

Multi-device configurator user's guide

YubiKey device Windows configuration component

Version: 1.0

Date: 28th April 2010

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.

Trademarks

Yubico and YubiKey are trademarks of Yubico AB.

Contact Information

Yubico AB
Mäster Samuelsgatan 60, 8 floor
111 21 Stockholm
Sweden
info@yubico.com

Contents

1	Document Information	4
1.1	Purpose	4
1.2	Audience	4
1.3	Related documentation	4
1.4	Document History	4
1.5	Definitions	4
2	Introduction	5
3	Preparing for use	6
3.1	USB port enumeration	8
3.2	Setting configuration options	11
4	Running the configuration utility	15
5	The configuration output file	18
5.1	Yubico OTP mode	18
5.2	OATH HOTP mode	19

1 Document Information

1.1 Purpose

The purpose of the multi-device configuration tool is to speed up configuration of Yubikey devices in small- to medium scale deployments without need for any specialized hardware.

This utility is intended as a complement to the Yubikey Configuration Utility, providing a higher throughput and a more structured workflow with a less degree of configuration flexibility.

For high volume deployments, ordering pre-configured Yubikeys is usually the most practical and cost efficient option. Contact sales@yubico.com for options regarding pre-configured Yubikeys.

The utility is currently available for Microsoft Windows only.

1.2 Audience

Systems integrators

1.3 Related documentation

- YubiKey Configuration Utility – The Configuration Tool for the YubiKey
- The YubiKey Manual – Usage, configuration and introduction of basic Yubikey concepts
- Yubico online forum – <http://forum.yubico.com>

1.4 Document History

Date	Version	Author	Activity
2010-04-19	0.1	JE	First draft
2010-04-28	1.0	JE	First release

1.5 Definitions

Term	Definition
YubiKey device	Yubico's authentication device for connection to the USB port
USB	Universal Serial Bus
HID	Human Interface Description. A specification of typical USB devices used for human interaction, such as keyboards, mice, joysticks etc.
API	Application Programmer Interface, the software module that communicates with the IPP and provides an interface to the User Program
COM	Component Object Model – a component based programming model developed by Microsoft.
AES	Advanced Encryption Standard. A NIST approved symmetric encryption algorithm.
OATH-HOTP	Initiative for Open Authentication (RFC 4226)

2 Introduction

Although the standard Yubikey Configuration Utility provides means to sequentially configure Yubikeys, the slow operating system response in recognizing device insertions and removals can make this process painstakingly slow.

The Yubikey Multi-device configuration utility allows a reasonably high throughput for custom configuration of non-preconfigured Yubikeys, without the need for any specialized hardware. An ordinary off-the-shelf USB hub or even a built-in computer root hub is sufficient, i.e. no external hub is necessary.

The user determines the number of USB ports needed for the most practical setup.



In this case, two standard low-cost, off-the-shelf 5-ports hubs forms a 10-set batch setup. The operator then inserts the Yubikeys one by one in the hub ports and configuration then starts automatically. By the time the last key has been inserted, the first ones have their configuration completed. As these are removed the last ones become ready as well.

With this setup, the workflow can be outlined as:

1. Insert blank Yubikeys from right to left
2. When the last Yubikey has been inserted, remove the finished Yubikeys from right to left.
3. When all keys have been removed, repeat from step one

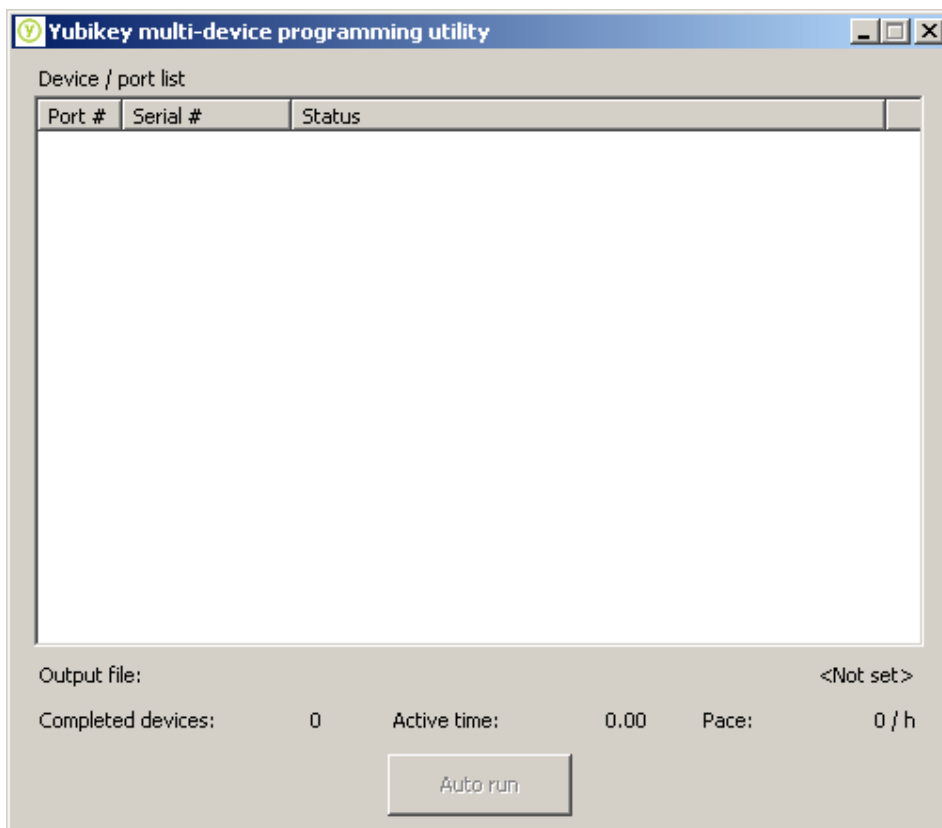
Apart from practically eliminating waiting time, the workflow of separating the tasks of insertion, removal and handling of finished Yubikeys typically reduces errors.

3 Preparing for use

The application is a single file executable that does not need any particular installation steps.

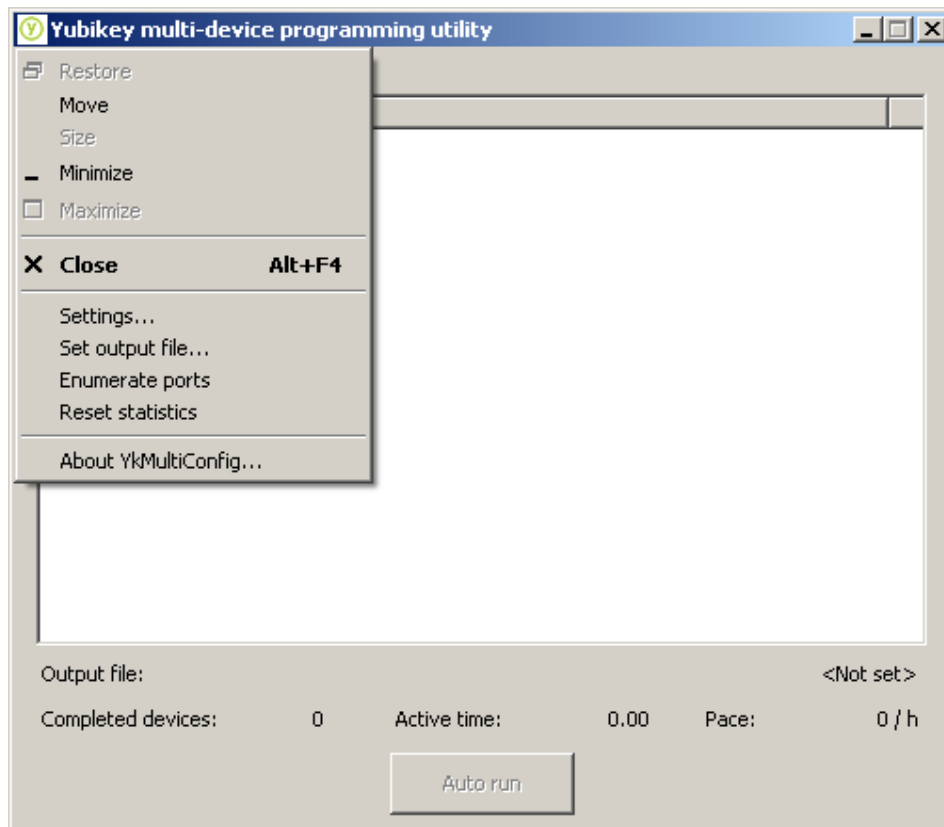
Start the application by invoking the executable `ykMultiConfig.exe`

The main working screen appears:



Here, no USB ports are assigned and the "Auto run" button is therefore disabled. The process of assigning USB ports is called "enumeration" and is further described in section 3.1.

A menu is accessible under the system menu under the Yubico logo in the upper right corner of the caption bar.

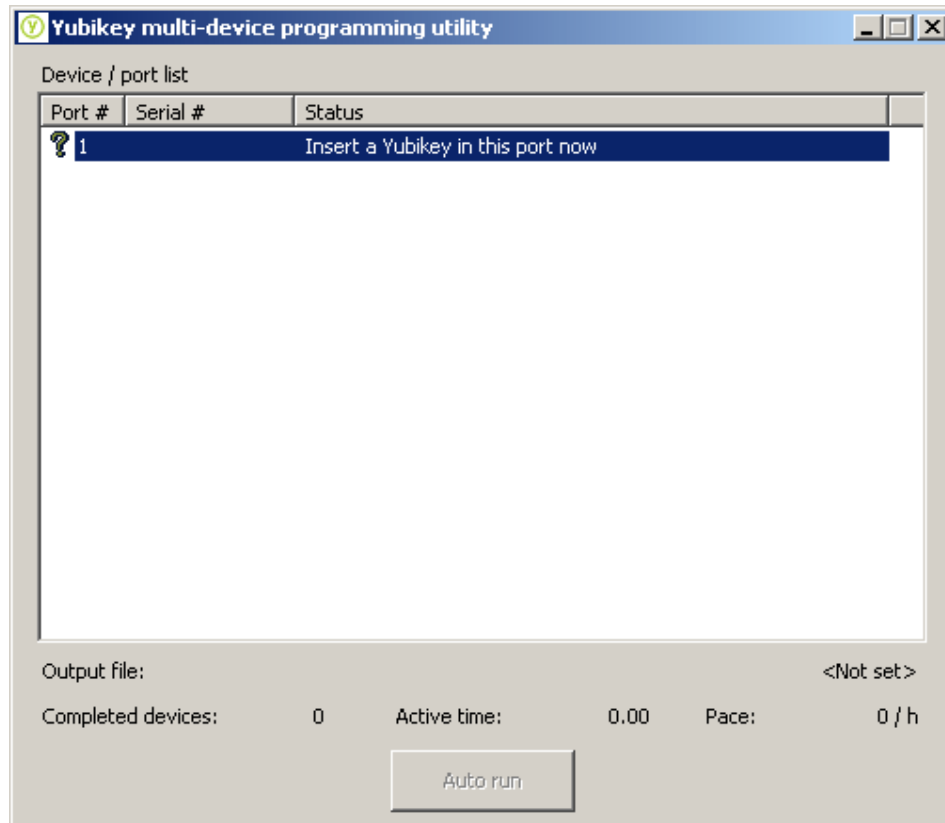


A traditional program "about box" is available, showing program version and build information.

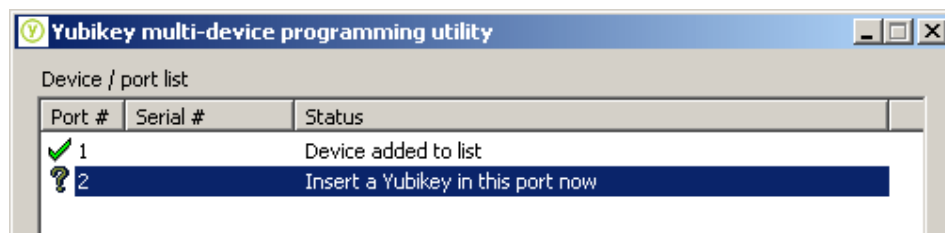


3.1 USB port enumeration

Before the configuration can begin, an association between each physical USB port present in the system with a logical sequence number must be made. This process is called enumeration and is invoked by selecting "Enumerate ports" from the system menu.



Here, the program prompts the user to insert a Yubikey in the USB port that will be assigned port sequence number 1. When a Yubikey is inserted and recognized, the process is repeated



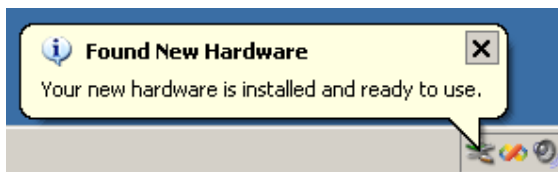
Continue to insert Yubikeys into the desired number of USB ports.

Just insert one Yubikey at a time and wait for it to be recognized by the application before inserting next. The same YubiKey can be used for each port. The YubiKey does not need to be programmed.

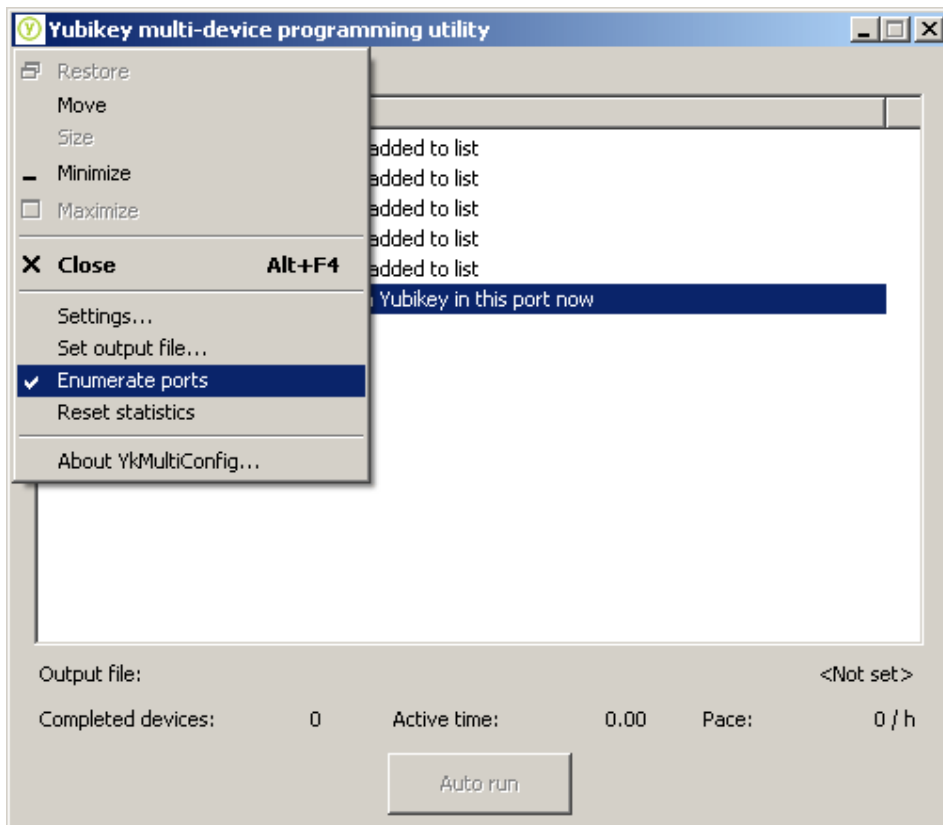
Please note that the first time a Yubikey is inserted into a specific USB port, the operating system will search for the appropriate HID driver for it. This takes a few seconds to complete and is only done once.



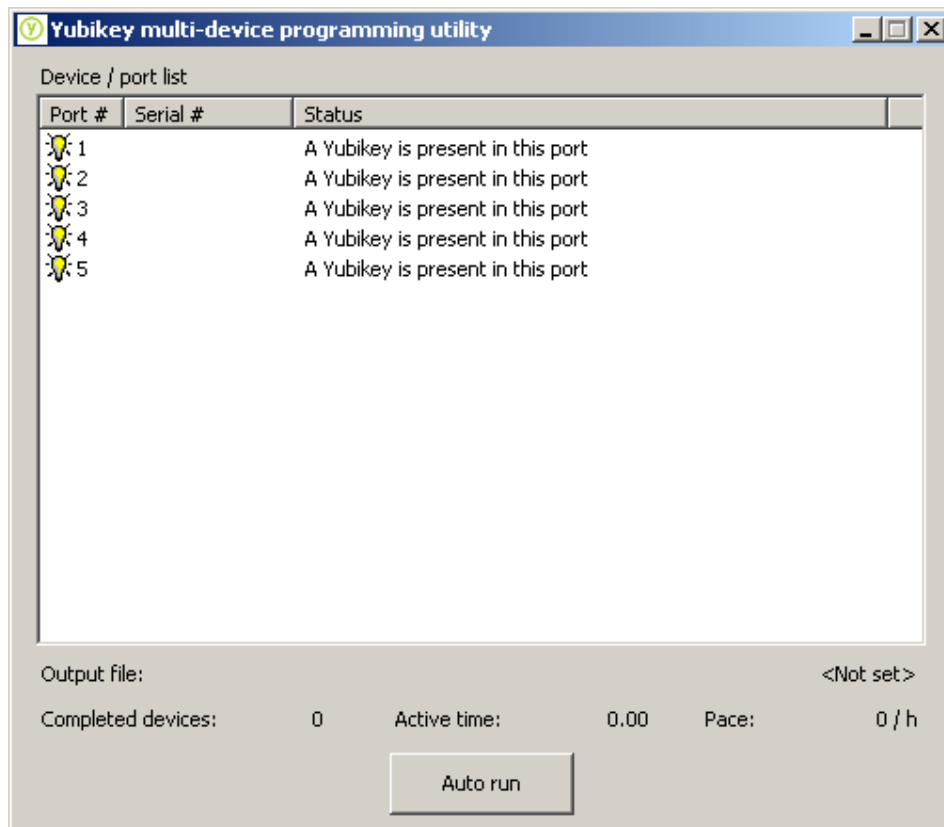
In this case, simply wait for the device to be fully recognized before inserting next device.



When finished, select "Enumerate ports" again from the system menu to complete the enumeration process.



In this example, five ports have been assigned. When the enumeration is finished, the program switches back to the idle screen:



Now, the Auto run button becomes enabled and the configuration can begin.

There is no application limit for the number of devices that can be assigned. Enumeration only needs to be performed once as the configuration will be saved by the program.

3.2 Setting configuration options

Before starting the configuration, first review the "Settings..." panel, available from the system menu.

The screenshot shows the 'Settings' dialog box with the following configuration:

- Configuration options:**
 - Erase configuration
 - Yubico OTP with 12 digit public ID
 - OATH HOTP
 - Use second configuration
 - Password protect configuration
 - Use 8 rather than 6 digits HOTP
 - Use OATH token identifier
- Customer prefix:** 220
- Serial number:** 100
- Sample id:** ub9022000100
- Mode of operation:**
 - Wait for all removed before restart
 - Remember output path
 - Don't overwrite existing configuration
- Optional sound alerts:**
 - Success: C:\WINDOWS\Media\ding.wav
 - Failure: C:\WINDOWS\Media\chord.wav
 - Device prog: C:\WINDOWS\Media\Windows XP Balloon.wav
- Optional shell execute command at success:**
 - Path to exec: C:\TEMP\printer2.exe
 - Execute for each device
 - Include public / token id
 - Test button

Configuration options

Here, the desired configuration type is selected

- Erase configuration – used to erase a configuration in a set of keys
- Yubico OTP – assigns a default Yubico 12 + 32 character OTP
- OATH HOTP – assigns a OATH HOTP

NOTE: This feature requires device firmware version 2.1.0 or later

- Use second configuration – Writes configuration to the second configuration slot rather than the first one

- Password protect configuration – Generate and set a random password to the configuration

CAUTION: *Enabling the password protection can effectively make the keys "read only" if the configuration password is lost. Only enable this option if you're fully aware of the implications of using it.*

- Use 8 rather than 6 digits HOTP – available for OATH HOTP mode only.
- Use OATH token identifier – assigns a OATH token identifier in the format ub <pppp> <sssss> formed by the customer prefix and the serial number fields.
- Customer prefix – enter the customer prefix for your particular range of Yubikeys. A customer prefix can be obtained free of charge from Yubico. Instructions on how obtain a customer prefix can be found on the Developer's page at www.yubico.com

Customer prefixes 1 to 9 are available for test and are not assigned. If you don't have a customer prefix, use these for test if needed.

- Serial number – assign the starting serial number here. This number is incremented by one for each Yubikey being successfully configured. Serial numbers range from 0 to 2^{24} (approx 16,000,000) for Yubikey OTP and 10^4 (100,000) for HOTP.
- Sample id – Shows the encoded identity with the current prefix and serial number.

The disposition of the resulting public ID or OATH token identifier is described further in section 5

Mode of operation

Here, operational parameters can be set

- Wait for all removed before restart – With this option set, the configuration will be suspended until all configured devices have been removed. Depending on the workflow, this can prevent operator errors
- Remember output path – Normally the output file is prompted for each time the application is invoked. With this option set, the output file is maintained when the application is closed.
- Don't overwrite existing configuration – With this option set, the application ensures that each device is not already configured before the new configuration is written.

NOTE: *When using version 2.0.x firmware versions, the firmware does not report which of the two (or both) of the two configurations are set. Therefore, this feature does not work properly for version 2.0.x firmware versions.*

Optional sound alerts

Here, optional sound alerts can be assigned to simplify the workflow by giving audio signals of events. It is recommended to use these sound alerts in production programming.

- Success – played when an operation has been completed successfully
- Failure – played when an operation has ended up in a failure
- Device prog – played for each device being successfully configured

Optional shell execute command at success

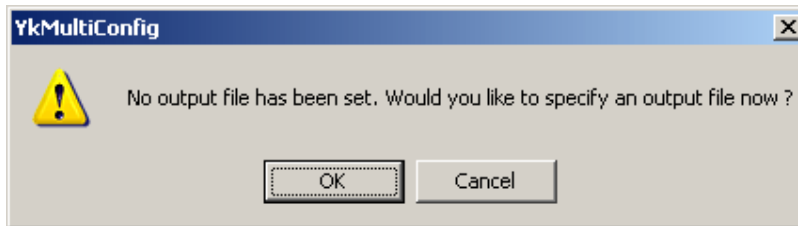
This allows a custom executable, such as a label printing application to be invoked for each successful configuration. Serial numbers are passed as arguments

- Path to exec – This specifies the path to the executable to be launched
- Execute for each device – With this option set, the application is invoked for each device being successfully configured. The default is that the application is invoked when all devices in a set has been completed
- Include public / token id – With this set, the public id is passed as an argument as well

4 Running the configuration utility

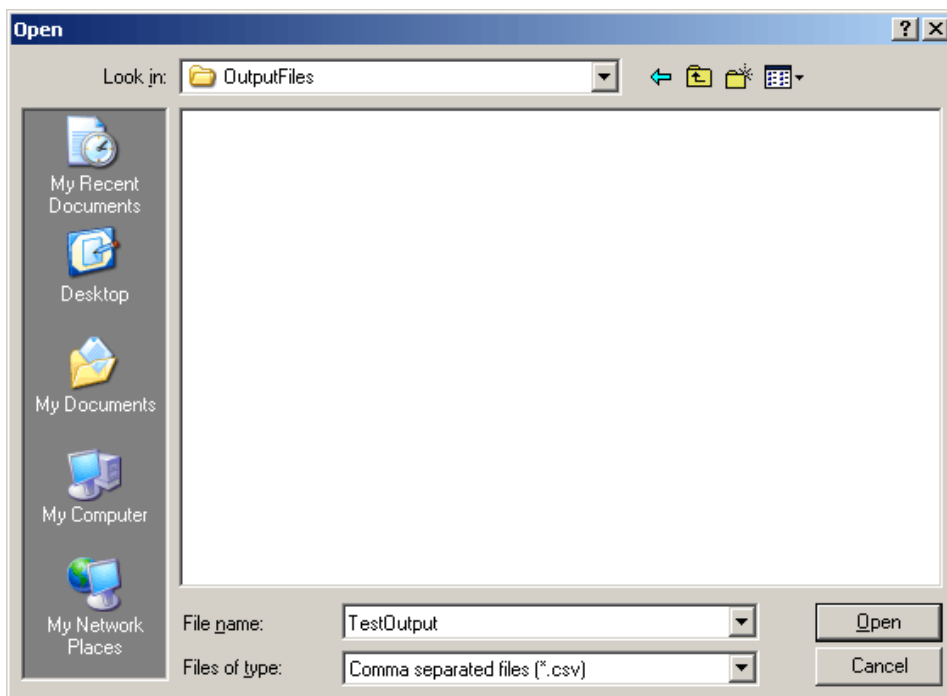
When the enumeration is completed (section 3.1) and the desired settings have been set (section 3.2), the application is ready to start device configuration

Press the "Auto run" button



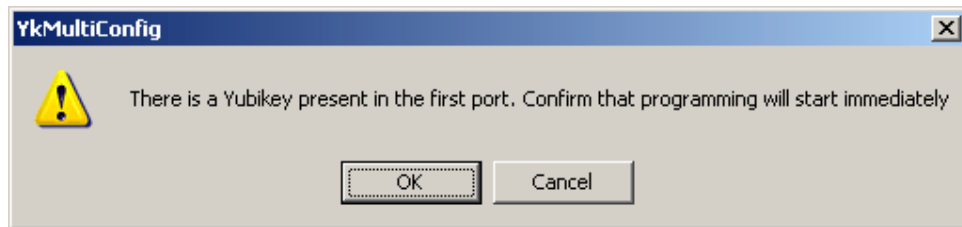
In order to proceed, an output file storing the generated device configuration (see section 5) must be set. The default action is that the output file is set every time the application is invoked. If the user wants the output file settings to be persistent, this can be configured (see section 3.2)

Press OK and a file dialog is displayed

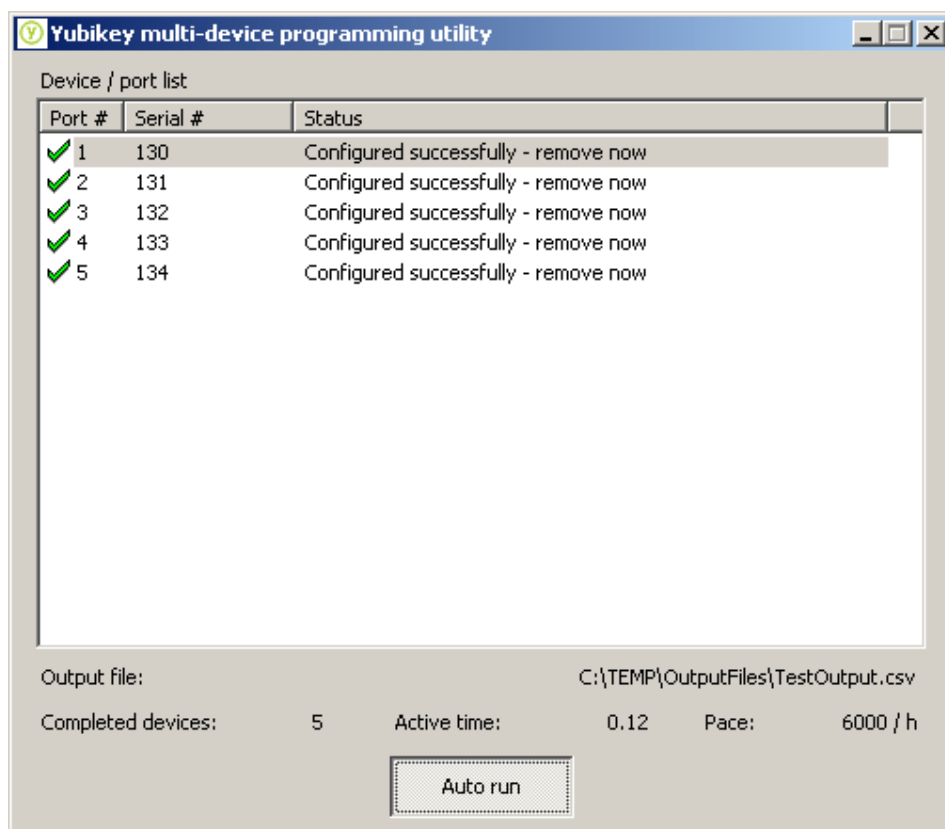


Enter a valid file name and press Open to proceed

In this case, there is a Yubikey in the first enumerated USB port. In order to protect anything from being accidentally overwritten, the user is prompted to confirm that the configuration will start immediately.

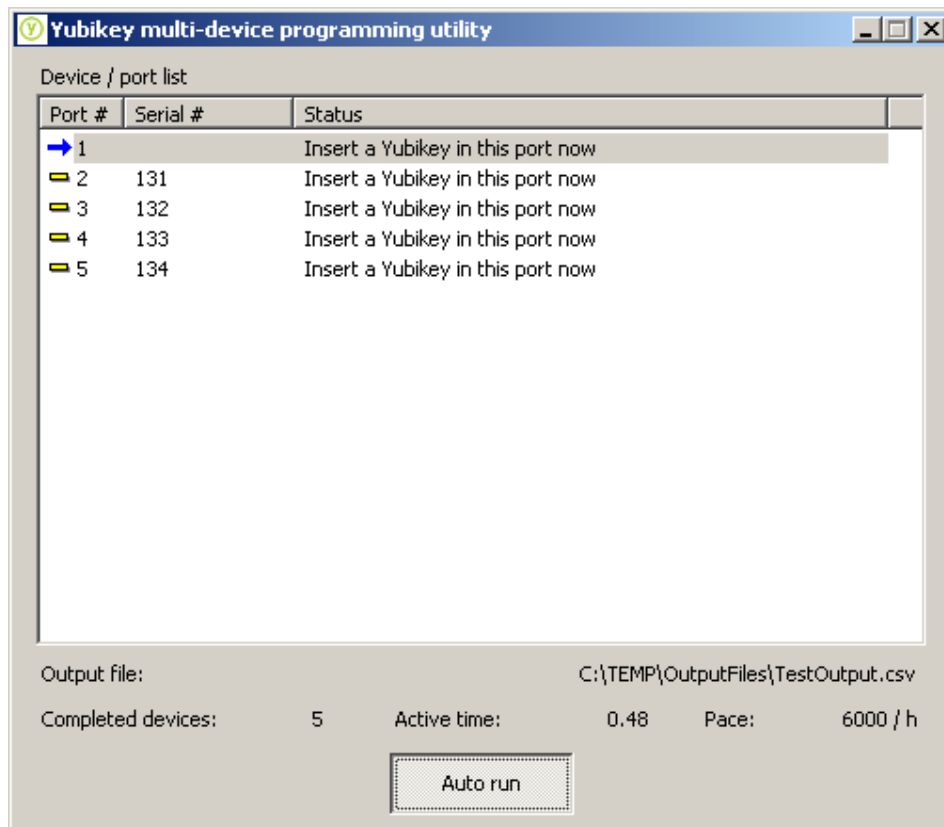


Press OK and the configuration starts



The devices are now configured sequentially and are ready to be removed.

When removed, the application prompts for the next set of Yubikeys to be inserted



Insert the keys in the sequence of choice – the application will configure the devices in sequential order anyway.

For each device being configured, the statistics is updated:

Completed devices:	15	Active time:	1.58	Pace:	500 / h
--------------------	----	--------------	------	-------	---------

Here, 15 devices have passed in 1 minute and 58 seconds. At the current rate, 500 devices per hour would be completed. Please note that due to the nature of this simple calculation, the pace field will show unrealistic values for the first couple of set until a proper history has been built.

The Active time is triggered by activity. If nothing has been done for 3 minutes, the active time is halted. It is automatically restarted when the configuration operation is continued.

5 The configuration output file

The data generated as a result of the configuration operations is written as comma separated text files with the following formats

5.1 Yubico OTP mode

Sample file

```
120,djctrccccij,f560c6f21a96,af620ec093747719584e917fee2f1db,000000000000,20  
10-04-19T01:47:45,
```

```
121,djctrccccik,c3282e1fe189,bc2737a312852ac69e071236280d436c,000000000000,20  
10-04-19T01:47:46,
```

```
122,djctrccccil,472bef38a6a3,8c31581d784162182a2a876cfe6ca36b,000000000000,20  
10-04-19T01:47:46,
```

The fields are:

- Numeric serial number
- Modhex public id (12 digits = 6 bytes)
 - Offset 0: Pre-defined customer prefix code 'dj' (=0x28)
 - Offset 1: Customer prefix, high part (bits 8..15)
 - Offset 2: Customer prefix, high part (bits 0..7)
 - Offset 3: Serial number high (bits 16..23)
 - Offset 4: Serial number high (bits 8..15)
 - Offset 5: Serial number high (bits 0..7)
- Private id (12 hex digits = 6 bytes)
- AES key (32 hex digits = 16 bytes)
- Configuration password (12 hex digits = 6 bytes). All zeroes if not set.
- Time of configuration timestamp

5.2 OATH HOTP mode

Sample file

```
125,ub9020000125,0,7e4baa15979ee53e2695bed18a10259f4bd6ebd5,000000000000,2010-04-19T01:48:51,
```

```
126,ub9020000126,0,56f5ef6185bbdceb89e166182692c041e8d2f5e,000000000000,2010-04-19T01:48:51,
```

```
127,ub9020000127,0,cd2d5946fb302a74860365ec8acc38cfb8ef5981,000000000000,2010-04-19T01:48:52,
```

The fields are:

- Numeric serial number
- Token identifier with Yubico prefix 'ub' and token type 9x concatenated with customer prefix and serial number
- Initial moving factor (always zero for 2.1.x Yubikeys)
- Secret (40 hex digits = 20 bytes)
- Configuration password (12 hex digits = 6 bytes). All zeroes if not set.
- Time of configuration timestamp