Enova® X-Wall® XO

Frequently Asked Questions--FAQs

Q: What is "*X-Wall XO*"?

A: *X-Wall XO* is the fourth generation product that encrypts and decrypts the entire volume of the hard drive. The entire volume includes the boot sector, all temp files, all swap files, **and** the entire operating system. Enova accomplishes this without degrading overall system performance. This is accomplished by using **Enova's real-time hard drive cryptographic bridge ASIC** (Application Specific Integrated Circuit). The Enova XO product line is NIST, FIPS and CSE certified for DES, TDES and AES cryptographic engines.

Q: How does *X-Wall XO* differ from previous *versions?*

A: ***XO improvements over previous models include:***

Power On Self-Test (POST) – *XO is* equipped with POST, which facilitates manufacturing and testing procedures. The net result of POST is its logs can be pulled using software programming techniques.

Low Power Consumption – the *XO* internal cryptographic engine is running at a reduced clock speed of 66MHz (compared with 133MHz of previous versions) while achieving the same performance. The *XO* can burst a hard drive at 133MB/sec, which is the maximum bandwidth a modern IDE hard drive allows.

Built-in Application Programming Interface (API) – *XO* allows software to communicate directly through this specifically engineered interface. The API allows polling of *XO* microchip status, enabling an encryption mode (and/or By-Pass mode), delivering cryptographic key and other features through software programming techniques. Hardware modification is not required if the API is being utilized properly.

Q: What encryption strengths are available in X-Wall XO?

A: X-*Wall XO-64* – DES 64-bit encryption strength
X-Wall XO-128 – TDES 128-bit encryption strength
X-Wall XO-192 – TDES 192-bit encryption strength

Q: How can *X-Wall XO* encrypt the entire disk without sacrificing drive performance?

A: *X-Wall XO* is specifically engineered for high speed communications with the disk drive. It offers 1.1 Gbit/sec or greater throughput to enable real-time communications with all Parallel ATA (PATA), IDE and Ultra DMA compatible hard drives. The operations of encryption and decryption are accomplished using high-speed hardware circuitry to ensure no measured loss of performance. Software device drivers are not used to enable the *XO;* thus memory and interrupt overheads are completely eliminated.

Q: Is there a capacity limitation as with on other products?

A: No. *X-Wall XO* encrypts all data on the disk drive. If you have a 1TB hard drive, the entire 1 TB will be encrypted.

Q: Do I need to establish a separate "encrypted folder" under file directory as required by some software solutions?

A: No. All data written to the disk drive is automatically encrypted.

Q: If I back my data up to an external drive, is that backed up data encrypted?

A: Trick question. If the external backup drive has an Enova X-Wall XO chip installed, all data backed up will be encrypted. If the backup drive does not contain an encryption engine of any kind, the data will be in the clear, or, unencrypted. Enova recommends that your backup device be capable of encrypting its contents and that you back your data up on a regular basis. To

enable your secure back up, Enova recommends using Enova Secure USB2.0 to IDE external storage device. See below web link for product description and other Enova products: **http://www.enovatech.com/products/reference/usb2.0_ide.htm**.

Q: How does *X-Wall XO* function?

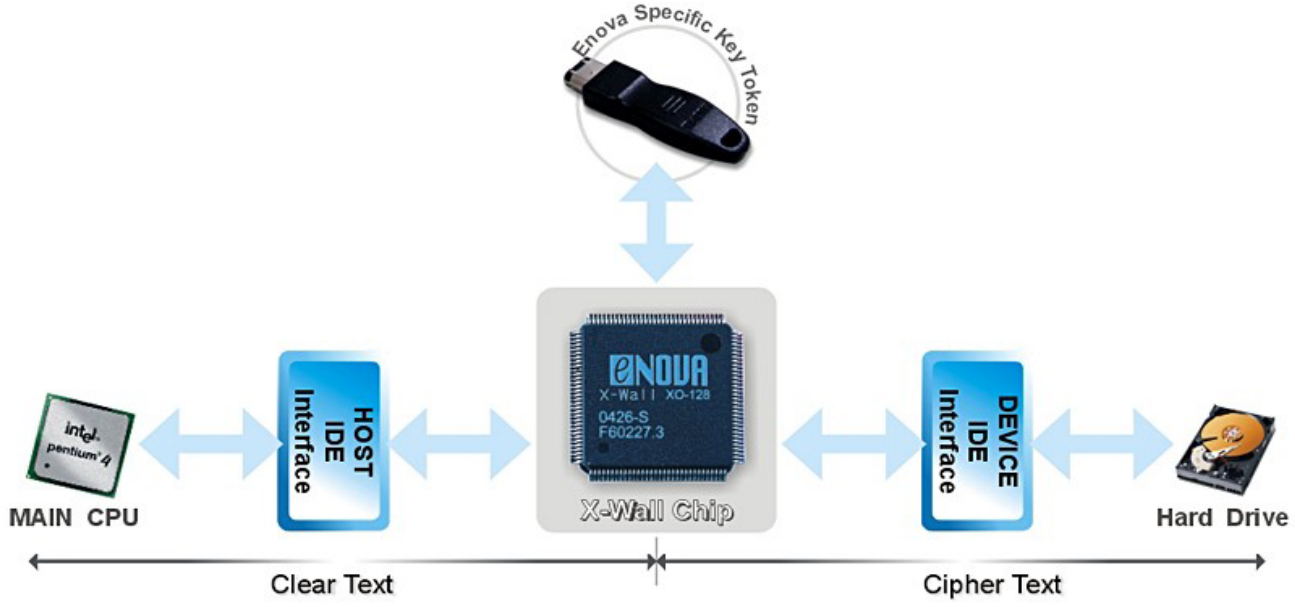
A: Enova's *X-Wall XO* sits before your IDE Ultra DMA disk drive. It intercepts, measures, audits, interprets, translates, and relays IDE commands & data to and from the disk drive. Data is automatically encrypted using the encryption key. Prior to data being written to the disk drive, *XO* encrypts the data, and saves the data to the disk drive.

When data is read to the disk drive, *XO* decrypts it before sending the data to the host. The encryption and decryption operations are transparent to the user, making *XO* invisible to the system.

The Secure Key Token contains the "Cryptographic Key" used by the *XO* cryptographic engine. Without this key token, attempts to access the encrypted data will be unsuccessful, even when the disk drive is moved to a different PC platform.

At power up, the "Cryptographic Key" is delivered to the *XO* register sets, using a proprietary hardware and/or software protocol. If the Cryptographic Key was incorrect or missing, *XO* will not allow access to the encrypted data on the disk drive. The X-Walled hard drive will be seen as a new drive; the entire encrypted content remains protected and secure. This is true even if the X-Walled hard drive has been moved to a different platform in an attempt to by-pass the authentication. Attempts to surface scan the entire disk drive platters in order to access protected data will be unsuccessful.

The Enova *XO* is a generic engine and it relies on the "Cryptographic Key" to enable all functionalities. The following illustration best describes how the *X-Wall* functions.



Q: Can *X-Wall XO* work with all types of disk drives?

A: The Enova XO products are compatible with PATA (IDE) interfaces. *X-Wall XO* can be operated with *Ultra ATA (Ultra DMA) 66/100/133* compliant disk drives with throughput of 1.1 Giga bit per

second. *X-Wall XO* is not compatible with SCSI or FC (fiber-channel) interfaces. Future plans are to introduce a SATA compatible product, suitable for use on 1.8", 2.5" and 3.5" drives.

Q: Can *X-Wall XO* work with all types of operating systems?

A: Yes -- the *X-Wall XO* is compatible with all operating systems, and does not require device drivers. The only requirement is an Ultra ATA PATA (Ultra DMA) compliant disk drive.

Q: Do I need any training to use *X-Wall XO*?

A: The good news is that you don't have to learn or manage anything. After inserting the *X-Wall Secure Key*, everything will function as before. The figure below presents an Enova *X-Wall Secure Key.* There is no bad news.

Q: How does *X-Wall XO* compare with Smart Card and PCMCIA encryption products?

A: *X-Wall XO* operates at drive interface speeds, and is much faster than PCMCIA or Smart Card solutions In addition, XO does not tax the Motherboard CPU, putting power back into the User's hands. XO encrypts all data on the disk drive, as opposed to selected files or directories. There is **no** possibility that any data or credentials will be unprotected on the hard drive. Drive locking and boot sector encryption solutions do not encrypt the data, leaving the data vulnerable to attack.

Q: Can I encrypt two or more hard drives via a single *X-Wall XO*?

A: It depends. Enova's *XO product line has been* engineered to encrypt one single hard drive. Multiple hard drives will require multiple *XOs.* However, in some **IDE to IDE RAID sub-systems**, one *XO* is able to drive the IDE to IDE RAID chip. All hard drives that are connected after the IDE to IDE RAID controller will be encrypted. In which case, one *XO* sits right in front of the IDE to IDE RAID chip, encrypting all hard drives that are directly connected through the IDE to IDE RAID controller. With respect to PCI IDE RAID subsystem applications, refer to the next question..

Q: Can *X-Wall XO* be utilized to protect the PCI IDE RAID sub-systems?

A: **Yes.** *XO* can be designed to encrypt the PCI IDE RAID subsystems. See below link for details about how ***Enova SecureIDE RAID*** controller is able to encrypt traditional PCI IDE RAID subsystems from Promise and 3 Waves controllers. In which case, the multiple *XO chips* sit right in front of all hard drives, encrypting all with real-time speed.
http://www.enovatech.com/products/reference/secureide_raid.htm

Q: Does *X-Wall XO* support 48-bit LBA addressing?

A: Yes. *X-Wall XO* supports 48-bit addressing and can control hard drive volumes greater than 137GB per drive.

Q: What is "DES/TDES"?

A: The NSA (National Security Agency) originally introduced DES (Data Encryption Standard). DES has since become a Federal data encryption standard as defined in FIPS 46-3 (Federal Information Processing Standards). DES works on 64-bit data segments with a 64-bit Cryptographic Key (of which 8 bits provide parity), resulting in a 56-bit effective length. A variant on DES is TDES, in which the plain text is processed three times with two or three different DES Cryptographic Keys. With two Cryptographic Keys used, the result is an encryption equivalent to using a 112-bit (128-bit) Cryptographic Key. With three Cryptographic Keys, the result is an encryption equivalent to using a 168-bit (192-bit) Cryptographic Key. In practice with a 128-bit TDES, the plain text is encrypted with the first key, decrypted with the second key, and then encrypted again with the first key.

DES, TDES, and AES (Advanced Encryption Standard) are called Symmetric Ciphers, which means the same Cryptographic Key is used for both encryption and decryption.

Q: How secure are DES and TDES?

A: Virtually impenetrable. Both DES and TDES algorithms are public, and have been surprisingly resistant to new cryptographic attacks over the last quarter century. Though Software DES 56-bit key length algorithms have been proven vulnerable, and are no longer proven against massive computer attacks, for most business applications DES remains adequate.

Q: How is key length related to security?

A: In the case of Symmetric Cipher (DES, TDES, and AES), a larger Cryptographic Key length creates a stronger cipher, which means an intruder must spend more time and resources to find the Cryptographic Key. For instance, a DES 40-bit strength represents a key space of 1,099,511,627,776 (2^{40}, 2's power 40) possible combinations. While this number may seem impressive, it is definitely feasible for a microprocessor or a specially designed ASIC to perform the huge number of calculations necessary to derive the Cryptographic Key. Surprisingly an investment of only about US$10,000 investment in FPGA (Field Programmable Gate Arrays) will be able to recover a 40-bit key in 12 minutes. Further, a US$10,000,000 investment in ASIC will be able to recover a 40-bit key in 0.05 second. A government agency that can afford investing US$100,000,000 or more will be able to recover a 40-bit key in a whopping 0.002 second! Thus a 40-bit length cipher offers a bare minimum protection for your confidentiality and privacy. Fortunately, the "work factor" increases exponentially as we increase the key length. For example, an increase of one bit in length doubles the key space, so 2^{41} represents key space of 2,199,023,255,552 possible combinations. A 2^{112} bit (128-bit) TDES cipher offers extremely strong security (5,192,296,858,534,827,628,530,496,329,220,096 possible combinations) that should resist known attacks for the next 15 to 20 years, considering the advance of semiconductor design and manufacturing.

Q: How secure is *X-Wall XO-64* (DES 64-bit strength)?

A: *X-Wall's* hardware-based encryption solution significantly reduces a hacker's successful entry into the hard drive. Every incorrect entry to the Cryptographic Key requires a hardware power cycle. To hack an *X-Wall LX-40* encrypted hard drive, one must process at least 500 billion times (50% of the available key space) reboots. As such, an *X-Wall* product using 64-bit encryption strength will be strong enough to withstand physical attack as well as sophisticated computer attacks.

Q: Has the Enova X-Wall XO product line been certified by government agencies?

A: Several times over. Enova's *XO* hardware DES/TDES cryptographic engines have been certified by ***NIST*** *(National Institute of Standards and Technology),* ***FIPS*** *(Federal Information Processing Standards) and* ***CSE*** *(The Communications Security Establishment).* These certificates are available on NIST web links: (http://csrc.nist.gov/cryptval/des/desval.html and http://csrc.nist.gov/cryptval/des/tripledesval.html).

These hardware algorithms are certified to provide reliable security. At full strength, it is virtually impossible to access the encrypted data by guessing or deriving the right DES/TDES Key. All data at rest on the hard drive is encrypted, which means that the data on that drive is safe even if attackers try to boot from their own disk, or to move your disk to an unprotected machine.

Q: Should I expect a lengthy login procedure and complex GUI that other systems require?

A: **No--not at all.** XO has been carefully designed not to change the user's regular computing behavior, nor does it require learning a complex GUI. Enova's objectives include building a secure product that will make the user's life a little more enjoyable. The User is not required to

memorize frequently used and cumbersome log on procedures. You need only to present your *Secure Key* token every time you power up your computer -- It is totally transparent to all users.

Q: Does the *Secure Key token provide authentication of the user?*

A: **Yes.** *X-Wall's Secure Key token contains a* ***Cryptographic Key***. This key is used by *X-Wall XO* to encrypt or decrypt data on the hard drive. Without this key, the hard drive **cannot** be booted or accessed. The *X-Wall Secure Key* token and *X-Wall XO* create an effective user authentication for access control, and strong encryption for data protection. The *X-Wall Secure Key token* serves as user authentication for access control, while the *X-Wall XO* encrypts and decrypts all data at rest on the hard drive.

Q: What happens if my *X-Wall Secure Key token* is lost or stolen?

A: There are no "backdoors" into *X-Wall XO* secure systems, so without the *X-Wall Secure Key* token you will not be able to access the data or operating system on the protected disk drive. This means you must keep the secure key token in a safe place at all times. Enova Technology has developed several key management systems that will allow the trace of lost keys. For the security conscious, you now have the ability to generate and maintain your own key distribution. For more information about how to manage the key token, please go to: **http://www.enovatech.com/key_management.htm**

Q: I'm an IT Director for a large enterprise. Instead of spending all my time worrying about security, can I create a 'Master' crypto key that has override capabilities on all my machines?

A: Absolutely! You have just created additional remote management capabilities for your network of PCs and Notebooks by adding another wall of security to your network -- that you control. For more specialized key management functionality and customization capabilities, please contact Enova directly.

Q: Can I order duplicate *X-Wall Secure Keys*?

A: Yes. You can order duplicate *X-Wall Secure Keys* from your reseller/distributor or directly from Enova Technology. Please visit our web site **http://www.enovatech.com/key_management.htm** or write to us **info@enovatech.com** for details. Note: Enova Technology does not maintain a database of *X-Wall Secure Keys* unless customers specifically require it. To have additional keys made, you must send your backup key with your order for duplication.

Q: Can I remove the *X-Wall Secure Key token* while my PC is on?

A: Yes. The Key token can be removed for safekeeping after your operating system has fully loaded. Remember that the *Secure Key* token **must** be used the next time you power up your PC or resume after the PC has been in hibernation.

Q: If the *X-Wall XO* malfunctions, will I lose my data?

A: **No.** The *XO* is a generic cryptographic engine and the *X-Wall Secure Key* token contains the DES/TDES cryptographic key. Consequently, you can simply replace the defective *X-Wall XO* component, if that ever occurs, and use your original *X-Wall Secure Key* token to access the data on your hard drive.

Q: What's the likelihood of an *X-Wall XO* malfunction?

A: Extremely unlikely. Every *X-Wall* family microchip is tested and complies with International quality assurance standards[1] prior to being shipped. Enova employs a zero tolerance policy for such

[1] Our quality assurance program including reliability tests are performed in accordance with MIL-STD-883E as the prime standard and with JEDEC-STD, where applicable. The JEDEC (Joint Electronic Device Engineering Council) Solid State Technology Association is the semiconductor engineering standardization body of the Electronic Industries Alliance (EIA), a trade association that represents all areas of the electronics industry.

errors. However, there may be occasions that a chip might malfunction after some period of time, or at some unique circumstances. This problem can be resolved by simply replacing the defective *XO* with the same microchip**.** A malfunctioning *XO* unit can easily be replaced, and the encrypted contents of the disk drive will be intact and accessible (as long as the original "Cryptographic Key" is intact).

The contents of the disk drive will not be lost as long as you retain the original *X-Wall Secure Key* token. Nevertheless, hard drive failures can occur, so it is good practice to always keep a backup of your important data, for which we do have a good solution on the back up device: Enova Secure USB2.0 to IDE. Please refer to http://www.enovatech.com/products/reference/usb2.0_ide.htm for details. In case of system failure, please double-check with your disk drive prior to reporting any malfunction of the *X-Wall*.

Q: Can I replace the Secure Key token with Passwords, Biometrics and/or Smartcard authentication?

A: **Yes!** Please contact your supplier for assistance, or contact Enova directly.

Q: Can I exchange the *X-Wall XO* encrypted files over the public Internet?

A: **Yes, but in an unencrypted state.** Enova's *X-Wall* system has specifically designed to protect **data at rest** (stored) on the hard drive in your PC. The DES/TDES cryptographic engine does not support the Public Key Infrastructure (PKI). Therefore, you will not be able to exchange *X-Walled* files over the internet. Data leaving the hard drive interface is not encrypted.

Q: Does *X-Wall XO* increase the original file size after encryption?

A: No. DES/TDES is an encryption algorithm that computes the original data with 64/128/192-bit cryptographic key length. Regardless of the size of the key, the size of data file after encryption remains unchanged.

Q: I am currently using the *X-Wall XO-64* (DES 64-bit strength). Can I upgrade the same disk drive to an *X-Wall XO-128* (TDES 128-bit strength) or more?

A: **Yes.** Follow these two essential steps:

1. You can order the *X-Wall XO-128 (or any strength other than XO-64) circuit* board from your supplier. The package you will receive will have a new *Secure Key token*.
2. Copy the content of your disk drive to a safe location, and then install the new *X-Wall XO-128* board and restore the data to the disk drive, using the new *Secure Key token*. This is necessary because the disk content will be lost due to re-performing of FDISK and FORMAT commands. Only one cipher strength can be used on the same disk drive.

