

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



Contents

Introduction						
	Disclai	mer2				
	Traden	narks2				
	Contac	2 Information				
1	Doc	ument Information5	,			
	1.1	Purpose5	;			
	1.2	Audience5	,			
	1.3	References	;			
	1.4	Document History	;			
	1.5	Definitions5	;			
2	Intro	duction6	;			
3	Bacl	kground and Pre-Requisites7	,			
	3.1	System Requirements	,			
	3.1.1	1 Windows Platform7	,			
	3.1.2	2 Linux Platform7	,			
	3.1.3	3 MAC OS X Platform7	,			
	3.2	Random numbers7	,			
	3.2.1	1 Windows Platform7	,			
	3.2.2	2 Linux Platform7	,			
	3.2.3	3 MAC OS X Platform	,			
	3.3	Security and cryptographic practices	;			
4	Insta	allation)			
	4.1	Downloading the cross-platform YubiKey Personalization Tool)			
	4.2	Installing the application)			
	4.2.2	1 Windows Platform)			
	4.2.2	2 Linux Platform				
	4.2.3	3 MAC OS X Platform				
5	Usin	g the application14	ļ			
	5.1	Common Tasks and settings14	ļ			
	5.1.1	1 Getting the YubiKey Firmware version14	ļ			
	5.1.2	2 Settings	;			
	5.1.3	3 Tools17	,			
	5.1.4	4 Getting help	;			
	5.2	Creating a Yubico OTP configuration	;			
	5.2.2	1 Quick Option	5			

5.2.2	Advanced Option	22
5.3 C	reating a OATH-HOTP Configuration	27
5.3.1	Quick Option	27
5.3.2	Advanced Option	30
5.4 C	reate a static configuration (Static Password)	34
5.4.1	Scan code	34
5.4.2	Advanced Option	39
5.5 C	hallenge-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 <u>http://forum.yubico.com</u>
- 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:

🙀 YubiKey Personalization Tool	
Welcome to the YubiKey Personalization Tool Y Setup Wizard	ubico
The installer will guide you through the steps required to install YubiKey Personalizati computer. WABNING: This computer program is protected by copyright law and international tr	on Tool on your aaties
Unauthorized duplication or distribution of this program, or any portion of it, may result or criminal penalties, and will be prosecuted to the maximum extent possible under th	in severe civil e law.
Cancel < Back	<u>N</u> ext >

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

👸 YubiKey Personalization Tool	
Select Installation Folder	yubico
The installer will install YubiKey Personalization Tool to the following folder. To install in this folder, click "Next". To install to a different folder, enter it be Folder:	łow or click "Browse".
C:\Program Files\Yubico\YubiKey Personalization Tool\ Install YubiKey Personalization Tool for yourself, or for anyone who uses t	Browse Disk Cost
⊙ Everyone O Just me	
Cancel < <u>B</u> ack	<u>N</u> ext>

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

🛱 YubiKey Personalization Tool	
Installing YubiKey Personalization Tool	yubico
YubiKey Personalization Tool is being installed.	
Please wait	
Cancel	ck <u>N</u> ext >

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

😽 YubiKey Personalization Tool	
Installation Complete	yubico
YubiKey Personalization Tool has been successfully installed. Click "Close" to exit.	
Cancel < <u>B</u> ack	

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

🛗 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

	Finder	File	Edit	View	Go	Window	Help	
	10							
	Nubili							
P	ersonalir	.ey nac.dm	Ig					
	Contraction of the local division of the loc	-					CONTRACTOR OF CONTRACTOR	ļ

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.



Cross-platform YubiKey Personalization Tool





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

0	00		0	YubiKey Personalization T	ool				
Y	ubico OTP	OATH-HOTP	Static Password	Challenge-Response	Settings	Tools	About	Exit	
								No YubiKey inser	ted
								•	
		The	Swiss Army Kı	nife for the YubiK	ey			TUI	
	Person	alize your YubiKey	in:					Firmware Version: N/A	
		TUDICO UTP MODE						Control Number	
		OATH-HOTP Mode						Serial Number	
	-	Static Password Mo	de					Dec: N/A	
								Hex: N/A	
	- T	Unationge-Respons	e Mode					Modhex: N/A	
	If you ha	we any questions or si	uggestions, please send a	n email to support@yubk	10.com				
								Features Support	ed
								Yubico OTP	N/A
								2 Configurations	N/A
				Application Versi	ap: 3.0.1			CATH-HOTP Static Parcented	N/A
				Puppicedon Vers				Scan Code Node	N/A
				Build Timestamp	x JUI 6 2011 1	1:44:17	_	Challenge-Response	N/A
	Copyrigh	t © 2011 Yubico. All R	ights Reserved.						
								yubic the key to the clo	CO Nud

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

0	YubiKey Per	sonalization Tool							
1	ubico OTP	OATH-HOTP	Static Password	Challenge-Response	Settings	Tools	About	Exit	
								No YubiKey inse	rted
		The :	Swiss Army K	nife for the YubiK	(ey				
	Person	alize your YubiKey Yubico OTP Mode	in:					Firmware Version N/A	i:
	-	OATH-HOTP Mode Static Password No	ude					Serial Number	
	+	Challenge-Respons	e Made					Modhex: N/A	
	3f yau h	ave any questions or	suggestions, please send	i an armail to <u>succontribuubi</u> :	<u>20.00m</u>			Features Suppor Yubics OTP 2 Configurations OATH-HOTP	N/A N/A N/A
				Application Vers	ion: 3.0.1			Static Password	N/A
				Build Timestern	p: Jul 6 2011 :	10:28:59		Scan Code Mode Challence-Respons	N/A e N/A
	Copyrig	ht © 2011 Yubico. All	Rights Reserved.						
								yubic	CO

- 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.

O YubiKey Personalization Tool	
Yubico OTP OATH-HOTP Static Password Challenge-Response Settings Tools About	Exit
Yubikey Personalization Tool Yubico OTP OATH-HOTP Static Password Challenge-Response Settings Settings © Use and enforce customer prefix (Decimal) • • Output Settings • • Output Format • • Tab Public ID Tab • Output Speed Throttling • • Output Character Rate Standard • Add a short delay before sending OTP part • • Serial # Visibility Settings (YubiKey 2.2) • • © USB descriptor • • • Ø usban et startup • • • • Ø usban et s	Exit YubiKey is inserted YubiKey is inserted Firmware Version: 2.2.9 Serial Number Dec: 1234 Mex: 04d2 Mex: 04d2 Mex: 04d2 Modhex:cftd Vubice OTP 2 Configurations OATH-HOTP Static Pessmord Static Pessmord Challenge-Response V
Actions Press Save to save your settings Save Cancel Restore Defaults	yubico

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

 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 ext 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

I	D YubiKey Per	sonalization Tool							
Γ	Yubico OTP	OATH-HOTP	Static Password	Challenge-Response	Settings	Tools	About	Exit	
								No YubiKey in	serted
		The s	Swiss Army K	nife for the Yubik	ey				
l	Person	alize your YubiKey	in:					Firmware Versi N/A	on:
L	-	Yubico OTP Made							
L	-	OATH-HOTP Mode						Serial Number	· · · · ·
L	-	Static Password Mc	de					Dec: N/A	
l	-	Chalence-Respons	e Mode					Modhes: N/A	
	If you h	ave any questions or :	sugpestions, please serv	d an email to <u>support@vubi</u>	10.00m			Features Supp Yubico OTP 2 Configurations	orted N/A N/A
L				Application Vers	ion: 3.0.1			OATH-HOTP Static Password	N/A
l				Build Timestam	p: Jul 6 2011 1	10:28:59		Scan Code Mode Challence-Baspo	N/A
	Copyrig	ht © 2011 Yubico. All i	Rights Reserved.						
								yubi	CO

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.

O YubiKey Perse	malization Tool						
Yubico OTP	OATH-HOTP	Static Password	Challenge-Response	8 ettings	Tools	About	Exit
	Dreed	aram in Vubica	OTD mede - Oui	a la			YubiKey is inserted
	Ριοί	gram in Yubico	5 OTP mode - Qui	ск			•
Configuration	Slot						0
Select the confi Cenfiguratio	guration elot to be p e Skyt 1	Configuration Si	lot z				
Yubico OTP Pa	arameters (auto c	(enerated)				_	
Public Identity ((6 bytes Nodhex)	vv kā ve iolītij					Firmmere Version:
Hide values							2.2.9
Private Edentity	(6 bytes Hex)	••••••	•				Serial Number
Secret key (16	bytes Mex)	**********				۳	Dec: 1234
Actions	vieranien hetten te	ameran usur Vahidada	calastad coofficientics dat				Hexi 04d2
Write Con	figuration	Upload to Yubice	Regenerate	Back			Machexichd
							Features Supported
							Yubice OTP 🕜
							2 Configurations V OATH-HOTP V
							Static Password 🛷
							Challenge-Response 🗸
							vubico
							yubicu
•	• =	Yubico /	AES Key Upl	oad			
Please Please Servie Your e Serial Yuhik	e enter informa e note: It taka ers. Please wa e-mail address i number: ev nrefix:	ation about your r as 15 minutes for it 15-20 minute: :: 1234 vv&tveinilii	newly personalized Yu r an uploaded identit s before testing an u	/biKey. y to becon ploaded id	ne valid entity.	on our	validation
laters	of prons.	50-17-(50-(07))					
AEG V	ovi	1864969646412	sh8h5c59715ad962				
ALS N	rom the Yubik's	1000000003110	ADD0000071000002				
		V SI 185	9 MCNTDRA- MORP ROOM. Face B books.				

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

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

YubiKey Personalization	n Tool						×
Yubico OTP OATH	-HOTP Static Password	f Challenge-Response	Settings	Tools	About	Exit	
						No YubiKey inserted	1
						\circ	
	The Swiss Army	Knife for the Yubik	(ey				
Personalize your	YubiKey in:					Firmware Version: N/A	
Yubico OT	P Mode					Serial Number	_
ATH-HO	P Mode					Dec: N/A	
Static Pas	sword Mode					Hexi N/A	
Chalenge	Response Mode					Modhex::N/A	
3f you have any qu	estions or suggestions, please se	end an email to <u>Support@vubi</u>	<u></u>			Features Supported	5
						2 Configurations N/	A A
						OATH-HOTP N/	A
		Application Vers	tion: 3.0.1			Static Password N/	A
		Build Timestam	p: Jul 6 2011 10	1:28:59		Challenge-Response N/	a.
Copyright @ 2011 \	ubico. All Rights Reserved.						
						yubico)

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

YubiKey Personalization Tool	
Yubico OTP OATH-HOTP Static Password Challenge-Response Bettings Tools Abou	t Exit
Program in Yubico OTP mode	YubiKey is inserted
Quick Quicky program a YubiKey for use with Yubico Validation Server Advanced Allows you to program one or more YubiKeys with greater control over the configuration values	Firmware Version: 2.2.9
	Dec: 1234 Dec: 1
	Peatures Supported Yubico OTP V 2 Configurations V 0ATH-HOTP V Static Password V Scan Code Mode V Challenge-Response V
	yubico

- 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:

🛛 YubiKey Personalization Tool 📃 🗖 🔀									
Yubico OTP OATH-HOTP S	tatic Password	Challenge-Response	Settings	Tools Al	bout Exit				
Program Configuration Slot	YubiKey is inserted								
Select the configuration slot to be prog Configuration Slot 1									
Program Multiple YubiKeys		Configuration Protection	on (6 bytes H	ен)	, Ш				
Automatically program YubiKeys wh	en inserted	YubiKey(s) protected - Cf	lange access o	ode N	Firmware Version:				
Parameter Generation Scheme		Current Access Code	00 00 00 00 00	00 00	2.2.9				
Increment Identities; Randomize Seco Increment Identities; Randomize Seco	et 💌	New Access Code	00 00 00 00	00 00	Serial Number				
Randomize all parameters					0ec: 1234				
Public Identity (1-16 bytes Nodhex)	ejrett trifoc			Generate	Mex: 04d2				
Public Identity Length	6 🤤 (6 bytes is	default length as required by	Yubico OTP va	idation server)	Modhex:cftd				
Private Identity (6 bytes Hex)	53 a0 b9 f1 ec f7			Generate					
Secret Key (16 bytes Hex)	c2 94 9a be a7 57	36 38 06 03 ab 0b 3e 14 42 6	d C	Generate	Features Supported				
Actions Press Write Configuration button to p	Actions Press Write Configuration button to program your YubiKey's selected configuration slot								
Write Configuration 5	itop Res	et Back			Static Password V Scap Code Mode				
Results Public Identity (Modhex)	Challenge-Response v								
				5	yubico				

- 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:

8

💿 YubiKey Perso	nalization Tool							
Yubico OTP	OATH-HOTP	Static Password	Challenge-Response	Settings	Tools	About	Exit	
	Progra	ım in Yubico O)TP mode - Advar	nced			YubiKey is insert	ed
Configuration Select the confi O Configuration	Slot puration slot to be p n Slot 1	rogrammed O Configuration SI	ot 2			0	0	
Program Mi	ultiple YubiKeys		Configuration Protectio	n (6 bytes H	ен)			
Automatical	y program YubiKeys	when inserted	YubiKey(s) unprotected -	Keep it that w	νγ	~	Firmware Version:	
Parameter Gene	Parameter Generation Scheme							
Increment Iden	rtities; Randomize S	ecret 🕑	YubiKey(s) protected - Do YubiKey(s) protected - Ke	ep it that way	n ode		Serial Number	
Yubico OTP Pa	rameters		- (Iddine)(s) protected - ci	ange access c			Dec: 1234	۵
Public Identi	ty (1-16 bytes Madh	ex) ej re tt tr rf gf			Generate	0	Hext: 04d2	۵
Public Identity L	ength	6 🤤 (6 bytes is	default length as required by	Yubico OTP ve	lidation serv	(er)	Modhex: oftd	۵
Private Iden	lity (6 bytes Hex)	53 a0 b9 f1 ec f7			Generate	0		
Secret Key (16	bytes Hex)	21 ee 2b e7 b4 84	aa 35 8d 82 3f 02 bd 53 02 ci	2	Generate	0	Features Support	ed
Actions							Yubico OTP	1
Press Write C	onfiguration button t	to program your YubiKey	's selected configuration slot				2 Configurations	1
Write Con	figuration	Stop Res	et Back				Static Password	1
							Scan Code Mode	*
Results							Challenge-Response	1
# Pub	lic Identity (Modhex) Status Timestamp				~		
						×	vubic	0
<u> </u>							the key to the clou	

- 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 **1** 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.

2 YubiKey Personalization Tool					
Yubico OTP OATH-HOTP Static Password	Challenge-Response	Settings T	ools About	Exit	
YubiKey (Public ID: drbechithet) has been successfully Program in Yubico OT	configured I P mode - Advar	iced		YubiKey is insert	ed
Configuration Slot Select the configuration slot to be programmed Configuration Slot 1 Configuration Slot	:2			0	
Program Multiple YubiKeys	Configuration Protectio	n (6 bytes Hex)	0	(140)	
Automatically program YubiKeys when inserted	YubiKey(s) unprotected - I	Ceep it that way	*	Firmware Version:	
Parameter Generation Scheme	Current Access Code			2.2.9	
Increment Identities; Randomize Secret	New Access Code			Serial Number	
Yubico OTP Parameters Publico Identity (1-16 bytes Mothex) dr be ol ni fh ef Publico Identity Length 6 Ø Private Identity (6 bytes Hex)	lefault length as required by	Ger Yubico OTP valida Ger	tion server)	Dec: 1234 Hex: 04d2 Modhex:dtd	
Actions Press Write Configuration button to program your Yub Key's Write Configuration Stop Reset	selected configuration slot	Ger	ierate 😈	Features Supports Yubico OTP 2 Configurations OATH-HOTP Static Password Scan Code Node	ed > > > > > > > >
Results # Public Identity (Nodhex) State If Grbechniftef YubiKey has been succession	us Ti cessfully configured 7/21/20	mestamp 11 8:17:33 PM	×	Challenge-Response yubic	• •

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

YubiKey Perso	onalization Tool							
Yubico OTP	OATH-HOTP	Static Password	Challenge-Response	Settings	Tools	About	Exit	
							No YubiKey	inserted
	The S	Swiss Army Kr	nife for the Yubik	(ey				Γ
Personal	lize your YubiKey	in:					Firmware Ver x/A	sion:
🔶 X	ubico OTP Mode						-Serial Numb	er
• • •	OATH-HOTP Mode						Dec: N/A	
🔶 🔶 S	tatic Password Mo	de					Hexi M/A	
ء 🔶	hallenge-Respons	e Mode					Modhes:: N/A	
3f you hav	ve any questions or s	ruggestions, please send	an emeil to <u>Support@w.b</u> i	60.60M			Features Su Yubico OTP 2 Configuratio	pported N/A ns N/A N/A
			Application Ven	sion: 3.0.1			Static Passwor	d N/A
			Build Timestam	p: Jul 6 2011	10:28:59		Scan Code No	de N/A
Copyright	© 2011 Yubico. All F	lights Reserved.					Challenge-Res	ponse N/A
							yub	ico he cloud

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



YubKey Personalization Tool		
Yubico OTP OATH-HOTP Static Password Challenge-Response Settings To	ols About	Exit
Program in OATH-HOTP mode - Quick		YubiKey is inserted
Configuration Slot Select the configuration slot to be programmed Configuration Slot 1 Configuration Slot 2		○
OATH-HOTP Parameters (auto generated) Image: OATH Token Identifier (6 bytes) ubnu 00 00 12 34 HOTP Length Image: Origits Image: Mide secret	0	Firmware Version: 2.2.9
Secret Key (20 bytes Hex)	0	Serial Number
Actions Press Write Configuration button to program your YubiKey's selected configuration slot Write Configuration Programsta Progra		Hexi 04d2 📋 Modhexii dtd
		Features Supported Yubico OTP * 2 Configurations * OATH-HOTP * Static Password * Static Code Node * Challenge-Response *
		yubico

- 6) The YubiKey supports the Token Identification Specification as outlined by 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 sutton.

- 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



ĺ	YubiKey Personalization Tool							
	Yubico OTP OATH-HOTP	Static Password	Challenge-Response	Settings	Tools Ab	bout	Exit	
	Configuration Slot Select the configuration slot to be	programmed	HOTP mode - Qui	ck			YubiKey is inserte	ed
	DATH HOTP Parameters (auto	annerstad)						
	OATH Token Identifier (6 bytes HOTP Length Kide secret) ubnu 00 00 12 34	Gen Digits	erate MUI	6	9	Firmware Version: 2.2.9	
	Secret Key (20 bytes Hex)						Serial Number	
	Actions Press Write Configuration button t Write Configuration	o program your YubiKey's Regenerate	s selected configuration slot. Back				Dec: 1234 Hexi 04d2 Mothexi oftd	
							2 Configurations	4
							OATH-HOTP Static Password Scan Code Node Challenge-Response	* * * *
							yubic	0

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

Yubico OTP OATH-HOTP Batic Password Challenge-Response Bettings Tools About Exit * YubiKey (OATH ID: ubnu00001234) has been successfully configured Program in OATH-HOTP mode - Quick YubiKey (OATH ID: ubnu00001234) has been successfully configured YubiKey (ID: Ubnu00001234) has been successfully configured Image: Ubnu00001234 has been successfully configured YubiKey (ID: Ubnu00001234) has been successfully configured Image: Ubnu00001234 has been successfully configured Image: Ubn	📴 YubiKey Personalization Tool		
Vubikey (0ATH ID: ubnu00001234) has been successfully configured Program in OATH-HOTP mode - Quick Configuration Slot Select the configuration slot to be programmed Image: Configuration Slot 1 Image: Configuration Slot 2 Image:	Yubico OTP OATH-HOTP Static Password Challenge-Response Settings Tools	About	Exit
	YubiKey Personalization Teol YubiCo OTP OATH-HOTP Static Password Challenge-Response Settings Tools ✓ YubiKey (OATH ID: ubnu00001234) has been successfully configured Program in OATH-HOTP Product Configuration Slot Select the configuration slot to be programmed Quick © Configuration Slot 1 © Configuration Slot 2 Configuration Slot 2 DATH-HOTP Parameters (auto generated) © OATH Taken Identifier (6 bytes) ubnu 00 00 12 34 WOTH Length © 6 Digits © 8 Digits ✓ Hide secret Secret Key (20 bytes Hex)	About Q Q Q	Exit Exit Yubitey is inserted Firmware Version: 2.2.9 Serial Number Deci 1234 Hexi 04d2 Hexi 04d2 Modhexi offd Peatures Supported Yubics OTP

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

YubiKey Personalization	Tool					
Yubico OTP OATH-P	IOTP Static Passwo	ord Challenge-Response	Settings	Tools	About	Exit
						No YubiKey inserted
	The Swiss Army	/ Knife for the Yubik	(ey			
Personalize your Y	ubiKey in: Mode					Firmware Version: x/A
	Mode					Serial Number
Static Passe Chalence-B	vord Mode Jesponse Mode					Hexi N/A Nodhexi:N/A
If you have any quest	ions or suggestions, please	i send an email to <u>Support@w.kbi</u>	60.00m			Features Supported Yubico OTP N/A 2 Configurations M/A
		Application Ver Build Timestam	tion: 3.0.1 p: Jul 6 2011 :	10:28:59		OATH-HOTP N/A Static Password N/A Scan Code Mode N/A
Copyright @ 2011 Yub	ico. All Rights Reserved.					Challenge-Response N/A
Ck on either "(YubKey Personalization Yubico OTP OATH-F	DATH-HOTP" Tsol IOTP Static Passwa	or "OATH-HOTP	Mode" Settings	as hig Tools	hligh	ted in the ima
						No YubiKey Inserted
	The Swiss Army	/ Knife for the Yubił	(ey			

2) C below

	The S							No YubiKey Insert
	The S							
		wiss Army Kı	nife for t	he YubiK	ey			
Personalize you	ur YubiKey	in:					Fi N/	irmware Version: /A
Yubice C QATH-49 Static P: Challence If you have any c	OTP Mode OTP Mode assword Mo ae-Respons questions or s	de <u>e Mode</u> upgestions, please send	d an smail to 💈	aupport@yubic	0.00m		с ни т	Serial Number Nac: N/A Isathex: N/A Isathex: N/A Peatures Supports Ubico OTP
			A E	Application Versi Build Timestamp	ian: 3.0.1): Jul 6 2011 3	0:28:59	2 0 5 5	Configurations XATH-HOTP Ratic Password ican Code Node
Copyright © 2013	L Yubico, All P	tights Reserved.						hallenge-Response.

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

YubiKey Perso	nalization Tool							
Yubico OTP	OATH-HOTP	Static Password	Challenge-Response	Settings	Tools	About	Exit	
	1	Program in OA	TH-HOTP mode				YubiKey is in	serted
Quick Quicky program	m a YubiKey in OAT	TH-HOTP mode				_		
Advanced Allows you to p	program one or mo	are YubiKeys in CATH-HO)TP mode with greater control	over the config	juration va	lues	Firmware Versi 2.2.9	ion:
L							Serial Number	
							Dec: 1234	۵
							Heixi 04d2 Modhexi oftd	Ŭ
							Features Supr	ported-
							Yubico OTP	1
							OATH-HOTP	÷.
							Static Password Scan Code Node	. 1
							Challenge-Respo	inse 🗸
							yubi	CO

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

9 YubiKey Personalization Tool								
Yubico OTP OATH-HOTP 8	tatic Password	Challenge-Response	Settings	Tools	About	Exit		
Program	in OATH-HC)TP mode - Adva	nced			YubiKey is insert	ed	
Configuration Slot Select the configuration slot to be prog Configuration Slot 1	rammed O Configuration SI	ot 2 Configuration Protectio	e (6 bytes H	ex)	9			
Automatically program Yub Keys wh	~	Firmware Version:						
Parameter Generation Scheme 😢 Current Access Code						2.2.9		
Increment Identities; Randomize Seco	Serial Number	_						
DATH-HOTP Parameters						Dec: 1234	٥	
OATH Token Identifier (6 bytes)	All numeric		×			Hex: 04d2		
OMP (1) + TT (1) + MUI (4)	00 00 00 00	Generate	MUL			Modhex: cftd	٥	
HOTP Length	⊙ 6 Digits ○ 8 I	Digits						
Moving Factor Seed	Pixed zero	M 0				Features Supported		
Secret Key (20 bytes Hex)	00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 0		Generate		Yubico OTP	1	
Actions						OATH-HOTP	2	
Press Write Configuration button to pro	gram your YubiKey's	selected configuration slot				Static Password	1	
Write Configuration S	itop Resi	t Back				Scan Code Node	1	
						Challenge-Response	×	
OATH Token Identifier St	tatus Timestamp					yubic	0	

- 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.

- The YubiKey supports the Token Identification Specification as outlined by 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 ¹² 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:



Yubico OTP	OATH-HOTE	Static Bassword	Challenge-Response	Sottings	Tools	About	Evit	
TUBICO OTP	OATH-HOTP	atatic Password	Gnatienge-Kespanse	aettings	TODIS	ABOUT	esit	
	Progra	m in OATH-H	OTP mode - Adva	nced			YubiKey is inse	rted
	riogra		orr mode ridea				•	
Configuration S	ilot						\odot	
Select the config.	iration slot to be p	programmed				~	\sim	
 Configuration 	Slat 1	 Configuration 5 	ilat 2				ΠΠ	
🗹 Program Mul	tiple YubiKeys		Configuration Protectio	n (6 bytes H	ex)	0	1	
🗹 Automatically	program YubiKeys	s when inserted	YubiKey(s) unprotected -	Keep it that w	ày	*	Firmware Version	n:
Parameter Gener	ation Scheme		Current Access Code				2.2.9	
Increment Identi	Kies; Randomize S	šecret 🤟	New Access Code				Serial Number	
OATH-HOTP Par	ameters						Dec: 1234	ſ
OATH Token 1	dentifier (6 bytes)	All numeric		~			Hexi 04d2	ĩ
OMP (1) + TT (1)	+ MUI (4)	00 00 70 6	0 11 60 Generate	MUT			Nodhex:cftd	Ē
HOTP Length		⊙ 6 Digits ○ 8	Digits			0		
Moving Factor Se	ed	Fixed zero	✓ 0				Features Suppo	rted
Secret Key (20 b	ytes Hex)	Fixed Fixed	oc f 7 d4 98 15 2	6 06 93	Generate	0	Yubico OTP	
Actions		Randomize					2 Configurations	
Press Write Confi	guration button to	program your YubiKey'	s selected configuration slot				Static Password	
Write Confi	guration	Stop Res	et Back				Scan Code Node	
							Challenge-Respons	
Results	Talan Ideald	Challens Time and service						
# QATH	roken sdehötler	atatus rimestamp						
							a constanti a	_
						-	yubi	
						1.74	the key to the d	bud

- ii) Fixed
- iii) Randomize



- 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
- Click on either "Static Password" or "Static Password Mode" as highlighted in the image below

0 Yı	abiKey Perso	nalization Tool									
Yu	bico OTP	OATH-HOTP	Static Password	Challenge-I	Response	Settings	Tools	About	Exit		
Yu	Personali	The state of the s	Static Password Swiss Army Kr in: in: suggestions, please cend Rights Reserved.	Challenge-I nife for th an email to Si Ap Ba	Response re Yubik innort&wbi splication Ver aid Timestam	8ettings (ey iien: 3.0.1 p: 3.1 6 2011 1	Tools	About	Exit YubiKey Firmware 2.2.9 Secial Nu Dec: 12 Hexi 04 Mochesi off Yubics OTP 2 Configun OATH-HOT Statio Pass Scan Code Challenge-	Version: Wersion: 34 42 43 Support Support Node Response	
									yul	bic to the close	0



4) From "Program in Static Password mode", click on the "Scan Code" button



5) From the "Configuration Slot", select the appropriate configuration slot.

10 YubiKey Personalization Tool						
Yubico OTP OATH-HOTP Static Password	Challenge-Response	Settings	Tools	About	Exit	
Program in Static Passy	word mode - Sca	n Code			YubiKey is insert	ed
Configuration Slot Select the configuration slot to be programmed C Configuration Slot 1 Configuration Slot	et 2				0	
Program Hultiple YubiKeys						
Automatically program YubiKeys when inserted	Automatically program YubiKeys when inserted YubiKey(s) unprotected - Keep it that way					
	Current Access Code				2.2.9	
	New Access Code				Serial Number	
Password Hide Password Password Length Password Insert Tab It is strongly recommended to create a backup YubiKey Actions Press Write Configuration button to program your YubiKey's Write Configuration Stop Results Password Length Stabus Timestamp	sken	Dec: 1234 Hexi 0442 Mothexi oftd Features Support Yubico OTP 2 Configurations OATH-HIOTP Statio Password Scari Code Mode Challenge-Response	4 4 4 4 4 B			
					the key to the close	O

- 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:

YubiKey Personalization Tool					
Yubico OTP OATH-HOTP Static Password	Challenge-Response	Settings	Tools About	Exit	
Program in Static Pass Configuration Slot Select the configuration slot to be programmed O Configuration Slot 1 O Configuration Slot	word mode - Sca	n Code	e	YubiKey is insert	ed
Program Hultiple YubiKeys Automatically program YubiKeys when inserted	Configuration Protection YubiKey(s) unprotected - YubiKey(s) unprotected YubiKey(s) protected - Dir YubiKey(s) protected - Ke	n (6 bytes Hea Keep it that way Enable protection sable protection ep it that way		Firmware Version: 2.2.9	
Password Hide Password Password Registry (Nax. 38 chara	for YubiKey 2.2 and 16 char	a for 2.0 and 2.1)		Dec: 1234 Hex: 0442 Modhex: cftd	0 0 0
Insert Tab It is strongly recommended to create a backup YubiKe Actions Press Write Configuration button to program your YubiKey's Write Configuration Stop Reso Results	Clear y with same password in case selected configuration slot et Back	original YubiKey	is lost/broken	Features Supports Yubico OTP 2 Configurations OATH-HOTP Static Password Scan Code Mode Challenge-Response	4 + + + + + + + + + + + + + + + + + + +
Password Length Status Timestamp				yubic	0

- 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.

YubiKey Personalization Tool					
Yubico OTP OATH-HOTP Static Password	Challenge-Response	Settings	Tools /	About	Exit
Program in Static Pass	word mode - Sca	n Code			YubiKey is inserted
Select the configuration slot to be programmed Configuration Slot 1 Configuration S	lot 2	o 16 hosto e He		0	
Automatically program Whiteys when inserted	Wiki/av/c) unpertented a	n (o bytes He	(x)		
Automatically program subikeys when inserved		Firmware Version: 2.2.9 Serial Number			
Password Password Length Password Length Password Length Password Password It is strongly recommended to create a backup YubiKo	n for Yubikay 2.2 and 16 chan Clear	original YubiKe	1) by is lost/brok	• • • •	Deci 1234 Hexi D4d2 Wodhexi otd Yubico OTP Conformation d
Actions Press Write Configuration button to program your YubiKey' Write Configuration Stop Res	s selected configuration slot et Back				CATH-HOTP & Static Password & Scan Code Node & Challenge-Response &
Password Length Status Timestamp					yubico

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

YubiKey Personalization Tool						
Yubico OTP OATH-HOTP Static Pas	sword Ch	allenge-Response	Settings	Tools	About	Exit
YubiKey (Password Length: 14 chars) has b Program in Static Configuration Stat	een successf : Passwo	uly configured ord mode - Sca	n Code			YubiKey is inserted
Select the configuration slot to be programmed Configuration Slot 1 Config Program Multiple Yub/Fave	puration Slot 2	opfiquention Protection	n (6 hytes He		0	
Automatically program YubiKeys when inserted	4 B	ubiKev(s) unprotected - 1	Keep it that wa	ar .	V	Circurate Vention
		Serial Number				
Password Tide Password Password Length 14 (Ma	G 38 chars for	YubiKey 2.2 and 16 char:	; for 2.0 and 2.	1)		Dec: 1234 () Hex: D4d2 () Modhex: cftd ()
Password subically, Inser It is strongly recommended to create a back Actions Press Write Configuration button to program your Write Configuration Stop	ubikey t Tab up YubiKey wit YubiKey's sele Reset	Clear th same password in case exted configuration slot Beck	original YubiK	ey is lost/bro	oken	Features Supported Yubico OTP v² 2 Canfigurations v² OATH-HOTP v² Static Password v² Scan Code Mode v² Challenge-Response v²
Passward Length Si ✓ 1 14 YubiKey has been s	tatus uccessfully co	Timestamp ingured 7/22/2011 3:07:	39 PM		X	yubico

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

0	ubiKey Perso	nalization Tool						
Y	ubico OTP	OATH-HOTP	Static Password	Challenge-Response	Settings	Tools	About	Exit
								No YubiKey inserted
		The S	Swiss Army Ki	nife for the Yubik	(ey			
	Personali	ize your YubiKey ubico OTP Mode MTH-HOTP Mode tatic Password Mc hallence-Respons e any questions or i	in: de a Mode suggestions, please send	an emailto <u>Support@uubi</u>				Firmware Version: K/A Serial Number Dec: N/A Hex: N/A Moshex:N/A Features Supported Yubico OTP N/A 2 Configurations K/A
	Copyright	© 2011 Yubico. All	Rights Reserved.	Application Ver Build Timestam	ion: 3.0.1 p: Jul 6 2011 ;	10:28:59	_	OATH-HOTP N/A Static Password N/A Scan Code Mode N/A Challenge-Response N/A
								yubico

- 2) Insert the YubiKey in the USB port
- 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

🛛 YubiKey Perso	nalization Tool							
Yubico OTP	OATH-HOTP	Static Password	Challenge-Response	Settings	Tools	About	Exit	
Yubico OTP	Pro Pro le m a Yubikey to em	Static Password ogram in Stati	Challenge-Response	Bettings	Tools	About	Exit YubiKey i	s inserted
							Serial Num Dec: 123 Hexi 04d Nochexi ofd Yubico OTP 2 Configurat OATH-HOTP Static Passw Scan Code P Challenge-Ro Challenge-Ro	aber 4 1 2 1 Supported isns 4 ord 4 tode 4 esponse 4 Dicco the cloud

- 5) From the "Configuration Slot" select the appropriate configuration slot
- 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:

Yubico OTP OATH-HOTP Static Password Challenge-Response Settings Tools About Exit Program in Static Password mode - Advanced YubiKey is inserted Select the configuration Slot 1 O Cenfiguration Slot 2 Image: Configuration Slot
Program in Static Password mode - Advanced YubiKey is inserted Configuration Slot Select the configuration slot to be programmed Image: Configuration Slot 1 Image: Configuration Slot 2 Image: Configuration Slot 1 Image: Configuration Slot 2 Image:
Select the configuration slot to be programmed O Configuration Slot 1 O Configuration Slot 2
Program Hultiple YubiKeys Configuration Protection (6 bytes Hex)
Automatically program YubiKeys when inserted YubiKey(s) unprotected - Keep it that way Yersion:
Parameter Generation Scheme Current Access Code 2.2.9
Pised parameters Mew Access Code Serial Number
Randomice all parameters Dec: 1234
Password Langth O 16 chars (16 chars for YubiKey 2.0 and above only) Hext 0442
Public Identity (1-16 bytes Madhex) Generate 😝 Nodhex: dtd
Private Identity (6 bytes Hex) 00 00 00 00 00 00 00 Generate 😝
Secret Key (16 bytes Hex) 00 00 00 00 00 00 00 00 00 00 00 00 00
Strong Password Policy Upper and lower case Alphanumeric Send Las prefix Yubico OTP
2 Configurations 🗸
Actions OATH-HOTP &
Scan Code Node 🗸
Write Configuration Stop Reset Back Challenge-Response V
Results
Password Length Public Identity (Modhex) Status Timestamp public Dentity (Modhex) Status Timestamp public Dentity (Modhex) the key to the cloud

- 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:

8

YubiKey Personalization Tool							
Yubico OTP OATH-HOTP Static Passwo	rd Challenge-Response	Settings	Tools About	Exit			
Program in Static P	assword mode - Adv	vanced		YubiKey is inserte	ed		
Configuration Slot Select the configuration slot to be programmed O Configuration Slot 1 O Configurat	ion Slot 2						
Program Multiple YubiKeys	Configuration Protectio	n (ő bytes He	x) 🕡				
Automatically program YubiKeys when inserted	YubiKey(s) unprotected -	Keep it that way	r 💌	Firmware Version:			
Parameter Generation Scheme	O YubiKey(s) unprotected - YubiKey(s) unprotected -	Enable protection	20	2.2.9			
Fixed parameters	Fixed parameters YubiKey(s) protected - Disable protection YubiKey(s) protected - Keep it that way						
Password Parameters	YubiKey(s) protected - Ch	lange access co	de	Der: 1234			
Password Leonth 0 16 chara	🛞 📴 chars. (16 chars fo	r YuhiKey 2.0 av	d above only)	Hex: 04d2	ň		
Public Identity (1-16 bytes Mothey)	a the state (see state to	6	enerate 🙃	Modher:cftd	ň		
Private Identity (6 bytes Hex) 00 00 00 00	0.00	Generate 0 00 00 00 00 00 00 00 00 00 00 00 Generate 0					
Secret Key (16 bytes Hex) 00 00 00 00	0 00 00 00 00 00 00 00 00 00 00 00 00 0						
Strong Password Policy Upper and	lower case Alphanumeric	Send Lar	prefix	Yubico OTP	4		
				2 Configurations	1		
Actions				OATH-HOTP	1		
Press Write Configuration button to program your Yu	biKey's selected configuration slot			Scan Code Mode	5		
Write Configuration Stop	Reset Back			Challenge-Response	1		
Results							
# Password Length Public Identity (Mode	ez) Status Timestamp						
				vubic	Ο		
			<u>N</u>	the key to the clou	d		

- 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.

vubico

🛛 YubiKey Perso	nalization Tool						
Yubico OTP	OATH-HOTP	Static Password	Challenge-Response	Settings	Tools	About	Exit
- Configuration	Program	in Static Pass	word mode - Adv	/anced			YubiKey is inserted
Select the config O Configuration	uration slot to be ; Slot 1	Configuration SI	ot 2			0	
Program Hu	itiple TubiCeys		Configuration Protection	m (6 bytes H	ex)		
Automatically program YubiKeys when inserted TubiKey(s) unprotected - Keep it that way Parameter Generation Scheme Food parameters V New Access Code				×	Firmware Version: 2.2.9		
- Research Bara	meters						
Researd Length		O 16 chars) 32 🗯 chara (16 chara fa	r Yabilları 2.0 i	and above or	Cele	Hex: 04d2
Public Identity (1	L-16 bytes Modhex				Generate		Nathers: cftd
Secret Key (16 b	(e bytes Hez) sytes Hez)	00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 0		Generate Generate	ē	- Features Supported
Strong Password	I Policy	Upper and lower	case 🗌 Alphanumeric	Send 1	as prefix		Yubice OTP 🛛 🗸 2 Configurations 🗸
Actions Press Write Co	nfiguration button	ta program yaur YubiKey	's selected configuration slot				OJCTH-HOTP 🖌
Write Conf	iguration	Stop Res	nt Back				Scan Code Mode 🗸 🗸 Challenge-Response 🗸
Results # Pauly	eard Length Pu	blic Identity (Modhex)	Status Timestamp				
						×	yubico

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



For more information, click on the help button



10) From the "Strong Password Policy", select the appropriate options

💿 YubiKey Person	alization Tool							
Yubico OTP	OATH-HOTP	Static Password	Challenge-Response	Settings	Tools	About	Exit	
- Configuration 5	Program	in Static Pass	word mode - Adv	vanced			YubiKey is inserts	ed
Select the configuration	ration slot to be p Slot 1 tiple YubiKeys	ogrammed O Configuration SI	lot 2	n (6 bytes H	ен)	0		
Automatically Parameter Gener Fixed parameter	program YubiKeys ation Scheme s	when inserted 9 V	YubiKey(s) unprotected - Current Access Code New Access Code	Keep it that we	Y .		Firmware Version: 2.2.9	
Password Paras Password Length Public Identity (1	meters -16 bytes Modhex)	0 16 chars 💿) 32 🗘 chars (16 chars fo	r YubiKey 2.0 -	and above o Generate	niy)	Dec: 1234 Hex: 04d2 Nodhex:cftd	0 0 0
Private Identity (Secret Key (16 b	6 bytes Hex) ytes Hex)	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00		Generate Generate	0	Features Supports	ed
Actions Press Write Confi	nfiguration button to guration	Upper and lower o program your YubiKay Stop Res	r case Alphanumeric	Send !	as prefix		Yubico OTP 2 Configurations GATH-HOTP Static Password Scan Code Mode Challenge-Response	*****
Results # Passw	ord Length Pub	iic Identity (Modhex)	Status Timestamp			8	yubic	0

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

YubiKey Personalization Tool				
Yubico OTP OATH-HOTP Static Password	Challenge-Response	Settings Tools	About	Exit
YubiKey (Password Length: 64 chars) has been succes Program in Static Passy Configuration Stat	ssfully configured vord mode - Adv	anced		YubiKey is inserted
Select the configuration slot to be programmed O Configuration Slot 1 O Configuration Slot	2 Configuration Protection	(6 bytes Hey)		
Automatically program YubiKeys when inserted	Whitewis) unprotected - 8	(eep it that way		Element Handland
Parameter Generation Scheme 🔮		2.2.9		
Password Parameters Password Length 16 chars Public Identity (1-16 bytes Modhex) rt jf te io ro fh ee If v Private Identity (6 bytes Hex) 15 5e 09 29 bd of Secret Key (16 bytes Hex) 2e 20 bb 79 d7 7f df Strong Password Policy Upper and lower of	64 € chans (16 chars for c vinto dk ni ul vn v) 55 7c 05 6c 93 d2 12 02 0e case ☐ Alphanumeric	YubiKey 2.0 and above Generate Generate Send Las prefix	only) • • • •	Dec: 1234 Hex: 04d2 Modhex: oftd Vubico OTP 2 Configurations
Actions Press Write Configuration button to program your Yubikey's Write Configuration Stop Reset Results # Password Length Public Identity (Modhex) # 1 64 rtjfteiordfieelfvovirbikniu/wy) <	selected configuration slot Back Status YubiKey has been successfu	Tin Ity configured 7/22/201	vesta 1 4 i	onthe-HortP * Static Password * Scan Code Rode * Challenge-Response *

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

ubico OTP	OATH-HOTP	Static Password	Challenge-Response	Settings	Tools	About	Exit	
							No YubiKey i	nserte
							•	
	The S	Swiss Army Kı	nife for the Yubik	ey				
Personal	ize your YubiKey	in:					Firmware Vers N/A	ion:
🔶 🍝 🖄	ubico OTP Mode							
- 🔶 🧕	ATH-HOTP Mode						Serial Numbe	,r
	tatic Password Mo	de					Hext N/A	
🔶 s	hallenge-Respons	e Mode					Modhex::N/A	
3f you hav	e any questions or r	suggestions, please send	f an amail to <u>Support@vubi</u>	20.00M			Features Sup Yubica OTP 2 Configuration	iporte
			Application Merce	ine: 101			OATH-HOTP	
			Build Timestam	p: Jul 6 2011 :	10:28:59		Scan Code Nod	e pase
Copyright	© 2011 Yubico. All f	Rights Reserved.						0130
							yubi	ic

- 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

YubiKey Personalization Tool							
Yubico OTP OATH-HOTP	Static Password	Challenge-Response	8ettings	Tools	About	Exit	
Yubico OTP OATH-HOTP Yubico OTP OATH-HOTP Prog Allows you to program one or mo Allows you to program one or mo	Static Password ram in Challer are Yubikeys in "Yubico C	Challenge-Response mo TP* Challenge-Response mod	Bettings de	Tools	About	Exit TubiKey is inse TubiKey is inse United States 2:2:9 Serial Number Dec: 1234 Hex: 04d2	rted
						Peatures Suppo Yubico OTP 2 Configurations OATH-HOTP Static Password Scan Code Mode Challenge-Respon	set ed

- 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:

YubiKey Personalization Tool						
Yubico OTP OATH-HOTP Static Passwork	Challenge-Response	Settings	Tools	About	Exit	
Program in Challenge-R	esponse mode - Y	ubico OT	Р		YubiKey is insert	ed
Select the configuration slot to be programmed Configuration Slot 1 Configuration	Slot 2	n (6 hatas li		0		
Automatically program WithKeys when inserted	VishiCarda) unprotected a	un (o urples m	см)			
Parameter Generation Scheme	Current Access Code	Comp is clinit inte	•1	-	2.2.9	
Increment Identities; Randomize Secret	New Access Code				Could block on	
Increment Identities; Randomize Secret Randomize all parameters					Serval Number	
Require user input (button press)					Hex: 04d2	ň
Private Identity (6 bytes Hex) 00 00 00 00 00	00		Generate) õ	Nodhex: cftd	ŏ
Secret Key (16 bytes Hex) d9 of 49 cb 60 5	f bb 32 9d a3 ef 5b bc 07 29 96		Senerate			
Actions					Features Support	ed
Press Write Configuration button to program your YubiO	y's selected configuration slot				Yubico OTP 2 Coofigurations	1
Write Configuration Stop R	eset Back				OATH-HOTP	4
					Static Password	1
Results					Scan Code Node	1
# Status Timestamp				_	Challenge-Response	1
				2	vubic	0
					the key to the close	d

- 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:

2)

YubiKey Personalization Tool					
Yubico OTP OATH-HOTP Static Password	Challenge-Response	Settings	Tools Ab	out Exit	
Program in Challenge-R	esponse mode - Y	ubico OTI	P	YubiK	ry is inserted
O Configuration Slot 1 O Configuration					
Program Hultiple Tubiceys Automatically program YubiKeys when inserted Parameter Generation Scheme Increment Identities; Randomize Secret	*) U	Firmware Version: 2.2.9			
Yubico OTP Parameters Require user input (button press) Private Identity (6 bytes Hex) 00 00 00 00 00 00 Sepert Key (16 bytes Hex) d9 et 49 ob 60 5	0		enerate 0	Dec: Hexi Modhexi	1234 🗋 04d2 🗋 oftd 🗋
Actions Press Write Configuration button to program your Yubike Write Configuration Stop Re Results Status Timestamp	r's selected configuration slot set Back			Featurn Yubico O 2 Configi OATH-HC Static Pa Scan Co Challeng	es Supported TP & urations & UTP & soword & de Mode & e-Response &
			R	yu	bico

- 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



10) From the "Actions", click on the "Write Configuration" button to configure the YubiKey in standard Yubico OTP challenge response mode.

PubiKey Personalization Tool							
Yubico OTP OATH-HOTP St	atic Password	Challenge-Response	Settings	Tools	About	Exit	
VubiKey1 has been successfully co Program in Ch	YubiKey is insert	ed					
Select the configuration slot to be progr Configuration Slot 1	rammed O Configuration SI	lot 2					
Program Multiple YubiKeys		Configuration Protectio	n (6 bytes H	ex)	0		
 Automatically program YubiKeys who 	en inserted	YubiKey(s) unprotected - I	Geep it that w	iy.	~	Firmware Version:	
Parameter Generation Scheme	0	Current Access Code				2.2.9	
Increment Identities; Randomize Secre	st 🗠	New Access Code				Serial Number	
Yubico OTP Parameters Require user input (button press) Private Identity (6 bytes Hex) Secret Key (16 bytes Hex)	00 00 00 00 00 00 00 d9 ef 49 cb 60 Sf b	b 32 9d a3 ef 5b bc 07 29 96		Generate Generate	0000	Dec: 1234 Hex: 04d2 Modhex: cftd	0 0
Actions						Features Support	ed]
Press Write Configuration button to pro Write Configuration	pram your YubiKey's itop Res	selected configuration slot et Back				Yubico OTP 2 Configurations OATH-HOTP Static Password	* * * *
Results						Scan Code Node	1
 Status 1 YubiKey has been successful: 	Ti y configured 7/22/20	mestamp 311 4:44:51 PM			<	Challenge-Response	*
						yubic the key to the close	0

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:

1) Start the YubiKey Personalization Tool



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

0	YubiKey Per	sonalization Tool							
┝	Yubico OTP	OATH-HOTP	Static Password	Challenge-Response	Settings	Tools	About	Exit	
								YubiKey is	inserted
								Ċ	
		The S	Swiss Army Ki	nife for the Yubik	(ey				
	Person	alize your YubiKey	in:					Firmware Ver 2.2.9	rsion:
	-	Yubice OTP Mode						- Secial Numb	
	-	OATH-HOTP Mode						Due: 1234	0
	-	Static Password Mo	<u>de</u>					Hez: D4d2	
	>	Challenge-Respons	e Mode					Modhex: cftd	ŏ
	If you h	ave any questions or :	suggestions, please send	l an email to <u>support@yubi</u>	<u>mo. com</u>			Features Su	pported
								Yubico OTP	*
								2 Configuratio OATH-HOTP	ns 🗸
				Application Vers	sion: 3.0.1			Static Passwor	nd 🛷
				Build Timestam	p: Jul 6 2011	10:28:59		Scan Code No Challenge-Res	de 🗸
	Copyrig	ht © 2011 Yubico. All I	Rights Reserved.						
								yub	ico

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



0	YubiKey Perso	nalization Tool								
Γ	Yubico OTP	OATH-HOTP	Static Password	Challenge-Response	Settings	Tools	About	Exit		
		Prog	ram in Challer	nge-Response mo	de			YubiKe	ey is insert	ed
	Yubice Allows you to	OTP 🛛 😧 program one or mo	ire YubiKeys in "Yubico O	TP" Challenge-Response mod	•				○ [III]	
	HMAC-S Allows you to	HA1 🛛 😝	re YubiKeys in "HMAC-S	HA1" Challenge-Response mo	de			Firmwar 2.2.9	e Version:	
L								-Serial P	Number	
L								Dec:	1234	۵
								Hex: Nother:	04d2 cftd	0
								Feature	es Support	ed
L								Yubica O 2 Config	TP urations	1
L								OATH-HO	TP .	*
								Static Pa Scan Coo Challeng	e-Response	1
								yu	bic y to the clo	0

- 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":

YubiKey Personalization Tool						
Yubico OTP OATH-HOTP Static Password	Challenge-Response	Settings	Tools	About	Exit	
Program in Challenge-Res	ponse mode - HN	IAC-SHA	1		YubiKey is insert	ted
Configuration Slot Select the configuration slot to be programmed O Configuration Slot 1 O Configuration Slot	at 2					
Program Hultiple YubiKeys	Configuration Protectio	n (6 bytes H	ex)			
Automatically program YubiKeys when inserted	YubiKey(s) unprotected - I	Keep it that wa	ah.	~	Firmware Version:	
Parameter Generation Scheme	Current Access Code			-11	2.2.9	
Randomize Secret	New Access Code				Serial Number	
HMAC-SHAI Parameters Require user input (button press) HMAC-SHAI Mode Start Hord (button press) HMAC-SHAI Mode Start Hord (button press) HMAC-SHAI Parameters Start Hord (button press) HMAC-SHAI Parameters HMAC-SHAI Paramete	O Fixed 64 byte input			•	Dec: 1234 Hex: 04d2 Modhex: cftd	0 0 0
2ecuer Keil (2n piles Hex) 5/ 8L 00 33 08 eD 5/	r ed 82 56 d4 52 ef 98 70 e2 8	12 15 43	senerate		- Features Support	ed -
Actions Press Write Configuration button to program your 'YubiKey's Write Configuration Stop Reso Results	selected configuration slot. et Back			8	Yubico OTP 2 Configurations OATH-HOTP Static Password Scan Code Node Challenge-Response	

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:

🗵 YubiKey Personi	elization Tool							
Yubico OTP	ОАТН-НОТР	Static Password	Challenge-Response	Settings	Tools	About	Exit	
Pr	ogram in C	Challenge-Res	ponse mode - HM	IAC-SH	1		YubiKey is inse	rted
Configuration Si Select the configu O Configuration :	lot ration slot to be pr Slot 1 tiple YubiKeys	rogrammed O Configuration SI	ot 2 Configuration Protectio	n (6 bytes H	ен)	0		
Automatically : Parameter Genery Randomize Secre	program YubiKeys «tion Scheme rt	when inserted	YubiKey(s) unprotected - YubiKey(s) unprotected - YubiKey(s) unprotected - Di YubiKey(s) protected - Ke YubiKey(s) protected - Ch	Keep it that we keep it that we Enable protects sable protectio ep it that way ange access o	ey ion n ode		Firmware Version 2.2.9 Serial Number	•
HMAC-SHA1 Par Require user in HMAC-SHA1 Mode Secret Key (20 by	ameters nput (button press) (tes Hex)) • Variable input • 7 5f ed 33 e8 4b 21	O Fixed 64 byte input 7 ed 82 56 d4 52 ef 9a 70 e2 :	82 f5 43	Generate	9] 0	Dec: 1234 Hex: 04d2 Nodhex: cftd	0 0 0
Actions Press Write Config Write Config Results # Status	guration button to ; guration	program your YubiKey's Stop Res	selected configuration slot et Back				Peatures Suppor Yubico OTP 2 Configurations OATH-HOTP Static Password Scan Code Node Challenge-Respons	rted
						×	yubic	CO

- 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.

YubiKey Personalization Tool				
Yubico OTP OATH-HOTP Static Password	Challenge-Response	8ettings	Tools About	Exit
✓ YubiKey1 has been successfully configured. Please re Program in Challenge-Res	YubiKey is inserted			
Configuration Slot Select the configuration slot to be programmed Configuration Slot Configuration Slot	* 2			
Program Hultiple YubiKeys	Configuration Protectio	n (6 bytes Hex	0 😶	_
Automatically program YubiKeys when inserted Parameter Generation Scheme Randomize Secret		Firmware Version: 2.2.9		
				Serial Number
HMAC-SHA1 Parameters C Require user input (button press) HMAC-SHA1 Mode O Variable input	Fixed 64 byte input			Dec: 1234 🗍 Hexi 04d2 📋 Modhexi oftd 📋
PL 01 00 03 00 40 27	e0 82 86 04 82 ef 98 70 e2 1	92 F9 43	merate o	- Features Supported
Actions Press Write Configuration button to program your Yub Key's Write Configuration Stop Results # Status 1 Yub Key has been successfully configured 7/22/20	selected configuration slot t Back mestamp 11 5:02:30 PM			Yubico OTP V 2 Configurations V OATH-HOTP V Static Password V Scain Cade Node V Challenge-Response V
			×	yubico

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