [USERNAME] is replaced with your user name and [YUBIKEY SERIAL NUMBER] is replaced with your YubiKey's 7-digit serial number):

```
sudo cp /var/root/.yubico/challenge-[YUBIKEY SERIAL NUMBER]
/Users/[USERNAME]/.yubico
```

Potential error messages:

***Yubikey core error: no yubikey present*** – This error means the YubiKey is not currently plugged into your Mac. If you receive this, please insert the YubiKey, wait a moment for the YubiKey to initialize, then retry step 3.

***Failed to read serial number*** – This error means the YubiKey has been inserted, but has not yet properly initialized. Please remove and reinsert the YubiKey, then wait about 10 seconds before retrying step 3. If you are still experiencing this issue, please go to the Apple menu > About This Mac > System Report. Under Hardware, click on "USB". The YubiKey needs to be

found in this section. If it's not showing up, please open up a Support Case with Yubico Support at yubi.co/support for further troubleshooting steps.

***USB Error: kIOReturnSuccess*** – This error is related to permissions. Try running the command again elevated as "sudo" (i.e. *sudo ykpamcfg -2*).

## 7.2 Backup YubiKeys

It is a good idea to program at least two YubiKeys when implementing the PAM login requirement. If only one is configured and something happens to the YubiKey, you will need to restore the system from a Time Machine backup created prior to implementing PAM in order to log back in to your account. To prepare a backup YubiKey:

1) Follow the procedure in Section 1 to program the backup YubiKey with a Challenge-Response credential.
2) Log in to the user account that needs a backup YubiKey.
3) Open a Terminal window and then run the following command (to create a file to store the initial challenge and expected response):

```
ykpamcfg -2
```

At this point, please verify that ykpamcfg has stored the initial challenge and expected response. You should see a confirmation similar to this:

```
Stored initial challenge and expected response in '/Users/[USERNAME]
/.yubico/challenge-[YUBIKEY SERIAL NUMBER].
```

## 7.3 Multiple user accounts and PAM

If your OS X computer has multiple user accounts, performing the steps in section 7.4 or 7.5 will affect all users that log in to the computer, so a YubiKey needs to be added to each account. If you need to program additional YubiKeys, refer to section 1 for instructions. You can use the same YubiKey for all accounts, or use a different YubiKey for each account. Follow the steps below on each account:

1) Log in to the user account that needs a backup YubiKey.
2) Open a Terminal window and then run the following command (to create a file to store the initial challenge and expected response):

```
ykpamcfg -2
```

At this point, please verify that ykpamcfg has stored the initial challenge and expected response. You should see a confirmation similar to this:

```
Stored initial challenge and expected response in '/Users/[USERNAME]
/.yubico/challenge-[YUBIKEY SERIAL NUMBER].
```

Repeat steps 1-2 for all user accounts that require a backup YubiKey.

## 7.4 Configure the OS X User Account to require YubiKey presence when deactivating the Screensaver

To require the YubiKey be present in your Mac to deactivate the screensaver, follow the steps below. Please note that the instructions are written using the command line application "vi", which is already present in OS X. There are other ways to edit system files, so please feel free to use an alternative method if you prefer:

1) Open Terminal and change directory to **/etc/pam.d**
    a. Type ***cd ..*** and press Enter
    b. Type ***cd ..*** and press Enter
    c. Type ***cd ./etc/pam.d*** and press Enter
2) Now in the /etc/pam.d directory, type ***sudo vi screensaver*** and press Enter. Verify the Terminal window now begins with:

    ***# screensaver: auth account***

3) Press the "i" key on your keyboard (to change from Command Mode to Insert Mode, which is required to edit the text in a system file). You should now see ***– INSERT –*** at the bottom of the Terminal window.
4) Arrow down to the first letter of the first line that begins with "account", and then press Enter.
5) Arrow up one line to the newly-created blank line, and then type ***auth*** , press the Spacebar seven (7) times, type ***required*** , press the Spacebar seven (7) times, and type ***pam_yubico.so mode=challenge-response***
6) Press the "Esc" key on your keyboard to exit Insert Mode and return to Command Mode.
7) Type ***ZZ*** to save the changes you've made (it is important to use capital z's, as lowercase z's will not save the file).
8) Close the Terminal window. Next time your Mac goes to screensaver, you should be able to remove your YubiKey, type in your password, and the unlock attempt should fail. For testing purposes, you can also speed up this process by going to the Apple Menu > System Preferences > Desktop & Screensaver, and change the "Start After" (at the bottom left corner) to 1 Minute.

## 7.5 Configure the OS X User Account to require YubiKey presence when logging in to the current account

To require the YubiKey be present in your Mac to log into your account, follow the steps below. Please note that the instructions are written using the command line application "vi", which is already present in OS X. There are other ways to edit system files, so please feel free to use an alternative method if you prefer. The instructions are nearly identical to that of Section 7.4:

1) Open Terminal and change directory to **/etc/pam.d**
    a. Type ***cd ..*** and press Enter
    b. Type ***cd ..*** and press Enter
    c. Type ***cd ./etc/pam.d*** and press Enter
2) Now in the /etc/pam.d directory, type ***sudo vi authorization*** and press Enter. Verify the Terminal window now begins with:

    ***# authorization: auth account***

3) Press the “i” key on your keyboard (to change from Command Mode to Insert Mode, which is required to edit the text in a system file). You should now see ***– INSERT –*** at the bottom of the Terminal window.

4) Arrow down to the first letter of the first line that begins with “account”, and then press Enter.

5) Arrow up one line to the newly-created blank line, and then type ***auth*** , press the Spacebar seven (7) times, type ***required*** , press the Spacebar seven (7) times, and type ***pam_yubico.so mode=challenge-response***

6) Press the “Esc” key on your keyboard to exit Insert Mode and return to Command Mode.

7) Type ***ZZ*** to save the changes you’ve made (it is important to use capital z’s, as lowercase z’s will not save the file).

8) Close the Terminal window.

9) Log out of your user account, and then attempt to log back in without the YubiKey inserted. The login should fail. Next, insert your YubiKey, wait approximately 10 seconds, and then attempt to login again. The login should be successful.