yubico

YubiKey OSX Login

Via Yubico-PAM Challenge-Response

Version 1.2

October 2, 2015

El Capitan 10.11 (15A284)
Homebrew

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.com/contact

Contents

1 Configuration of YubiKeys

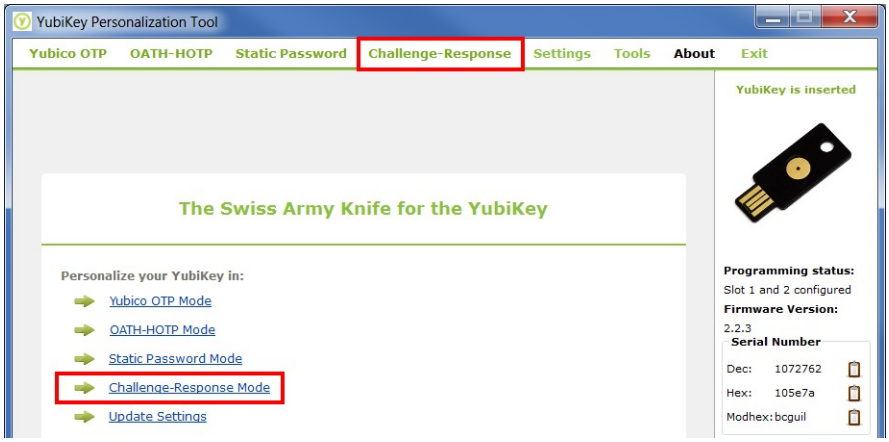
It is recommended to have YubiKeys pre-configured with the HMAC-SHA1 Challenge-Response configuration before setting up the OS X Login. The YubiKey configuration can easily be done ahead of time, or even by Yubico at the initial purchase (for orders larger than 500 YubiKeys).

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.

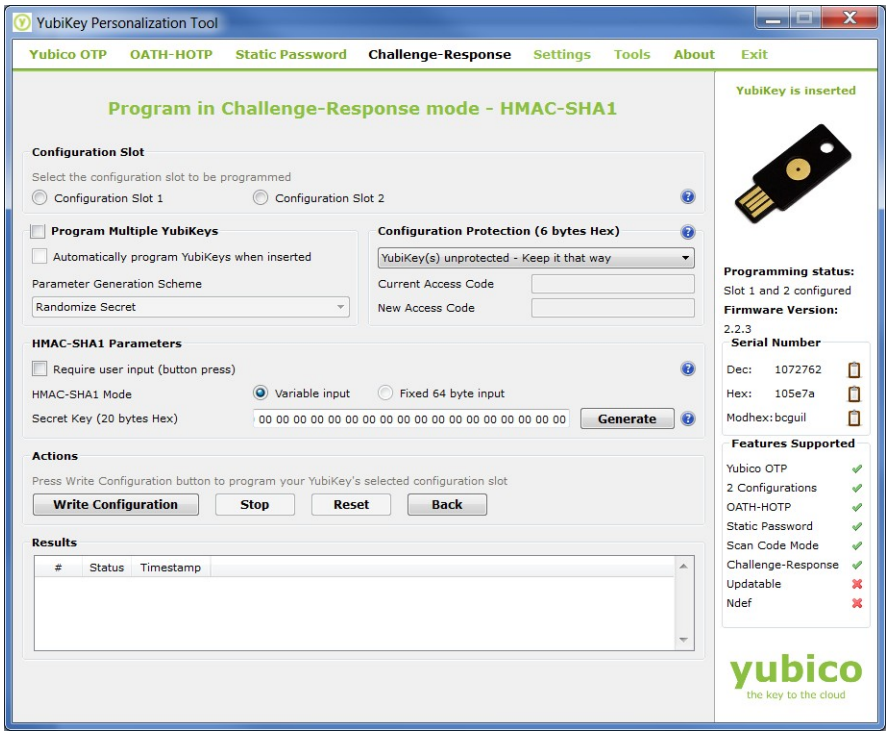
1.1 Personalization Tool (recommended)

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

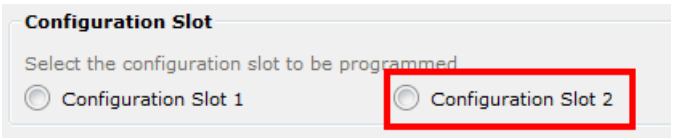
1) First, install the latest version of the YubiKey Personalization Tool from the App Store - https://itunes.apple.com/us/app/yubikey-personalization-tool/id638161122?mt=12.
2) Once the YubiKey Personalization Tool has been installed, insert a YubiKey in a USB port on your Mac and launch the YubiKey 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:



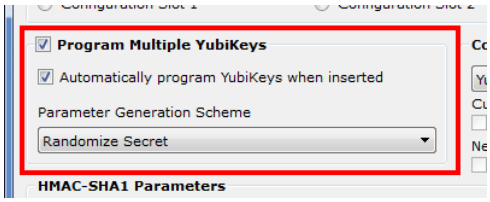
5) In the “Program in Challenge-Response mode” menu, click on “HMAC-SHA1”. You’ll then see the following window:



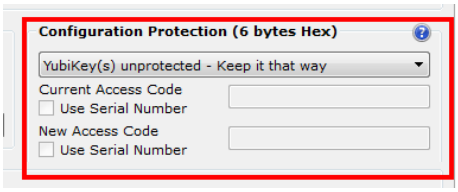
6) Locate the Configuration Slot section and select the “Configuration Slot 2” option



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.



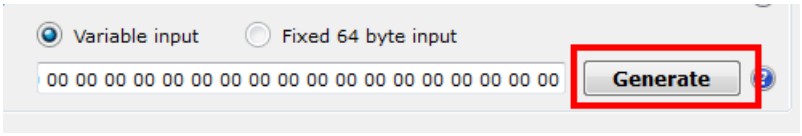
8) For added security, you may apply a Configuration Access Code – this locks down the configuration so it cannot be changed without supplying the code. In the Configuration Protection section, select “YubiKey(s) unprotected – enable protection” from the drop down menu, and either enter a 12 character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



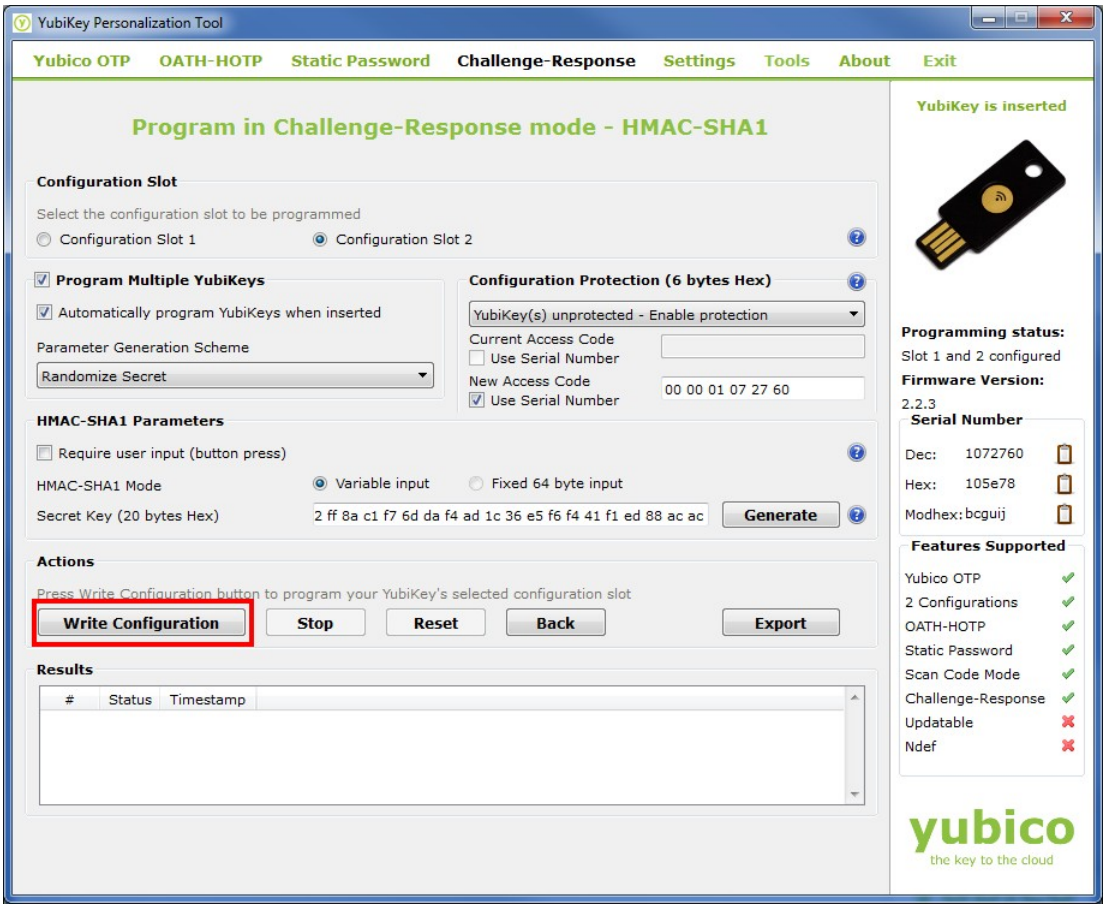
9) Locate the HMAC-SHA1 Section. In this section, ensure the checkbox “Require User input (button press)” is NOT selected.

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). Please 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 Install Xcode, Xcode Command Line Tools and Homebrew

Before installing the Yubico PAM module, Xcode, Xcode Command Line Tools and Homebrew should be installed on your Mac. We'd recommend starting at the following website: http://brew.sh/

The process is as follows:

1) Install Xcode from the App Store - https://itunes.apple.com/us/app/xcode/id497799835?mt=12.
2) Once installed, open a Terminal window and run the following command to view and accept the License Agreement:

```
sudo xcodebuild -license
```

3) After accepting the License Agreement, 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 according to the instructions as described on the website. i.e.,

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

5) Once Xcode, Xcode Command Line Tools, and Homebrew are installed, we recommend restarting your Mac before proceeding to the next section.

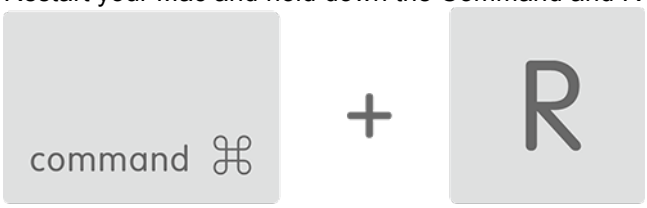
3 Install the Yubico-PAM Module

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

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

```
$ brew install pam_yubico
```

2. This next step will disable a security feature
   a. Restart your Mac and hold down the Command and R keys at startup.



   b. Hold these keys until the Apple logo appears. After your computer finishes starting up, you should see a desktop with an OS X menu bar and an OS X Utilities window with the options listed above. If you see a login window or your own desktop instead of the Utilities window, it's possible that you didn't press Command-R early enough. Restart your computer and try again.
   c. Once in Recovery go to Utilities > Terminal

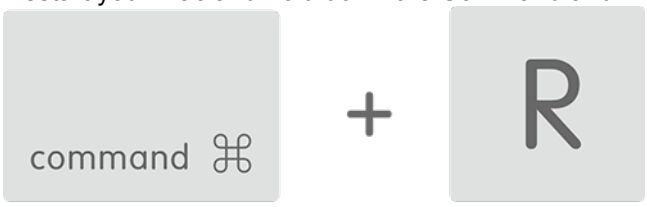
   d. Type in the following command then reboot

```
-bash-3.2# csrutil disable
-bash-3.2# reboot
```

3. Open a terminal and run the following command

```
$ sudo cp /usr/local/Cellar/pam_yubico/2.19/lib/security/pam_yubico.so
/usr/lib/pam/pam_yubico.so
```

4. Now re-enable the security feature
   a. Restart your Mac and hold down the Command and R keys at startup.



   b. Hold these keys until the Apple logo appears. After your computer finishes starting up, you should see a desktop with an OS X menu bar and an OS X Utilities window with the options listed above. If you see a login window or your own desktop instead of the Utilities window, it's possible that you didn't press Command-R early enough. Restart your computer and try again.
   c. Once in Recovery go to Utilities > Terminal

   d. Type in the following command then reboot

```
-bash-3.2# csrutil enable
-bash-3.2# reboot
```

3.1 Note for Developers (advanced users)

If installing the Yubico-PAM module manually, the code can be accessed directly from the yubico developer's website at https://developers.yubico.com/yubico-pam. There are some pre-requisites for Yubico PAM:

- YubiKey C Client Library (libykclient) https://developers.yubico.com/yubico-c-client/
- yubico-c low-level C software development kit https://developers.yubico.com/yubico-c/
- YubiKey Personalization package Library (https://developers.yubico.com/yubikey-personalization/)

The Yubico developer pages will list release packages as well as GitHub repositories for all projects.

4 Configuring an OS X user account with YubiKey Authentication

To this point, we have configured a YubiKey for Challenge Response, and installed Xcode, the Xcode Command Line Tools, Homebrew, and the Yubico-PAM module. Next, we will configure the desired user account for YubiKey Authentication. You will have two different options – Screensaver (section 4.1) and User Account login (section 4.2).

1. Log into the account you want to add YubiKey Logon to, and open a Terminal window.
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 Mac 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
```

4. 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].
```

a. If the response is:

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

1. Do the following:

```
$ sudo mkdir -m0700 -p /Users/[USERNAME]/.yubico
$ sudo cp /var/root/.yubico/challenge-[YUBIKEY SERIAL NUMBER]
/Users/[USERNAME]/.yubico
```

If you have received a different response, there are a few potential errors that have occurred:

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 https://www.yubico.com/support for further troubleshooting steps.

4.1 Configuring 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.

4.2 Configuring 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 4.1:

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.