

PROGRAMMING YUBIKEYS IN OTP MODE FOR GREENRADIUS

1. INTRODUCTION

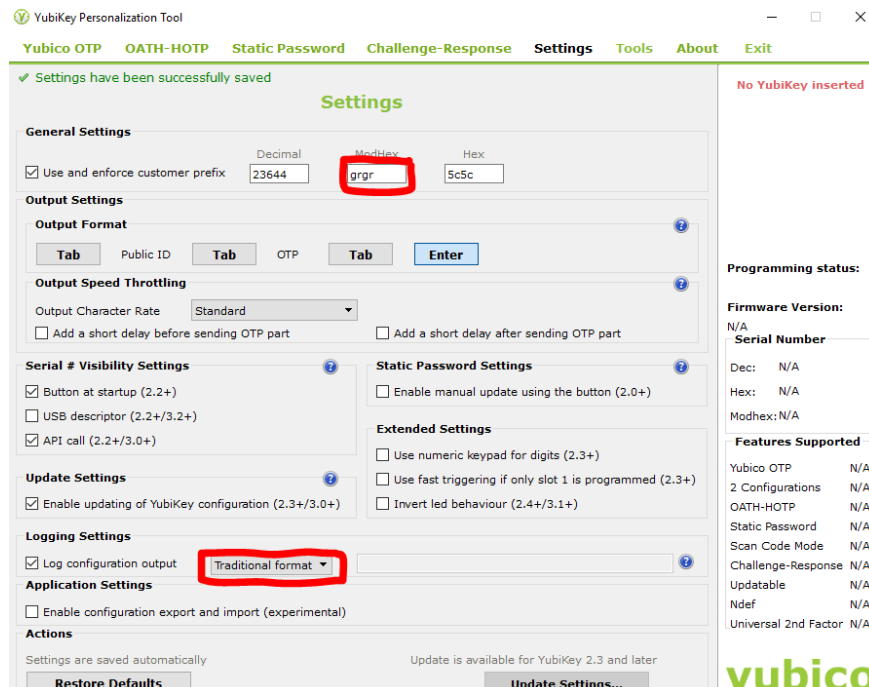
This document will show you how to program YubiKeys in OTP mode so secrets can be “local” in GreenRADIUS instead of using the default YubiKey secrets and using the YubiCloud

2. PREREQUISITES

- Have all YubiKeys that you want programmed with you
- Download and install the Yubico Personalization Tool v3.1.25 ([linked here](#))

3. PROGRAMMING THE YUBIKEYS

1. Open the Yubico Personalization Tool
2. Select the **Settings** menu
 - a. Check the “Use and enforce customer prefix” box, and enter “**grgr**” in the ModHex field.
 - b. select **Traditional format** under **Log configuration output**



Yubico Personalization Tool

Yubico OTP OATH-HOTP Static Password Challenge-Response **Settings** Tools About Exit

✓ Settings have been successfully saved

Settings

No YubiKey inserted

General Settings

Use and enforce customer prefix

Decimal: 23644 ModHex: **grgr** Hex: 5c5c

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

Restore Defaults Update Settings...

Programming status:

Firmware Version:

N/A

Serial Number

Dec: N/A

Hex: N/A

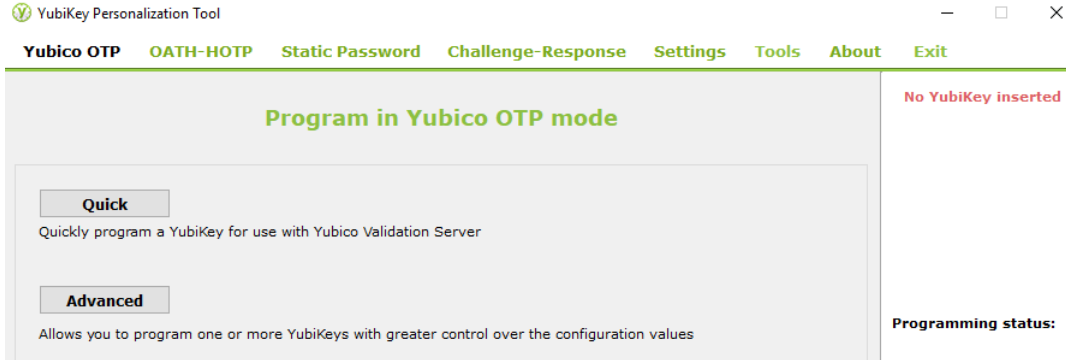
Modhex: N/A

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

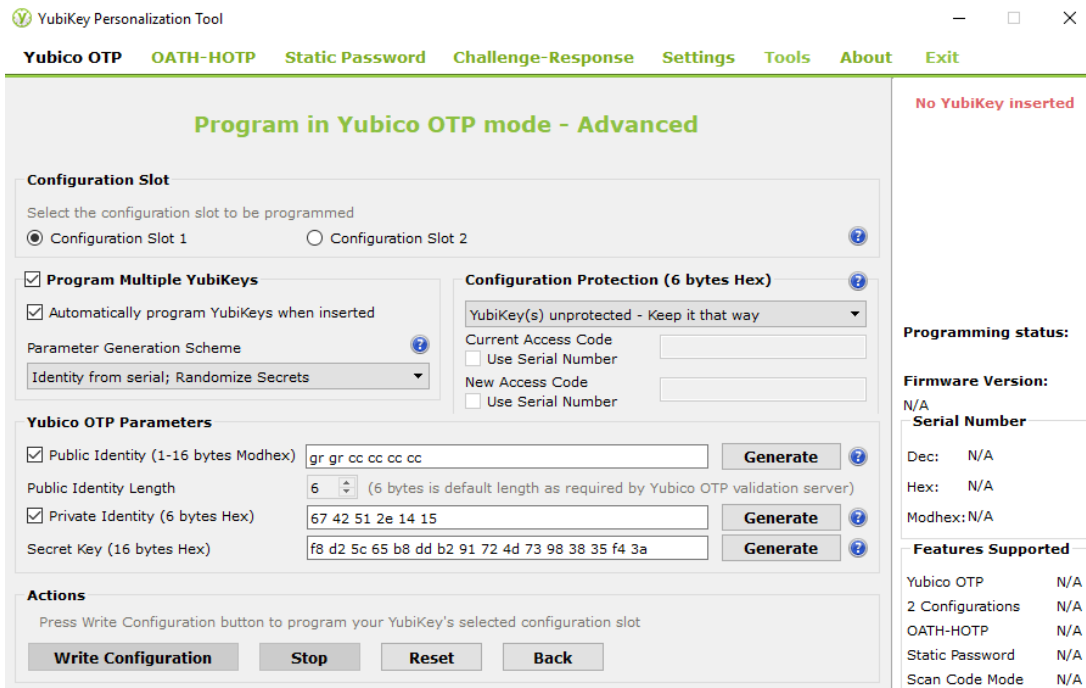
yubico

3. Select the Yubico OTP menu, and click on Advanced



4. You will see a screen as shown below:


- a. Select Configuration Slot 1
- b. Select Program Multiple YubiKeys
- c. Select Automatically program YubiKeys when inserted
- d. Under Parameter Generation Scheme, select Identity from serial; Randomize Secrets



5. Insert the first YubiKey and click on Write Configuration. Name the output file to be created and save it somewhere. (Note: Make sure the file name of the output file does not contain spaces.) This file will contain the new secrets of the programmed YubiKeys. Please keep it in a secure place until it is uploaded into GreenRADIUS.
6. The already inserted YubiKey will be programmed, and you will see a success message. Remove the YubiKey.
7. Without exiting the tool, insert the next YubiKey. Wait for the tool to program the inserted YubiKey (you will see a success message), then remove it. Continue this process for the rest of your YubiKeys.
8. After all YubiKeys are programmed, click on Stop, and close the tool.

4. IMPORTING THE NEW SECRETS FILE INTO GREENRADIUS

1. Open a new browser tab and navigate to the GreenRADIUS web admin console.
2. Make sure the validation server is set to “Local Validation Server on GreenRADIUS”. You can set this under the Global Configuration tab, Validation Server.

Module Index Validation Server Configuration 

Validation Server Configuration


Validation Server

YubiCloud - Online Validation Service
 Local validation Server on GreenRADIUS Virtual Appliance
 Other (for example: "http://192.168.1.1/wsapi/2.0/verify")

[Save](#)

[Return to Global Configuration](#)

3. Go to the Import Secrets tab.
4. Select “Cross-Platform Personalization tool-Import YubiKey Secrets”. Then click on “Browse...”.

Module Config **GreenRADIUS - Virtual Appliance** 

[Domain](#) [Global Configuration](#) [Diagnostics](#) [Troubleshoot](#) [Reports](#) [Updates](#) **[Import Secrets](#)** [List Tokens](#) [License](#) [Alerts](#) [About](#)

Import Secrets

This section can be used to import the AES secrets in to the local YK-KSM or YubiHSM database if the local validation server on GreenRADIUS Virtual Appliance is used to validate the OTPs.

Log file source

Original Windows Personalization tool-Import YubiKey Secrets
 Cross-Platform Personalization tool-Import YubiKey Secrets
 Import OATH Tokens (PSKC Container)

Select a file to upload No file selected.

[Upload](#)

5. Select the new secrets file that was just created.
6. Click on Upload. Do not navigate away from the page. Wait for a success message to appear.
7. After the upload is complete, you can see the newly imported tokens in the List Tokens tab.