

# Cross-platform YubiKey Personalization Tool

---

## User Guide

Software Version 3.0.1  
Document Version 1.1

**May 14, 2012**

## Introduction

Yubico is the leading provider of simple, open online identity protection. The company's flagship product, the YubiKey®, uniquely combines driverless USB hardware with open source software. More than a million users in 100 countries rely on YubiKey strong two-factor authentication for securing access to computers, mobile devices, networks and online services. Customers range from individual Internet users to e-governments and Fortune 500 companies. Founded in 2007, Yubico is privately held with offices in California, Sweden and UK.

## 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**  
228 Hamilton Avenue, 3rd Floor  
Palo Alto, CA 94301  
USA  
[info@yubico.com](mailto:info@yubico.com)

## Contents

---

Introduction.....	2
Disclaimer.....	2
Trademarks .....	2
Contact Information.....	2
1 Document Information.....	5
1.1 Purpose.....	5
1.2 Audience .....	5
1.3 References.....	5
1.4 Document History.....	5
1.5 Definitions.....	5
2 Introduction.....	6
3 Background and Pre-Requisites .....	7
3.1 System Requirements.....	7
3.1.1 Windows Platform .....	7
3.1.2 Linux Platform .....	7
3.1.3 MAC OS X Platform .....	7
3.2 Random numbers.....	7
3.2.1 Windows Platform .....	7
3.2.2 Linux Platform .....	7
3.2.3 MAC OS X Platform .....	7
3.3 Security and cryptographic practices .....	8
4 Installation .....	9
4.1 Downloading the cross-platform YubiKey Personalization Tool .....	9
4.2 Installing the application.....	9
4.2.1 Windows Platform .....	9
4.2.2 Linux Platform .....	12
4.2.3 MAC OS X Platform .....	12
5 Using the application.....	14
5.1 Common Tasks and settings.....	14
5.1.1 Getting the YubiKey Firmware version.....	14
5.1.2 Settings .....	15
5.1.3 Tools.....	17
5.1.4 Getting help .....	18
5.2 Creating a Yubico OTP configuration .....	18
5.2.1 Quick Option.....	18

5.2.2	Advanced Option.....	22
5.3	Creating a OATH-HOTP Configuration.....	27
5.3.1	Quick Option.....	27
5.3.2	Advanced Option.....	30
5.4	Create a static configuration (Static Password).....	34
5.4.1	Scan code .....	34
5.4.2	Advanced Option.....	39
5.5	Challenge-Response mode.....	45
5.5.1	Yubico OTP .....	45
5.5.2	HMAC-SHA1 .....	49

# 1 Document Information

---

## 1.1 Purpose

The purpose of this document is to provide an in-depth explanation of the YubiKey configuration process using the Cross-platform YubiKey Personalization Tool (earlier known as YubiKey Configuration Utility).

The document does not cover a “systems perspective”, but rather focuses on the process of configuring.

## 1.2 Audience

This document is intended primarily for readers with a technical/IT background. The document assumes knowledge of basic security concepts and terminology.

Furthermore, basic knowledge of YubiKey concepts is assumed. More information about this topic can be found in the “Related documentation section”

## 1.3 References

- The YubiKey Manual – Usage, configuration and introduction of basic concepts
- YubiKey configuration COM API – Describes the configuration component
- YubiKey Client COM API – Describes the client-side API
- YubiKey Server COM API – Describes the server-side API
- Yubico online forum – <http://forum.yubico.com>
- RFC 2104 - HMAC: Keyed-Hashing for Message Authentication
- RFC 4226 – HOTP: An HMAC-Based One-Time Password Algorithm

## 1.4 Document History

Date	Version	Author	Activity
2011-07-22	1.0	KL and SP	New release
2012-05-14	1.1	ZD	Changed document template

## 1.5 Definitions

Term	Definition
YubiKey device	Yubico’s authentication device for connection to the USB port
USB	Universal Serial Bus
HID	Human Interface Device. A specification of typical USB devices used for human interaction, such as keyboards, mice, joysticks etc.
AES	Advanced Encryption Standard, FIPS-197
UID	Unit Identity, a.k.a. Private Id or Secret Id
Ticket	A general term for an access code generated by the Yubikey, a.k.a. OTP.
OTP	One Time Password
Modhex	Modified Hexadecimal coding

## 2 Introduction

---

Yubico, a security company founded in 2007, with offices located in London and Stockholm Sweden, for the European offices and in Sunnyvale California, for the North American office.

Yubico's mission is to "make Internet identification secure, easy, and affordable for everyone". The Company offers a physical authentication device/token, the YubiKey, which is used to provide secure authentication to web services and various other applications.

The YubiKey device is a tiny key-sized one-button authentication device, emulating a USB keyboard and designed to generate a unique user identity and a one-time password without requiring any software installed on the computer. When YubiKey is inserted to a USB port on a computer and the illuminated button on the device is pressed, YubiKey sends an OTP (One Time Password) to the computer as a sequence of keyboard characters, thus saving the user from typing.

The Yubico Personalization Tool is a cross platform utility (working on Windows, Linux and MAC) designed to configure the YubiKey. The utility follows a simple step-by-step approach to make configuration easy to follow and to understand, while still being powerful enough to exploit all functionality both of the YubiKey 1 and YubiKey 2 generation of keys.

The YubiKey Configuration Utility provides the following main functions:

Programming a YubiKey in dynamic "OTP" mode

Programming a YubiKey in static "password" mode

Programming the YubiKey in OATH-HOTP dynamic "OTP" mode

Programming the YubiKey in Challenge-Response mode

Checking the type and firmware version of a YubiKey

The YubiKey Configuration Utility provides basic means of batch processing where a larger number of keys can be configured sequentially.

Configuration input can be randomized or increased in sequential order. Output of the configuration process can be written to a text file which later can be imported into various Yubico applications.

## 3 Background and Pre-Requisites

---

Before installing the cross-platform YubiKey Personalization Tool, the following pre-requisites need to be met:

### 3.1 System Requirements

The cross-platform YubiKey Personalization Tool is available for Windows, Linux and MAC OS X platforms. The cross-platform tool has the following system requirements on each platform:

#### 3.1.1 Windows Platform

The YubiKey Personalization Tool is designed to run on all Microsoft Windows Win 32 and 64 bit environments from Windows XP and onwards.

#### 3.1.2 Linux Platform

The YubiKey Personalization Tool can run on any Linux based system. The Graphical User Interface is required for running the application.

#### 3.1.3 MAC OS X Platform

The YubiKey Personalization Tool is available for the Intel based MAC OS X.

### 3.2 Random numbers

#### 3.2.1 Windows Platform

Wherever random number generation is used in the application, the random values are generated using the Win32 Crypto API function CryptGenRandom, which should satisfy most needs. There is no special seeding or additional obfuscation added.

#### 3.2.2 Linux Platform

Wherever random number generation is used in the application, the random values are generated using any one of /dev/srandom, /dev/urandom or /dev/random devices. First the application tries to open and read random bytes from the "/dev/srandom" device. If the device is not found or random bytes cannot be read, then it tries to achieve the same thing with the next device i.e. "/dev/urandom" and so on.

#### 3.2.3 MAC OS X Platform

Wherever random number generation is used in the application, the random values are generated using any one of /dev/srandom, /dev/urandom or /dev/random devices. First the application tries to open and read random bytes from the "/dev/srandom" device. If the device is not found or random bytes cannot be read, then it tries to achieve the same thing with the next device i.e. "/dev/urandom" and so on.

### 3.3 Security and cryptographic practices

The user must be aware of the appropriate security and cryptographic practices needed to maintain the integrity of the generated configurations.

There is absolutely “no black magic” with the application in this respect, but because cryptographically sensitive information is handled and potentially read from and/or stored on persistent local storage, security aspects need to be fully understood.



## 4 Installation

---

Please follow the steps below to install the cross-platform YubiKey Personalization Tool for Windows, Linux and MAC platforms

### 4.1 Downloading the cross-platform YubiKey Personalization Tool

Please download the latest YubiKey Personalization Tool for your platform from the link below:

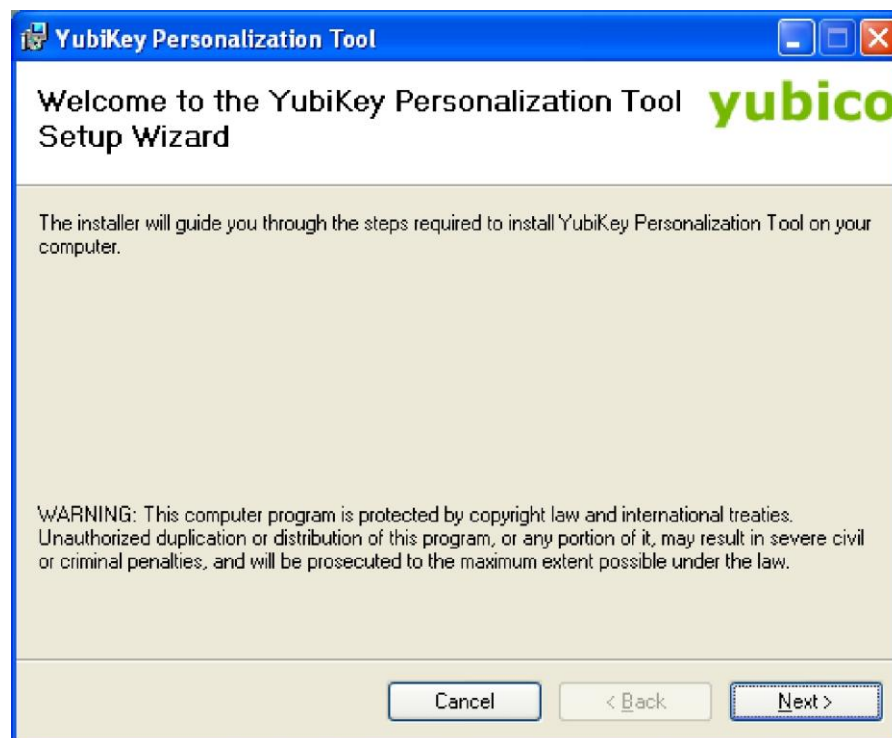
<http://www.yubico.com/personalization-tool>

### 4.2 Installing the application

The YubiKey Personalization Tool is a stand-alone application that runs without any other dependencies. This means that the application file alone can simply be copied to a second computer without running the installer.

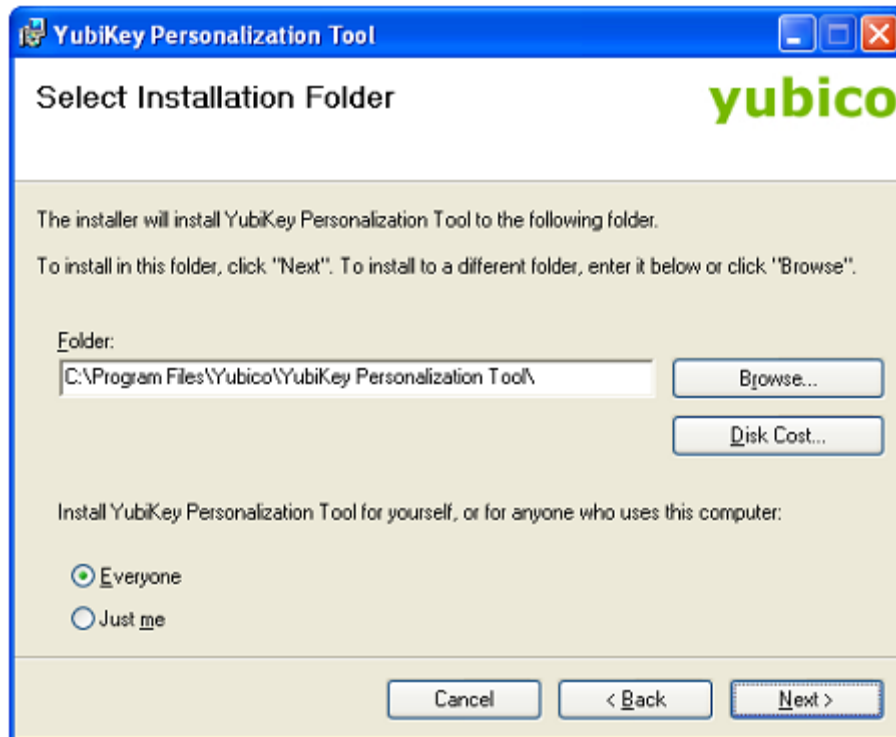
#### 4.2.1 Windows Platform

- 1) Download the Cross-Platform Personalization tool for Windows
- 2) Double click on the downloaded “YubiKey Personalization Tool Installer-win signed.msi” file
- 3) The setup wizard will start as shown in the image below:



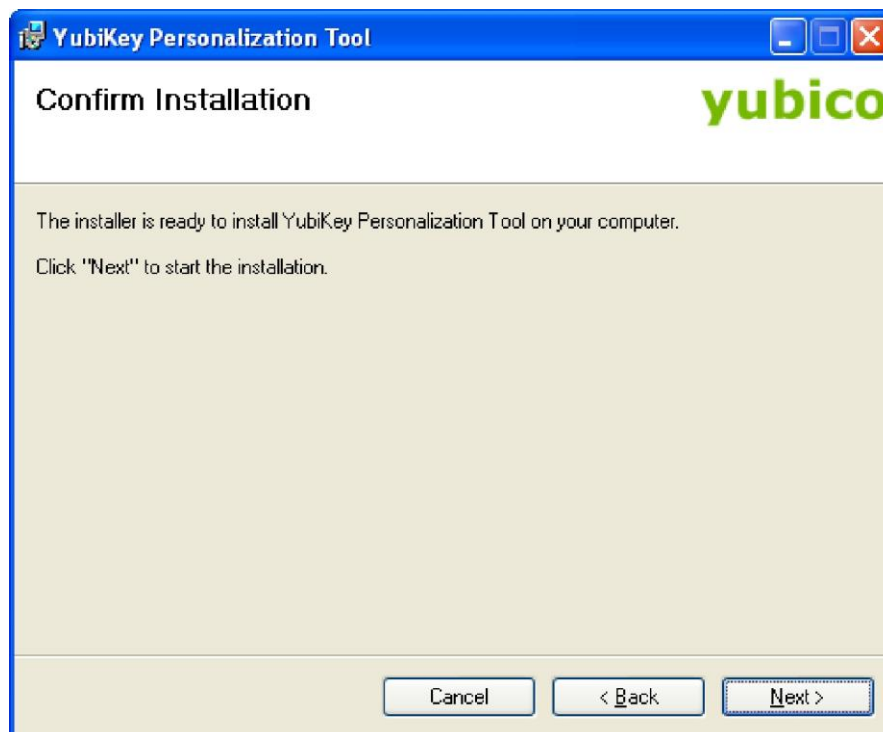
Click on the “Next” button.

- 4) Select the desired installation folder. By default, the tool will be installed in the “Program Files” directory of your Windows boot partition

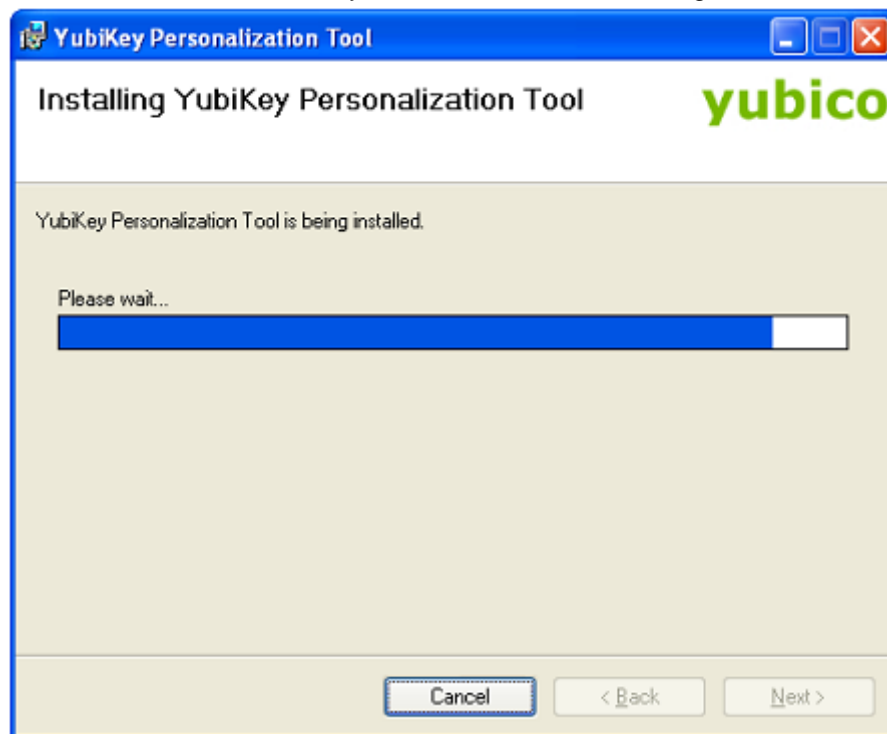


Click on the "Next" button

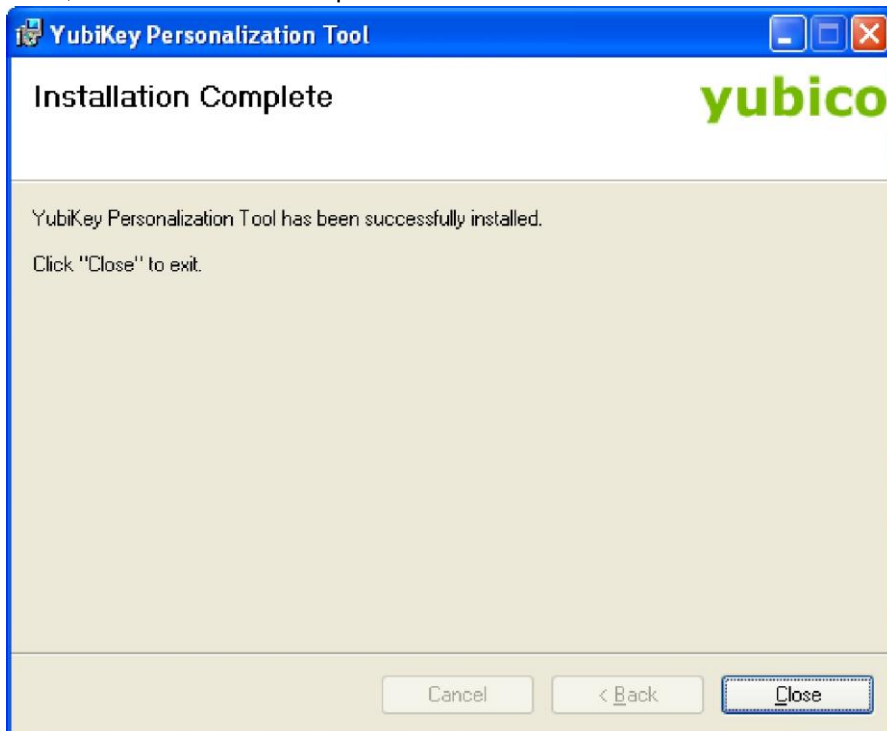
- 5) At the "Confirm Installation" screen, click on the "Next" button



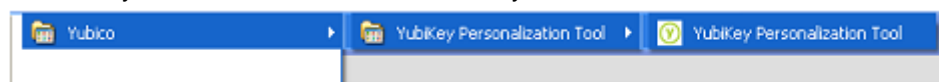
- 6) The installation of the YubiKey Personalization Tool will begin



- 7) Once, the installation is complete click on the "Close" button



- 8) You can start the YubiKey Personalization Tool from start → All Programs → Yubico → YubiKey Personalization Tool → YubiKey Personalization Tool



#### 4.2.2 Linux Platform

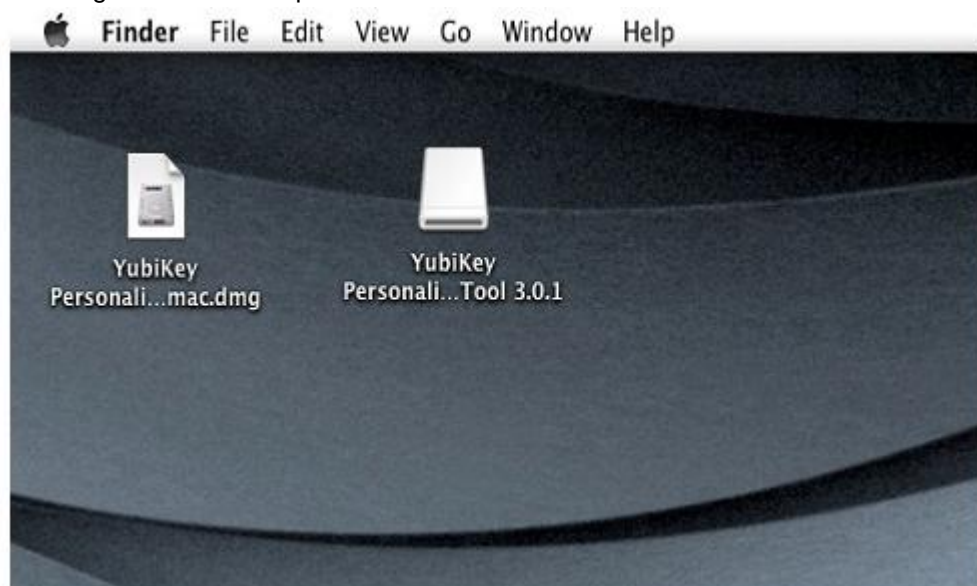
- 1) Download the Cross-Platform Personalization tool for Linux
- 2) Open the command shell
- 3) Extract the YubiKey Personalization Tool files by executing the following command:  
`# tar -xvzf "YubiKey Personalization Tool Installer-lin.tgz"`  
This will extract the files under the Yubico folder
- 4) Run the YubiKey Personalization Tool by executing the following command:  
`# sudo sh "Yubico/YubiKey\ Personalization\ Tool.sh"`

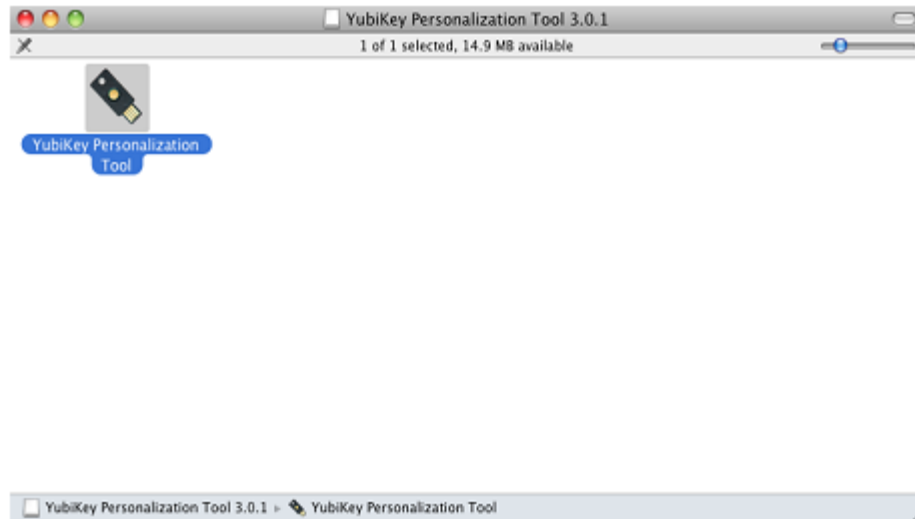
#### 4.2.3 MAC OS X Platform

- 1) Download the Cross-Platform Personalization tool for Mac OS X (Intel)
- 2) Double click on the "YubiKey Personalization Tool Installer-mac.dmg" file

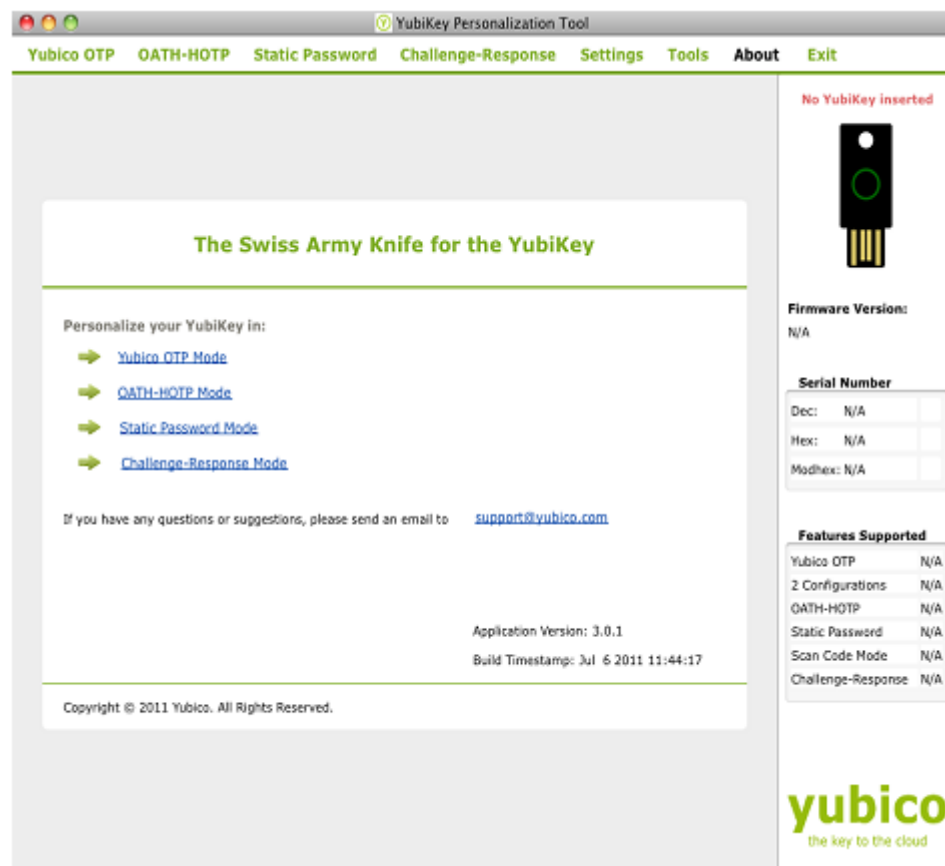


- 3) This will mount the content of the YubiKey Personalization Tool dmg package as a file storage disk and will open the content of the mounted disk in a file browser.





- 4) Double click on the YubiKey Personalization Tool. This will open the YubiKey Personalization Tool



## 5 Using the application

The cross-platform YubiKey Personalization Tool provides the same functionality and user interface on Windows, Linux and MAC platforms.

In this guide we are using the cross platform YubiKey Personalization Tool on Windows platform but the functionality is the same on all platforms.

The functionality provided by the YubiKey Personalization Tool is explained in detail in the following sections.

### 5.1 Common Tasks and settings

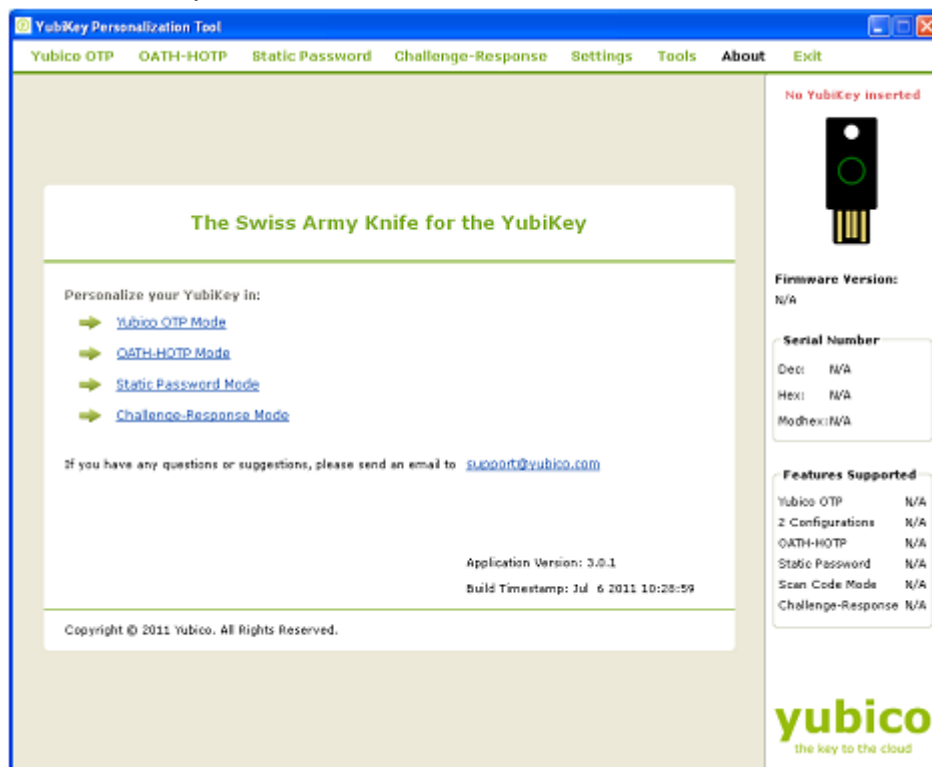
You can use the YubiKey Personalization Tool to carry out some common tasks like finding out the YubiKey firmware information and other details.

Also, there are settings which apply to all the tasks. These tasks and settings are described below:

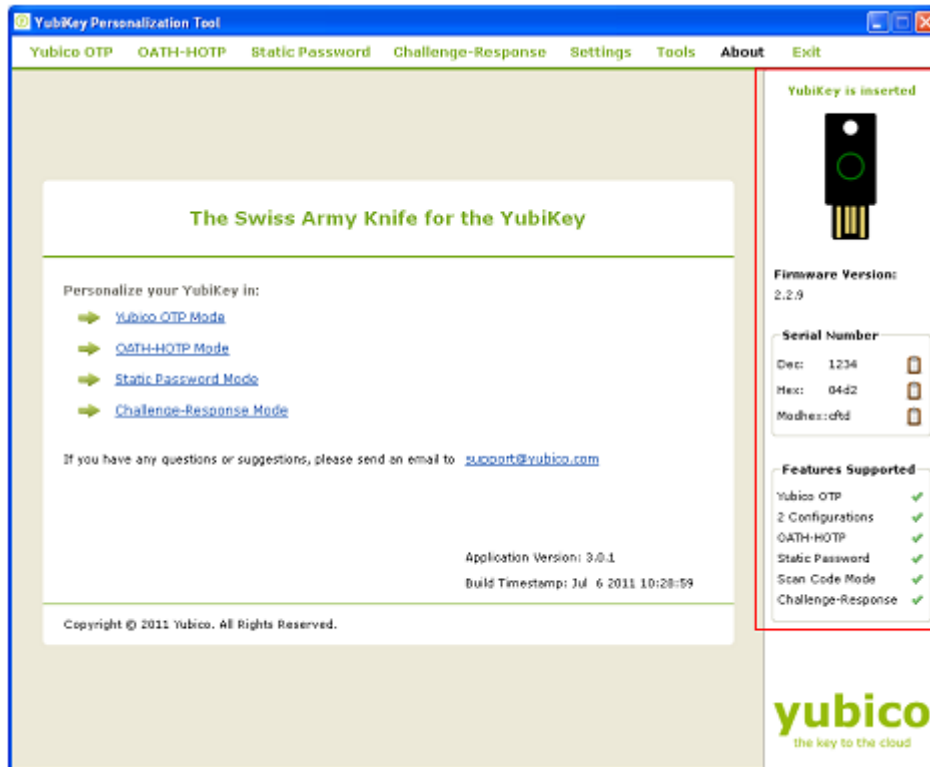
#### 5.1.1 Getting the YubiKey Firmware version

To get the YubiKey Firmware version, serial number of the YubiKey and the features available in the YubiKey, follow the steps below:

- 1) Start the YubiKey Personalization Tool

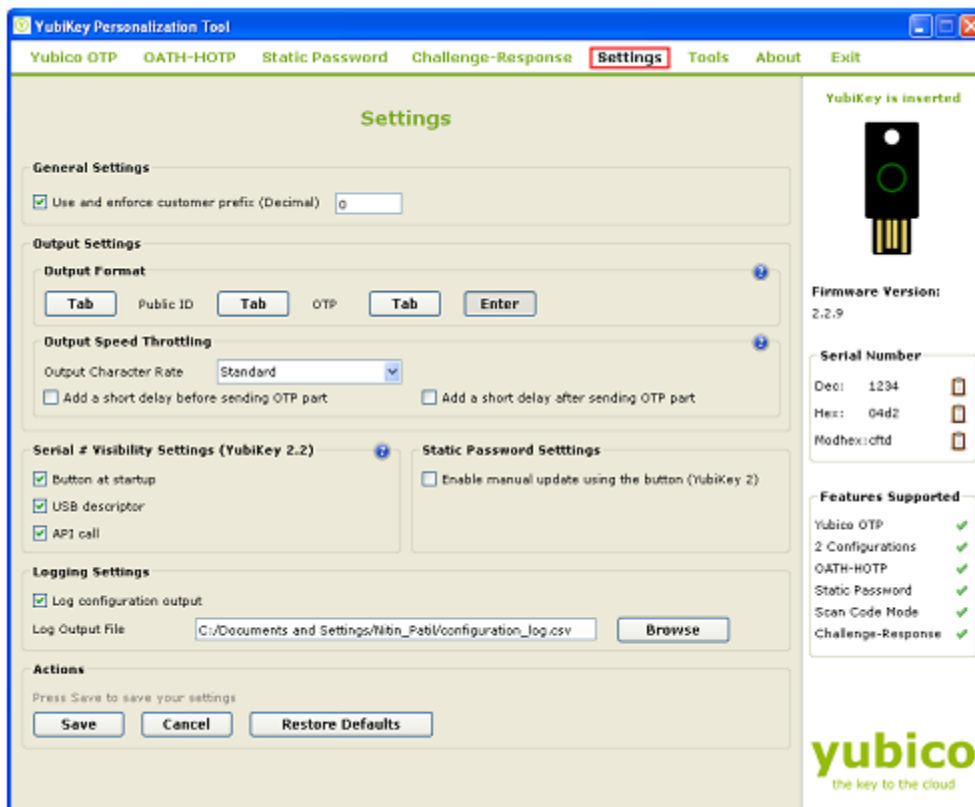


- 2) Insert the YubiKey into a USB port
- 3) The YubiKey related information will be displayed on the right hand side of the tool as highlighted in the image below:



## 5.1.2 Settings

The settings available under the “Settings” tab are common and applicable for all configuration modes.



The settings are described below:

1) General Settings:

Use and enforce customer prefix (Decimal): This is not common but if your organization has been provided with a customer prefix by Yubico, enter it here in decimal format and all public identities when you program YubiKeys will have this customer prefix enforced. If no customer prefix is entered a default prefix will be used.

2) Output Settings:

a) Output Format: Output Format specifies how the OTP will be emitted from the YubiKey.

If the first "Tab" button is pressed (highlighted when activated), then the first character emitted from the YubiKey will be a TAB, typically used to move the cursor to the next input field.

If the "Tab" button between Public ID and OTP is pressed, then in order to separate the fixed (public identity) part and the OTP part, a TAB can be inserted to move the cursor to the next input field

If the "Tab" button after OTP is pressed, then a final TAB will be sent after the OTP part, typically used to move the cursor to the next input field after the password.

If the "Enter" button is pressed, then an ENTER as the final keystroke will be sent, typically used to trigger a default (OK) button or to complete input from a command prompt.

Un-pressing (button not highlighted) these buttons will cause the corresponding Tab or Enter button not to be active.

b) Output Speed Throttling: Normally, the USB host polls the IN interrupt endpoint at the rate it can receive characters. The default poll rate is 10 ms which means that Yubikey will output characters at a full speed, a key entry is sent every 10ms. Each complete keystroke represents a key-down and a key-up cycle, which means that about 50 characters per second can be output.

If there are issues with lost characters due to a too high character output rate, the output can be slowed down. This can be needed on slow or busy computers/servers.

There are four speed options:

- i. Standard: If Standard is selected, then no delay will be added
- ii. Slow down by 20 ms: This selection adds a 20 ms additional delay for each keystroke (10 at down and 10 at up). Given a default endpoint poll rate of 10 ms, this throttles the rate to about 25 characters per second.
- iii. Slow down by 40 ms: To further slow down the output, an additional 40 ms delay will be added.
- iv. Slow down by 60 ms: To further slow down the output, an additional 60 ms delay will be added.

Add a short delay before sending the OTP part:

If there is some parsing - or GUI rendering delay for a particular application, an additional 500 ms delay can be inserted before sending the OTP.



### 3) Serial # Visibility Settings

Introduced with Yubikey 2.2, a non-alterable, factory programmed unique serial number is included. The serial number has no direct link to the public identities configured. The configuration bits are logically ORed between the two configurations so if a bit is set in at least one of the configurations 1 or 2, that specific serial number feature is enabled.

It has three options:

- i. Button at startup: Checking this option allows the serial number to be read at device power up. Simply hold the YubiKey button while inserting the YubiKey in the USB port. Then release the button after one second and within 5 seconds. The serial number is outputted as keystrokes so keep a text editor or something similar open while performing this action so that you can capture the information.
- ii. USB descriptor: Checking this option makes the device serial number visible in the serial number field in the USB device descriptor. Please note that the device must be removed and reinserted after this bit is set in order for the operating system to recognize the updated device descriptor.
- iii. API call: Checking this option allows the device serial number to be read via a client-side application via a software interface, such as the YubiKey Client API.

### 4) Static Password Settings

Allow the user to manually update using button:

This function can be used with legacy password systems where the user can update the device secret ID part by holding the YubiKey button for 8-15 seconds and then release it. The YubiKey LED then flashes and a single press confirms the update. When pressed, the secret ID part is updated with a new random number and the new static password is outputted automatically.

### 5) Logging Settings

In “Logging Settings”, you can specify whether to log all the parameters used for programming the YubiKey in a log file. Selecting the “Log configuration output” will enable logging. You can store the log file anywhere on the system. Browse to your desired location. The log output file will be in .csv format.

### 6) Actions

In “Actions”, you can save the selected settings or you can select restore to default.


#### 5.1.3 Tools

The Tools option provides a simple “calculator” to allow quick conversion between different numeric representation formats

- 1) Hexadecimal: This field shows and accepts only packed (non-delimited) hexadecimal strings
- 2) Modhex: This field shows and accepts only packed (non-delimited) Modhex strings

- 3) Decimal: This field uses the first four bytes to represent a 32-bit unsigned long integer (DWORD). Byte ordering can either be Little Endian (LSB leftmost) or Big Endian (MSB leftmost)

## 5.1.4 Getting help

If you want more help about any settings/ terminology used in the YubiKey Personalization Tool, then you can click on the help button  next to that settings/ terminology

## 5.2 Creating a Yubico OTP configuration

You can configure the YubiKey to emit the standard Yubico OTP of 44 characters. There are two options available to configure the YubiKey in standard Yubico OTP mode, one is “Quick” and another is “Advanced”.

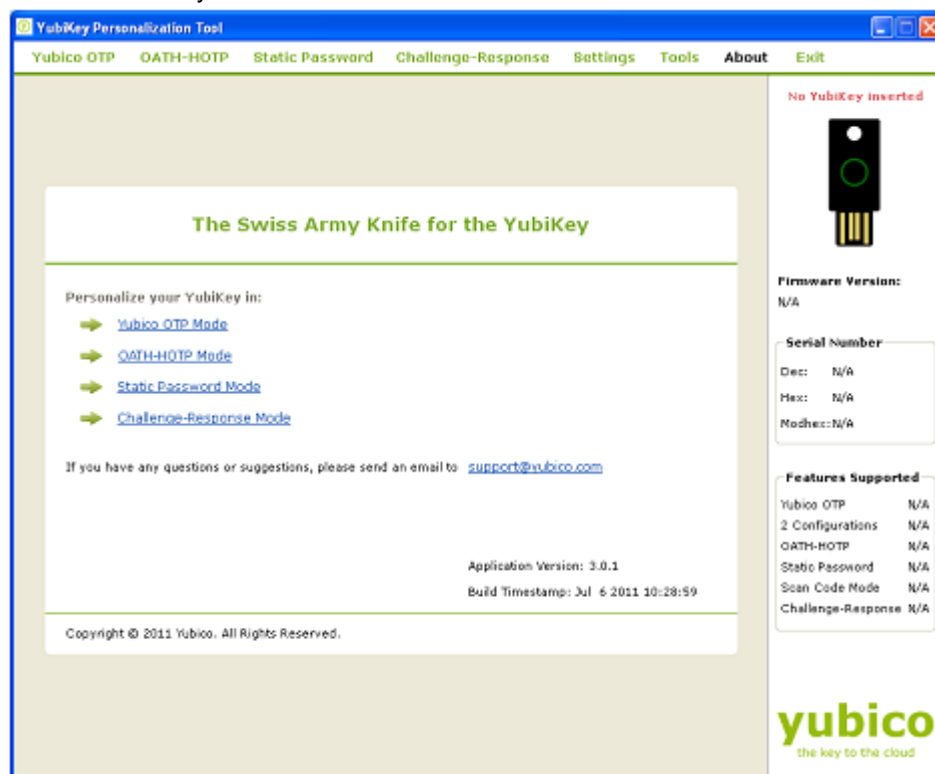
Both the options are explained below:

### 5.2.1 Quick Option

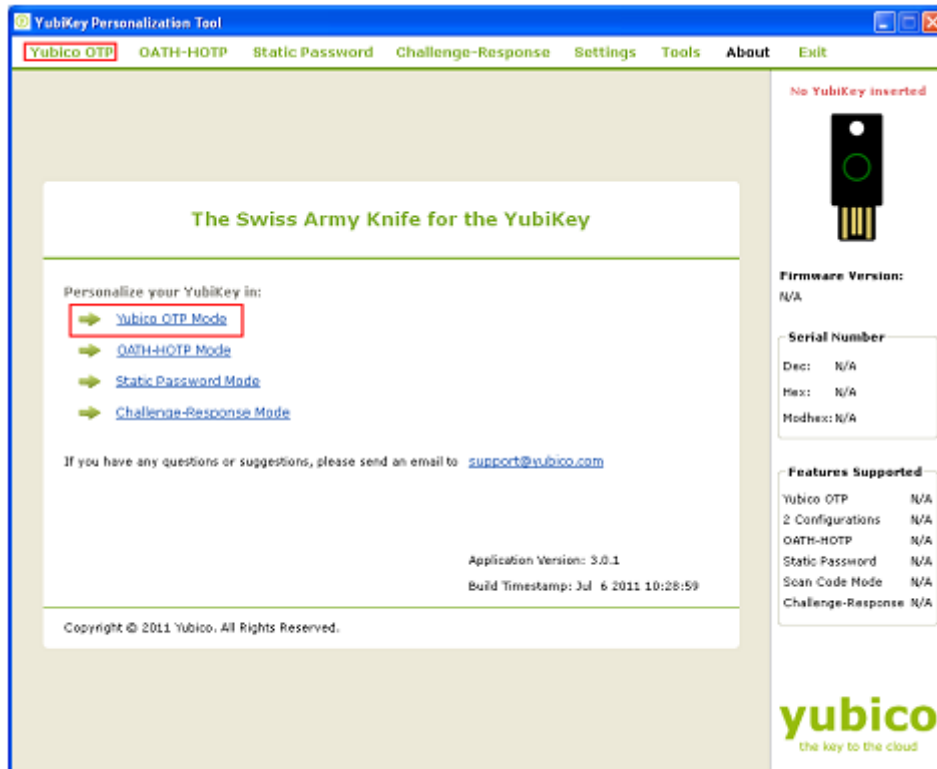
You can use the “Quick” option to quickly configure the YubiKey to upload the AES Key to the online Yubico OTP validation server.

To configure the YubiKey using “Quick” option, follow the steps below:

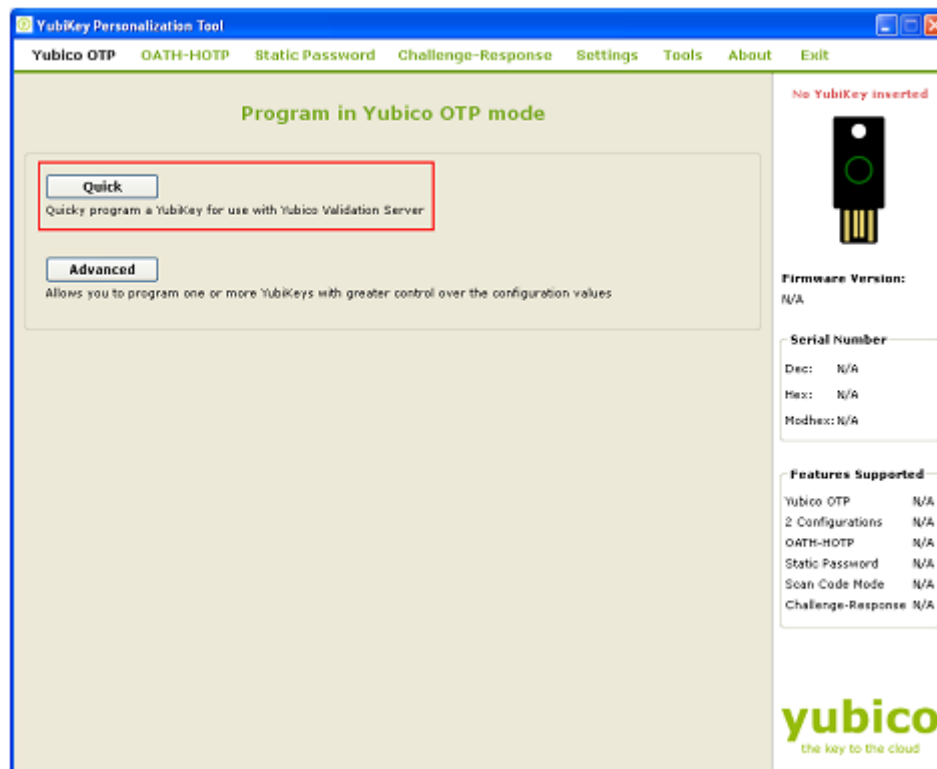
- 1) Start the YubiKey Personalization Tool



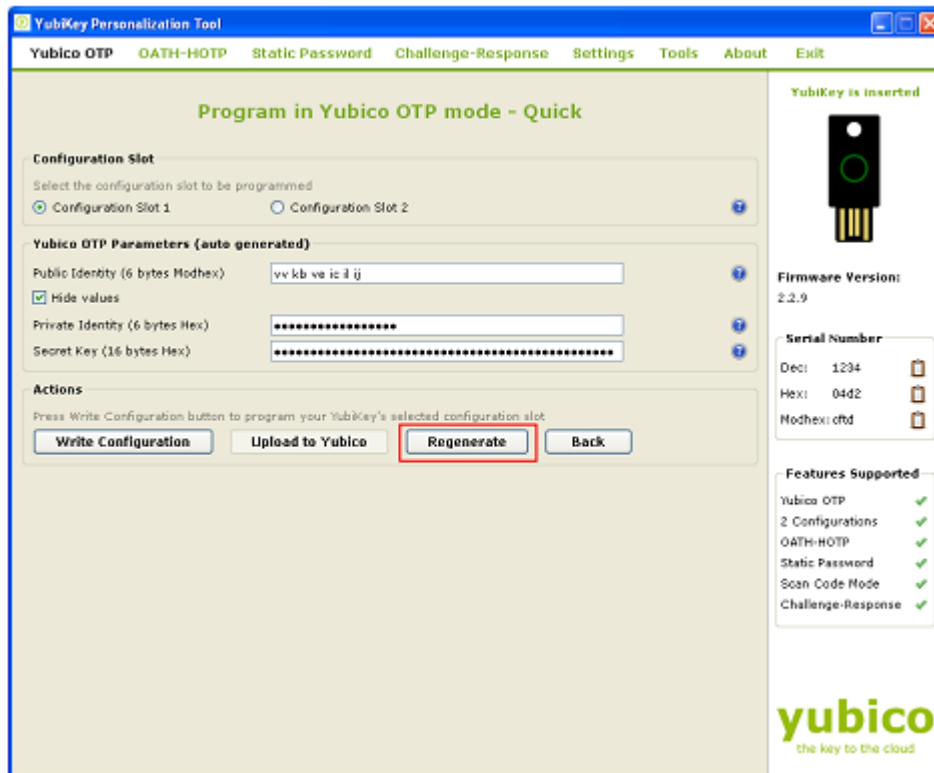
- 2) Click on either “Yubico OTP” or “Yubico OTP Mode” as highlighted in the image below:



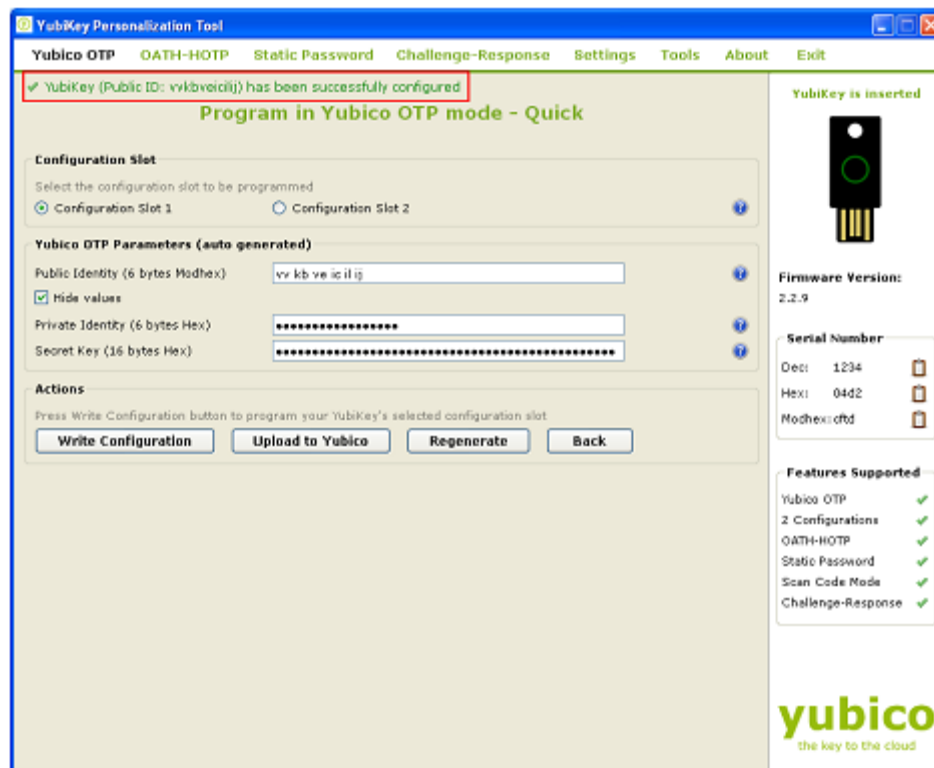
3) Now, click on “Quick” button as highlighted in the image below



- 4) Insert the YubiKey into the USB port
- 5) From the “Configuration Slot” select the appropriate configuration slot
- 6) The “Yubico OTP Parameters” will be auto generated. If you want to regenerate the parameters click on “Regenerate” button

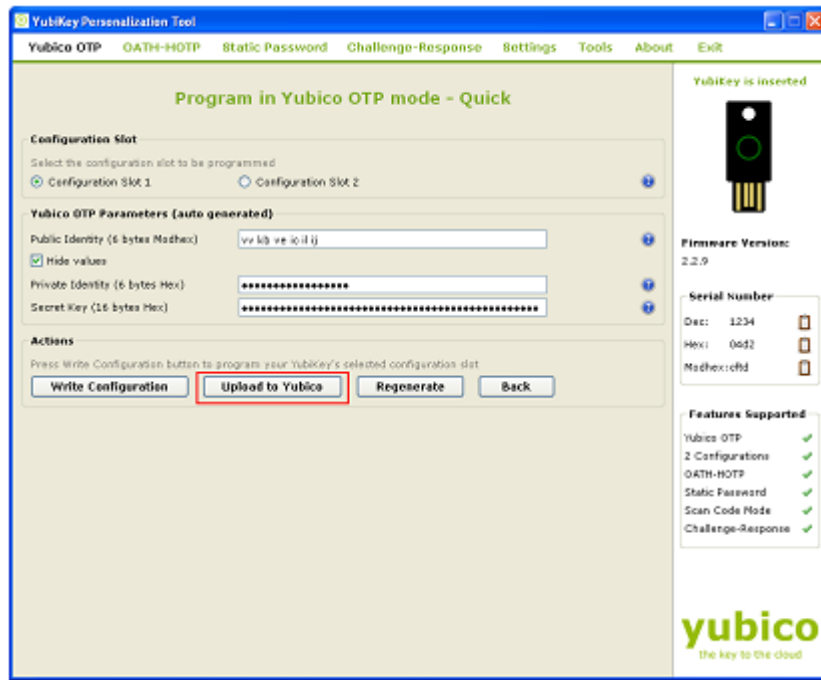


- 7) Now, from “Actions” click on “Write Configuration” button. This will reprogram the YubiKey in standard Yubico OTP mode.



- 8) Now, click on “Upload to Yubico” button. This will open a new internet browser window and will redirect automatically to the Yubico AES Key upload page. This will also populate

the corresponding fields on the AES Key upload page with the values used for reprogramming of the YubiKey.



## Yubico AES Key Upload

Please enter information about your newly personalized YubiKey.

**Please note: It takes 15 minutes for an uploaded identity to become valid on our validation servers. Please wait 15-20 minutes before testing an uploaded identity.**

Your e-mail address:

Serial number:

YubiKey prefix:


Internal identity:

AES Key:

OTP from the YubiKey:

**goolysi 1859**

Type the two words:



Provide email address and tab to the OTP from Yubikey filed and press the YubiKey button. Finally enter the captcha and click on "Upload AES key" button.

This will upload the AES Key to the Yubico OTP validation server. Please note that, the AES Key upload functionality takes some time to update all the corresponding databases so wait for 10-15 minutes before you try to validate the OTPs with the online Yubico OTP validation server using link [http://demo.yubico.com/php-yubico/one\\_factor.php](http://demo.yubico.com/php-yubico/one_factor.php)

## 5.2.2 Advanced Option

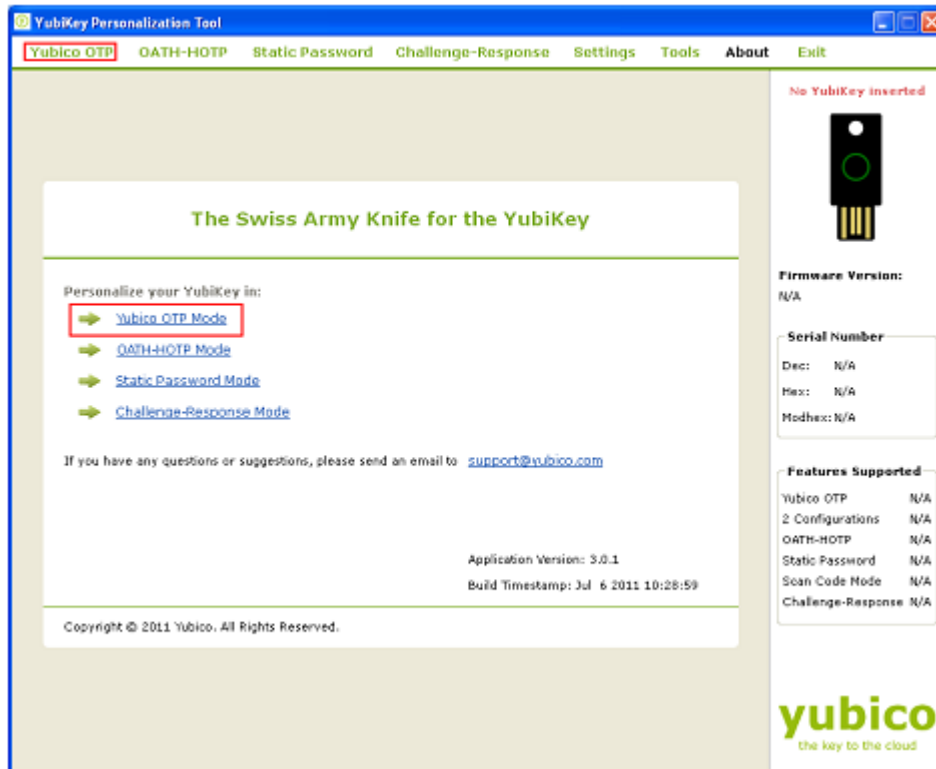
To program the YubiKey using your own parameters to the standard Yubico OTP mode, you can use the “Advanced” option.

To program the YubiKey in “Advanced” option, follow the steps below:

- 1) Start the YubiKey Personalization Tool



- 2) Click on either “Yubico OTP” or “Yubico OTP Mode” as highlighted in the image below:

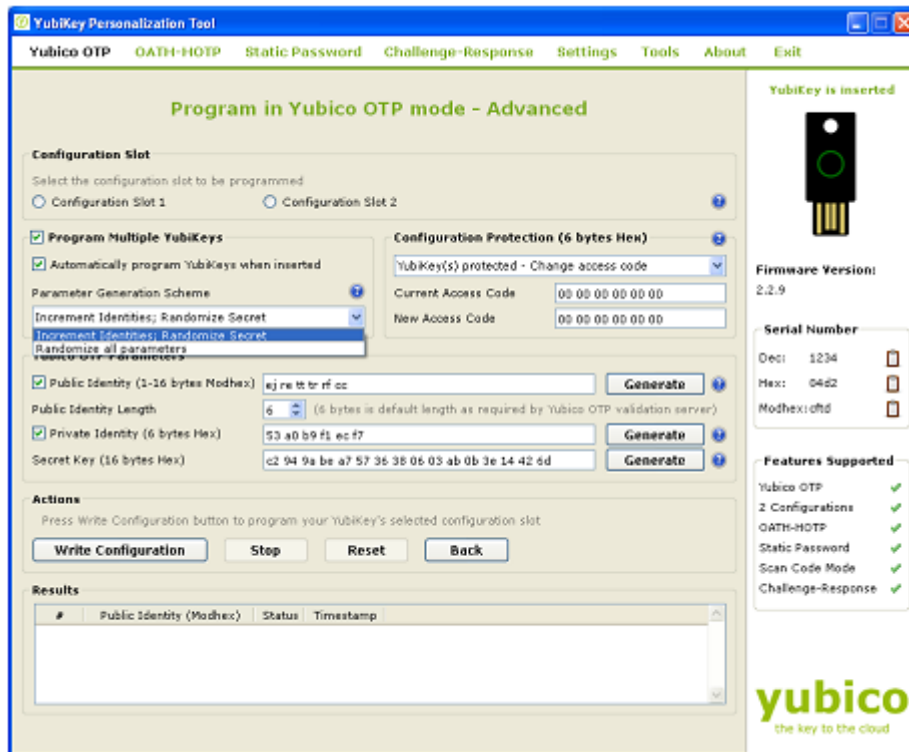


- 3) Insert the YubiKey to the USB port
- 4) Now, click on “Advanced” button as highlighted in the image below




- 5) From the “Configuration Slot” select the appropriate configuration slot
- 6) If you want to program multiple YubiKeys, then select the “Program
- 7) If the Program Multiple YubiKeys” option is selected, you can specify if you want to automatically program the YubiKeys when inserted or you want to click on the “Write Configuration” button every time to program a new YubiKey. Also, you can specify how

the parameters used for programming the YubiKeys will be generated. There are two options:



- i) Increment Identities; Randomize Secret
- ii) Randomized all parameters

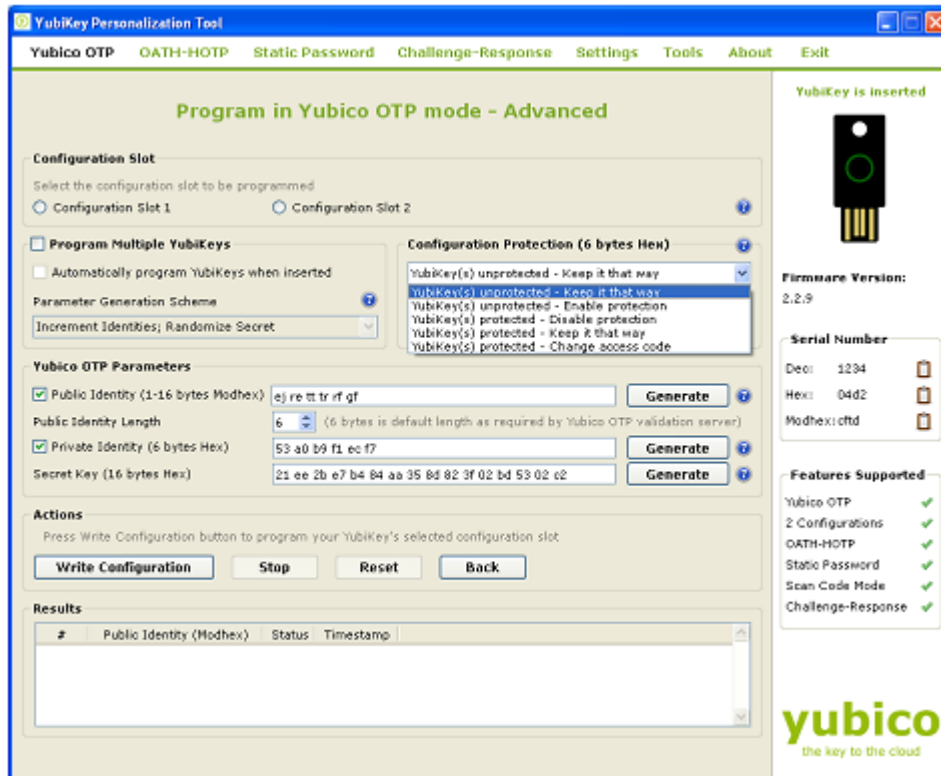
Select the appropriate option. For more information, please click on the help button .

- 8) To protect against unauthorized update of a specific configuration, a configuration protection password can be added. Then, in order to update or remove this configuration, the corresponding configuration protection password must be used, otherwise the request is rejected.


In the “Configuration Protection” section, you can specify if you want to set the configuration protection password.

There are five options available:





- i) YubiKey(s) unprotected – Keep it that way:
- ii) YubiKey(s) unprotected – Enable protection:
- iii) YubiKey(s) protected – Disable protection:
- iv) Key(s) protected – Keep it that way:
- v) YubiKey(s) protected –Change access code:

Select the appropriate option. Click on the help button  for more information.

- 9) From the “Yubico OTP Parameters”, you can select Public Identity, Private Identity and Secret Key.
  - i) Public Identity: The public identity is the first optional fixed part of the OTP string, used to identify a YubiKey. This field is sent in clear text.

The public identity is optional. If there is no requirement for it, uncheck the “Public Identity”.

If used, a length between 1 and 16 bytes has to be specified. Any length between 1 and 5 bytes is considered a “private scope” and won’t create any interoperability issues. A public ID length of 6 bytes or more is for use with the Yubico validation server architecture or for future extensions. A unique customer prefix can be acquired from Yubico. The customer prefix is set in the Settings, see section <need to update>. If a customer prefix is set in the configuration, a public ID length of 6 bytes is enforced, where the first three bytes contain the unique customer prefix.

By default, it is randomly generated and set to 6 bytes length. You can regenerate it by clicking on the “Generate” button next to it.

For more information, click on the help  button.

- ii) Private Identity: The private identity is a secret field, included as an input parameter in the OTP generation algorithm.

Utilizing the private identity field is optional. If there is no requirement for it, uncheck the “Private Identity” and the field will be forced to all zeroes.

By default, it is randomly generated and set to 6 bytes length. You can regenerate it by clicking on the “Generate” button next to it.

For more information, click on the help  button.

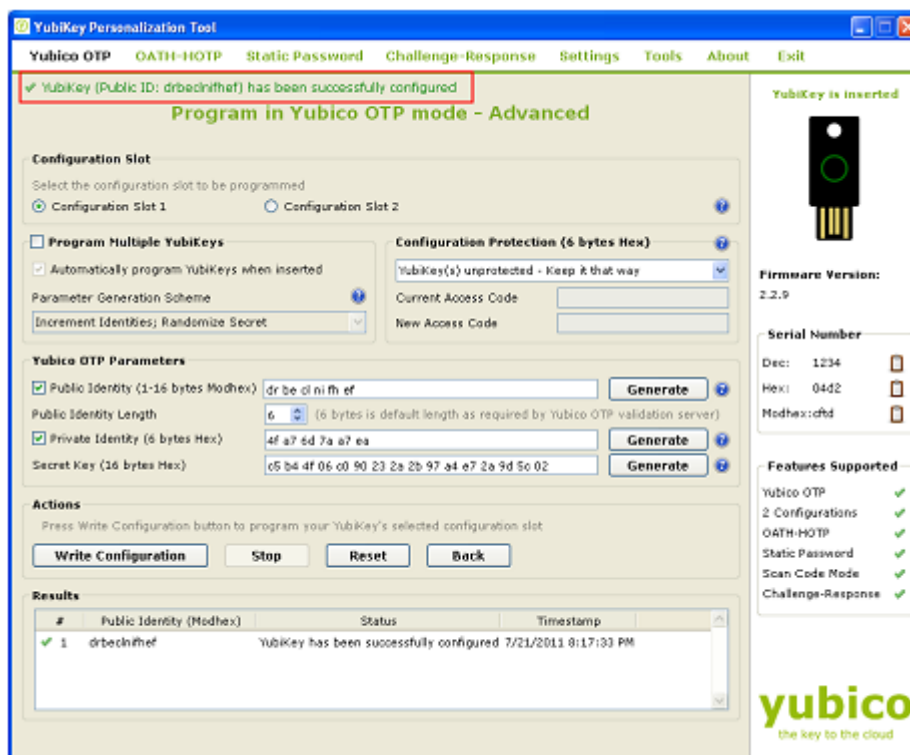
- iii) Secret Key: The secret key is used to encrypt the OTP. By default, it is randomly generated and set to 128bit length. You can regenerate it by clicking on the “Generate” button next to it.

For more information, click on the help  button

- 10) From the “Actions”, click on the “Write Configuration” button to configure the YubiKey in standard Yubico OTP mode.

If you are programming multiple YubiKeys and have selected the “Automatically program YubiKeys when inserted” option, then at the time of programming the first YubiKey, you need to click on the “Write Configuration” button. Afterwards, you need to just remove the programmed YubiKey from the USB port and need to insert the new YubiKey. The new YubiKey will be programmed automatically.

If the “Automatically program YubiKeys when inserted” option is not selected, then you need to click on the “Write Configuration” button every time you program a new YubiKey.



## 5.3 Creating a OATH-HOTP Configuration

The OATH-HOTP configuration allows the YubiKey to be used in an OATH HOTP ecosystem as outlined by the RFC 4226 specification.

The OATH-HOTP functionality is available from firmware version 2.1.

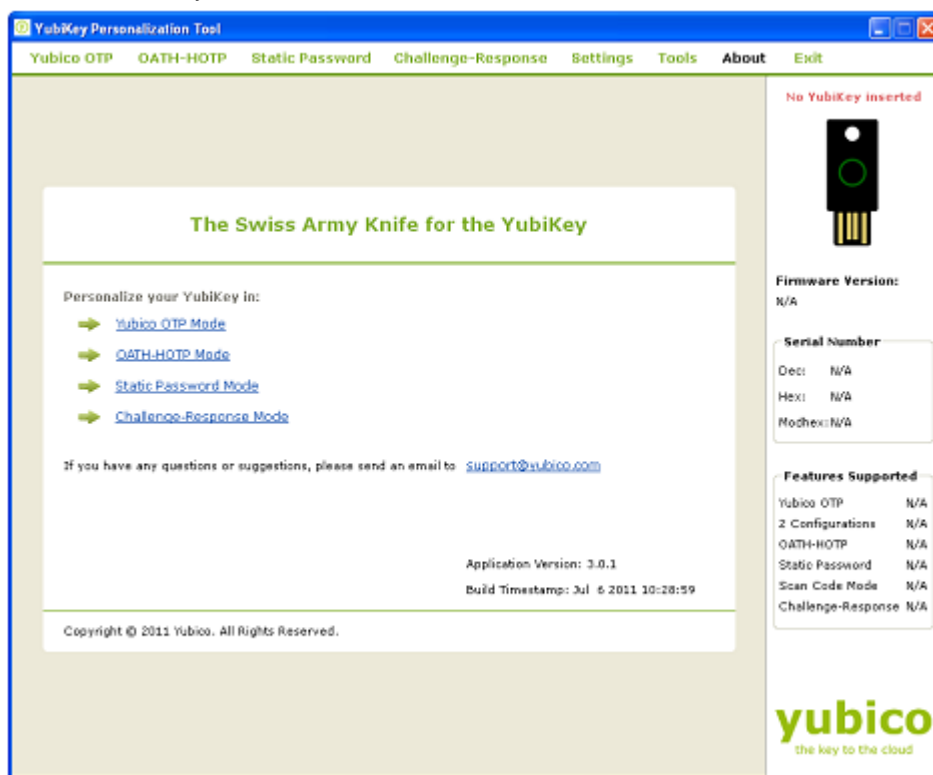
There are two options available to configure the YubiKey in OATH-HOTP mode, one is “Quick” and another is “Advanced”. Both the options are explained below:

### 5.3.1 Quick Option

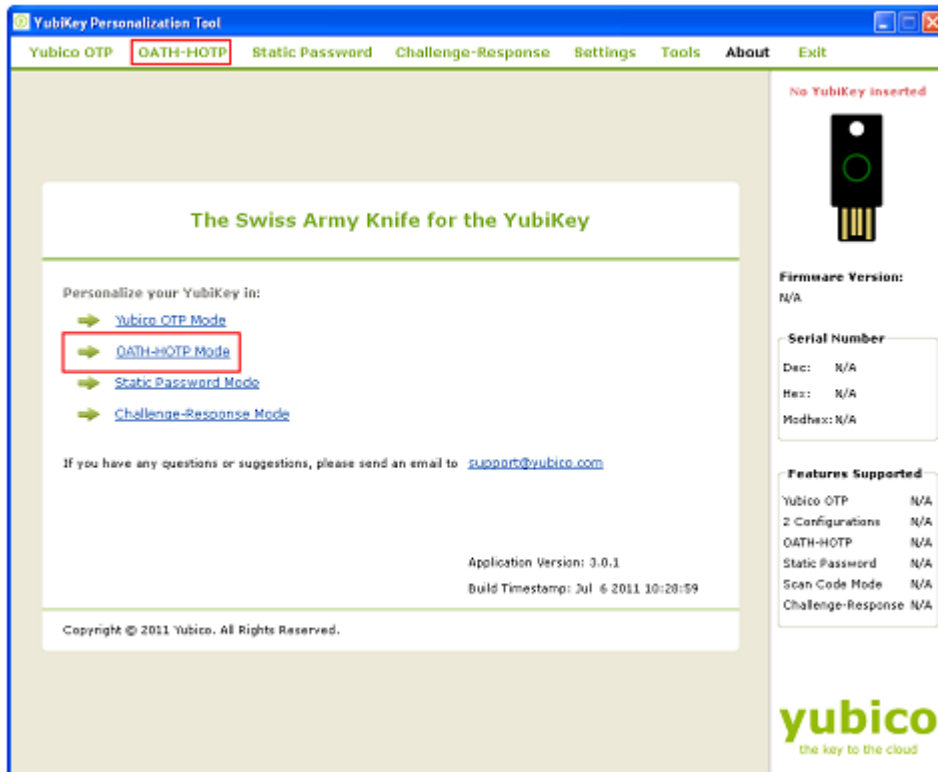
You can use the “Quick” option to quickly configure the YubiKey in OATH-HOTP mode.

To use the “Quick” mode, follow the steps below:

- 1) Start the YubiKey Personalization Tool



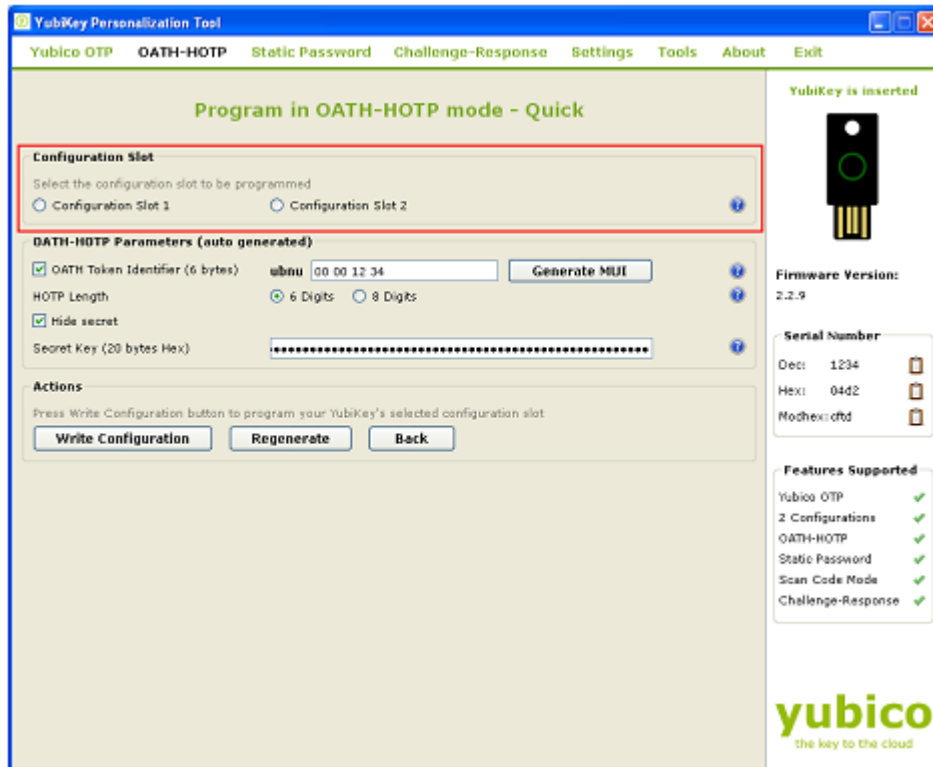
- 2) Click on either “OATH-HOTP” or “OATH-HOTP Mode” as highlighted in the image below



- 3) From the "Program in OATH-HOTP" mode click on "Quick" button




- 4) Insert the YubiKey in the USB port
- 5) From the "Configuration Slot" select the appropriate configuration slot

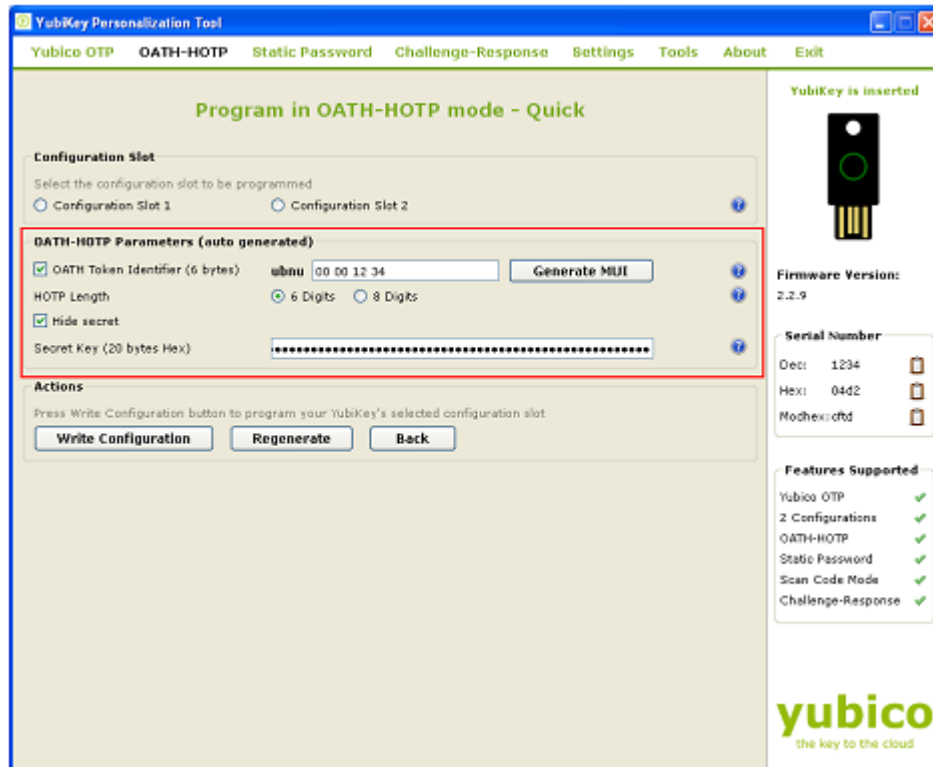


- 6) The YubiKey supports the Token Identification Specification as outlined by [openauthentication.org](http://openauthentication.org). If enabled, the YubiKey can automatically output a unique identification string preceding the HOTP.
- 7) From the OATH-HOTP Parameters (auto generated), select the OATH Token Identifier (6 bytes) if you want the YubiKey to output the OATH Token Identifier.

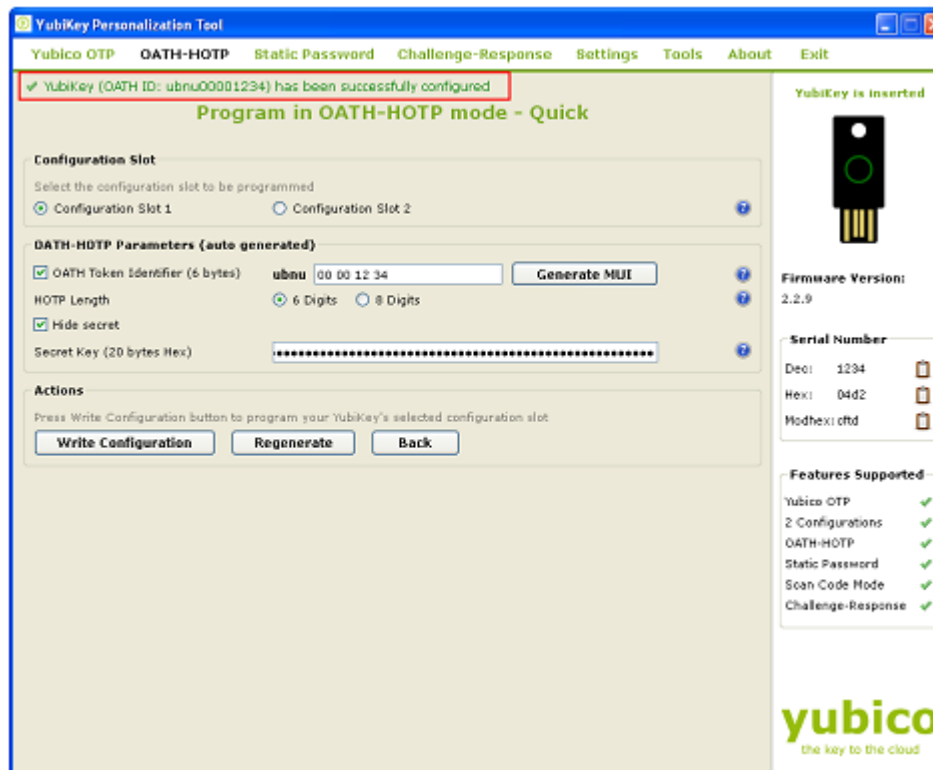
By default, the MUI will be set to the serial number of the YubiKey (if reading the serial number of the YubiKey is enabled). If you want to change it, you can click on the “Generate MUI” button.

For more information, click on the help  button.

- 8) Select the appropriate HOTP Length. For more information, click on the help  button.
- 9) Deselect the “Hide secret”, if you want to view the “Secret Key”. The Secret Key will be randomly generated



- 10) From the “Actions”, click on the “Write Configuration”. This will program the YubiKey in the OATH-HOTP format.

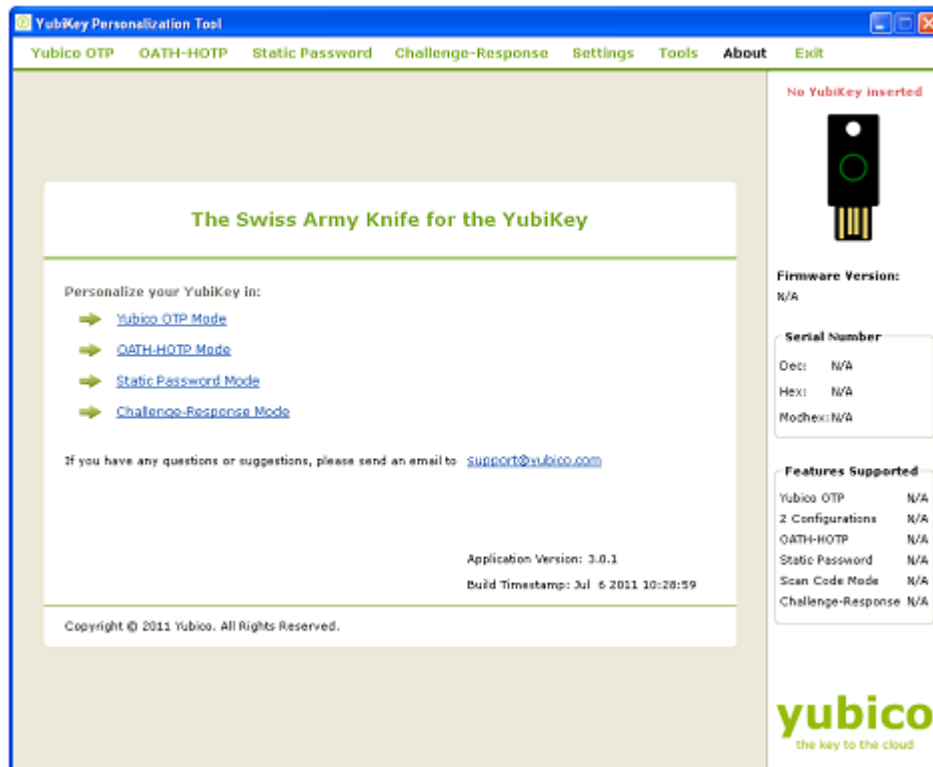


### 5.3.2 Advanced Option

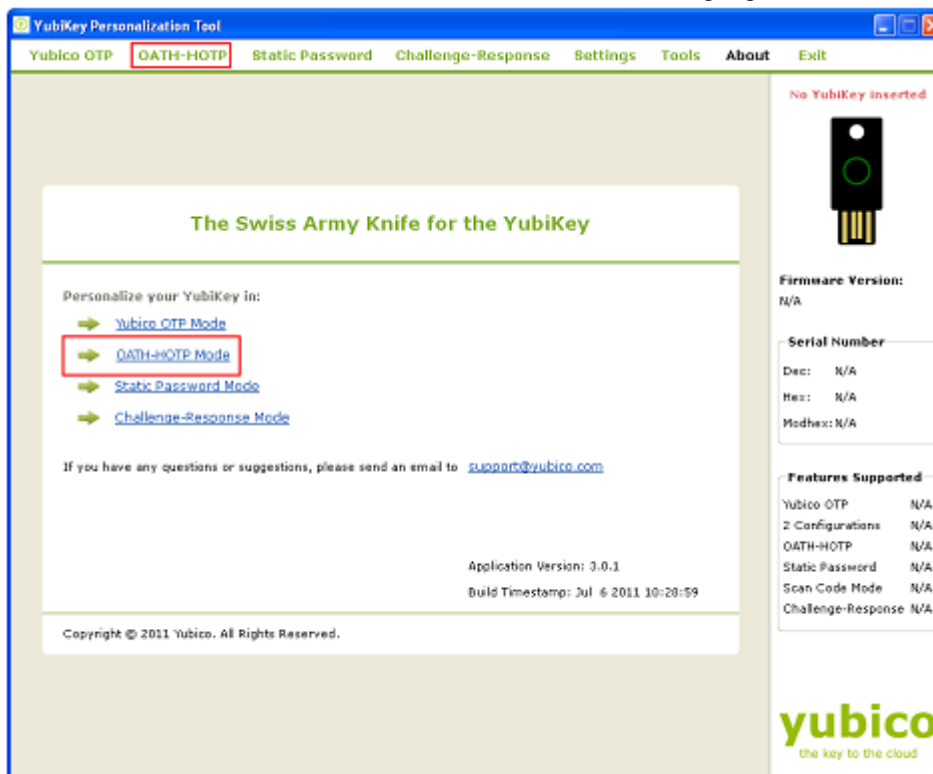
To program the YubiKey using your own and with greater control over parameters to the OATH-HOTP mode, you can use the “Advanced” option.

To program the YubiKey in “Advanced” option, follow the steps below:

- 1) Start the YubiKey Personalization Tool



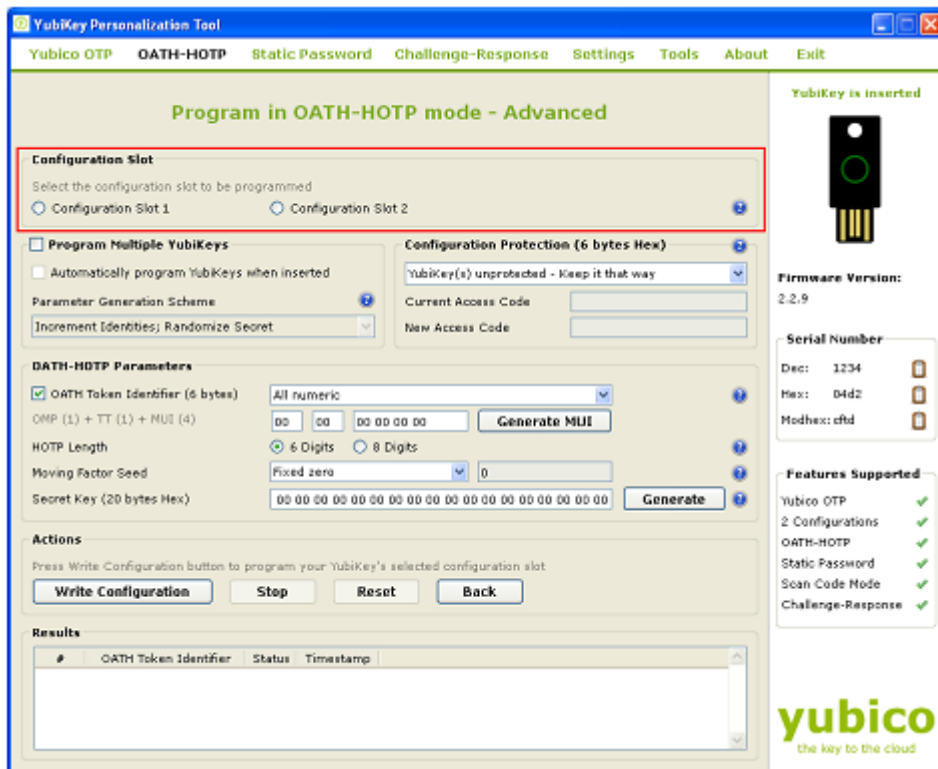
- 2) Click on either “OATH-HOTP” or “OATH-HOTP Mode” as highlighted in the image below



- 3) From “Program in OATH-HOTP” mode, click on the “Advanced” button



- 4) Insert the YubiKey in the USB port
- 5) From the “Configuration Slot”, select the appropriate configuration slot.




- 6) If you want to program multiple YubiKeys, then select the “Program Multiple YubiKeys” option
- 7) If the Program Multiple YubiKeys” option is selected, you can specify if you want to automatically program the YubiKeys when inserted or you want to click on the “Write Configuration” button every time to program a new YubiKey. Also, you can specify how



the parameters used for programming the YubiKeys will be generated. There are two options:

- i) Increment Identities; Randomize Secret
- ii) Randomized all parameters


Select the appropriate option. For more information, please click on the help button 

- 8) To protect against unauthorized update of a specific configuration, a configuration protection password can be added. Then, in order to update or remove this configuration, the corresponding configuration protection password must be used, otherwise the request is rejected.


In the “Configuration Protection” section, you can specify if you want to set the configuration protection password.

There are five options available:


- i) YubiKey(s) unprotected – Keep it that way:
- ii) YubiKey(s) unprotected – Enable protection:
- iii) YubiKey(s) protected – Disable protection:
- iv) Key(s) protected – Keep it that way:
- v) YubiKey(s) protected –Change access code:

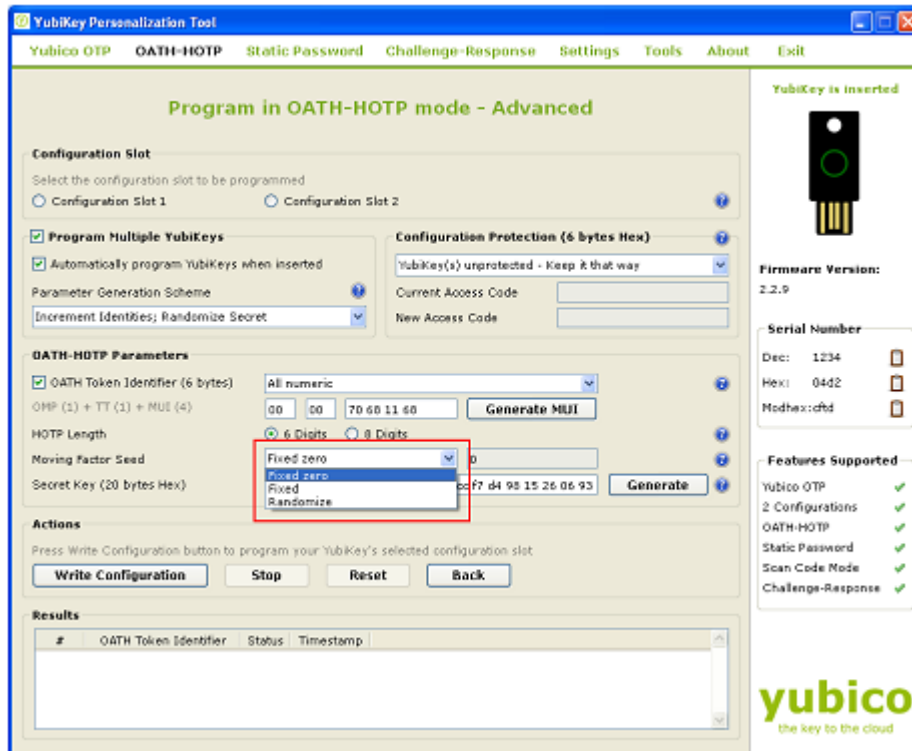
Select the appropriate option. Click on the help button  for more information.

- 9) The YubiKey supports the Token Identification Specification as outlined by [openauthentication.org](http://openauthentication.org). If enabled, the YubiKey can automatically output a unique identification string preceding the HOTP.
- 10) From the “OATH-HOTP” Parameters, deselect the “OATH Token Identifier (6 Bytes)” if you don’t want the YubiKey to automatically output the identifier.
- 11) If the “OATH Token Identifier (6 Bytes)” parameter is selected then, there are four options available to output the OATH Token Identifier.
  - i) All Numeric
  - ii) OMP Modhex, rest numeric
  - iii) OMP + TT Modhex, rest numeric
  - iv) All Modhex

For more information about the OMP, TT and MUI, click on the help button  next to OATH Token Identifier.

Select the appropriate option.

- 12) Select the HOTP length. For more information, click on the help button .
- 13) Select the appropriate option for the “Moving Factor Seed”. There are there option:



- i) Fixed zero
- ii) Fixed
- iii) Randomize

For more information, click on the help button .

- 14) To generate a random Secret Key, click on the “Generate” button.
- 15) From the Actions field, write on the “Write Configuration” button. The YubiKey will be programmed in OATH-HOTP mode

## 5.4 Create a static configuration (Static Password)

The static mode is provided to create “hard to guess and remember” password. There are two options for password configuration – Scan code and Advanced.

Both the options are explained below:

### 5.4.1 Scan code

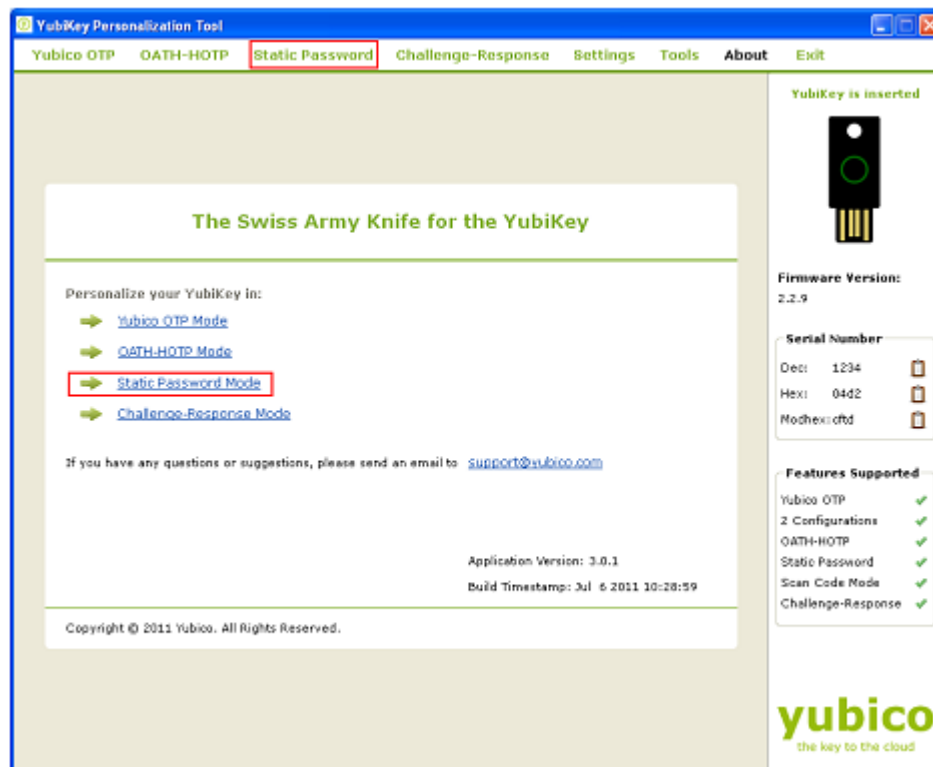
The scan code mode provides a mechanism to generate a string based on any arbitrary keyboard scan code. Please note, this mode may create incompatibilities if different national keyboard layouts are used as the mapping varies between countries. It is therefore recommended to primarily be used on the same keyboard layouts and/or on the same computer. The scan code functionality is available for YubiKey 2 only. YubiKey 2.2 adds support for up to 38 characters (compared to 16 characters in 2.0 and 2.1).

To program the YubiKey in the Scan code mode follow the steps below:

- 1) Start the YubiKey Personalization Tool



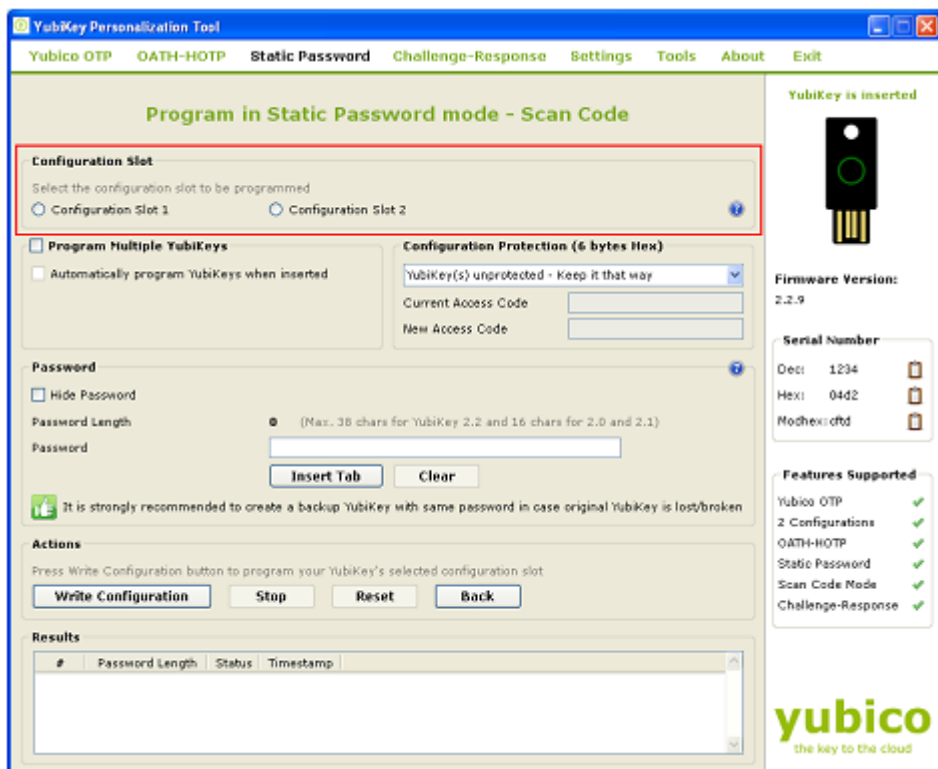
- 2) Insert the YubiKey in the USB port
- 3) Click on either “Static Password” or “Static Password Mode” as highlighted in the image below



- 4) From “Program in Static Password mode”, click on the “Scan Code” button



- 5) From the “Configuration Slot”, select the appropriate configuration slot.

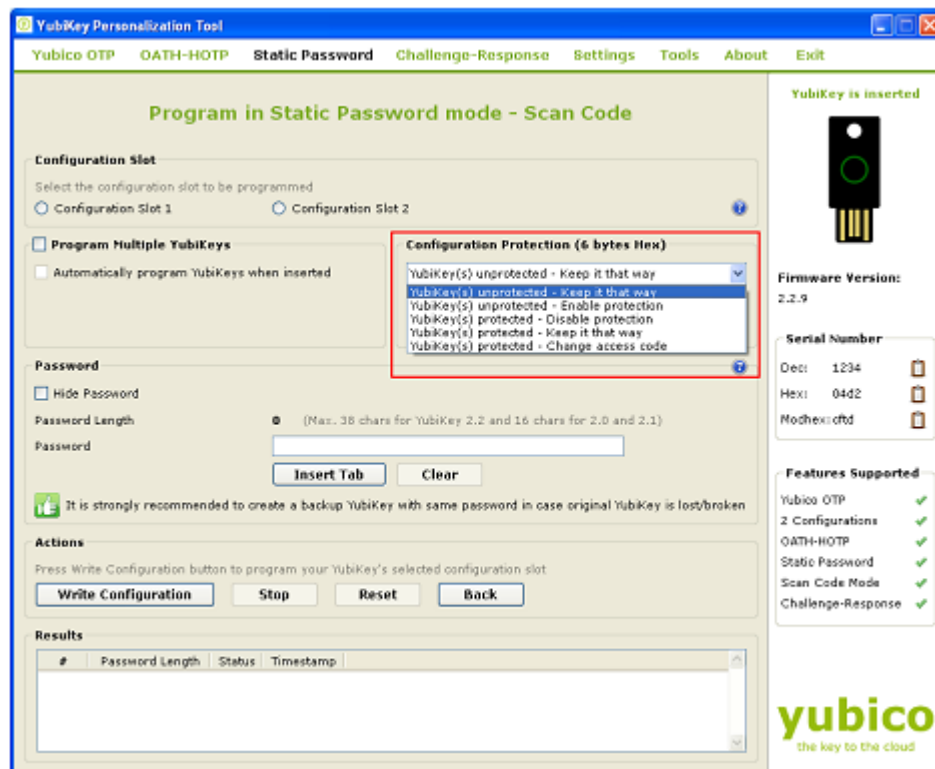


- 6) If you want to program multiple YubiKeys, then select the “Program Multiple YubiKeys” option
- 7) If the Program Multiple YubiKeys” option is selected, you can specify if you want to automatically program the YubiKeys when inserted or you want to click on the “Write Configuration” button every time to program a new YubiKey.


- 8) To protect against unauthorized update of a specific configuration, a configuration protection password can be added. Then, in order to update or remove this configuration, the corresponding configuration protection password must be used, otherwise the request is rejected.

In the “Configuration Protection” section, you can specify if you want to set the configuration protection password.

There are five options available:



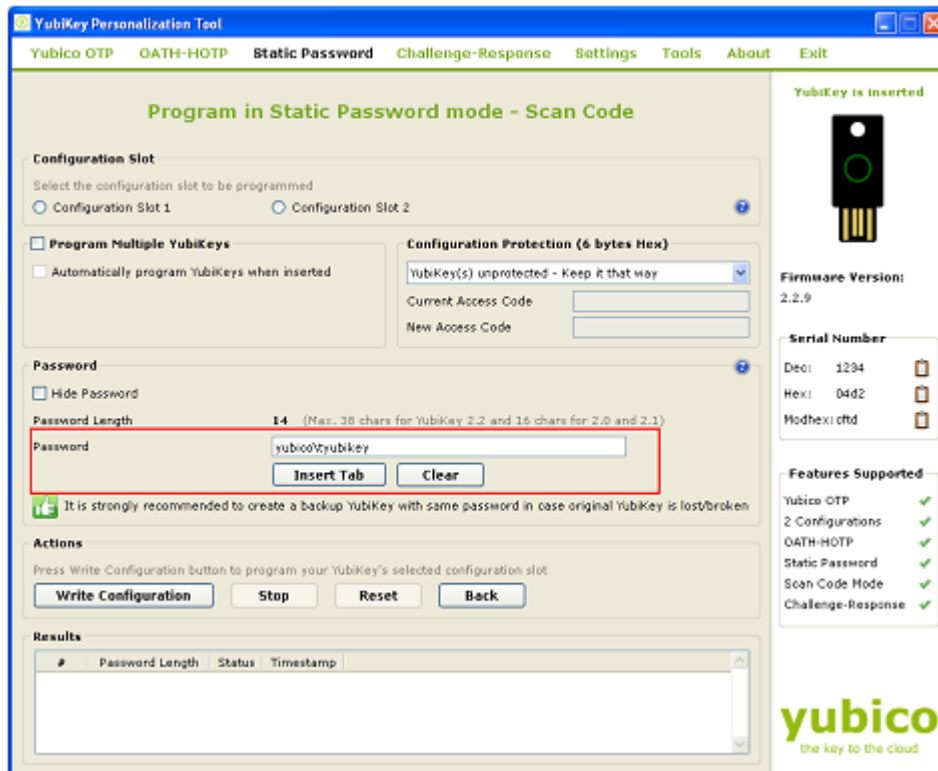
- i) YubiKey(s) unprotected – Keep it that way:
- ii) YubiKey(s) unprotected – Enable protection:
- iii) YubiKey(s) protected – Disable protection:
- iv) Key(s) protected – Keep it that way:
- v) YubiKey(s) protected –Change access code:

Select the appropriate option. Click on the help button  for more information.

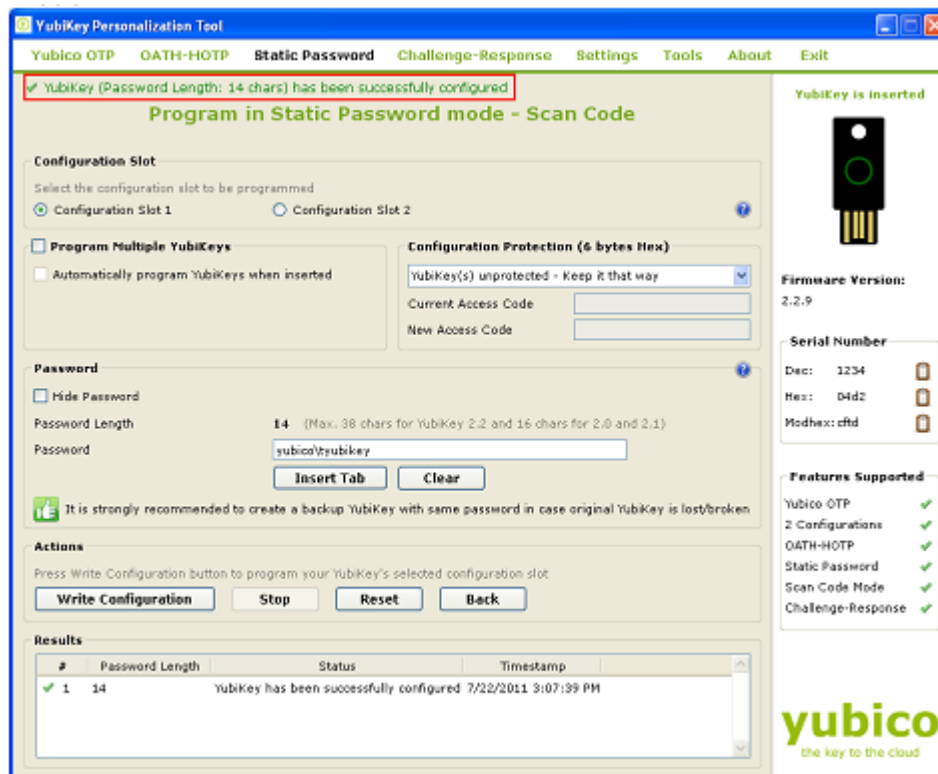
From “Password” menu select the “Hide Password” if you want to hide the entered password.

- 9) In the “Password” field, enter your password. If you want a “Tab” in your password, then click on the “Insert Tab” button. If you want to correct/re-enter the password, then click on the “Clear” button.

The total length of the password will be displayed in the “Password Length” field.



- 10) From the “Actions” menu, click on the “Write Configuration” button. This will program the YubiKey in Scan code mode.



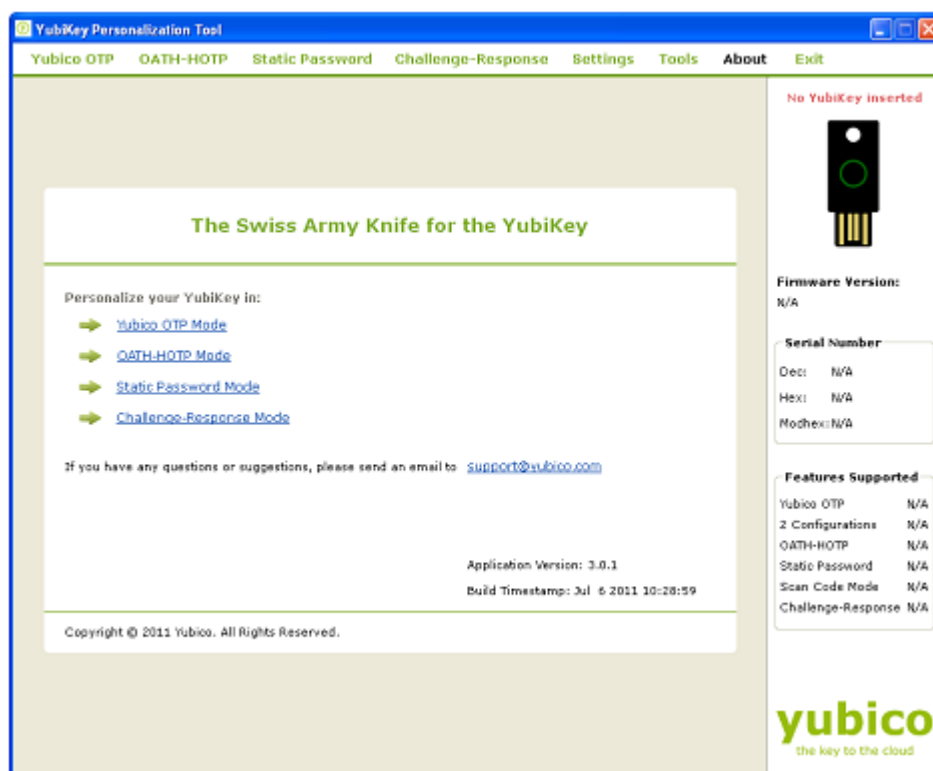
### 5.4.2 Advanced Option

YubiKey 2.x provides an interesting feature called "Strong password policy" where you can program the YubiKey to generate very long static passwords with upper, lower case letters, numbers and an "!" special character. Using the Advanced option, you can reprogram your YubiKey to output such a password.

Please also note that the static password emitted from the YubiKey when configured in "Advanced" static YubiKey configuration mode cannot be set by the user. The Static password is generated as a result of an encryption function involving the AES key and YubiKey parameters.

To program the YubiKey in the "Advanced" option, please follow the steps below:

- 1) Start the YubiKey Personalization Tool



- 2) Insert the YubiKey in the USB port
- 3) Click on either "Static Password" or "Static Password Mode" as highlighted in the image below



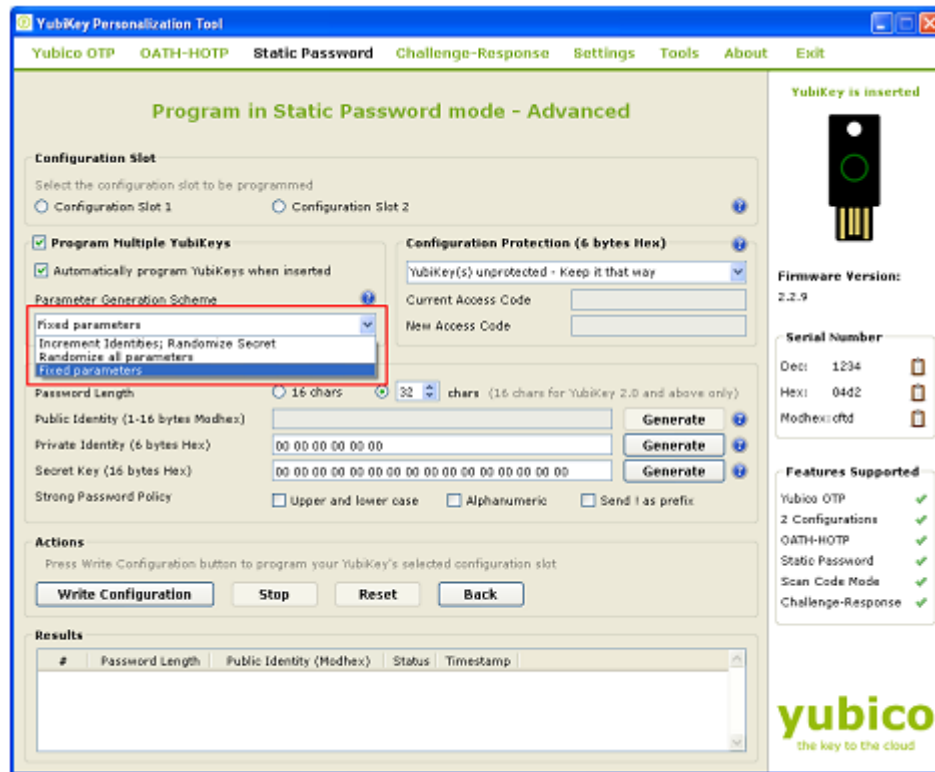
- 4) From “Program in Static Password mode”, click on the “Advanced” button




- 5) From the “Configuration Slot” select the appropriate configuration slot  
 6) If you want to program multiple YubiKeys, then select the “Program Multiple YubiKeys” option  
 7) If the Program Multiple YubiKeys” option is selected, you can specify if you want to automatically program the YubiKeys when inserted or you want to click on the “Write Configuration” button every time to program a new YubiKey. Also, you can specify how



the parameters used for programming the YubiKeys will be generated. There are two options:



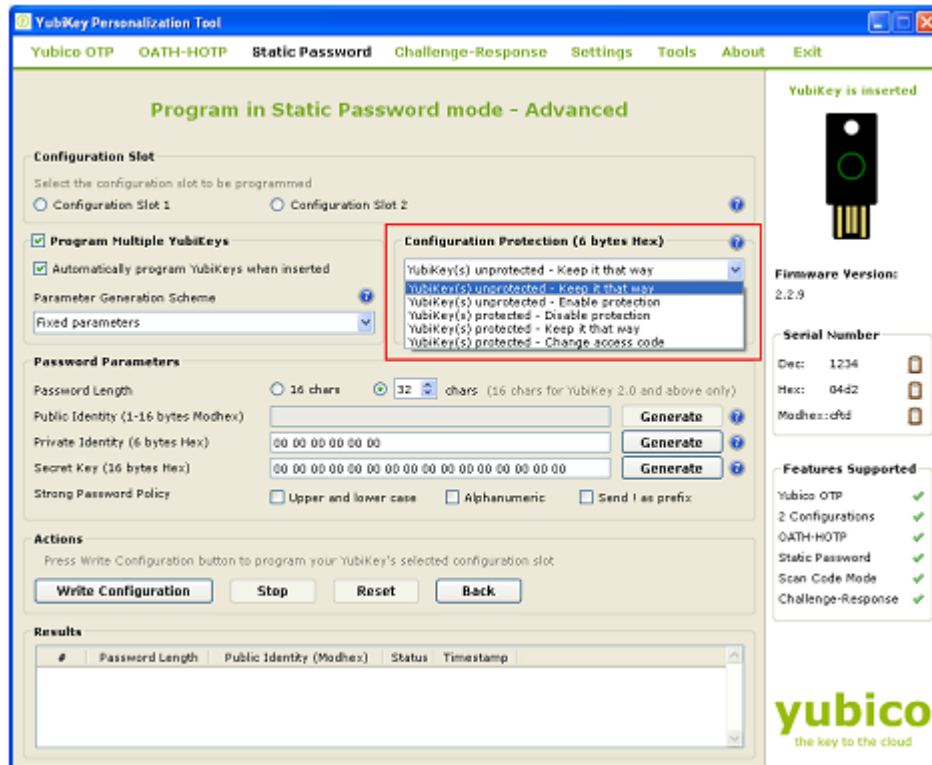
- i) Increment Identities; Randomize Secret
- ii) Randomized all parameters
- iii) Fixed parameters

Select the appropriate option. For more information, please click on the help button 


- 8) To protect against unauthorized update of a specific configuration, a configuration protection password can be added. Then, in order to update or remove this configuration, the corresponding configuration protection password must be used, otherwise the request is rejected.

In the “Configuration Protection” section, you can specify if you want to set the configuration protection password.

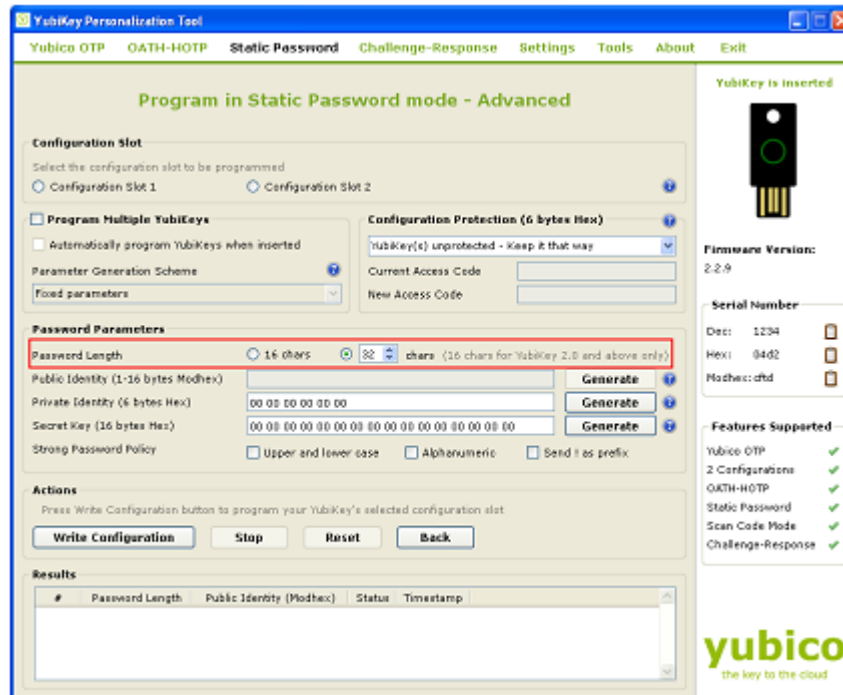
There are five options available:



- i) YubiKey(s) unprotected – Keep it that way:
- ii) YubiKey(s) unprotected – Enable protection:
- iii) YubiKey(s) protected – Disable protection:
- iv) Key(s) protected – Keep it that way:
- v) YubiKey(s) protected –Change access code:

Select the appropriate option. Click on the help button  for more information.

- 9) From the “Password Parameters”, you can select Public Identity, Private Identity and Secret Key.
  - i) Password Length: You can create a static password of up to 64 characters. If you selected the “16 chars” option, then only the Public Identity part will be used. If you selected “33” chars onward option, then all the Public, Private Identity and the AES Key will be used for static password generation. If 32 charsoption is selected then Public ID will not be used.



- ii) **Public Identity:** The public identity is the first optional fixed part of the OTP string, used to identify a YubiKey. This field is sent in clear text.

If used, a length between 1 and 16 bytes has to be specified. Any length between 1 and 5 bytes is considered a “private scope” and won’t create any interoperability issues. A public ID length of 6 bytes or more is for use with the Yubico validation server architecture or for future extensions. A unique customer prefix can be acquired from Yubico. The customer prefix is set in the Settings, see section <need to update>. If a customer prefix is set in the configuration, a public ID length of 6 bytes is enforced, where the first three bytes contain the unique customer prefix.

By default the Public ID will be generated as 0 i.e. modhex character c depending on the length of password selected. You can regenerate it by clicking on “Generate” button

For more information, click on the help button  .

- iii) **Private Identity:** The private identity is a secret field, included as an input parameter in the OTP generation algorithm.

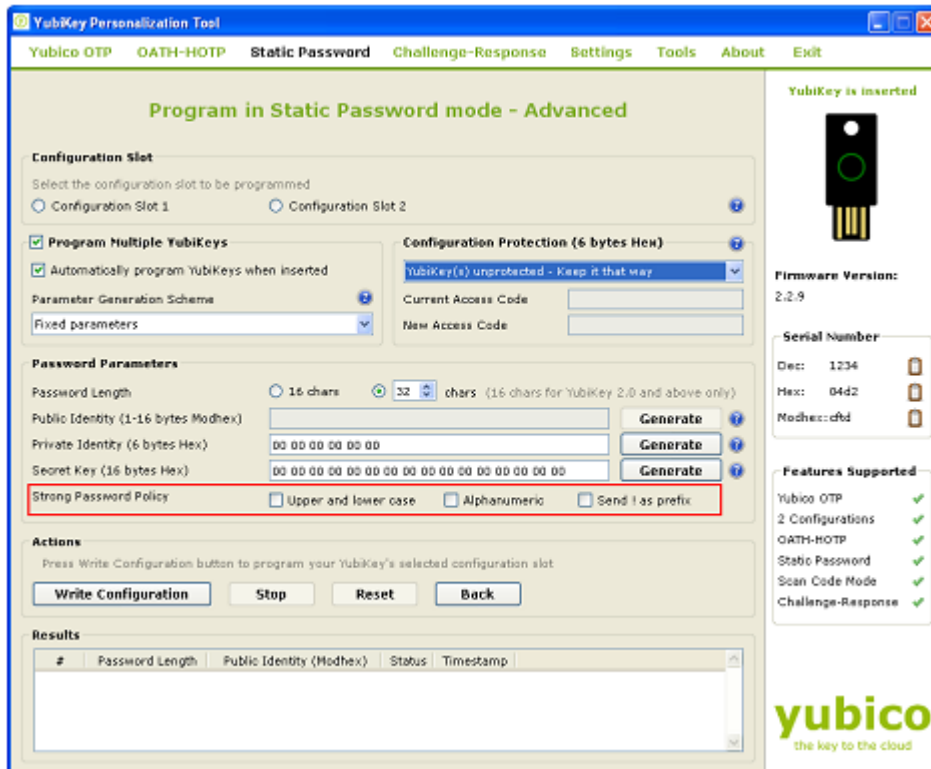
By default, it will be set to 0. You can generate it by clicking on the “Generate” button next to it.

For more information, click on the help button  .

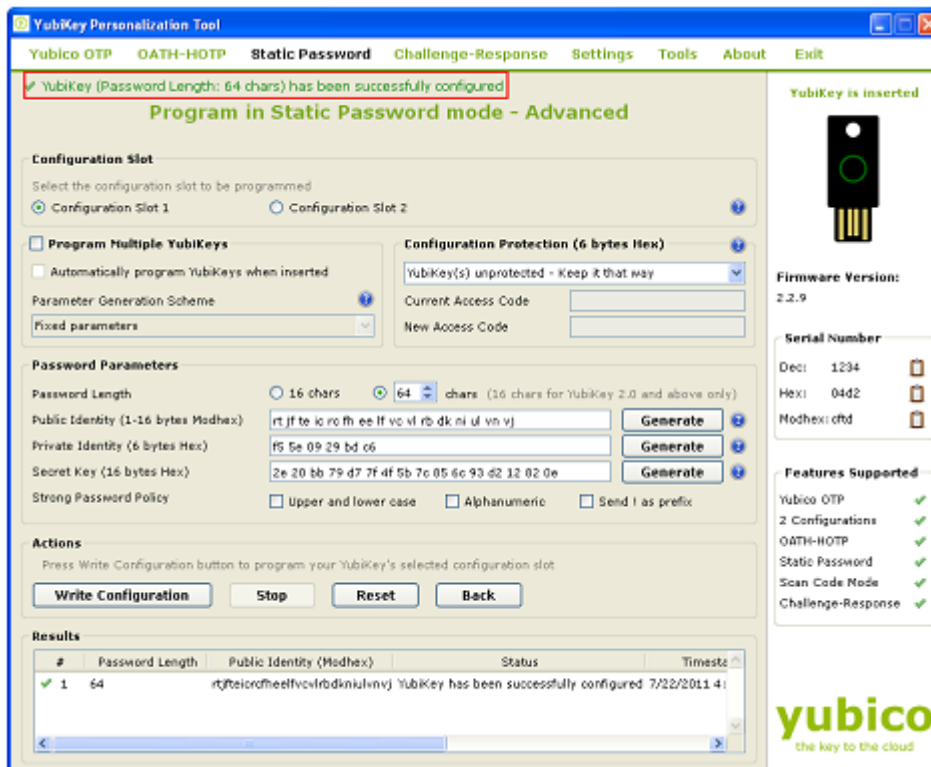
- iv) **Secret Key:** The secret key is used to encrypt the OTP. By default, it will be set to 0. You can generate it by clicking on the “Generate” button next to it.

For more information, click on the help button  .

- 10) From the “Strong Password Policy”, select the appropriate options



- 11) From the “Actions”, click on the “Write Configuration” button to configure the YubiKey in Advanced static password mode.



If you are programming multiple YubiKeys and have selected the “Automatically program YubiKeys when inserted” option, then at the time of programming the first YubiKey, you need to click on the “Write Configuration” button. Afterwards, you need to just remove the

programmed YubiKey from the USB port and need to insert the new YubiKey. The new YubiKey will be programmed automatically.

If the “Automatically program YubiKeys when inserted” option is not selected, then you need to click on the “Write Configuration” button every time you program a new YubiKey.

## 5.5 Challenge-Response mode

The Challenge-response operation allows interaction between a client-side application and the YubiKey by support of a client-side application and interface software, such as the YubiKey Client API. The challenge-response scheme can either be Yubico OTP compatible mode or HMAC-SHA1.

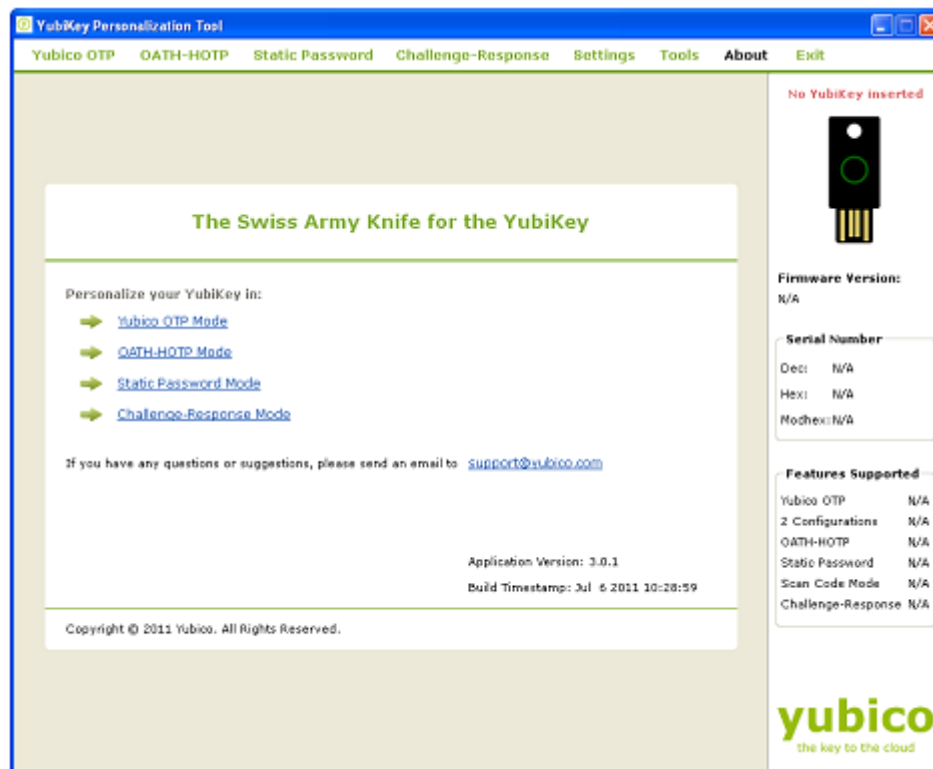
Both the options are explained below:

### 5.5.1 Yubico OTP

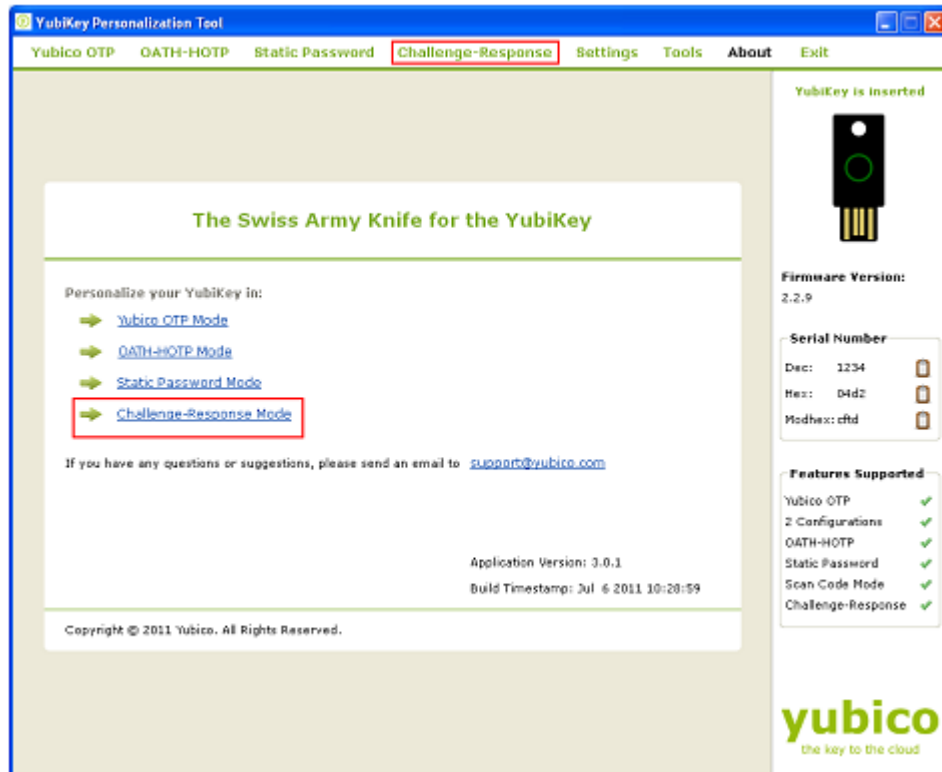
The response is formed as a Yubico OTP where the challenge is first exclusive-ored with the private ID field prior to encryption. Yubico OTP mode inserts timer - and counter fields and therefore creates a different response even if the challenge is identical.

To program the YubiKey in Yubico OTP Challenge Response mode, follow the steps below:

- 1) Start the YubiKey Personalization Tool



- 2) Insert the YubiKey in the USB port
- 3) Click on either “Static Password” or “Static Password Mode” as highlighted in the image below

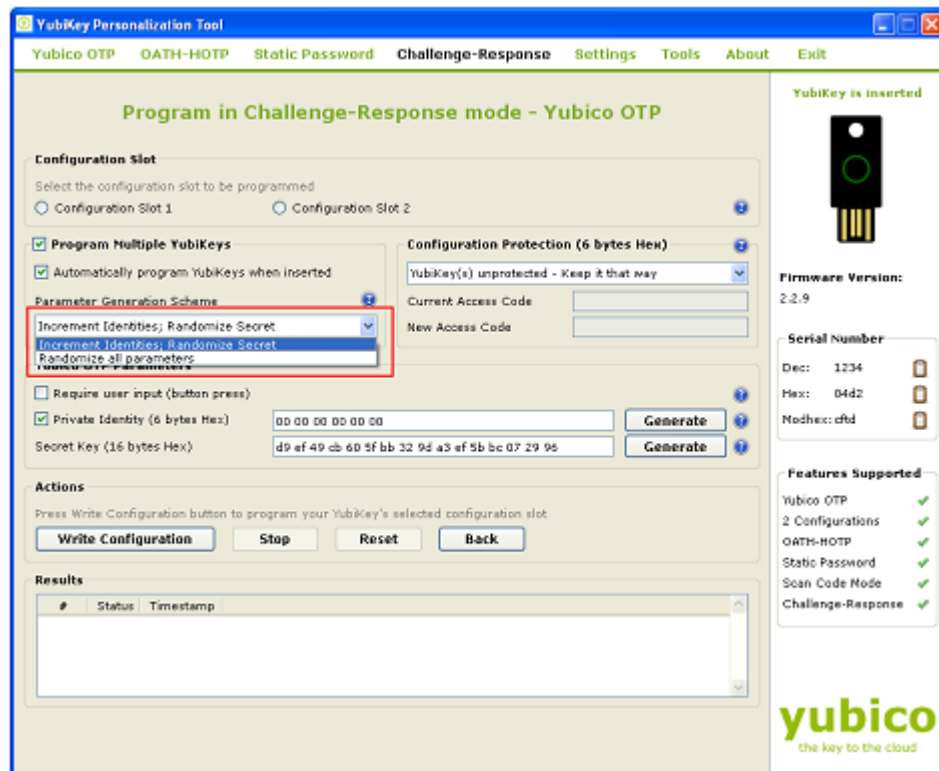


- 4) From “Program in Challenge-Response mode”, click on the “Yubico OTP” button



- 5) From the “Configuration Slot” select the appropriate configuration slot
- 6) If you want to program multiple YubiKeys, then select the “Program Multiple YubiKeys” option
- 7) If the Program Multiple YubiKeys” option is selected, you can specify if you want to automatically program the YubiKeys when inserted or you want to click on the “Write

Configuration” button every time to program a new YubiKey. Also, you can specify how the parameters used for programming the YubiKeys will be generated. There are two options:



- i) Increment Identities; Randomize Secret
- ii) Randomized all parameters

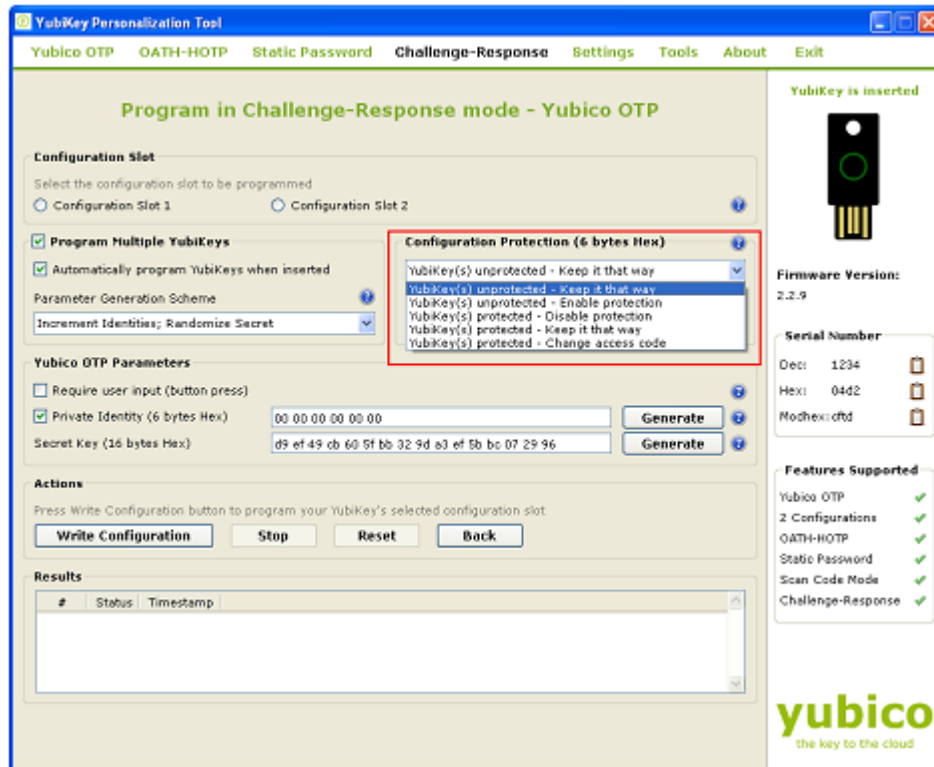
Select the appropriate option. For more information, please click on the help button




- 8) To protect against unauthorized update of a specific configuration, a configuration protection password can be added. Then, in order to update or remove this configuration, the corresponding configuration protection password must be used, otherwise the request is rejected.

In the “Configuration Protection” section, you can specify if you want to set the configuration protection password.

There are five options available:



- i) YubiKey(s) unprotected – Keep it that way:
- ii) YubiKey(s) unprotected – Enable protection:
- iii) YubiKey(s) protected – Disable protection:
- iv) Key(s) protected – Keep it that way:
- v) YubiKey(s) protected –Change access code:

Select the appropriate option. Click on the help button  for more information.

- 9) From the “Yubico OTP Parameters”, you can select Private Identity and Secret Key.
  - i) Select “Require user input (button press)” if you want the users to press the button in order to generate the response to the challenge. If this option is not selected then the response will be generated automatically without user intervention.
  - ii) Private Identity: The private identity is a secret field, included as an input parameter in the OTP generation algorithm.

Utilizing the private identity field is optional. If there is no requirement for it, uncheck the “Private Identity” and the field will be forced to all zeroes.

By default, it is set to 0 and is of 6 bytes length. You can generate it by clicking on the “Generate” button next to it.

For more information, click on the help button .

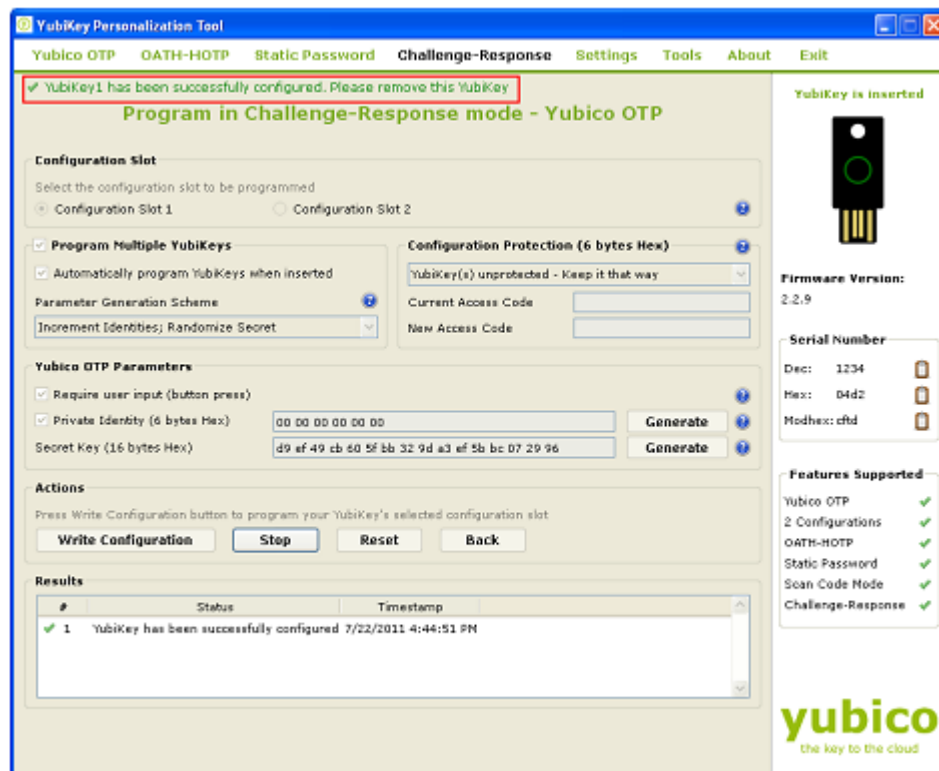
- iii) Secret Key: The secret key is used to encrypt the OTP. By default, it is randomly generated and set to 20 bytes length.

You can regenerate it by clicking on the “Generate” button next to it.



For more information, click on the help button .

- From the “Actions”, click on the “Write Configuration” button to configure the YubiKey in standard Yubico OTP challenge response mode.



If you are programming multiple YubiKeys and have selected the “Automatically program YubiKeys when inserted” option, then at the time of programming the first YubiKey, you need to click on the “Write Configuration” button. Afterwards, you need to just remove the programmed YubiKey from the USB port and need to insert the new YubiKey. The new YubiKey will be programmed automatically.

If the “Automatically program YubiKeys when inserted” option is not selected, then you need to click on the “Write Configuration” button every time you program a new YubiKey.

## 5.5.2 HMAC-SHA1

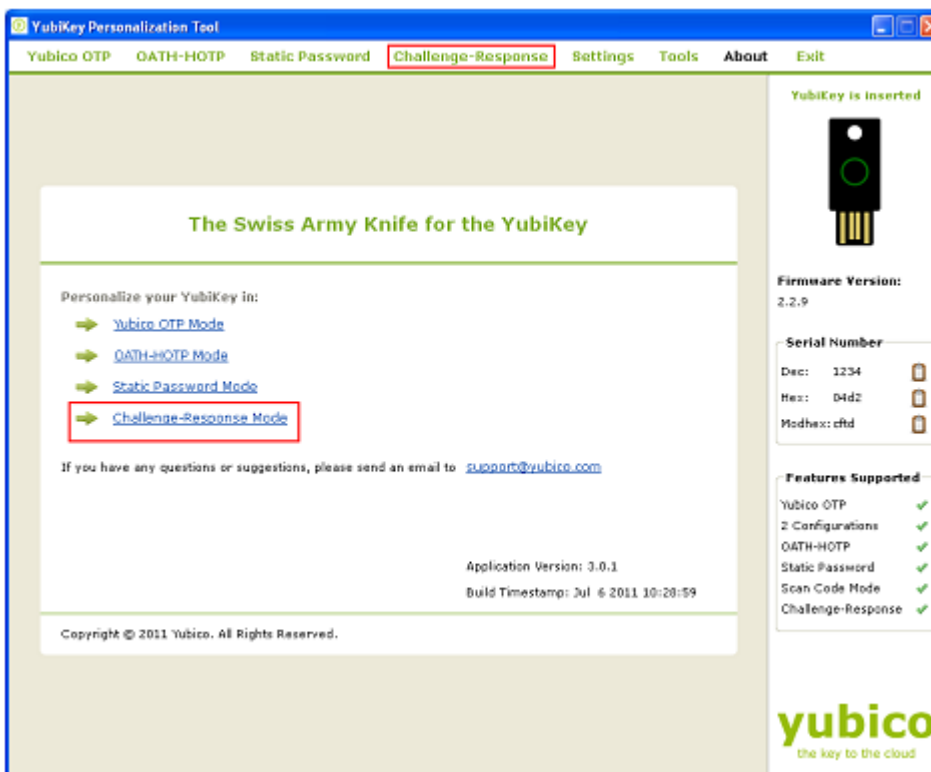
The response is formed as a HMAC-SHA1 operation of the challenge. The secret is fixed 20 bytes (160 bits). The challenge (data) can either be variable 0-63 bytes input or a fixed 64-byte string. In order to be compatible with the low-level USB interface, these modes have to be explicitly selected at the time of configuration.

To program the YubiKey in Yubico OTP Challenge Response mode, follow the steps below:

- Start the YubiKey Personalization Tool



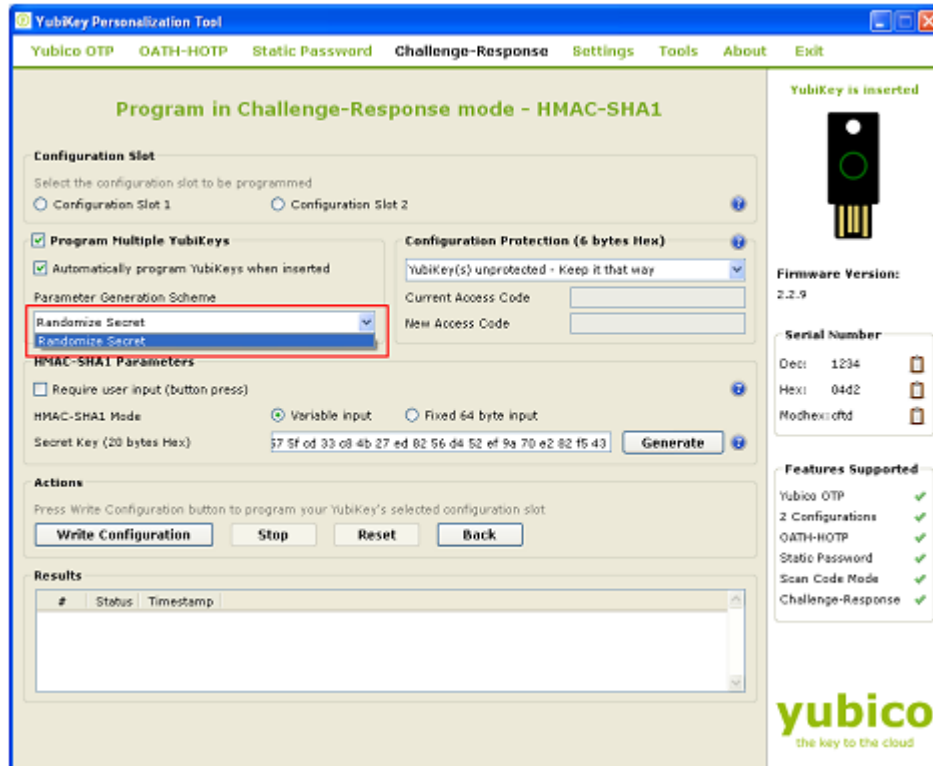
- 2) Insert the YubiKey in the USB port
- 3) Click on either “Static Password” or “Static Password Mode” as highlighted in the image below




- 4) From “Program in Challenge-Response mode”, click on the “Yubico OTP” button



- 5) From the "Configuration Slot" select the appropriate configuration slot
- 6) If you want to program multiple YubiKeys, then select the "Program Multiple YubiKeys" option.
- 7) If the "Program Multiple YubiKeys" option is selected, you can specify if you want to automatically program the YubiKeys when inserted or you want to click on the "Write Configuration" button every time to program a new YubiKey. Also, you can specify how the parameters used for programming the YubiKeys will be generated. There is only one option "Randomized Secret":

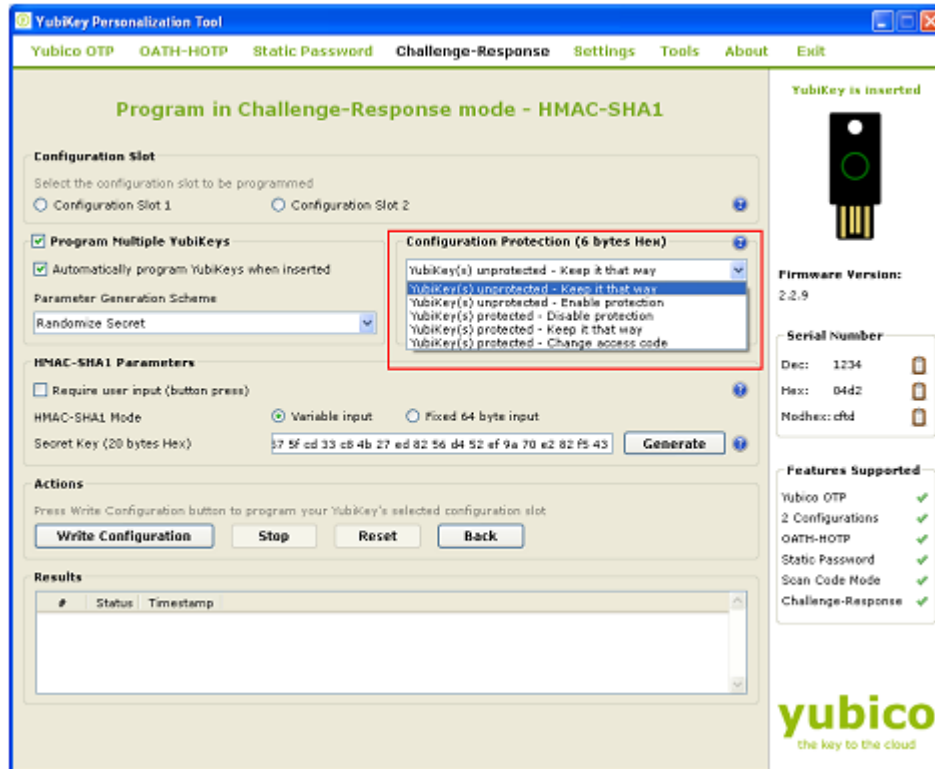


For more information, please click on the help button .


- 8) To protect against unauthorized update of a specific configuration, a configuration protection password can be added. Then, in order to update or remove this configuration, the corresponding configuration protection password must be used, otherwise the request is rejected.

In the “Configuration Protection” section, you can specify if you want to set the configuration protection password.

There are five options available:




- i) YubiKey(s) unprotected – Keep it that way:
- ii) YubiKey(s) unprotected – Enable protection:
- iii) YubiKey(s) protected – Disable protection:
- iv) Key(s) protected – Keep it that way:
- v) YubiKey(s) protected –Change access code:

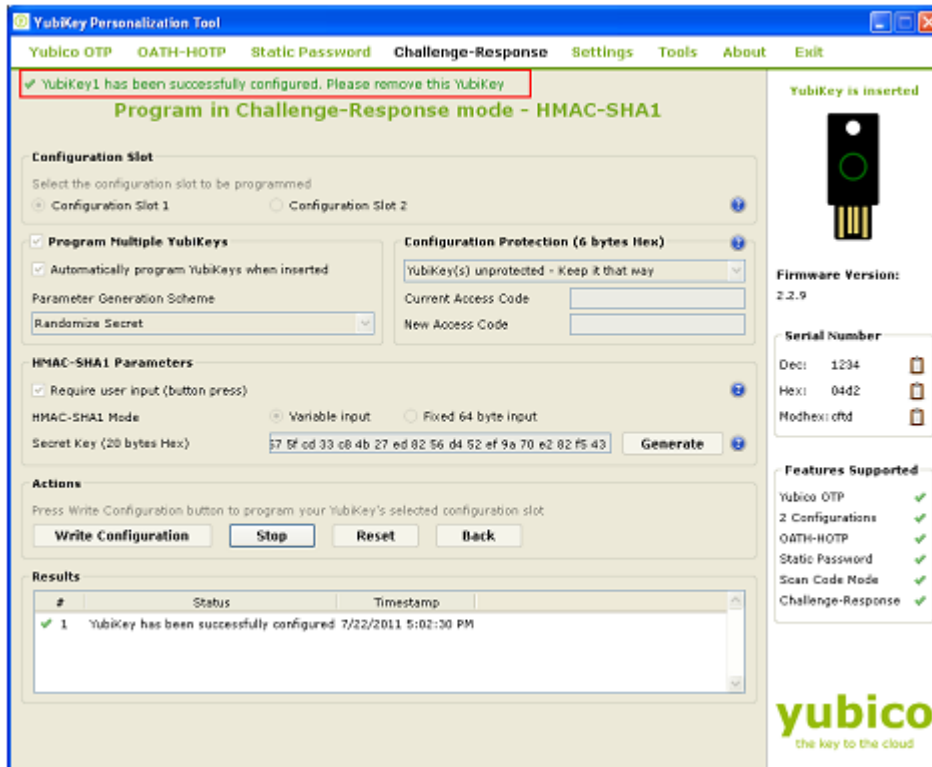
- 9) Select the appropriate option. Click on the help button  for more information.
- 10) From “HMAC-SHA1” Parameters, you can select HMAC-SHA1 mode and the Secret Key.
  - i) Select “Require user input (button press)” if you want the users to press the button in order to generate the response to the challenge. If this option is not selected then the response will be generated automatically without user intervention.

Click on the help button for more information.

- ii) HMAC-SHA1 Mode: You can select either “Variable input” or “Fixed 64 bytes input”
- iii) Secret Key: The secret key is used to encrypt the OTP. By default, it is randomly generated and set to 20 bytes length. You can regenerate it by clicking on the “Generate” button next to it.

For more information, click on the help button .

- 11) From the “Actions”, click on the “Write Configuration” button to configure the YubiKey in HMAC-SHA1 challenge response mode.



If you are programming multiple YubiKeys and have selected the “Automatically program YubiKeys when inserted” option, then at the time of programming the first YubiKey, you need to click on the “Write Configuration” button. Afterwards, you need to just remove the programmed YubiKey from the USB port and need to insert the new YubiKey. The new YubiKey will be programmed automatically.

If the “Automatically program YubiKeys when inserted” option is not selected, then you need to click on the “Write Configuration” button every time you program a new YubiKey