mike@csis.dk

# Contents

# Introduction

This manual describes the CSIS Enrollment Station located at https://github.com/CSIS/EnrollmentStation. The Enrollment Station was created to facilitate enrollment of Yubico Smartcards (specifically using the Yubikey NEO Premium with CCID functionality) using a Windows AD CS (Active Directory Certificate Services) CA.

The current version of the Enrollment Station is coded in C#.Net Winforms and is a GUI application.

## Requirements

There are a number of requirements for this system to work.

- The computer running the ES must be domain-joined.
- The Windows CA must also be domain-joined, and online.
- The user running the ES must have an Enrollment Agent certificate in their personal certificate store.
- The user running the ES must have permissions to manage certificates on the CA server.

## Local files

The program creates and maintains a series of local files, listed below:

- settings.xml
  This file contains all persistent settings in the application.

- store.xml
  This file contains all enrolled certificates and their associated secret data, such as PUK keys.

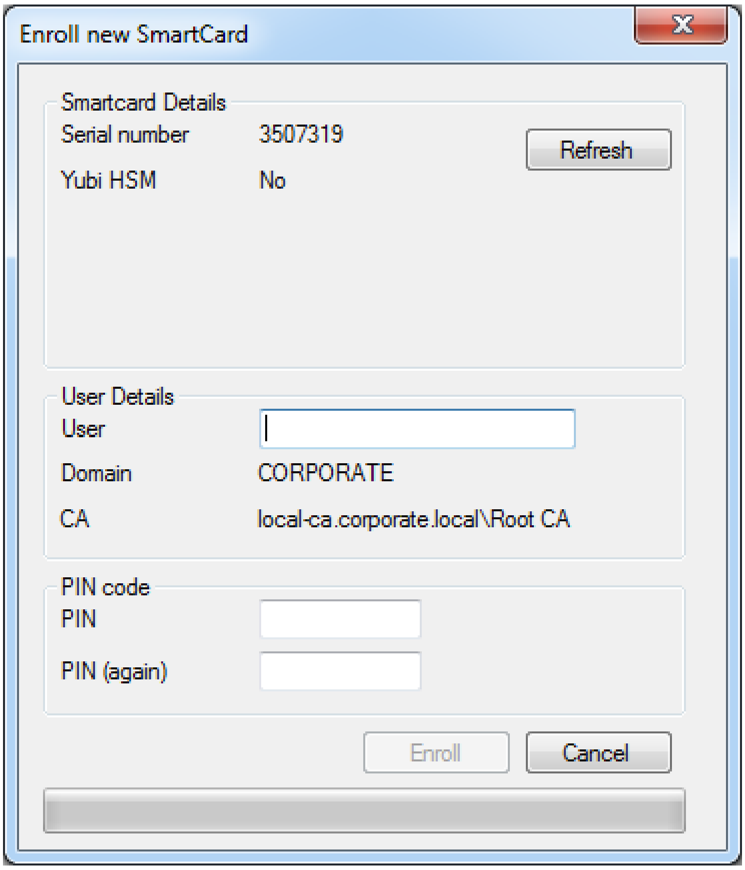
- store.xml.bak
  To combat corrupt stores, a backup is always created before saving.

## Procedures

Following is a series of different use cases, accompanied by screenshots.

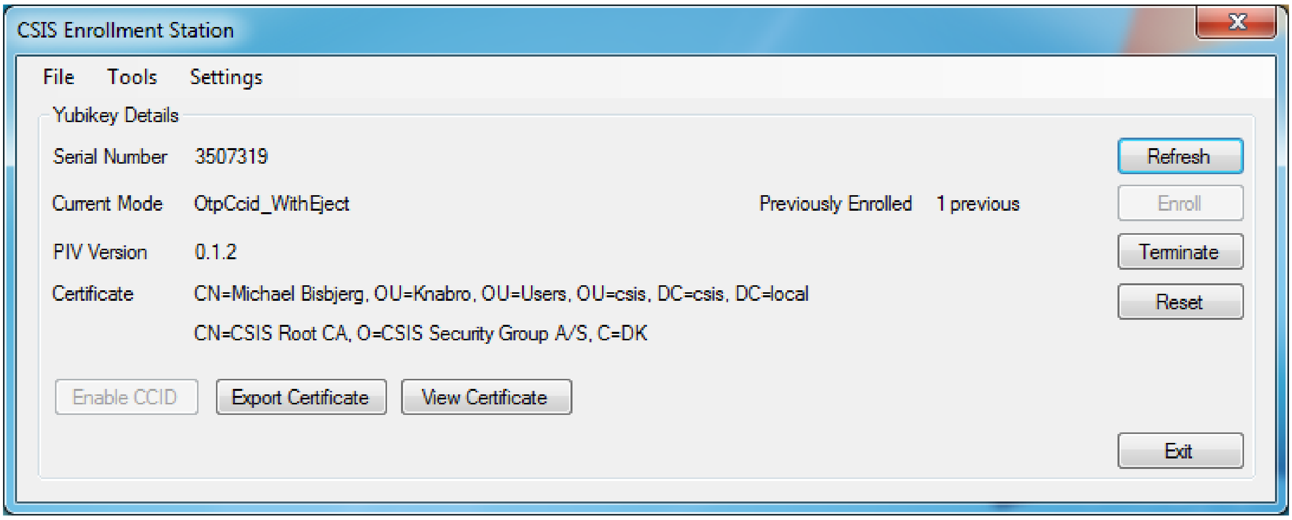
## Enrolling a Yubikey Smartcard

Enrolling a new Smartcard will present a new window requiring you to enter information. By using the information store in the Settings, the only information needed at this point is the username to enroll for, as well as a PIN code. The normal use case for this procedure is that the user is physically standing at the enrollment station, and will enter a PIN code that only they know. PIN codes can be 1 to 8 characters in length.



Serial number 3507319
Yubi HSM No
Domain CORPORATE
CA local-ca.corporate.local\Root CA

The enrollment process can take a little while, so a progress bar will indicate the progress. Once successful, the dialogue will close and the newly enrolled Yubikey is displayed.

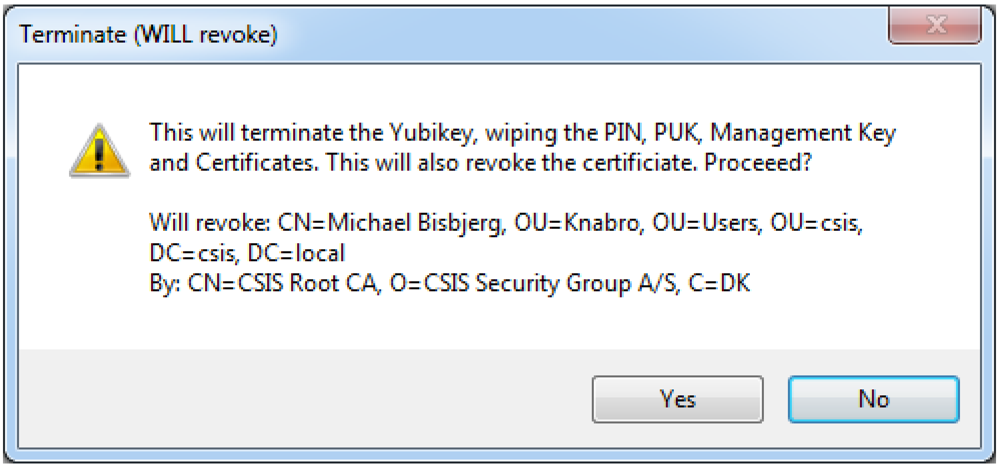


Serial Number 3507319
Current Mode OtpCcid_WithEject
Previously Enrolled 1 previous
PIV Version 0.1.2
Certificate CN=Michael Bisbjerg, OU=Knabro, OU=Users, OU=csis, DC=csis, DC=local
CN=CSIS Root CA, O=CSIS Security Group A/S, C=DK

## Terminating a Yubikey Smartcard

This is the process, in which a Smartcard is revoked and reset. This is the normal method of wiping a Smartcard as it will simultaneously revoke the active certificate and reset the Smartcard (making it possible to use the card again).

Clicking the Terminate button on the main windows will present a series of dialogue boxes, asking questions to confirm the operation(s). Answer them as needed.

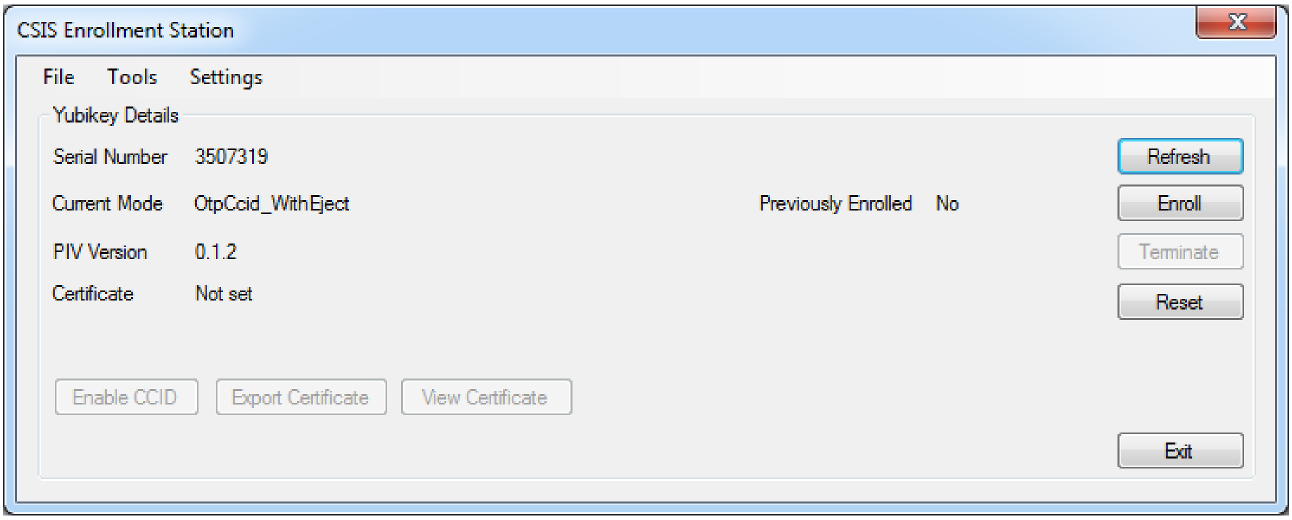


Terminate (WILL revoke)

This will terminate the Yubikey, wiping the PIN, PUK, Management Key and Certificates. This will also revoke the certificiate. Proceeed?

Will revoke: CN=Michael Bisbjerg, OU=Knabro, OU=Users, OU=csis, DC=csis, DC=local
By: CN=CSIS Root CA, O=CSIS Security Group A/S, C=DK

The terminated Yubikey will also remove the item in the Data Store. Once wiped (it takes a little while), you're returned to the main screen:



CSIS Enrollment Station

Yubikey Details

Serial Number 3507319

Current Mode OtpCcid_WithEject

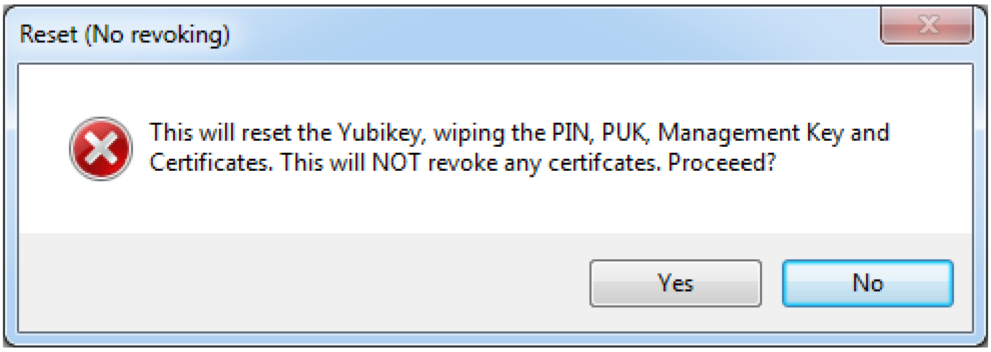
Previously Enrolled No

PIV Version 0.1.2

Certificate Not set

## Resetting a Yubikey Smartcard

Resetting a Yubikey can be used to wipe it without revoking any certificate. This is useful for previously unknown cards that cannot be revoked (as we do not know the CA to revoke at). When clicking the reset button, the following dialogue is presented.

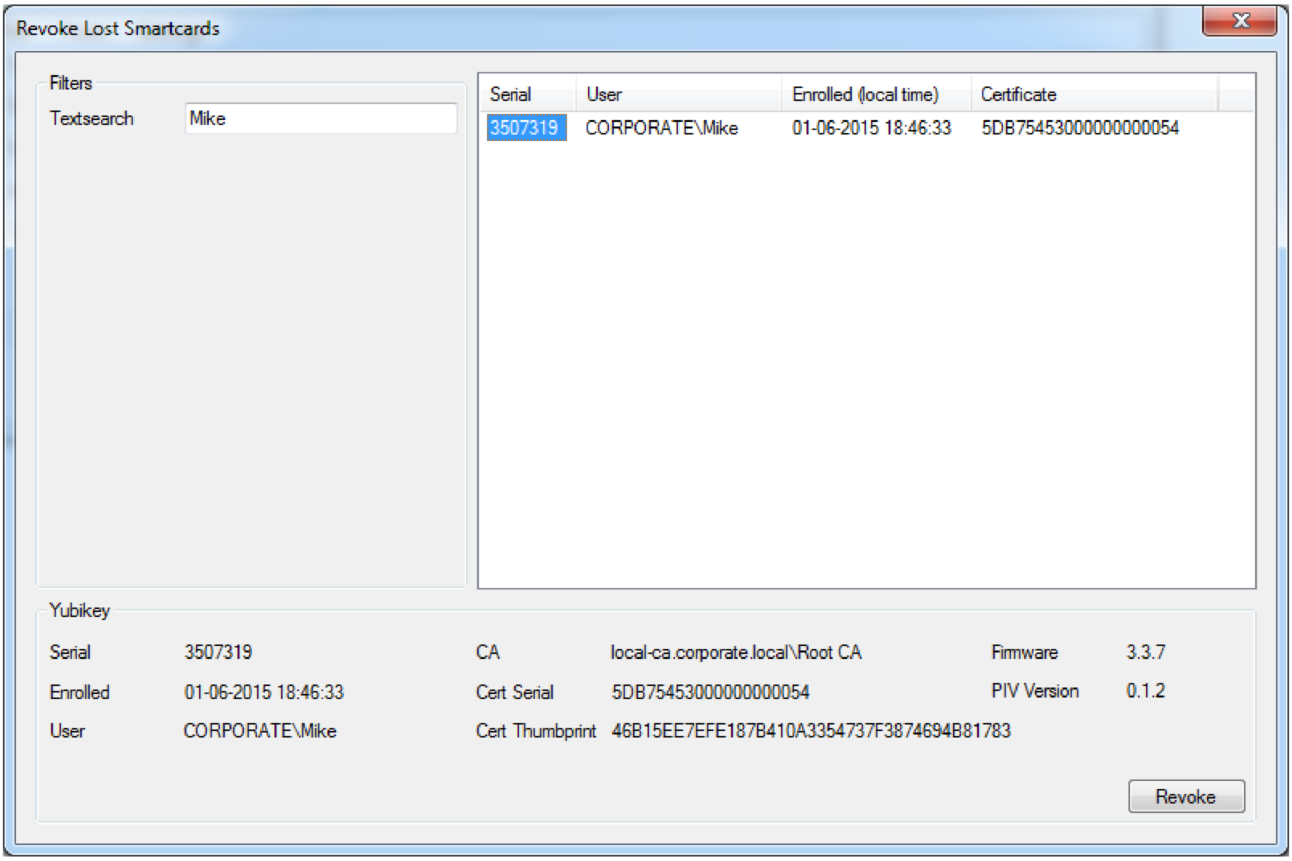


This will reset the Yubikey, wiping the PIN, PUK, Management Key and Certificates. This will NOT revoke any certifcates. Proceeed?

Resetting a Yubikey will not remove any information from the Data Store.

## Revoking a lost Smartcard

When a user loses a Smartcard, it should be revoked as soon as possible. Using the "Revoke Lost Smartcards" menu item. This window will allow you to search through the Data Store for previously enrolled Smartcards, and revoke any one of them.



Textsearch: Mike

| Serial | User | Enrolled (local time) | Certificate |
|---|---|---|---|
| 3507319 | CORPORATE\Mike | 01-06-2015 18:46:33 | 5DB75453000000000054 |

| | | | | | |
|---|---|---|---|---|---|
| Serial | 3507319 | CA | local-ca.corporate.local\Root CA | Firmware | 3.3.7 |
| Enrolled | 01-06-2015 18:46:33 | Cert Serial | 5DB75453000000000054 | PIV Version | 0.1.2 |
| User | CORPORATE\Mike | Cert Thumbprint | 46B15EE7EFE187B410A3354737F3874694B81783 | | |

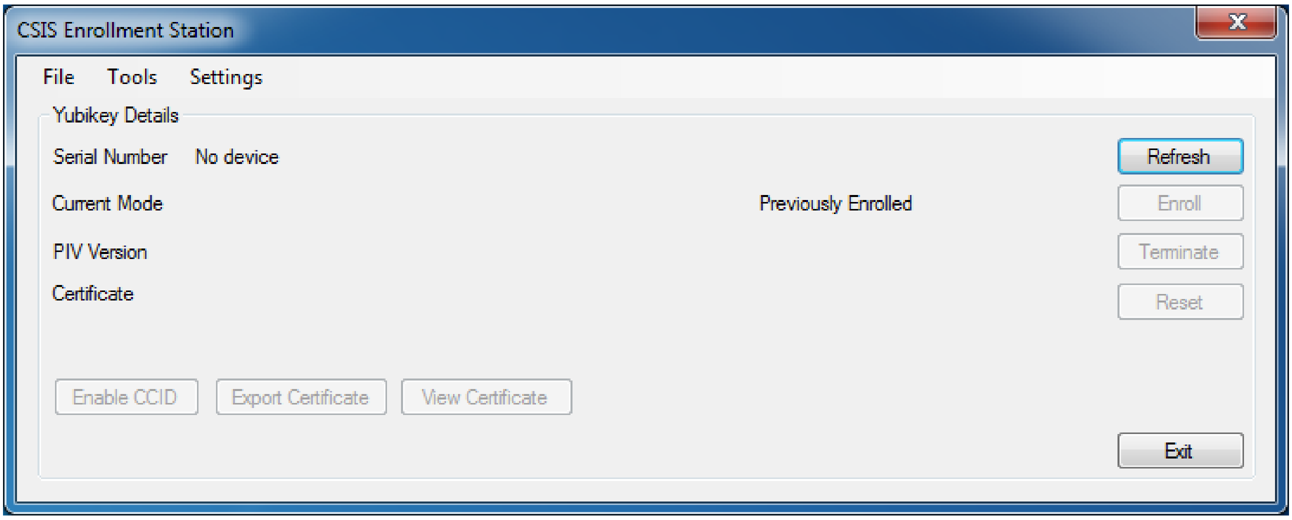
When revoking, a confirmation dialogue will be shown presenting all the information known to the application. It is not possible to un-revoke Smartcards later on, as they are revoked with "Cease of Operations".

# Operations

The following operations will achieve various purposes, but are not every day tasks. The Procedures section will describe every day tasks.

## First run

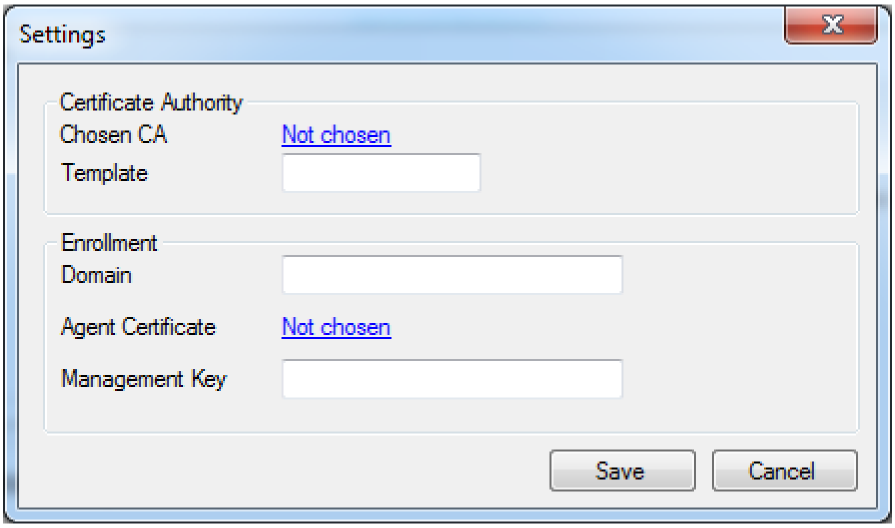
When the program is first run, with no Smart Card inserted, it will show something similar to the below screenshot.



Serial Number No device

## Setting up

To setup the program, open the Settings menu and the Configure menu item. The window below will appear. This dialog allows you to configure defaults for the program, and is required for normal operation. Some field are subject to validation (CA, Agent Certificate) while others are not, so beware when entering data to do so correctly.



Chosen CA: Not chosen

Template:

Domain:

Agent Certificate: Not chosen

Management Key:

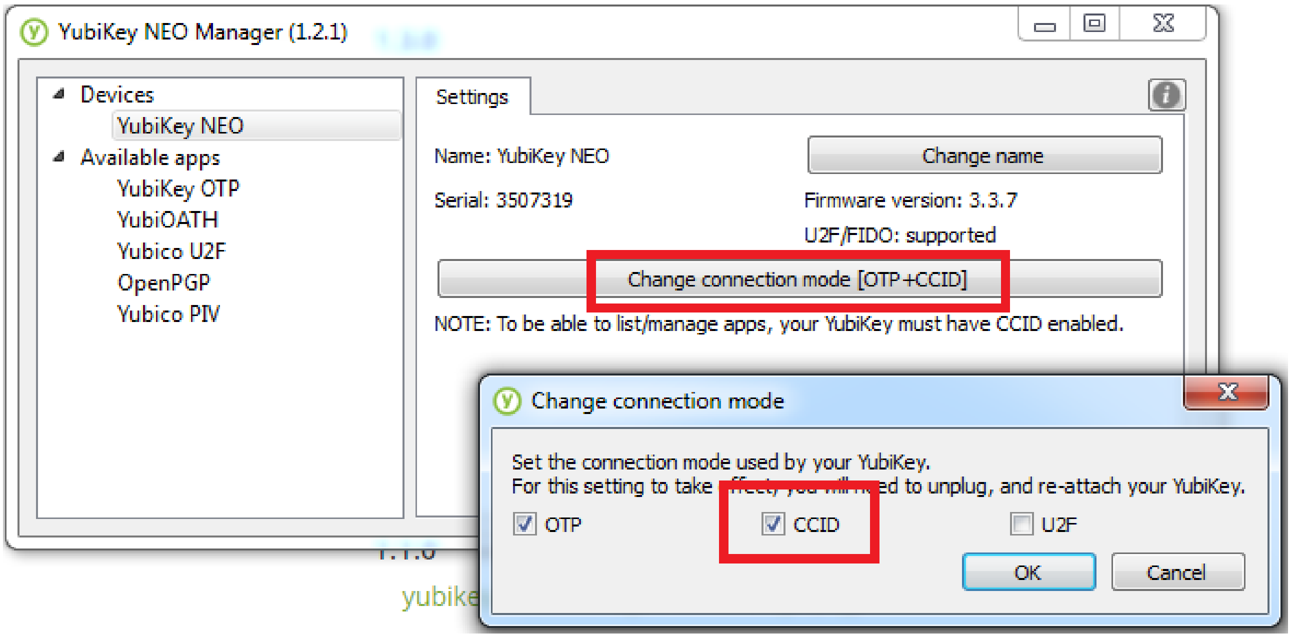
## Preparing a Smartcard for enrollment

In our experience, Yubikey NEO Premiums are not set up to enable the CCID applet. This step has to be taken first, to allow the rest of the program to operate correctly. This is a one-time step for any new Yubikey.

It has not been possible to create this feature in code (yet), so for now a separate tool from Yubico is needed. There are two tools available to perform this task.

### NEO Manager

This GUI will allow you to control various aspects of the NEO device. When the GUI is open and the Yubikey has been detected, click the “Change connection mode” and check the “CCID” option. Finally click “Ok” and unplug and plug the device again. It will now be ready for use with the ES.



Name: YubiKey NEO

Serial: 3507319

Firmware version: 3.3.7

U2F/FIDO: supported

NOTE: To be able to list/manage apps, your YubiKey must have CCID enabled.

Set the connection mode used by your YubiKey.
For this setting to take effect, you will need to unplug, and re-attach your YubiKey.

☑ OTP ☑ CCID ☐ U2F

Home page: https://developers.yubico.com/yubikey-neo-manager/

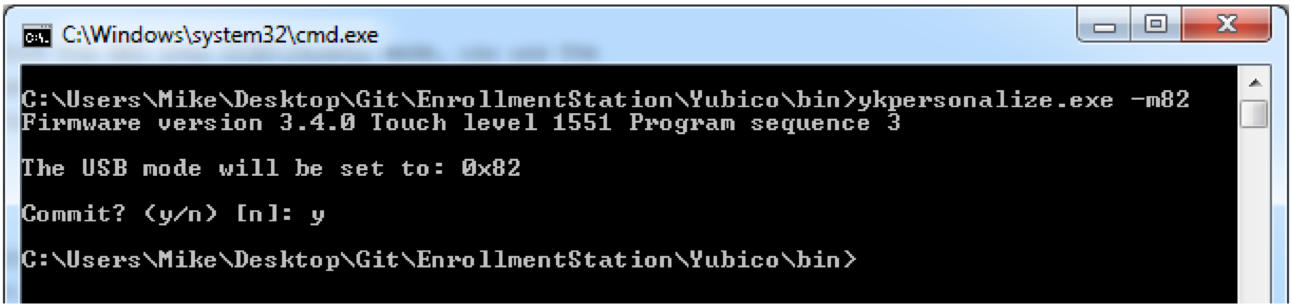
Download page: https://developers.yubico.com/yubikey-neo-manager/Releases/

## Yubikey Personalize

This command line utility will set the mode for you using a simple argument. When downloaded, open a new command prompt and navigate to the directory. Run the following command:

ykpersonalize.exe –m82

The "-m" parameter sets the mode of the device, where 82 is an option found in the documentation. 82 enabled OTP and CCID and allows for button presses to eject/insert the Smartcard. After running the command, unplug and plug the Yubikey to enable the new mode.



```
C:\Users\Mike\Desktop\Git\EnrollmentStation\Yubico\bin>ykpersonalize.exe -m82
Firmware version 3.4.0 Touch level 1551 Program sequence 3

The USB mode will be set to: 0x82

Commit? (y/n) [n]: y

C:\Users\Mike\Desktop\Git\EnrollmentStation\Yubico\bin>
```

Home page: https://developers.yubico.com/yubikey-personalization/

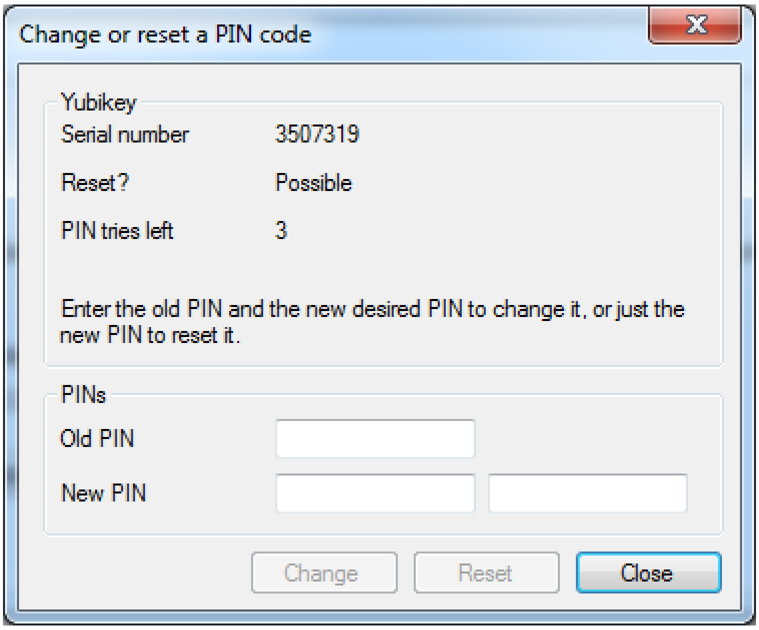
Download page: https://developers.yubico.com/yubikey-personalization/Releases/

Documentation: https://yubico.github.io/yubikey-personalization/ykpersonalize.1.html

# Other procedures

## Changing or resetting a PIN code

When a user has forgotten their PIN code or wishes to change it, it is possible directly in the application to do so. When we have enrolled the Yubikey using the ES (meaning the PUK code will be stored in the Data Store), it is possible to Reset the PIN code. Otherwise it is only possible to Change the PIN code.



Change or reset a PIN code

Yubikey

| | |
|---|---|
| Serial number | 3507319 |
| Reset? | Possible |
| PIN tries left | 3 |

Enter the old PIN and the new desired PIN to change it, or just the new PIN to reset it.

PINs

Old PIN

New PIN