USB Raptor

Documentation

General description

USB Raptor is an open source utility hosted on Sourceforge servers. The utility is distributed under the Creative Commons Attribution License and it can be freely downloaded and used as long the license is respected.

USB Raptor is a Windows utility which can run in system tray and lock or unlock the computer by using USB memory drives as keys. USB Raptor created having in mind that when a user is locking and especially when unlocking a computer is wasting time and gets into an inconvenient and frustrating process of typing complex passwords. With USB Raptor the locking and unlocking of the system is made automatically and easy.

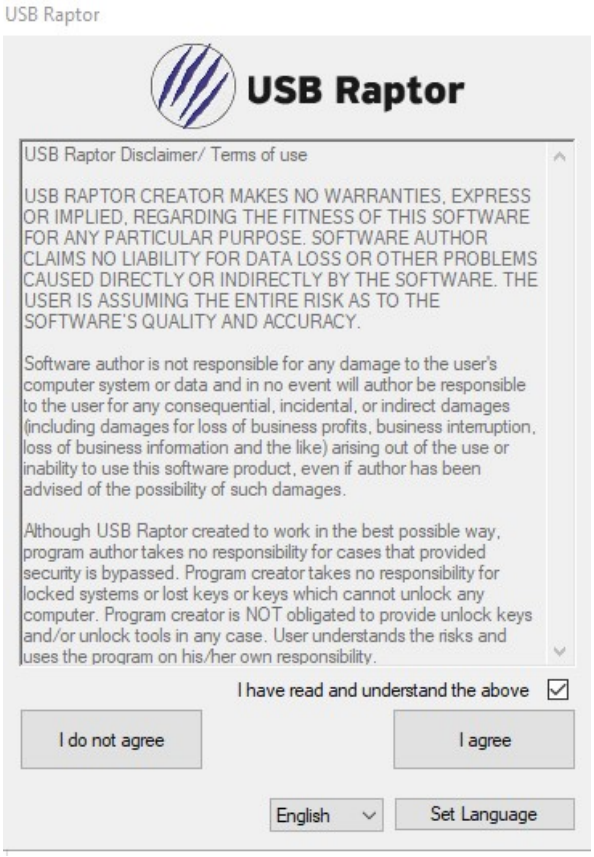
> This is a simple yet effective way to lock and protect your computer when you are taking a lunch break on your work. Just take the USB key with you to lock your computer and put back on the USB port when you are back on your desk to unlock it.

How it works

By activating USB Raptor to a system and creating an unlock USB key, the computer stays unlocked as long the key is detected in one of the USB ports. When a user removes the USB key from the computer the lock is activated and when the USB key is plugged back in to the USB port the lock is released.

The utility checks the USB drives to find an unlock file with encrypted content. Once the file is found and the decoding result is matching the password set by the user then the computer unlocks automatically and stays unlocked. If the unlock file is not found or the decryption result is different than the password set then the computer is locked and protected.

USB Raptor first run - Disclaimer

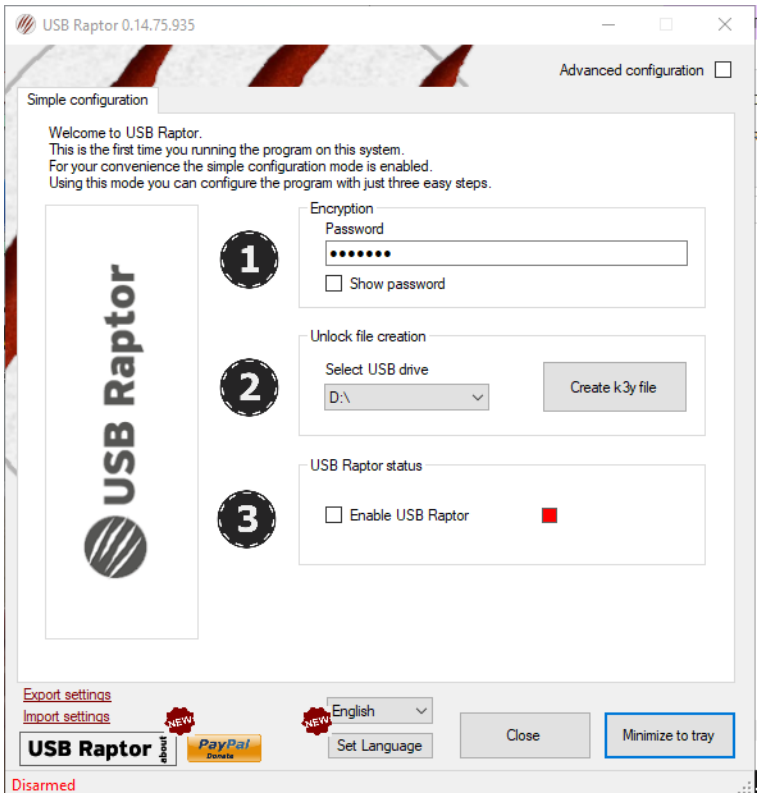


When program is executed for the first time the disclaimer window appears asking user to agree with the terms of use. This window appears only one time on each computer and once the “I agree” is clicked, the program will start working normally.

You can also select the GUI language from “Disclaimer” screen by clicking on the dropdown menu and clicking on “Set Language” button.

USB Raptor Interface - Simple configuration

On the first run USB Raptor comes up with simple configuration enabled in order to give you the configuration basics in just three steps.



Step One: Set your own password.

> Remember your password! Although USB Raptor is made to lock and unlock your system automatically you may need your password in the future.

Step Two: Plug a USB flash key to your system and select the drive letter

> Drive letter is not critical for unlock operation it is need only to indicate where you want to write the file.

Step Three: Enable USB Raptor to get the system protected.

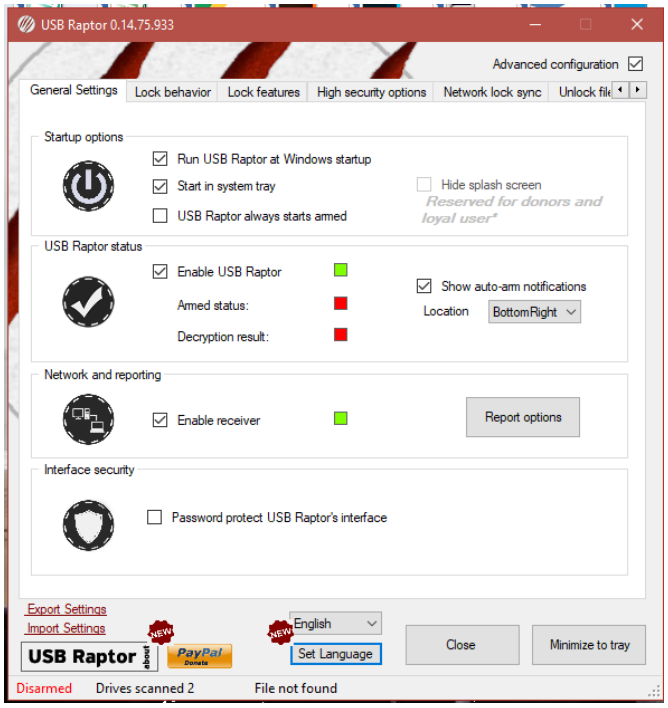
> Once USB Raptor activated and the USB key is in place, a popup message will appear on your screen indicating that USB Raptor is armed and ready for use.

Once the three above steps completed you are ready to use USB Raptor by minimizing it to system tray. However there are lots of other interesting and important options available in advanced configuration which you are advised to check out and set according to your needs.

USB Raptor Interface – Advanced configuration

The advanced configuration is separated in six categories: General settings, Lock behavior, Lock features, High security options, Network lock synch and Unlock file settings.

General settings



General settings > Startup options

Run USB Raptor at Windows startup: Select this option to run USB Raptor automatically when your computer starts.

Start in system tray: Select this option to start USB Raptor directly to the system tray without seeing the configuration window.

USB Raptor always starts armed: If you like to lock the computer on startup (if no USB key found) you have to enable the "USB Raptor always starts armed".

> USB Raptor arm function: To avoid accidental locking USB Raptor needs to be armed prior lock activation. USB Raptor is armed when a valid unlock file is detected, otherwise the utility remains idle. The only exception on this functionality is when user enables the "USB Raptor always starts armed".

Hide splash screen: Hides the splash logo screen during program startup.

> "Hide splash screen" option is enabled for donors or after 30 program executions. Normally users who are using USB Raptor daily they will able to disable the splash screen after a month of usage or so.

General settings > USB Raptor status

Enable USB Raptor: Enables or disables the USB Raptor. The utility status is indicated on the corresponding indicator. Green = Enabled, Red = Disabled

Armed status: Indicates the arm status of USB Raptor. Green = Armed (ready to lock the computer once the USB key removed), Red = Disarmed (no valid USB key detected)

Decryption result: Indicates the when a valid key file found or not. Green = A valid unlock key found, Red = No file found (or USB Raptor is disabled) Purple = A key found but it is invalid.

Show auto-arm notifications: Enables USB Raptor to display a small popup window in a screen corner every time is going to arm state. This notification is a helpful reminder not to remove the USB key by mistake.

Notification location: Allows user to select on which screen corner the popup should be displayed to avoid window interference with Windows 10 notification on bottom right.

General settings > Network and reporting

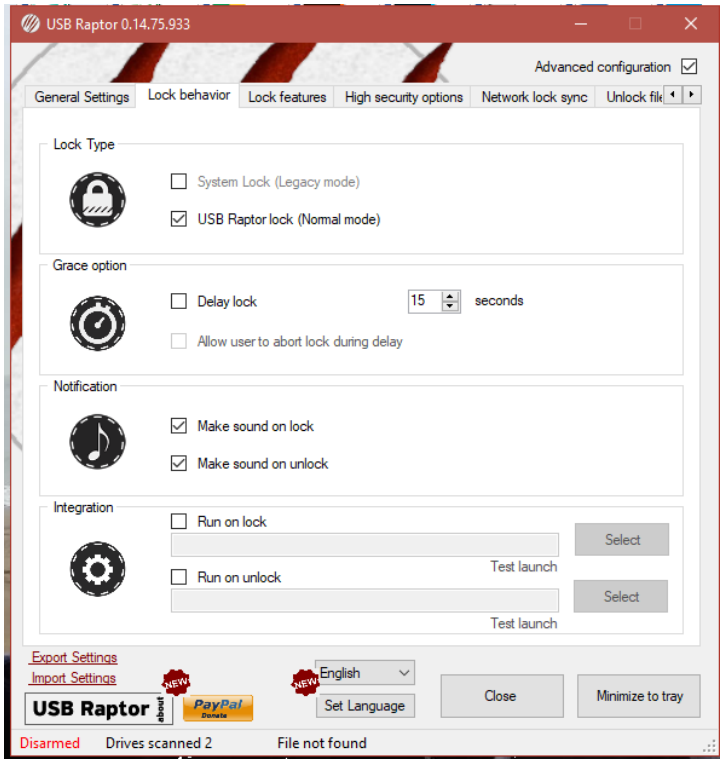
Enable receiver: Enables or disables internal UDP server. The server is used for remote command receiving (aka network backdoor), color synchronization across the LAN and lock/unlock synchronization. Disabling receiver, nothing of the above is working. The server status is indicated on the corresponding indicator. Flashing Green = Enabled, Red = Disabled

Report button: See page 16 (“***Additional screens”***)

General settings > Interface security

Password protect USB Raptor’s interface: Enables password protection to settings screen. Every time user wants to enable/disable the program or needs to access program settings and the program should enter the password.

Lock behavior



Lock behavior > Lock type

System lock: Selecting system lock USB Raptor will use simple window lock method once the USB key removed. In this case there is no automatic unlock supported.

USB Raptor lock: The USB Raptor's lock. This is the most advanced and USB Raptor is fully functional under this choice. So it is highly recommended to use this option.

Lock behavior > Grace option

Delay lock: Enables a short (user defined) delay time up to 20 seconds before activate lock. During this time a countdown message appears on the screen.

Allow cancel during delay: Enables user to cancel lock by clicking "Abort lock" button while the countdown numbers are displayed on the screen.

Lock behavior > Notification

Make sound on lock: Enables USB Raptor to generate a notification sound while the system is locking.

Make sound on unlock: Enables USB Raptor to generate a notification sound while the system is unlocking.

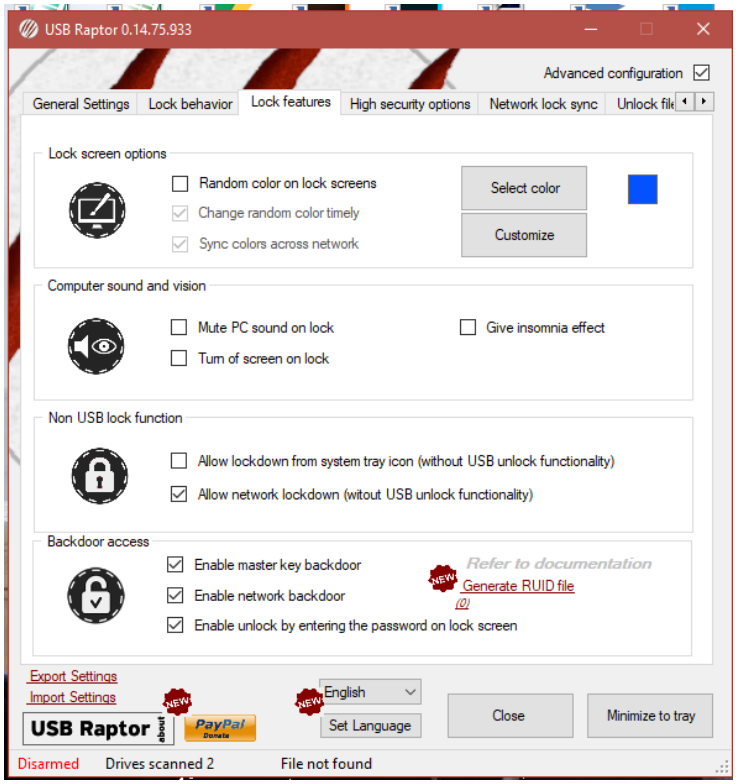
Lock behavior > Integration

Run on lock: Enables USB Raptor to run a third party program or script on lock.

Run on unlock: Enables USB Raptor to run a third party program or script on unlock.

> Run on lock/unlock can be used to integrate with other executable and script files. However it is not limited to these file types, it can be used to navigate to web sites or even open specific files. Just enter the file path or the website address and use the test hyperlinks to verify that the functions are working.

Lock features



Lock features > Lock screen options

Random color on lock screens: Selecting this option will force the utility to display a lock screen of random color; otherwise the lock screen goes gray.

Change random color timely: Enables a random color generator which changes the lock screen color from time to time.

Sync color across network: Allow program to receive color codes from other USB Raptors in the same network. This option created to give a uniform look to computers while locked.

Select color. This button allows you to select steady color for your lock screens. This control is enabled only if "Random color on lock screen" is NOT enabled. On each color change an additional panel is displayed to preview the color. The selected color is displayed also on the little square indicator. For more see page 20 ("***Additional screens***")

Customize button: See page 16 ("***Additional screens***")

Lock features > Computer sound and vision

Mute PC sound on lock: Sends mute command to system sound when locking and un-mute while unlocking.

Turn off screen on lock: Turns off computer screen when locking. The screen will turn on again on mouse movement or if a keyboard key is pressed. USB Raptor can also turn back on the screen automatically when the computer is unlocked.

Give insomnia effect: Keeps computer awake and doesn't allow it to activate screen saver.

Lock features > Non USB lock functions

Allow lockdown from system tray: Add a command to tray icon's right click menu which enables user to lockdown computer immediately. This lock forces USB Raptor to accept password to unlock even this kind of backdoor access is disabled in options.

Allow network lockdown: Enables USB Raptor to accept network lockdown (and lockdown removal) commands from other devices and utilities.

Lock features > Backdoor access

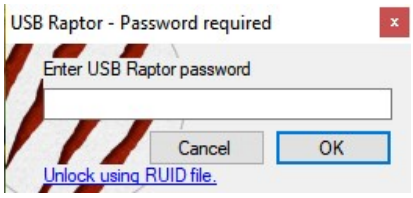
Enable master key backdoor: Enables USB Raptor to accept master keys in order to override any lock type. See page 15 ("***Create master k3y***")

Enable network backdoor: Enables USB Raptor to accept network messages to lock and unlock.

Enable unlock by entering the password in lock screen: Enables USB Raptor to accept its password to lock screen while the system is locked. In order to enter the password you have to double click the lock screen on the first monitor and the password input field appears.

Generate RUID file: Generates a "RUID.dat" on desktop. This file can be used as backup unlock for USB Raptor interface, if the password is forgotten. This feature is provided as additional interface unlock option because some users are like to have the USB Raptor interface locked but eventually they are forget their password.

The file can be imported to USB Raptor by using the appropriate link label on Password window. This window is visible after a failed unlock attempt.



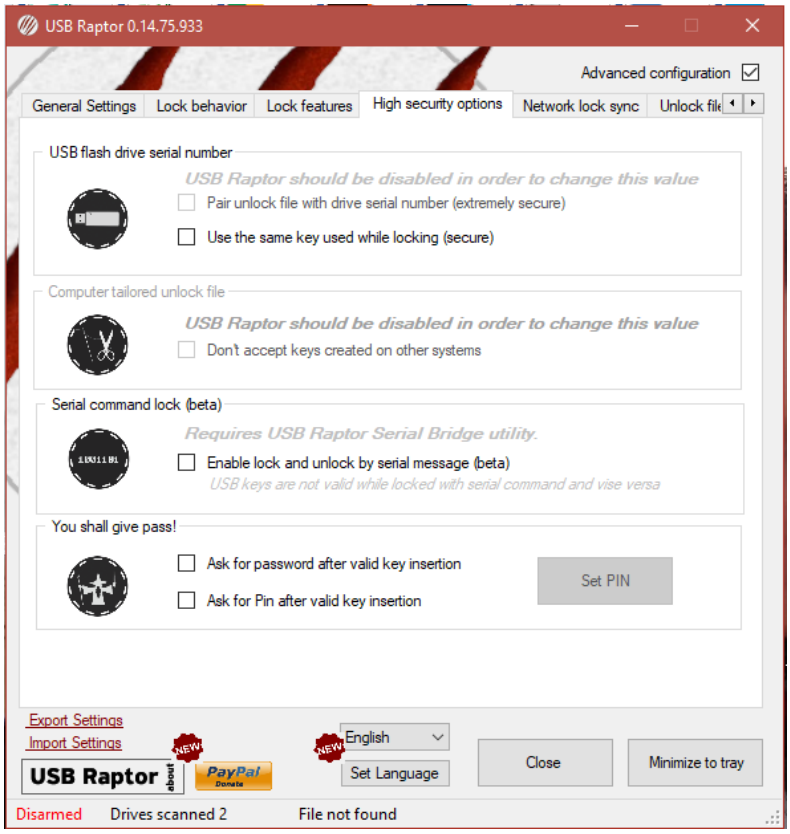
This feature is provided as additional interface unlock option because some users like to have the USB Raptor interface locked, but there is a risk for the password is eventually forgotten.

This file cannot be used to release USB Raptor lock. This file is used only to unlock USB Raptor interface.

The file should be generated again if the USB Raptor password is changed.

The file is unique for each system!

High security options



High security options > USB flash drive serial number

Pair unlock file with drive serial number: Enabling this option forces the encryption key to use serial number of the selected drive as well to generate the unlock.k3y. Practically this means that the k3y file generated cannot be copied to any other media and unlock the computer because USB Raptor wants to detect the same serial number used while the k3y file created. This option allows the user to create multiple keys but the k3y files cannot be copied from media to media. Disabling this option the k3y file can be copied to any USB drive and would be functional.

Use the same key used while locking the system: Once enabled the system will memorize the serial number of the key removed from the PC causing USB Raptor to lock. This specific USB key should be used in order to unlock the system otherwise the system stays locked. This function is not working with USB Raptor always starts armed option. When USB Raptor starts armed accepts any key for the first unlock even if this option is enabled.

High security options > Computer tailored unlock file

Don't accept keys created on other systems: Enabling this option forces the encryption key to use computer info as well to generate the unlock.k3y. This protects the system from unlocking with keys generated with the same password in other computers. Disabling this option the encryption stays the same on all computers and relies only on the password or any other high security option selected.

High security options > Serial command lock

Enable lock unlock by serial message: Introduced on USB Raptor Carrot and later. This function enables USB Raptor to use hardware keys (like Arduino running custom sketch) to lock and unlock instead of USB flash drives. This option enables also USB Raptor to receive commands from other devices such POS systems and lock or unlock the computer. A demo video presenting this function using an Arduino key is available on YouTube: https://www.youtube.com/watch?v=PLT4WWGwaIc

> The function is under development. For stability reasons currently "USB Raptor Serial Bridge" is required in order to receive serial messages.

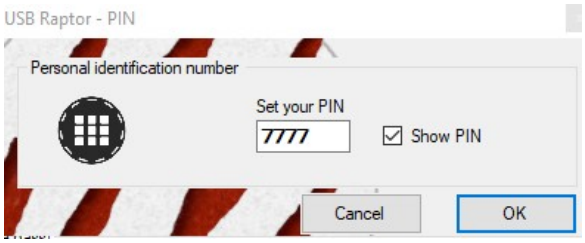
High security options > You shall give pass!

These two options added as an additional security when a valid key is detected on the USB port.

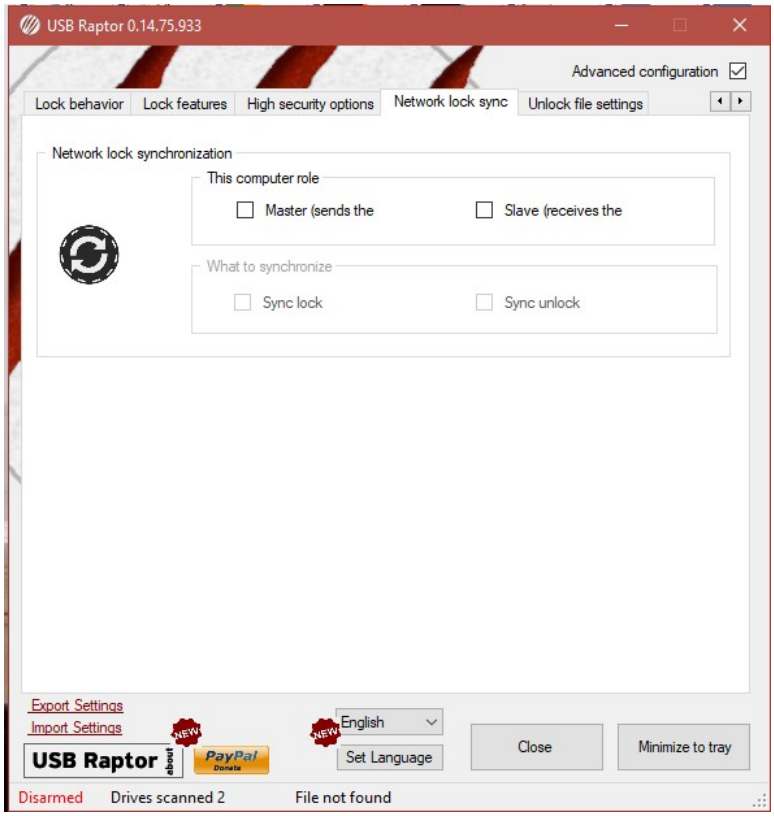
Ask for password after valid key insertion: Forces user to enter its password in order to release the lock.

Ask for PIN after valid key insertion: Forces user to enter its PIN in order to release the lock (default pin is 7777).

Set PIN: Displays the set pin window. A four digit PIN can be set on this window. Show PIN check box reveals the value.



Network lock sync



The purpose of this function is to control more than one computer lock with one USB key. This is helpful in controlled environments like school classrooms with multiple computers connected to the same LAN. One USB Raptor should be set as Master and the other should be set as Slaves. The Master will broadcast the selected messages to the network and the Slaves will receive them.

Communication scheme used is UDP.

There are three target IPs supported so if the Slave computers are more than three broadcast address should be used (xxx.xxx.xxx.255). IPs are saved under more_settings.ini

In order to achieve communication *MyID* and *MyPassword* in more_settings.ini should be the same on Master and Slaves.

Network lock synchronization > This computer role

Master: Sends commands to other USB Raptors

Slave: Receives commands

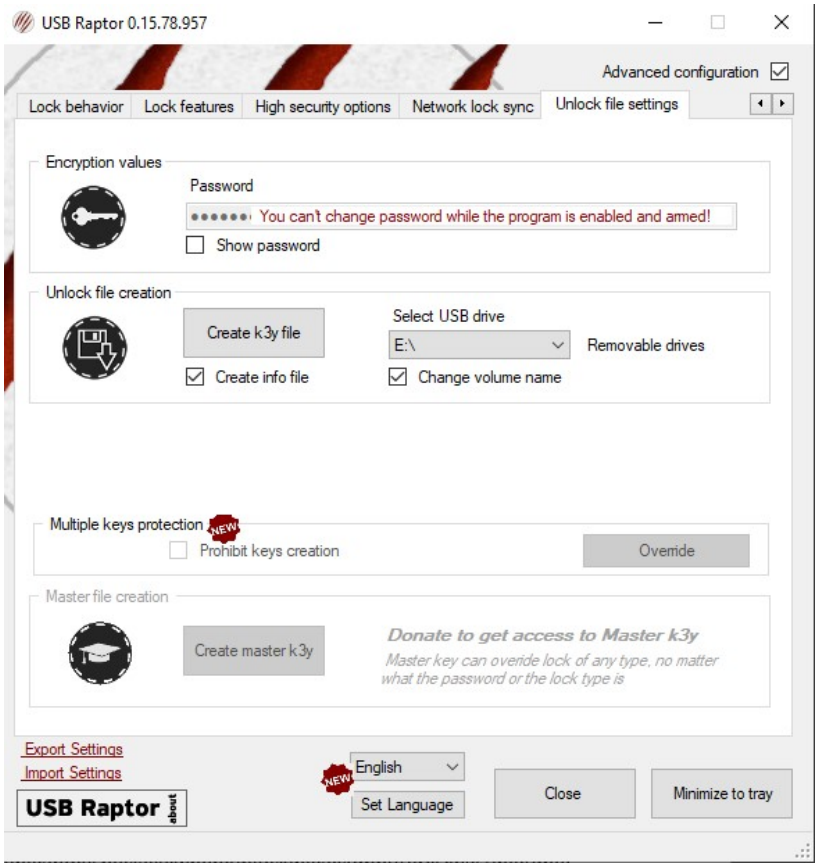
Network lock synchronization > What to synchronize

Sync lock: Selected on Master allows lock synch commands to be sent on the network, selected on Slave enables it to receive lock command.

Sync unlock: Selected on Master allows unlock synch commands to be sent on the network, selected on Slave enables it to receive unlock command.

Detect USB Raptors: see page 19 (“***Additional screens”***)

Unlock file settings



Unlock file settings > Encryption values

Password: Same as the on Simple configuration. The password is used by the encryption engine in order to create the unlock file. It is also used to unlock the protected user interface and unlock the computer when the password backdoor is enabled. Normally the password is not used since USB lock and USB unlock is the most common way to use USB Raptor but it is highly recommended to remember the password.

Unlock file settings > Unlock file creation

Create k3y file: Saves the generated file to the selected drive.

Select USB drive: Selects on which drive should be save the file. This is not the unlock drive. Unlock drive is detected automatically by USB Raptor.

Create info file: If enabled USB Raptor saves an informational file to USB drive as well. This file can be deleted but it is suggested to keep it to remind you that the USB key is used for security purposes.

Change volume name: If enabled USB Raptor renames the USB Drive to “USB RAPTOR”.

Unlock file settings > Multiple keys protection *(experimental option)*
Available only for donors.

Prohibit keys creation: If enabled USB Raptor doesn't allow users to create keys. This is option can be used to avoid creating copies of keys once a key is already is made.

Override: When a valid unlock key is detected on one USB port the button can give the ability to create an additional key.

Unlock file settings > Master file creation

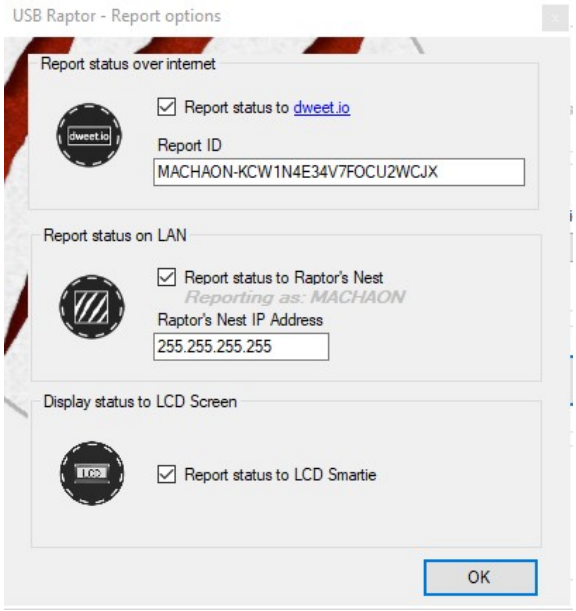
Create master k3y: Saves the generated master k3y to the previous selected USB drive. Access to master key is limited to donors. See page 23 ("***Donation package"***)

Master key can be used as backdoor solution in case of lost key, forgotten password and other bad situations. Master key can override any kind of lock applied to the system.

USB Raptor version 0.0.6.56 and later uses a different master k3y scheme. This means that any previous key is useless with this version. You should re-create master keys for this version.

Additional screens

Report options



Report options > Report status over internet

Report status to dweet.io: Enables the program to report its state to the dweet.io and the user can be informed by visiting the appropriate web page about the USB Raptor's status. Currently the following status values are reported: *Enabled, Disabled, Armed, Locked, Unlocked, Wrong Password, Wrong Key, Report Enabled, Report Disabled.* The page can be accessed by clicking the blue hyperlink (dweet.io) on the configuration panel.

> Dweet.io service is a third party service which is offered for free as you long you agree with their terms. Please visit the F.A.Q. pages to get more info about it: http://dweet.io/faq

Report ID: It is a unique ID (auto generated by USB Raptor) which is used to report the status to dweet.io. This ID can be changed by the user. Once it is changed the report function will use the new ID automatically. It is recommended to use a long key to avoid conflicts with already used ids on dweet.io service.

> USB Raptor can't provide any ID availability check for Dweet.io service. Please use a complex ID to ensure that your ID is not already used by another device. Default random ID is quite ok in most of the cases.

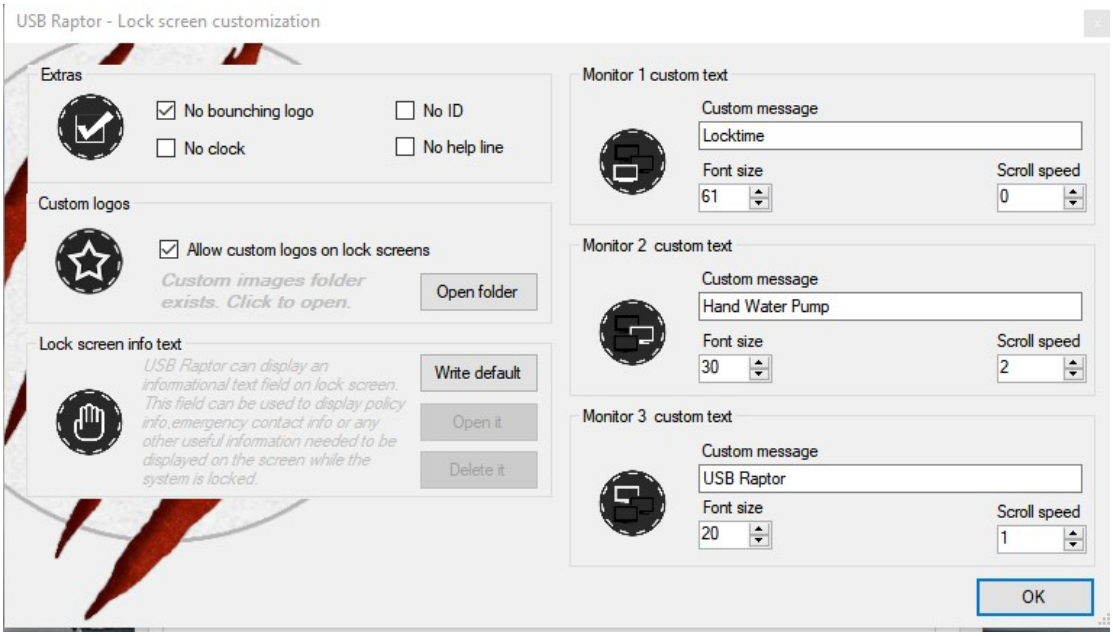
Report options > Report status on LAN

Report status to Raptor's Nest: Enables the program to report its state to the Raptor's Nest utility. This utility is contained in the main release package. For more info please contact developer.

Report options > Display status to LCD screen

Enables interaction with LCD Smartie to display the status on an LCD creen attached on the computer.

Lock screen customization



Lock screen customization > Extras

No bouncing logo: Disables the USB Raptor popup logo on lock screens.

No clock: Disables the digital clock displayed on the middle top of the screen.

No ID: Removes the ID from lock screen.

No help line: Disables the bottom help line which contains the accepted unlock methods and removes the local IP indication as well.

Lock screen customization > Monitor 1 custom text

Custom Message: The message should be displayed on the 1st monitor. User can select any text to be displayed while the system locked. The following keywords are accepted as well: Clock = displays clock, Uptime = displays the time the system is active, UptimeRaw = displays the raw uptime value as system reports it.

Font size: Sets the size of the message.

Font size: Sets the text scrolling speed. Setting this value to 0 keeps the text steady.

Lock screen customization > Monitor 2 custom text

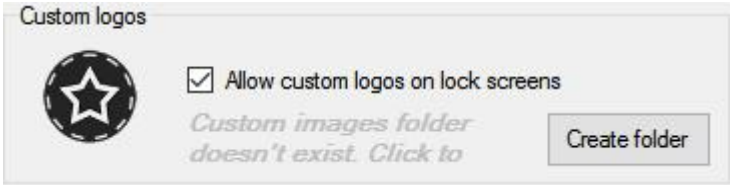
As in "Monitor 1 custom text" without keyword support.

Lock screen customization > Monitor 3 custom text

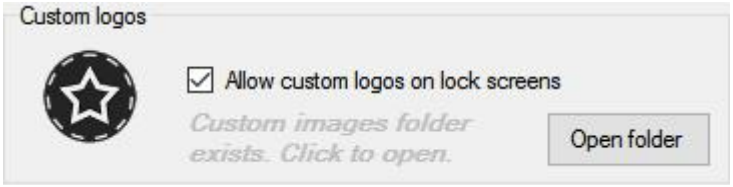
As in "Monitor 1 custom text" without keyword support.

Lock screen customization > Custom Logos

Allow custom logos on lock screens: Enables USB Raptor to load custom images to lock screens instead of the standard logos. Depending on the existence of the "customimages" folder the program will display one of the following menu structures on the screen.

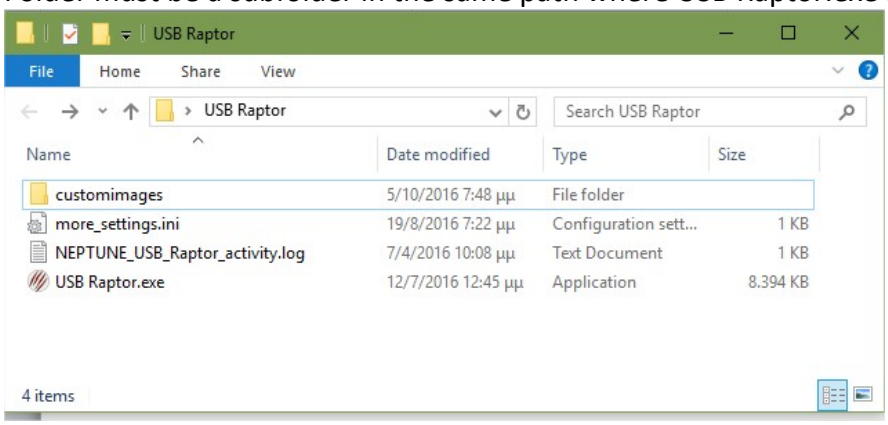
1. 

Folder doesn't exist and user can create it using the "Create folder" button.

2. 

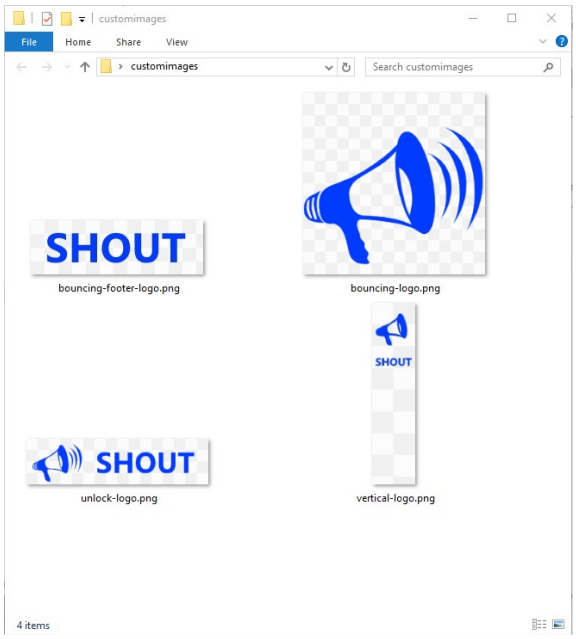
Folder exists and user can open it using the "Open folder" button.

Folder must be a subfolder in the same path where USB Raptor.exe lies.



Custom images should be in png format and filenames are predefined (filenames are case sensitive):

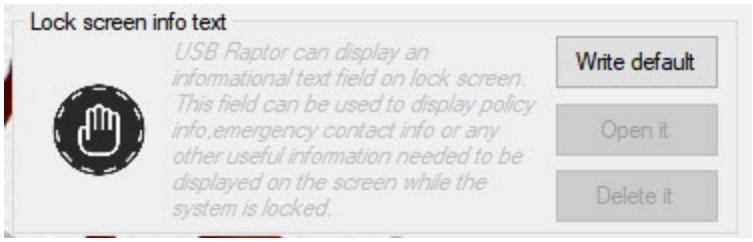
- **bouncing-logo.png** is the image which will replace the bouncing logo.
- **bouncing-footer-logo.png** is the image which will replace the bouncing logo footer.
- **unlock-logo.png** is the image which will displayed on the password screen.
- **vertical-logo.png** is the image will be displayed on the left edge of the screen when bouncing logo is disabled.



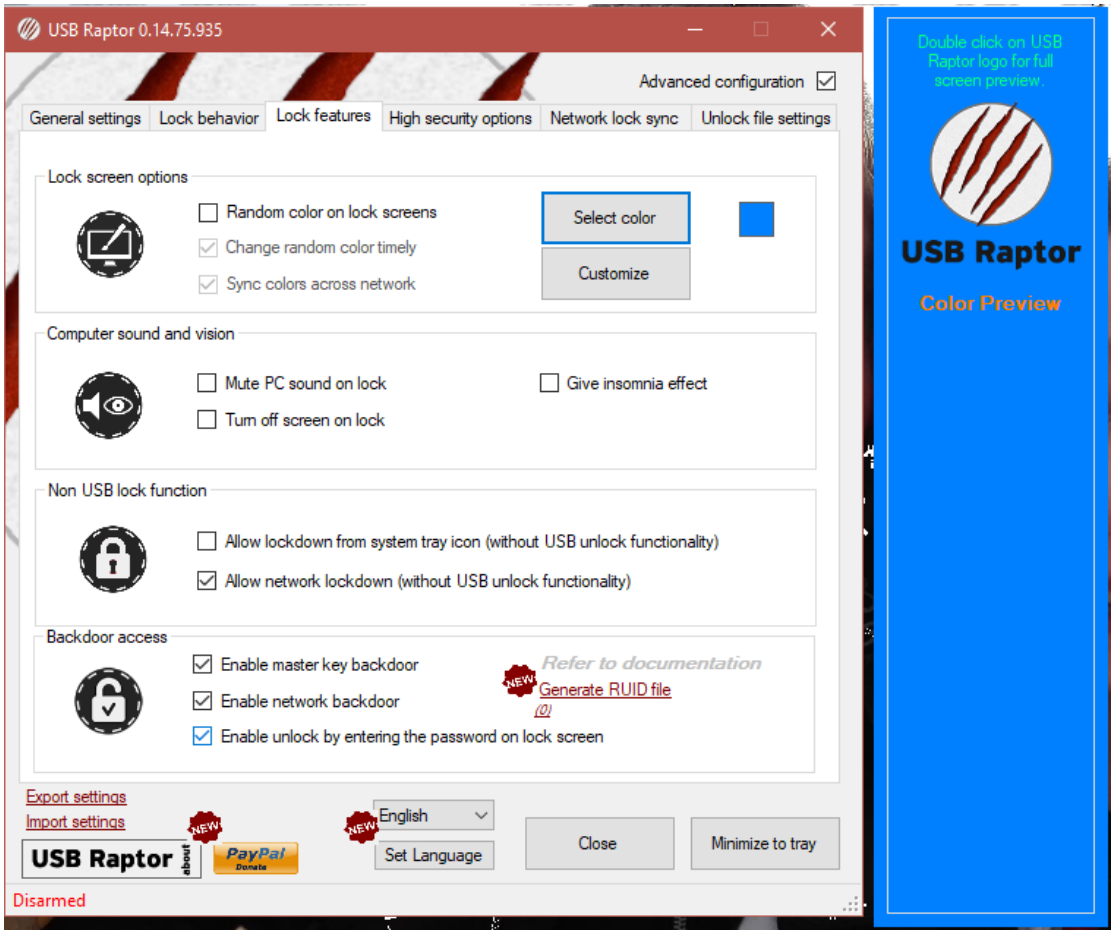
Lock screen customization > Lock screen info text

This special function is for the cases where a company disclaimer must be displayed on lock screen. All informational text should be placed in a text file on the same folder with USB Raptor.exe called “lockinfo.txt “.

Three buttons are available on the settings window to help users create edit or delete the file. Buttons “Open it” and “Delete it” are available only when a valid file is detected on program folder.

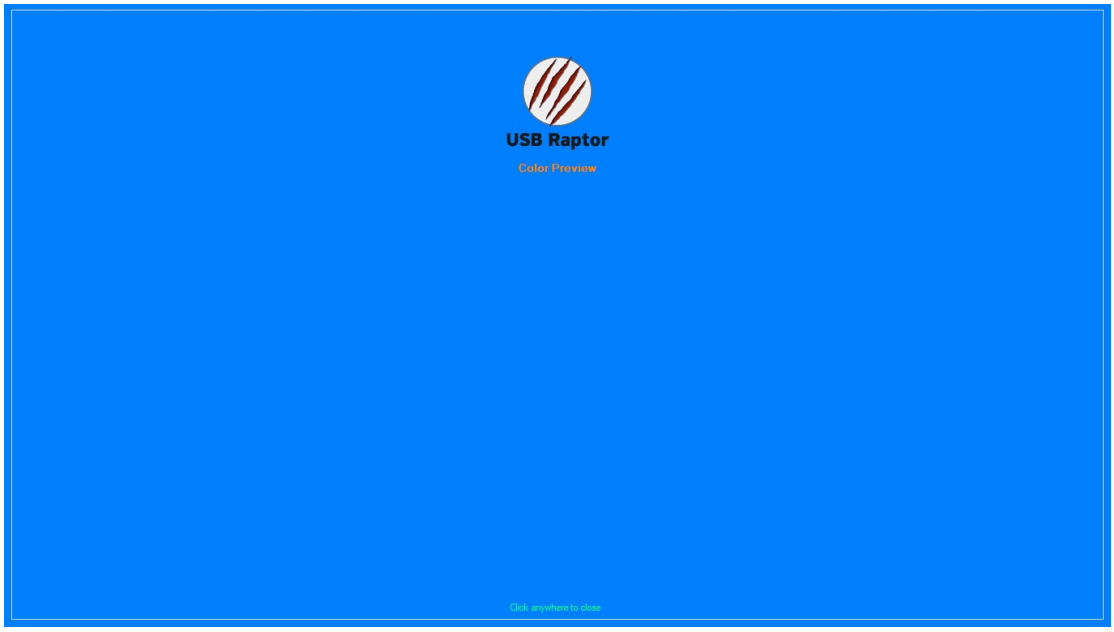


Color preview window



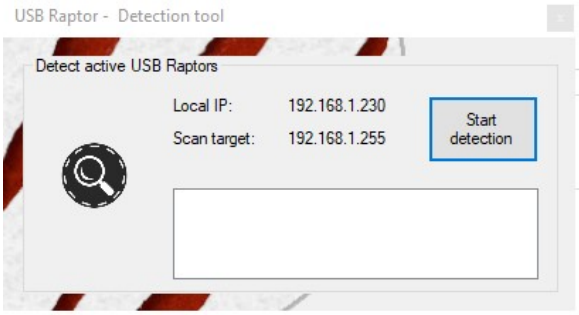
When a new steady color is selected on the drop down box a preview window appears in order to give the user the ability to test the new lock screen color. This window is closing automatically after 3 seconds.

By double clicking the USB Raptor logo on this preview window the preview window goes full screen, this way the user can see the real result on full screen preview and decide which color is suitable for lock screen.



To close this preview window just click anywhere on the screen.

Detection tool



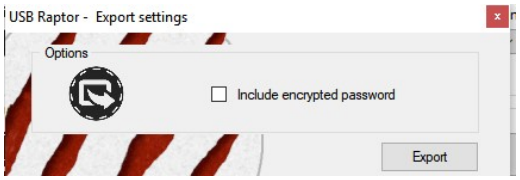
Detection tool > Detects active USB Raptors

Start detection: Starts network discovery for other computers running USB Raptors. The list populated with computer name, IP address and USB Raptor's ID.

Import and Export Settings

Using the Export settings and Import settings you can save USB Raptor configuration into a file and restore them. This is a convenient way to back up your configuration and restore it in a later time or setup a multiple instances of USB Raptor with the exact same settings.

Exporting is simplified and can contain (if selected) the USB Raptor password in encrypted format.



Export and Import functions are reserved for donors and will be enabled once a donation is send to the developer.

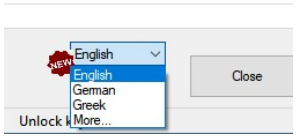
Auto import on first start

Upon first start the auto the program can get its full configuration but a specific file. This file should be located on the same directory with the executable and named as *predefined_settings.txt*. The structure should be the same with exported file. After the successful import the settings file will be automatically deleted.

> Restoring encrypted password is automated by USB Raptor. The value of "EncryptionKey2" filed is automatically processed during the process. This is convenient to export and import the same settings keeping the password secure.
>
> However if you want to apply a new password upon import (or auto import) you can use plain text entry as well. For this you have to remove the EncryptionKey2 field from the settings file (if it is exists) and add a field called EncryptionKey1.
> Once Encryptionkey1 filed is detected, USB Raptor will set the text value as new password.

Language

Well pretty much self-explained. USB Raptor is now moving to multi language support, but in order to have more languages included your help is needed.
Please contribute new languages by using the "More..." option under the dropdown menu.



USB Raptor usage scenarios

1. **Lock your computer while you are leaving your desk.**
   When you are in company environment you may want to lock your computer while you are away from your desk. USB Raptor can help you to lock your computer by just removing your USB flash drive from your computer port. When you are back you can plug in again your USB flash drive to automatically unlock your computer.

2. **Synchronized lock and unlock for computers on your work environment.**
   If you have two or even more computers on your "cubicle", locking and unlocking when you leaving for a short period is a pain. USB Raptor offers sync lock/unlock. By removing the USB drive on the master computer all computers will lock. Placing back the USB drive to master computer with unlock them immediately.

3. **Remote computer lockdown.**
   i) When you are away from your desk and you have left your computer unlocked, you can remotely set it to lock state (even if you have the unlock USB drive fitted to one of its USB ports). Remote unlock is also possible by sending remote commands. You can easily set an Android device to send the commands and control lock and unlock state remotely.
   ii) If your kid plays more than its allowed time on the PC and you want to lock the computer remotely, USB Raptor is the solution for the case. Just use the remote lockdown command. You can also display custom messages on the screen.

4. **Be the master of the class.**
   In classroom with computers you can control when all computers unlock simultaneously. This gives teacher the ability to control students access to their PCs.

5. **Create a hardware key for computer controlled machines.**
   Computer controller cutters, routers and other industrial machines can be dangerous when used by unauthorized personnel. Using USB Raptor you can control who is working with the controlling computer.

Reset settings to default – Clear computer

A special tool lies “under the hood” in order to help users to clear all settings to default. In order to access this tool you have to follow the procedure as described below.

While you **already running the USB Raptor**

- Disable USB Raptor.
- Place a text file named “allowrestoredefaults.txt” to program folder (the same folder where USB Raptor.exe is located).
- Double click on USB Raptor status image ( ).
  The following screen will appear:

- Click on the “Clear all settings to default” button which is located on the top right corner.
- A new window will appear (shown below). Check the “Clear all settings” check box and confirm by clicking on OK button.

The program will give you a warning message and will close.
All settings including the password will be reset to default values.

WARNING: The restore default process cannot be undone.

WARNING: To protect your program from unauthorized access you are highly advised to enable password protection on USB Raptor interface!

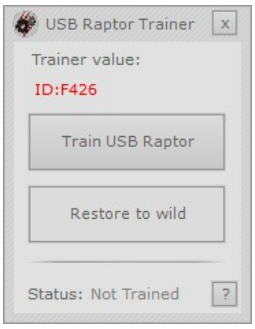
Donation package

Donors will receive a link to download a package with info for network communication scheme and master keys creation.
Additional utilities, such is “USB Raptor Serial Bridge” and “USB Raptor Talon” (network command utility), may be included depending on their development and stability status.
A minimum € 8.00 donation is required for individual users and € 21.00 for business or other organizations.

Custom master key

Currently master key encoding scheme is hardcoded into executable.
By forking the source code, it is possible to create your own “special” edition of USB Raptor which is not following the standard master key scheme.

Master key customizer - USB Raptor Trainer



USB Raptor Trainer is a new utility created especially for users who want to get a **special master key for USB Raptor**. This utility can change the Master key “channel” in order to use a different Master key than the standard one which all donors are able to create.
Using USB Raptor Trainer you can be sure that no other donor can unlock your system with his Master key.
USB Raptor trainer can be used in as many computers as you like setting them to the same Master key “channel” and making them accept the same Master key.

This method enables user to download and use normally the future USB Raptor updates without losing their own special Master key functionality.

This utility is available upon request under a small fee. Please contact to *ngeorgousis(at)hotmail.com* for more info about this utility.