

---

# **YubiKey Manager (ykman) CLI and GUI Guide**

**Yubico**

**Jul 16, 2021**



# CONTENTS

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	YubiKey Firmware . . . . .	1
<b>2</b>	<b>Installation</b>	<b>3</b>
2.1	Download ykman . . . . .	3
2.2	OS-independent Installation . . . . .	3
2.3	Windows . . . . .	3
2.4	MacOS . . . . .	4
2.5	Linux . . . . .	4
2.6	Developers . . . . .	5
<b>3</b>	<b>Using the YubiKey Manager GUI</b>	<b>7</b>
3.1	Checking Firmware Version . . . . .	7
3.2	Managing Applications . . . . .	8
3.3	Managing Interfaces . . . . .	9
3.4	Resetting FIDO2 Function . . . . .	9
<b>4</b>	<b>Using the YubiKey Manager CLI</b>	<b>11</b>
4.1	Windows . . . . .	11
4.2	macOS . . . . .	12
<b>5</b>	<b>Base Commands</b>	<b>13</b>
5.1	ykman [OPTIONS] COMMAND [ARGS]... . . . .	13
5.2	ykman config [OPTIONS] COMMAND [ARGS]... . . . .	15
5.3	ykman config mode [OPTIONS] MODE . . . . .	15
5.4	ykman config nfc [OPTIONS] . . . . .	16
5.5	ykman config set-lock-code [OPTIONS] . . . . .	17
5.6	ykman config usb [OPTIONS] . . . . .	18
5.7	ykman info [OPTIONS] . . . . .	19
5.8	ykman list [OPTIONS] . . . . .	19
5.9	Acronyms . . . . .	20
<b>6</b>	<b>FIDO Commands</b>	<b>21</b>
6.1	ykman fido [OPTIONS] COMMAND [ARGS]... . . . .	21
6.2	ykman fido access [OPTIONS] COMMAND [ARGS]... . . . .	22
6.3	ykman fido access change-pin [OPTIONS] . . . . .	22
6.4	ykman fido access unlock [OPTIONS] (Deprecated) . . . . .	22
6.5	ykman fido access verify-pin [OPTIONS] . . . . .	23
6.6	ykman fido credentials [OPTIONS] COMMAND [ARGS]... . . . .	23
6.7	ykman fido credentials delete [OPTIONS] QUERY . . . . .	24
6.8	ykman fido credentials list [OPTIONS] . . . . .	24

6.9	ykman fido fingerprints [OPTIONS] COMMAND [ARGS]...	25
6.10	ykman fido fingerprints add [OPTIONS] NAME	25
6.11	ykman fido fingerprints delete [OPTIONS] ID	26
6.12	ykman fido fingerprints list [OPTIONS]	26
6.13	ykman fido fingerprints rename [OPTIONS] ID NAME	26
6.14	ykman fido info	27
6.15	ykman fido reset [OPTIONS]	27
<b>7</b>	<b>OATH Commands</b>	<b>29</b>
7.1	ykman oath [OPTIONS] COMMAND [ARGS]...	29
7.2	ykman oath access [OPTIONS] COMMAND [ARGS]...	30
7.3	ykman oath access change [OPTIONS]	30
7.4	ykman oath access forget [OPTIONS]	30
7.5	ykman oath access remember [OPTIONS]	31
7.6	ykman oath accounts [OPTIONS] COMMAND [ARGS]...	31
7.7	ykman oath accounts add [OPTIONS] NAME [SECRET]	32
7.8	ykman oath accounts code [OPTIONS] [QUERY]	33
7.9	ykman oath accounts delete [OPTIONS] QUERY	33
7.10	ykman oath accounts list [OPTIONS]	34
7.11	ykman oath accounts rename [OPTIONS] QUERY NAME	34
7.12	ykman oath accounts uri [OPTIONS] URI	35
7.13	ykman oath info [OPTIONS]	35
7.14	ykman oath reset [OPTIONS]	35
<b>8</b>	<b>OpenPGP Commands</b>	<b>37</b>
8.1	ykman openpgp [OPTIONS] COMMAND [ARGS]...	37
8.2	ykman openpgp access [OPTIONS] COMMAND [ARGS]...	38
8.3	ykman openpgp access set-retries [OPTIONS] PIN-RETRIES RESET-CODE-RETRIES ADMIN-PIN-RETRIES	38
8.4	ykman openpgp certificates [OPTIONS] COMMAND [ARGS]...	39
8.5	ykman openpgp certificates delete [OPTIONS] KEY	39
8.6	ykman openpgp certificates export [OPTIONS] KEY CERTIFICATE	40
8.7	ykman openpgp certificates import [OPTIONS] KEY CERTIFICATE	40
8.8	ykman openpgp keys [OPTIONS] COMMAND [ARGS]...	41
8.9	ykman openpgp keys attest [OPTIONS] KEY CERTIFICATE	41
8.10	ykman openpgp keys import [OPTIONS] KEY PRIVATE-KEY	42
8.11	ykman openpgp keys set-touch [OPTIONS] KEY POLICY	42
8.12	ykman openpgp info [OPTIONS]	43
8.13	ykman openpgp reset [OPTIONS]	43
<b>9</b>	<b>OTP Commands</b>	<b>45</b>
9.1	ykman otp [OPTIONS] COMMAND [ARGS]...	45
9.2	ykman otp calculate [OPTIONS] {1 2} [CHALLENGE]	46
9.3	ykman otp chalresp [OPTIONS] {1 2} [KEY]	47
9.4	ykman otp delete [OPTIONS] {1 2}	47
9.5	ykman otp hotp [OPTIONS] {1 2} [KEY]	47
9.6	ykman otp info [OPTIONS]	48
9.7	ykman otp ndef [OPTIONS] {1 2}	48
9.8	ykman otp settings [OPTIONS] {1 2}	49
9.9	ykman otp static [OPTIONS] {1 2} [PASSWORD]	50
9.10	ykman otp swap [OPTIONS]	50
9.11	ykman otp yubiotp [OPTIONS] {1 2}	51
<b>10</b>	<b>PIV Commands</b>	<b>53</b>
10.1	ykman piv [OPTIONS] COMMAND [ARGS]...	53

10.2	ykman piv access [OPTIONS] COMMAND [ARGS]...	54
10.3	ykman piv access change-management-key [OPTIONS]	54
10.4	ykman piv access change-pin [OPTIONS]	55
10.5	ykman piv access change-puk [OPTIONS]	56
10.6	ykman piv access set-retries [OPTIONS] PIN-RETRIES PUK-RETRIES	56
10.7	ykman piv access unblock-pin [OPTIONS]	56
10.8	ykman piv certificates [OPTIONS] COMMAND [ARGS]...	57
10.9	ykman piv certificates delete [OPTIONS] SLOT	57
10.10	ykman piv certificates export [OPTIONS] SLOT CERTIFICATE	58
10.11	ykman piv certificates generate [OPTIONS] SLOT PUBLIC-KEY	58
10.12	ykman piv certificates import [OPTIONS] SLOT CERTIFICATE	59
10.13	ykman piv certificates request [OPTIONS] SLOT PUBLIC-KEY CSR	60
10.14	ykman piv info [OPTIONS]	60
10.15	ykman piv keys [OPTIONS] COMMAND [ARGS]...	61
10.16	ykman piv keys attest [OPTIONS] SLOT CERTIFICATE	61
10.17	ykman piv keys export [OPTIONS] SLOT PUBLIC-KEY	62
10.18	ykman piv keys generate [OPTIONS] SLOT PUBLIC-KEY	62
10.19	ykman piv keys import [OPTIONS] SLOT PRIVATE-KEY	63
10.20	ykman piv objects [OPTIONS] COMMAND [ARGS]...	64
10.21	ykman piv objects export [OPTIONS] OBJECT OUTPUT	65
10.22	ykman piv objects generate [OPTIONS] OBJECT	65
10.23	ykman piv objects import [OPTIONS] OBJECT DATA	66
10.24	ykman piv reset [OPTIONS]	66
<b>11</b>	<b>YubiHSM Commands</b>	<b>67</b>
11.1	Enable or Disable YubiHSM Auth on a YubiKey	67
<b>12</b>	<b>Copyright</b>	<b>69</b>
12.1	Disclaimer	69
12.2	Contact Information	69
12.3	Document Updated	70



## INTRODUCTION

The YubiKey Manager (ykman) is a cross-platform application for managing and configuring a YubiKey via a graphical user interface (GUI) and a Python 3.6 (or later) library and command line interface (CLI). It provides an easy way to perform the most common configuration tasks on a YubiKey, such as:

- Displaying the serial number and firmware version of a YubiKey (see *YubiKey Firmware*)
- Configuring a FIDO2 PIN
- Resetting the FIDO applications
- Configuring the OTP application. A YubiKey has two slots (Short Touch and Long Touch). This tool can configure a Yubico OTP credential, a static password, a challenge-response credential or an OATH HOTP credential in either or both of these slots.
- Manage certificates and PINs for the PIV application
- Swap the credentials between two configured slots
- Enable and disable USB and NFC interfaces

Some of the more advanced options are only available through the command line.

This guide contains the instructions for using both ykman's CLI and its GUI.

- For the GUI, see *Using the YubiKey Manager GUI* in this guide.
- For the CLI, see the balance of this guide. The commands are organized by protocol. CLIs that do not relate specifically to a particular protocol are listed in Base Commands.

### 1.1 YubiKey Firmware

The YubiKey firmware is separate from the YubiKey itself in the sense that it is put onto each YubiKey in a process separate from the manufacture of the physical key. Nonetheless, it can be neither removed nor altered. Yubico periodically updates the YubiKey firmware to take advantage of features and capabilities introduced into operating systems (OSs) such as Windows, etc., as well as to enable new YubiKey features and capabilities.

The firmware version on a YubiKey therefore determines whether or not a feature or a capability is available to that YubiKey. The quickest and most convenient way to determine your YubiKey's firmware version is to use ykman.





## INSTALLATION

YubiKey Manager (ykman) can be installed on Windows, macOS, and Linux systems.

### 2.1 Download ykman

Download ykman installers from: [YubiKey Manager Releases](#).

The installers include both the full graphical application and command line tool.

Additional installation packages are available from third parties. Refer to the third party provider for installation instructions. This applies to:

- Pre-built packages from platform package managers.
- Homebrew and MacPorts for macOS.
- Linux distribution third party package maintainers.

### 2.2 OS-independent Installation

ykman can be installed independently of platform by using pip (or equivalent). From a command line, run:

```
pip install --user yubikey-manager
```

### 2.3 Windows

To install ykman on Windows:

1. As Administrator, run the `.exe` executable.
2. As Administrator, open a command window with Run.
3. From the download directory, run the installer executable, `C: yubikey-manager-qt-1.2.3.win64.exe`.

### 2.3.1 PowerShell

If you are using PowerShell you may need to either prefix an ampersand, or use two commands: one to change directory, then one to run the executable from the working directory. For example:

```
C: & "C:\Users..."
```

or

```
C: cd "C:\Users..."
```

```
C: .\yubikey-mana..."
```

### 2.3.2 Silent Install

Adding /S to this makes the installation silent. The S must be capitalized.

### 2.3.3 Mapped Drives

If running from a mapped drive, you might need to add /D <install path>. This ensures ykman is installed in the correct drive.

```
C: .\yubikey-manager-qt-1.2.3.exe /S /D "C:\Program Files\Yubico\Yubico Authenticator"
```

### 2.3.4 Uninstaller

Once installed, the application uninstaller, `ykman-uninstall.exe`, is located in the ykman install directory.

Running the uninstaller starts the uninstall process. The /S silent install option described above works with the uninstaller.

## 2.4 MacOS

To install on Mac, double-click the `.dmg` file and follow the prompts.

## 2.5 Linux

On Linux platforms you need to have `pcscd` installed and running to communicate with a YubiKey over the SmartCard interface. Additionally, you might need to set permissions for your user to access YubiKeys via the HID interfaces.

Some of the libraries used by ykman have C-extensions, and might require additional dependencies to build, such as `swig` and potentially `PCSC lite`.

## 2.5.1 Third Party Linux Distributions

Yubico provides packages for Ubuntu in the yubico/stable PPA.

---

**Note:** For Linux amd64 ONLY and other architectures such as ARM, use the general pip instructions above.

---

If you are using packages from one of the several Linux distributions' third party repositories, follow the installation steps from the Linux distribution.

For example:

```
sudo apt-add-repository ppa:yubico/stable
sudo apt update
sudo apt install yubikey-manager
```

See also the Yubico Support Knowledge Base article [Installing Yubico Software on Linux](#).

## 2.6 Developers

For more information, see the ykman CLI page on [developers.yubico.com](#).

---

To get in touch with Yubico Support, [click here](#).



## USING THE YUBIKEY MANAGER GUI

The YubiKey Manager's (ykman's) graphical user interface (GUI) is a quick, convenient way to find out what firmware your YubiKey has and/or to reset it - unless you prefer to use ykman's CLI. Note that the CLI has more options, so if you do not find what you want in the GUI, check to see if the CLI has it.

### 3.1 Checking Firmware Version

Launch the **YubiKey Manager App** and connect your YubiKey if it is not already connected. Note that the tool will only read a single YubiKey at a time, so if you have multiple keys connected, it might not be evident which one the tool is identifying.

ykman opens the **Home** tab by default, displaying the following:

- YubiKey series (e.g., YubiKey 5)
- Firmware (e.g., 5.4.X)
- Images of the various form factors within that series.

# YubiKey 4

Firmware: 4.3.7

Serial: 8535201



*YubiKey Manager GUI, Home tab*

## 3.2 Managing Applications

### 3.2.1 Enabling/Disabling

ykman can be used to check which applications are enabled on which interface and to enable or disable each application on each physical interface.

To find out which applications are enabled, select the **Interfaces** tab. A checkbox with a tick is shown next to each enabled application. To change which applications are enabled, use the checkboxes to select the ones you want enabled and click **Save Interfaces**.

---

**Note:** For the YubiKey 5Ci, any modifications made to the applications over the USB interface will also apply to the applications over Lightning®.

---

### 3.2.2 Locking

Once the desired applications have been selected, a lock code can be set to prevent changes to the set of enabled applications. This is done using the `ykman config set-lock-code`. The lock code is 16 bytes presented as 32 hex characters. For more information, see `ykman config set-lock-code [OPTIONS]`.

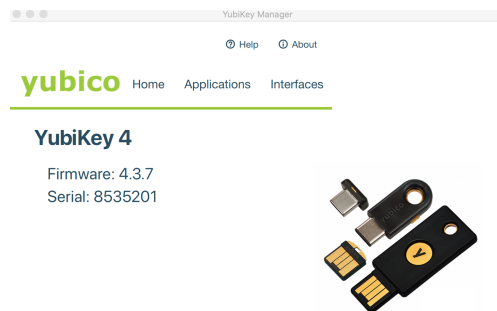
## 3.3 Managing Interfaces

The **Interfaces** tab displays your key's form factor (e.g., USB), and the interfaces it has. Use the **Interfaces** tab to configure what is available on that key. For example, you can disable the interfaces by deselecting the respective checkboxes.

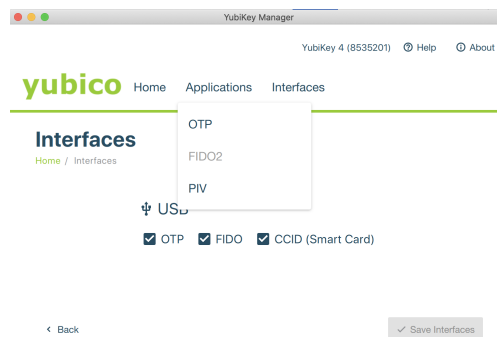
## 3.4 Resetting FIDO2 Function

Resetting the key is not the same as unblocking it. Because resetting the FIDO2 function returns the key to its beginning state when it has no PIN, you must set a new PIN and enroll the key again after resetting it.

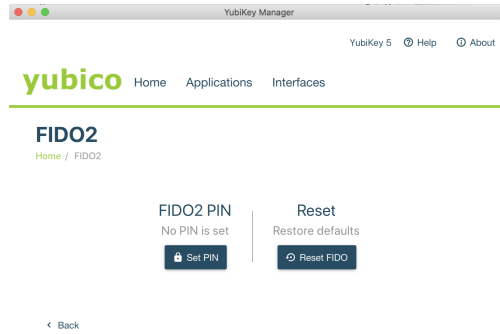
**Step 1** Remove your YubiKey if it is still connected to your machine, then launch `ykman` and insert your key.



**Step 2** Click on the word **Applications** at the top of that tab. A list of menu options appears. The specific options depend on the key.



**Step 3** Select **FIDO2**. The FIDO2 page appears.




**Step 4** Click the **Reset FIDO** button. The Reset FIDO confirmation popup appears.



**Step 5** Click **Yes**. Everything on the key is removed: the PIN (if set) is deleted. The **Remove and re-insert your YubiKey!** prompt appears.

Remove and re-insert your YubiKey!

**Step 6** Remove and re-insert your YubiKey. The **Touch your YubiKey** prompt appears, and the green LED flashes.

Touch your YubiKey! 

**Step 7** Touch your YubiKey. The message “FIDO applications have been reset” appears at the bottom of the **Applications** page.

**Step 8** Remove the key in preparation for re-enrolling it.

---

To get in touch with Yubico Support, [click here](#).



## USING THE YUBIKEY MANAGER CLI

ykman can be used to configure all aspects of the YubiKey. This manual covers the options for each command as well as examples.

### 4.1 Windows

Run the commands from Command Prompt.

#### 4.1.1 Directory

If your environment variable is not set to automatically find YubiKey Manager or `ykman`, change directory to the location of the `ykman` executables. For example, with Windows 64-bit version of YubiKey Manager installed, `C:\` \cd `"C:\Program Files\Yubico\YubiKey Manager\"`.

#### 4.1.2 Launch ykman

Launch `ykman` in GUI mode or CLI mode from the command line.

- Launch YubiKey Manager CLI, (32-bit)  
`C:\` \ "C:\Program Files (x86)\Yubico\YubiKey Manager\ykman.exe"
- Launch YubiKey Manager CLI, (64-bit)  
`C:\` \ "C:\Program Files\Yubico\YubiKey Manager\ykman.exe"
- Launch YubiKey Manager GUI, (32-bit)  
`C:\` \ "C:\Program Files (x86)\Yubico\YubiKey Manager\ykman-gui.exe"
- Launch YubiKey Manager GUI, (64-bit)  
`C:\` \ "C:\Program Files\Yubico\YubiKey Manager\ykman-gui.exe"

Launch YubiKey Manager with debug logging enabled. Add the following to the execution command.

```
--log-level DEBUG --log-file %USERPROFILE%\Desktop\ykman-log.txt
```

### 4.1.3 User Accounts

Check whether user accounts are local or Microsoft accounts.

```
C://Get-LocalUser | Where-Object { $_.Enabled -match "True"} | Select-Object  
Name,PrincipalSource,SID
```

## 4.2 macOS

From your Mac's Terminal application, run the listed commands as needed.

### 4.2.1 Directory

Change directory to the location of the ykman executables:

```
% cd "/Applications/YubiKey Manager.app/Contents/MacOS/"
```

### 4.2.2 Run YubiKey Manager

Launch ykman in GUI mode or CLI mode from the command line.

- Run YubiKey Manager CLI

```
% /Applications/YubiKey Manager.app/Contents/MacOS/ykman
```

- Run YubiKey Manager GUI

```
% /Applications/YubiKey Manager.app/Contents/MacOS/ykman-gui
```

Run ykman with debug logging (to a file) enabled. Add the following to the run command:

```
--log-level DEBUG --log-file ~/Desktop/ykman.txt
```

### 4.2.3 Sleep Mode

Terminal Commands to eliminate the power drain issue when a YubiKey is plugged in to a sleeping Mac:

```
% sudo pmset -a hibernatemode 25  
% sudo pmset -a standbydelay 15  
  
Error message (bash) if macOS Logon Tool is not installed  
% -bash: ykpamcfg: command not found
```

### 4.2.4 Mac Logon Tool

To install Mac Logon Tool through a terminal:

```
% cd ~/Downloads  
% curl -O https://developers.yubico.com/yubico-pam/Releases/pam_yubico-2.26.pkg  
% sudo installer -pkg pam_yubico-2.26.pkg -target / -verboseR
```

---

To get in touch with Yubico Support, [click here](#).

## BASE COMMANDS

The base commands are those that do not apply to any specific protocol. However, they do apply to the different connection methods such as USB and NFC.

Acronyms and their definitions are listed at the bottom of this page.

### 5.1 ykman [OPTIONS] COMMAND [ARGS]...

**Description** Configure your YubiKey via the command line.

#### 5.1.1 Examples

- List connected YubiKeys, only output serial number:  

```
$ ykman list --serials
```
- Show information about the YubiKey with serial number 0123456:  

```
$ ykman --device 0123456 info
```

### 5.1.2 Options

Option	Description
<code>-h, --help</code>	Show this message and exit.
<code>-d, --device SERIAL</code>	Specify YubiKey to interact with by serial number.
<code>--diagnose</code>	Show diagnostics information for troubleshooting.
<code>--full-help</code>	Show <code>-help</code> , including hidden commands, and exit.
<code>--log-file FILE</code>	Write logs to a given FILE instead of standard error. Ignored unless <code>--log-level</code> also set.
<code>-l, --log-level [DEBUG INFO WARNING ERROR CRITICAL]</code>	Enable logging at given verbosity level.
<code>-r, --reader NAME</code>	Use an external smart card reader. Conflicts with <code>--device</code> and <code>list</code> .
<code>-v, --version</code>	Show version information about the app [ykman]

### 5.1.3 Commands

Command	Description
<code>config</code>	Enable/Disable applications.
<code>fido</code>	Manage the FIDO applications.
<code>info</code>	Show general information.
<code>list</code>	List connected YubiKeys.
<code>oath</code>	Manage the OATH Application.
<code>openpgp</code>	Manage the OpenPGP Application.
<code>otp</code>	Manage the OTP Application.
<code>piv</code>	Manage the PIV Application.

## 5.2 ykman config [OPTIONS] COMMAND [ARGS]...

**Description** Enable or disable applications. The applications may be enabled and disabled independently over different transports (USB and NFC). The configuration may also be protected by a lock code.

### 5.2.1 Examples

- Disable PIV over NFC:  
\$ ykman config nfc --disable PIV
- Enable all applications over USB:  
\$ ykman config usb --enable-all
- Generate and set a random application lock code: \$ ykman config set-lock-code --generate

### 5.2.2 Options

Option	Description
-h, --help	Show this message and exit.

### 5.2.3 Commands

Command	Description
mode	Manage connection modes (USB interfaces).
nfc	Enable or disable applications over NFC.
set-lock-code	Set or change the configuration lock code.
usb	Enable or disable applications over USB.

## 5.3 ykman config mode [OPTIONS] MODE

**Description** Manage connection modes (USB Interfaces). This command is generally used with YubiKeys prior to the 5 series. Use `ykman config usb` for more granular control on YubiKey 5 and later. Get the current connection mode of the YubiKey, or set it to `MODE`.

### 5.3.1 Examples

- Set the OTP and FIDO mode:  
\$ ykman config mode OTP+FIDO
- Set the CCID only mode and use touch to eject the smart card:  
\$ ykman config mode CCID --touch-eject

### 5.3.2 Arguments

Argument	Description
MODE	MODE can be a string, such as OTP+FIDO+CCID, or a shortened form: o+f+c. It can also be a mode number.

### 5.3.3 Options

Option	Description
-h, --help	Show this message and exit.
--autoeject-timeout SECONDS	When set, the smartcard automatically ejects after the given time. Implies --touch-eject (CCID mode only).
--chalresp-timeout SECONDS	Sets the timeout when waiting for touch for challenge response.
-f, --force	Confirm the action without prompting.
--touch-eject	When set, the button toggles the state of the smartcard between ejected and inserted (CCID mode only).

## 5.4 ykman config nfc [OPTIONS]

**Description** Enable or disable applications over NFC.

### 5.4.1 Options

Option	Description
-h, --help	Show this message and exit.
-a, --enable-all	Enable all applications.
-d, --disable [OTP U2F FIDO2 OATH PIV OPENPGP HSMAUTH]	Disable applications.
-D, --disable-all	Disable all applications.
-e, --enable [OTP U2F FIDO2 OATH PIV OPENPGP HSMAUTH]	Enable applications.
-f, --force	Confirm the action without prompting.
-l, --list	List enabled applications.
-L, --lock-code HEX	Current application configuration lock code.

## 5.5 ykman config set-lock-code [OPTIONS]

**Description** Set or change the configuration lock code. A lock code may be used to protect the application configuration. The lock code must be a 32 characters (16 bytes) hex value.

### 5.5.1 Options

Option	Description
-h, --help	Show this message and exit.
-c, --clear	Clear the lock code.
-f, --force	Confirm the action without prompting.
-g, --generate	Generate a random lock code. Conflicts with --new-lock-code.
-l, --lock-code HEX	Current lock code.
-n, --new-lock-code HEX	New lock code. Conflicts with --generate.

## 5.6 ykman config usb [OPTIONS]

**Description** Enable or disable applications over USB.

### 5.6.1 Options

Option	Description
-h, --help	Show this message and exit.
-a, --enable-all	Enable all applications.
--autoeject-timeout SECONDS	When set, the smartcard automatically ejects after the specified time. Implies --touch-eject.
--chalresp-timeout SECONDS	Sets the timeout when waiting for touch response to the challenge-response from the OTP application.
-d, --disable [OTP U2F FIDO2 OATH PIV OPENPGP HSMAUTH]	Disable applications.
-e, --enable [OTP U2F FIDO2 OATH PIV OPENPGP HSMAUTH]	Enable applications.
-f, --force	Confirm the action without prompting.
-l, --list	List enabled applications.
-L, --lock-code HEX	Current application configuration lock code.
--no-touch-eject	Disable touch eject (CCID only).
--touch-eject	When set, the button toggles the state of the smartcard between ejected and inserted (CCID only).



## 5.7 ykman info [OPTIONS]

**Description** Show general information. Displays information about the connected YubiKey such as serial number, firmware version, applications, etc.

### 5.7.1 Options

Option	Description
-h, --help	Show this message and exit.
-c, --check-fips	Check if YubiKey is in FIPS-approved mode. Available on YubiKey 4 FIPS only.

### 5.7.2 Example

```
$ ./ykman info
Device type: YubiKey 5Ci
Serial number: 12345678
Firmware version: 5.2.3
Form factor: Keychain (USB-C, Lightning)
Enabled USB interfaces: OTP, FIDO, CCID

Applications
OTP           Enabled
FIDO U2F      Enabled
OpenPGP       Enabled
PIV           Enabled
OATH          Enabled
FIDO2         Enabled
```

## 5.8 ykman list [OPTIONS]

**Description** List connected YubiKeys.

### 5.8.1 Options

Option	Description
-h, --help	Show this message and exit.
-r, --readers	List available smart card readers.
-s, --serials	Output only serial numbers of the connected YubiKeys, one per line. Devices without serial numbers are not listed.

To get in touch with Yubico Support, [click here](#).

## 5.9 Acronyms

**3DES** Triple Data Encryption Algorithm

**AES** Advanced Encryption Standard

**CCC** Card Capability Container

**CCID** Chip card interface device, a USB protocol for a smartcard.

**CHUID** Card Holder Unique ID

**CN** Common name

**CSR** Certificate Signing Request

**ECC** Elliptic curve cryptography

**FIDO** Fast Identity Online

**FIPS** Federal Information Processing Standards (US government) covering codes and encryption standards.

**HMAC** Hash-based message authentication code

**HOTP** HMAC-based One-Time Password algorithm

**OATH** The Initiative for Open Authentication is an organization that specifies two open authentication standards, TOTP and HOTP

**OTP** One-Time Password

**PUK** PIN Unlock Key

**stdin** standard input - usually keyboard or CLI instructions

**stdout** standard output - usually print to screen

**TOTP** Time-based One-Time Password algorithm

**X.509** The standard defining the format of a public key certificate

## FIDO COMMANDS

Acronyms and their definitions are listed at the bottom of the *Base Commands* page.

### 6.1 ykman fido [OPTIONS] COMMAND [ARGS]...

**Description** Manage FIDO applications.

#### 6.1.1 Examples

- Reset the FIDO (FIDO2 and U2F) applications:  
`$ ykman fido reset`
- Change the FIDO2 PIN from 123456 to 654321:  
`$ ykman fido access change-pin --pin 123456 --new-pin 654321`

#### 6.1.2 Options

Option	Description
<code>-h, --help</code>	Show this message and exit.

#### 6.1.3 Commands

Command	Description
<code>access</code>	Manage the PIN for FIDO.
<code>credentials</code>	Manage discoverable (resident) credentials.
<code>fingerprints</code>	Manage fingerprints.
<code>info</code>	Display status of FIDO2 application.
<code>reset</code>	Reset all FIDO applications.

## 6.2 ykman fido access [OPTIONS] COMMAND [ARGS]...

**Description** Manage the PIN for FIDO.

### 6.2.1 Options

Option	Description
-h, --help	Show this message and exit.

### 6.2.2 Commands

Command	Description
change-pin	Set or change the PIN code.
verify-pin	Verify the FIDO PIN against a YubiKey.

## 6.3 ykman fido access change-pin [OPTIONS]

**Description** Set or change the PIN code. The FIDO2 PIN must be at least 4 characters long and can be any type of alphanumeric character. On YubiKey FIPS, a PIN can be set for FIDO U2F. That PIN must be at least 6 characters long.

### 6.3.1 Options

Option	Description
-h, --help	Show this message and exit.
-n, --new-pin TEXT	A new PIN.
-P, --pin TEXT	Current PIN code.
-u, --u2f	Set FIDO U2F PIN instead of FIDO2 PIN.

## 6.4 ykman fido access unlock [OPTIONS] (Deprecated)

Replaced unlock command with verify-pin command.

**Description** Verify U2F PIN for YubiKey FIPS. Unlock the YubiKey FIPS and allow U2F registration.

### 6.4.1 Options

Option	Description
-h, --help	Show this message and exit.
-P, --pin TEXT	Current PIN code.

## 6.5 ykman fido access verify-pin [OPTIONS]

**Description** Verify the FIDO PIN against a YubiKey. For YubiKeys supporting FIDO2 this resets the “retries” counter of the PIN. For YubiKey FIPS this unlocks the session, allowing U2F registration.

### 6.5.1 Options

Option	Description
-h, --help	Show this message and exit.
-P, --pin TEXT	Current PIN code.

## 6.6 ykman fido credentials [OPTIONS] COMMAND [ARGS]...

**Description** Manage discoverable (resident) credentials. This command lets you manage credentials stored on your YubiKey. Credential management is only available when a FIDO PIN is set on the YubiKey.

---

**Note:** Managing credentials requires having a PIN. Set a PIN first.

---

### 6.6.1 Examples

- List stored credentials (providing PIN via argument):  

```
$ ykman fido credentials list --pin 123456
```
- Delete a credential by user name (PIN is prompted for):  

```
$ ykman fido credentials delete example_user
```

### 6.6.2 Options

Option	Description
-h, --help	Show this message and exit.

### 6.6.3 Commands

Command	Description
delete	Delete a resident credential.
list	List resident credentials.

## 6.7 ykman fido credentials delete [OPTIONS] QUERY

**Description** Delete a credential.

### 6.7.1 Arguments

Argument	Description
QUERY	A unique substring match of a credentials RP ID, user ID (hex) or name, or credential ID.

### 6.7.2 Options

Option	Description
-h, --help	Show this message and exit.
-f, --force	Confirm deletion without prompting
-P, --pin TEXT	PIN code.

## 6.8 ykman fido credentials list [OPTIONS]

**Description** List credentials.

### 6.8.1 Options

Option	Description
-h, --help	Show this message and exit.
-P, --pin TEXT	PIN code.

## 6.9 ykman fido fingerprints [OPTIONS] COMMAND [ARGS]...

**Description** Manage fingerprints. Requires a YubiKey with fingerprint sensor. Fingerprint management is only available when a FIDO PIN is set on the YubiKey.

### 6.9.1 Examples

- Register a new fingerprint (providing PIN via argument):

```
$ ykman fido fingerprints add "Left thumb" --pin 123456
```

- List already stored fingerprints (providing PIN via argument):

```
$ ykman fido fingerprints list --pin 123456
```

- Delete a stored fingerprint with ID “f691” (PIN is prompted for):

```
$ ykman fido fingerprints delete f691
```

### 6.9.2 Options

Option	Description
-h, --help	Show this message and exit.

### 6.9.3 Commands

Command	Description
add	Add a new fingerprint.
delete	Delete a fingerprint.
list	List registered fingerprint.
rename	Set the label for a fingerprint.

## 6.10 ykman fido fingerprints add [OPTIONS] NAME

**Description** Add a new fingerprint.

### 6.10.1 Arguments

Argument	Description
NAME	A short readable name for the fingerprint (eg. “Left thumb”).

## 6.10.2 Options

Option	Description
-h, --help	Show this message and exit.
-P, --pin TEXT	PIN code.

## 6.11 ykman fido fingerprints delete [OPTIONS] ID

**Description** Delete a fingerprint. Delete a fingerprint from the YubiKey by its ID.

### 6.11.1 Arguments

Argument	Description
ID	To see the ID run the <code>list</code> subcommand.

### 6.11.2 Options

Option	Description
-h, --help	Show this message and exit.
-f, --force	Confirm deletion without prompting.
-P, --pin TEXT	PIN code.

## 6.12 ykman fido fingerprints list [OPTIONS]

**Description** List registered fingerprint. Lists fingerprints by ID and (if available) label.

### 6.12.1 Options

Option	Description
-h, --help	Show this message and exit.
-P, --pin TEXT	PIN code.

## 6.13 ykman fido fingerprints rename [OPTIONS] ID NAME

**Description** Set the label for a fingerprint.



### 6.13.1 Arguments

Argument	Description
ID	The ID of the fingerprint to rename (as shown in <code>list</code> ).
NAME	A short readable name for the fingerprint (eg. "Left thumb").

### 6.13.2 Options:

Option	Description
<code>-h, --help</code>	Show this message and exit.
<code>-P, --pin TEXT</code>	PIN code.

## 6.14 ykman fido info

**Description** Display general status of the FIDO2 application.

### 6.14.1 Options

Option	Description
<code>-h, --help</code>	Show this message and exit.

## 6.15 ykman fido reset [OPTIONS]

**Description** Reset all FIDO applications. This action wipes all FIDO credentials on the YubiKey, including FIDO U2F credentials, and removes the PIN code. The reset is triggered immediately after the YubiKey is inserted, and it requires that the YubiKey be touched.

### 6.15.1 Options

Option	Description
<code>-h, --help</code>	Show this message and exit.
<code>-f, --force</code>	Confirm the action without prompting.

To get in touch with Yubico Support, go to <https://support.yubico.com/hc/en-us/requests/new>.

To get in touch with Yubico Support, [click here](#).



## OATH COMMANDS

Acronyms and their definitions are listed at the bottom of the *Base Commands* page.

### 7.1 ykman oath [OPTIONS] COMMAND [ARGS]...

**Description** Manage OATH application.

#### 7.1.1 Examples

- Generate codes for accounts starting with yubi:  
\$ ykman oath accounts code yubi
- Add an account, with the secret key f5up4ub3dw and the name yubico, that requires touch:  
\$ ykman oath accounts add yubico f5up4ub3dw --touch
- Set a password for the OATH application:  
\$ ykman oath access change-password

#### 7.1.2 Options

Option	Description
-h, --help	Show this message and exit.

#### 7.1.3 Commands

Command	Description
access	Manage password protection for OATH.
accounts	Manage and use OATH accounts.
info	Display general status of OATH application.
reset	Reset all OATH data.

## 7.2 ykman oath access [OPTIONS] COMMAND [ARGS]...

**Description** Manage password protection for OATH.

### 7.2.1 Options

Option	Description
-h, --help	Show this message and exit.

### 7.2.2 Commands

Command	Description
change	Change the password used to protect OATH accounts.
forget	Remove a stored password from this computer.
remember	Store the YubiKey password on this computer to avoid having to enter it on each use.

## 7.3 ykman oath access change [OPTIONS]

**Description** Change the password used to protect OATH accounts. Allows you to set or change a password that is required to access the OATH accounts stored on the YubiKey.

### 7.3.1 Options

Option	Description
-h, --help	Show this message and exit.
-c, --clear	Clear the current password.
-n, --new-password TEXT	Provide a new password as an argument.
-p, --password TEXT	Provide a password to unlock the YubiKey.

## 7.4 ykman oath access forget [OPTIONS]

**Description** Remove a stored password from this computer.

### 7.4.1 Options

Option	Description
-h, --help	Show this message and exit.
-a, --all	Remove all stored passwords.

## 7.5 ykman oath access remember [OPTIONS]

**Description** Store the YubiKey password on this computer to avoid having to enter it on each use.

### 7.5.1 Options

Option	Description
-h, --help	Show this message and exit.
-p, --password TEXT	Provide a password to unlock the YubiKey.

## 7.6 ykman oath accounts [OPTIONS] COMMAND [ARGS]...

**Description** Manage and use OATH accounts.

### 7.6.1 Options

Option	Description
-h, --help	Show this message and exit.

### 7.6.2 Commands

Command	Description
add	Add a new account.
code	Generate codes.
delete	Delete an account.
list	List all accounts.
rename	Rename an account (Requires YubiKey 5.3 or later).
uri	Add a new account from an otpauth:// URI.

## 7.7 ykman oath accounts add [OPTIONS] NAME [SECRET]

**Description** Add a new account. This adds a new OATH account to the YubiKey.

### 7.7.1 Arguments

Argument	Description
NAME	Provide a name for this account.
SECRET	Optional.

### 7.7.2 Options

Option	Description
-h, --help	Show this message and exit.
-a, --algorithm [SHA1 SHA256 SHA512]	Algorithm to use for code generation.[default: SHA1]
-c, --counter INTEGER	Initial counter value for HOTP accounts.
-d, --digits [6 7 8]	Number of digits in generated code. [default: 6]
-f, --force	Confirm the action without prompting.
-i, --issuer TEXT	Issuer of the account.
o, --oath-type [[HOTP TOTP]	Time-based (TOTP) or counter-based (HOTP) account. [default: 32]
-p, --password TEXT	Provide a password to unlock the YubiKey.
-p, --period INTEGER	Number of seconds a TOTP code is valid. [default: 30]
-r, --remember	Remember the password on this machine.
-t, --touch	Require touch on YubiKey to generate code.

## 7.8 ykman oath accounts code [OPTIONS] [QUERY]

**Description** Generate codes. Generate codes from OATH accounts stored on the YubiKey. Accounts of type HOTP or those that require touch, also require a single match to be triggered.

### 7.8.1 Arguments

Argument	Description
QUERY	Provide a query string to match one or more specific accounts.

### 7.8.2 Options

Option	Description
-h, --help	Show this message and exit.
-H, --show-hidden	Include hidden accounts.
-p, --password TEXT	Provide a password to unlock the YubiKey.
-r, --remember	Remember the password on this machine.
-s, --single	Ensure only a single match, and output only the code.

## 7.9 ykman oath accounts delete [OPTIONS] QUERY

**Description** Delete an account. Delete an account from the YubiKey. Provide a query string to match the account to delete.

### 7.9.1 Arguments

Argument	Description
QUERY	Provide a query string to match one or more specific accounts.

### 7.9.2 Options

Option	Description
-h, --help	Show this message and exit.
-f, --force	Confirm deletion without prompting
-p, --password TEXT	Provide a password to unlock the YubiKey.
-r, --remember	Remember the password on this machine.

## 7.10 ykman oath accounts list [OPTIONS]

**Description** List all accounts. List all accounts stored on the YubiKey.

### 7.10.1 Options

Option	Description
-h, --help	Show this message and exit.
-H, --show-hidden	Include hidden accounts.
-o, --oath-type	Display the OATH type.
-p, --password TEXT	Provide a password to unlock the YubiKey.
-P, --period	Display the period.
-r, --remember	Remember the password on this machine.

## 7.11 ykman oath accounts rename [OPTIONS] QUERY NAME

**Description** Rename an account (Requires YubiKey 5.3 or later).

### 7.11.1 Arguments

Argument	Description
QUERY	A query to match a single account (as shown in list).
NAME	The name of the account (use <issuer>:<name> to specify the issuer).

### 7.11.2 Options

Option	Description
-h, --help	Show this message and exit.
-f, --force	Confirm rename without prompting.
-p, --password TEXT	Provide a password to unlock the YubiKey.
-r, --remember	Remember the password on this machine.



## 7.12 ykman oath accounts uri [OPTIONS] URI

**Description** Add a new account from an otpauth:// URI. Use a URI to add a new account to the YubiKey.

### 7.12.1 Arguments

Argument	Description
URI	Specify URI path for account.

### 7.12.2 Options

Option	Description
-h, --help	Show this message and exit.
-f, --force	Confirm the action without prompting.
-p, --password TEXT	Provide a password to unlock the YubiKey.
-r, --remember	Remember the password on this machine.
-t, --touch	Require touch on YubiKey to generate code.

## 7.13 ykman oath info [OPTIONS]

**Description** Display status of OATH application.

### 7.13.1 Options

Option	Description
-h, --help	Show this message and exit.

## 7.14 ykman oath reset [OPTIONS]

**Description** Reset all OATH data. This action deletes all accounts and restores factory settings for the OATH application on the YubiKey.

### 7.14.1 Options

Option	Description
-h, --help	Show this message and exit.
-f, --force	Confirm the action without prompting.

To get in touch with Yubico Support, go to <https://support.yubico.com/hc/en-us/requests/new>.

To get in touch with Yubico Support, [click here](#).



## OPENPGP COMMANDS

Acronyms and their definitions are listed at the bottom of the *Base Commands* page.

### 8.1 ykman openpgp [OPTIONS] COMMAND [ARGS]...

**Description** Manage OpenPGP Application.

#### 8.1.1 Examples

- Set the retries for PIN, Reset Code and Admin PIN to 10:

```
$ ykman openpgp set-retries 10 10 10
```

- Require touch to use the authentication key:

```
$ ykman openpgp set-touch aut on
```

#### 8.1.2 Options

Option	Description
-h, --help	Show this message and exit.

#### 8.1.3 Commands

Command	Description
access	Manage PIN, Reset Code, and Admin PIN.
certificates	Manage certificates.
info	Display general status of the OpenPGP application.
keys	Manage private keys.
reset	Reset all OpenPGP data.

## 8.2 ykman openpgp access [OPTIONS] COMMAND [ARGS]...

**Description** Manage PIN, Reset Code and Admin PIN.

### 8.2.1 Options

Option	Description
-h, --help	Show this message and exit.

### 8.2.2 Commands

Command	Description
set-retries	Set PIN, Reset Code and Admin PIN retries.

## 8.3 ykman openpgp access set-retries [OPTIONS] PIN-RETRIES RESET-CODE-RETRIES ADMIN-PIN-RETRIES

**Description** Set PIN, Reset Code and Admin PIN retries.

### 8.3.1 Arguments

Argument	Description
PIN-RETRIES	Set number of retries for PIN attempts.
RESET-CODE-RETRIES	Set number of retries for RESET CODE attempts.
ADMIN-PIN-RETRIES	Set number of retries for ADMIN PIN attempts.

### 8.3.2 Options

Option	Description
-h, --help	Show this message and exit.
-a, --admin-pin TEXT	Admin PIN for OpenPGP.
-f, --force	Confirm the action without prompting.

## 8.4 ykman openpgp certificates [OPTIONS] COMMAND [ARGS]...

**Description** Manage certificates.

### 8.4.1 Options

Option	Description
-h, --help	Show this message and exit.

### 8.4.2 Commands

Command	Description
delete	Delete an OpenPGP certificate.
export	Export an OpenPGP certificate.
import	Import an OpenPGP certificate.

## 8.5 ykman openpgp certificates delete [OPTIONS] KEY

**Description** Delete an OpenPGP certificate.

### 8.5.1 Arguments

Argument	Description
KEY	Key slot to delete certificate from sig, enc, aut, or att

### 8.5.2 Options

Option	Description
-h, --help	Show this message and exit.
-a, --admin-pin TEXT	Admin PIN for OpenPGP.

## 8.6 ykman openpgp certificates export [OPTIONS] KEY CERTIFICATE

**Description** Export an OpenPGP certificate.

### 8.6.1 Arguments

Argument	Description
CERTIFICATE	File to write certificate to. Use '-' to use stdout.
KEY	Key slot to read from (sig, enc, aut, or att).

### 8.6.2 Options

Option	Description
-h, --help	Show this message and exit.
-F, --format [PEM DER]	Encoding format. [Default: PEM]

## 8.7 ykman openpgp certificates import [OPTIONS] KEY CERTIFICATE

**Description** Import an OpenPGP certificate.

### 8.7.1 Arguments

Argument	Description
CERTIFICATE	File containing the certificate. Use '-' to use stdin.
KEY	Key slot to import certificate to (sig, enc, aut, or att).

## 8.7.2 Options

Option	Description
-h, --help	Show this message and exit.
-a, --admin-pin TEXT	Admin PIN for OpenPGP.

## 8.8 ykman openpgp keys [OPTIONS] COMMAND [ARGS]...

**Description** Manage private keys.

### 8.8.1 Options

Option	Description
-h, --help	Show this message and exit.

### 8.8.2 Commands

Command	Description
attest	Generate an attestation certificate for a key.
import	Import a private key (ONLY SUPPORTS ATTESTATION KEY).
set-touch	Set touch policy for OpenPGP keys.

## 8.9 ykman openpgp keys attest [OPTIONS] KEY CERTIFICATE

**Description** Generate an attestation certificate for a key. Attestation is used to show that an asymmetric key was generated on the YubiKey and therefore doesn't exist outside the device.

### 8.9.1 Arguments

Argument	Description
KEY	Key slot to attest (sig, enc, aut).
CERTIFICATE	File to write attestation certificate to. Use '-' to use stdout.

## 8.9.2 Options

Option	Description
-h, --help	Show this message and exit.
-F, --format [PEM DER]	Encoding format. [Default: PEM]
-P, --pin TEXT	PIN code.

## 8.10 ykman openpgp keys import [OPTIONS] KEY PRIVATE-KEY

**Description** Import a private key (ONLY SUPPORTS ATTESTATION KEY). Import a private key for OpenPGP attestation.

### 8.10.1 Arguments

Argument	Description
KEY	Key slot to import (sig, enc, aut).
PRIVATE-KEY	File containing the private key. Use '-' to use stdin.

### 8.10.2 Options

Option	Description
-h, --help	Show this message and exit.
-a, --admin-pin TEXT	Admin PIN for OpenPGP.

## 8.11 ykman openpgp keys set-touch [OPTIONS] KEY POLICY

**Description** Set touch policy for OpenPGP keys.

### 8.11.1 Arguments

Argument	Description
KEY	Key slot to set (sig, enc, aut or att).
POLICY	Touch policy to set (on, off, fixed, cached or cached-fixed).

The touch policy is used to require user interaction for all operations using the private key on the YubiKey. The touch policy is set individually for each key slot. To see the current touch policy, run:

```
$ ykman openpgp info
```



## 8.11.2 Touch Policies

Policy	Description
Cached	Touch required, cached for 15s after use.
Cached-Fixed	Touch required, cached for 15s after use, can't be disabled without a full reset.
Fixed	Touch required, can't be disabled without a full reset.
Off	No touch required. (default)
On	Touch required.

## 8.11.3 Options

Option	Description
-h, --help	Show this message and exit.
-a, --admin-pin TEXT	Admin PIN for OpenPGP.
-f, --force	Confirm the action without prompting.

## 8.12 ykman openpgp info [OPTIONS]

**Description** Display status of OpenPGP application.

### 8.12.1 Options

Option	Description
-h, --help	Show this message and exit.

## 8.13 ykman openpgp reset [OPTIONS]

**Description** Reset OpenPGP application. This action wipes all OpenPGP data, and sets all PINs to their default values.

### 8.13.1 Options

Option	Description
-h, --help	Show this message and exit.
-f, --force	Confirm the action without prompting.

To get in touch with Yubico Support, go to <https://support.yubico.com/hc/en-us/requests/new>.

To get in touch with Yubico Support, [click here](#).



## OTP COMMANDS

Acronyms and their definitions are listed at the bottom of the *Base Commands* page.

### 9.1 ykman otp [OPTIONS] COMMAND [ARGS]...

**Description** Manage OTP application. The YubiKey provides two keyboard-based slots that can each be configured with a credential. Several credential types are supported. A slot configuration can be write-protected with an access code. This prevents the configuration from being overwritten without the access code provided.

---

**Note:** Mode-switching the YubiKey is not possible when a slot is configured with an access code.

---

#### 9.1.1 Examples

- Swap the configurations between the two slots:  

```
$ ykman otp swap
```
- Program a random challenge-response credential to slot 2:  

```
$ ykman otp chalresp --generate 2
```
- Program a Yubico OTP credential to slot 1, using the serial as public id:  

```
$ ykman otp yubiotp 1 --serial-public-id
```
- Program a random 38 character long static password to slot 2:  

```
$ ykman otp static --generate 2 --length 38
```

#### 9.1.2 Options

Option	Description
-h, --help	Show this message and exit.
--access-code HEX	A 6-byte access code. Set to empty to use a prompt for input.

### 9.1.3 Commands

Command	Description
calculate	Perform a challenge-response operation.
chalresp	Program a challenge-response credential.
delete	Deletes the configuration stored in a slot.
hotp	Program an HMAC-SHA1 OATH-HOTP credential.
info	Display general status of the YubiKey OTP slots.
ndef	Configure a slot to be used over NDEF (NFC).
settings	Update the settings for a slot.
static	Configure a static password.
swap	Swaps the two slot configurations.
yubiotp	Program a Yubico OTP credential.

## 9.2 ykman otp calculate [OPTIONS] {1|2} [CHALLENGE]

**Description** Perform a challenge-response operation. Send a challenge (in hex) to a YubiKey slot with a challenge-response credential, and read the response. Supports output as an OATH-TOTP code.

### 9.2.1 Arguments

Argument	Description
CHALLENGE	

### 9.2.2 Options

Option	Description
-h, --help	Show this message and exit.
-d, --digits [6 8]	Number of digits in generated TOTP code. [Default: 6]
-T, --totp	Generate a TOTP code, use the current time if challenge is omitted.

## 9.3 ykman otp chalresp [OPTIONS] {1|2} [KEY]

**Description** Program a challenge-response credential.

### 9.3.1 Arguments

Argument	Description
KEY	If KEY is not specified, an interactive prompt asks for it.

### 9.3.2 Options

Option	Description
-h, --help	Show this message and exit.
-f, --force	Confirm the action without prompting.
-g, --generate	Generate a random secret key. Conflicts with KEY argument.
-t, --touch	Require touch on the YubiKey to generate a response.
-T, --totp	Use a base32-encoded key for TOTP credentials.

## 9.4 ykman otp delete [OPTIONS] {1|2}

**Description** Deletes the configuration in the specified slot.

### 9.4.1 Options

Option	Description
-h, --help	Show this message and exit.
-f, --force	Confirm the action without prompting.

## 9.5 ykman otp hotp [OPTIONS] {1|2} [KEY]

**Description** Program an HMAC-SHA1 OATH-HOTP credential.

### 9.5.1 Arguments

Argument	Description
KEY	

### 9.5.2 Options

Option	Description
-h, --help	Show this message and exit.
-d, --digits [6 8]	Number of digits in generated code. [Default: 6]
-c, --counter INTEGER	Initial counter value.
--no-enter	Do not send an <b>Enter</b> keystroke after outputting the code.
-f, --force	Confirm the action without prompting.

## 9.6 ykman otp info [OPTIONS]

**Description** Display general status of YubiKey OPT slots.

### 9.6.1 Options

Option	Description
-h, --help	Show this message and exit.

## 9.7 ykman otp ndef [OPTIONS] {1|2}

**Description** Configure a slot to be used over NDEF (NFC). The default prefix is used if no prefix is specified:

“https://my.yubico.com/yk/#”

## 9.7.1 Options

Option	Description
-h, --help	Show this message and exit.
-p, --prefix TEXT	Added before the NDEF payload. Typically a URI.

## 9.8 ykman otp settings [OPTIONS] {1|2}

**Description** Update the settings for a slot. Change the settings for a slot without changing the stored secret. All settings not specified are written with default values.

### 9.8.1 Options

Option	Description
-h, --help	Show this message and exit.
-A, --new-access-code HEX	Set a new 6-byte access code for the slot. Set to empty to use a prompt for input.
--delete-access-code	Remove access code from the slot.
--enter / --no-enter	Should send <b>Enter</b> keystroke after slot output. [Default: True]
-f, --force	Confirm the action without prompting.
-p, --pacing [0 20 40 60]	Throttle output speed by adding a delay (in ms) between characters emitted. [Default: 0]
--use-numeric-keypad	Use scancodes for numeric keypad when sending digits. Helps with some keyboard layouts. [Default: False]

## 9.9 ykman otp static [OPTIONS] {1|2} [PASSWORD]

**Description** Configure a static password. To avoid problems with different keyboard layouts, the following characters (upper and lower case) are allowed by default:

c b d e f g h i j k l n r t u v

Use the `--keyboard-layout` option to allow more characters based on preferred keyboard layout.

### 9.9.1 Arguments

Argument	Description
PASSWORD	Specify if required.

### 9.9.2 Options

Option	Description
<code>-h, --help</code>	Show this message and exit.
<code>-f, --force</code>	Confirm the action without prompting.
<code>-g, --generate</code>	Generate a random password.
<code>-k, --keyboard-layout</code> [[MODHEX US UK DE FR IT BEPO NORMAN]	Keyboard layout to use for the static password. [Default: KEYBOARD_LAYOUT.MODHEX]
<code>-l, --length LENGTH</code>	Length of generated password. [Default: 38;1<=x<=38]
<code>--no-enter</code>	Do not send an <b>Enter</b> keystroke after outputting the password.

## 9.10 ykman otp swap [OPTIONS]

**Description** Swaps the two slot configurations.



## 9.10.1 Options

Option	Description
-h, --help	Show this message and exit.
-f, --force	Confirm the action without prompting.

## 9.11 ykman otp yubiotp [OPTIONS] {1|2}

**Description** Program a Yubico OTP credential.

### 9.11.1 Options

Option	Description
-h, --help	Show this message and exit.
-f, --force	Confirm the action without prompting.
-k, --key HEX	16-byte secret key.
-g, --generate-private-id	Generate a random private ID. Conflicts with --private-id.
-G, --generate-key	Generate a random secret key. Conflicts with --key.
--no-enter	Do not send an <b>Enter</b> keystroke after emitting the OTP.
-P, --public-id MODHEX	Public identifier prefix.
-p, --private-id HEX	6-byte private identifier.
-S, --serial-public-id	Use YubiKey serial number as public ID. Conflicts with --public-id.
-u, --upload	Upload credential to YubiCloud (opens in browser). Conflicts with --force.

To get in touch with Yubico Support, go to <https://support.yubico.com/hc/en-us/requests/new>.

To get in touch with Yubico Support, [click here](#).

## PIV COMMANDS

Acronyms and their definitions are listed at the bottom of the *Base Commands* page.

### 10.1 ykman piv [OPTIONS] COMMAND [ARGS]...

**Description** Manage the PIV Application.

#### 10.1.1 Examples

- Generate an ECC P-256 private key and a self-signed certificate in slot 9a:

```
$ ykman piv keys generate --algorithm ECCP256 9a pubkey.pem
$ ykman piv certificates generate --subject "yubico" 9a pubkey.pem
```

- Change the PIN from 123456 to 654321:  
\$ ykman piv access change-pin --pin 123456 --new-pin 654321
- Reset all PIV data and restore default settings:  
\$ ykman piv reset

#### 10.1.2 Options

Option	Description
-h, --help	Show this message and exit.

#### 10.1.3 Commands

Command	Description
access	Manage PIN, PUK and Management Key.
certificates	Manage certificates.
info	Display general status of the PIV application.
keys	Manage private keys.
objects	Manage PIV data objects.
reset	Reset all PIV data.

## 10.2 ykman piv access [OPTIONS] COMMAND [ARGS]...

**Description** Manage PIN, PUK, and Management Key.

### 10.2.1 Options

Option	Description
-h, --help	Show this message and exit.

### 10.2.2 Commands

Command	Description
change-management-key	Change the management key.
change-pin	Change the PIN code.
change-puk	Change the PUK code.
set-retries	Set the number of PIN and PUK retry attempts.
unlock-pin	Unlock the PIN (using PUK).

## 10.3 ykman piv access change-management-key [OPTIONS]

**Description** Change the management key. Management functionality is guarded by a management key. This key is required for administrative tasks, such as generating key pairs. A random key may be generated and stored on the YubiKey, protected by PIN.

### 10.3.1 Options

Option	Description
-h, --help	Show this message and exit.
-a, --algorithm [TDES AES128 AES192 AES256]	Management key algorithm. [Default: TDES]
-f, --force	Confirm the action without prompting.
-g, --generate	Generate a random management key. Implied by --protect unless --new-management-key is also given. Conflicts with --new-management-key.
-m, --management-key TEXT	Current management key.
-n, --new-management-key TEXT	A new management key.
-p, --protect	Store new management key on the YubiKey, protected by PIN. A random key is used if no key is provided.
-P, --pin TEXT	PIN code.
-t, --touch	Require touch on YubiKey when prompted for management key.

## 10.4 ykman piv access change-pin [OPTIONS]

**Description** Change the PIN code. The PIN must be between 6 and 8 characters long, and it can be any type of alphanumeric character. For cross-platform compatibility, numeric PINs are recommended.

### 10.4.1 Options

Option	Description
-h, --help	Show this message and exit.
-n, --new-pin TEXT	A new PIN.
-P, --pin TEXT	Current PIN code.

## 10.5 ykman piv access change-puk [OPTIONS]

**Description** Change the PUK code. If the PIN is lost or blocked it can be reset using a PUK. The PUK must be between 6 and 8 characters long, and it can be any type of alphanumeric character.

### 10.5.1 Options

Option	Description
-h, --help	Show this message and exit.
-n, --new-puk TEXT	A new PUK code.
-p, --puk TEXT	Current PUK code.

## 10.6 ykman piv access set-retries [OPTIONS] PIN-RETRIES PUK-RETRIES

**Description** Set the number of PIN and PUK retry attempts.

---

**Note:** This resets the PIN and PUK to their factory defaults.

---

### 10.6.1 Arguments

Argument	Description
PIN-RETRIES	Set number of retries for PIN attempts.
PUK-RETRIES	Set number of retries for PUK attempts.

### 10.6.2 Options

Option	Description
-h, --help	Show this message and exit.
-f, --force	Confirm the action without prompting.
-m, --management-key TEXT	The management key.
-P, --pin TEXT	PIN code.

## 10.7 ykman piv access unblock-pin [OPTIONS]

**Description** Unblock the PIN (using PUK).

## 10.7.1 Options

Option	Description
-h, --help	Show this message and exit.
-n, --new-pin NEW-PIN	A new PIN code.
-p, --puk TEXT	Current PUK code.

## 10.8 ykman piv certificates [OPTIONS] COMMAND [ARGS]...

**Description** Manage certificates.

### 10.8.1 Options

Option	Description
-h, --help	Show this message and exit.

### 10.8.2 Commands

Option	Description
delete	Delete a certificate.
export	Export an X.509 certificate.
generate	Generate a self-signed X.509 certificate.
import	Import an X.509 certificate.
request	Generate a Certificate Signing Request (CSR).

## 10.9 ykman piv certificates delete [OPTIONS] SLOT

**Description** Delete a certificate. Delete a certificate from a PIV slot on the YubiKey.

### 10.9.1 Arguments

Argument	Description
SLOT	PIV slot of the certificate.

## 10.9.2 Options

Option	Description
-h, --help	Show this message and exit.
-m, --management-key TEXT	The management key.
-P, --pin TEXT	PIN code.

## 10.10 ykman piv certificates export [OPTIONS] SLOT CERTIFICATE

**Description** Export an X.509 certificate. Reads a certificate from one of the PIV slots on the YubiKey.

### 10.10.1 Arguments

Argument	Description
SLOT	PIV slot of the certificate.
CERTIFICATE	File to write certificate to. Use '-' to use <code>stdout</code> .

### 10.10.2 Options

Option	Description
-h, --help	Show this message and exit.
-F, --format [PEM DER]	Encoding format. [Default: PEM]

## 10.11 ykman piv certificates generate [OPTIONS] SLOT PUBLIC-KEY

**Description** Generate a self-signed X.509 certificate. A self-signed certificate is generated and written to one of the slots on the YubiKey. A private key must already be present in the corresponding key slot.

### 10.11.1 Arguments

Argument	Description
SLOT	PIV slot of the certificate.
PUBLIC-KEY	File containing a public key. Use '-' to use <code>stdin</code> .



### 10.11.2 Options

Option	Description
-h, --help	Show this message and exit.
-a, --hash-algorithm [SHA1 SHA256 SHA384 SHA512]	Hash algorithm. [default: SHA256]
-d, --valid-days INTEGER	Number of days until the certificate expires. [Default: 365]
-m, --management-key TEXT	The management key.
-P, --pin TEXT	PIN code.
-s, --subject TEXT	Subject for the certificate, as an RFC 4514 string. [required].

## 10.12 ykman piv certificates import [OPTIONS] SLOT CERTIFICATE

**Description** Import an X.509 certificate. Write a certificate to one of the PIV slots on the YubiKey.

### 10.12.1 Arguments

Argument	Description
SLOT	PIV slot of the certificate.
CERTIFICATE	File containing the certificate. Use '-' to use <code>stdin</code> .

### 10.12.2 Options

Option	Description
-h, --help	Show this message and exit.
-m, --management-key TEXT	The management key.
-p, --password TEXT	A password may be needed to decrypt the data.
-P, --pin TEXT	PIN code.
-v, --verify	Verify that the certificate matches the private key in the slot.

## 10.13 `ykman piv certificates request [OPTIONS] SLOT PUBLIC-KEY CSR`

**Description** Generate a Certificate Signing Request (CSR). A private key must already be present in the corresponding key slot.

### 10.13.1 Arguments

Argument	Description
CSR	File to write CSR to. Use '-' to use stdout.
PUBLIC-KEY	File containing a public key. Use '-' to use stdin.
SLOT	PIV slot of the certificate.

### 10.13.2 Options

Option	Description
<code>-h, --help</code>	Show this message and exit.
<code>-a, --hash-algorithm [SHA1 SHA256 SHA384 SHA512]</code>	Hash algorithm. [default: SHA256]
<code>-P, --pin TEXT</code>	PIN code.
<code>-s, --subject TEXT</code>	Subject for the requested certificate, as an RFC 4514 string. [Required]

## 10.14 `ykman piv info [OPTIONS]`

**Description** Display general status of PIV application.

### 10.14.1 Options

Option	Description
<code>-h, --help</code>	Show this message and exit.

## 10.15 ykman piv keys [OPTIONS] COMMAND [ARGS]...

**Description** Manage private keys.

### 10.15.1 Options

Option	Description
-h, --help	Show this message and exit.

### 10.15.2 Commands

Command	Description
attest	Generate an attestation certificate for a key pair.
export	Export a public key corresponding to a stored private key.
generate	Generate an asymmetric key pair.
import	Import a private key from file.

## 10.16 ykman piv keys attest [OPTIONS] SLOT CERTIFICATE

**Description** Generate an attestation certificate for a key pair. Attestation is used to show that an asymmetric key was generated on the YubiKey and therefore doesn't exist outside the device.

### 10.16.1 Arguments

Argument	Description
CERTIFICATE	File to write attestation certificate to. Use '-' to use stdout.
SLOT	PIV slot of the private key.

### 10.16.2 Options

Option	Description
-h, --help	Show this message and exit.
-F, --format [PEM DER]	Encoding format. [Default: PEM]

## 10.17 `ykman piv keys export [OPTIONS] SLOT PUBLIC-KEY`

**Description** Export a public key corresponding to a stored private key. This command uses several different mechanisms for exporting the public key corresponding to a stored private key, which may fail. If a certificate is stored in the slot it is assumed to contain the correct public key. If this is not the case, the wrong public key will be returned. The `--verify` flag can be used to verify that the public key being returned matches the private key, by using the slot to create and verify a signature. This may require the PIN to be provided.

### 10.17.1 Arguments

Argument	Description
PUBLIC-KEY	File containing the generated public key. Use <code>-</code> to use <code>stdout</code> .
SLOT	PIV slot of the private key.

### 10.17.2 Options

Option	Description
<code>-h, --help</code>	Show this message and exit.
<code>-F, --format [PEM DER]</code>	Encoding format. [default: PEM]
<code>-P, --pin TEXT</code>	PIN code (used for <code>--verify</code> ).
<code>-v, --verify</code>	Verify that the public key matches the private key in the slot.

## 10.18 `ykman piv keys generate [OPTIONS] SLOT PUBLIC-KEY`

**Description** Generate an asymmetric key pair. The private key is generated on the YubiKey, and written to one of the slots.

### 10.18.1 Arguments

Argument	Description
PUBLIC-KEY	File containing the generated public key. Use <code>'-'</code> to use <code>stdout</code> .
SLOT	PIV slot of the private key.

## 10.18.2 Options

Option	Description
-h, --help	Show this message and exit.
-a, --algorithm [RSA1024 RSA2048 ECCP256 ECCP384]	Algorithm to use in key generation. [Default: RSA2048]
-F, --format [PEM DER]	Encoding format. [Default: PEM]
-m, --management-key TEXT	The management key.
-P, --pin TEXT	PIN code.
--pin-policy [DEFAULT  NEVER ONCE ALWAYS]	PIN policy for slot.
--touch-policy [DEFAULT  NEVER ALWAYS CACHED]	Touch policy for slot.

## 10.19 ykman piv keys import [OPTIONS] SLOT PRIVATE-KEY

**Description** Import a private key from file. Write a private key to one of the PIV slots on the YubiKey.

### 10.19.1 Arguments

Argument	Description
PRIVATE-KEY	File containing the private key. Use '-' to use stdin.
SLOT	PIV slot of the private key.

## 10.19.2 Options

Option	Description
-h, --help	Show this message and exit.
-m, --management-key TEXT	The management key.
--pin-policy [DEFAULT NEVER ONCE ALWAYS]	PIN policy for slot.
-p, --password TEXT	Password used to decrypt the private key.
-P, --pin TEXT	PIN code.
--touch-policy [DEFAULT NEVER ALWAYS CACHED]	Touch policy for slot.

## 10.20 ykman piv objects [OPTIONS] COMMAND [ARGS]...

**Description** Manage PIV data objects.

### 10.20.1 Examples

- Write the contents of a file to data object with ID: abc123:
 

```
$ ykman piv objects import abc123 myfile.txt
```
- Read the contents of the data object with ID: abc123 into a file:
 

```
$ ykman piv objects export abc123 myfile.txt
```
- Generate a random value for CHUID:
 

```
$ ykman piv objects generate chuid
```

### 10.20.2 Options

Option	Description
-h, --help	Show this message and exit.

### 10.20.3 Commands

Command	Description
<code>export</code>	Export an arbitrary PIV data object.
<code>generate</code>	Generate and write data for a supported data object.
<code>import</code>	Write an arbitrary PIV object.

## 10.21 ykman piv objects export [OPTIONS] OBJECT OUTPUT

**Description** Export an arbitrary PIV data object.

### 10.21.1 Arguments

Argument	Description
<code>OBJECT</code>	Name of PIV data object, or ID in HEX.
<code>OUTPUT</code>	File to write object to. Use '-' to use stdout.

### 10.21.2 Options

Option	Description
<code>-h, --help</code>	Show this message and exit.
<code>-P, --pin TEXT</code>	PIN code.

## 10.22 ykman piv objects generate [OPTIONS] OBJECT

**Description** Generate and write data for a supported data object.

### 10.22.1 Arguments

Argument	Description
<code>OBJECT</code>	Name of PIV data object, or ID in HEX. Supported data objects are: CHUID (Card Holder Unique ID) CCC (Card Capability Container)

## 10.22.2 Options

Option	Description
-h, --help	Show this message and exit.
-m, --management-key TEXT	The management key.
-P, --pin TEXT	PIN code.

## 10.23 ykman piv objects import [OPTIONS] OBJECT DATA

**Description** Write an arbitrary PIV object. Write a PIV object by providing the object id. Yubico writable PIV objects are available in the range 5f0000 - 5ffff.

### 10.23.1 Arguments

Argument	Description
DATA	File containing the data to be written. Use '-' to use stdin.
OBJECT	Name of PIV data object, or ID in HEX.

### 10.23.2 Options

Option	Description
-h, --help	Show this message and exit.
-m, --management-key TEXT	The management key.
-P, --pin TEXT	PIN code.

## 10.24 ykman piv reset [OPTIONS]

**Description** Reset all PIV data. This action wipes all data and restores factory settings for the PIV application on your YubiKey.

### 10.24.1 Options

Option	Description
-h, --help	Show this message and exit.
-f, --force	Confirm the action without prompting.

---

To get in touch with Yubico Support, [click here](#).



## YUBIHSM COMMANDS

For a full description of YubiHSM Auth, see [the corresponding chapter in the YubiKey 5 Series Technical Manual](#). YubiHSM Auth is disabled in firmware version 5.4.X.

### 11.1 Enable or Disable YubiHSM Auth on a YubiKey

This section includes the expected output and testing methods.

- Enable YubiHSM Auth by running:

```
ykman config usb --enable HSMAUTH YubiHSM Auth successfully enabled.
```

- Test enablement by connecting to the YubiHSM with YubiHSM-Shell:

```
yubihsm> session ykopen 1 "default key" "my secret" Session authenticated to YubiHSM2.
```

- Disable YubiHSM Auth by running:

```
ykman config usb --disable HSMAUTH YubiHSM Auth successfully disabled.
```

- Test disablement by connecting to the YubiHSM with YubiHSM-Shell:

```
yubihsm> session ykopen 1 "default key" "my secret" No access to the YubiKey application YubiHSM Auth.
```

---

To get in touch with Yubico Support, [click here](#).



## COPYRIGHT

© 2021 Yubico AB. All rights reserved.

### Trademarks

Yubico and YubiKey are registered trademarks of Yubico AB. All other trademarks are the property of their respective owners.

## 12.1 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.

## 12.2 Contact Information

To get in touch with Yubico Support, [click here](#).

Yubico Inc.  
530 Lytton Street  
Suite 301  
Palo Alto, CA 94301  
USA

More options for getting touch with us are available on the Contact page of [Yubico's website](#).

## 12.3 Document Updated

2021-07-16 20:49:24 UTC