YubiKey Manager (ykman) CLI and GUI Guide

Yubico

Aug 09, 2024

CONTENTS

CHAPTER

ONE

INTRODUCTION

Note: The Yubico site from which you download the ykman CLI - Releases - refers to the ykman CLI version as yubiKey-manager. In general, when installing, the distinction between the tools is made by calling one of them YubiKey Manager GUI and the other YubiKey Manager CLI. Also, the GUI has "qt" in its download URL. This guide makes the distinction by calling the CLI "ykman" after its command line.

This guide contains the instructions for using both YubiKey Manager GUI and ykman CLI.

- For common GUI tasks, see *Using the YubiKey Manager GUI* in this guide.
- For CLI commands, 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.

The CLI version is updated more frequently than the GUI version, so there is functionality you can use through the CLI that is not available in the GUI.

The GUI version includes an older version of the CLI. If you are going to use the CLI, install the latest version by going to Releases. See also *Installation*.

If you attempt to use a CLI command or GUI option and it fails, check the release notes to confirm the command is supported in the ykman version you are using.

- YubiKey Manager CLI Release Notes
- YubiKey Manager GUI Release Notes

1.1 YubiKey Firmware

Click for Yubico Support.

CHAPTER

TWO

INSTALLATION

Important: Yubico strongly recommends that those who want to use a GUI for configuring individual YubiKeys choose Yubico Authenticator instead of the YubiKey Manager GUI. The Authenticator is newer and has much more functionality.

Both YubiKey Manager (the GUI) and ykman (the CLI) can be installed on **Windows**, **macOS**, and **Linux** systems. The GUI is bundled with an old version of the CLI. Each has its own installer for each OS platform. Unfortunately, on developers.yubico.com both the GUI and the CLI are frequently referred to as "YubiKey Manager". In this guide we try to make the distinction by calling the GUI "YubiKey Manager" and the CLI "ykman".

2.1 Download YubiKey Manager

- Download the **YubiKey Manager GUI** installers from: YubiKey Manager Releases. Note that the URL includes `qt` - this means the GUI.

  The installers include both the full graphical application and an older version of the command line tool.

- Download **YubiKey Manager (ykman) CLI installer** from: yubikey-manager Releases.

Note: The GUI is bundled with an older version of the CLI. If you are going to use the CLI, install the latest version separately.

Note: Additional installation packages may be available from third parties.

To download ykman (CLI version) please refer to: YubiKey Manager Releases (CLI).

2.1.1 YubiKey Manager Versions and Installers

The table lists the latest installers released. See the download pages for previous versions.

For GUI releases see, yubikey-manager-qt Releases. Notice there is a `-qt` in all the GUI version installer filenames.

For CLI releases see, yubikey-manager Releases.

Table 1: **YubiKey Manager (GUI) Installers**

Version	Installer	OS	Release Date
1.2.6	yubikey-manager-qt-1.2.6-win32.exe	Windows 32 bit	2024-04-04
1.2.6	yubikey-manager-qt-1.2.6-win64.exe	Windows 64 bit	2024-04-04
1.2.5	yubikey-manager-qt-1.2.5.tar.gz	Linux - Ubuntu	2023-02-03
1.2.5	yubikey-manager-qt-1.2.5-linux.AppImage	Linus_AppImage	2023-02-03
1.2.5	yubikey-manager-qt-1.2.5-mac.pkg	macOS	2023-02-03

Table 2: **ykman (CLI) Installers**

Version	Installer	OS	Release Date
5.4.0	yubikey_manager-5.4.0.tar.gz	Ubuntu	2024-03-26
5.4.0	yubikey-manager-5.4.0-mac.pkg	macOS	2024-03-26
5.4.0	yubikey-manager-5.4.0-win64.msi	Windows 64 bit	2024-03-26

2.2 OS-independent Installation

ykman (CLI version) can be installed independently of platform by using `pip` (or equivalent). This installation method uses the Python package manager, which might be useful for people who are using the libraries that come with ykman for writing Python software. See the YubiKey Manager CLI for Python.

Note: PIP (or equivalent) must first be installed on the target system.

For the latest ykman version:

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

(For the YubiKey Manager GUI version (which has an outdated ykman CLI):

```
pip install --user yubikey-manager-qt-<version>)
```

2.2.1 Command Prompt

To install YubiKey Manager (the GUI and the (old) CLI) on Windows from Command Prompt (CMD):

1. Press the Windows key and type: “cmd”
2. Select **Run as administrator**
3. Select **Yes** when prompted to run the app in elevated mode
4. Change directory (`cd`) to where ykman was downloaded
5. Type (paste) the following: `yubikey-manager-qt-1.2.3.win64.exe` and press **Enter**.

   Replace the filename, with the actual the filename that includes the version information. For example: `yubikey-manager-1.2.3.win64.exe`. Then press **Enter**.

   ```
   ``pip install --user yubikey-manager-<version>``
   ```

Note: The YubiKey Manager installers with the `-qt` in the filename are for the GUI version. The installers without the `-qt` in the filename are for ykman, the CLI.

2.3 Windows Installation

Install the YubiKey Manager GUI and the YubiKey Manager CLI separately.

2.3.1 Install YubiKey Manager GUI

When installing from the `.exe` package (see below), installation can be made to run silently (i.e., without user interaction) by adding `/S` to the install command.

1. Download the installer. See *Download YubiKey Manager*.
2. Open a command terminal and change to your downloads directory.

```
C:\Users\<user_name> > cd Downloads
C:\Users\<user_name>\Downloads >
```

3. Confirm the installer is downloaded. Enter directory command, `dir`. View the response for the installer. For example, `yubikey-manager-qt-1.2.6-win32.exe`.
4. Enter the installation command. The example includes designating the installation path using the `/D` option.

```
C:\Users\<user_name>\Downloads >.\yubikey-manager-qt-1.2.6-win32.exe /D "C:\Program␣
↪Files\Yubico\YubiKey Manager
```

5. Complete the YubiKey Manager Setup wizard.
   a. In the Welcome screen, click **Next**.
   b. In the Choose Install Location screen, click **Next** to select the default. Optionally, click Browse to select a different location, then click **Next**.
   c. In the Choose Start Menu Folder screen, click **Install**. Optionally, select a different folder and choose to create shortcuts, then click **Install**.
   d. If a pop-up asks, Do you want to allow this app to make changes to your device?, click **Yes**.
   e. Wait while the YubiKey Manager GUI is installed. In the Installing screen, a progress bar shows the status.
   f. In the Completing YubiKey Manager Setup screen, click **Finish**. Optionally, deselect the Run YubiKey Manager.

   The YubiKey Manager icon is added to the Start menu panel.
6. Optionally, right-click the YubiKey Manager icon in the Start menu panel and select, **Pin to Start** or **Pin to taskbar**.

2.3.2 Install YubiKey Manger CLI

1. Download the installer. See *Download YubiKey Manager*.
2. Open a File Explorer and browse to the Downloads folder.
3. Double-click the installer for the latest version. For example, `yubikey-manager-5.4.0-win64.msi`.
4. Complete the YubiKey Manager CLI Setup wizard.
   a. In the Welcome screen, click **Next**.
   b. In the Destination Folder screen, click **Next** to select the default. Optionally, click Change to select a different location, then click **Next**.
   c. In the Ready to install YubiKey Manager CLI screen, click **Install**.
   d. If a pop-up asks, Do you want to allow this app to make changes to your device?, click **Yes**.
   e. Wait while the YubiKey Manager GUI is installed. In the Installing screen, a progress bar shows the status.
   f. In the Completed the YubiKey Manager CLI Setup Wizard screen, click **Finish**.
5. Optionally, from the command prompt, change to the installation directory and confirm the YubiKey Manager CLI is listed. If running from a mapped drive, you might need to add `/D <install path>`. This ensures YubiKey Manager (the GUI and the (old) CLI) is installed in the correct drive.

```
C:\Program Files> dir
Volume in drive C
Volume Serial Number is


Directory of C:\Program Files

05/31/2024  03:22 PM    <DIR>          .
02/27/2024  09:29 PM    <DIR>          Common Files
05/24/2024  01:30 PM    <DIR>          Google
05/31/2024  03:41 PM    <DIR>          Internet Explorer
05/07/2022  01:00 AM    <DIR>          WindowsPowerShell
05/31/2024  03:22 PM    <DIR>          Yubico
         0 File(s)              0 bytes
        14 Dir(s)  238,592,212,992 bytes free
```

2.4 MacOS

2.4.1 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.

2.5 MacOS Installation

Install the YubiKey Manager GUI and the YubiKey Manager CLI separately.

The installers for both the GUI and CLI versions are macOS packages.

2.5.1 Install YubiKey Manager GUI

1. Download the installer. See *Download YubiKey Manager*.
2. Open a Finder and browse to the Downloads folder.
3. Double-click the installer. For example, `yubikey-manager-qt-1.2.5-mac.pkg`.
4. Complete the YubiKey Manager installer wizard.
    a. In the Introduction screen, click **Continue**.

       The Destination Select screen is skipped and defaults are applied.

    b. In the Installation Type screen, click **Install**.
    c. If a pop-up ask to allow the installation, enter your password or use Touch ID and click **Install Software**.
    d. Wait while the YubiKey Manager is installed. In the Installation screen, a progress bar shows the status.
    e. In the Summary screen, click **Close**.
    f. Optionally, open Launchpad and locate the YubiKey Manager icon.

2.5.2 Install YubiKey Manager CLI

1. Download the installer. See *Download YubiKey Manager*.
2. Open a Finder and browse to the Downloads folder.
3. Double-click the installer for the newest version. For example, `yubikey-manager-5.4.0-mac.pkg`.
4. Complete the YubiKey-manager installer wizard.
    a. In the Introduction screen, click **Continue**. The Destination Select screen is skipped and defaults are applied.
    b. In the Installation Type screen, click **Install**.
    c. If a pop-up ask to allow the installation, enter your password or use Touch ID and click **Install Software**.
    d. Wait while the YubiKey Manager is installed. In the Installation screen, a progress bar shows the status.
    e. In the Summary screen, click **Close**.
    f. Optionally, open a terminal and run the ykman help command.

```
~ % ykman -h
Usage: ykman [OPTIONS] COMMAND [ARGS]...

Configure your YubiKey via the command line.

Examples:

List connected YubiKeys, only output serial number:
```

(continues on next page)

(continued from previous page)

```
$ ykman list --serials

Show information about YubiKey with serial number 123456:
$ ykman --device 123456 info
. . .
```

2.5.3 Using Homebrew for CLI

From the Mac's terminal run the `brew` command below.

This is the preferred install method for the CLI as it also enables native `ykman` command functionality without the need to change directories.

```
brew install ykman
```

2.6 Linux Installation

On Linux platforms you need to have `pcscd` installed and running to communicate with a YubiKey over the Smart Card 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`.

2.6.1 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.

2.7 Developers

For more information, see the ykman CLI page on developers.yubico.com. For APDUs, see the APDU page in the .NET YubiKey SDK User's Manual.

Click for Yubico Support.

CHAPTER

THREE

USING THE YUBIKEY MANAGER GUI

The Yubico Authenticator is a quick, convenient way to find out what firmware your YubiKey has and/or to reset it - unless you prefer to use ykman (CLI), which is less powerful. If you are using the YubiKey Manager and do not find what you want in it, check to see if ykman (the CLI) has it.

3.1 Launch YubiKey Manager GUI

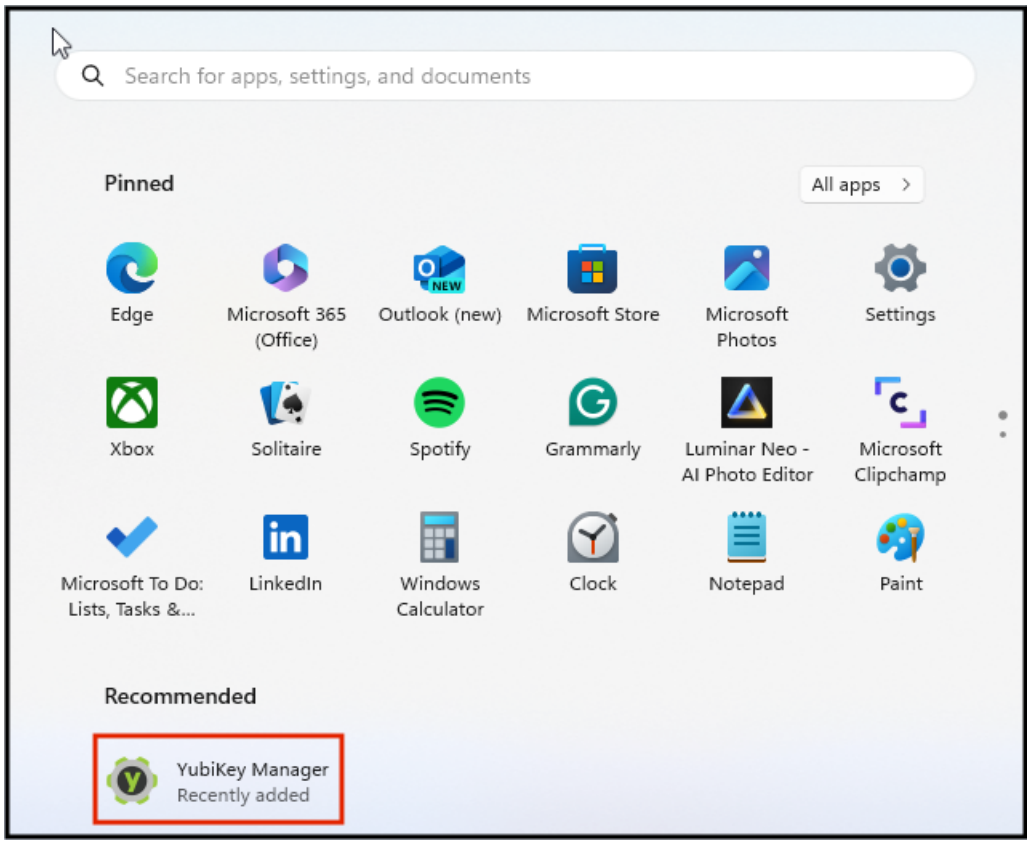
To launch YubiKey Manager follow the steps for your platform below.

3.1.1 Windows Launch

1. Open the Start menu panel, locate and click the YubiKey Manager app.
2. Optionally, right-click the YubiKey Manager icon and select, **Pin to Start** or **Pin to taskbar**.

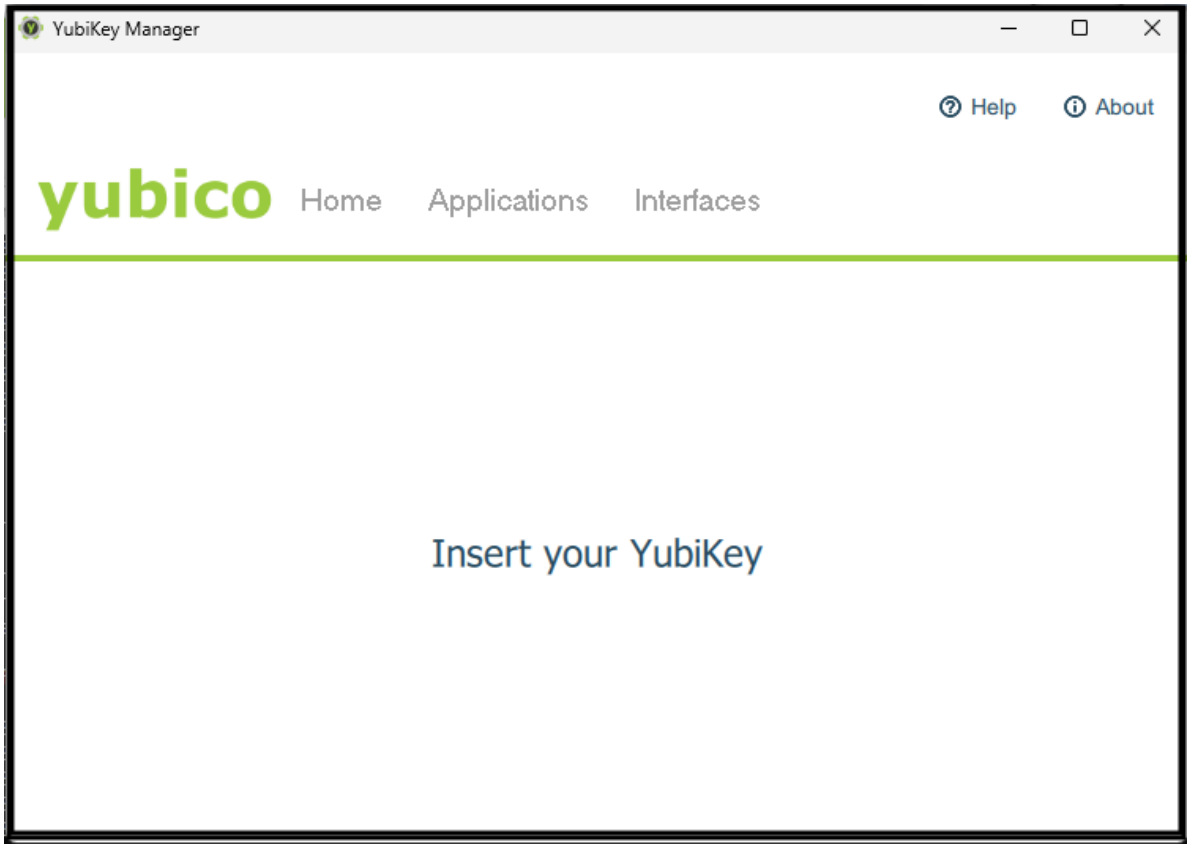
3.1.2 MacOS Launch

1. Open Launchpad, locate and click the YubiKey Manager icon.
2. Optionally, right-click the YubiKey Manager icon in the task bar and select **Options > Keep in Dock**.



3.2 View YubiKey Firmware Version

1. Launch the **YubiKey Manager**, GUI version.
2. At the YubiKey Manager prompt, insert your YubiKey and touch.



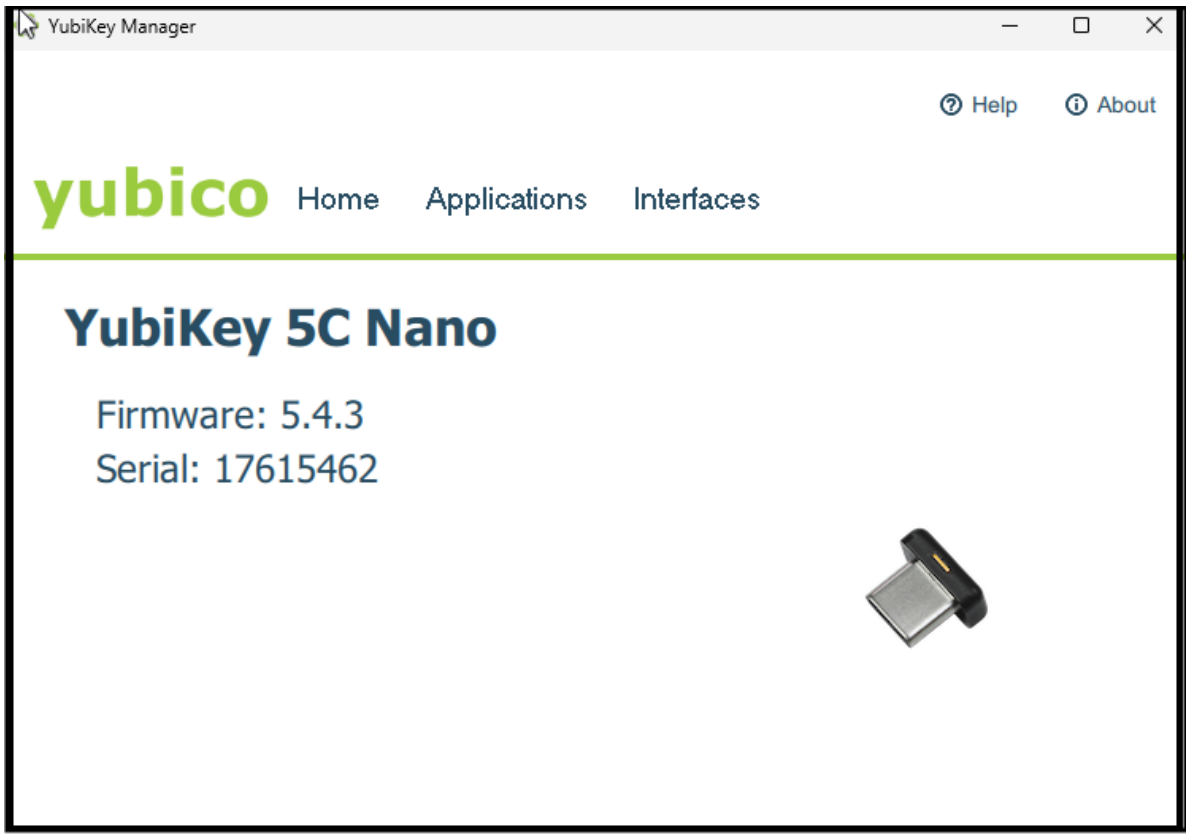
If your YubiKey is already connected, the YubiKey Manager Home tab is displayed.

Note that the tool only reads a single YubiKey at a time, so if you have multiple keys connected, it might not be evident which one YubiKey Manager is identifying.

3. View the listed YubiKey firmware version.

   When your YubiKey credential is accepted YubiKey Manager opens the **Home** tab and lists the accepted YubiKey firmware:

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



3.3 Managing Applications

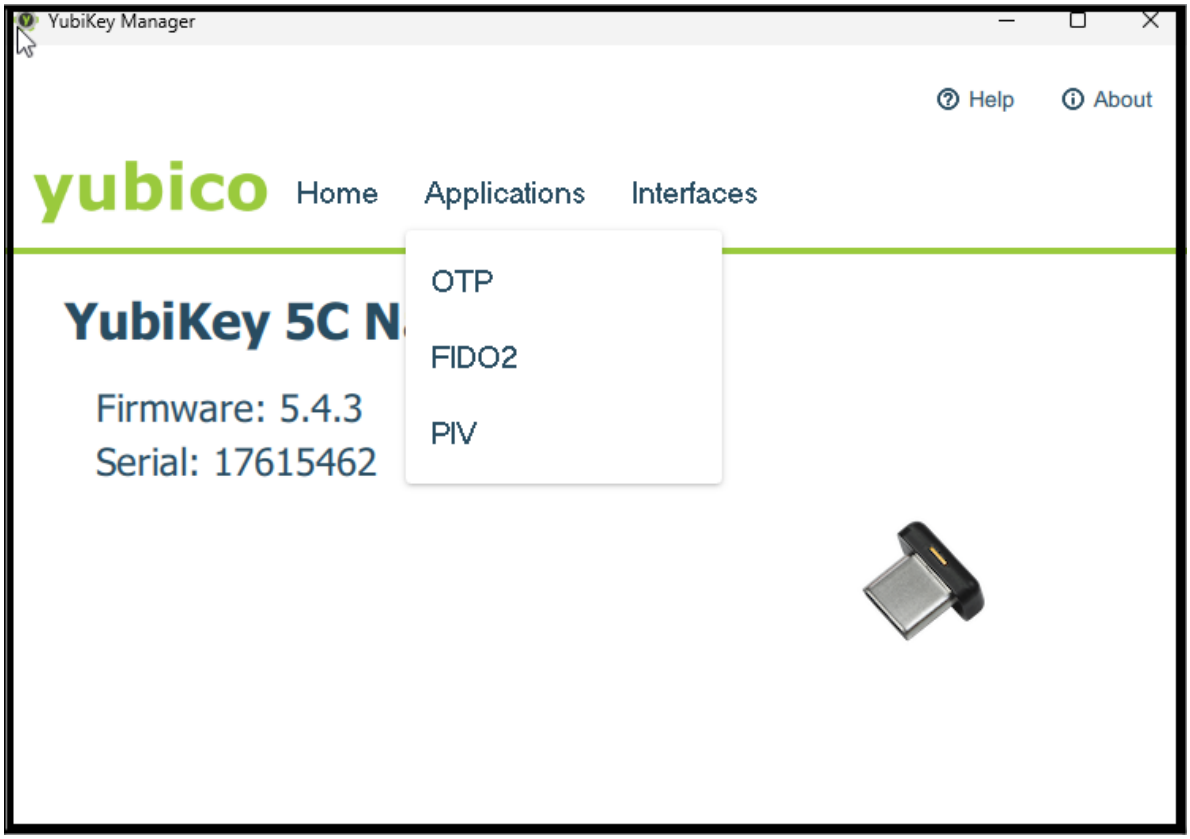
YubiKey Manager can be used to check which applications are enabled on which interface and to enable or disable each application on each physical interface.

3.3.1 View Available Interfaces

The **Interfaces** tab displays your key's form factor (for example, 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/applications by deselecting the respective checkboxes.

3.3.2 View YubiKey Enabled Applications

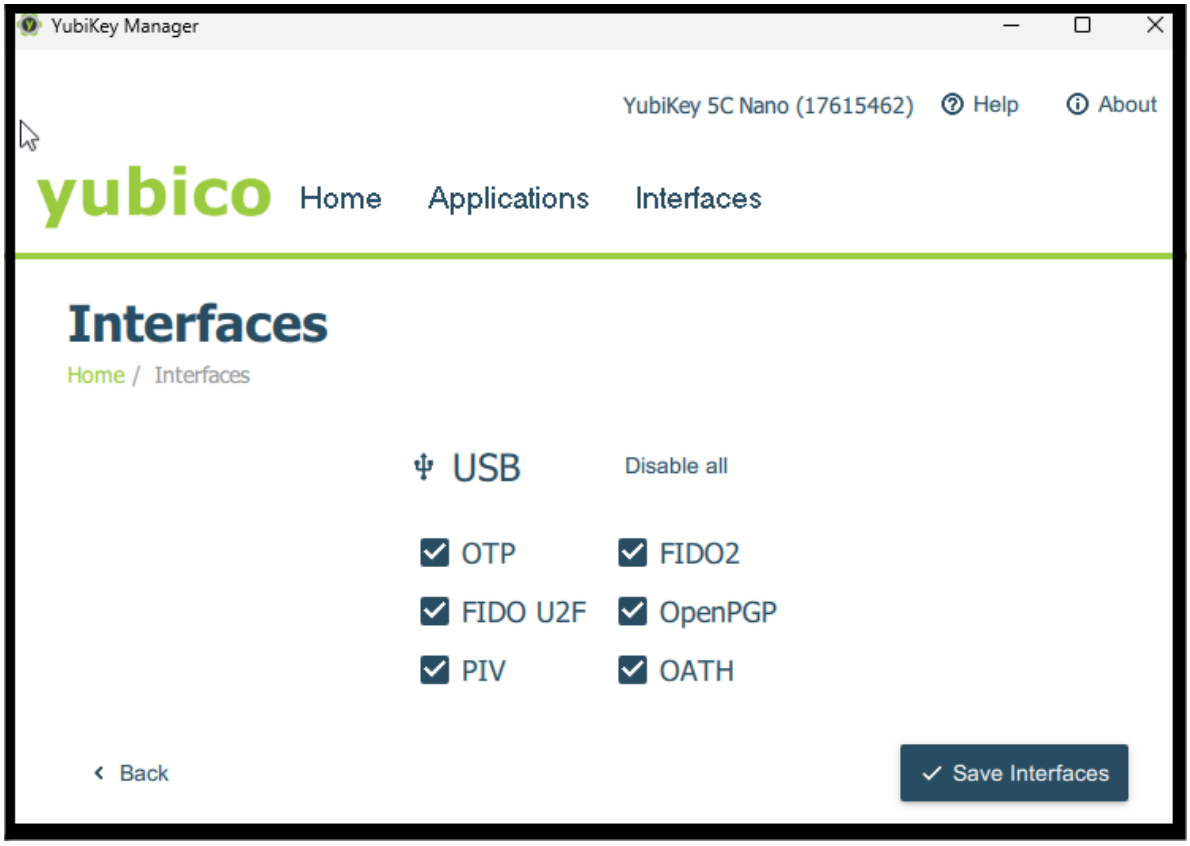
1. Launch the **YubiKey Manager**, GUI version.
2. Insert the YubiKey whose applications you want to manage.
3. View available applications. Select the **Applications** tab.



3.3.3 Enable and Disable Applications

1. Launch the **YubiKey Manager**, GUI version.
2. Insert the YubiKey whose applications you want to manage.
3. View available applications. Select the **Interfaces** tab.

   A checkbox with a tick is shown next to each enabled applications.
4. Enable to disable applications for the YubiKey.
   a. Select the checkbox to enable an application.
   b. Unselect the checkbox to disable an application.
   c. Click **Save Interfaces**.



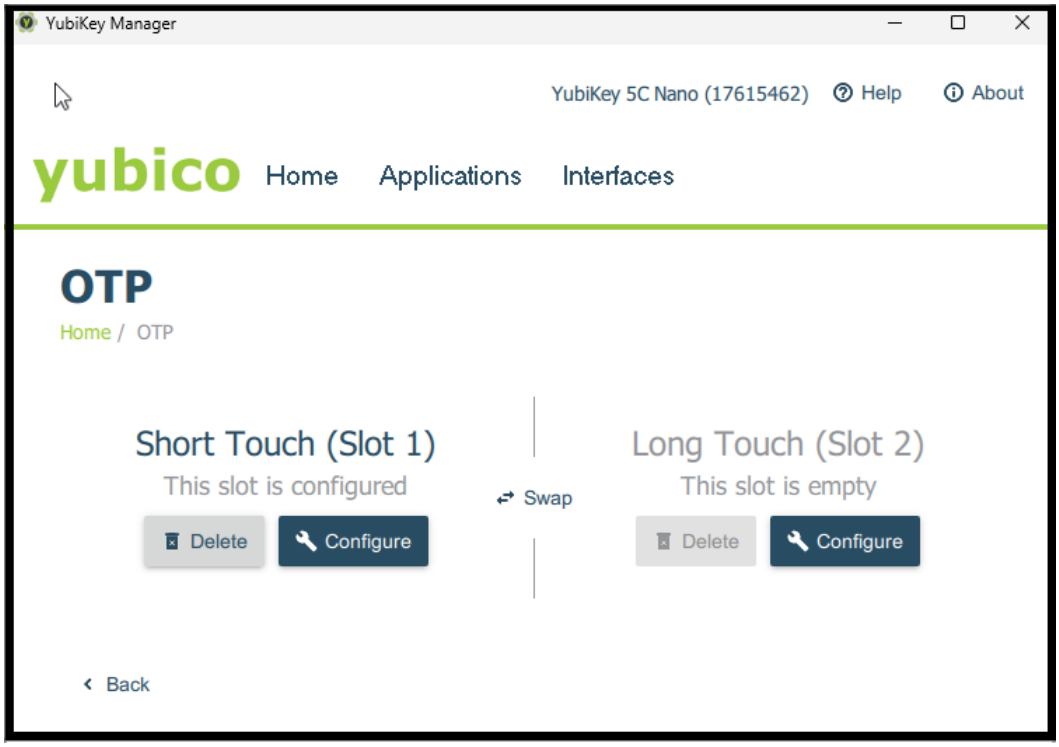
Note: For the YubiKey 5Ci, any modifications made to the applications over the USB interface also apply to the applications over Lightning®.

3.3.4 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 CLI `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]*.

3.4 Configure YubiKey Slot on YubiKey

1. Launch the **YubiKey Manager**, GUI version.
2. Insert the YubiKey whose applications you want to manage.
3. Select application to configure.
   a. Select the **Applications** tab.
   b. Select from the displayed list of applications.
4. Select the YubiKey slot to configure. Click the slot **Configure** button.

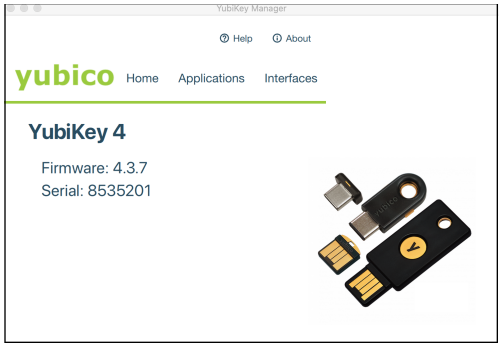


5. Complete the configuration options. These are specific to each application type.

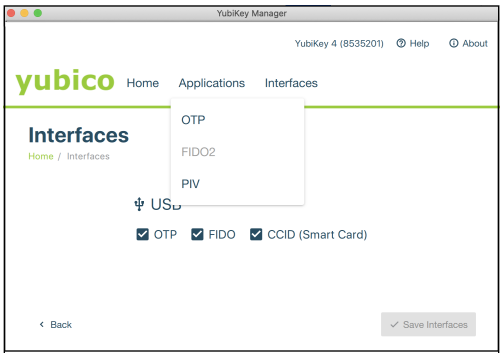
3.5 Resetting FIDO2 Function

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.

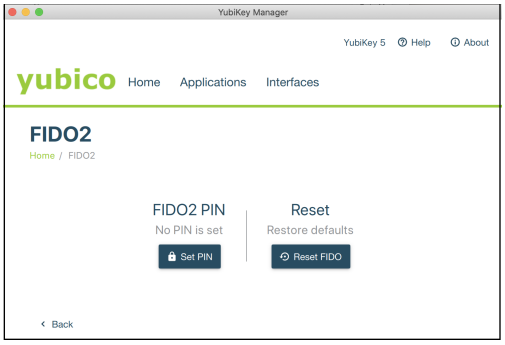
1. Remove your YubiKey if it is still connected to your machine, then launch ykman and insert your key.



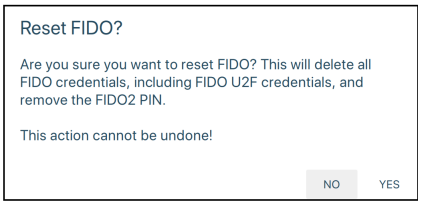
2. Click on the word **Applications** at the top of that tab. A list of menu options appears. The specific options depend on the key.



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



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



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

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

7. Touch your YubiKey. The message "FIDO applications have been reset" appears at the bottom of the **Applications** page.
8. Remove the key in preparation for re-enrolling it.

Click for Yubico Support.

CHAPTER

FOUR

USING THE YUBIKEY MANAGER CLI

The YubiKey Manager - ykman - can be used to configure all aspects of the YubiKey. This section covers the options for accessing and launching both the CLI and GUI application.

4.1 Windows Launch

Run the ykman commands from command prompt. You do not need to specifically set PATH variables for ykman.

You can launch the ykman CLI and GUI versions through the command line, select and run the command for one of the options listed below:

4.1.1 64-bit Systems

- Launch ykman **CLI**

```
C:\>"C:\Program Files\Yubico\YubiKey Manager\ykman.exe"
```

- Launch ykman **GUI**

```
C:\>"C:\Program Files\Yubico\YubiKey Manager\ykman-gui.exe"
```

4.1.2 32-bit Systems

- Launch ykman **CLI**

```
C:\>"C:\Program Files (x86)\Yubico\YubiKey Manager\ykman.exe"
```

- Launch ykman **GUI**

```
C:\>"C:\Program Files (x86)\Yubico\YubiKey Manager\ykman-gui.exe"
```

4.1.3 Debug Logging Mode

To launch ykman with **debug logging** enabled, add the following to the execution command:

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

Example:

```
C:\>"C:\Program Files (x86)\Yubico\YubiKey Manager\ykman-gui.exe"
   --log-level DEBUG --log-file %USERPROFILE%\Desktop\
   ykman-log.txt
```

4.2 macOS Launch

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

If you have installed ykman using Homebrew, referenced in the ykman Installation for MacOS, you do not need to change directories to run ykman commands in Mac's terminal. The CLI runs native commands natively.

4.2.1 Change Directory

Change directory to the location of the ykman executables. On macOS you must escape the space in the filename "YubiKey Manager.app" by putting in a backslash before the space, or you must enclose the filename in double quotes. Examples of both are given below:

```
cd /Applications/YubiKey\ Manager.app/Contents/MacOS/
```

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

4.2.2 Launch ykman CLI Mode

From the command line:

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

4.2.3 Launch ykman GUI Mode

From the command line:

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

4.2.4 Launch ykman Debug Log Mode

To run ykman with **debug logging** (to a file) enabled, add the following to the run command:

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

Example:

```
% /Applications/YubiKey Manager.app/Contents/MacOS/ykman
   --log-level DEBUG --log-file ~/Desktop/ykman.txt
```

4.3 Launch Issues

If ykman did not start as expected, there might be a PATH issue. Run the command:

```
> ykman -v
```

If you do not see the version you are expecting, you might have a PATH issue. Set the PATh variables to point to the correct version or run the ykman launch command from the ykman installation directory.

Click for Yubico Support.

CHAPTER

FIVE

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.

See the bottom of this page for acronyms and their definitions.

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

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

5.1.3 Commands

Command	Description
`config`	Enable/Disable applications.
`fido`	Manage the FIDO applications.
`hsmauth`	Manage the YubiHSM Auth application.
`info`	Show general information.
`list`	List connected YubiKeys.
`oath`	Manage the OATH Application.
`openpgp`	Manage the OpenPGP Application.
`otp`	Manage the OTP Application.
`piv`	Manage the PIV Application.
`script`	Run a python script.

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

Configure the YubiKey, enable or disable applications. The applications can be enabled and disabled independently over different transports (USB and NFC). The configuration can 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

Commmand	Description
`mode`	Manage connection modes (USB interfaces).
`nfc`	Enable or disable applications over NFC.
`reset`	Reset all YubiKey data.
`set-lock-code`	Set or change the configuration lock code.
`usb`	Enable or disable applications over USB.

5.3 ykman config mode [OPTIONS] MODE

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 the smartcard between ejected and inserted (CCID mode only).

5.4 ykman config nfc [OPTIONS]

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 Usage: ykman config reset [OPTIONS]

Reset all YubiKey data.

This command is used with the YubiKey Bio Multi-protocol Edition.

This action wipes all data and restores factory settings for all applications on the YubiKey.

5.5.1 Options

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

5.6 ykman config set-lock-code [OPTIONS]

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.

5.6.1 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.

5.7 ykman config usb [OPTIONS]

Enable or disable applications over USB.

5.7.1 Options

Option	Description
`-h, --help`	Show this message and exit.
`-a, --enable-all`	Enable all applications.
`--autoeject-timeout SECONDS`	When set, the smartcard automaticall 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).

5.8 ykman info [OPTIONS]

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

5.8.1 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.

5.8.2 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

FIPS approved applications
FIDO2:        False
OATH:         True
PIV:          False
OpenPGP:      False
YubiHSM Auth: False
```

5.9 ykman list [OPTIONS]

List connected YubiKeys.

5.9.1 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.

5.10 ykman script [OPTIONS] FILE [ARGUMENTS]

Run a python script.

Warning: Never run a script without fully understanding what it does!

Scripts are very powerful, and have the power to harm to both your YubiKey and your computer.

ONLY run scripts that you fully trust!

Argument can be passed to the script by adding them after the end of the command. These will be accessible inside the script as sys.argv, with the script name as the initial value. For more information on scripting, see the "Scripting" page in the documentation.

5.10.1 Examples

Run the file `myscript.py`, passing arguments `123456` and `indata.csv`:

```
$ ykman script myscript.py 123456 indata.csv
```

5.10.2 Options

Option	Description
`-h, --help`	Show this message and exit.
`-f, --force`	Confirm the action without prompting.
`-s, --site-dir DIR`	Specify additional path(s) to load python modules from

5.11 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

Click for Yubico Support.

CHAPTER

SIX

FIDO COMMANDS

On Windows, FIDO operations are privileged. Therefore you must run Command Prompt or PowerShell as administrator in order to be able to run commands that begin with `ykman fido`.

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

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

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
`-h, --help`	Show this message and exit.

6.1.3 Commands

Command	Description
`access`	Manage the PIN for FIDO.
`config`	Manage FIDO configuration.
`credentials`	Manage discoverable (resident) credentials.
`fingerprints`	Manage fingerprints.
`info`	Display status of FIDO2 application.
`reset`	Reset all FIDO applications.

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

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.
`force-change`	Force the PIN to be changed to a new value before use. As of YubiKey Manager CLI version 5.3.0.
`set-min-length`	Set the minimum length allowed for PIN. As of ykman (CLI) version 5.3.0.
`verify-pin`	Verify the FIDO PIN against a YubiKey.

6.3 ykman fido access change-pin [OPTIONS]

Set or change the PIN code.

The FIDO2 PIN must be at least 4 characters long, and supports any type of alphanumeric characters. Some YubiKeys can be configured to require a longer PIN.

On YubiKey FIPS (4 Series), 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 force-change [OPTIONS]

Force the PIN to be changed to a new value before use.

6.4.1 Options

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

6.5 ykman fido access set-min-length [OPTIONS] LENGTH

Set the minimum length allowed for PIN.

Optionally use the `--rp` option to specify which RPs are allowed to request this information.

6.5.1 Options

Option	Description
`-h, --help`	Show this message and exit.
`-P, --pin TEXT`	PIN code.
`-R, --rp-id TEXT`	RP ID to allow.

6.6 ykman fido access unlock [OPTIONS] (Deprecated)

Replaced unlock command with verify-pin command.

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

6.6.1 Options

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

6.7 ykman fido access verify-pin [OPTIONS]

Verify the FIDO PIN against a YubiKey. For YubiKeys supporting FIDO2 this resets the `retries` counter of the PIN. For YubiKey FIPS (4 Series) this unlocks the session, allowing U2F registration.

6.7.1 Options

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

6.8 ykman fido config [OPTIONS] COMMAND [ARGS]...

Manage FIDO configuration.

6.8.1 Options

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

6.8.2 Commands

Command	Description
`enable-ep-attestation`	Enables Enterprise Attestation for Authenticators pre-configured to support it. As of ykman (CLI) version 5.3.0.
`toggle-always-uv`	Toggles the state of Always Require User Verification. As of ykman (CLI) version 5.3.0.

6.9 ykman fido config enable-ep-attestation [OPTIONS]

Enables Enterprise Attestation for Authenticators pre-configured to support it.

6.9.1 Options

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

6.10 ykman fido config toggle-always-uv [OPTIONS]

Toggles the state of Always Require User Verification.

6.10.1 Options

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

6.11 ykman fido credentials [OPTIONS] COMMAND [ARGS]...

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.

6.11.1 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
```

6.11.2 Options

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

6.11.3 Commands

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

6.12 ykman fido credentials delete [OPTIONS] CREDENTIAL_ID

Delete a credential. List stored credential IDs using the `list` subcommand.

6.12.1 Arguments

Argument	Description
`CREDENTIAL_ID`	A unique substring match of a Credentials ID.

6.12.2 Options

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

6.13 ykman fido credentials list [OPTIONS]

List credentials. Shows a list of credentials stored on the YubiKey.

The `--csv` flag returns more complete information about each credential, in CSV (comma separated values) format.

6.13.1 Options

Option	Description
`-h, --help`	Show this message and exit.
`-c, --csv`	Returns full credential information in CSV format.
`-P, --pin TEXT`	PIN code.

6.14 ykman fido fingerprints [OPTIONS] COMMAND [ARGS]...

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

6.14.1 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
```

6.14.2 Options

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

6.14.3 Commands

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

6.15 ykman fido fingerprints add [OPTIONS] NAME

Add a new fingerprint.

6.15.1 Arguments

Argument	Description
`NAME`	Short readable name for the fingerprint. For example, “Left thumb”.

6.15.2 Options

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

6.16 ykman fido fingerprints delete [OPTIONS] ID

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

6.16.1 Arguments

Argument	Description
`ID`	To see the ID run the `fingerprints list` subcommand.

6.16.2 Options

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

6.17 ykman fido fingerprints list [OPTIONS]

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

6.17.1 Options

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

6.18 ykman fido fingerprints rename [OPTIONS] ID NAME

Set the label for a fingerprint.

6.18.1 Arguments

Argument	Description
`ID`	The ID of the fingerprint to rename. See `fingerprints list`.
`NAME`	Short readable name for the fingerprint. For example, “Left thumb”.

6.18.2 Options:

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

6.19 ykman fido info

Display general status of the FIDO2 application.

6.19.1 Options

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

6.20 ykman fido reset [OPTIONS]

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.

6.20.1 Options

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

Click for Yubico Support.

CHAPTER

SEVEN

HSMAUTH COMMANDS

7.1 ykman hsmauth [OPTIONS] COMMAND [ARGS]...

Manage the YubiHSM Auth application

7.1.1 Options

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

7.1.2 Commands

Command	Description
`access`	Manage Management Key for YubiHSM Auth.
`credentials`	Manage YubiHSM Auth credentials.
`info`	Display general status of the YubiHSM Auth application.
`reset`	Reset all YubiHSM Auth data.

7.2 ykman hsmauth info [OPTIONS]

Display general status of the YubiHSM Auth application.

7.2.1 Options

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

7.3 ykman hsmauth reset [OPTIONS]

Reset all YubiHSM Auth data.

This action wipes all data and restores factory setting for the YubiHSM Auth application on the YubiKey.

7.3.1 Options

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

7.4 ykman hsmauth access [OPTIONS] COMMAND [ARGS]...

Manage the Management Key for YubiHSM Auth.

7.4.1 Options

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

7.4.2 Commands

Command	Description
`change-management-key`	Change the management key.

7.5 ykman hsmauth access change-management-key [OPTIONS]

Change the management key.

Allows you to change the management key. This is required to add and delete YubiHSM Auth credentials stored on the YubiKey.

7.5.1 Options

Option	Description
`-h, --help`	Show this message and exit.
`-m, --management-key TEXT`	Current management key. Default: b'x00x00x00x00x00x00x00 x00x00x00x00x00x00x00x00x00'
`-n, --new-management-key TEXT`	A new management key to set.
`-g, --generate`	Generate a random management key. Can't be used with `--new-management-key`.

7.6 ykman hsmauth credentials [OPTIONS] COMMAND [ARGS]...

Manage YubiHSM Auth credentials.

7.6.1 Options

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

7.6.2 Commands

Command	Description
`delete`	Delete a credential.
`derive`	Import a symmetric credential derived from a password.
`export`	Export the public key corresponding to an asymmetric credential.
`generate`	Generate an asymmetric credential.
`import`	Import an asymmetric credential.
`list`	List all credentials.
`symmetric`	Import a symmetric credential.

7.7 ykman hsmauth credentials delete [OPTIONS] LABEL

Delete a credential.

This deletes a YubiHSM Auth credential from the YubiKey.

7.7.1 Arguments

Argument	Description
`LABEL`	A label to match a single credential, as shown in `credential list`.

7.7.2 Options

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

7.8 ykman hsmauth credentials derive [OPTIONS] LABEL

Import a symmetric credential derived from a password.

This imports a symmetric YubiHSM Auth credential by deriving ENC and MAC keys from a password.

7.8.1 Arguments

Argument	Description
`LABEL`	A label for the YubiHSM Auth credential.

7.8.2 Options

Option	Description
`-h, --help`	Show this message and exit.
`-d, --derivation-password TEXT`	Derivation password for ENC and MAC keys.
`-c, --credential-password TEXT`	Password to protect credential.
`-m, --management-key TEXT`	The management key.
`-t, --touch`	Requires touch on YubiKey to access credential.

7.9 ykman hsmauth credentials export [OPTIONS] LABEL PUBLIC-KEY

Export the public key corresponding to an asymmetric credential.

This exportS the long-term public key corresponding to the asymmetric YubiHSM Auth credential stored on the YubiKey.

7.9.1 Arguments

Argument	Description
`LABEL`	A label for the YubiHSM Auth credential.
`PUBLIC-KEY`	File to write the public key to. Use '-' to use stdout.

7.9.2 Options

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

7.10 ykman hsmauth credentials generate [OPTIONS] LABEL

Generate an asymmetric credential.

This generates an asymmetric YubiHSM Auth credential (private key) on the YubiKey.

7.10.1 Arguments

Argument	Description
LABEL	A label for the YubiHSM Auth credential.

7.10.2 Options

Option	Description
-h, --help	Show this message and exit.
-c, --credential-password TEXT	Password to protect credential.
-m, --management-key TEXT	The management key.
-t, --touch	Requires touch on YubiKey to access credential.

7.11 ykman hsmauth credentials import [OPTIONS] LABEL PRIVATE-KEY

Import an asymmetric credential.

This imports a private key as an asymmetric YubiHSM Auth credential to the YubiKey.

7.11.1 Arguments

Argument	Description
LABEL	A label for the YubiHSM Auth credential.
PRIVATE-KEY	File containing the private key. Use '-' to use stdin.

7.11.2 Options

Option	Description
`-h, --help`	Show this message and exit.
`-c, --credential-password TEXT`	Password to protect credential.
`-m, --management-key TEXT`	The management key.
`-p, --password TEXT`	Password used to decrypt the private key.
`-t, --touch`	Requires touch on YubiKey to access credential.

7.12 ykman hsmauth credentials list [OPTIONS]

List all credentials stored on the YubiKey.

7.12.1 Options

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

7.13 ykman hsmauth credentials symmetric [OPTIONS] LABEL

Import a symmetric credential.

This imports an encryption and mac key as a symmetric YubiHSM Auth credential on the YubiKey.

7.13.1 Arguments

Argument	Description
`LABEL`	A label for the YubiHSM Auth credential.

7.13.2 Options

Option	Description
`-h, --help`	Show this message and exit.
`-c, --credential-password TEXT`	Password to protect credential.
`-E, --enc-key TEXT`	The ENC key.
`-g, --generate`	Generate a random encryption and mac key.
`-m, --management-key TEXT`	The management key.
`-M, --mac-key TEXT`	The MAC key.
`-t, --touch`	Requires touch on YubiKey to access credential.

CHAPTER

EIGHT

OATH COMMANDS

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

8.1 ykman oath [OPTIONS] COMMAND [ARGS]...

Manage OATH application.

8.1.1 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
```

8.1.2 Options

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

8.1.3 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.

8.2 ykman oath access [OPTIONS] COMMAND [ARGS]...

Manage password protection for OATH.

8.2.1 Options

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

8.2.2 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.

8.3 ykman oath access change [OPTIONS]

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.

8.3.1 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.
`-r, --remember`	Remember the password on this machine.

8.4 ykman oath access forget [OPTIONS]

Remove a stored password from this computer.

8.4.1 Options

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

8.5 ykman oath access remember [OPTIONS]

Store the YubiKey password on this computer to avoid entering it on each use.

8.5.1 Options

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

8.6 ykman oath accounts [OPTIONS] COMMAND [ARGS]...

Manage and use OATH accounts.

8.6.1 Options

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

8.6.2 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.

8.7 ykman oath accounts add [OPTIONS] NAME [SECRET]

Add a new OATH account to the YubiKey.

8.7.1 Arguments

Argument	Description
NAME	Provide a name for this account.
SECRET	Optional. Base32-encoded secret/key value provided by the server.

8.7.2 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	Optional. 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.

8.8 ykman oath accounts code [OPTIONS] [QUERY]

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.

8.8.1 Arguments

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

8.8.2 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.

8.9 ykman oath accounts delete [OPTIONS] QUERY

Delete an account from the YubiKey.

8.9.1 Arguments

Argument	Description
QUERY	Provide a query string to match a single account, as shown in `oath accounts list`.

8.9.2 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.

8.10 ykman oath accounts list [OPTIONS]

List all accounts stored on the YubiKey.

8.10.1 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.

8.11 ykman oath accounts rename [OPTIONS] QUERY NAME

Rename an account. Requires YubiKey 5.3 or later.

8.11.1 Arguments

Argument	Description
`QUERY`	A query to match a single account, as shown in `oath accounts list`.
`NAME`	The name of the account. Use format `<issuer>:<name>` to specify the issuer.

8.11.2 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.

8.12 ykman oath accounts uri [OPTIONS] URI

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

8.12.1 Arguments

Argument	Description
`URI`	Specify URI path for account.

8.12.2 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.

8.13 ykman oath info [OPTIONS]

Display status of OATH application.

8.13.1 Options

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

8.14 ykman oath reset [OPTIONS]

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

8.14.1 Options

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

Click for Yubico Support.

CHAPTER

NINE

OPENPGP COMMANDS

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

9.1 ykman openpgp [OPTIONS] COMMAND [ARGS]...

Manage OpenPGP Application.

9.1.1 Examples

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

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

Require touch to use the authentication key:

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

9.1.2 Options

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

9.1.3 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.

9.2 ykman openpgp access [OPTIONS] COMMAND [ARGS]...

Manage PIN, Reset Code, and Admin PIN.

9.2.1 Options

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

9.2.2 Commands

Command	Description
`change-admin-pin`	Change the Admin PIN.
`change-pin`	Change the User PIN.
`change-reset-code`	Change the Reset Code.
`set-retries`	Set the number of retry attempts for the user.
`set-signature-policy`	Set the Signature PIN policy.
`unblock-pin`	Unblock the PIN, using Reset Code or Admin PIN.

9.3 ykman openpgp access change-admin-pin [OPTIONS]

Change the Admin PIN. The Admin PIN has a minimum length of 8, and supports any type of alphanumeric characters.

9.3.1 Options

Option	Description
`-h, --help`	Show this message and exit.
`-a, --admin-pin TEXT`	Current Admin PIN.
`-n, --new-admin-pin TEXT`	New Admin PIN.

9.4 ykman openpgp access change-pin [OPTIONS]

Change the User PIN. The PIN has a minimum length of 6, and supports any type of alphanumeric characters.

9.4.1 Options

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

9.5 ykman openpgp access change-reset-code [OPTIONS]

Change the Reset Code. The Reset Code has a minimum length of 6, and supports any type of alphanumeric characters.

9.5.1 Options

Option	Description
`-h, --help`	Show this message and exit.
`-a, --admin-pin TEXT`	Admin PIN.
`-r, --reset-code TEXT`	A new Reset Code.

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

Set PIN, Reset Code, and Admin PIN retries.

9.6.1 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.

9.6.2 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.

9.7 ykman openpgp access set-signature-policy [OPTIONS] POLICY

Set the Signature PIN policy. The Signature PIN policy is used to control whether the PIN is always required when using the Signature key, or if it is required only once per session.

9.7.1 Arguments

Argument	Description
POLICY	Signature PIN policy to set (always, once).

9.7.2 Options

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

9.8 ykman openpgp access unblock-pin [OPTIONS]

Unblock the PIN, using Reset Code or Admin PIN.

If the PIN is lost or blocked you can reset it to a new value using the Reset Code. Alternatively, the Admin PIN can be used with the -a, --admin-pin option, instead of the Reset Code.

The new PIN has a minimum length of 6, and supports any type of alphanumeric characters.

9.8.1 Options

Option	Description
-h, --help	Show this message and exit.
-a, --admin-pin TEXT	Admin PIN. Use - as a value to prompt for input.
-n, --new-pin TEXT	A new PIN.
-r, --reset-code TEXT	Reset Code.

9.9 ykman openpgp certificates [OPTIONS] COMMAND [ARGS]...

Manage certificates.

9.9.1 Options

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

9.9.2 Commands

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

9.10 ykman openpgp certificates delete [OPTIONS] KEY

Delete an OpenPGP certificate.

9.10.1 Arguments

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

9.10.2 Options

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

9.11 ykman openpgp certificates export [OPTIONS] KEY CERTIFICATE

Export an OpenPGP certificate.

9.11.1 Arguments

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

9.11.2 Options

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

9.12 ykman openpgp certificates import [OPTIONS] KEY CERTIFICATE

Import an OpenPGP certificate.

9.12.1 Arguments

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

9.12.2 Options

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

9.13 ykman openpgp keys [OPTIONS] COMMAND [ARGS]...

Manage private keys.

9.13.1 Options

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

9.13.2 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.

9.14 ykman openpgp keys attest [OPTIONS] KEY CERTIFICATE

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.

9.14.1 Arguments

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

9.14.2 Options

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

9.15 ykman openpgp keys import [OPTIONS] KEY PRIVATE-KEY

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

9.15.1 Arguments

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

9.15.2 Options

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

9.16 ykman openpgp info [OPTIONS]

Display status of OpenPGP application.

9.16.1 Options

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

9.17 ykman openpgp keys set-touch [OPTIONS] KEY POLICY

Set touch policy for OpenPGP keys. 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 the `openpgp info` subcommand.

9.17.1 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
```

9.17.2 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 deleting the private key.
`Fixed`	Touch required, can't be disabled without deleting the private key.
`Off`	No touch required. (default)
`On`	Touch required.

9.17.3 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.

9.18 ykman openpgp reset [OPTIONS]

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

9.18.1 Options

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

Click for Yubico Support.

CHAPTER

TEN

OTP COMMANDS

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

10.1 ykman otp [OPTIONS] COMMAND [ARGS]...

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.

To provide an access code to commands which require it, use the `--access-code` option. This option must be given directly after the `otp` command, before any sub-command.

10.1.1 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
```

Remove a currently set access code from slot 2:

```
$ ykman otp --access-code 0123456789ab settings 2 --delete-access-code
```

10.1.2 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.

10.1.3 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.

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

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

Challenge default is hex, but base32 with `--totp` setting. Slot options are 1 or 2.

10.2.1 Arguments

Argument	Description
`CHALLENGE`	

10.2.2 Options

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

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

Program a challenge-response credential for slot 1 or 2.

10.3.1 Arguments

Argument	Description
`KEY`	A key given in hex. If `--totp` specified, key is in base32. If `KEY` is not specified, an interactive prompt asks for it.

10.3.2 Options

Option	Description
`-h, --help`	Show this message and exit.
`-f, --force`	Confirm the action without prompting.
`-g, --generate`	Generate a random secret key. Cannot be used with `KEY` argument.
`-t, --touch`	Require touch on the YubiKey to generate a response.
`-T, --totp`	Use a base32 encoded key for TOTP credentials. Optionally, can be padded.

10.4 ykman otp delete [OPTIONS] {1|2}

Deletes the configuration in the specified slot, 1 or 2.

10.4.1 Options

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

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

Program an HMAC-SHA1 OATH-HOTP credential for slot 1 or 2.

The YubiKey can be configured to output an OATH Token Identifier as a prefix to the OTP itself, which consists of OMP+TT+MUI. Using the `--identifier` option. Specify the

- OMP+TT as 4 characters
- MUI as 8 characters
- full OMP+TT+MUI as 12 characters.

If omitted, the default value of `ubhe` is used for OMP+TT, and the YubiKey serial number is used as MUI.

10.5.1 Arguments

Argument	Description
KEY	A key given in hex. If KEY is not specified, an interactive prompt asks for it.

10.5.2 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.
-f, --force	Confirm the action without prompting.
-i, --identifier TEXT	Token identifier.
--no-enter	Do not send an **Enter** keystroke after outputting the code.

10.6 ykman otp info [OPTIONS]

Display general status of YubiKey OPT slots.

10.6.1 Options

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

10.7 ykman otp ndef [OPTIONS] {1|2}

Configure slot 1 or 2 to be used over NDEF (NFC).

If `--prefix` is not specified, a default value is used, based on the type:

- For URI the default value is: "https://my.yubico.com/yk/#"
- For TEXT the default is an empty string

10.7.1 Options

Option	Description
`-h, --help`	Show this message and exit.
`-p, --prefix TEXT`	Added before the NDEF payload. Typically a URI.
`-t, --ndef-type [TEXT|URI]`	NDEF payload type [default: URI]

10.8 ykman otp settings [OPTIONS] {1|2}

Update the settings for slot 1 or 2. Change the settings for a slot without changing the stored secret. All settings not specified are written with default values.

10.8.1 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. Use - as value to prompt for input.
`--delete-access-code`	Remove access code from the slot.
`--enter / --no-enter`	Send **Enter** keystroke after slot output. [Default: `enter`]
`-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 scan codes for numeric keypad when sending digits. Helps with some keyboard layouts. [Default: `False`]

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

Configure a static password for slot 1 or 2. 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.

10.9.1 Arguments

Argument	Description
`PASSWORD`	Specify if required.

10.9.2 Options

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

10.10 ykman otp swap [OPTIONS]

Swaps the two slot configurations.

10.10.1 Options

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

10.11 ykman otp yubiotp [OPTIONS] {1|2}

Program a Yubico OTP credential for slot 1 or 2.

10.11.1 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. Cannot be used with `--private-id`.
`-G, --generate-key`	Generate a random secret key. Cannot be used with `--key`.
`--no-enter`	Do not send an **Enter** keystroke after emitting the OTP.
`-O, --config-output FILENAME`	Output configuration to a file Existing files are appended.
`-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. Cannot be used with `--public-id`.
`-u, --upload`	Upload credential to YubiCloud. This opens a browser. Cannot be used with `--force`.

Click for Yubico Support.

CHAPTER

ELEVEN

PIV COMMANDS

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

11.1 ykman piv [OPTIONS] COMMAND [ARGS]...

Manage the PIV Application.

11.1.1 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
```

11.1.2 Options

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

11.1.3 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.

11.2 ykman piv access [OPTIONS] COMMAND [ARGS]...

Manage PIN, PUK, and Management Key.

11.2.1 Options

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

11.2.2 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.
`unblock-pin`	Unblock the PIN (using the PUK).

11.3 ykman piv access change-management-key [OPTIONS]

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.

With the release of the 5.7 YubiKey firmware version, Advanced Encryption Standard 192 bit (AES-192) is the default **security type** for the PIV Management Key. Triple Data Encryption Standard (TDES or 3DES) is the default security type for YubiKey firmware versions older than 5.7.

The default **value** is the same for all firmware versions, regardless of the security type. For this value as well as the default PIN and PUK codes, see the "General Information" section of "Yubico PIV Tool" on our developer site.

11.3.1 Options

Option	Description
`-h, --help`	Show this message and exit.
`-a, --algorithm [TDES/3DES|AES128|AES192|AES256]`	Management key algorithm. Default v5.7: `AES-192` Default pre-v.5.7: `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. Cannot be used with `--new-management-key`.
`-m, --management-key TEXT`	Current management key. TEXT = identifier.
`-n, --new-management-key TEXT`	A new management key. TEXT = identifier.
`-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.

11.4 ykman piv access change-pin [OPTIONS]

Change the PIN code. The PIN must be between 6 and 8 alphanumeric characters. For cross-platform compatibility, numeric PINs are recommended.

11.4.1 Options

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

11.5 ykman piv access change-puk [OPTIONS]

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.

11.5.1 Options

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

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

Set the number of PIN and PUK retry attempts.

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

11.6.1 Arguments

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

11.6.2 Options

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

11.7 ykman piv access unblock-pin [OPTIONS]

Unblock the PIN (using PUK).

11.7.1 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.

11.8 ykman piv certificates [OPTIONS] COMMAND [ARGS]...

Manage certificates.

11.8.1 Options

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

11.8.2 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).

11.9 ykman piv certificates delete [OPTIONS] SLOT

Delete a certificate from a PIV slot on the YubiKey.

11.9.1 Arguments

Argument	Description
SLOT	PIV slot of the certificate.

11.9.2 Options

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

11.10 ykman piv certificates export [OPTIONS] SLOT CERTIFICATE

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

11.10.1 Arguments

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

11.10.2 Options

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

11.11 ykman piv certificates generate [OPTIONS] SLOT PUBLIC-KEY

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.

11.11.1 Arguments

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

11.11.2 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. TEXT = identifier.
-P, --pin TEXT	PIN code.
-s, --subject TEXT	Subject for the certificate, as an RFC 4514 string. [required].

11.12 ykman piv certificates import [OPTIONS] SLOT CERTIFICATE

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

11.12.1 Arguments

Argument	Description
SLOT	PIV slot of the certificate.
CERTIFICATE	File containing the certificate. Use - to use stdin.

11.12.2 Options

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

11.13 ykman piv certificates request [OPTIONS] SLOT PUBLIC-KEY CSR

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

11.13.1 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.

11.13.2 Options

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

11.14 ykman piv info [OPTIONS]

Display general status of PIV application.

11.14.1 Options

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

11.15 ykman piv keys [OPTIONS] COMMAND [ARGS]...

Manage private keys.

11.15.1 Options

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

11.15.2 Commands

Command	Description
`attest`	Generate an attestation certificate for a key pair.
`delete`	Delete a key.
`export`	Export a public key corresponding to a stored private key.
`generate`	Generate an asymmetric key pair.
`import`	Import a private key from file.
`info`	Show metadata about a private key.
`move`	Moves a key.

11.16 ykman piv keys attest [OPTIONS] SLOT CERTIFICATE

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.

11.16.1 Arguments

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

11.16.2 Options

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

11.17 ykman piv keys delete [OPTIONS] SLOT

Delete a key from a PIV slot on the YubiKey.

11.17.1 Arguments

Argument	Description
SLOT	PIV slot of the key.

11.17.2 Options

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

11.18 ykman piv keys export [OPTIONS] SLOT PUBLIC-KEY

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 is returned.

Use the --verify flag to verify that the public key being returned matches the private key, by using the slot to create and verify a signature. This might require the PIN to be provided.

11.18.1 Arguments

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

11.18.2 Options

Option	Description
`-h, --help`	Show this message and exit.
`-F, --format [PEM|DER]`	Encoding format. Default: `PEM`
`-P, --pin TEXT`	PIN code. This is used with the `--verify` option.
`-v, --verify`	Verify that the public key matches the private key in the slot.

11.19 ykman piv keys generate [OPTIONS] SLOT PUBLIC-KEY

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

11.19.1 Arguments

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

11.19.2 Options

Option	Description
`-h, --help`	Show this message and exit.
`-a, --algorithm [RSA1024 |RSA2048|RSA3072|RSA4096 ECCP256|ECCP384|ED25519 X25519]`	Algorithm to use in key generation. [Default: RSA2048]
`-F, --format [PEM|DER]`	Encoding format. Default: PEM
`-m, --management-key TEXT`	The management key. TEXT = identifier.
`-P, --pin TEXT`	PIN code.
`--pin-policy [DEFAULT |NEVER|ONCE|ALWAYS |MATCH-ONCE|MATCH-ALWAYS]`	PIN policy for slot.
`--touch-policy [DEFAULT |NEVER|ALWAYS|CACHED]`	Touch policy for slot.

11.20 ykman piv keys import [OPTIONS] SLOT PRIVATE-KEY

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

11.20.1 Arguments

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

11.20.2 Options

Option	Description
`-h, --help`	Show this message and exit.
`-m, --management-key TEXT`	The management key. TEXT = identifier.
`--pin-policy [DEFAULT|NEVER ONCE|ALWAYS|MATCH-ONCE MATCH-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.

11.21 ykman piv keys info [OPTIONS] SLOT

Show metadata about a private key. This shows what type of key is stored in a specific slot, whether it was imported into the YubiKey, or generated on-chip, and what the PIN and Touch policies are for using the key.

11.21.1 Arguments

Argument	Description
`SLOT`	PIV slot of the private key.

11.21.2 Options

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

11.22 ykman piv keys move [OPTIONS] SOURCE DEST

Moves a key from one PIV slot into another.

11.22.1 Arguments

Argument	Description
SOURCE	PIV slot of the key to move.
DEST	PIV slot to move the key into.

11.22.2 Options

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

11.23 ykman piv objects [OPTIONS] COMMAND [ARGS]...

Manage PIV data objects.

11.23.1 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
```

11.23.2 Options

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

11.23.3 Commands

Command	Description
`export`	Export an arbitrary PIV data object.
`generate`	Generate and write data for a supported data object.
`import`	Write an arbitrary PIV object.

11.24 ykman piv objects export [OPTIONS] OBJECT OUTPUT

Export an arbitrary PIV data object.

11.24.1 Arguments

Argument	Description
`OBJECT`	Name of PIV data object, or ID in HEX.
`OUTPUT`	File to write object to. Use - to use `stdout`.

11.24.2 Options

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

11.25 ykman piv objects generate [OPTIONS] OBJECT

Generate and write data for a supported data object.

11.25.1 Arguments

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

11.25.2 Options

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

11.26 ykman piv objects import [OPTIONS] OBJECT DATA

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

11.26.1 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.

11.26.2 Options

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

11.27 ykman piv reset [OPTIONS]

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

This option is not available in CLI version 5.4.0.

11.27.1 Options

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

Click for Yubico Support.

CHAPTER

TWELVE

YUBIHSM COMMANDS

For a full description of YubiHSM Auth, see the *YubiKey 5 Series Technical Manual*, Protocols and Applications > YubiHSM Auth chapter.

12.1 Enable or Disable YubiHSM Auth on a YubiKey

This section includes the expected output and testing methods.

YubiHSM Auth is available as of firmware version 5.4.X and is disabled by default.

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.
```

Click for Yubico Support.

CHAPTER

THIRTEEN

COPYRIGHT

13.1 Trademarks

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

13.2 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.

13.3 Contact Information

Yubico AB
Kungsgatan 44
111 35 Stockholm
Sweden

13.4 Getting Help

Documentation is continuously updated on https://docs.yubico.com/ (this site). Additional support resources are available in the Yubico Knowledge Base.

Click the links to:

- Submit a support request
- Contact our sales team

13.5 Feedback

Yubico values and welcomes your feedback. If you think you may have discovered a flaw in our product, please submit a support request at https://support.yubico.com/hc/en-us and provide as much detail as you can.

13.6 Document Updated

2024-08-09 17:37:15 UTC