RankSecure

Pocket Rocket FLE

Model: Addonics Pocket Rocket

File Level Encryption

User Guide

RankSecure

OVERVIEW

The Pocket Rocket works by encrypting data using a 256- bit algorithm set by a password key. It encrypts files by overwriting the same sectors used by the file with encrypted data. Then renaming the file with a new filename extension. The Pocket Rocket comes new in a pass-through mode, and will not function until a password is a set using the software utility.

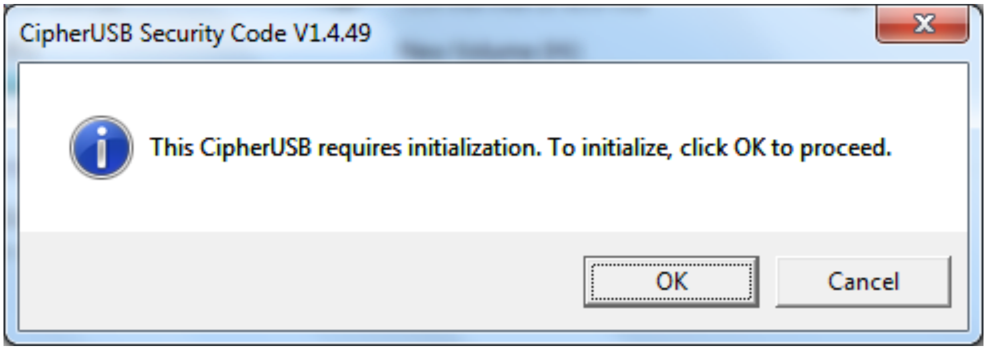
TWO –FACTOR AUTHENTICATION

Once a Pocket Rocket with two-factor authentication (CAUF1W-2, CAUF1M-2, CAUF2W-2, and CAUF2M-2 M-2) has been activated with a password, it will not allow the storage to connect to the operating system until the Pocket Rocket utility has been run once and the correct password is given. The Pocket Rocket will only accept the password it was programmed with during the initial setup process. These models include an emulated CDROM drive that will auto-start the cipher utility, which immediately prompts for the password.

Initial Setup

This procedure only needs to be done when setting up the Pocket Rocket for the first time, or when a new password is desired. The Pocket Rocket will retain the last password it was programmed with the and models without two – factor authentication do not require any driver or software to work.

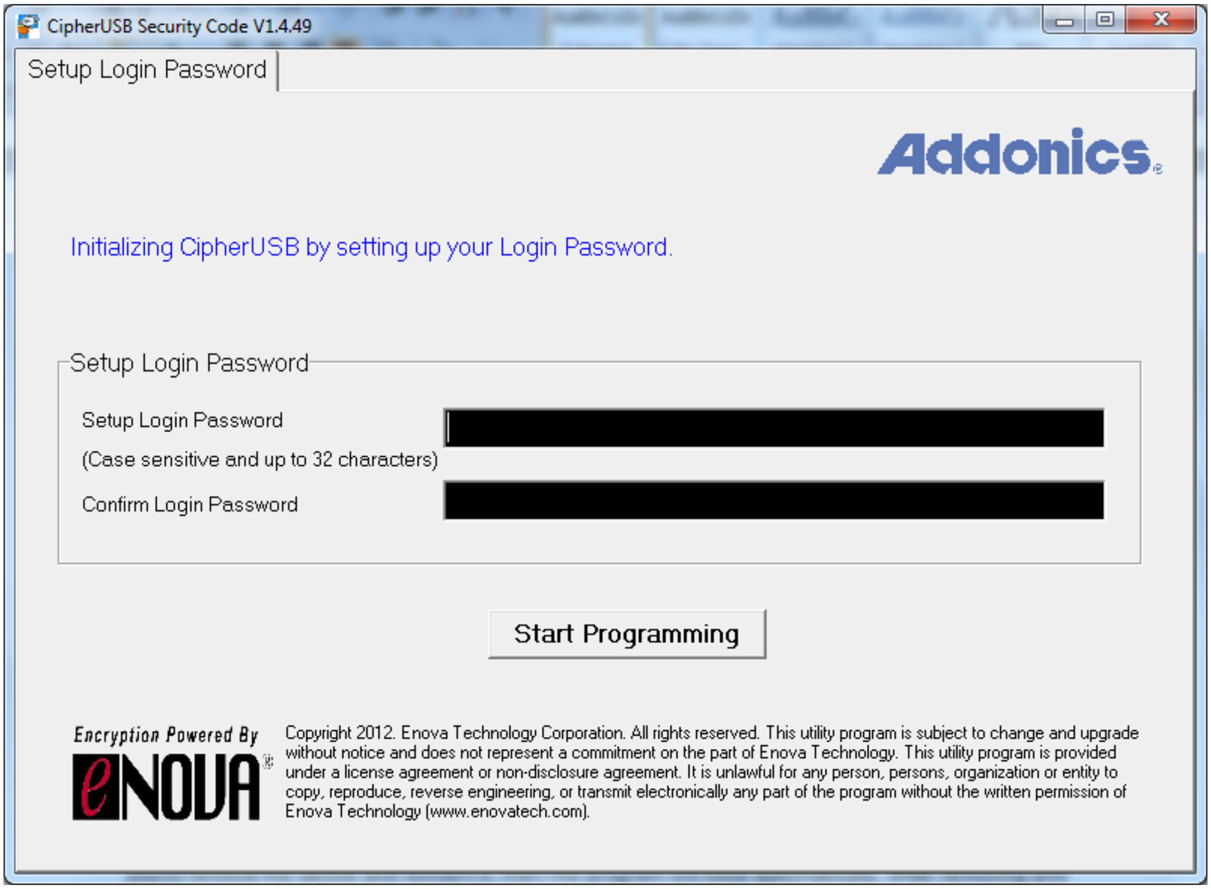
1. Connect the Pocket Rocket to a computer running windows, and connect a USBstorage device into the Pocket Rocket . The Pocket Rocket will not respond until a working storage device is connecxted to its USB devciceport.
2. For models without two-factor authentication, insert the Pocket Rocket password utility disc. If an autorun menu appears select “run Pocket Rocket .exe or browise to your cd drive using windows explorer and launch the Pocket Rocket program. If you are setting up the Pocket Rocket for the first time.
   The following dialog box should appear:



CipherUSB Security Code V1.4.49

This CipherUSB requires initialization. To initialize, click OK to proceed.

3. Click ok to proceed to the utility. Choose a password as short or as long (up to 32 characters) as desired and enter it into the “setup”and “Confirm fields. Then click start.



Initializing CipherUSB by setting up your Login Password.

Setup Login Password

Setup Login Password [redacted]

(Case sensitive and up to 32 characters)

Confirm Login Password [redacted]

Copyright 2012. Enova Technology Corporation. All rights reserved. This utility program is subject to change and upgrade without notice and does not represent a commitment on the part of Enova Technology. This utility program is provided under a license agreement or non-disclosure agreement. It is unlawful for any person, persons, organization or entity to copy, reproduce, reverse engineering, or transmit electronically any part of the program without the written permission of Enova Technology (www.enovatech.com).

CAUTION: KEEP YOUR PASSWORD SAFE AND REMEMBER IT.OTHER POCKET ROCKET DEVICES CAN USE THE SAME PASSWORD TO UNLOCK MEDIA ENCRYPTED BY THIS DEVICE.IF THE PASSWORD IS LOST THE DATA IS LOST THERE IS NO “BACK DOOR “TO UNLOCK OR RECOVER THE PASSWORD OR THE ENCRYYPTION KEY.

After confirming once more for security, the Pocket Rocket will be programmed with a 256-bit encryption key seeded by the password. Once the Pocket Rocket has been programmed, a dialog will appear instructing you to remove the device and reinsert it, and then the program will close automatically. After removing and reinserting the Pocket Rocket it will be properly initialized.

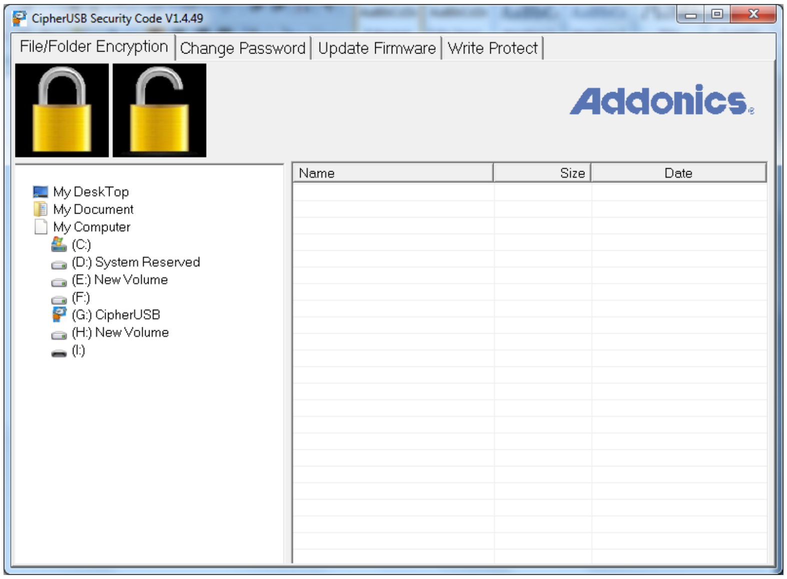
USING THE POCKET ROCKET WITH STORAGE

Data that is encrypted will only be readable after being decrypted again using a Pocket Rocket programmed with the correct password.

While it is required to connect the Pocket Rocket with a storage device attached in order to encrypt files, it is not necessary to encrypt files on the attached storage. Files may be encrypted or decrypted on any of the computers storage devices.

USING THE CIPHERE USB FLE TO ENCRYPT FILES

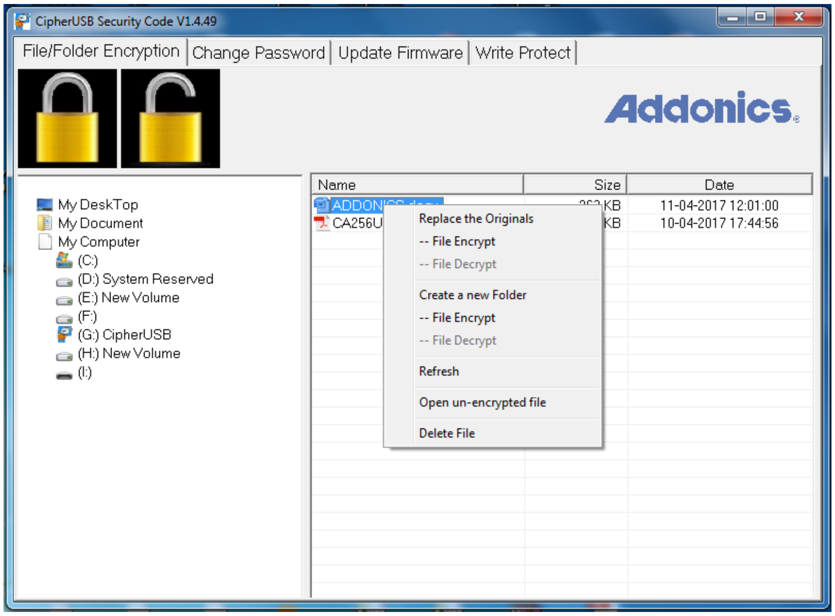
Once the Pocket Rocket file has been initialized with a password (and has been unlocked if the two factor feature is included).the software will present the file / folder encryption screen similar to this



On the left side of the window is a tree view of the computers storage devices. Clicking on any of these will show their contents on the right side.

To encrypt files, select one or more items on the right side, then drag them to the closed padlock icon in the upper left corner of the window. To decrypt files, select one or more encrypted files on the right side, and then drag them to the open padlock icon in the upper left corner of the window.

Alternatively right clicking on any selected item will bring up the context menu as shown below:



Name	Size	Date
ADDON	KB	11-04-2017 12:01:00
CA256U	KB	10-04-2017 17:44:56

The files encrypt and decrypt selections in the replace the originals section work the same as dragging to the padlock icons.
Choosing file encrypt in the create a new folder section will cause a new folder to appear called AES_Decrypt, containing the decrypted version of the files.

Performing encryption on a folder or drive will operate on all of the files in that folder or drive. Note: the encryption and decryption functions do not traverse through subfolders. Only the actual files in the selected folder or drive will be encrypted. Files located in subfolders will not be affected.

Write Protect

Write protection only works with storage devices that are removable media. Such as USB flash drives or flash media in a standard reader. Write protection will not work with fixed disk media, such as USB hard drives or SSD DRIVES, THE Adonis pocket Esata/usb DigDrive, or SATA Adapter or the addonics USB 3.0 TO esata mini adapter.

Write protection works by blocking requests from the computer to write to the media and does not protect the media from being written to if the media is not connected to the Pocket Rocket device. It only works with the drive connected through the Pocket Rocket.

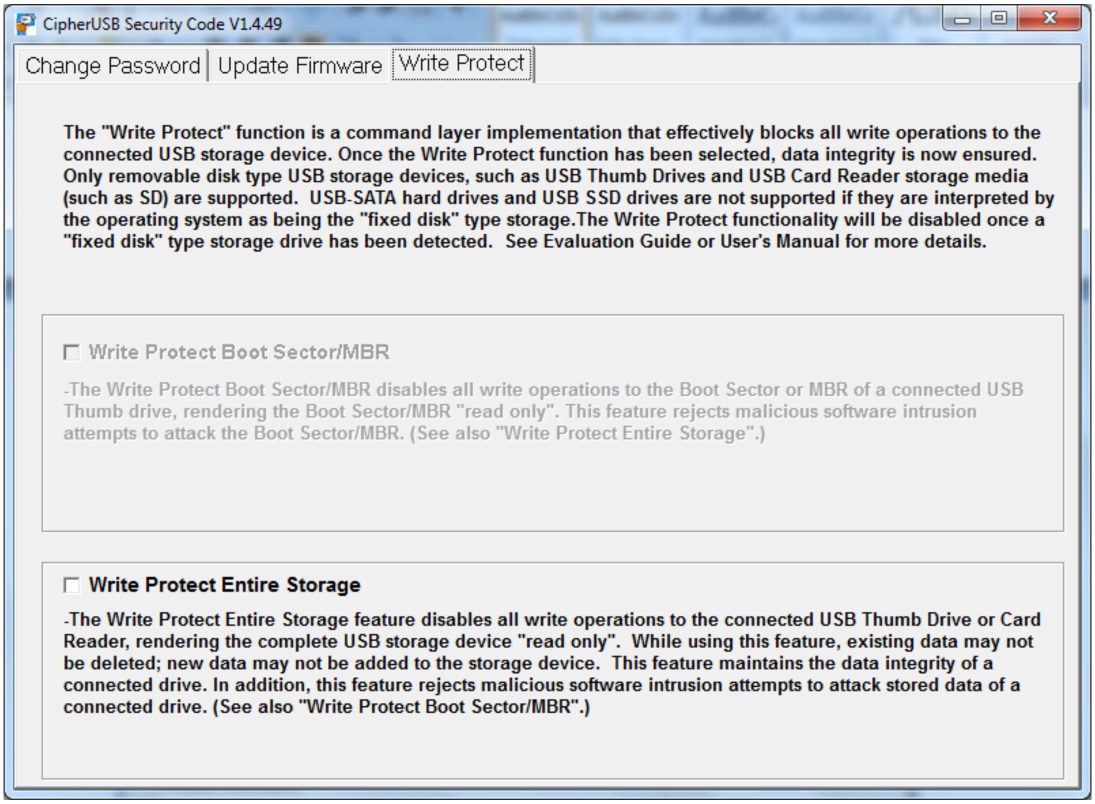
There are two types of write protection available:

Write Protect book record/MBR

Checking this box will cause the Pocket Rocket to refuse any write requests from the computer to the first logical sector of the removable media. This feature provides basic protection against malware attacks that attempt to deploy payload at boot time or upon insertion of removable media.

Write Protect Entire Storage

Checking this box will cause the Pocket Rocket to refuse ALL write requests from the computer to the removable media. This feature will protect all data on the media from being erased or overwritten while in use with the Pocket Rocket device.



The "Write Protect" function is a command layer implementation that effectively blocks all write operations to the connected USB storage device. Once the Write Protect function has been selected, data integrity is now ensured. Only removable disk type USB storage devices, such as USB Thumb Drives and USB Card Reader storage media (such as SD) are supported. USB-SATA hard drives and USB SSD drives are not supported if they are interpreted by the operating system as being the "fixed disk" type storage.The Write Protect functionality will be disabled once a "fixed disk" type storage drive has been detected. See Evaluation Guide or User's Manual for more details.

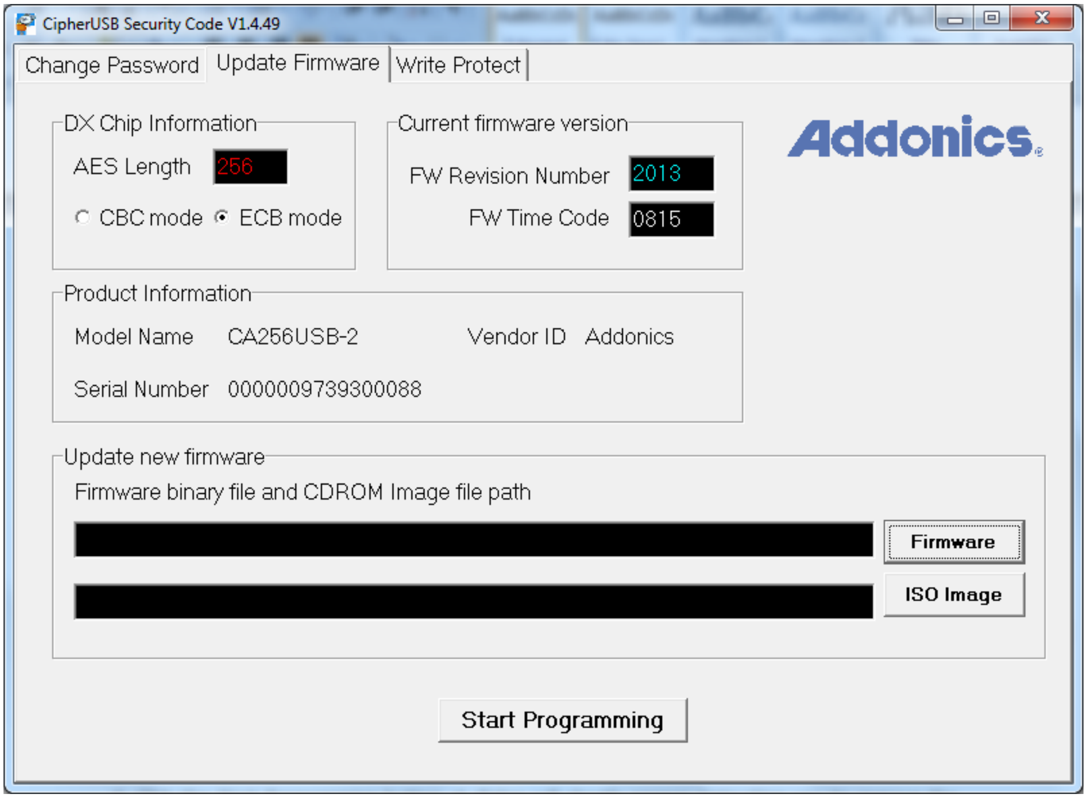
☐ Write Protect Boot Sector/MBR

-The Write Protect Boot Sector/MBR disables all write operations to the Boot Sector or MBR of a connected USB Thumb drive, rendering the Boot Sector/MBR "read only". This feature rejects malicious software intrusion attempts to attack the Boot Sector/MBR. (See also "Write Protect Entire Storage".)

☐ Write Protect Entire Storage

-The Write Protect Entire Storage feature disables all write operations to the connected USB Thumb Drive or Card Reader, rendering the complete USB storage device "read only". While using this feature, existing data may not be deleted; new data may not be added to the storage device. This feature maintains the data integrity of a connected drive. In addition, this feature rejects malicious software intrusion attempts to attack stored data of a connected drive. (See also "Write Protect Boot Sector/MBR".)

Updated Firmware



DX Chip Information

AES Length 256

○ CBC mode ● ECB mode

Current firmware version

FW Revision Number 2013

FW Time Code 0815

Product Information

Model Name CA256USB-2 Vendor ID Addonics

Serial Number 0000009739300088

Update new firmware

Firmware binary file and CDROM Image file path

1. Read the firmware update for important changes to the units operation or the update procedure. If a firmware release note contradicts these instructions, follow the release notes instead.

2. Insert the Pocket Rocket with a storage device. The Pocket Rocket will not respond unless a storage device is attached to it. 3. Run the Pocket Rocket, exe program. If the Pocket Rocket unit has not been

3. Initializing with a password, the update firmware tab will not appear. Initialize the unit with a password, unplug it, plug it back in, then select the update firmware tab.

4. Be sure the DX Information section shows AES Length is 256 and ECB mode is selected for the CAUF1W, CAUF1W-2, CAUF1W-2, CAUF1M-2 or CAUF1M.CBCmode for the CAUF2W, CAUF2W2, CAUF2M, CAUF2M-2.

5. In the update new firmware section, click the firmware button. Change the file type to “Binary file (*256) if necessary, then browse to the folder containing the new firmware and open it.

6. Click the start Programming button. A dialog will shortly appear instructing you to remove the Pocket Rocket and reinsert it. After removing and reinserting the device, the firm ware update will be completed.

NOTE: The Pocket Rocket may or may not need to be initialized with the password again . if a storage device using the existing password is connected when the Pocket Rocket is reinserted and the file system appears intact, the password has been retained. Otherwise it may be necessary to set the password again.

Technical Support

If you need any assistance to get your unit functioning properly, please contact RankSecure technical support by clicking on this link: http://ranksecure.in/support/

CONTACT US

RANKSECURE

Ground Floor, Krishna Bhavan, Next to Bus Depot,
Sion (West), Mumbai 400 022. India.

Tel: (022) 24030820 / 24097579 / 9773 444 007
Email: sales@ranksecure.in
Web: www.ranksecure.in