Programming YubiKeys for Okta Adaptive Multi-Factor Authentication

September 25, 2015

Copyright

Trademarks

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.

Contact Information

Yubico Inc
420 Florence Street, Suite 200
Palo Alto, CA 94301
USA
yubi.co/contact

Contents

Introduction to the YubiKey

One key. Two form factors. The YubiKey delivers a one-time passcode (OTP) with a simple touch of a button. No SMS-like passcodes to retype from one device to another. Our YubiKey identifies itself as an external keyboard, which eliminates the need for client software or drivers. The nearly indestructible key holds tight onto its secrets, and its design ensures it will never be a vector for viruses or malware.

yubico
YubiKey Product Family
fido Ready
fido Ready
YubiKey Standard & YubiKey Nano
YubiKey Edge & YubiKey Edge-n
YubiKey NEO & YubiKey NEO-n

When used with Okta, the YubiKey adds the strength of multi-factor authentication to protect accounts, eliminating the risk of a stolen password allowing malicious access to secured sites or services.

Each YubiKey acts as two OTP devices in one body, allowing the same device to be used with both Okta as well as for a second service.

With Yubico’s YubiKey Personalization Tool, users or administrators can load their own secrets and configuration onto their YubiKey, ensuring that these secrets are never out of their control, and thereby limiting the risk of a breach compromising their security.

For larger orders, Yubico also provides YubiKeys that are custom-configured for Okta for an additional fee. Contact Yubico Sales for more details.

Generating a YubiKey Secrets File

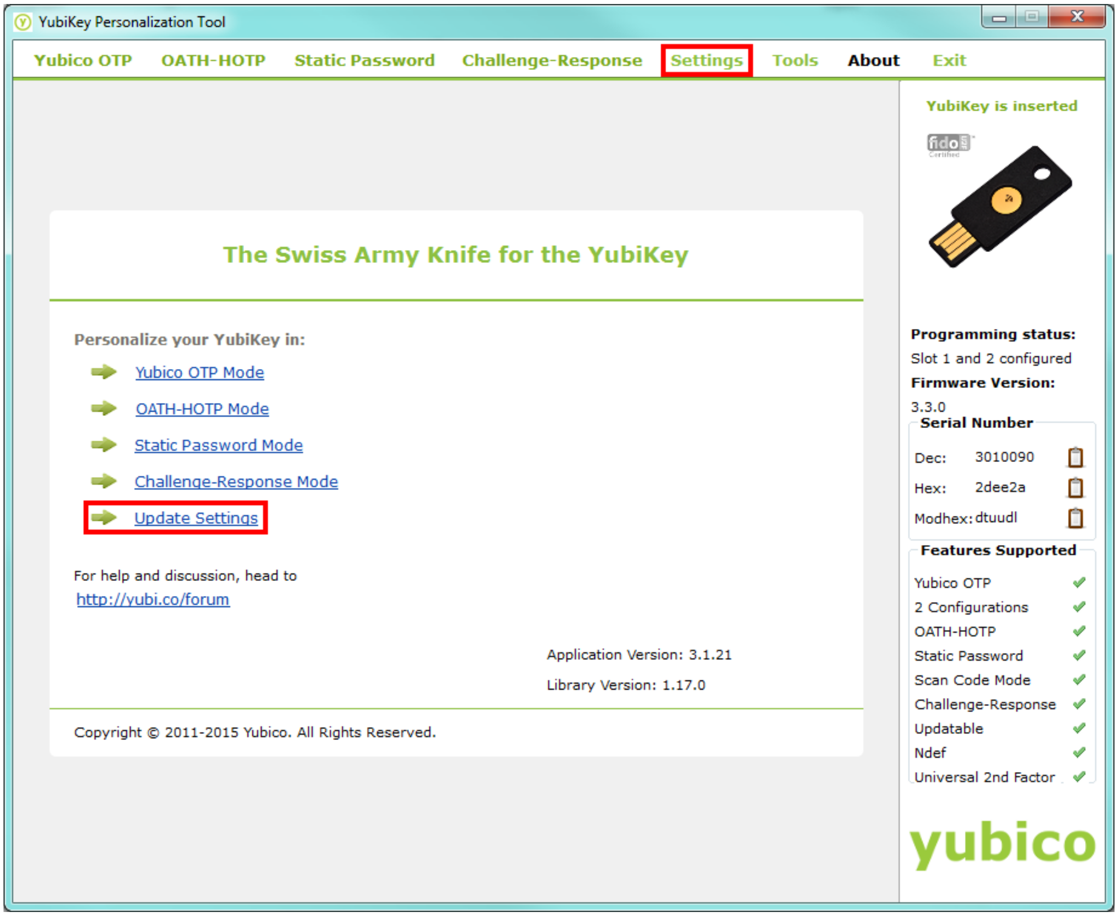
To generate a log containing the YubiKey secrets, for importing into the Okta service, the Yubico Cross-Platform Personalization tool is the simplest way to proceed. Download the YubiKey Personalization Tool installation files for Microsoft Windows, Mac OS X, or Linux from the Yubico download site.

For the most secure configuration and loading of secrets, we recommend you install the tool on a secured (preferably air-gapped) computer. The YubiKey Personalization tool generates a file with all the secret information loaded onto the YubiKeys. Be sure keep a backup of this file in a secure location, ideally one that is not connected to a corporate network.

The YubiKey Personalization tool can be configured to program multiple YubiKeys at a time, as well as for a single device. For instructions on setting up the YubiKey Personalization tool for multiple YubiKeys, see Programming Multiple YubiKeys. In addition, the YubiKeys can be locked with a Configuration Access code, preventing any modification to the setting or secrets loaded on the YubiKey if the code is not used. Steps to set up the Access code for configured YubiKeys are included in the chapter named YubiKey Configuration Protection.

To generate the secrets file

1. To begin, download and install the Personalization tool on your system.
2. Once installed, insert a YubiKey into the USB port on your computer.
3. Launch the YubiKey Personalization tool.



YubiKey is inserted

The Swiss Army Knife for the YubiKey

Personalize your YubiKey in:

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

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

Application Version: 3.1.21

Library Version: 1.17.0

Copyright © 2011-2015 Yubico. All Rights Reserved.

Programming status: Slot 1 and 2 configured

Firmware Version: 3.3.0

Serial Number

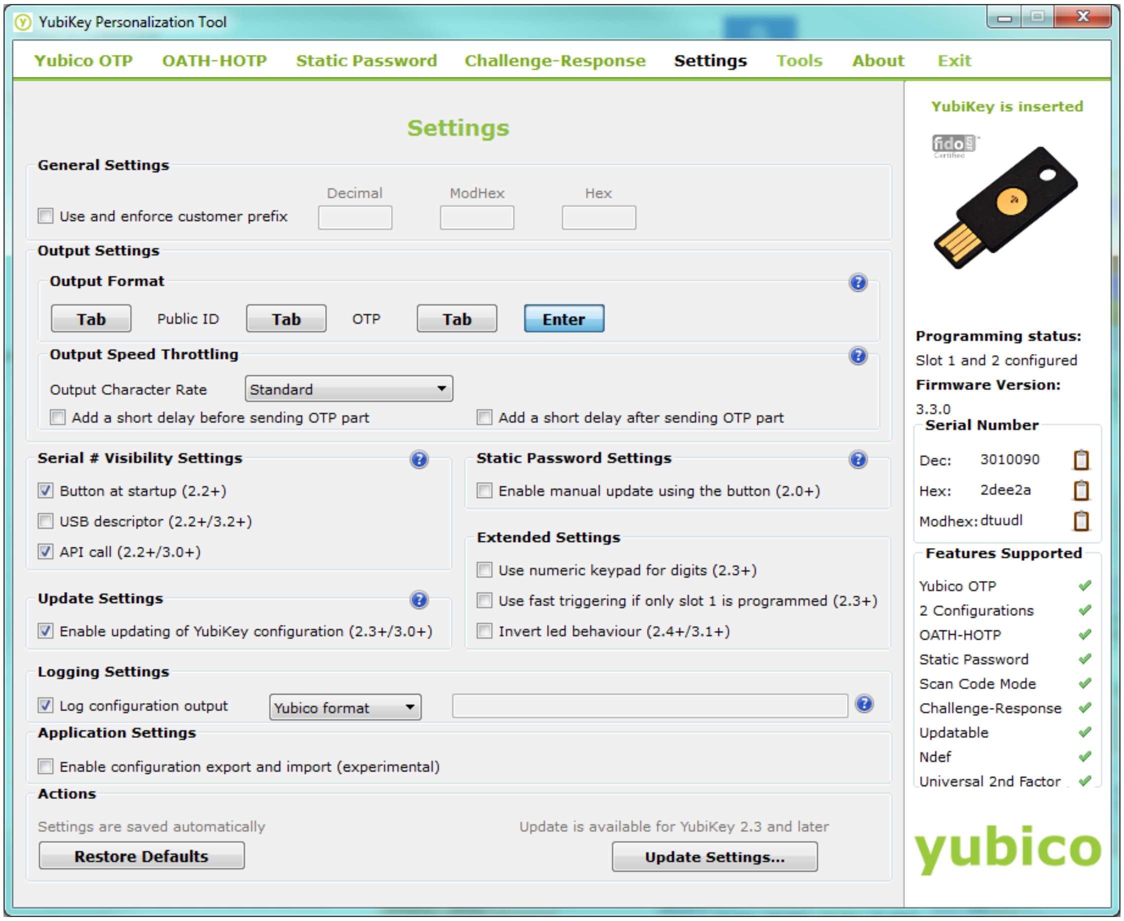
Dec:	3010090
Hex:	2dee2a
Modhex:	dtuudl

Features Supported

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

4. Click Update Settings.

   Tip: You can also click **Settings** in the top menu.



Settings

General Settings

Decimal ModHex Hex

□ Use and enforce customer prefix

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+)

Update Settings

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

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+)

Logging Settings

☑ Log configuration output: Yubico format

Application Settings

□ Enable configuration export and import (experimental)

Actions

Settings are saved automatically

Update is available for YubiKey 2.3 and later

YubiKey is inserted

Programming status:
Slot 1 and 2 configured

Firmware Version:
3.3.0

Serial Number

Dec:	3010090
Hex:	2dee2a
Modhex:	dtuudl

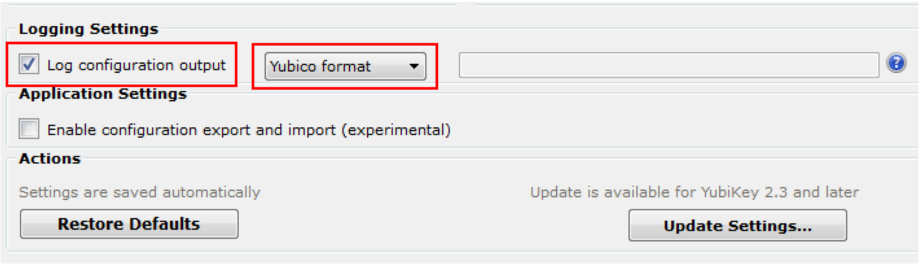
Features Supported

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

5. To configure YubiKeys for Okta, change the following settings:

   a. Under General Settings, ensure the option to **Use and enforce customer prefix** is not selected.

   b. Under Logging Settings, select the check box for **Log configuration output** and then click the arrow to select **Yubico Format**.



Logging Settings

☑ Log configuration output: Yubico format

Application Settings

□ Enable configuration export and import (experimental)

Actions

Settings are saved automatically

Update is available for YubiKey 2.3 and later

Settings are saved automatically as they are entered.

The next step is to configure the YubiKey with the entered settings to generate the configuration file. Continue with the next section, Configuring the YubiKeys.

Configuring the YubiKeys

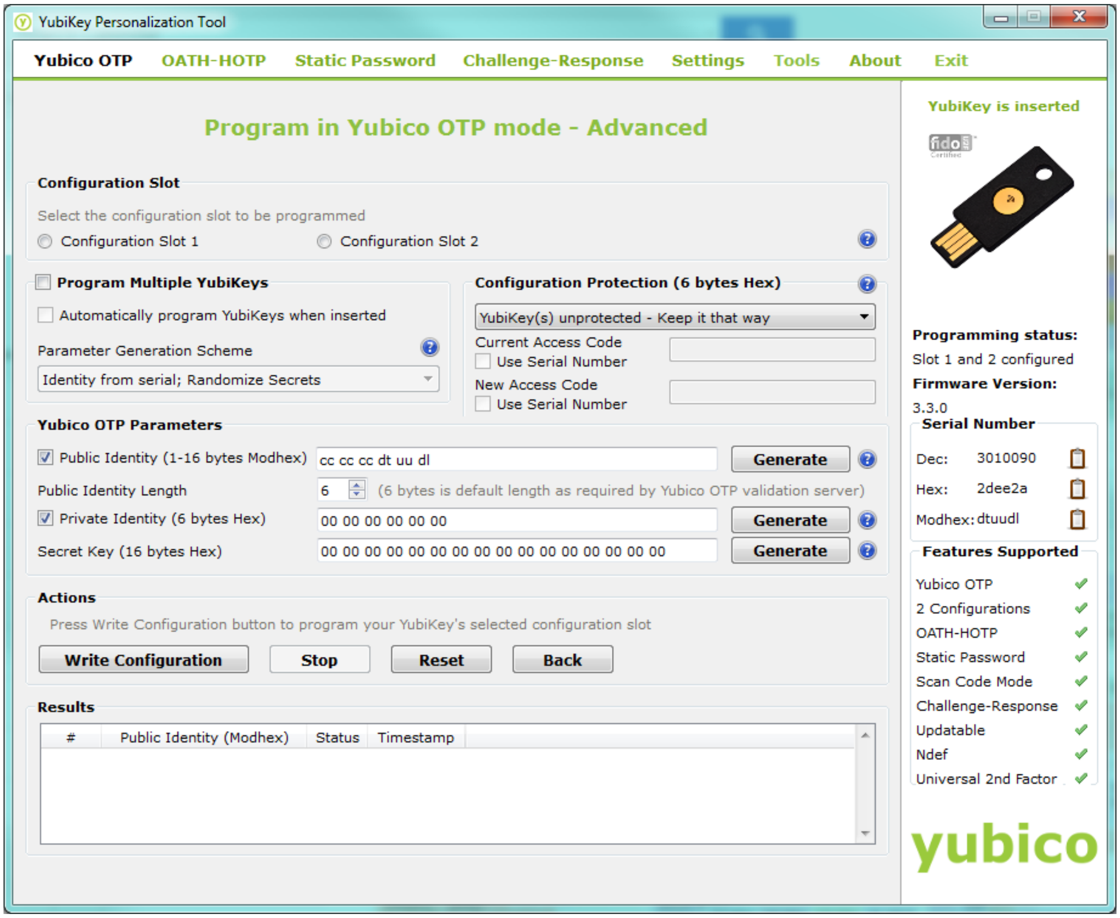
This section describes how to configure the YubiKeys using the Okta secrets file.

To configure the YubiKeys

1. Launch the YubiKey Personalization Tool, if it is not already running.

2. Select Yubico OTP from the menu.

3. In the Program in Yubico OTP mode screen, click **Advanced**.



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 cc cc dt uu dl

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

YubiKey is inserted

Programming status: Slot 1 and 2 configured

Firmware Version: 3.3.0

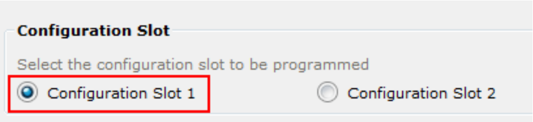
Serial Number

Dec:	3010090
Hex:	2dee2a
Modhex:	dtuudl

Features Supported

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

4. The first setting is for the Configuration Slot. Select the Configuration Slot to be programmed.



Configuration Slot

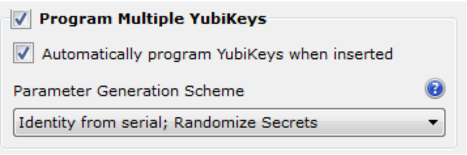
Select the configuration slot to be programmed

● Configuration Slot 1 ○ Configuration Slot 2

Each YubiKey has two configuration slots, which can be selected by the length of time the user touches the button. A short touch (1~2 seconds) triggers reading from the first slot, while a longer touch, (3~5 seconds) triggers reading the second slot.

By default, each YubiKey is configured for the YubiCloud in slot 1. If you plan to use your YubiKeys with additional services other than Okta, then you may want to configure slot 2 for Otka. However, if the YubiKeys are only to be used with the Okta service, overwriting the existing configuration in slot 1 will reduce confusion.

5. To configure multiple YubiKeys at the same time, select the box to **Program Multiple YubiKeys**. For make it easier to program the YubiKeys, also check the box to **Automatically program YubiKeys when inserted** and set the Parameter Generation Scheme to **Identify from Serial; Randomize Secrets**. (For more information on these options, see Programming Multiple YubiKeys.)

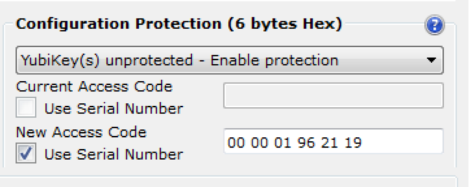


☑ Program Multiple YubiKeys

☑ Automatically program YubiKeys when inserted

Parameter Generation Scheme: Identity from serial; Randomize Secrets

6. In the section under Configuration Protection, select the option for **YubiKey(s) unprotected - Enable protection**. Then check the box under New Access Code to **Use Serial Number**. (For more information on these options, see YubiKey Configuration Protection.)

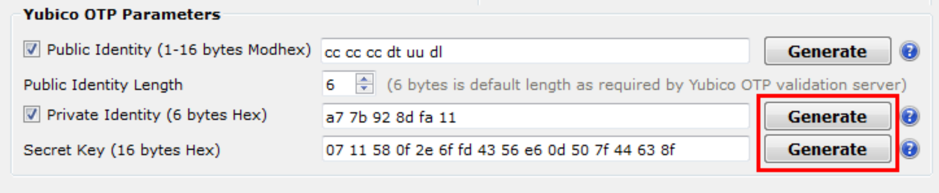


Configuration Protection (6 bytes Hex): YubiKey(s) unprotected - Enable protection

Current Access Code: ☐ Use Serial Number

New Access Code: ☑ Use Serial Number — 00 00 01 96 21 19

7. In the section under Yubico OTP Parameters, for Private Identity, click both **Generate** buttons to initialize the values for the Private Identity and Secret Key:



Yubico OTP Parameters

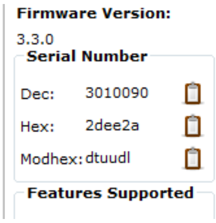
☑ Public Identity (1-16 bytes Modhex): cc cc cc dt uu dl

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

☑ Private Identity (6 bytes Hex): a7 7b 92 8d fa 11

Secret Key (16 bytes Hex): 07 11 58 0f 2e 6f fd 43 56 e6 0d 50 7f 44 63 8f

The Public Identity should already be entered, in the field. The Pubic Identity is a string of 6 c’s (“cc cc cc”) followed by 6 additional characters matching the Modhex value of the Serial number for the YubiKey. This value is also displayed in the right pane (status bar) in the YubiKey Personalization Tool in the status bar on the right of the tool.



Firmware Version:
3.3.0

Serial Number

Dec: 3010090

Hex: 2dee2a

Modhex: dtuudl

Features Supported

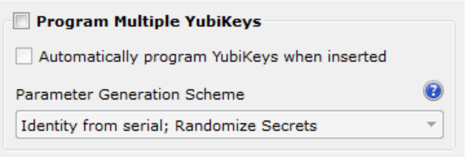
8. When you have configured all settings, click **Write Configuration**. The YubiKey Personalization tool displays a message so you can save a `configuration_log.csv` file - this is the configuration secrets file you will need to import.

9. If you have set the tool to program multiple YubiKeys, it automatically programs each YubiKey after the previous one is removed and a new YubiKey is inserted.

10. When you have finished programming all YubiKeys, click **Stop**. Remove the last YubiKey, and you have completed programming the YubiKeys!

Programming Multiple YubiKeys

When configuring large batches of YubiKeys, the YubiKey Personalization Tool can be configured to automate the process, generating unique secrets for each device while conforming to the settings entered by the user. The options for this function are in the section under Program Multiple YubiKeys.



□ Program Multiple YubiKeys

□ Automatically program YubiKeys when inserted

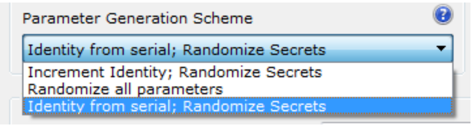
Parameter Generation Scheme

Identity from serial; Randomize Secrets

- **Program Multiple YubiKeys** – Select this option to enable the other options for automatically programming a batch of YubiKeys. If this option is not selected, each YubiKey will have to have a Public ID, Private ID, and AES key manually generated by the user. When selected, this option automates that process.

- **Automatically Program YubiKeys when inserted** – When this option is enabled, the YubiKey Personalization Tool automatically programs a YubiKey as soon it registers the previous one was removed and a new key has been inserted. If this option is not selected, you need to click **Write Configuration** for each YubiKey being programmed.

- **Parameter Generation Scheme** – This list allows you to define how you want the Public Identity, Private Identity, and AES key generated for each YubiKey.



Parameter Generation Scheme

Identity from serial; Randomize Secrets

Increment Identity; Randomize Secrets
Randomize all parameters
Identity from serial; Randomize Secrets

  - **Increment Identity; Randomize Secrets** – This option has the Public ID for each YubiKey incremented by one from a base value (in modhex), with the Private ID and AES key randomly generated.

  - **Randomize all parameters** – This option randomizes the Public ID, Private ID, and AES key to randomly generated values.

  - **Identity from serial; Randomize Secrets** – This option sets the Public ID to be equal to the serial number of the YubiKey (in modhex), ensuring a unique Public ID for the device, with the Private ID and AES key randomly generated.

YubiKey Configuration Protection

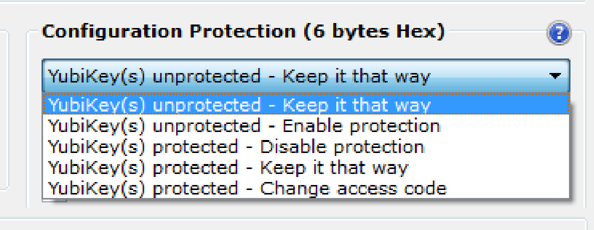
Applying Protection at Configuration

The YubiKey allows for the settings configured into either or both Configuration Slots to be locked down with an access code, so that only users who have the code can modify the settings on the YubiKey. Each slot can have this protection applied individually, allowing for the greatest amount of flexibility.

The simplest way to protect your YubiKey is to use the YubiKey Personalization Tool and apply the Access code when configuring the slots on the YubiKey.

To protect the configuration of your YubiKey

1. In the section under Configuration Protection, click the arrow to display the list of options:



Configuration Protection (6 bytes Hex)
YubiKey(s) unprotected - Keep it that way
YubiKey(s) unprotected - Keep it that way
YubiKey(s) unprotected - Enable protection
YubiKey(s) protected - Disable protection
YubiKey(s) protected - Keep it that way
YubiKey(s) protected - Change access code

2. Do one of the following.

   a. If the YubiKey slot you are configuring is not currently protected with an access code, select **YubiKey(s) unprotected – Enable protection**.

   b. If the YubiKey slot you are configuring is currently protected with an access code, and you want to keep the current access code, select **YubiKey(s) protected – Keep it that way**.

   c. If the YubiKey slot you are configuring is currently protected with an access code, and you want to set a new access code, select **YubiKey(s) protected – Change Access code**.

   The Access Code fields become available, depending on the option you select.

3. Do one of the following:

   a. If **Current Access code** is available, enter the access code you currently use to secure the YubiKey. If you use the YubiKey Serial Number as an access code, select the option to automatically fill in the access code.

   b. If **New Access code** is available, enter the access code you want to use. The access code must be 12 characters (hexadecima 0-9, a-f).

   c. To use the YubiKey Serial Number as an access code, select **Use Serial Number**. An Access code created based off of the serial number is entered into the field.

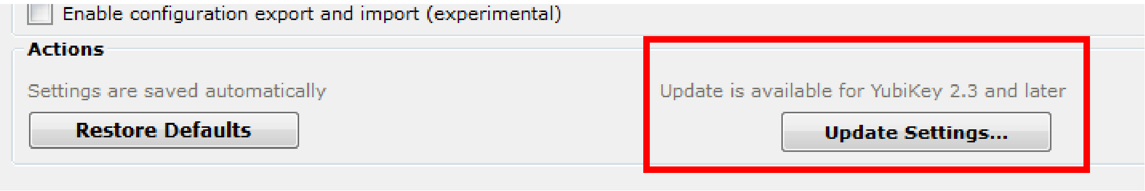
4. Click **Write Configuration** to write the configuration to the YubiKey. The status will be updated showing that the YubiKey configuration has been updated. If logging is enabled, the access code is recorded in the `configuration_log.csv` file.

Applying Protection to Existing Configurations

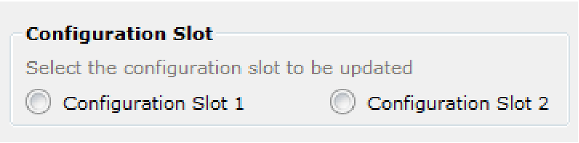
YubiKeys with firmware version 2.3 and above can have Configuration Protection applied (or removed) to existing configurations in either slot. Use the YubiKey Personalization Tool to apply Configuration Protection.

To apply or remove configuration protections

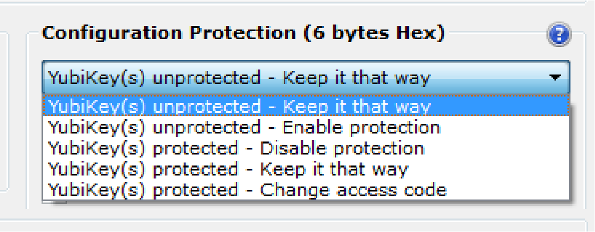
1. Launch the Personalization tool, and select **Update Settings**.
2. Insert your YubiKey into the USB port, if it is not already inserted.
3. In the lower right corner of the Settings page, locate and click the button to **Update Settings**.


□ Enable configuration export and import (experimental)
Actions
Settings are saved automatically
Restore Defaults
Update is available for YubiKey 2.3 and later
Update Settings...

4. On the Update Settings page, select the slot from which you want to remove Configuration Protection.



5. On the Update Settings page, in the section under Configuration Protection, click the arrow to display the list of options:


Configuration Protection (6 bytes Hex)
?
YubiKey(s) unprotected - Keep it that way
YubiKey(s) unprotected - Keep it that way
YubiKey(s) unprotected - Enable protection
YubiKey(s) protected - Disable protection
YubiKey(s) protected - Keep it that way
YubiKey(s) protected - Change access code

6. Do one of the following.

   a. If the YubiKey slot you are configuring is not currently protected with an access code, select **YubiKey(s) unprotected – Enable protection**.

   b. If the YubiKey slot you are configuring is currently protected with an access code, and you want to keep the current access code, select **YubiKey(s) protected – Keep it that way**.

c. If the YubiKey slot you are configuring is currently protected with an access code, and you want to set a new access code, select **YubiKey(s) protected – Change Access code**.

The Access Code fields become available, depending on the option you select.

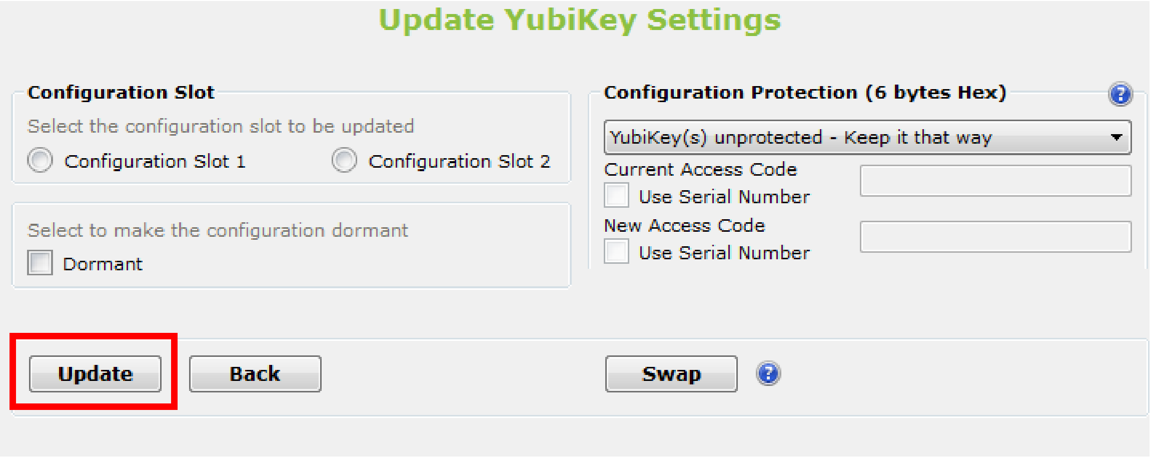
7. Do one of the following:

   a. If **Current Access code** is available, enter the access code you currently use to secure the YubiKey. If you use the YubiKey Serial Number as an access code, select the option to automatically fill in the access code.

   b. If **New Access code** is available, enter the access code you want to use. The access code must be 12 characters (hexadecimal 0-9, a-f).

   c. To use the YubiKey Serial Number as an access code, select **Use Serial Number**. An Access code created based off of the serial number is entered into the field.

8. Click **Update** to write the configuration to the YubiKey. If logging is enabled, the access code is recorded in the `configuration_log.csv` file.



Update YubiKey Settings

Configuration Slot

Select the configuration slot to be updated

○ Configuration Slot 1 ○ Configuration Slot 2

Select to make the configuration dormant

□ Dormant

Configuration Protection (6 bytes Hex)

YubiKey(s) unprotected - Keep it that way

Current Access Code

□ Use Serial Number

New Access Code

□ Use Serial Number