

# How to Rewrite YubiKey AES Information?

For YubiOn Windows Logon Standalone

2022/7/21



## Copyright ©2022 SoftGiken Co. Ltd. All rights reserved.

## **Contact Information**

SoftGiken Co. Ltd.

Sakuragaokacho 4-23 Shibuyasakuraoka Building 6F Shibuya, Tokyo 150-0031 <sub>Japan</sub>

presales@yubion.com

## **Table of Contents**

Copyright	2
Contact Information	2
1. Overview	.4
2. How to Rewrite YubiKey Secret Key Information?	. 5
2.1. Using YubiKey Personalization Tool	5
2.1.1. Prerequisites	5
2.1.2. Steps	5
2.2. Using YubiKey Manager	8
2.2.1. Prerequisites	8
2.2.2. Steps	8

## 1. Overview

YubiOn Windows Logon Standalone authentication requires YubiKey secret key information. Based on it, we will create a license file and hand it to the customer. Then the customer will import the license file into YubiOn Windows Logon Standalone software to enable using YubiKey.

As a factory default, the YubiKey secret key information is not revealed, so to get this information, we have to use a tool to rewrite the YubiKey secret key information.

For users in Japan, we sell YubiKey, which has been rewritten the secret key information, but for foreign users who we cannot send YubiKey, customers have to rewrite their YubiKeys by themselves.

**NOTE:** After rewriting, the YubiKey factory default secret key information will be deleted, and you will not be able to use that key with others services using the default Yubico OTP. So make sure to use the YubiKey which does not have any problems even if you rewrite it.

#### The introduction process is as below:

### Rewrite the symmetric-key information of Yubico OTP 🏼 🌽 softgiken



The necessary information in the CSV file includes "Serial No.", "Public ID", "Private ID", "Secret key".

% The secret key is important information used for authentication. Please handle it carefully so that you do not leak it to third parties.

e.g.)

This document describes how to rewrite the YubiKey secret key information.

## 2. How to Rewrite YubiKey Secret Key Information?

There are 2 ways to rewrite YubiKey secret information: using "YubiKey Personalization Tool" or using "YubiKey Manager".

### 2.1. Using YubiKey Personalization Tool

### 2.1.1. Prerequisites

Download and install "YubiKey Personalization Tool" from the Yubico homepage.

https://www.yubico.com/support/download/yubikey-personalization-tools/

#### 2.1.2. Steps

- 1 Open the "YubiKey Personalization Tool" application. Plug in the YubiKey you want to rewrite to the USB port.
- 2 Set the format:

Select the "Settings" tab.

Change the "Logging Settings" to "Yubico format".

🛞 YubiKey Personalization Tool				_		×	
Yubico OTP OATH-HOTP Static Password	Challenge-Response	Settings	Tools	About	Exit		
Setti	ngs				YubiKey i	s inserte	d
General Settings     Decimal     Mo       Use and enforce customer prefix     Image: Control of the set of the	dHex Hex						
Output Settings Output Format Tab Public ID Tab OTP Tab	Enter			0			
Output Speed Throttling       Output Character Rate       Standard       Add a short delay before sending OTP part	Add a short delay aft	er sending OTP	part	0	Programmi Slot 1 and 2 Firmware V 5.1.2 Serial Nur	ng status configured <b>'ersion:</b> nber	e 1
Serial # Visibility Settings	Static Password Setting	<b>gs</b> te using the but	ton (2.0+)	0	Dec: 101 Hex: 9ac	.45512   xee8	
Update Settings     Image: Control of the setting se	Extended Settings	for digits (2.3+ only slot 1 is pr	) rogrammed	(2.3+)	Features : Yubico OTP 2 Configurat	Supported	d ~
Logging Settings          Log configuration output         Application Settings		(2.4+/3.1+)		0	OATH-HOTP Static Passw Scan Code I Challenge-R Updatable	ord Mode esponse	* * * * *
Enable configuration export [Flexible format nta]) Actions Settings are saved automatically	Update is available	for YubiKey 2.3	and later			d Factor	<u>،</u>
Restore Defaults	U	pdate Setting	s		yur		

3 Rewrite the secret information: Select the "Yubico OTP" tab. Click the "Advanced" button.

🛞 YubiKe	y Personaliz	ation Tool				_		>	<
Yubico OTP	ОАТН-НОТР	Static Password	Challenge-Response	Settings	Tools	About	Exit		
		Program in Yu	ibico OTP mode				YubiKey	/ is inser	ted
Quick Quickly progra	am a YubiKey for u	se with Yubico Validation	Server						
Advance Allows you to	d program one or me	ore YubiKeys with greater	r control over the configuration	n values			Programm Slot 1 and Firmware 5.1.2 Serial Nu Dec: 11 Hex: 9 Modhex: kl Feature: Yubico OTI 2 Configur OATH-HOT Static Pass Scan Code Challenge Updatable Ndef Universal	ning stat 2 configur Version: umber 0145512 acee8 Iruuj s Support P rations rP sword a Mode -Response	us: ed
							yu	bic	:0

Select the slot to rewrite. Slot 1 works with a short touch and Slot 2 works with a long touch. Click the 3 "Generate" buttons in the "Yubico OTP Parameters" part to generate key information. Click the "Write Configuration" button to execute the rewrite.

🛞 YubiKey Personalization Tool				_		X	
Yubico OTP OATH-HOTP Static Password	Challenge-Response	Settings	Tools	About	Exit		
Program in Yubico C	)TP mode - Advar	nced			YubiKey is inse	rted	
Configuration Slot							
Select the configuration slot to be programmed Configuration Slot 1 Configuration	Slot 2			•			
Program Multiple YubiKeys	Configuration Protection	on (6 bytes H	ex)	0			
Automatically program YubiKeys when inserted	YubiKey(s) unprotected -	Keep it that wa	зу	•			
Parameter Generation Scheme	Current Access Code				Programming status: Slot 1 and 2 configured		
Identity from serial; Randomize Secrets	New Access Code				Firmware Version		
Yubico OTP Parameters	Use Serial Number	_			5.1.2 Serial Number		
Public Identity (1-16 bytes Modhe> iu vg ru ul dv vv			Generate	•	Dec: 10145512		
Public Identity Length 6 文 (6 bytes is	default length as required by	Yubico OTP va	lidation ser	ver)	Hex: 9acee8		
Private Identity (6 bytes Hex) 68 be da 75 41 91			Generate	2	Modhex: klruuj		
Secret Key (16 bytes Hex) ec 0a f7 66 2d 4b	b2 bb 06 9f 1c ae 20 07 d5 c2		Generate	2	Features Support	rted	
Actions					Yubico OTP	1	
Press Write Configuration button to program your YubiKey	's selected configuration slot				2 Configurations	4	
Write Configuration Stop Res	et Back				Static Password		
White configuration Stop Res	Duck				Scan Code Mode	1	
Results					Challenge-Respons	e 🗸	
# Public Identity (Modhex) Status Timesta	mp			~	Updatable	×	
					Ndet	- 4	
						n . v _	
				~	yubio	CO	

When rewriting, a window to specify the output destination of the CSV file is displayed. Save the CSV file in any directory.

The default is saved under the file name "configuration\_log.csv".

- 4 If there are multiple YubiKeys, plug in the next YubiKey and repeat the secret key information rewriting procedure.
- % The second and subsequent rewriting information will be added to the first specified CSV file. e.g.)

Make sure that all YubiKey secret key information is entered in the above CSV file, and send the file to us.

### 2.2. Using YubiKey Manager

### 2.2.1. Prerequisites

Download and install "YubiKey Manager" from the Yubico homepage.

https://www.yubico.com/support/download/yubikey-manager/

### 2.2.2. Steps

1 Open the "YubiKey Manager" application. Plug in the YubiKey you want to rewrite to the USB port. The information of YubiKey will be displayed. Write down the value of "Serial".

🐠 YubiKey Manager	- 🗆	$\times$
	Help	O About
yubico Home Applications Interfaces		
YubiKey 5 NFC		
Firmware: 5.1.2 Serial:	C	

2 Click the "Application" tab, and select "OTP".



3 Click the "Configure" button under the slot you want to set.

🚳 YubiKey Manager	_		×
	YubiKey 5 NFC ( )	Help	About
yubico Home Applications Interfaces			
Here / OTP Here / OTP			
< Back			

4 Choose "Yubico OTP" and click the "Next" button.

🛞 YubiKey Manager	_		×
	YubiKey 5 NFC ( )	Help	③ About
yubico Home Applications Interfaces			
Select Credential Type Home / OTP / Short Touch (Slot 1)			
Yubico OTP     O Challenge-response			
○ Static password ○ OATH-HOTP			
< Back			Vext >

5 Check "Use Serial" of "Public ID".
Click the "Generate" button of "Private ID".
Click the "Generate" button of the "Secret key".
Write down the values of "Public ID", "Private ID", and "Secret key".
Click the "Finish" button to execute the rewrite.

💇 YubiKey Manager	_		×
	YubiKey 5 NFC )	Help	About
yubico Home Applications Interfaces			
Yubico OTP Home / OTP / Short Touch (Slot 1) / Yubico OTP			
Public ID		Use	e serial
Private ID		Gene	erate
< Back			Finish

- 6 If there are multiple YubiKeys, plug in the next YubiKey and repeat the secret key information rewriting procedure.
- 7 Create the secret key file:

Finally, create a CSV file for all YubiKey secret key information and send it to us. The file format: "Serial No.", "Public ID", "Private ID", "Secret key"

e.g.)

•••