MyID MFA and PSM
Version 5.3.2

YubiKey Reprogramming Guide

Copyright

Conventions used in this document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important.
  - Bulleted lists are used when the order is unimportant or to show alternatives.
- **Bold** is used for menu items and for labels.

  For example:
  - Record a valid email address in **'From' email address**.
  - Select **Save** from the **File** menu.
- *Italic* is used for emphasis:

  For example:
  - Copy the file *before* starting the installation.
  - Do *not* remove the files before you have backed them up.
- ***Bold and italic*** hyperlinks are used to identify the titles of other documents.

  For example: "See the ***Release Notes*** for further information."

  Unless otherwise explicitly stated, all referenced documentation is available on the product installation media.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.
- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

  Warning: You must take a backup of your database before making any changes to it.

Contents

1 Introduction

This document describes the process for configuring your YubiKey device so that you can use it to authenticate YubiKey-generated One Time PINs (OTPs) locally, without requiring access to the Internet-based YubiKey servers for validation.

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.

1.1 Considerations

You must have MyID Multi-Factor Authentication (MFA) version 4 or above installed, configured, and fully operational. You must also provision all users issued with YubiKey devices with MyID One Time Codes (formerly known as PINpass) before customizing and provisioning YubiKeys for local MyID server validation.

2 YubiKey personalization

Intercede introduced the ability to process YubiKey generated one-time codes locally in MyID Multi-Factor Authentication version 4. Before you can use your YubiKeys locally without requiring them to be validated using the YubiKey published servers over the Internet, you must customize and configure the devices for MyID use.

The process described in this chapter generates a Comma Separated Value (CSV) file that you can import into MyID MFA.
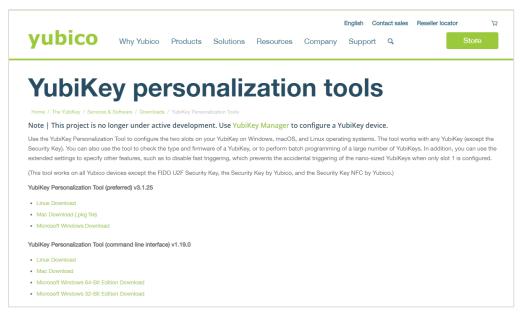
Note: If you do not customize the YubiKey according to the instructions in this chapter, YubiKey OTPs are still sent to YubiKey-hosted servers on the Internet, and no local server processing occurs. As such, outbound Internet access to the YubiKey servers is still required from the MyID Authentication servers.

2.1 Configuring YubiKey devices

You can carry out the customization using the YubiKey Personalization Tool.

You are recommended to use the Graphical User Interface version, not the command-line tool. You can download this tool from the YubiKey website:

www.yubico.com/products/services-software/download/yubikey-personalization-tools/
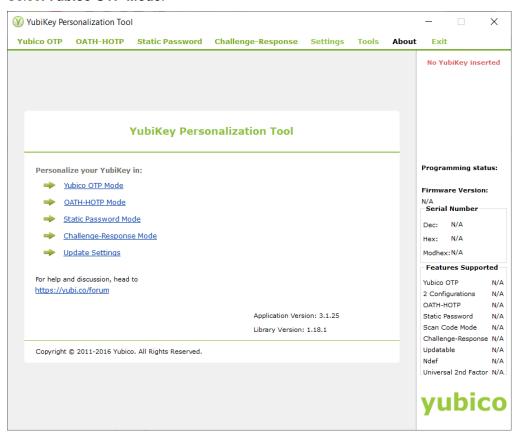
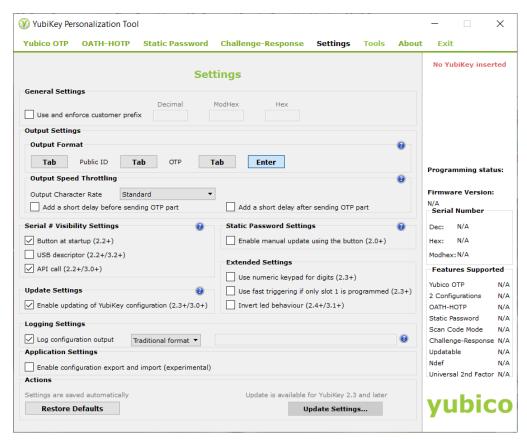To customize the YubiKey using the YubiKey Personalization Tool:

1. Ensure that no YubiKey devices are inserted into your workstation.

2. Launch the YubiKey Personalization Tool.

3. Select **Yubico OTP Mode**.
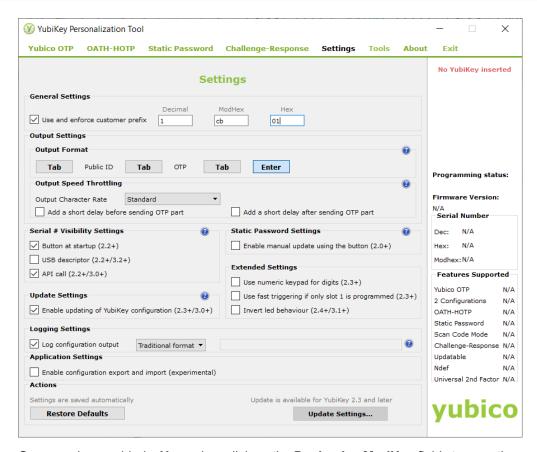

4. Select **Settings**.

5. In the **General Settings** section, enable the **Use and enforce customer prefix** option and specify a value between `01` and `FF` in the HEX field.
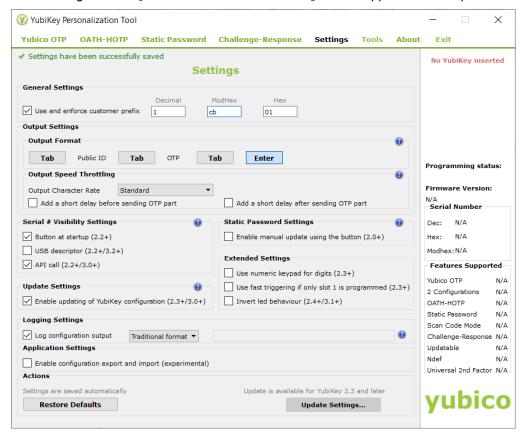
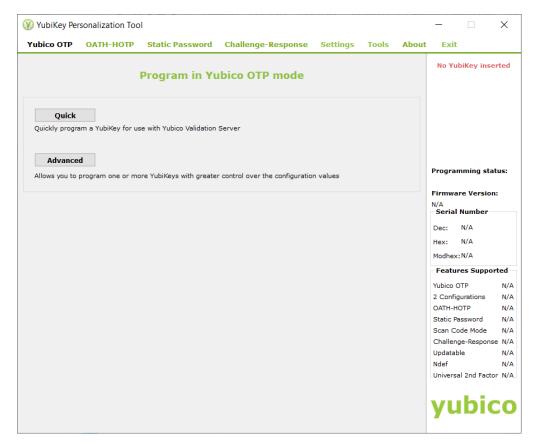6. Once you have added a **Hex** value, click on the **Decimal** or **ModHex** fields to save the settings.

The message `Settings have been successfully saved` appears in the top left.
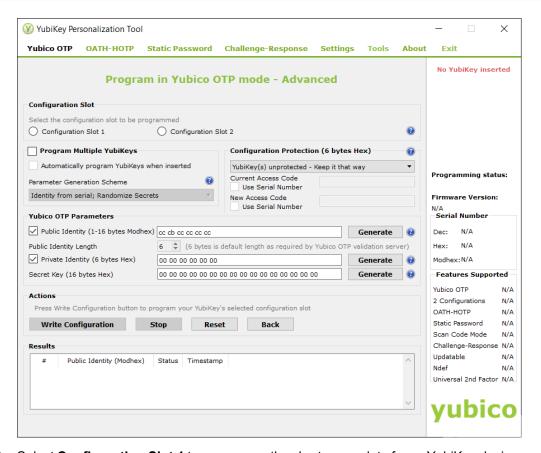

7. Select the **Yubico OTP** section.
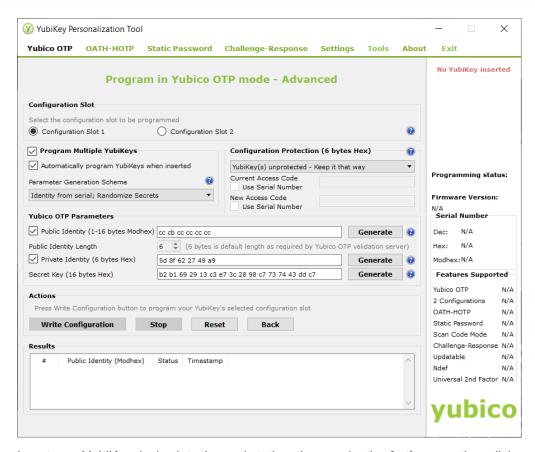
8. Select **Advanced**.

9. Select **Configuration Slot 1** to re-program the short press slot of your YubiKey device.

10. Enable the **Program Multiple YubiKeys** and **Automatically program YubiKeys when inserted** options.
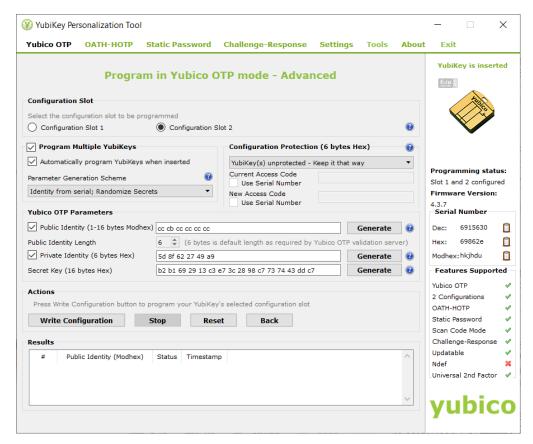
11. Insert your YubiKey device into the workstation, then, under the **Actions** section, click the **Write Configuration** option.
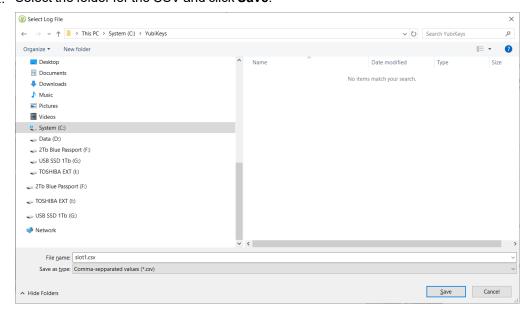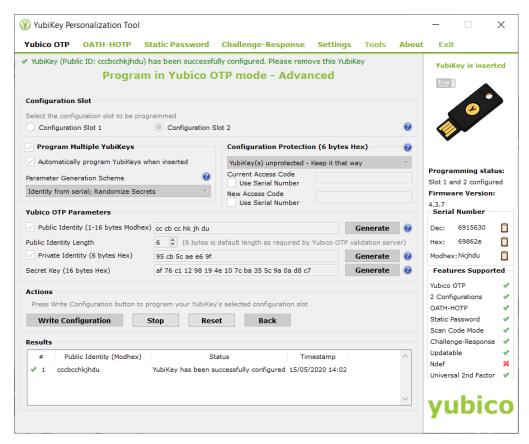
The tool creates a CSV file named `slot1.csv`.

12. Select the folder for the CSV and click **Save**.

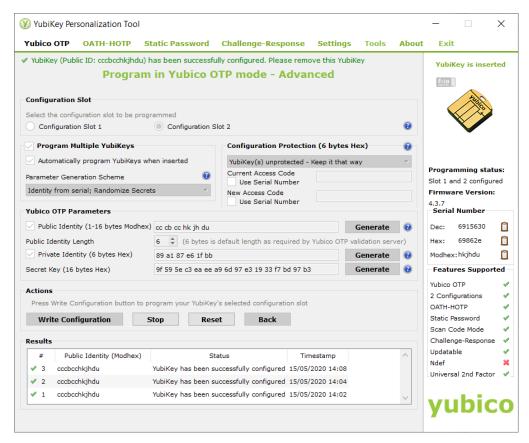The **Results** field reflects the changes to the YubiKey device.

13. Remove your YubiKey device and insert the next device.

    Each device you insert is reprogrammed with the details written to the CSV file you created.

    All new devices inserted are listed in the **Results** pane.

All your devices have now been reprogrammed, and the CSV file is ready to be imported into the MyID Authentication Server. For more information on importing this file, see the *YubiKey OTP Configuration Wizard* section of the *MyID Authentication Server Installation and Configuration Guide*.