yubico

YubiKey Personalization Tool

User's Guide

Copyright

Trademarks

Disclaimer

Contact Information

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

Document Release Date

March 25, 2016

Contents

Introduction

Yubico changes the game for strong authentication, providing superior security with unmatched ease-of-use. Our core invention, the YubiKey, is a small USB and NFC device supporting multiple authentication and cryptographic protocols. With a simple touch, it protects access to computers, networks, and online services for the world's largest organizations.

Our innovative keys offer strong authentication via Yubico one-time passwords (OTP), FIDO Universal 2nd Factor (U2F), and smart card (PIV, OpenPGP, OATH) — all with a simple tap or touch of a button. YubiKeys protect access for everyone from individual home users to the world's largest organizations.

Introduction to the YubiKey Personalization Tool

Use the YubiKey Personalization Tool to configure the two slots on your YubiKey on Windows, Linux, and Mac OS X operating systems. The tool follows a simple step-by-step approach to configuring YubiKeys and is valid with any YubiKey (except the Security Key). Using the YubiKey Personalization Tool, you can program your YubiKey in the following modes:

- Yubico OTP
- OATH-HOTP
- Static Password
- Challenge-Response

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.

IMPORTANT: Re-programming your YubiKey's first configuration slot will overwrite the YubiCloud configuration, and you cannot undo this action. Use care when you re-configure your YubiKey.

This document describes the following topics:

Getting Additional Help

For more information, and to get help with your YubiKeys, see:

- Support home page
- Documentation and FAQs
- Start a Support ticket

System Requirements and Prerequisites

Before installing the YubiKey Personalization Tool, be sure your computer meets the system requirements, that you understand the random number generation that the YubiKey Personalization Tool uses, and that you understand security and cryptographic practices.

In this Chapter

System Requirements

The YubiKey Personalization Tool is available for Microsoft Windows, Linux, and Mac OS X. The tool has the following system requirements on each platform:

- **Microsoft Windows**: The YubiKey Personalization Tool is designed to run on all Microsoft Windows Windows 32-bit and 64-bit operating systems, from Microsoft Windows 7 and later.
- **Linux**: The YubiKey Personalization Tool can run on any Linux based system. The Graphical User Interface is required for running the YubiKey Personalization Tool.
- **Mac OS X**: The YubiKey Personalization Tool is available for the Intel based Mac OS 10.7.

Understanding Random Number Generation

This section describes the random number generation that is used for the YubiKey Personalization Tool for each operating system.

Microsoft Windows

The YubiKey Personalization Tool uses the **Win32 Crypto API function CryptGenRandom** to generate random numbers as needed.

Linux and Mac OS X

The YubiKey Personalization Tool uses any one of `/dev/srandom`, `/dev/urandom`, or `/dev/random` devices for random number generation. The YubiKey Personalization Tool first attempts to open and read random bytes from the `/dev/srandom` device. If the device is not found, or random bytes cannot be read, then the YubiKey Personalization Tool attempts the same thing with the next device, such as `/dev/urandom`, and so on.

Security and Cryptographic Best Practices

Be sure you understand the appropriate security and cryptographic best practices needed to maintain the integrity of the generated configurations.

The YubiKey Personalization Tool does not store cryptographically sensitive information, 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. The YubiKey secrets in the configuration log should be stored in a secure manner, as their exposure can compromise the protection of the YubiKey.

Installing the YubiKey Personalization Tool

You can install the YubiKey Personalization Tool on Microsoft Windows, Linux, and Mac OS X operating systems.

In this Chapter

Installing the Tool

The YubiKey Personalization Tool is a standalone application that functions without any dependencies. This means that you can copy the application file itself to another computer without launching the installation wizard.

To install the YubiKey Personalization Tool

1. Download the latest version of the YubiKey Personalization Tool from the Yubico website for the operating system you are using.
2. To install the application, do one of the following:

   - For Windows:

   a. To launch the installation wizard, click the `yubikey-personalization-gui-3.1.24` file.

   b. Complete the installation wizard.

   - For Mac OS X:

   a. To launch the installation wizard, double-click the `YubiKey Personalization Tool Installer-mac.dmg` file.

   b. Complete the installation wizard.

   - For Linux:

   a. Build the YubiKey Personalization Tool on a Linux distro.
   TIP: For information on how to build the project and create the YubiKey Personalization Tool executable on your Linux platform, see the Yubico Developers website.

   b. Launch and complete the installation process for your Linux distro.

Understanding the YubiKey Personalization Tool User Interface

The YubiKey Personalization Tool provides the same functionality and user interface on Microsoft Windows, Linux, and Mac OS X operating systems.

In this guide we are using the YubiKey Personalization Tool on Microsoft Windows, but the functionality is the same across all operating systems.

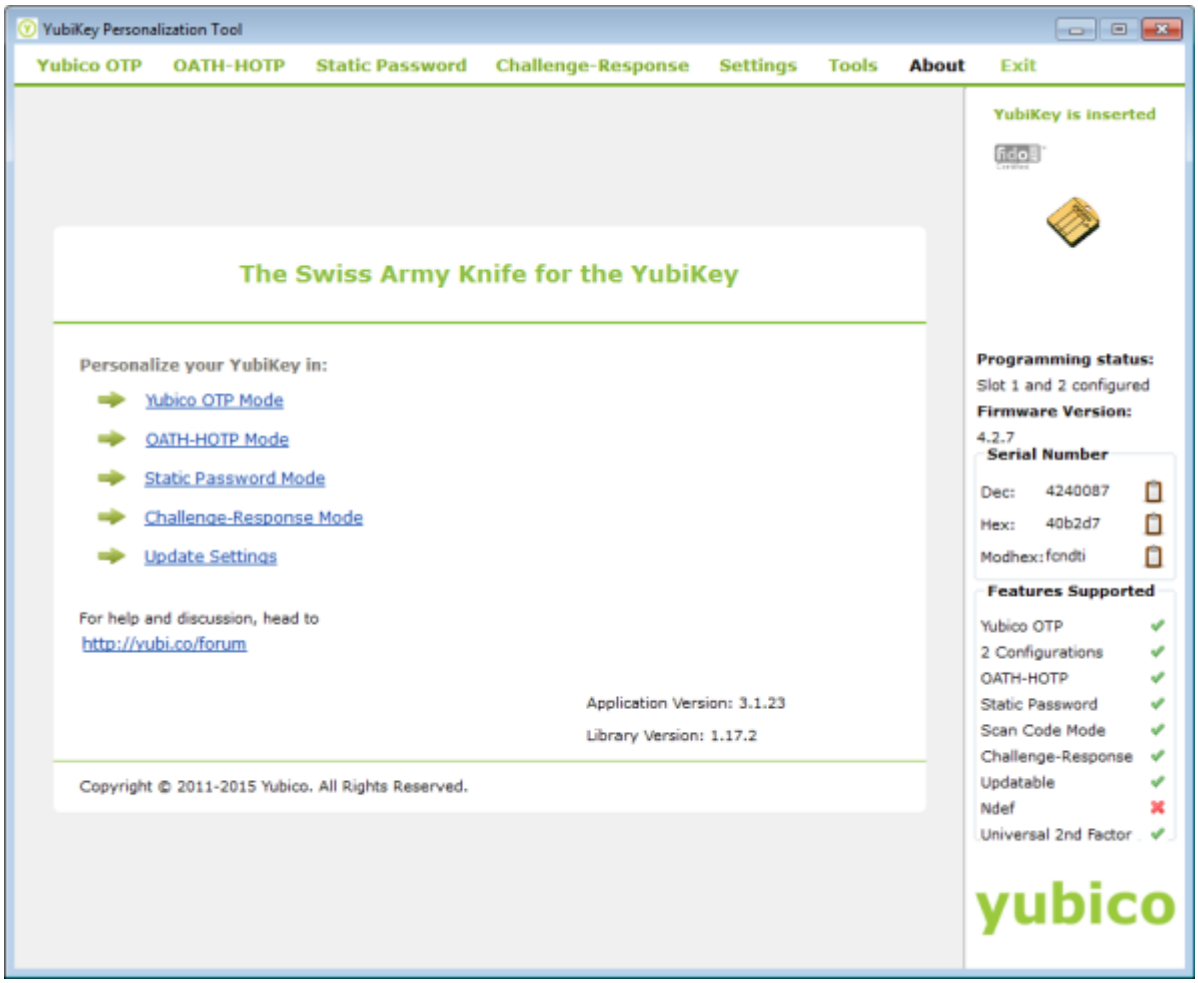
In this Chapter

Viewing the YubiKey Details

You can use the YubiKey Personalization Tool to perform common tasks, such as viewing the YubiKey firmware version, serial number, and other details.

To view details about a YubiKey

1. Insert the YubiKey into a USB port of your computer.
2. Launch the YubiKey Personalization Tool. To do this:
    - On Windows:
        - Double-click the YubiKey Personalization Tool shortcut.
    - On Mac OS X:
        - Start the YubiKey Personalization Tool.
    - On Linux:
        - Start the YubiKey Personalization Tool.



3. On the right side of the tab, view the information related to the specific YubiKey that is inserted into the USB port of your computer.
   NOTE: The configuration details of the YubiKey are never exposed; this includes the mode type (Yubico OTP, OATH-HOTP, Challenge-Response, and Static Password) that is loaded in each slot. This means the YubiKey Personalization Tool cannot help you determine what is loaded on the OTP mode of the YubiKey. The YubiKey Personalization Tool can help you determine whether something is loaded.

Viewing Help Topics From Within the YubiKey Personalization Tool

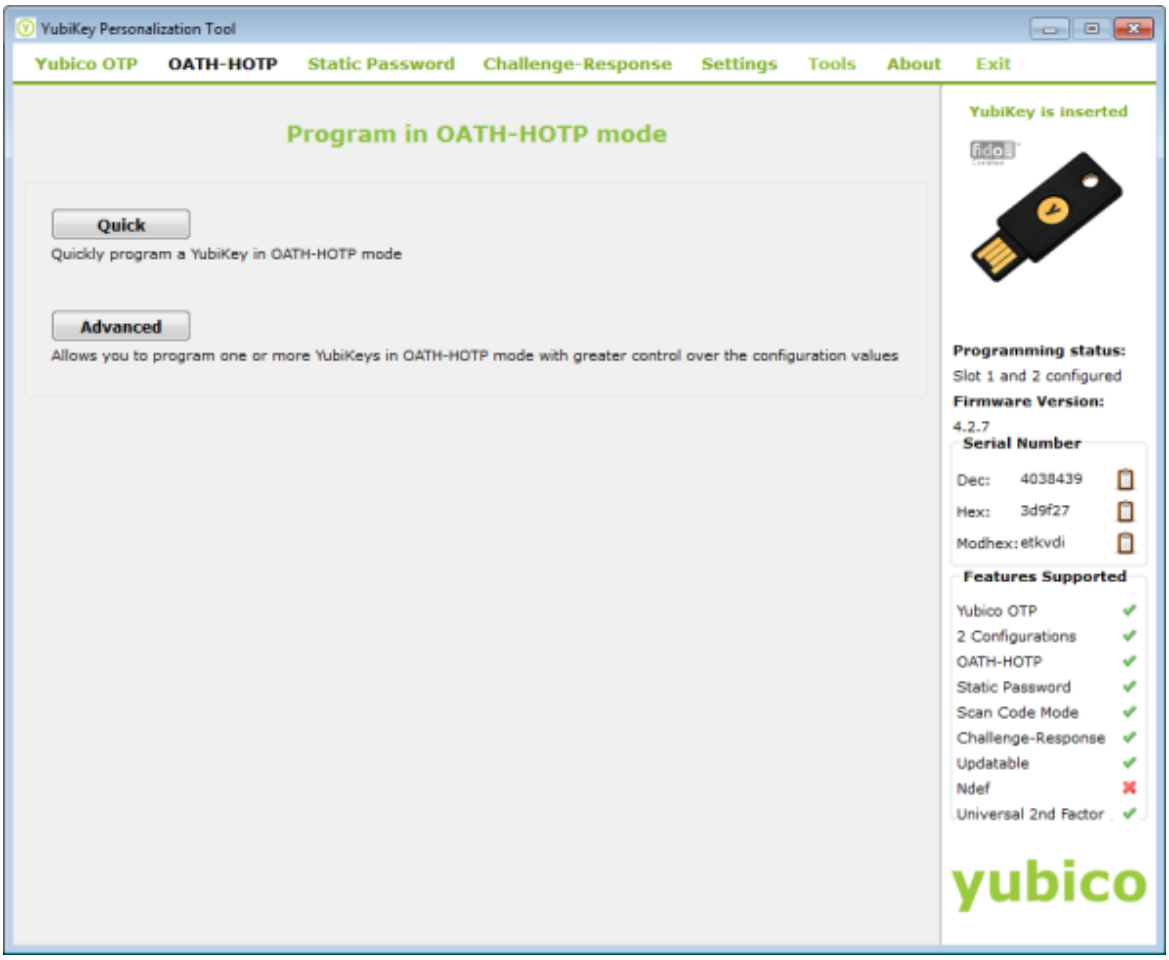
Throughout the YubiKey Personalization Tool, there are help topics specific to different areas of the interface.

To view help topics throughout the user interface

- Click the question mark (help button) to read more information about the available options.

Understanding Quick and Advanced Options

Each of the configuration modes—Yubico OTP, OATH-HOTP, Static Password, and Challenge-Response—includes two programming options. For example, the programming modes for **Yubico OTP** and **OATH-HOTP** are Quick and Advanced:



For more information about the details for each configuration option, see the chapters next in this document:

- Creating a Yubico OTP Configuration
- Creating an OATH-HOTP Configuration
- Creating a Static Password Configuration
- Creating a Challenge-Response Configuration

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 the other is Advanced.

In this Chapter

Configuring a YubiKey Using Quick Mode

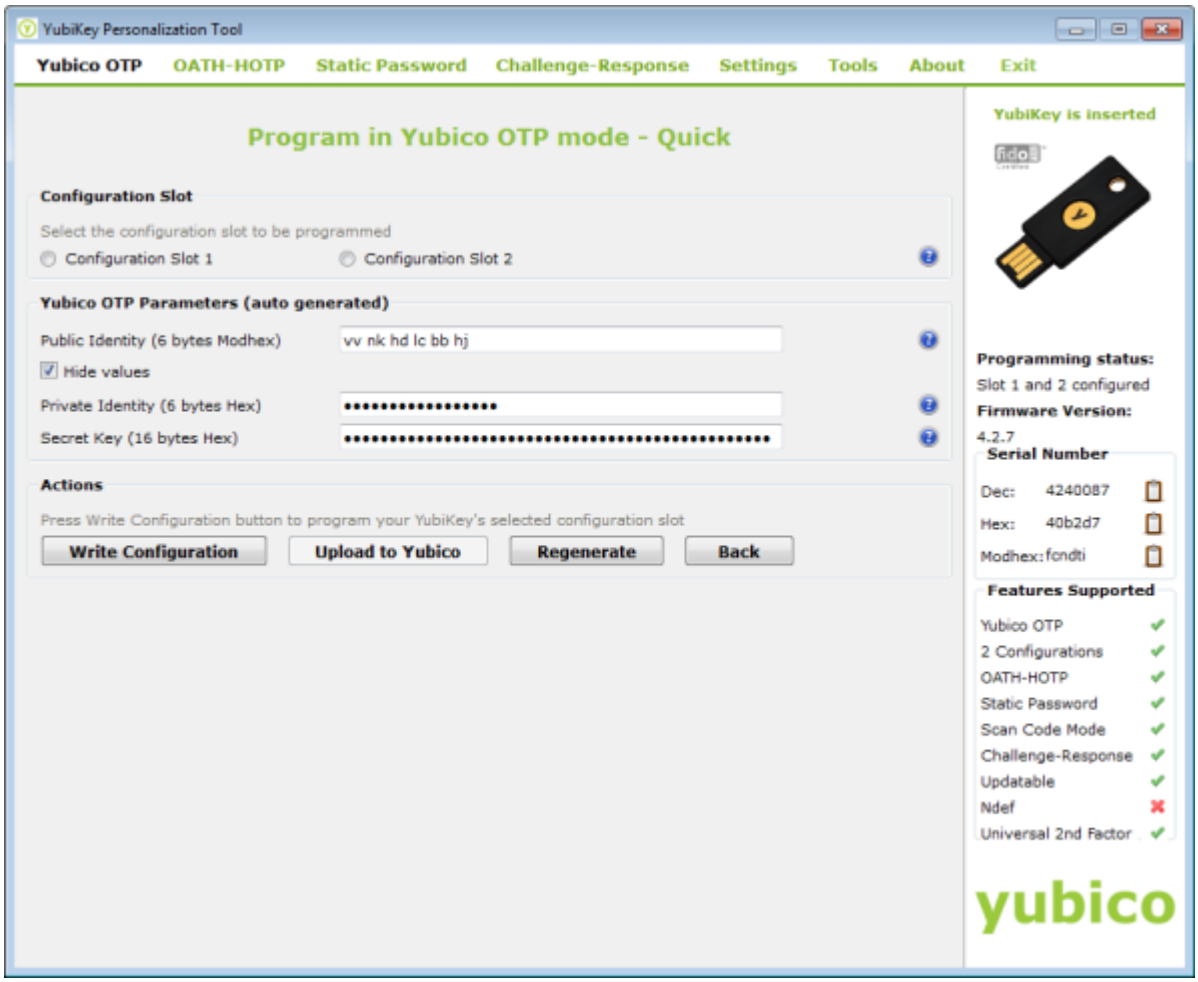
You can use the Quick option to quickly configure the YubiKey to upload the AES Key to the online Yubico OTP validation server.

NOTE: An internet connection is required for the online Yubico OTP validation server.

To configure a YubiKey using Quick mode

1. Launch the YubiKey Personalization Tool.
2. Click **Yubico OTP** or **Yubico OTP Mode**.
3. Insert a YubiKey into a USB port of your computer, and click **Quick**.
4. In the **Configuration Slot** group, select the YubiKey configuration slot that you want to configure, **Configuration Slot 1** or **Configuration Slot 2**. The YubiKey Personalization Tool automatically generates the Yubico OTP Parameters.

5. If you want to regenerate the Yubico OTP Parameters, in the **Actions** group, click **Regenerate**.



6. To reprogram the YubiKey in standard Yubico OTP mode, in the **Actions** group, click **Write Configuration**.
TIP: When the YubiKey configuration is successful, a message displays at the top of the window confirming the configuration.

7. To upload the AES key to the Yubico validation server, in the **Actions** group, click **Upload to Yubico**.
NOTE: This also populates the corresponding fields on the AES Key upload page with the values for reprogramming the YubiKey.

8. Type your email address, and place your cursor in **OTP from the YubiKey**.

9. Before you click Upload AES key, verify that your YubiKey prefix is correct:

    a. Open a text editor and touch the YubiKey. The first twelve characters are the YubiKey prefix.

    b. In the **Yubico AES Key Upload** window, compare **YubiKey prefix** with the results from the text editor.

10. Type the CAPTCHA, and click **Upload AES key**.

NOTE: It can take approximately 10-15 minutes to update all the corresponding databases and be able to validate the OTPs with the online Yubico OTP validation server.

To test your YubiKey with the YubiCloud validation servers

- See the demonstration on the Yubico website.

Configuring a YubiKey Using Advanced Mode

To program the YubiKey using your own parameters for Yubico OTP mode, use the **Advanced** option.

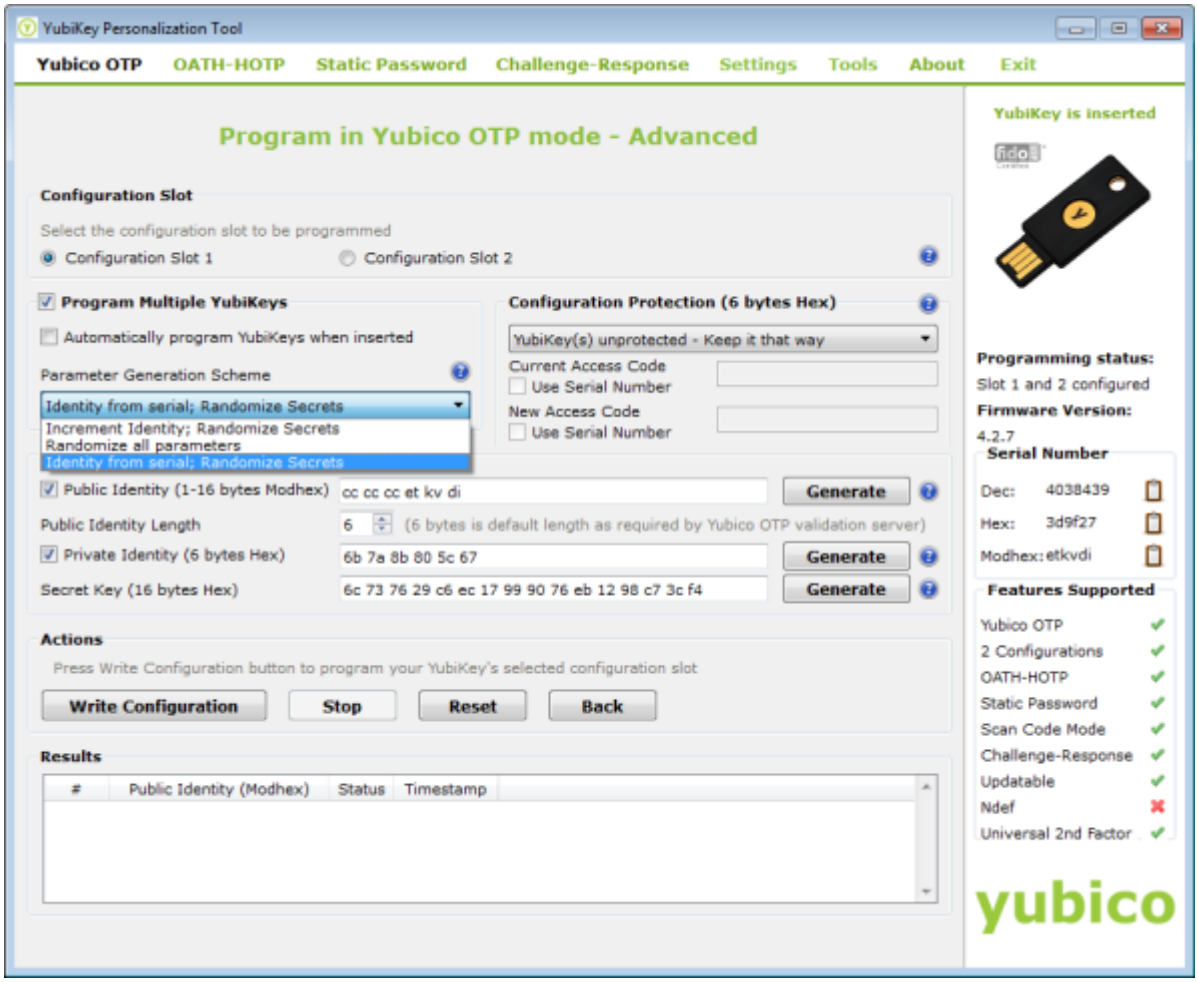
To program a YubiKey in Advanced mode

1. Launch the YubiKey Personalization Tool.
2. Click **Yubico OTP** or **Yubico OTP Mode**.
3. Insert the YubiKey into a USB port of your computer, and click **Advanced**.
4. In the **Configuration Slot** group, select the YubiKey configuration slot that you want to configure.
5. If you want to program multiple YubiKeys, select **Program Multiple YubiKeys** and do one of the following:
   - If you want to automatically program each YubiKey when you insert it, select **Automatically program YubiKeys when inserted**.

- If you want to click **Write Configuration** each time you insert a YubiKey, do not select **Automatically program YubiKeys when inserted**.

6. If you want to specify how the parameters used for programming the YubiKeys will be generated, in the **Parameter Generation Scheme** group, select one of the following:

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



7. In the **Configuration Protection** group, do one of the following:

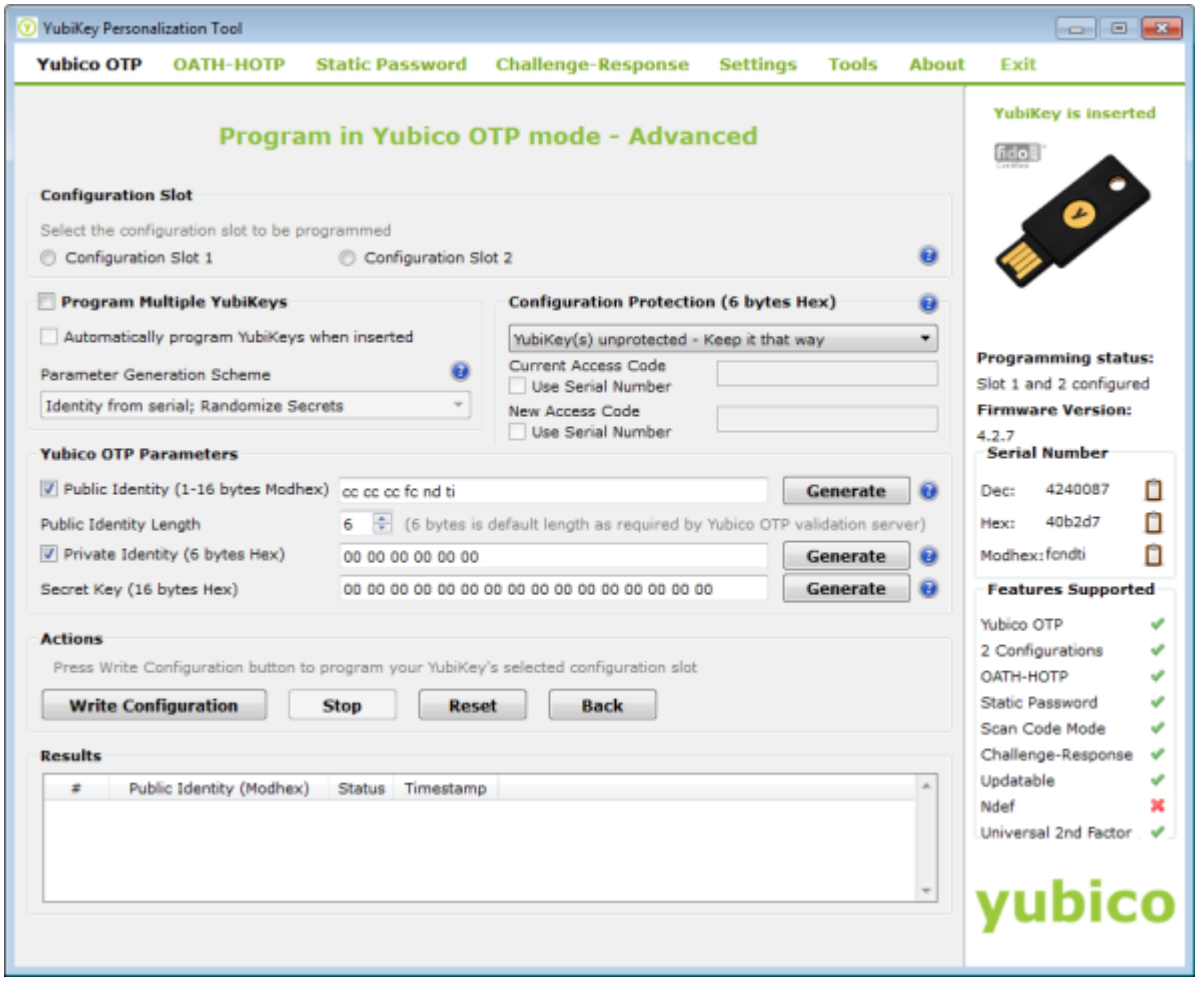
   - To lock the configuration so that you must type an access code to make changes to the configuration, select one of the following:
     - **YubiKey(s) unprotected – Enable protection**
     - **YubiKey(s) protected – Disable protection**
     - **YubiKey(s) protected – Keep it that way**
     - **YubiKey(s) protected –Change access code**

- If you do not want to use an access code, keep the default, **YubiKey(s) unprotected – Keep it that way**.

8. To choose the type of access code to lock the YubiKey configuration, in the **Configuration Protection** group, do one of the following:

   a. Type a twelve character hexadecimal access code.

   b. Select **Use Serial Number**. This is the serial number of the YubiKey that is inserted into the USB port of your computer. The decimal serial number is located on the right side of the **Yubico OTP** tab.



9. From the **Yubico OTP Parameters** group, select the following options, as needed:

   a. If needed, set the **Public Identity**, which is the first optional fixed part of the OTP string used to identify a YubiKey:

   - If there is no requirement for it, do not select **Public Identity**. By default, it is randomly generated and set to 6 bytes length.

   - If you set the Public Identity, be sure to type a length between 1 and 16 bytes:

     - Any length between 1 and 5 bytes is considered a private scope and will not create any interoperability issues.

- A Public Identity 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. If a customer prefix is set in the configuration, a Public Identity length of 6 bytes is enforced, where the first 2 bytes (or first 4 characters), contain the unique customer prefix. For more information about setting a unique customer prefix, see Using General Settings, in the next chapter of this document.

- To generate a new, random value for the **Public Identity**, click **Generate**.

b. Set **Private Identity**, which is a required secret value and included as an input parameter in the OTP generation algorithm:

- By default, **Private Identity** is required and is randomly generated and set to 6 bytes length.
- If there is a requirement not to include it, clear **Private Identity**.
- To regenerate **Private Identity**, click **Generate**.

c. Set the **Secret Key**, which is required and used to encrypt the OTP:

- By default, the **Secret Key** is randomly generated and set to 128-bit length.
- To regenerate the **Secret Key**, click **Generate**.

10. To configure the YubiKey in standard Yubico OTP mode, from the **Actions** group, click **Write Configuration**.
TIP: When the YubiKey configuration is successful, a message displays at the top of the window confirming the configuration.

11. If you are programming multiple YubiKeys, do the following:

a. Remove the YubiKey you just configured and insert another YubiKey to be configured into the USB port of your computer.

b. Continue to configure the YubiKeys, one at a time, until you finish configuring all your YubiKeys.

c. If you did not select **Automatically program YubiKeys when inserted**, click **Write Configuration** each time you insert a new YubiKey.

12. Click **Stop** when you are finished configuring YubiKeys.

Creating an OATH-HOTP Configuration

The OATH-HOTP configuration allows the YubiKey to be used in an OATH HOTP ecosystem as described in the RFC 4226 specification.

The OATH-HOTP mode is available with YubiKeys that use firmware version 2.1 and later.

There are two options available to configure the YubiKey in OATH-HOTP mode, one is Quick and the other is Advanced.

In this Chapter

Configuring a YubiKey for OATH-HOTP Using the Quick Option

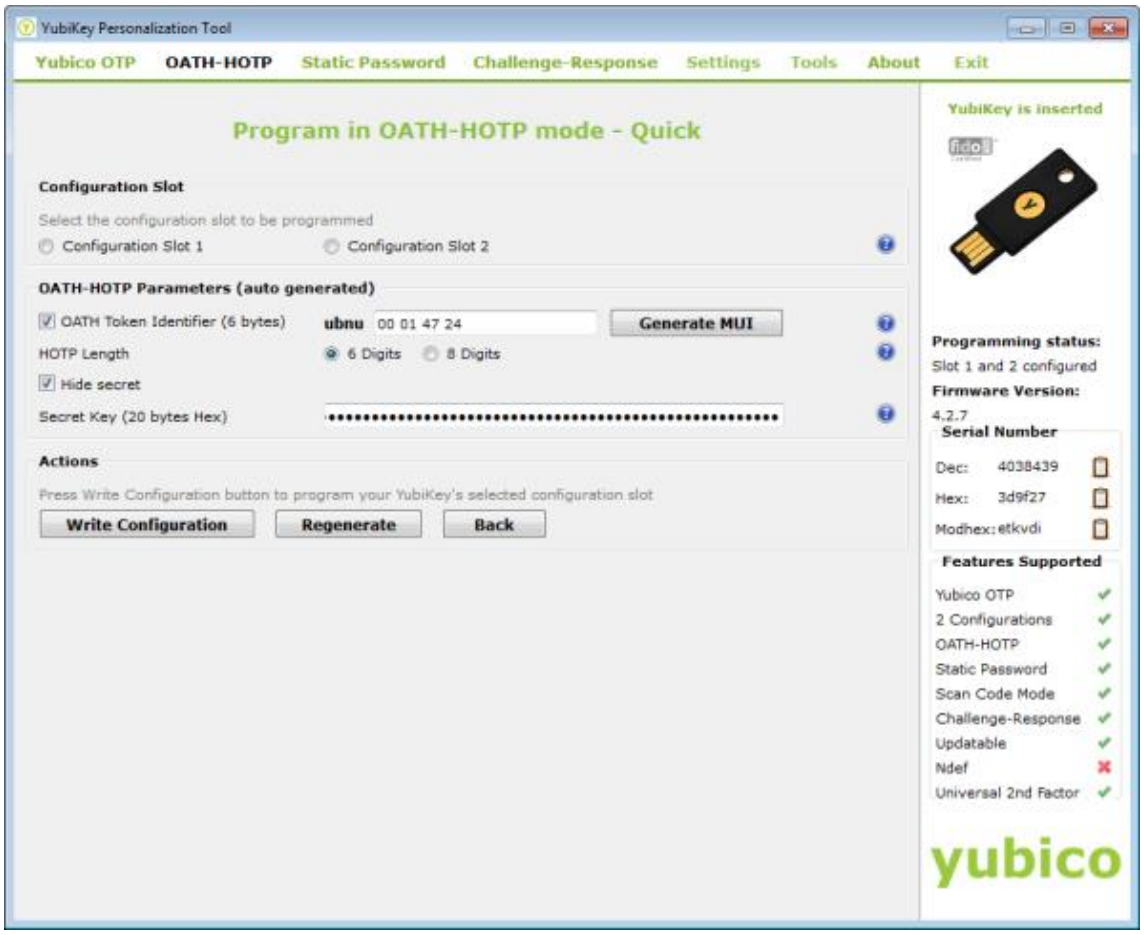
You can use the Quick option to quickly configure the YubiKey in OATH-HOTP mode using default parameters.

NOTE: By default, Quick mode sets the moving factor seed to `0`.

To program a YubiKey for OATH-HOTP using the Quick option

1. Launch the YubiKey Personalization Tool.
2. Click **OATH-HOTP** or **OATH-HOTP Mode**.
3. Click **Quick**, and insert a YubiKey into a USB port of your computer.

4. In the **Configuration Slot** group, select the YubiKey configuration slot that you want to configure.



5. If you want the YubiKey to output the OATH Token Identifier, from the **OATH-HOTP Parameters (auto generated)**, select the **OATH Token Identifier (6 bytes)**.
   TIP: The YubiKey supports the Class A Token Identifier Specification as outlined by openauthentication.org.

6. If you want to change the MUI to the 8 characters that uniquely identifies the token for a given manufacturer and token type, click **Generate MUI**.
   TIP: By default, the MUI is set to the serial number of the YubiKey.

7. Select the **HOTP Length**.

8. If you want to view the **Secret Key**, clear **Hide secret**.
   NOTE: The **Secret Key** will be randomly generated.

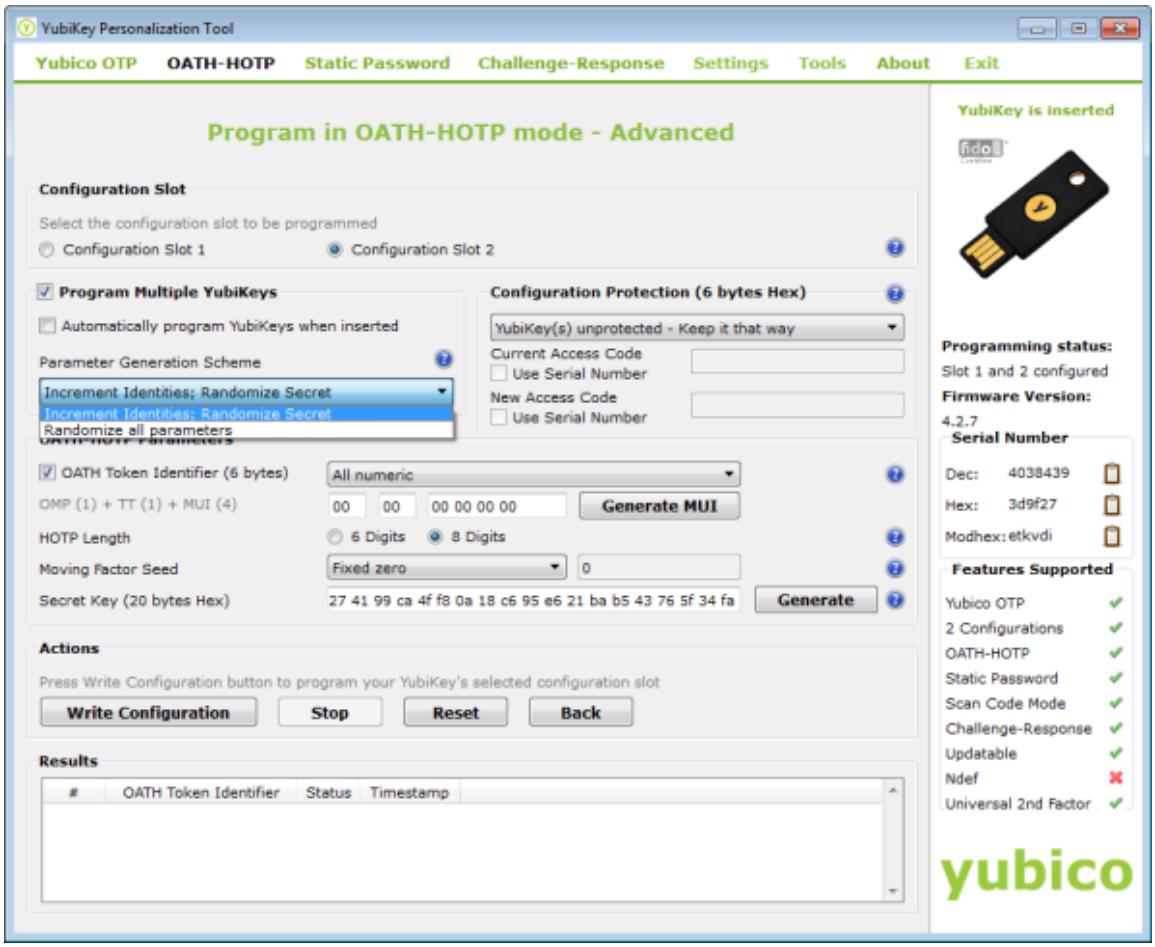
9. To program the YubiKey in the OATH-HOTP format, from the **Actions** group, click **Write Configuration**.
   TIP: When the YubiKey configuration is successful, a message displays at the top of the window confirming the configuration.

Configuring a YubiKey for OATH-HOTP Using the Advanced Option

To program the YubiKey for OATH-HOTP using your own parameters, use the **Advanced** option.

To program a YubiKey for OATH-HOTP using the Advanced option

1. Launch the YubiKey Personalization Tool.
2. Click **OATH-HOTP** or **OATH-HOTP Mode**.
3. Click **Advanced**, and insert a YubiKey into the USB port of your computer.
4. In the **Configuration Slot** group, select the YubiKey configuration slot that you want to configure.



5. If you want to program multiple YubiKeys, select **Program Multiple YubiKeys** and do one of the following:
   - If you want to automatically program each YubiKey when you insert it, select **Automatically program YubiKeys when inserted**.
   - If you want to click **Write Configuration** each time you insert a YubiKey, do not select **Automatically program YubiKeys when inserted**.
6. If you want to specify how the parameters used for programming the YubiKeys will be generated, in the **Parameter Generation Scheme** group, select one of the following:
   - **Increment Identities; Randomize Secret**

- **Randomize all parameters**

7. In the **Configuration Protection** group, do one of the following:

   - To lock the configuration so that you must type an access code to make changes to the configuration, select one of the following:

     - **YubiKey(s) unprotected – Enable protection**
     - **YubiKey(s) protected – Disable protection**
     - **YubiKey(s) protected – Keep it that way**
     - **YubiKey(s) protected –Change access code**

   - If you do not want to use an access code, keep the default, **YubiKey(s) unprotected – Keep it that way**

8. To choose the type of access code to lock the YubiKey configuration, in the **Configuration Protection** group, do one of the following:

   - Type a twelve character hexadecimal access code.
   - Select **Use Serial Number**. This is the serial number of the YubiKey that is inserted into the USB port of your computer. The decimal serial number is located on the right side of the tab.
     TIP: If enabled, the YubiKey can automatically output a unique identification string preceding the HOTP.

9. If you want the YubiKey to output the OATH Token Identifier, from the **OATH-HOTP Parameters (auto generated)**, select the **OATH Token Identifier (6 bytes)**.
   TIP: The YubiKey supports the Class A Token Identifier Specification as outlined by openauthentication.org.

10. If you want to change the MUI to the 8 characters that uniquely identifies the token for a given manufacturer and token, type it, and click **Generate MUI**.
    TIP: By default, the MUI is set to the serial number of the YubiKey.

11. If **OATH Token Identifier (6 Bytes)** is selected, there are four options available to output the OATH Token Identifier:

    - **All Numeric**
    - **OMP Modhex, rest numeric**
    - **OMP + TT Modhex, rest numeric**
    - **All Modhex**

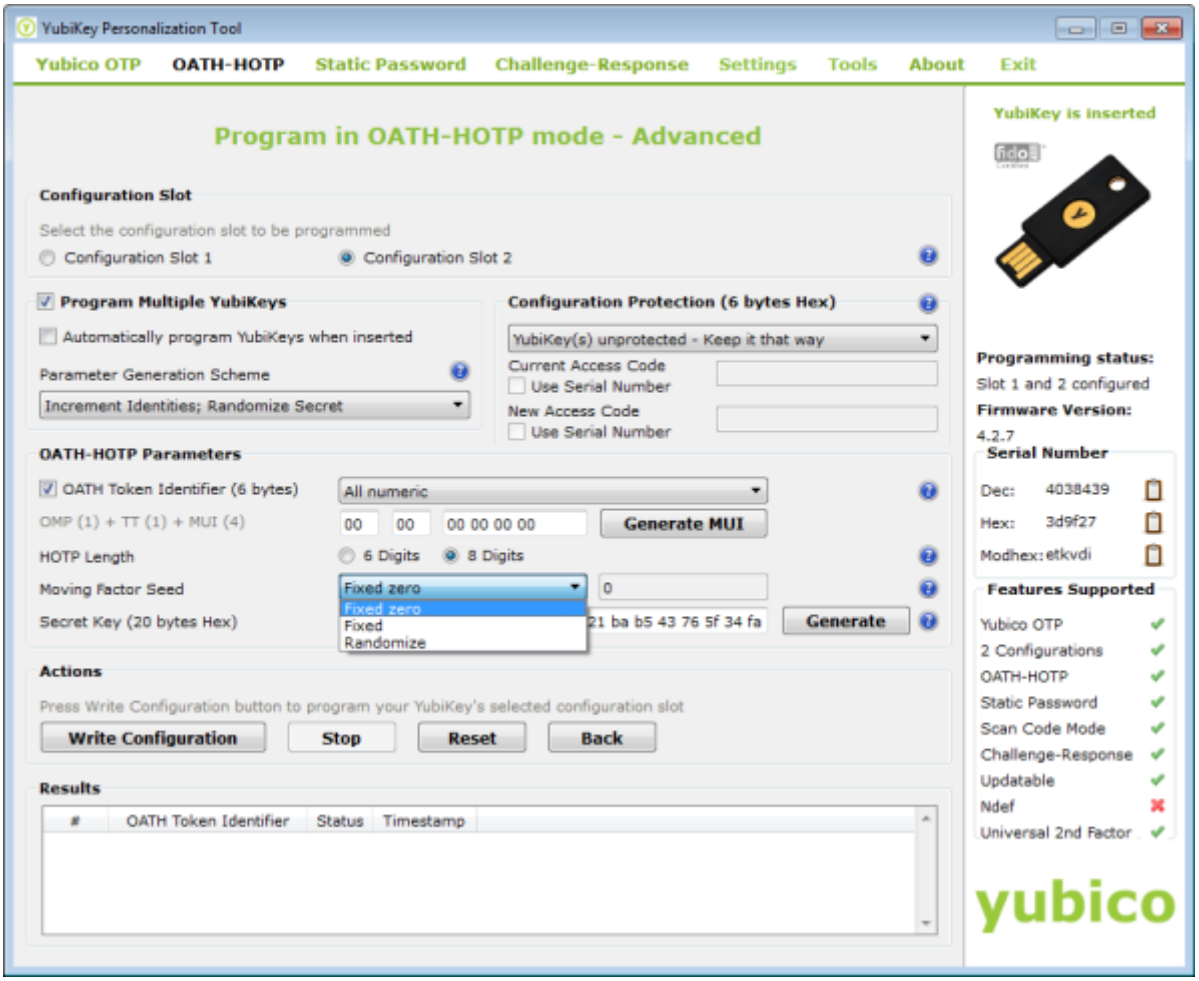
    NOTE: If you have a custom prefix set, the **Token Identifier** is set to **OMP + TT Modhex** or **All Modhex**. The first four characters are the Modhex public ID.

12. Select the appropriate **HOTP Length**.

13. For **Moving Factor Seed**, select one of the following:

    - **Fixed zero**
    - **Fixed**
    - **Randomize**

    TIP: According to the OATH-HOTP standard, RFC 4226, moving factor is a counter value that must be synchronized between the HOTP generator (YubiKey) and the HOTP validator (server).



14. To generate a random Secret Key, click **Generate**.

15. To program the YubiKey in OATH-HOTP mode, from the **Actions** group, click **Write Configuration**.
    TIP: When the YubiKey configuration is successful, a message displays at the top of the window confirming the configuration.

16. If you are programming multiple YubiKeys, do the following:

    a. Remove the YubiKey you just configured and insert another YubiKey to be configured into the USB port of your computer.

    b. Continue to configure the YubiKeys, one at a time, until you have finished configuring all your YubiKeys.

c. If you did not select **Automatically program YubiKeys when inserted**, click **Write Configuration** each time you insert a new YubiKey.

17. Click **Stop** when you are finished configuring YubiKeys.

Creating a Static Password Configuration

The Static mode is provided to create hard to guess and remember passwords. There are two options for static password configuration, Scan Code and Advanced.

In this Chapter

Configuring a YubiKey for Static Password Using the Scan Code Option

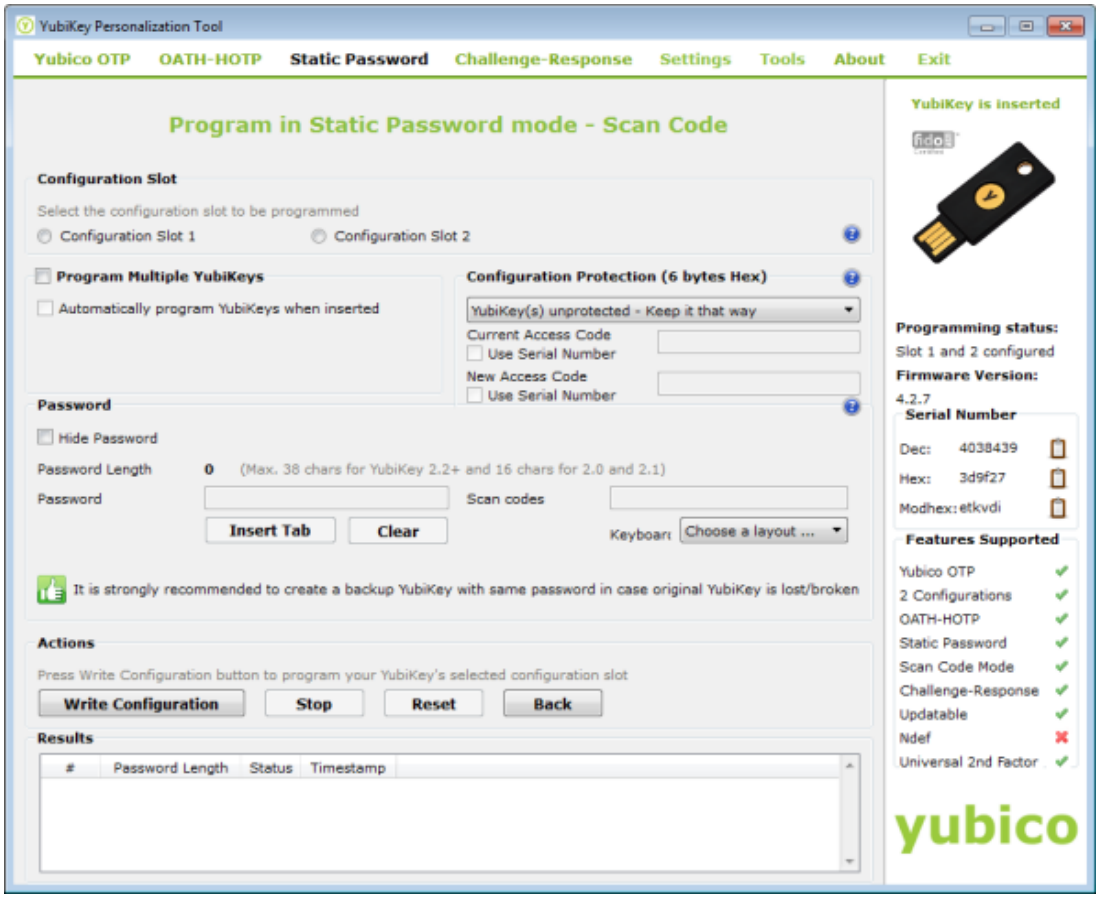
Scan Code mode provides a way to quickly program a YubiKey to emit your desired static password. This method generates a string based on any arbitrary keyboard scan code.

NOTE: Scan Code mode may create incompatibilities if different national keyboard layouts are used, because the keyboard mapping varies between countries. We recommend that you use the same keyboard layouts on the same computer, if possible, if you are using the Scan Code option.

To program a YubiKey using the Scan Code option

1. Launch the YubiKey Personalization Tool.
2. Insert the YubiKey into a USB port of your computer.
3. Click **Static Password** or **Static Password Mode**.

4. Click **Scan Code**, and from the **Configuration Slot** group, select the YubiKey configuration slot that you want to configure.



5. If you want to program multiple YubiKeys, select **Program Multiple YubiKeys** and do one of the following:

   - If you want to automatically program each YubiKey when you insert it, select **Automatically program YubiKeys when inserted**.
   - If you want to click **Write Configuration** each time you insert a YubiKey, do not select **Automatically program YubiKeys when inserted**.

6. In the **Configuration Protection** group, do one of the following:

   - To lock the configuration so that you must type an access code to make changes to the configuration, select one of the following:
     - **YubiKey(s) unprotected – Enable protection**
     - **YubiKey(s) protected – Disable protection**
     - **YubiKey(s) protected – Keep it that way**
     - **YubiKey(s) protected –Change access code**
   - If you do not want to use an access code, keep the default, **YubiKey(s) unprotected – Keep it that way**.

7. To choose the type of access code to lock the YubiKey configuration, in the **Configuration Protection** group, do one of the following:

    - Type a twelve character hexadecimal access code.
    - Select **Use Serial Number**. This is the serial number of the YubiKey that is inserted into the USB port of your computer. The decimal serial number is located on the right side of the tab.

8. If you want to hide the typed password, from the **Password** group, select **Hide Password**.
9. In the **Keyboard** list, select your keyboard layout language.
10. In **Password**, type your password, and:

    - If you want a Tab in your password, click **Insert Tab**.
    - If you want to correct or type your password again, click **Clear**.

    TIP: The total length of the password appears in **Password Length**.

11. To program the YubiKey in Scan Code mode, from the **Actions** group, click **Write Configuration**.

    TIP: When the YubiKey configuration is successful, a message displays at the top of the window confirming the configuration.

12. If you are programming multiple YubiKeys, do the following:

    a. Remove the YubiKey you just configured and insert another YubiKey to be configured into the USB port of your computer.

    b. Continue to configure the YubiKeys, one at a time, until you have finished configuring all your YubiKeys.

    c. If you did not select **Automatically program YubiKeys when inserted**, click **Write Configuration** each time you insert a new YubiKey.

13. Click **Stop** when you are finished configuring YubiKeys.

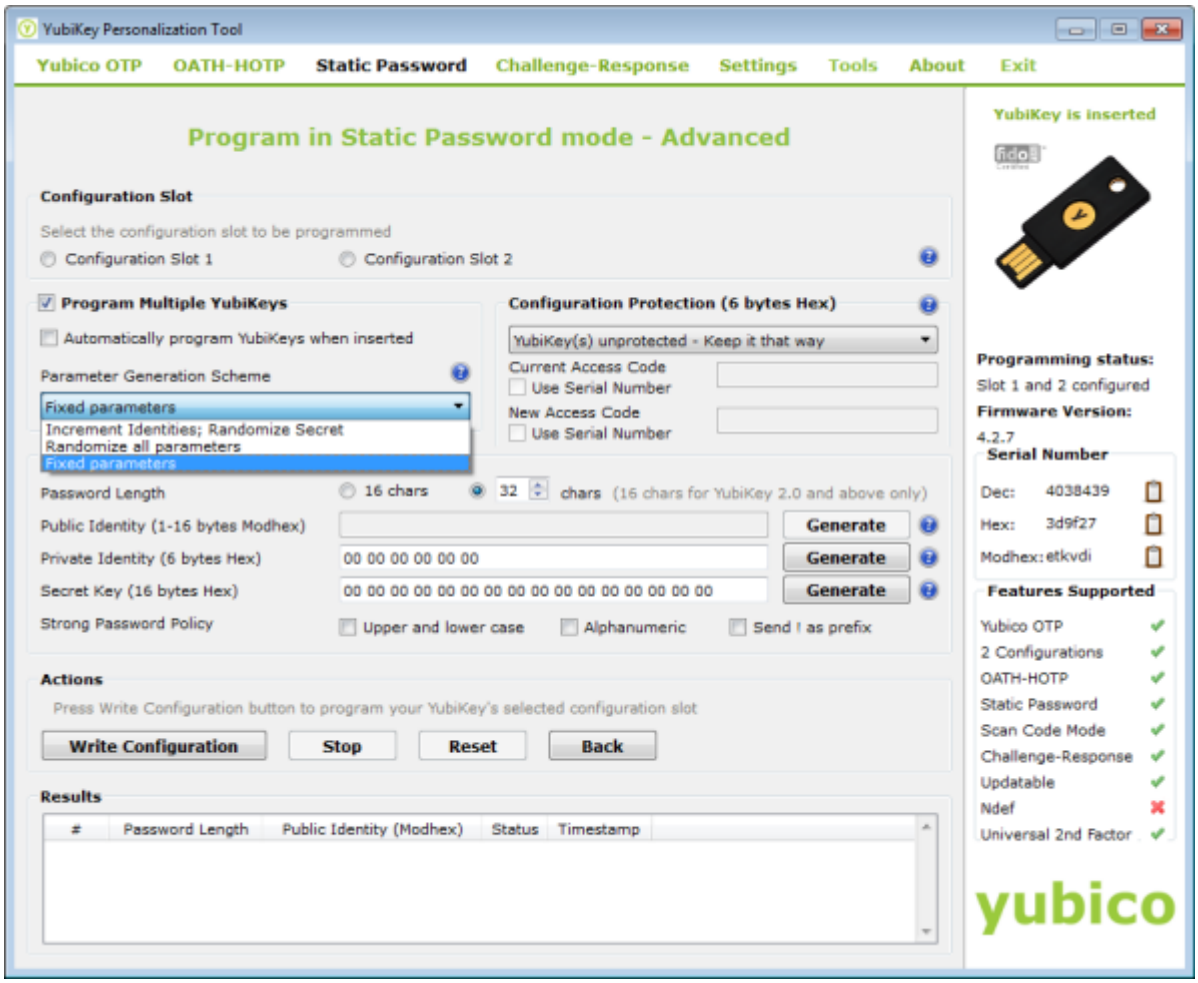
Configuring a YubiKey for Static Password Using the Advanced Option

YubiKeys 2.x and later provide a feature called Strong Password Policy. Using the Advanced option, you can program the YubiKey to generate very long static passwords with one uppercase letter, one capitalized letter, lowercase letters, numbers, and the ! special character.

When you program a YubiKey in Advanced mode for Static Password configuration, this password cannot be set by the user. The YubiKey Personalization Tool generates the static password using an encryption function involving the AES key and YubiKey parameters.

To configure a YubiKey for Static Password using the Advanced option

1. Launch the YubiKey Personalization Tool.
2. Insert a YubiKey into a USB port of your computer.
3. Click **Static Password** or **Static Password Mode**.
4. Click **Advanced**.
5. In the **Configuration Slot** group, select the YubiKey configuration slot that you want to configure.
6. If you want to program multiple YubiKeys, select **Program Multiple YubiKeys** and do one of the following:
   - If you want to automatically program each YubiKey when you insert it, select **Automatically program YubiKeys when inserted**.
   - If you want to click **Write Configuration** each time you insert a YubiKey, do not select **Automatically program YubiKeys when inserted**.
7. If you want to specify how the parameters used for programming the YubiKeys will be generated, in the **Parameter Generation Scheme** group, select one of the following:
   - **Increment Identities; Randomize Secret**
   - **Randomize all parameters**
   - **Fixed parameters**



8. In the **Configuration Protection** group, do one of the following:

   - To lock the configuration so that you must type an access code to make changes to the configuration, select one of the following:

     - **YubiKey(s) unprotected – Enable protection**
     - **YubiKey(s) protected – Disable protection**
     - **YubiKey(s) protected – Keep it that way**
     - **YubiKey(s) protected –Change access code**

   - If you do not want to use an access code, keep the default, **YubiKey(s) unprotected – Keep it that way**

9. To choose the type of access code to lock the YubiKey configuration, in the **Configuration Protection** group, do one of the following:

   - Type a twelve character hexadecimal access code.
   - Select **Use Serial Number**. This is the serial number of the YubiKey that is inserted into the USB port of your computer. The decimal serial number is located on the right side of the tab.

10. From the **Password Parameters** group, select the following options, as needed:

    a. Set the static **Password Length** (up to 64 characters in length):

    - To use only the **Public Identity** for the password, select **16 chars**.
    - To use the **Public Identity**, **Private Identity**, and the **AES Key** to generate the static password, select **33 chars** (or more).
      TIP: If **32 chars** is selected then **Public Identity** will not be used.

    b. Set the **Public Identity**, which is the first optional fixed part of the OTP string used to identify a YubiKey.

    - The **Public Identity** is required if the **Password Length** is set to 33 characters or more.
    - If used, be sure to type a length between 1 and 16 bytes:
        - By default, **Public Identity** is randomly generated and set to 6 bytes length.
        - Any length between 1 and 5 bytes is considered a private scope and will not create interoperability issues.
        - A **Public Identity** length of 6 bytes or more is for use with the Yubico validation server architecture or for future extensions.
        - If a customer prefix is set in the configuration, a **Public Identity** length of 6 bytes is enforced. In this case, the first three bytes contain the unique customer prefix. For more information about setting a unique customer prefix, see Using General Settings.
        - To regenerate the **Public Identity**, click **Generate**.
            - By default the **Public Identity** is generated as `0` (this is modhex character `c`, which is twelve `c`s: `cccccccccccc`), depending on the length of the password selected.
                - For example, if no input is provided, the **Public Identity** default is `cccccccccccc` (twelve `c`s).
                - As another example, if partial input is provided, such as a custom prefix, then each of the remaining characters defaults to the letter c (for example, with the custom prefix `eeee`, the Public Identity default would be `eeeecccccccc`, for a total of 12 characters).

    c. Set the **Private Identity**, which is required on this tab and is included as an input parameter in the OTP generation algorithm.

    - By default, it will be set to `0`.
    - To regenerate **Private Identity**, click **Generate**.

    d. Set the **Secret Key**, which is required and used to encrypt the OTP:

    - By default, it is randomly generated and set to `0`.

- To regenerate the **Secret Key**, click **Generate**.

11. In the **Strong Password Policy** group, select the applicable options.

12. To configure the YubiKey in Advanced static password mode, from the **Actions** group, click **Write Configuration**.
    TIP: When the YubiKey configuration is successful, a message displays at the top of the window confirming the configuration.

13. If you are programming multiple YubiKeys, do the following:

    a. Remove the YubiKey you just configured and insert another YubiKey to be configured into the USB port of your computer.

    b. Continue to configure the YubiKeys, one at a time, until you have finished configuring all your YubiKeys.

    c. If you did not select **Automatically program YubiKeys when inserted**, click **Write Configuration** each time you insert a new YubiKey.

14. Click **Stop** when you are finished configuring YubiKeys.

Creating a Challenge-Response Configuration

The Challenge-Response configuration enables interaction between the YubiKey and a client-side application and interface software, such as the YubiKey Client API. The Challenge-Response mode can be **Yubico OTP** compatible mode or **HMAC-SHA1**.

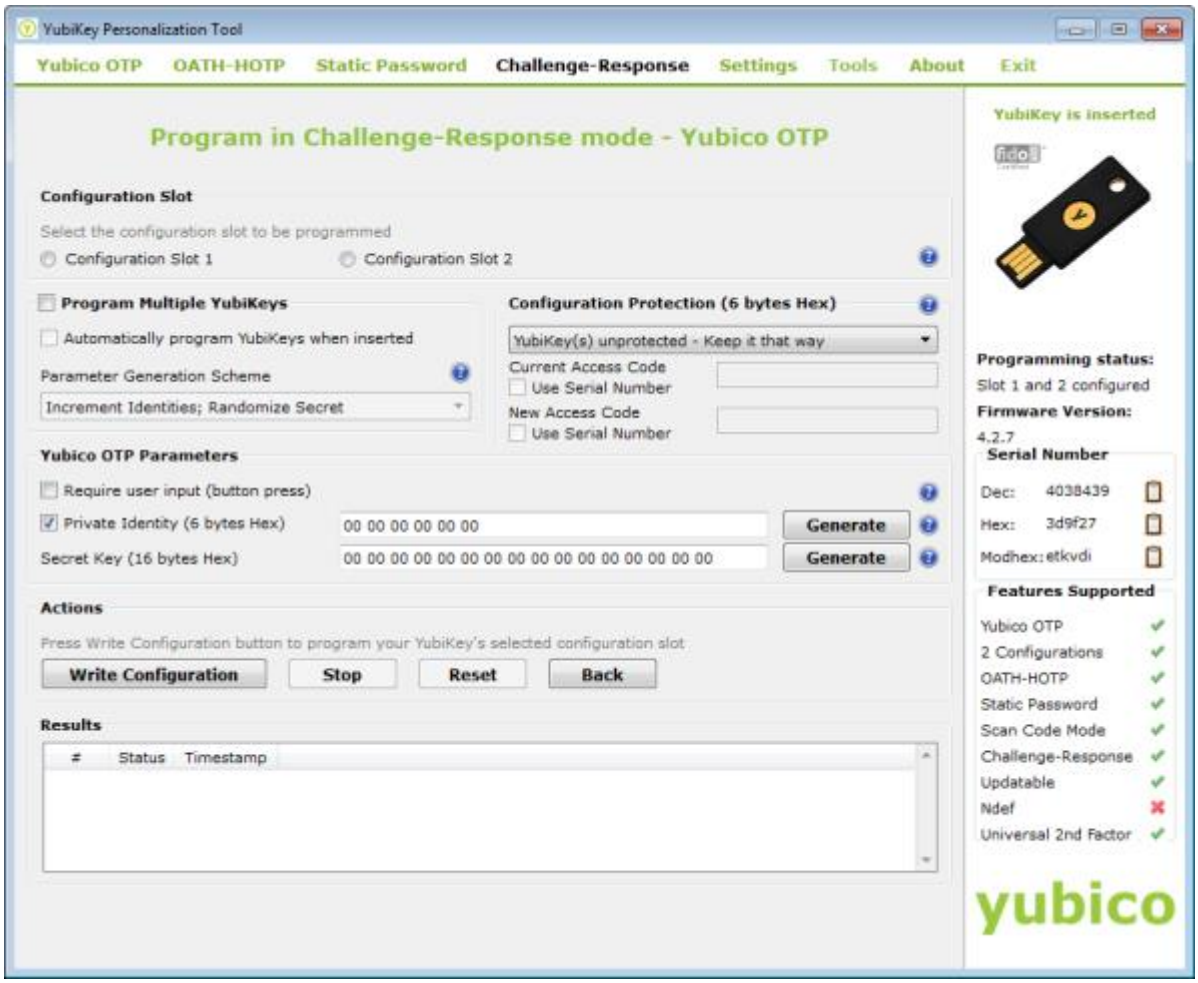
In this Chapter

Configuring a YubiKey for Challenge-Response Using Yubico OTP

The Yubico OTP Challenge-Response mode takes a 6-byte challenge and creates a response using the Yubico OTP algorithm. In this mode, the Yubico OTP includes the private identity of the YubiKey, counter and timer fields tracking how often the YubiKey has been used and the time between generating each OTP, a random number to add additional security to the encryption, and a closing CRD16 checksum of all fields. These variables create a different response each time even if the challenge is identical.

To configure a YubiKey for Challenge-Response using Yubico OTP

1. Launch the YubiKey Personalization Tool.
2. Insert the YubiKey into a USB port of your computer.
3. Click **Static Password** or **Static Password Mode**.
4. On the **Challenge-Response** tab, click **Yubico OTP**.
5. In the **Configuration Slot** group, select the YubiKey configuration slot that you want to configure.
6. If you want to program multiple YubiKeys, select **Program Multiple YubiKeys** and do one of the following:
    - If you want to automatically program each YubiKey when you insert it, select **Automatically program YubiKeys when inserted**.
    - If you want to click **Write Configuration** each time you insert a YubiKey, do not select **Automatically program YubiKeys when inserted**.
7. If you want to specify how the parameters used for programming the YubiKeys will be generated, in the **Parameter Generation Scheme** group, select one of the following:
    - **Increment Identities; Randomize Secret**
    - **Randomize all parameters**



8. In the **Configuration Protection** group, do one of the following:

    - To lock the configuration so that you must type an access code to make changes to the configuration, select one of the following:

        - **YubiKey(s) unprotected – Enable protection**
        - **YubiKey(s) protected – Disable protection**
        - **YubiKey(s) protected – Keep it that way**
        - **YubiKey(s) protected –Change access code**

    - If you do not want to use an access code, keep the default, **YubiKey(s) unprotected – Keep it that way**

9. To choose the type of access code to lock the YubiKey configuration, in the **Configuration Protection** group, do one of the following:

    - Type a twelve character hexadecimal access code.
    - Select **Use Serial Number**. This is the serial number of the YubiKey that is inserted into the USB port of your computer. The decimal serial number is located on the right side of the tab.

10. From the **Yubico OTP Parameters** group, select the following options, as needed:

    a. Set the **Private Identity**, which is required secret value included as an input parameter to the OTP generation algorithm:

        - By default, **Private Identity** is randomly generated and set to 6 bytes length.
        - To regenerate **Private Identity**, click **Generate**.

    b. Set the **Secret Key**, which is required and used to encrypt the OTP:

        - By default, **Secret Key** is randomly generated and set to 20 bytes length.
        - To regenerate the **Secret Key**, click **Generate**.

    c. For **Require user input**, do one of the following:

        - If you want users to press the button to generate the response to the challenge, select **Require user input**.
        - If you want the response to be generated automatically without user intervention, do *not* select **Require user input**.

11. To configure the YubiKey in Challenge-Response Yubico OTP mode, from the **Actions** group, click **Write Configuration**.
    TIP: When the YubiKey configuration is successful, a message displays at the top of the window confirming the configuration.

12. If you are programming multiple YubiKeys, do the following:

    a. Remove the YubiKey you just configured and insert another YubiKey to be configured into the USB port of your computer.

    b. Continue to configure the YubiKeys, one at a time, until you have finished configuring all your YubiKeys.

    c. If you did not select **Automatically program YubiKeys when inserted**, click **Write Configuration** each time you insert a new YubiKey.

13. Click **Stop** when you are finished configuring YubiKeys.

Configuring a YubiKey for Challenge-Response Using HMAC-SHA1

The HMAC-SHA1 Challenge-Response mode takes a 0-64 byte challenge and creates a HMAC using the HMAC-SHA1 algorithm in combination with a 20-byte Secret Key. In this mode, the YubiKey does not make use of any variables and generates an identical response each time if the challenge is the same.

To program a YubiKey for Challenge-Response using HMAC-SHA1

1. Launch the YubiKey Personalization Tool.
2. Insert a YubiKey into a USB port of your computer.
3. Click **Static Password** or **Static Password Mode**.

4. From **Program in Challenge-Response mode**, click **Yubico OTP**.

5. In the **Configuration Slot** group, select the YubiKey configuration slot that you want to configure.

6. If you want to program multiple YubiKeys, select **Program Multiple YubiKeys** and do one of the following:

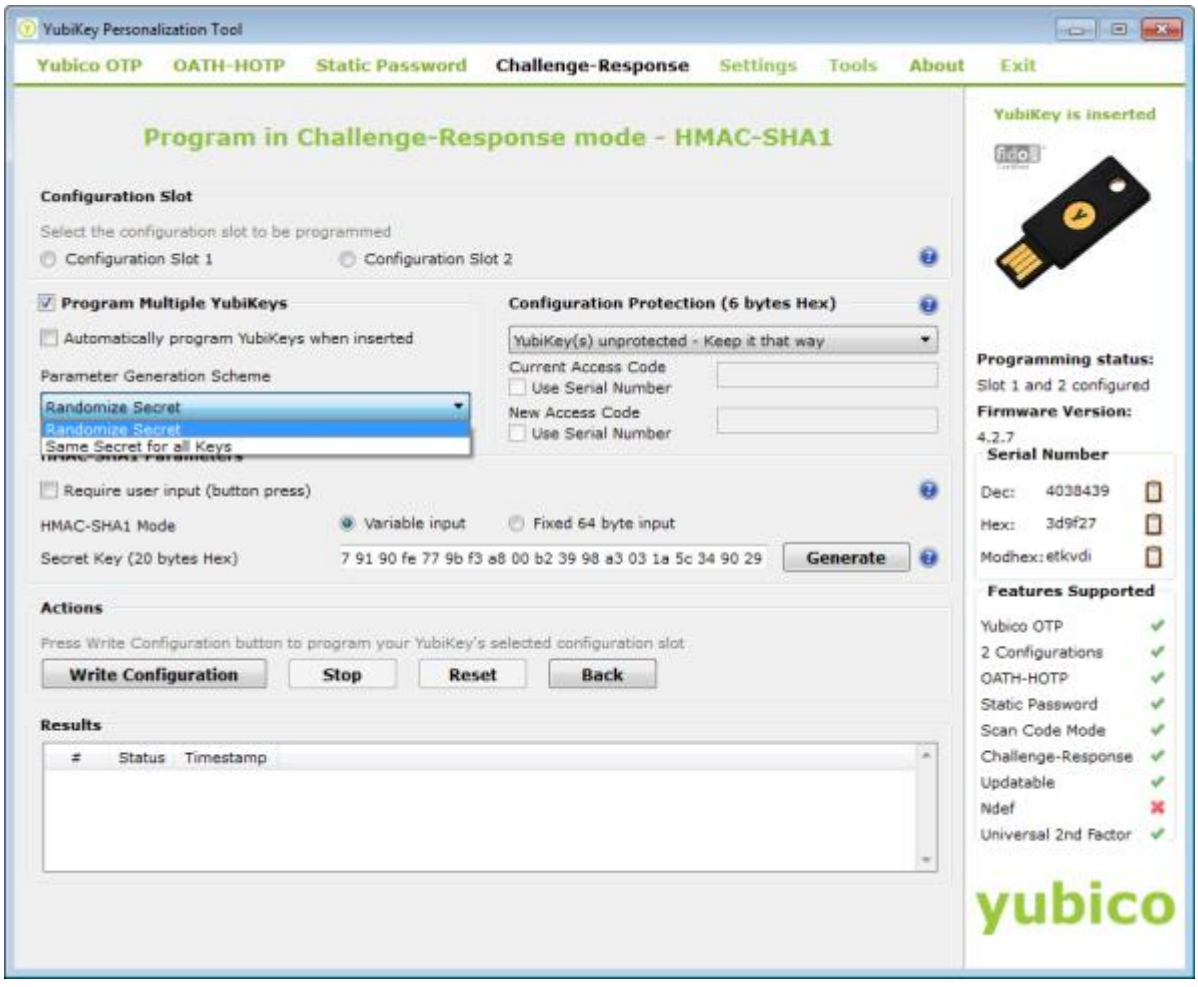
    - If you want to automatically program each YubiKey when you insert it, select **Automatically program YubiKeys when inserted**.

    - If you want to click **Write Configuration** each time you insert a YubiKey, do not select **Automatically program YubiKeys when inserted**.

7. If you want to specify how the parameters used for programming the YubiKeys will be generated, in the **Parameter Generation Scheme** group, select one of the following options:

    - **Randomize Secret**

    - **Same Secret for all Keys**



8. In the **Configuration Protection** group, do one of the following:

    - To lock the configuration so that you must type an access code to make changes to the configuration, select one of the following:

- **YubiKey(s) unprotected – Enable protection**
- **YubiKey(s) protected – Disable protection**
- **YubiKey(s) protected – Keep it that way**
- **YubiKey(s) protected –Change access code**

- If you do not want to use an access code, keep the default, **YubiKey(s) unprotected – Keep it that way**.

9. To choose the type of access code to lock the YubiKey configuration, in the **Configuration Protection** group, do one of the following:

   - Type a twelve character hexadecimal access code.
   - Select **Use Serial Number**. This is the serial number of the YubiKey that is inserted into the USB port of your computer. The decimal serial number is located on the right side of the tab.

10. In the **HMAC-SHA1 Parameters** group, select the following options as needed:

a. Do one of the following for **Require user input**:

- If you want users to press the button to generate the response to the challenge, select **Require user input**.
- If you want the response to be generated automatically without user intervention, do *not* select **Require user input**.

b. For **HMAC-SHA1 Mode**, select **Variable input** or **Fixed 64 bytes input**.

c. To regenerate the **Secret Key**, click **Generate**:

- The **Secret Key** is required and used to encrypt the OTP.
- By default, the **Secret Key** is randomly generated and set to 20 bytes length.

11. To configure the YubiKey for Challenge-Response in HMAC-SHA1 mode, from the **Actions** group, click **Write Configuration**.
TIP: When the YubiKey configuration is successful, a message displays at the top of the window confirming the configuration.

12. If you are programming multiple YubiKeys, do the following:

a. Remove the YubiKey you just configured and insert another YubiKey to be configured into the USB port of your computer.

b. Continue to configure the YubiKeys, one at a time, until you finish configuring all your YubiKeys.

c. If you did not select **Automatically program YubiKeys when inserted**, click **Write Configuration** each time you insert a new YubiKey.

13. Click **Stop** when you are finished configuring YubiKeys.

Specifying Settings Using the YubiKey Personalization Tool

This chapter describes the settings available on the **Settings** tab. The settings are common and applicable across all the configuration modes.

In this Chapter

Using General Settings

If your organization is using a customer prefix from Yubico, use the General Settings group to enforce its usage. You can type it in decimal, modhex, or hex formats.

Whenever the YubiKey generates a Yubico OTP, the YubiKey Personalization Tool always uses the customer prefix to replace the first four characters of the Public ID (the Public ID is part of the output string). If you do not use a customer prefix, the YubiKey Personalization Tool instead uses the default characters, `cccc`.

To use General Settings

1. If your organization has been issued, or is using, a custom prefix from Yubico, click **Use and enforce customer prefix**.
2. Type the customer prefix in the applicable field: **Decimal**, **Hex**, or **ModHex**.

Using Output Settings

Output Format specifies how the OTP will be emitted from the YubiKey. When any option is active, the corresponding button will have a blue background.

To specify the Output Format

- Select the following options, as needed:
  TIP: A blue background indicates that the option is selected.

a. To indicate that the first character emitted from the YubiKey will be a **Tab** keystroke, which is typically used to move the cursor to the next input field, click the first **Tab** (so that the first **Tab** is highlighted).

b. To separate the fixed (public identity) part and the OTP part of the OTP output, click the **Tab** between **Public ID** and **OTP**, which moves the cursor to the next input field.

c. To move the cursor to the next input field after the password (which adds a **Tab** keystroke to the end of the OTP part of the output), click the **Tab** to the right of **OTP**.

d. To indicate that **Enter** is the final keystroke, click **Enter**. This is typically used to trigger a default (OK) or to complete input from a command prompt.

e. To specify that the **Tab** or **Enter** keystroke should not be inserted during the OTP generation, click the corresponding button again (so that the button is not highlighted).

Using 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 your YubiKey outputs characters at full speed, with a key entry sent every 10 ms. Each complete keystroke represents a key-down and a key-up cycle, which means that about 50 characters per second can be sent to the host computer.

If there are issues with lost characters due to a too high character output rate (such as with BIOS keyboard drivers), you can slow down the output rate. This option is useful on slow or busy computers and servers.

To adjust Output Speed Throttling

1. Select one of the following options for **Output Character Rate**, as needed:

   a. To specify no delay, select **Standard**. This is the default option.

   b. To add a 20 ms additional delay for each keystroke (10 ms down and 10 ms up), select **Slow down by 20 ms**. Given a default endpoint poll rate of 10 ms, this option changes the rate to about 25 characters per second.

   c. To slow down the output by 40 ms, select **Slow down by 40 ms**.

   d. To slow down the output by 60 ms, select **Slow down by 60 ms**.

2. If you want to add a short delay before or after sending the OTP part, or both, select these options as needed:

   a. If you want to add a short delay before sending the OTP part, select **Add a short delay before sending the OTP part**. This is useful if there is some parsing or GUI rendering delays for a particular application.

   b. If you want to add a short delay after sending the OTP part, select **Add a short delay after sending the OTP part**.

Using Serial # Visibility Settings (YubiKeys Version 2.2 and Later)

Starting with YubiKeys version 2.2, a non-alterable, factory programmed unique serial number is included with each YubiKey. The serial number has no direct link to the public identities configured. You can enable the serial number feature when you program either configuration slot on the YubiKey.

To use Serial # Visibility Settings

- Select the following options, as needed:

a. To allow the serial number to be read at device power up, select **Button at startup**. Simply touch and hold the YubiKey while inserting the YubiKey into a USB port of your computer. Then release the YubiKey after one second and before five seconds elapse.
TIP: The YubiKey emits the serial number as a keystroke. We recommend that you keep a text editor or something similar open while performing this action so that you can capture the information.

b. If you want the device serial number visible in the serial number field in the USB device descriptor, select **USB descriptor**.
NOTE: The YubiKey must be removed and reinserted into the USB port of your computer after you select this option so that the operating system recognizes the updated device descriptor.

c. To allow the device serial number to be read using a client-side software application, such as the YubiKey Client API, select **API call**.

Using Static Password Settings (YubiKey Standard and YubiKey Nano)

This option enables you to update the device secret ID part of the static password and is useful for legacy password systems.

To enable manual update of the secret ID

1. Select **Enable manual update using the button (2.0+)**.

2. While touching your YubiKey, insert your YubiKey into a USB port of your computer, and continue holding the YubiKey for 8-15 seconds.
   NOTE: This option is available for YubiKey Standard and YubiKey Nano (this feature is not available for YubiKey Edge, YubiKey NEO, and YubiKey 4).

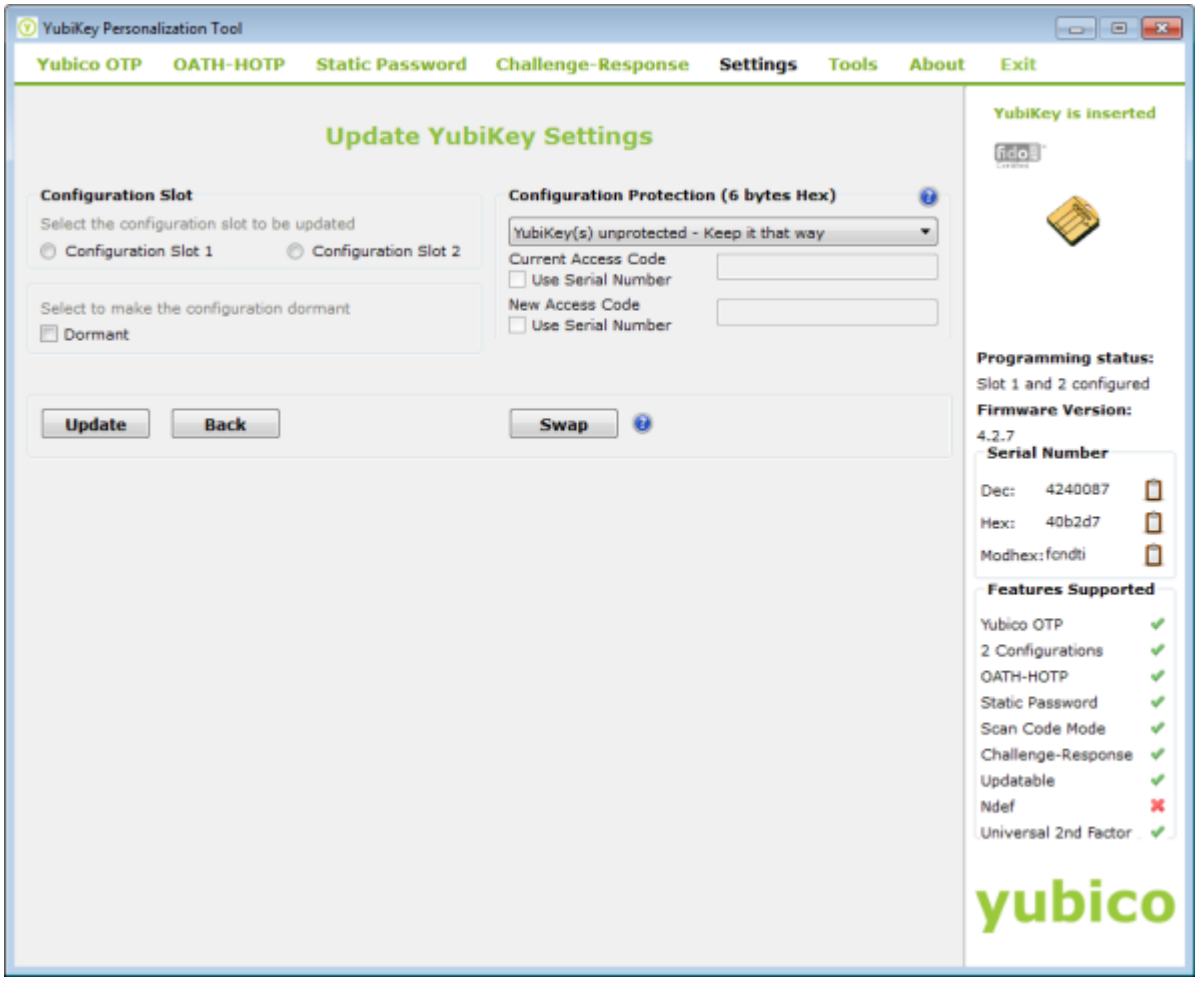
3. When the YubiKey LED flashes, touch the YubiKey once to confirm the update.
   The secret ID part of the static password is now updated with a new random number.

Using Update Settings (YubiKeys Version 2.3 and Later)

Starting with YubiKeys version 2.3 and later, you can update the settings on previously configured YubiKeys without overwriting the configurations stored in the slots. To do so, the configuration slot you want to update must be cycled through the dormant/active state on the **Update YubiKey Settings** window. You can update only the non-security settings when updating the configuration

To update the settings on previously configured YubiKeys without overwriting the configuration

1. On the **Settings** tab, click **Update**.



2. Select the slot to be updated, **Configuration Slot 1** or **Configuration Slot 2**.
   TIP: Only one configuration slot can be modified at a time.

3. The **Configuration Protection (6 bytes Hex)** group enables you to apply, modify or remove the access code preventing the modification of the YubiKey Configuration. Select one of the following:

   - **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**

   TIP: If an access code is required for updating this YubiKey, you must provide the access code prior to removing the requirement for the access code or before changing any other configuration protection.

4. Do one of the following:

   - To preserve the configuration of the selected configuration slot (the YubiKey will not be able to activate the preserved configuration), select **Dormant**.
   - To update the settings of the selected configuration slot without overwriting the current configuration, clear **Dormant**.

5. To update the selected configuration slot's settings without overwriting the configuration, click **Update**.

6. To swap the configurations stored in **Configuration Slot 1** and **Configuration Slot 2**, click **Swap**.

7. When you are finished updating this window and want to return to the **Settings** tab, click **Back**.

Using Extended Settings (YubiKeys Versions 2.3 and 2.4 and Later)

Starting with YubiKey versions 2.3 and 2.4, we introduced three new functions for generating output to host computers.

To use Extended Settings

- Select the following options as needed:

a. If you have a French or French-derived keyboard layout, select **Use numeric keypad for digits (2.3+)**. With this option active, any numeric character (0-9) will be generated using a keystroke corresponding to the number pad, instead of corresponding to the top line on the standard keyboard.
   NOTE: This option is a requirement for French and French-derived keyboard layouts.

b. To generate the output as soon as you touch the YubiKey, select **Use fast triggering if only slot 1 is programmed (2.3+)**. With this option enabled, the configuration in **Configuration Slot 1** of the YubiKey generates its output as soon as the YubiKey registers a touch.

c. To reverse the LED behavior, select **Invert led behavior (2.4/3.1+)**. With this option enabled, the LED emits light when you trigger the YubiKey; otherwise, the LED remains off.

Using Logging Settings

In Logging Settings, you can specify both the format for the log file and whether to record all the parameters used for programming the YubiKey in a log file.

To enable the Logging Settings

1. Select **Log configuration output**. You can store the log file anywhere on the system. Browse to your desired location.

2. Select the format for the log file. The log output file will be in `.csv` format.
   TIP: Each option for saving the log file organizes the data differently. The format for each option is `.csv`.

Using Application Settings

With this option enabled, after configuring a YubiKey with a Yubico OTP, OATH-HOTP, or Challenge-Response configuration, you can export the settings used for a template for future YubiKey configurations.

To enable the settings to be exported for a template for future YubiKeys

- Select **Enable configuration export and import (experimental)**.

Using Actions

The Actions option enables you to return any changes you've made on the **Settings** tab to the original default settings.

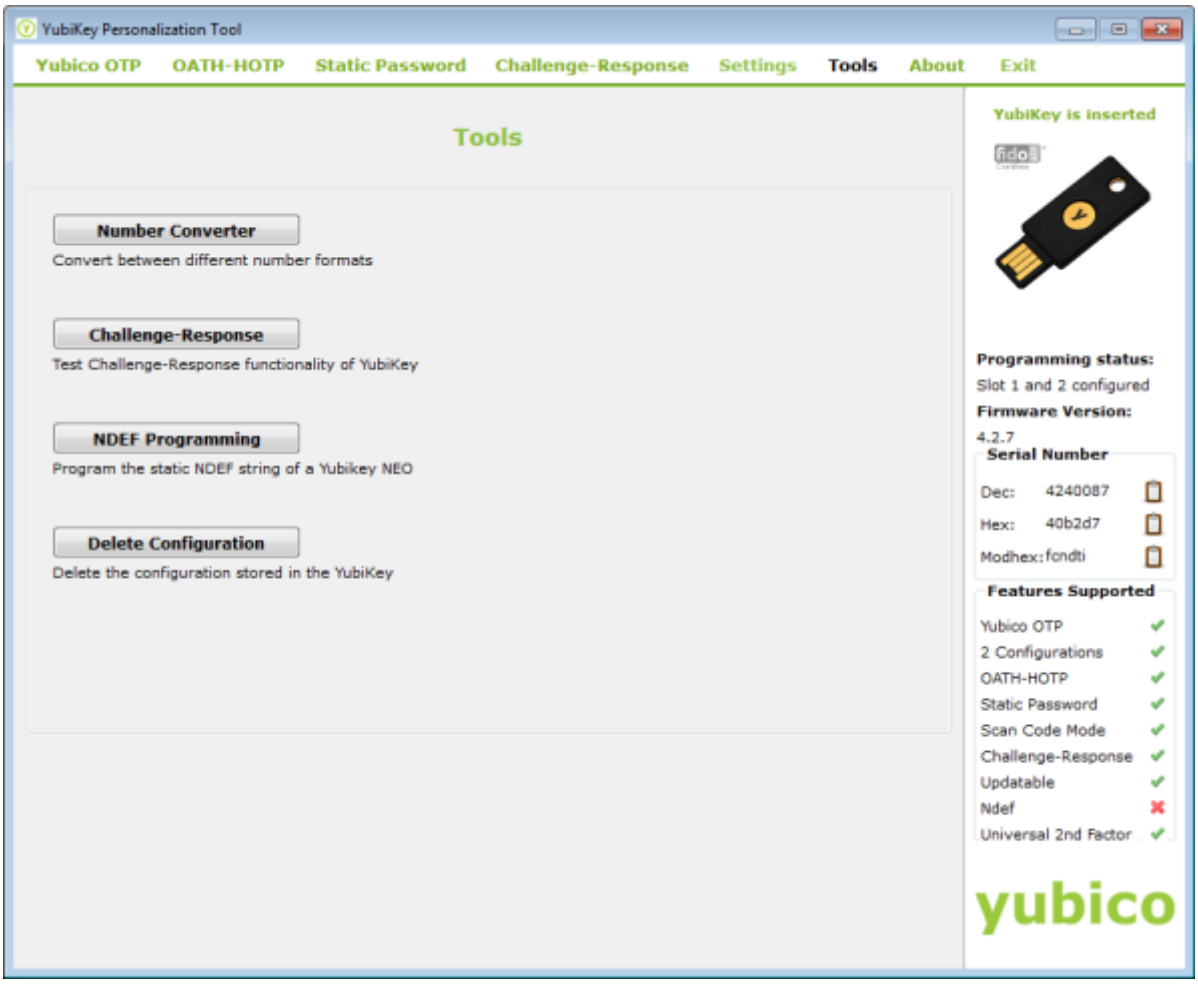
To return the Settings tab to the original settings

- In the **Actions** group, select **Return to Defaults**.

Using the Tools

The **Tools** tab includes four tools to help configure and test your YubiKeys.

In this Chapter

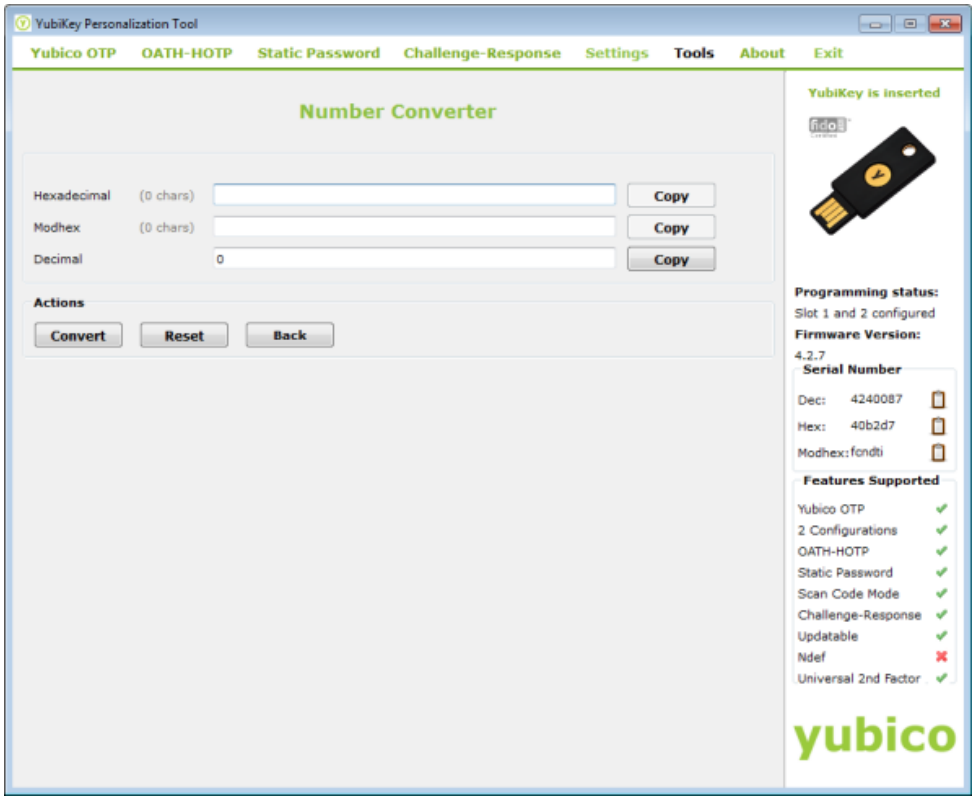


Using the Number Converter

The Number Converter provides a simple calculator to enable quick conversion between different numeric representation formats.

To use the Number Converter tool

1. In **Hexadecimal**, type a hexadecimal string. This field shows and accepts only non-delimited hexadecimal strings.
2. In **Modhex**, type a modhex string. This field shows and accepts only non-delimited modhex strings.
3. In **Decimal**, type a decimal:
   - This field accepts decimal input or shows the decimal conversion of the other modes.
   - The Number Converter uses the first four bytes to represent a 32-bit unsigned long integer (called a DWORD).
   - Byte ordering can be Little Endian (LSB leftmost) or Big Endian (MSB leftmost).
4. To convert the value that you typed to the other two formats, click **Convert**.
   TIP: Click **Reset** to clear all fields.
5. To return to the **Tools** tab, click **Back**.

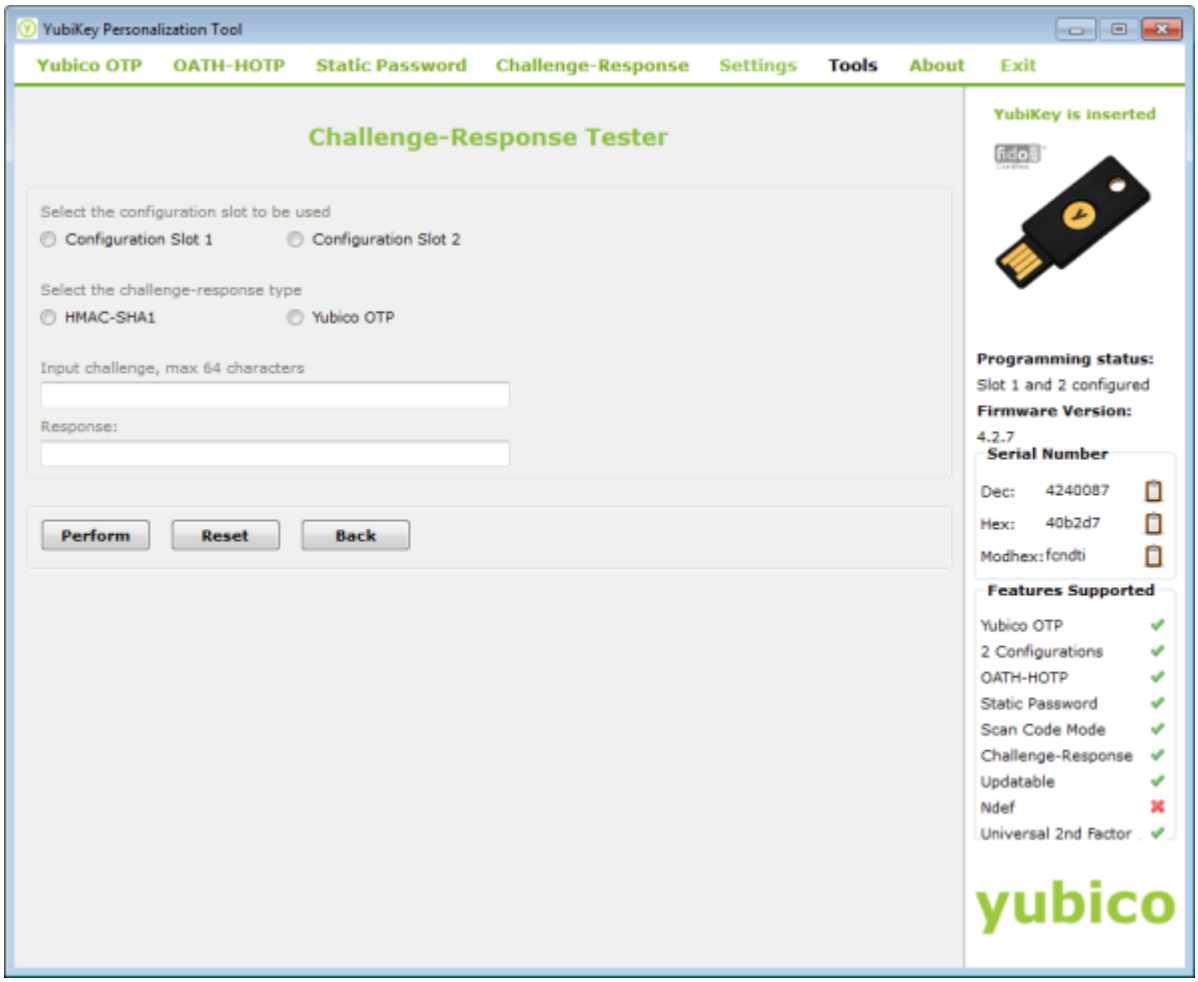


Using Challenge-Response

Use the Challenge-Response tool to test the Challenge-Response configuration of a YubiKey.

To test the Challenge-Response configuration of a YubiKey

1. From the **Tools** tab of the YubiKey Personalization Tool, click **Challenge-Response**.
2. In the **Configuration Slot** group, select the YubiKey configuration slot that you want to configure.
   TIP: Only one configuration slot can be selected at a time.
3. In **Select the challenge-response type**, select **HMAC-SHA1** or **Yubico OTP**, to match the challenge-response type of the YubiKey that you are testing.
4. In **Input challenge, max 64 characters**, type a challenge to be sent to your YubiKey. This field is optional.
5. To send the challenge to the YubiKey and view the response returned by the YubiKey, click **Perform**.
   Response displays the YubiKey's response to the challenge.
   TIP: Click **Reset** to clear all fields.
6. To return to the **Tools** tab, click **Back**.



Using NDEF Programming (For YubiKey NEOs Only)

When you are programing YubiKey NEOs, you can configure the NDEF output using the NDEF Programming tool. The NDEF output is the information transmitted through Near Field Communication. By default, the YubiKey NEO sends Configuration Slot 1 over NFC. You can change the YubiKey NEO to emit Configuration Slot 2 instead.

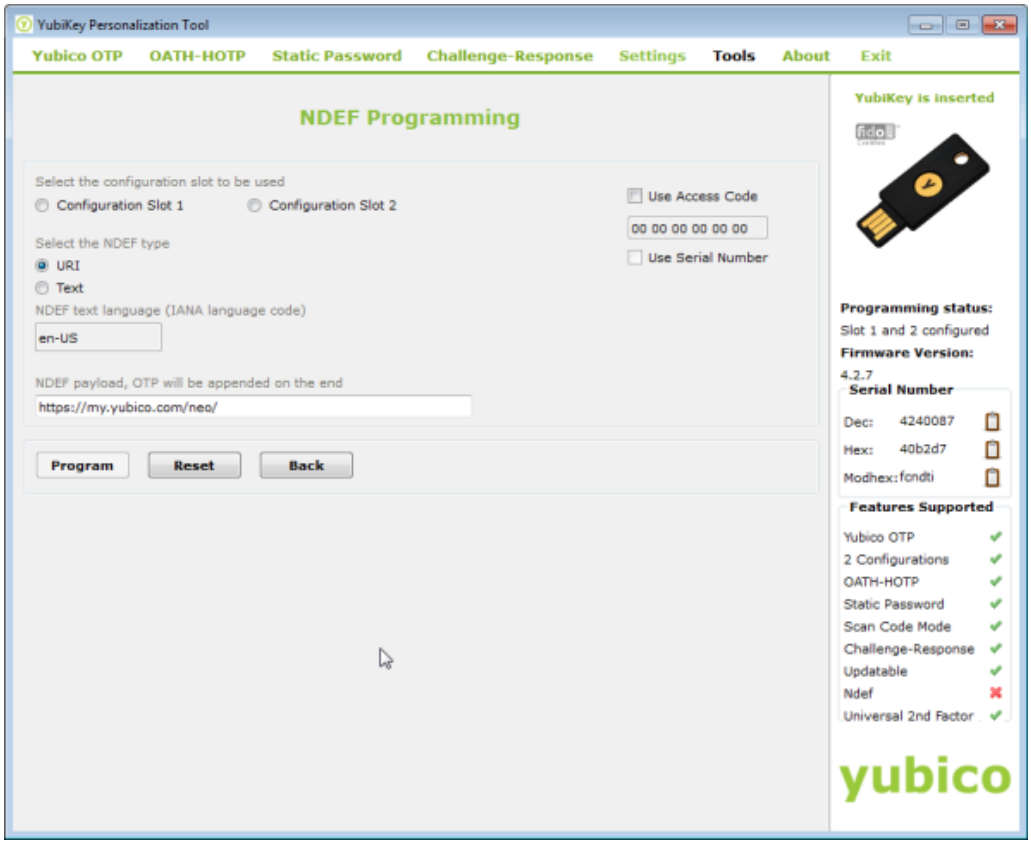
To configure the NDEF output of a YubiKey NEO

1. Insert a YubiKey NEO into a USB port of your computer.
2. From the **Tools** tab of the YubiKey Personalization Tool, click **NDEF Programming**.
3. To select the configuration slot to be used to generate the output for the NFC-transmitted information, select **Configuration Slot 1** or **Configuration Slot 2**.
4. If the selected configuration slot is locked with an access code, select **Use Access Code**.
5. When prompted, type the access code.
6. To select the **NDEF type**, do one of the following:

    - If you select **URI**, the **NDEF payload** stores the address of the website to open. This means the NDEF data will be transmitted as a website address. The OTP from the selected configuration slot will be added to the end of the text stored in **NDEF payload**.
    - If you select **Text**, **NDEF payload** stores the NFC tag as text. This means the NDEF data will be transmitted as an NFC tag. The OTP from the selected configuration slot will be added to the end of the text stored in **NDEF payload**.
    - If **Select the NDEF type** is set to **Text**, the **NDEF text language (IANA language code)** option enables you to set the language used through the IANA language code.
      TIP: Click **Reset** to clear all fields.

7. To configure the YubiKey NEO with the selected settings, click **Program**.

8. To return to the **Tools** tab, click **Back**.



Using Delete Configuration

This tool enables you to remove the configuration from the selected slot. If you are getting an error trying to write a new configuration to a configured slot, you can first delete the configuration and then save the new configuration to the now empty slot.

To remove the configuration stored in a YubiKey

1. Insert a YubiKey into a USB port of your computer. This is the YubiKey from which you want to remove a stored configuration.
2. From the **Tools** tab of the YubiKey Personalization Tool, click **Delete Configuration**.
3. To select the configuration slot from which to remove the stored configuration, select **Configuration Slot 1** or **Configuration Slot 2**.
   TIP: Only one configuration slot can be selected at a time. If a slot cannot be selected, insert a YubiKey into a USB port of your computer.
4. If an access code is required to delete the configuration, select **Use Access Code**.
5. To remove the configuration from the YubiKey that is inserted into the USB port of your computer, click **Delete**.
6. When prompted, type the access code.
7. To return to the **Tools** tab, click **Back**.