YubiKey Token Reprogramming

Generating YubiKey Device CSV for MyID MFA

Call us on:	+44 (0)1455 558 111 (UK & EMEA) +1 408 706 2866 (US)
Email us:	info@intercede.com

Intercede Ltd, Lutterworth Hall, St. Mary's Road, Lutterworth, Leicestershire, LE17 4PS, United Kingdom
UK Tel: +44 (0)1455 558 111   US Tel: +1 888 646 6943   email: info@intercede.com   web: www.intercede.com

Introduction

Note

MyID MFA and MyID PSM were previously known as Authlogics products. Authlogics is now an Intercede Group company and the products have been rebranded accordingly.

The term 'Authlogics' may still appear in certain areas of the product.

This document describes the process for configuring your YubiKey device so that it can be used to authenticate YubiKey generated One Time PIN (OTP) locally and not require access to the internet-based YubiKey servers for validation.

Consideration

MyID Multi-Factor Authentication version 4 and above needs to be installed, configured and fully operationally. Furthermore, users issued with YubiKey devices will need be provisioned to MyID PINpass prior to customising and provisioning YubiKeys for local MyID server validation.

YubiKey Personalisation

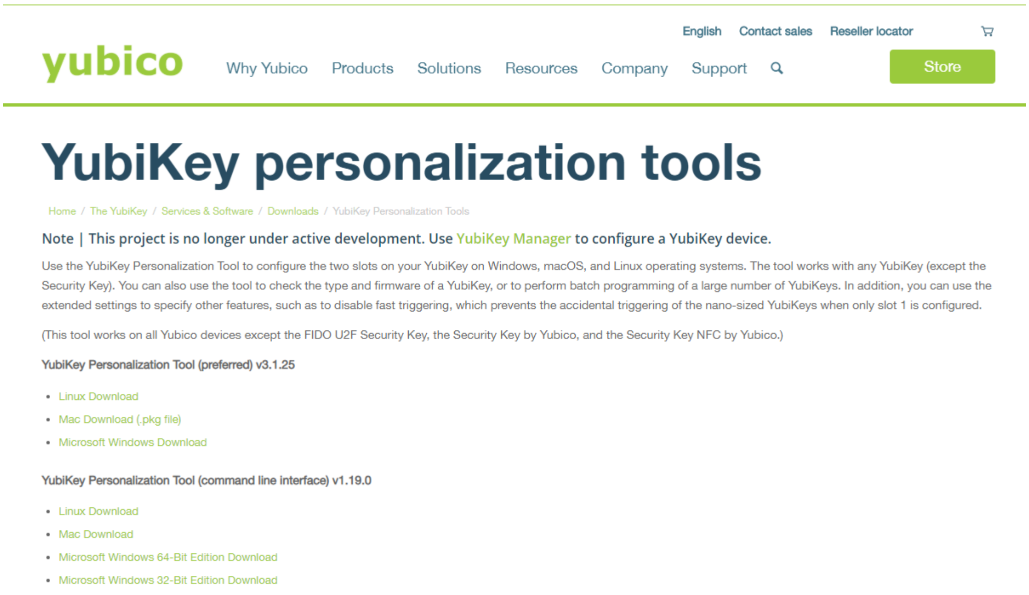
Intercede introduced the ability to locally process YubiKey generated one-time codes in Multi-Factor Authentication solution version 4. Before YubiKeys can be used locally and no longer be validated using the YubiKey published servers over the internet, the devices will need to be customised and configured for MyID use.

The process defined below will generate a Comma Separated Value (CSV) file which will need to be imported into MyID MFA.

If the YubiKey is not customised as per the instructions below, YubiKey OTPs will still be sent to YubiKey hosted servers on the Internet and no local server processing will occur. As such, outbound Internet access to the YubiKey servers will be required from the MyID Authentication servers will be required.

Configuring YubiKey Devices

Customisation is performed through the YubiKey Personalization Tool. We recommend using the Graphical User Interface version and not the command-line tool. This tool can be downloaded from https://www.yubico.com/products/services-software/download/yubikey-personalization-tools/



YubiKey personalization tools

Home / The YubiKey / Services & Software / Downloads / YubiKey Personalization Tools

Note | This project is no longer under active development. Use YubiKey Manager to configure a YubiKey device.

Use the YubiKey Personalization Tool to configure the two slots on your YubiKey on Windows, macOS, and Linux operating systems. The tool works with any YubiKey (except the Security Key). You can also use the tool to check the type and firmware of a YubiKey, or to perform batch programming of a large number of YubiKeys. In addition, you can use the extended settings to specify other features, such as to disable fast triggering, which prevents the accidental triggering of the nano-sized YubiKeys when only slot 1 is configured.

(This tool works on all Yubico devices except the FIDO U2F Security Key, the Security Key by Yubico, and the Security Key NFC by Yubico.)

YubiKey Personalization Tool (preferred) v3.1.25

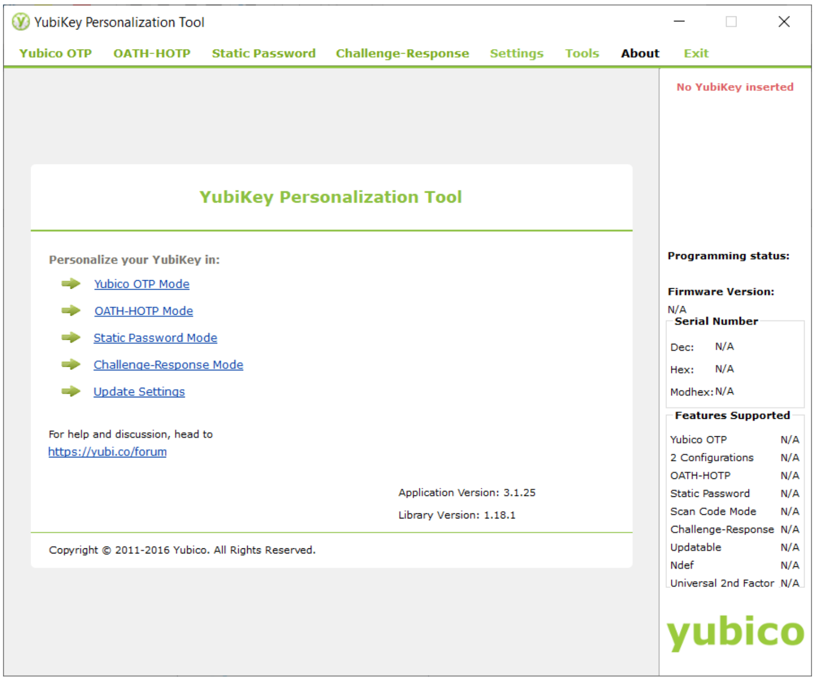
- Linux Download
- Mac Download (.pkg file)
- Microsoft Windows Download

YubiKey Personalization Tool (command line interface) v1.19.0

- Linux Download
- Mac Download
- Microsoft Windows 64-Bit Edition Download
- Microsoft Windows 32-Bit Edition Download

Once installed and executed, please follow the instructions to customise the YubiKey. To start, ensure that no YubiKey devices are inserted into the workstation.

(1) Start the YubiKey Personalization Tool and select **Yubico OTP Mode**.



No YubiKey inserted

YubiKey Personalization Tool

Personalize your YubiKey in:

- Yubico OTP Mode
- OATH-HOTP Mode
- Static Password Mode
- Challenge-Response Mode
- Update Settings

For help and discussion, head to https://yubi.co/forum

Application Version: 3.1.25

Library Version: 1.18.1

Copyright © 2011-2016 Yubico. All Rights Reserved.

Programming status:

Firmware Version:
N/A

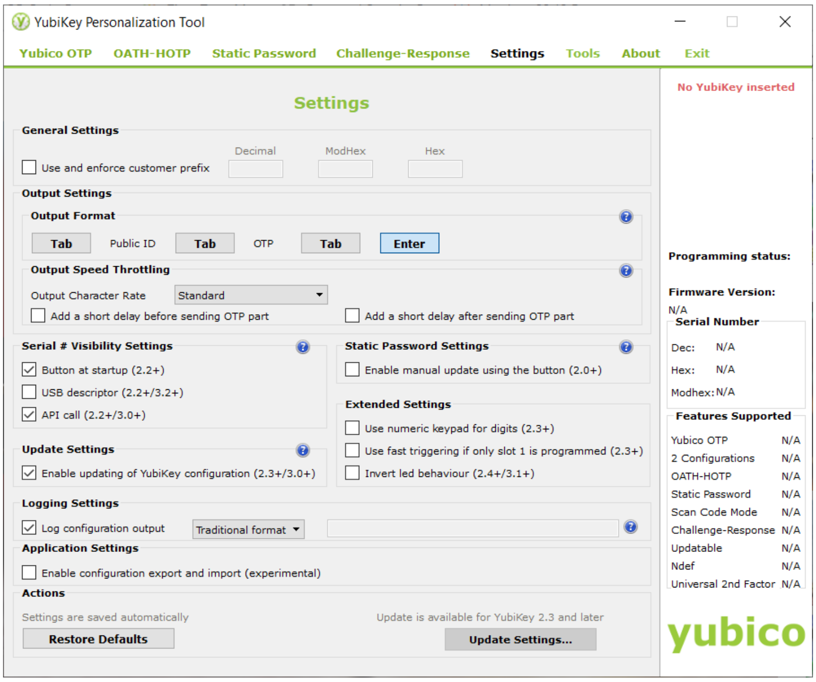
Serial Number

Dec:	N/A
Hex:	N/A
Modhex:	N/A

Features Supported

Yubico OTP	N/A
2 Configurations	N/A
OATH-HOTP	N/A
Static Password	N/A
Scan Code Mode	N/A
Challenge-Response	N/A
Updatable	N/A
Ndef	N/A
Universal 2nd Factor	N/A

(2) Select **Settings**



Settings

No YubiKey inserted

General Settings

	Decimal	ModHex	Hex
□ Use and enforce customer prefix			

Output Settings

Output Format

Output Speed Throttling

Output Character Rate: Standard

□ Add a short delay before sending OTP part

□ Add a short delay after sending OTP part

Serial # Visibility Settings

☑ Button at startup (2.2+)

□ USB descriptor (2.2+/3.2+)

☑ API call (2.2+/3.0+)

Static Password Settings

□ Enable manual update using the button (2.0+)

Extended Settings

□ Use numeric keypad for digits (2.3+)

□ Use fast triggering if only slot 1 is programmed (2.3+)

□ Invert led behaviour (2.4+/3.1+)

Update Settings

☑ Enable updating of YubiKey configuration (2.3+/3.0+)

Logging Settings

☑ Log configuration output: Traditional format

Application Settings

□ Enable configuration export and import (experimental)

Actions

Settings are saved automatically

Update is available for YubiKey 2.3 and later

Programming status:

Firmware Version:
N/A

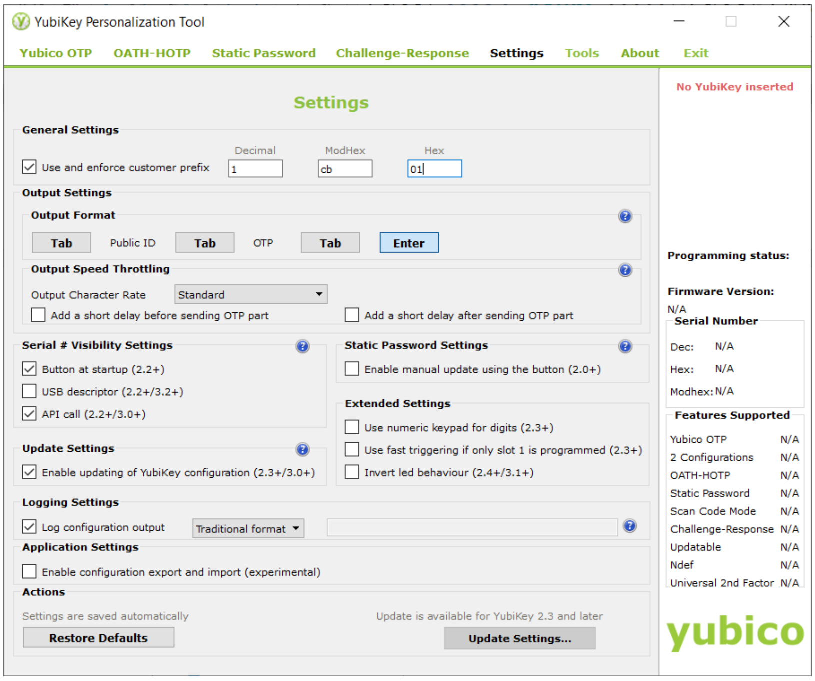
Serial Number

Dec: N/A
Hex: N/A
Modhex: N/A

Features Supported

Yubico OTP	N/A
2 Configurations	N/A
OATH-HOTP	N/A
Static Password	N/A
Scan Code Mode	N/A
Challenge-Response	N/A
Updatable	N/A
Ndef	N/A
Universal 2nd Factor	N/A

(3) In General Settings, enable **Use and enforce customer prefix** and specify a value between **01** and **FF** in the **HEX** field



Settings

No YubiKey inserted

General Settings

	Decimal	ModHex	Hex
☑ Use and enforce customer prefix	1	cb	01

Output Settings

Output Format

Output Speed Throttling

Output Character Rate: Standard

□ Add a short delay before sending OTP part

□ Add a short delay after sending OTP part

Serial # Visibility Settings

☑ Button at startup (2.2+)

□ USB descriptor (2.2+/3.2+)

☑ API call (2.2+/3.0+)

Static Password Settings

□ Enable manual update using the button (2.0+)

Extended Settings

□ Use numeric keypad for digits (2.3+)

□ Use fast triggering if only slot 1 is programmed (2.3+)

□ Invert led behaviour (2.4+/3.1+)

Update Settings

☑ Enable updating of YubiKey configuration (2.3+/3.0+)

Logging Settings

☑ Log configuration output: Traditional format

Application Settings

□ Enable configuration export and import (experimental)

Actions

Settings are saved automatically

Update is available for YubiKey 2.3 and later

Programming status:

Firmware Version:
N/A

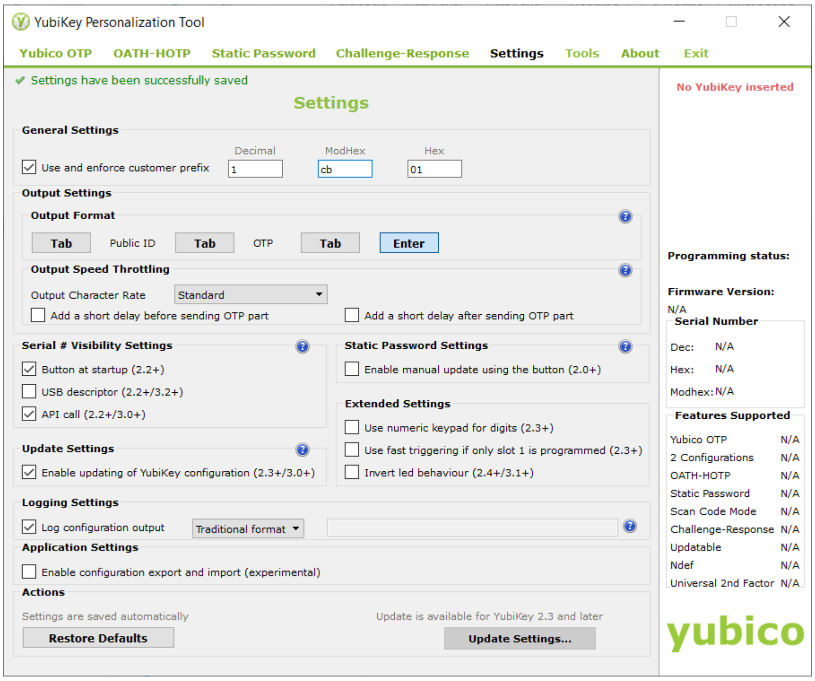
Serial Number

Dec: N/A
Hex: N/A
Modhex: N/A

Features Supported

Yubico OTP	N/A
2 Configurations	N/A
OATH-HOTP	N/A
Static Password	N/A
Scan Code Mode	N/A
Challenge-Response	N/A
Updatable	N/A
Ndef	N/A
Universal 2nd Factor	N/A

(4) Once a Hex has been added, click on the Decimal or ModHex fields for the settings to be saved. The message ***Settings has been successfully saved*** will be displayed in the top left corner.



✓ Settings have been successfully saved

Settings

General Settings

	Decimal	ModHex	Hex
☑ Use and enforce customer prefix	1	cb	01

Output Settings

Output Format: Tab, Public ID, Tab, OTP, Tab, Enter

Output Speed Throttling

Output Character Rate: Standard

☐ Add a short delay before sending OTP part
☐ Add a short delay after sending OTP part

Serial # Visibility Settings

☑ Button at startup (2.2+)
☐ USB descriptor (2.2+/3.2+)
☑ API call (2.2+/3.0+)

Static Password Settings

☐ Enable manual update using the button (2.0+)

Extended Settings

☐ Use numeric keypad for digits (2.3+)
☐ Use fast triggering if only slot 1 is programmed (2.3+)
☐ Invert led behaviour (2.4+/3.1+)

Update Settings

☑ Enable updating of YubiKey configuration (2.3+/3.0+)

Logging Settings

☑ Log configuration output: Traditional format

Application Settings

☐ Enable configuration export and import (experimental)

Actions

Settings are saved automatically

Update is available for YubiKey 2.3 and later

No YubiKey inserted

Programming status:

Firmware Version:
N/A

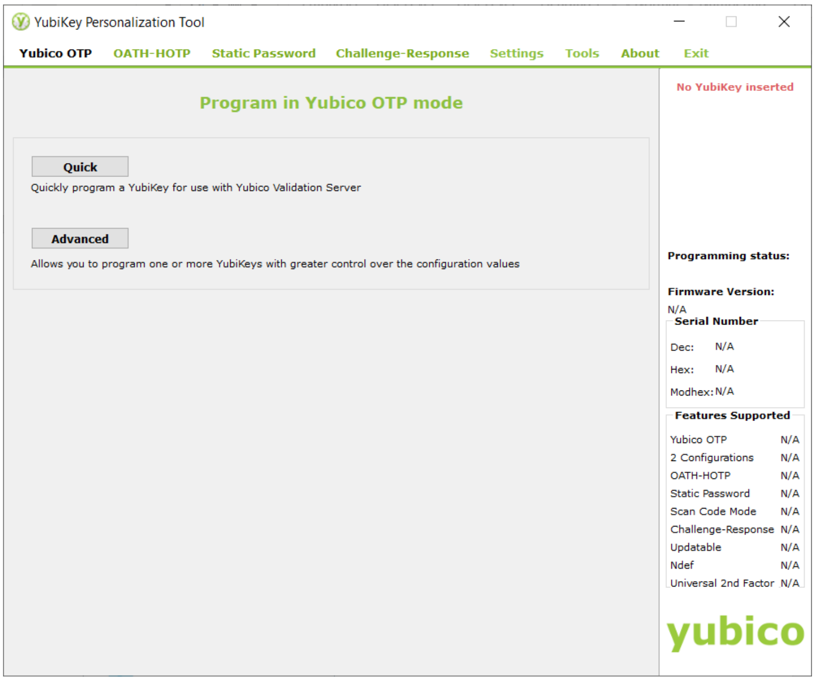
Serial Number

Dec:	N/A
Hex:	N/A
Modhex:	N/A

Features Supported

Yubico OTP	N/A
2 Configurations	N/A
OATH-HOTP	N/A
Static Password	N/A
Scan Code Mode	N/A
Challenge-Response	N/A
Updatable	N/A
Ndef	N/A
Universal 2nd Factor	N/A

(5) Select Yubico OTP



Program in Yubico OTP mode

Quick: Quickly 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

No YubiKey inserted

Programming status:

Firmware Version:
N/A

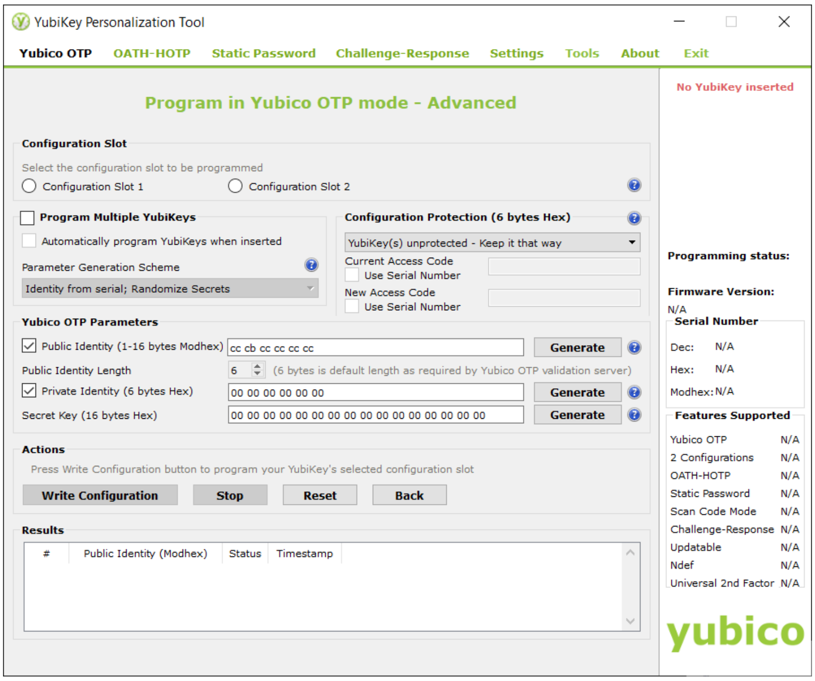
Serial Number

Dec:	N/A
Hex:	N/A
Modhex:	N/A

Features Supported

Yubico OTP	N/A
2 Configurations	N/A
OATH-HOTP	N/A
Static Password	N/A
Scan Code Mode	N/A
Challenge-Response	N/A
Updatable	N/A
Ndef	N/A
Universal 2nd Factor	N/A

(6) Select **Advanced**



No YubiKey inserted

Configuration Slot

Select the configuration slot to be programmed

○ Configuration Slot 1 ○ Configuration Slot 2

□ **Program Multiple YubiKeys**

□ Automatically program YubiKeys when inserted

Parameter Generation Scheme: Identity from serial; Randomize Secrets

Configuration Protection (6 bytes Hex): YubiKey(s) unprotected - Keep it that way

Current Access Code □ Use Serial Number

New Access Code □ Use Serial Number

Yubico OTP Parameters

☑ Public Identity (1-16 bytes Modhex): cc cb cc cc cc cc

Public Identity Length: 6 (6 bytes is default length as required by Yubico OTP validation server)

☑ Private Identity (6 bytes Hex): 00 00 00 00 00 00

Secret Key (16 bytes Hex): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Actions

Press Write Configuration button to program your YubiKey's selected configuration slot

Results

#	Public Identity (Modhex)	Status	Timestamp

Programming status:

Firmware Version: N/A

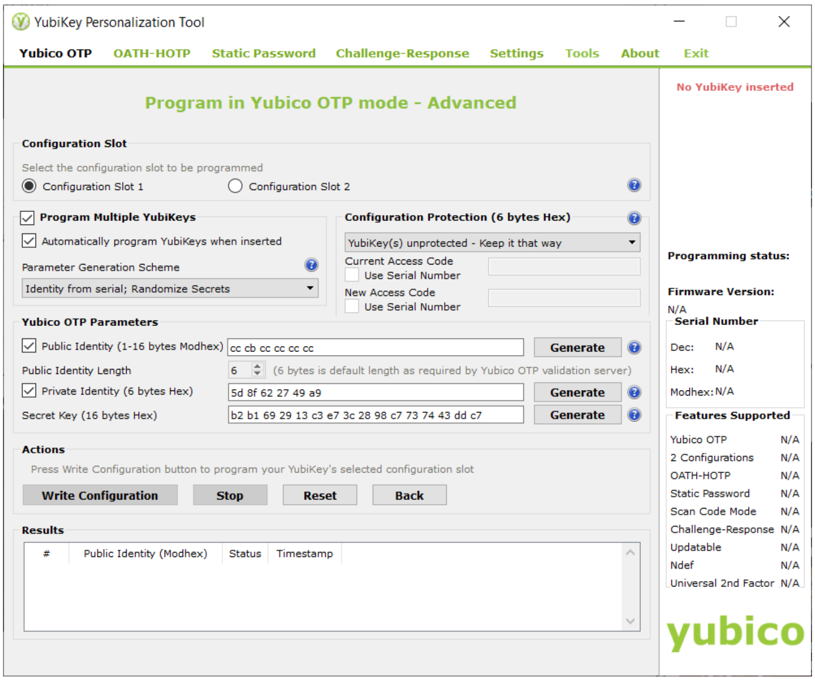
Serial Number

Dec:	N/A
Hex:	N/A
Modhex:	N/A

Features Supported

Yubico OTP	N/A
2 Configurations	N/A
OATH-HOTP	N/A
Static Password	N/A
Scan Code Mode	N/A
Challenge-Response	N/A
Updatable	N/A
Ndef	N/A
Universal 2nd Factor	N/A

(7) Select **Configuration Slot 1** to re-program the short press slot of your YubiKey device. Enable **Program Multiple YubiKeys** and **Automatically program Yubikeys when inserted**.



No YubiKey inserted

Configuration Slot

Select the configuration slot to be programmed

● Configuration Slot 1 ○ Configuration Slot 2

☑ **Program Multiple YubiKeys**

☑ Automatically program YubiKeys when inserted

Parameter Generation Scheme: Identity from serial; Randomize Secrets

Configuration Protection (6 bytes Hex): YubiKey(s) unprotected - Keep it that way

Current Access Code □ Use Serial Number

New Access Code □ Use Serial Number

Yubico OTP Parameters

☑ Public Identity (1-16 bytes Modhex): cc cb cc cc cc cc

Public Identity Length: 6 (6 bytes is default length as required by Yubico OTP validation server)

☑ Private Identity (6 bytes Hex): 5d 8f 62 27 49 a9

Secret Key (16 bytes Hex): b2 b1 69 29 13 c3 e7 3c 28 98 c7 73 74 43 dd c7

Actions

Press Write Configuration button to program your YubiKey's selected configuration slot

Results

#	Public Identity (Modhex)	Status	Timestamp

Programming status:

Firmware Version: N/A

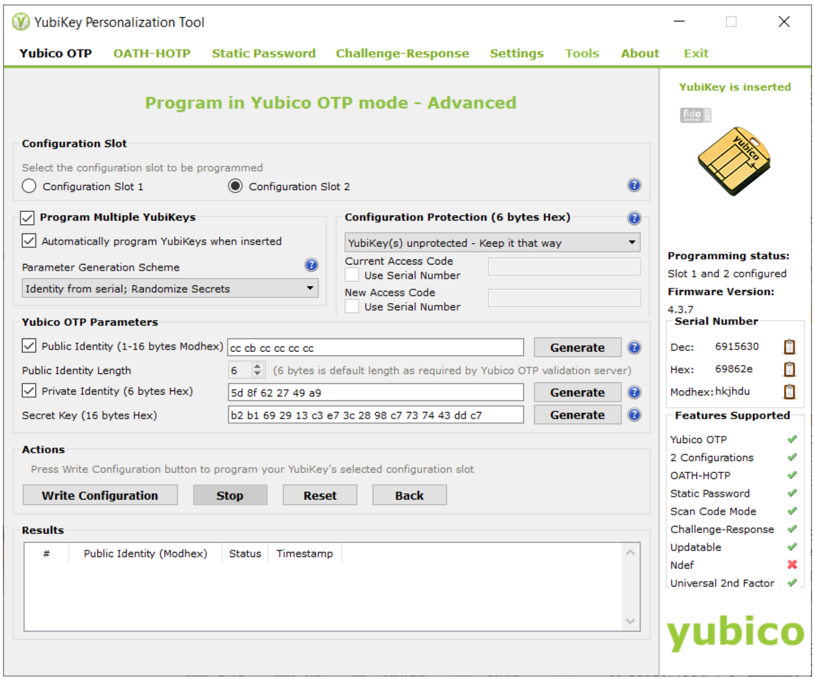
Serial Number

Dec:	N/A
Hex:	N/A
Modhex:	N/A

Features Supported

Yubico OTP	N/A
2 Configurations	N/A
OATH-HOTP	N/A
Static Password	N/A
Scan Code Mode	N/A
Challenge-Response	N/A
Updatable	N/A
Ndef	N/A
Universal 2nd Factor	N/A

(8) Insert your YubiKey device into the workstation and select **Write Configuration** under Actions.



Program in Yubico OTP mode - Advanced

Configuration Slot

Select the configuration slot to be programmed

○ Configuration Slot 1 ● Configuration Slot 2

☑ Program Multiple YubiKeys

☑ Automatically program YubiKeys when inserted

Parameter Generation Scheme: Identity from serial; Randomize Secrets

Configuration Protection (6 bytes Hex): YubiKey(s) unprotected - Keep it that way

Current Access Code □ Use Serial Number

New Access Code □ Use Serial Number

Yubico OTP Parameters

☑ Public Identity (1-16 bytes Modhex): cc cb cc cc cc cc

Public Identity Length: 6 (6 bytes is default length as required by Yubico OTP validation server)

☑ Private Identity (6 bytes Hex): 5d 8f 62 27 49 a9

Secret Key (16 bytes Hex): b2 b1 69 29 13 c3 e7 3c 28 98 c7 73 74 43 dd c7

Actions

Press Write Configuration button to program your YubiKey's selected configuration slot

Results

#	Public Identity (Modhex)	Status	Timestamp

YubiKey is inserted

Programming status: Slot 1 and 2 configured

Firmware Version: 4.3.7

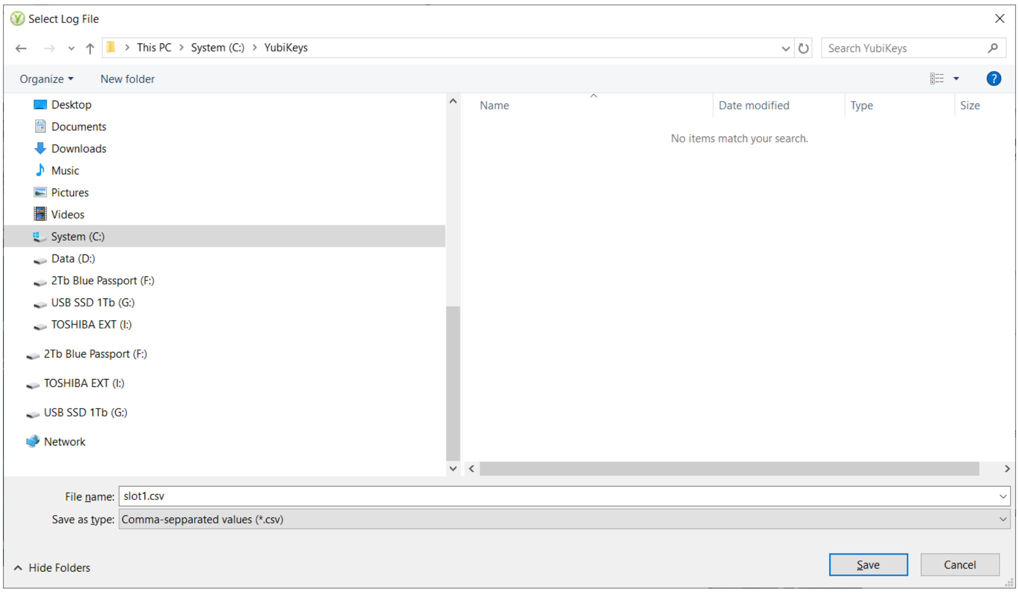
Serial Number

Dec:	6915630
Hex:	69862e
Modhex:	hkjhdu

Features Supported

Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✓
Ndef	✗
Universal 2nd Factor	✓

When Write Configuration is selected, a CSV file (slot1.csv) will be created and saved in a folder that you select.

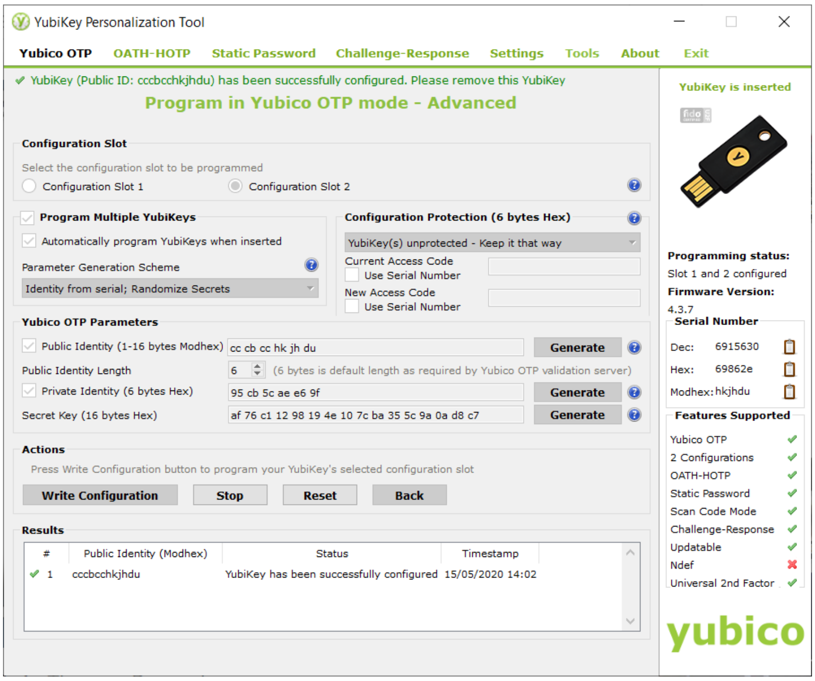


No items match your search.

File name: slot1.csv

Save as type: Comma-sepparated values (*.csv)

The **Results** field will reflect the changes to the YubiKey device.



✓ YubiKey (Public ID: cccbcchkjhdu) has been successfully configured. Please remove this YubiKey

Program in Yubico OTP mode - Advanced

Configuration Slot

Select the configuration slot to be programmed

○ Configuration Slot 1 ● Configuration Slot 2

☑ **Program Multiple YubiKeys**

☑ Automatically program YubiKeys when inserted

Parameter Generation Scheme: Identity from serial; Randomize Secrets

Configuration Protection (6 bytes Hex): YubiKey(s) unprotected - Keep it that way

Current Access Code ☐ Use Serial Number

New Access Code ☐ Use Serial Number

Yubico OTP Parameters

☑ Public Identity (1-16 bytes Modhex): cc cb cc hk jh du

Public Identity Length: 6 (6 bytes is default length as required by Yubico OTP validation server)

☑ Private Identity (6 bytes Hex): 95 cb 5c ae e6 9f

Secret Key (16 bytes Hex): af 76 c1 12 98 19 4e 10 7c ba 35 5c 9a 0a d8 c7

Actions

Press Write Configuration button to program your YubiKey's selected configuration slot

Results

#	Public Identity (Modhex)	Status	Timestamp
✓ 1	cccbcchkjhdu	YubiKey has been successfully configured	15/05/2020 14:02

YubiKey is inserted

Programming status: Slot 1 and 2 configured

Firmware Version: 4.3.7

Serial Number

Dec: 6915630

Hex: 69862e

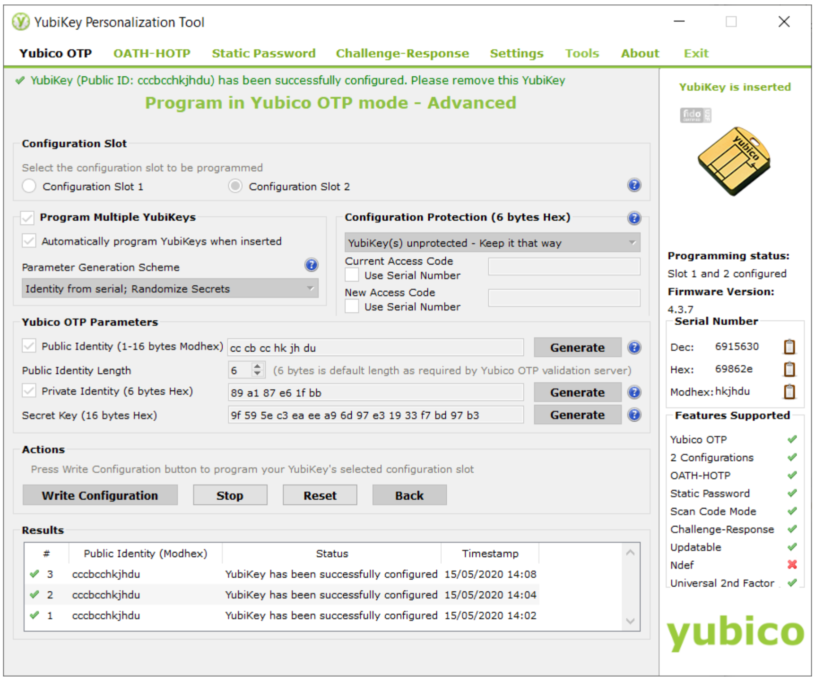
Modhex: hkjhdu

Features Supported

Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✓
Ndef	✗
Universal 2nd Factor	✓

(9) Remove your YubiKey device and insert the next device. Each device inserted will be reprogrammed with the details written to the CSV file selected in Step 8.

All new devices inserted will be listed in the Results pane.



✓ YubiKey (Public ID: cccbcchkjhdu) has been successfully configured. Please remove this YubiKey

Program in Yubico OTP mode - Advanced

Configuration Slot

Select the configuration slot to be programmed

○ Configuration Slot 1 ● Configuration Slot 2

☑ **Program Multiple YubiKeys**

☑ Automatically program YubiKeys when inserted

Parameter Generation Scheme: Identity from serial; Randomize Secrets

Configuration Protection (6 bytes Hex): YubiKey(s) unprotected - Keep it that way

Current Access Code ☐ Use Serial Number

New Access Code ☐ Use Serial Number

Yubico OTP Parameters

☑ Public Identity (1-16 bytes Modhex): cc cb cc hk jh du

Public Identity Length: 6 (6 bytes is default length as required by Yubico OTP validation server)

☑ Private Identity (6 bytes Hex): 89 a1 87 e6 1f bb

Secret Key (16 bytes Hex): 9f 59 5e c3 ea ee a9 6d 97 e3 19 33 f7 bd 97 b3

Actions

Press Write Configuration button to program your YubiKey's selected configuration slot

Results

#	Public Identity (Modhex)	Status	Timestamp
✓ 3	cccbcchkjhdu	YubiKey has been successfully configured	15/05/2020 14:08
✓ 2	cccbcchkjhdu	YubiKey has been successfully configured	15/05/2020 14:04
✓ 1	cccbcchkjhdu	YubiKey has been successfully configured	15/05/2020 14:02

YubiKey is inserted

Programming status: Slot 1 and 2 configured

Firmware Version: 4.3.7

Serial Number

Dec: 6915630

Hex: 69862e

Modhex: hkjhdu

Features Supported

Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✓
Ndef	✗
Universal 2nd Factor	✓

All your devices will now have been reprogrammed and the CSV file is ready for importing into the MyID Authentication Server. Details for importing can be found in the Authentication Server Installation and Configuration Guide: https://authlogics.com/download/authentication-server-installation-and-configuration-guide