yubico

How to Configure Identical Credentials in Challenge-Response

Configuration Guide

Copyright

Trademarks

Disclaimer

Contact Information

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

Document Release Date

June 22, 2016

yubico

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.

Configuring Two YubiKeys with Identical Credentials

This guide shows you how to configure two YubiKeys with identical credentials in challenge-response authentication with HMAC-SHA1 so you can use them interchangeably in applications that require challenge-response (for example, the PasswordSafe application).

CAUTION: YubiKeys come shipped with Configuration Slot 1 preconfigured for Yubico OTP. Be careful about overwriting this default configuration. This guide assumes that you will use Configuration Slot 2 which, by default, is not configured.

This document describes the following topics:

Getting Additional Help

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

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

Before You Begin

Before you configure two YubiKeys with identical credentials in challenge-response mode, be sure you: understand the requirements, install the YubiKey Personalization Tool, understand why you should configure at least two YubiKeys with the same credential, and install PasswordSafe or some other application to test your YubiKeys.

In this Chapter

Requirements

This section lists the required components to configure and test two YubiKeys with identical credentials:

- Two (2) YubiKeys with firmware version 2.2 or later (one will be used as a backup YubiKey)
- The YubiKey Personalization Tool (downloaded from the Yubico website for configuring your YubiKeys for challenge-response authentication with HMAC-SHA1
- An application, such as PasswordSafe, to test that your YubiKeys have identical credentials

Installing the YubiKey Personalization Tool

Before you configure two YubiKeys with the same credentials, be sure you install the YubiKey Personalization Tool if you have not already done so. The YubiKey Personalization Tool is needed to configure your YubiKeys for challenge-response authentication using HMAC-SHA1.

To install the YubiKey Personalization Tool

1. Download the latest version of the YubiKey Personalization Tool from the Yubico website for the operating system you are using.
2. To install the application, do one of the following:

   - For Windows:

   a. To launch the installation wizard, click the `yubikey-personalization-gui-x.x.x.exe` file.

      where `x.x.x` is the version for the file you downloaded.

   b. Complete the installation wizard.

   - For Mac OS X:

   a. To launch the installation wizard, and double-click the `YubiKey Personalization Tool Installer-mac.dmg` file.

   b. Complete the installation wizard.

   - For Linux:

   a. Build the YubiKey Personalization Tool on a Linux distro.
      TIP: For information on how to build the project and create the YubiKey Personalization Tool executable on your Linux platform, see the Yubico Developers website.

   b. Launch and complete the installation process for your Linux distro.

Configuring Two YubiKeys with the Same Secret Key

These instructions configure two YubiKeys -- one which will be used as a backup YubiKey. For two YubiKeys to work interchangeably in applications that require challenge-response authentication (such as, PasswordSafe), they need to be configured with the same secret key. When configuring two YubiKeys with the same credential, be sure you record the secret key so that you can configure each of your YubiKeys with the same secret key.

If you decide to program multiple YubiKeys at one time, the YubiKey Personalization Tool automatically configures each of your YubiKeys with the same secret key. The procedures described in the next chapter, Configuring your YubiKeys, provide detailed instructions about automatically configuring two YubiKeys with the same secret key.

IMPORTANT: If you do not configure a second YubiKey with the same credential as the original YubiKey, you risk locking yourself out of your applications. Be sure to use these instructions to configure at least

two YubiKeys with the same credential so that you always have a second YubiKey to use with your application.

Installing an Application to Test Your YubiKeys

After you are finished configuring your two YubiKeys with the same secret key, we recommend you test that they are configured identically by testing them in an application, such as PasswordSafe.

Configuring Your YubiKeys

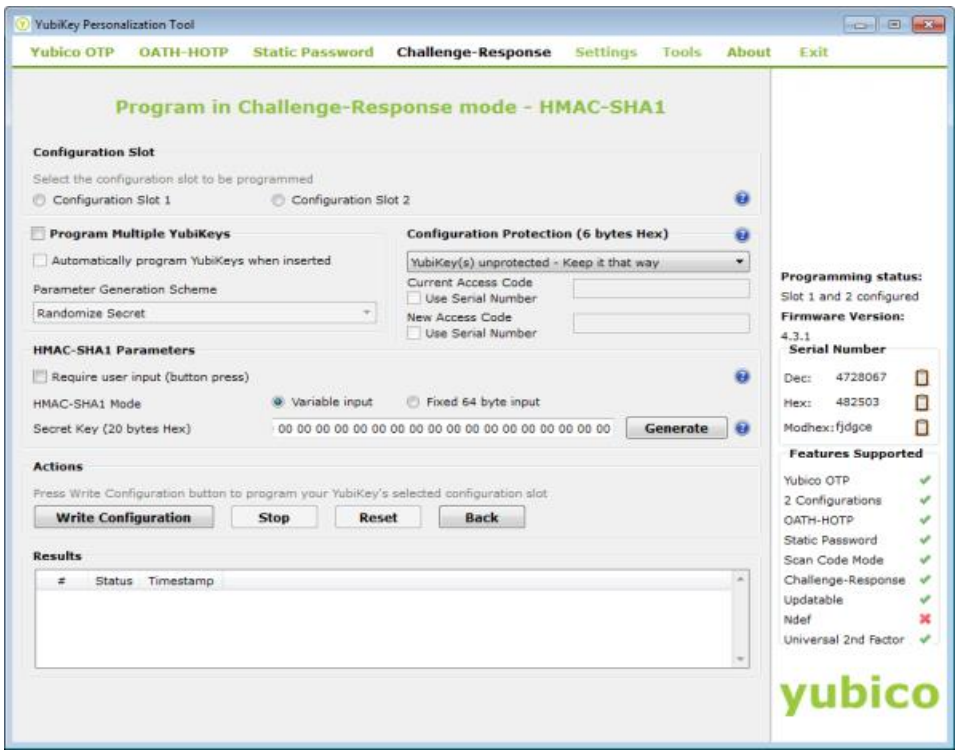
Before you can use your YubiKeys, you need to configure your YubiKeys for challenge-response authentication using the YubiKey Personalization Tool.

Using the challenge-response authentication mode with HMAC-SHA1 algorithm, a challenge and a response are created in combination with a secret key. In this mode, your YubiKey does not make use of any variables and generates an identical response each time if the challenge is the same.

In this Chapter

To program Your YubiKeys for challenge-response with HMAC-SHA1

1. Insert a YubiKey into a USB port of your computer.
2. Launch the YubiKey Personalization Tool.
3. Click the **Settings** tab, and:
   - Be sure that **Button at startup** and **API call** are selected.
   - Click **Update Settings**.
4. Click the **Challenge-Response** tab, and then click **HMAC-SHA1**.



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

6. To program a backup YubiKey (recommended), select **Program Multiple YubiKeys** and **Automatically program YubiKeys when inserted**.

7. In the **Parameter Generation Scheme** group, select **Same Secret for all Keys**.

8. In the **Configuration Protection** group, do one of the following:

    - To lock the configuration so that you must type an access code to make changes to the configuration, do the following:

        a. Locate **YubiKey(s) unprotected – Keep it that way** and set it to **YubiKey(s) unprotected – Enable Protection**. The **New Access Code** field below the menu becomes active.

        b. In **New Access Code**, type a 12-digit, numeric access code; or select **Use Serial Number**.

        NOTE: Record this access code in a safe location as you cannot update the YubiKey configuration without it.

    - If you do not want to use an access code, keep the default, **YubiKey(s) unprotected – Keep it that way**.

9. In the **HMAC-SHA1 Parameters** group, select the following options:

    - **IMPORTANT**: If you are configuring your YubiKeys for the YubiKey Windows Login application, be sure you do *not* select **Require user input**.

    - For HMAC-SHA1 Mode, select **Variable input**.

    - To create the **Secret Key**, click **Generate** and then:

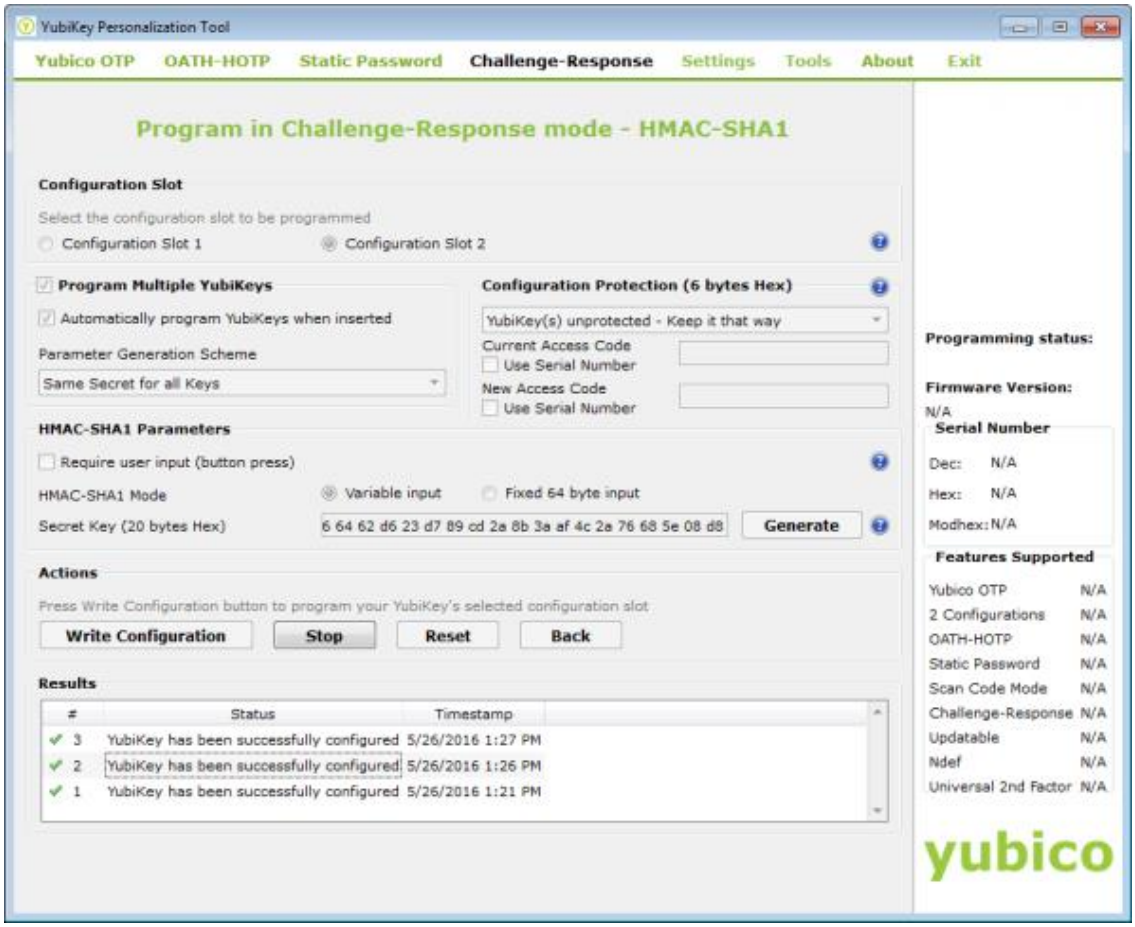
        - To configure your YubiKey for challenge-response in HMAC-SHA1 mode, from the **Actions** group, click **Write Configuration**.
          TIP: When your YubiKey configuration is successful, a message displays under **Results** confirming the configuration (for each YubiKey that you configure).

10. To program the second YubiKey with the same secret key:

    a. Remove the YubiKey you just configured and insert another YubiKey to be configured into a USB port of your computer.

    b. If you did not select **Automatically program YubiKeys when inserted**, click **Write Configuration** each time you insert a new YubiKey.

11. Click **Stop** when you are finished configuring both YubiKeys.



To test your YubiKeys

- Install an application (such as PasswordSafe), and test that your YubiKeys have identical credentials.

