yubico

YubiKey for YubiCloud Configuration Guide

With the YubiKey Personalization Tool

Copyright

© 2016 Yubico Inc. All rights reserved.

Trademarks

Yubico and YubiKey are registered trademarks of Yubico Inc. All other trademarks are the property of their respective owners.

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.

Contact Information

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

Document Release Date

June 20, 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.

YubiKey for YubiCloud

You can use the YubiKey Personalization Tool application to configure your YubiKey for Yubico OTP, and then upload the AES key to the Yubico validation server. You can then add your YubiKey to your supported service provider or application.

When we ship the YubiKey, Configuration Slot 1 is already programmed for Yubico OTP and ready to use, and Configuration Slot 2 is not configured. Use this guide to overwrite Configuration Slot 1 or to configure Configuration Slot 2 as needed.

This document describes the following topics:

- Installing the YubiKey Personalization Tool

- Configuring Your YubiKey for YubiCloud

Getting Additional Help

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

- Support home page

- Documentation and FAQs

- Start a Support ticket

Installing the YubiKey Personalization Tool

This chapter describes how to download and install the YubiKey Personalization Tool for your operating system.

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 Your YubiKey for YubiCloud

This chapter shows you how to configure your YubiKey for Yubico OTP, upload the AES key to the Yubico validation server, and test your YubiKey configuration so that you can add your YubiKey to a YubiCloud supporting site or service.

In this Chapter

About Yubico OTP

Each YubiKey has two slots. Configuration Slot 1 is used to generate the passcode when you touch the YubiKey button for between 0.3 and 1.5 seconds and then release. Configuration Slot 2 is used if you touch the button for between 2 and 5 seconds and then release.

When we ship the YubiKey, Configuration Slot 1 is already programmed for Yubico OTP and ready to use, and Configuration Slot 2 is not configured.

**To test that your YubiKey is generating One-Time Passwords**

1. Open a text editor.

2. Insert your YubiKey into a USB port of your computer, and touch the gold button. If you see `cccccc` in the text editor, then your YubiKey is generating OTPs, which means that you do not need to program your YubiKey for Yubico OTP.

To configure your YubiKey for Yubico OTP (or overwrite the existing configuration)

NOTE: You cannot use a FIDO U2F Security Key to configure for Yubico OTP.

1. Insert your YubiKey into a USB port of your computer.

2. Launch the YubiKey Personalization Tool. To do this:

   a. On Windows:

   - Double-click the YubiKey Personalization Tool shortcut.

   b. On Mac OS X:

   - Start the YubiKey Personalization Tool.

c. On Linux:

- Start the YubiKey Personalization Tool.

3. Click Yubico OTP or Yubico OTP Mode, and then click Quick.

4. In the **Configuration Slot** group, select a configuration slot. (By default, **Configuration Slot 1** is used). The YubiKey Personalization Tool automatically generates the Yubico OTP Parameters.

5. If you want to regenerate the Yubico OTP Parameters, in the **Actions** group, click **Regenerate**.
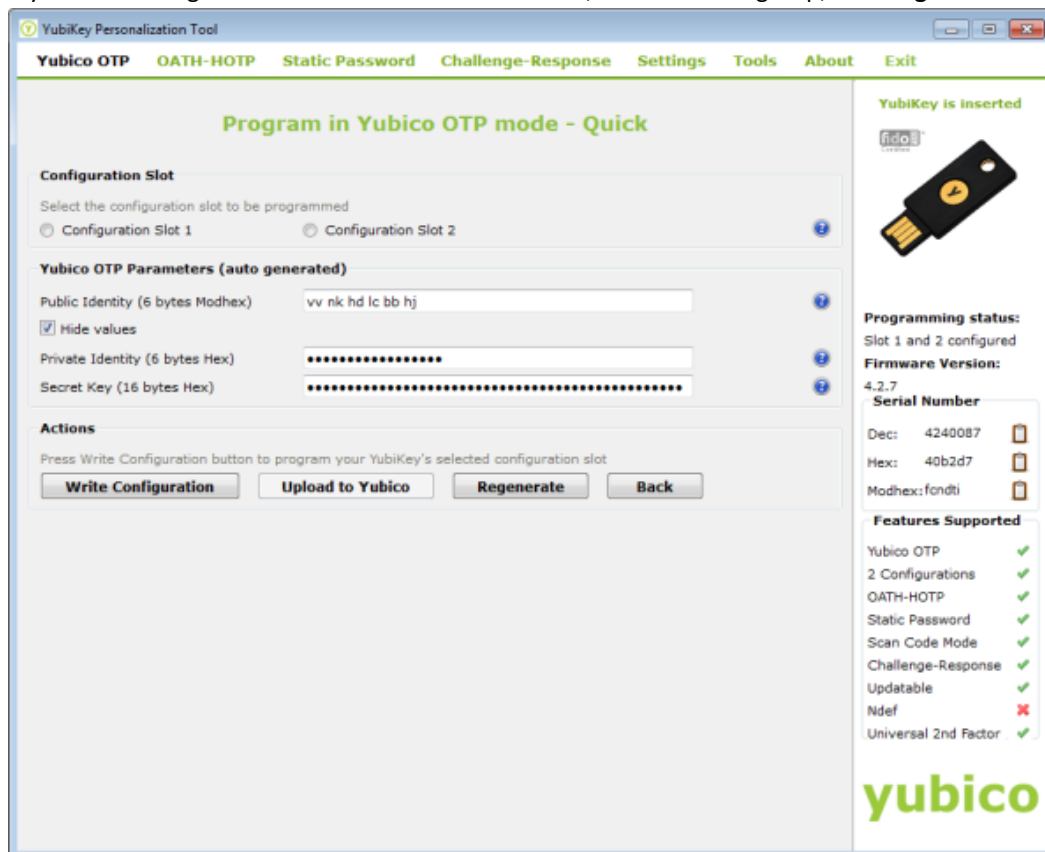
6. To reprogram your YubiKey in standard Yubico OTP mode, in the **Actions** group, click **Write Configuration**.
   TIP: When the YubiKey configuration is successful, a message displays in the window confirming the configuration.

7. To upload the AES key to the Yubico validation server, in the **Actions** group, click **Upload to Yubico**.
   NOTE: This also populates the corresponding fields on the **Yubico AES Key Upload** window with the values for reprogramming your YubiKey.

8. Type your email address, and place your cursor in **OTP from the YubiKey**.

9. Before you click Upload AES key, verify that your YubiKey prefix is correct:

   a. Open a text editor and touch your YubiKey. The first twelve characters are the prefix (the YubiKey Public Identity).

b. In the **Yubico AES Key Upload** window, compare **YubiKey prefix** with the results from the text editor.

Type the CAPTCHA, and click **Upload AES key**.

NOTE: Typically, you can test your YubiKey immediately. If necessary, wait approximately 10-15 minutes for all the corresponding databases to validate your OTP with the online Yubico OTP validation server.

To test your YubiKey with the YubiCloud validation server (demo.yubico.com)

- See our demo server to test your YubiKey.

To add your YubiKey to a YubiCloud supporting service

- Once your YubiKey is working with the demonstration server, you can add your YubiKey to your YubiCloud site or service. For more information about getting your YubiKey to work with a particular site or YubiCloud service, see the documentation on their website or contact their support department.