yubico

YubiKey Mac OS X Login Guide

Using Yubico Pluggable Authentication Module (PAM) with Challenge-Response

Copyright

Trademarks

Disclaimer

Contact Information

Yubico Inc
420 Florence Street, Suite 200
Palo Alto, CA 94301
USA
yubi.co/contact

Document Release Date

July 8, 2016

Contents

Introduction

Yubico changes the game for strong authentication, providing superior security with unmatched ease-of-use. Our core invention, the YubiKey, is a small USB and NFC device supporting multiple authentication and cryptographic protocols. With a simple touch, it protects access to computers, networks, and online services for the world's largest organizations.

Our innovative keys offer strong authentication via Yubico one-time passwords (OTP), FIDO Universal 2nd Factor (U2F), and smart card (PIV, OpenPGP, OATH) — all with a simple tap or touch of a button. YubiKeys protect access for everyone from individual home users to the world's largest organizations.

Introduction to Yubico Pluggable Authentication Module for your Mac

This document describes how to enable a YubiKey to protect your Mac OS X login using Yubico Pluggable Authentication Module (PAM). This includes configuring a YubiKey with the HMAC-SHA1 Challenge-Response credential needed to set up the Yubico PAM, installing the YubiKey Personalization Tool and the Yubico Pluggable Authentication Module, and configuring your Mac for Mac OS X login.

Important: Before setting up your Mac to require authentication with a YubiKey, back up your Mac using the Time Machine application. If you do not do this, you may not be able to recover your data if there is an error during setup and you are locked out of your Mac.

This document describes the following topics

Getting Help

For more information, and to get help with your YubiKeys, see:

- Support home page
- Documentation and FAQs
- Start a Support ticket

Configuring YubiKeys

We recommend that you configure the YubiKeys you plan to use with the HMAC-SHA1 Challenge-Response credential before setting up authentication with a YubiKey.

If you are configuring the YubiKeys yourself, use the YubiKey Personalization Tool (available in both graphical and command line interfaces). We recommend that you configure the YubiKeys with the YubiKey Personalization Tool graphical user interface.

Tip: You can manually program up to 100 YubiKeys easily (even more if necessary) but if you have more than 100 YubiKeys to be programmed, we recommend you contact us.

In this Chapter

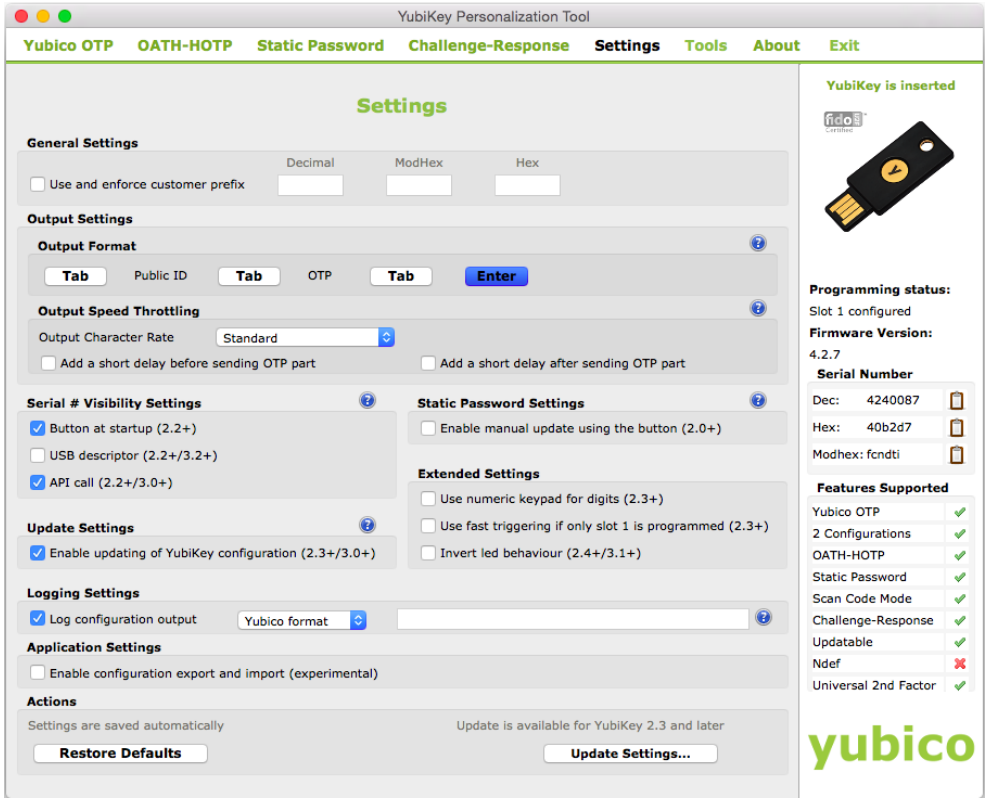
Configuring YubiKeys with the YubiKey Personalization Tool (Recommended)

The YubiKey Personalization Tool with graphical user interface is the simplest way to set up small numbers of YubiKeys with the Challenge-Response credential.

To configure your YubiKey using the YubiKey Personalization Tool graphical user interface

1. Download and install the latest version of the YubiKey Personalization Tool from the Yubico website.
2. Insert a YubiKey into a USB port of your Mac, and launch the YubiKey Personalization Tool.

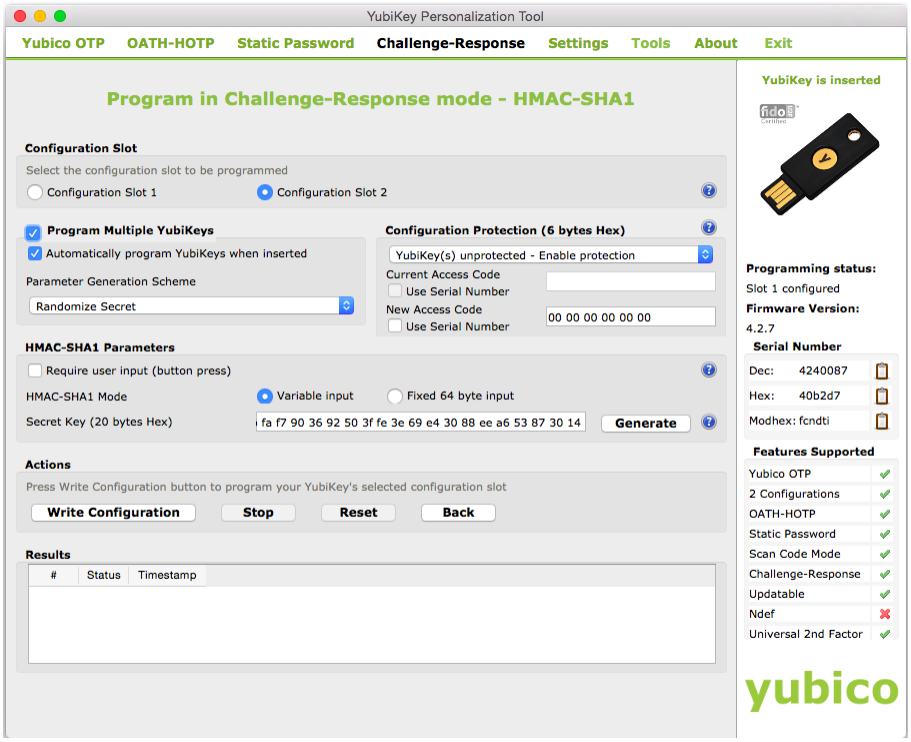
3. To create a log file that will store your secret key during configuration, click the **Settings** tab, and in the **Logging Settings** group, select **Log configuration output** and **Yubico format**.



4. Click the **Challenge-Response** tab, and click **HMAC-SHA1**.

5. In the **Configuration Slot** group, select **Configuration Slot 2**.

6. If you want to program multiple YubiKeys, select Program Multiple YubiKeys and Automatically program YubiKeys when inserted.

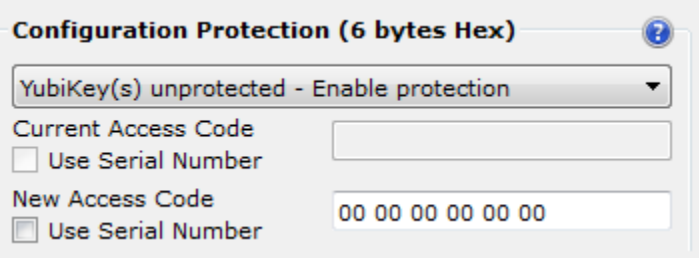


7. To lock the configuration so that you must type an access code to make changes to the configuration, in the **Configuration Protection** group, select **YubiKey(s) unprotected – enable protection**.
Important: If you set an access code and later forget it, you cannot make any programming changes to this YubiKey. You would need to buy another YubiKey.

8. To choose the type of access code to lock the YubiKey configuration, in the **Configuration Protection** group, do one of the following:

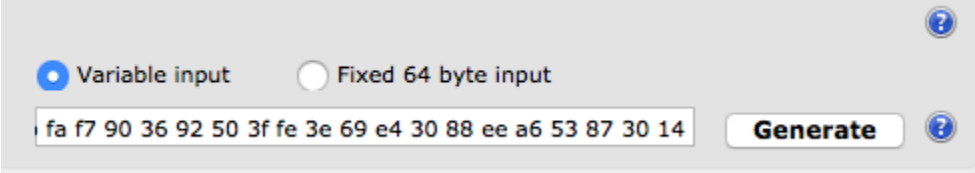
   - Type a twelve character hexadecimal access code.

- Select **Use Serial Number**. This is the serial number of the YubiKey that is inserted into the USB port on your Mac. The decimal serial number is located on the right side of the **Challenge-Response** tab.



9. In the **HMAC-SHA1 Parameters** group, clear **Require User input (button press)** and select **Variable input**.

10. To create your secret key, to the right of **Secret Key (20 bytes Hex)**, click **Generate**.



11. When you are finished configuring your YubiKey, click **Stop**.

12. If you are programming multiple YubiKeys, do the following:

    - Remove the YubiKey you just configured and insert another YubiKey to be configured into the USB port of your Mac.
    - Continue to configure the YubiKeys, one at a time, until you have finished configuring all your YubiKeys.
    - Click **Stop** when you are finished configuring YubiKeys.

Configuring YubiKeys with the Command Line Interface (Advanced Users)

Use the YubiKey Personalization Tool with the command line interface (CLI) to automate or integrate YubiKey configuration.

To configure your YubiKey using the YubiKey Personalization Tool command line interface

1. Download and install the latest version of the YubiKey Personalization Tool from the Yubico website.

2. Insert your YubiKey into a USB port on your Mac.

3. Launch a **Terminal** window.

4. To configure the YubiKey in Challenge-Response mode, from the directory where `ykpersonalize` is stored, type:

   ```
   ykpersonalize -2 -y -ochal-resp -ochal-hmac -o-chal-btn-trig -o-hmac-lt64 -
   oallow-update -c<access code> -a<secret key>
   ```

   Where you replace `<access code>` and `<secret key>` with your access code and secret key. The `<secret key>` is required and must be a 40 character hexadecimal string. The `<access code>` is optional and must be a twelve character hexadecimal string.

   Important: If you set an access code and later forget it, you cannot make any programming changes to this YubiKey. You would need to buy another YubiKey.

Example

Here is an example of a command line to type to configure a YubiKey in Challenge-Response mode. In this example, the `<access code>` is `35 8c 50 20 6a 9d` and the `<secret key>` is `66 1a 9a 32 3d 30 6d 96 90 63 33 cc 95 20 d4 8d c1 3a 73 2b`. In the actual command line, the `<access code>` and `<secret key>` do not include spaces:

```
ykpersonalize -2 -y -ochal-resp -ochal-hmac -o-chal-btn-trig -o-hmac-lt64 -
oallow-update -c358c50206a9d -a661a9a323d306d96906333cc9520d48dc13a732b
```

Installing Yubico Pluggable Authentication Module (PAM)

Once you have configured your YubiKeys with the HMAC-SHA1 Challenge-Response credential, download and install the Yubico Pluggable Authentication Module (PAM).

Yubico PAM is an application that enables you to configure your account to accept the YubiKey you programmed for authentication.

In this Chapter

To download and install Yubico PAM

1. Download the Yubico PAM package for Mac OS X logins from the Yubico Support website.
2. To start the installation, double-click the `.pkg` file you downloaded, and follow the prompts in the installation wizard.
3. To confirm the installation:
   a. Type this command at the prompt:

```
ls /usr/local/lib/security
```

   b. To determine the success of the installation:
      - If the installation was successful, the result of the `ls` command is `pam_yubico.so`.
      - If the installation was not successful, the result of the `ls` command is "`no such file or directory`."

Backing Up Your Mac Using Time Machine

Important: Before starting this process, be sure you back up your system with Time Machine. This is a very important requirement. If issues occur, it is possible to get locked out of your system and your accounts. If you get locked out, the only way to recover is to restore your Mac from a Time Machine backup that you create before editing the `authorization` file on your Mac.

You are responsible for creating the system backup before configuring your Mac for authentication with a YubiKey. To read more information about backing up your Mac with Time Machine, see Apple Support.

Configuring Yubico Pluggable Authentication Module (PAM)

Important: Before continuing with this chapter, make sure you created a system backup using Time Machine. For details, see the previous chapter, Backing up your Mac using Time Machine.

So far, you have backed up your Mac with Time Machine, configured a YubiKey with the HMAC-SHA1 Challenge-Response credential, and installed Yubico PAM.

After you create a system backup using Time Machine, use Yubico PAM to store the initial challenge and expected response, and configure the user account to require a YubiKey for authentication. You can configure your user account to require a YubiKey when deactivating the screensaver or to require a YubiKey when logging in, as described in the following sections.

In this Chapter

Storing the Initial Challenge and Expected Response with Yubico PAM

After you configure your YubiKeys with the HMAC-SHA1 Challenge-Response credential, store the initial challenge and expected response, and then verify the results. If you see error messages, be sure to correct the errors *before* continuing with this process.

To store the initial challenge and expected response

1. Log in to the account for which you want to add authentication with your YubiKey.
2. In the **Terminal** window, type the following command and press **Enter**:

   ```
   mkdir -m0700 -p ~/.yubico
   ```

3. Be sure your YubiKey is already configured for Challenge-Response (described in the previous section, Configuring YubiKeys).

4. Insert your YubiKey into a USB port on your Mac, and type the following command:

   ```
   ykpamcfg -2
   ```

5. Verify that the initial challenge and expected response were correctly stored. If the initial challenge and expected response were stored correctly, a confirmation message similar to the following appears:

   ```
   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]`, type the following command:

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

   where `[USERNAME]` is replaced with your user name and `[YUBIKEY SERIAL NUMBER]` is replaced with the seven-digit serial number for your YubiKey.

7. If you receive an error message, review the potential causes and fix the error *before* continuing with the next section. Here are the error descriptions and actions to take for each one:

   `YubiKey core error: no yubikey present`
   This error message indicates that your YubiKey is not inserted into a USB port on your Mac. If you receive this error message, insert your YubiKey into a USB port on your Mac, wait a moment for the YubiKey to initialize, then type `ykpamcfg -2` again.

   `YubiKey core error: Timeout`
   If you selected **Require User input (button press)** on the **Challenge-Response** tab of the YubiKey Personalization Tool while you were configuring your YubiKey, the YubiKey begins blinking immediately after you type the command `ykpamcfg -2`. The YubiKey blinks for approximately only two seconds and if you do not touch the YubiKey during this time, this error message appears. Remove, and then reinsert, the YubiKey into the USB port of your Mac. Type `ykpamcfg -2` again, and then touch the YubiKey when it starts blinking.

`Failed to read serial number`

This error message indicates that you inserted the YubiKey into a USB port on your Mac, but the YubiKey has not yet initialized. If you see this error message, remove and reinsert your YubiKey into a USB port on your Mac, wait about 10 seconds, then type `ykpamcfg -2` again. If you continue to experience this issue, select **Apple menu > About This Mac > System Report**. Under **Hardware**, click **USB**. The YubiKey must be found in this list. If it does not appear in this list, start a support ticket with Yubico Support.

`USB Error: kIOReturnSuccess`

This error message indicates a permissions issue. Type the command again with sudo:

```
sudo ykpamcfg -2
```

Creating a Second Set of YubiKeys for Use with Yubico PAM

Program at least two YubiKeys when implementing a requirement for authentication with a YubiKey on your Mac. If you configure only one YubiKey and something happens to the YubiKey, you must restore the Mac from a Time Machine backup that you created before editing the `authorization` file before you can log back in to your account.

To prepare a second YubiKey for Use with Yubico PAM

1. To program your second YubiKey with a Challenge-Response credential, follow the procedure in a previous chapter, Configuring YubiKeys.
2. Log in to the user account that needs a second YubiKey.
3. To create a file to store the initial challenge and expected response, open a **Terminal** window and type the following command:

   ```
   ykpamcfg -2
   ```

4. Verify that the initial challenge and expected response were stored correctly. If the challenge and response were stored correctly, a confirmation similar to the following appears:

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

Configuring the User Accounts on your Mac to Require a YubiKey

If your Mac has multiple user accounts, when you configure your Mac to require a YubiKey when deactivating the screensaver or upon logging in, that requirement applies to all user accounts. Therefore, if you have multiple user accounts, be sure each user account has a YubiKey programmed for that account. You can use the same YubiKey, or you can use a different YubiKey for each account.

For more information, see:

- Configuring Your Mac to Require a YubiKey When Deactivating the Screensaver
- Configuring Your Mac User Accounts to Require a YubiKey at Login

If you need to program additional YubiKeys, see the previous section, Configuring YubiKeys. Also be sure to create a second YubiKey for each YubiKey you configured. The second YubiKey serves as a backup for the first YubiKey you configured. You do not need to duplicate the credential you programmed for the first YubiKey. Even a backup YubiKey has its own Challenge-Response credential.

Configuring Your Mac to Require a YubiKey When Deactivating the Screensaver

The following instructions use the vi text editing application. You can use any other text editing application you prefer to use to edit system files.

Important: When you perform the steps in this section, remember that this requirement applies to all user accounts. Therefore, if you have multiple user accounts, be sure each user account has a YubiKey programmed for that account. You can use the same YubiKey, or you can use a different YubiKey for each account.

To configure your Mac to require a YubiKey when deactivating the screensaver

1. If you have multiple user accounts on your Mac and you previously configured a YubiKey for only one account, see Configuring YubiKeys previously in this document, and configure a YubiKey for each account on your Mac before continuing with these steps.
   Tip: You can program a unique Challenge-Response credential on the other YubiKeys. You do not need to duplicate the credential you programmed for the first YubiKey.
2. Open a **Terminal** window, and type this command:

   ```
   sudo vi /etc/pam.d/screensaver
   ```

3. Type your administrator password, and press **Enter**.
4. Verify that the **Terminal** window now begins with:

   ```
   # screensaver: auth account
   ```

5. To change from Command Mode to Insert Mode, press the **i** key.

   — INSERT — should appear at the bottom of the **Terminal** window..

6. Press the **Down Arrow** key to move to the first letter of the first line that begins with `account`.

7. To create a blank line, press **Enter**.

8. Press the **Up Arrow** key to move to the blank line that you just created. Type the following command:

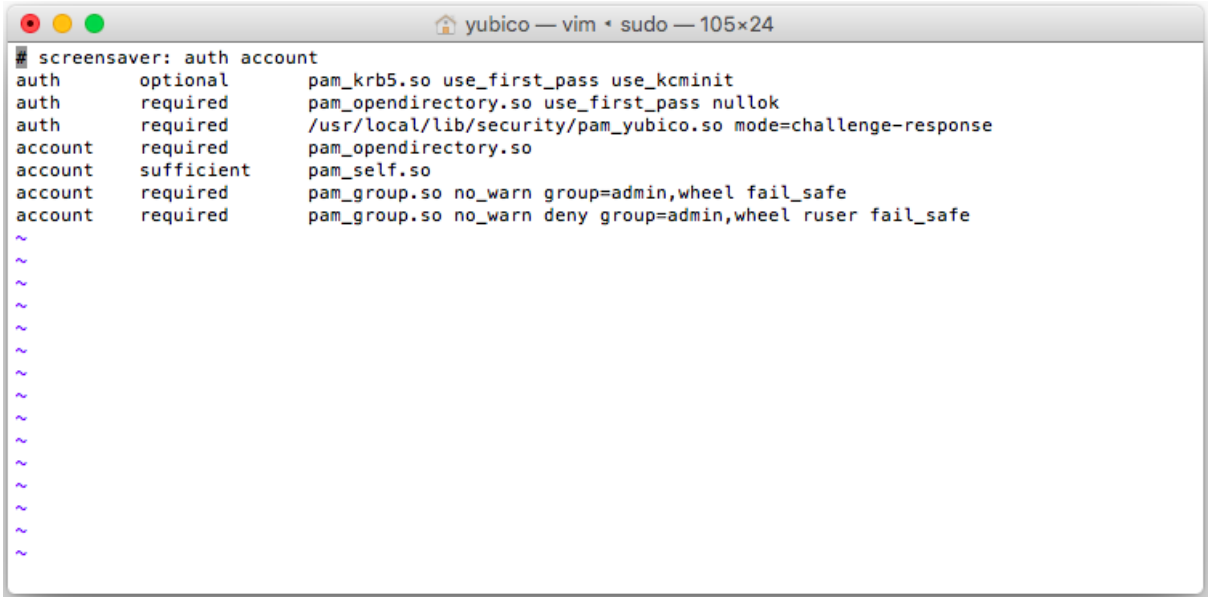
   ```
   Auth
   ```

9. Press **Spacebar** seven times (to align the text), and type:

   ```
   Required
   ```

10. Press **Spacebar** seven times again (to align the text), and type:

    ```
    /usr/local/lib/security/pam_yubico.so mode=challenge-response
    ```



11. To exit Insert Mode and return to Command Mode, press **Esc**.

12. To save the changes you made, type `ZZ` (it is important to capitalize the Z letters, as lowercase letters do not save the file).

13. Close the **Terminal** window.

14. To test that your YubiKey is required to deactivate the screensaver, remove your YubiKey when the screensaver activates, type your password, and the unlock attempt should fail.

    Note: To speed up this process for testing purposes, select **Apple Menu > System Preferences > Desktop & Screen Saver**, click **Screen Saver**, and change **Start after** to **1 Minute**.

Configuring Your Mac User Accounts to Require a YubiKey at Login

The following instructions use the vi text editing application. You can use any other text editing application you prefer to use to edit system files.

Important: When you perform the steps in this section, remember that this requirement applies to all user accounts. Therefore, if you have multiple user accounts, be sure each user account has a YubiKey programmed for that account. You can use the same YubiKey, or you can use a different YubiKey for each account.

To configure your Mac user accounts to require a YubiKey when logging in to the account

1. If you have multiple user accounts on your Mac and you previously configured a YubiKey for only one account, see Configuring YubiKeys previously in this document, and configure a YubiKey for each account on your Mac before continuing with these steps.
2. Open a **Terminal** window, and type:

   ```
   sudo vi /etc/pam.d/authorization
   ```

3. Type your administrator password, and press **Enter**.
4. Verify that the **Terminal** window now begins with:

   ```
   # authorization: auth account
   ```

5. To change from Command Mode to Insert Mode, press the **i** key.

   `-- INSERT --` should appear at the bottom of the **`Terminal`** window.
6. Press the **Down Arrow** key to move to the first letter of the first line that begins with `account`.
7. To create a blank line, press **Enter**.
8. Press the **Up Arrow** key to move to the blank line that you just created, and type this command:

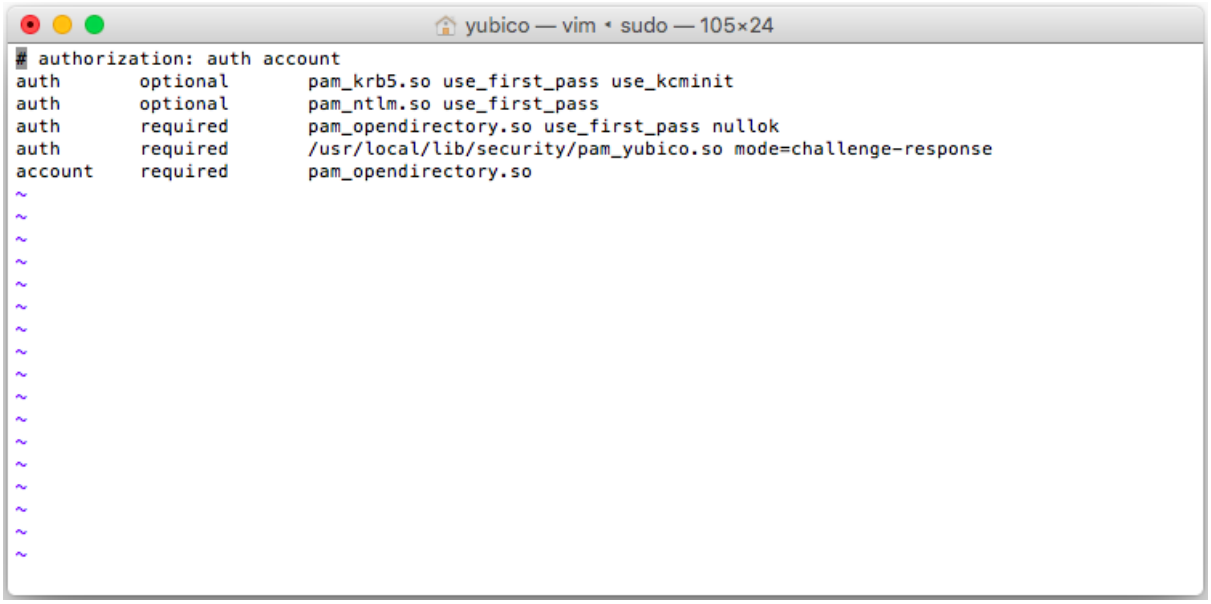
   ```
   auth.
   ```

9. Press **Spacebar** seven times (to align the text), and type:

   ```
   required
   ```


10. Press **Spacebar** seven times again (to align the text), and type:

    ```
    /usr/local/lib/security/pam_yubico.so mode=challenge-response
    ```



11. To exit Insert Mode and return to Command Mode, press **Esc**.

12. To save the changes you made, type `ZZ` (it is important to capitalize the Z letters, as lowercase z letters do not save the file).

13. Close the **Terminal** window.

14. To test that your YubiKey is required, log out of your user account, remove the YubiKey, and then attempt to log back in without the YubiKey inserted.

    The login should fail.

15. To test the Challenge-Response credential of your YubiKey, insert your YubiKey into a USB port on your Mac, wait a few moments, and then log in again.

    The login should succeed.

Disabling the YubiKey Requirement

This chapter describes how to remove the YubiKey requirement for unlocking the screensaver and for logging into the user accounts on your Mac.

In this Chapter

Disabling the YubiKey Requirement for Deactivating the Screensaver

This section shows you how to disable the YubiKey requirement for deactivating the screensaver.

Important: When you perform the steps in this section, remember that this change applies to all user accounts.

To remove the screensaver requirement

1. Open a **Terminal** window, and type this command:

   ```
   sudo vi /etc/pam.d/screensaver
   ```

2. Type your administrator password, and press **Enter**.

3. Verify that the **Terminal** window now begins with:

   ```
   # screensaver: auth account
   ```

4. To change from Command Mode to Insert Mode, press the **i** key.

   ```
   - INSERT - should appear at the bottom of the Terminal window.
   ```

5. Remove the line that you added in the previous section to enable the YubiKey requirement:

   ```
   auth  required  /usr/local/lib/security/pam_yubico.so mode=challenge-response
   ```

6. To exit Insert Mode and return to Command Mode, press **Esc**.

7. To save the changes you made, type `ZZ` (it is important to capitalize the Z letters, as lowercase z letters do not save the file.)

8. Close the **Terminal** window.

9. To test that your YubiKey is no longer required to deactivate the screensaver, remove your YubiKey when the screensaver activates, type your password, and the unlock attempt should succeed.

   NOTE: To speed up this process for testing purposes, select Apple Menu > System Preferences > Desktop & Screen Saver, click Screen Saver, and change Start after to 1 Minute.

Disabling the YubiKey Requirement for Logging into Your Mac

This section shows you how to disable the YubiKey requirement for logging into the Mac.

Important: When you perform the steps in this section, remember that this change applies to all user accounts.

To remove the authorization requirement

1. Open a **Terminal** window, and type:

   sudo vi /etc/pam.d/authorization

2. Type your administrator password, and press **Enter**.

3. To change from Command Mode to Insert Mode, press the **i** key.

   `- INSERT - should appear at the bottom of the Terminal window.`

4. Press the **Down Arrow** key to move to the first letter of the first line that begins with `account`.

5. Remove the line that you added in the previous section to enable the YubiKey requirement:

   `auth required /usr/local/lib/security/pam_`yubico.so mode=challenge-response

6. To exit Insert Mode and return to Command Mode, press **Esc**.

7. To save the changes you made, type `ZZ` (it is important to capitalize the Z letters, as lowercase z letters do not save the file.)

8. Close the **Terminal** window.

9. To test that your YubiKey is no longer required, log out of your user accounts, remove the YubiKey, and then attempt to log back in without the YubiKey inserted.

   The login should succeed.