

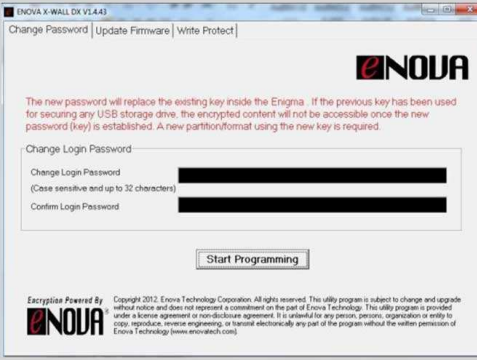


COMPARISON TABLE - ENIGMA I & ENIGMA II

Model	Enigma I	Enigma II
Product Picture		
Form Factor	USB pass through dongle encrypting any variety of USB MSC drive	USB dongle encrypting selective file/folder of host detectable storage drives
Secure Data	Data-at-Rest	Data-In-Motion
Encryption Method	(Full Disk Encryption) Encrypts any connected USB MSC device ¹	(File Folder Encryption) Encrypts selective file/folder of host detectable storage drive ²
Interface	USB2.0 (Compatible with USB 1.0/1.1/2.0/3.0)	USB2.0 (Compatible with USB 1.0/1.1/2.0/3.0)
Crypto Processor	X-Wall [®] DX-256/DX-256C	X-Wall [®] DX-256/DX-256C
AES Mode of Operation	ECB/ CBC	ECB/CBC
Encryption Strength	256-bit	256-bit
Supported OS for Login ³	Windows or MAC (supports up to MAC version 10.9)	Windows or MAC (supports up to MAC version 10.9)
2 Factor Authentication ⁴	Yes	Yes
Write Protect	Yes	Yes
Software/Driver	No	No
Certification	NIST/CSE	NIST/CSE
Dimension (mm)	60.7mm (L) x 19.6mm (W) x 10.1mm (H)	60.1mm (L) x 19.6mm (W) x 10.1mm (H)
Weight (g)	11g	11g
SKU	EMA-DX256E-2W (for ECB, Windows) EMA-DX256C-2W (for CBC, Windows) EMA-DX256E-2M (for ECB, Windows & MAC) EMA-DX256C-2M (for CBC, Windows & MAC)	EMA-DX256E-4W (for ECB, Windows) EMA-DX256C-4W (for CBC, Windows) EMA-256E-4M (for ECB Windows & MAC) EMA-256C-4M (for CBC Windows & MAC)



ENOVA X-WALL DX V1.4.4.3
Change Password | Update Firmware | Write Protect

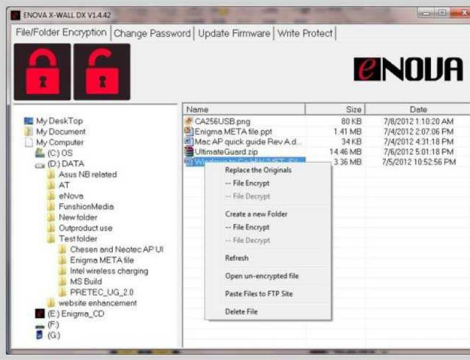
The new password will replace the existing key inside the Enigma. If the previous key has been used for securing any USB storage drive, the encrypted content will not be accessible once the new password (key) is established. A new partition/format using the new key is required.

Change Login Password
(Case sensitive and up to 32 characters)

Confirm Login Password

Start Programming

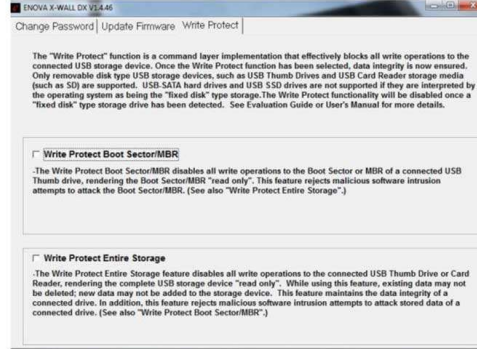
Encryption Powered By **ENOVA**
Copyright 2012, Enova Technology Corporation. All rights reserved. This utility program is subject to change and upgrade without notice and does not represent a commitment on the part of Enova Technology. The utility program is provided under a license agreement or non-disclosure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



ENOVA X-WALL DX V1.4.4.2
File/Folder Encryption | Change Password | Update Firmware | Write Protect

Replace the Originals

Name	Size	Date
CA256USB.png	80 KB	7/8/2012 1:16:20 AM
Enigma.META file.ppt	1.41 MB	7/4/2012 2:07:06 PM
Mac AP quick guide Rev A.d.	34 KB	7/4/2012 4:31:18 PM
UltimateGuard.zip	14.46 MB	7/6/2012 5:01:18 PM
	3.36 MB	7/5/2012 10:52:56 PM



ENOVA X-WALL DX V1.4.4.6
Change Password | Update Firmware | Write Protect

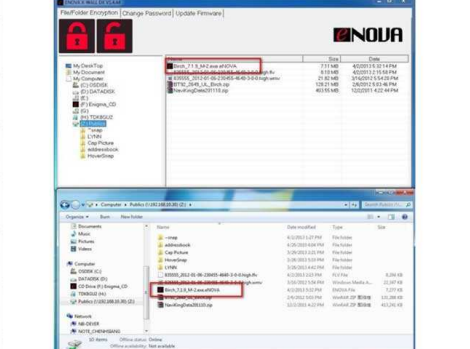
The "Write Protect" function is a command layer implementation that effectively blocks all write operations to the connected USB storage device. Once the Write Protect function has been selected, data integrity is now ensured. Only removable disk type USB storage devices, such as USB Thumb Drives and 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 complete USB storage device "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")



Windows Explorer showing encrypted files and folders.

References:

- 1 USB MSC device includes Blu-Ray DVD, DVD R/W, CD-R, thumb drive, hard disk or any flash card inserted into a USB card reader.
- 2 Selective files/folders of any OS detectable storage drives includes boot drive, external drive such as USB or 1394, network attached storage and virtual drives such as Dropbox, OneDrive, Google Drive and iCloud etc.
- 3 The initialization of the Enigma I & II equipped with 2-factor authentication requires either Windows or Mac OS. We also provide an alternative single factor authentication Enigma I which is independent from any OS.
- 4 Single factor means using the hardware Enigma HCM as a key without additional user's password.