Enova® X-Wall® LX

Frequently Asked Questions

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

A: *X-Wall LX* is the **third** generation of **Enova real-time hard drive cryptographic gateway ASIC** (Application Specific Integrated Circuit) that encrypts and decrypts the entire hard drive including boot sector, temp files, swap files and the operating system without degrading system overall performance. Within the heart of the *X-Wall* family chips are the *NIST (National Institute of Standards and Technology)* of the United States of America and *CSE (Communications Security Establishment)* of Government of Canada certified *DES (Data Encryption Standard)*, *TDES (Triple DES)*, and AES (Advanced Encryption Standard) hardware cryptographic engine.

Q: What's the variety of "*X-Wall LX*"?

A: *X-Wall LX* is available now through four different microchips:
X-Wall LX-40 – DES 40-bit encryption strength
X-Wall LX-64 – DES 64-bit encryption strength
X-Wall LX-128 – TDES 128-bit encryption strength
X-Wall LX-192 – TDES 192-bit encryption strength

Q: How can *X-Wall LX* encrypt the entire disk without losing performance?

A: *X-Wall LX* is specifically engineered for high speed communications with the disk drive. It offers 1.6 Giga bit per second or higher throughput to enable real-time communications with all the IDE Ultra DMA compatible hard drives. The operations of encryption and decryption are accomplished using high speed hardware circuit to ensure no performance loss. There isn't any extra software device driver required to enable the *LX* thus memory and interrupt overheads are completely eliminated.

Q: Entire disk drive? Not just 10 or 20GB as seen on other products?

A: *X-Wall LX* encrypts every thing on your disk drive without exception. It encrypts the entire volume of your disk drive such that if you have a 300GB hard drive, the entire 300GB will be encrypted.

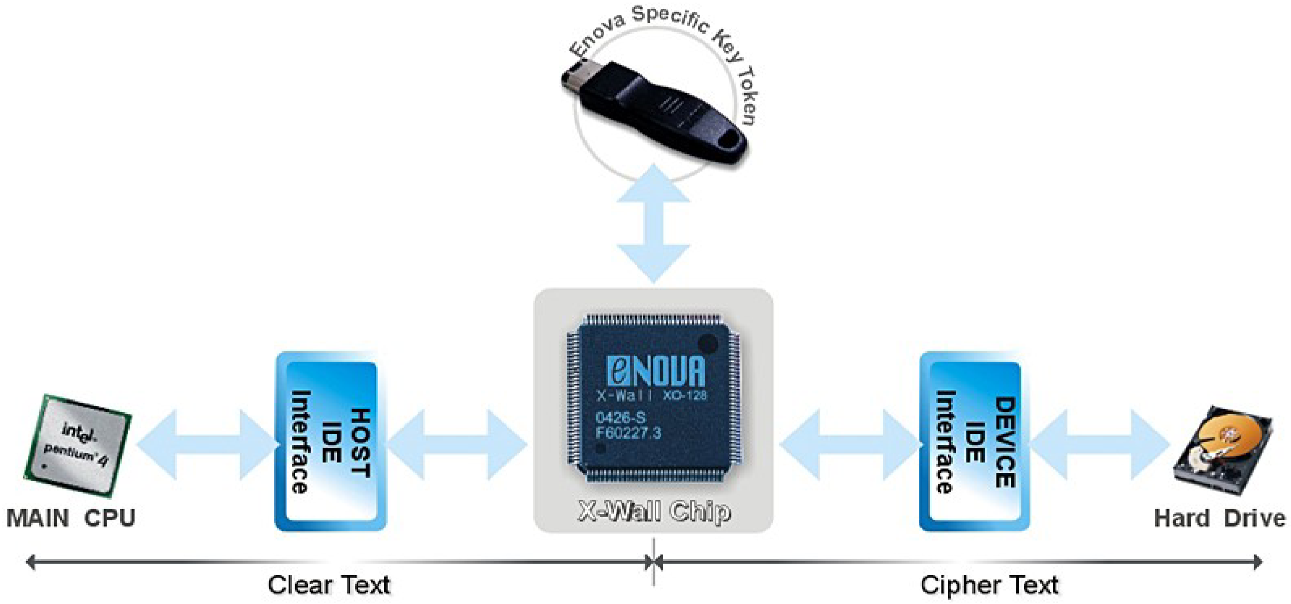
Q: Do I need to establish a separate "encrypted folder" under file directory as required by some software solutions?

A: No. Every thing you write to the disk drive is automatically strongly encrypted. There is no need to establish a separate "encrypted folder."

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

A: *X-Wall LX* sits before your IDE Ultra DMA disk drive. It intercepts, interprets, translates, and relays IDE commands & data to and from the disk drives, encrypting the data with DES/TDES strength. Before all data reach the disk drive, *LX* encrypts it then saves to disk drive. When there is a read to the disk drive, *LX* decrypts it before sending the data to the host. The operation of encryption and decryption is totally transparent to all users thus *LX* is invisible to the entire system. The Secure Key Token contains the ***"Cryptographic Key"*** that is to be used by the *LX* cryptographic engine. At power up, the "Cryptographic Key" will be delivered to the *LX* register sets using a proprietary hardware protocol. If somehow the Cryptographic Key was incorrect or missing, the *LX* will not decrypt the hard drive thus the *X-Walled* hard drive will only be seen as a brand new drive and the entire content is secure. It is also true even if the *X-Walled* hard drive has been moved to a different platform in an attempt to by pass the authentication process (Cryptographic Key verification process). Attempts to surface scan the entire disk drive platters will only prove futile.

As *LX* is a generic engine and it relies on the "Cryptographic Key" to enable all functionalities, a malfunctioned *LX* can be easily replaced with the same model and the content of your disk drive can be safely retrieved as long as your original "Cryptographic Key" is intact. The following illustration best describes how the *X-Wall* functions.



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

A: Yes. *X-Wall LX* can be operated with *Ultra ATA (Ultra DMA) 66/100/133* compliant disk drives with throughput of 1.6 Giga bit per second. *X-Wall LX* does not work with SCSI or fiber-channel drives.

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

A: Yes. The *X-Wall LX* requires no device drivers and is compatible with all operating systems. The only requirement is an Ultra ATA (Ultra DMA) compliant disk drive.

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

A: No. 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. There isn't any GUI for you to learn and manage and you don't have to memorize your password. Figure shown below is *X-Wall Secure Key*.

Q: How does *X-Wall LX* compare *w*ith Smart Card and PCMCIA encryption products?

A: *X-Wall LX* is dramatically faster than PCMCIA or Smart Card solutions, and encrypts the entire hard drive instead of just selected files. There is no possibility that any data or credentials can be left unprotected on the *X-Walled* hard drive. Drive locking and boot sector encryption solutions do not encrypt the data, and thus it is vulnerable to attack.

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

A: Maybe. As previously stated, the *LX* is engineered to encrypt one single hard drive. Multiple hard drives will require multiple *LXs.* However, in some **IDE to IDE RAID sub-systems**, one *LX* is able to drive the IDE to IDE RAID chip thus is able to encrypt all hard drives that are connected after the IDE to IDE RAID chip. In which case, one *LX* 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 chip. Please reference below question with regard to PCI IDE RAID subsystem applications.

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

A: Yes. *LX* 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 *LXs* sit right in front of all hard drives, encrypting all with real-time speed.

http://www.enovatech.net/products/reference/secureide_raid.htm

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

A: Yes. *X-Wall LX* supports 48-bit addressing and can control hard drive volume over than 137GB per drive.

Q: What is "DES/TDES"?

A: DES (Data Encryption Standard) was originally introduced by NSA (National Security Agency) and IBM and has since become a Federal data encryption standard as defined in FIPS 46-3 (Federal Information Processing Standard). 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 same Cryptographic Key is used for both encryption and decryption.

Q: How secure are DES and TDES?

A: Very secure as both algorithms are completely public, and have been surprisingly resistant to new cryptographic attacks over the last quarter century. Though software DES 56-bit key length is no longer proven against a massive computer attack, 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 eavesdropper 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: Such that *X-Wall LX-64* (DES 64-bit strength) is insecure?

A: Not true. Above explained key finding process is specifically relating to decrypting software-based encryption. The innovative *X-Wall* hardware based encryption solution increases the difficulties tremendously as every wrong guess of the Cryptographic Key requires a hardware reset (power on). To break 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, *X-Wall* even with its DES 40-bit strength will be strong enough against massive computer attacks.

Q: How would I make sure the security offered by *X-Wall LX* is solid?

A: The *LX* hardware DES/TDES cryptographic engine has been certified by the ***NIST*** *(National Institute of Standards and Technology) and* ***CSE*** *(The Communications Security Establishment)*, for which the certificates can be reviewed on NIST web links: http://csrc.nist.gov/cryptval/des/desval.html & http://csrc.nist.gov/cryptval/des/tripledesval.html. These hardware algorithms are certified to provide reliable security; at full strength it is nearly impossible to access the encrypted data by guessing or deriving the right DES/TDES Key. Because everything on the disk is encrypted, your data is safe even if attackers try to boot from their own disk, or to move your disk to an unprotected machine.

Q: Will I expect 19-step log on procedures & complex GUI (Graphical User's Interface) like other systems require?

A: No. LX does NOT change user's regular computing behavior, nor does it require learning a complex GUI. It does not require you to memorize frequently used and cumbersome log on procedures. It is totally transparent to all users. You need only to present your *Secure Key* token every time you power up your computer.

Q: Why do I need to use the *Secure Key token?*

A: The *X-Wall Secure Key token contains the* DES/TDES **"*Cryptographic Key*"** that is used by *X-Wall LX* to encrypt or decrypt data. Without the key, the *X-Wall*ed disk drive cannot be booted and there is no access into the PC. Together the *X-Wall Secure Key* token and *X-Wall LX* comprise an effective user authentication for access control and encryption for data protection. The *X-Wall Secure Key token* serves as user authentication for access control while *X-Wall LX* encrypts and decrypts.

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

A: **There are no "backdoors" into *X-Wall LX* 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 backup key in a safe place at all times. We at Enova Technology have developed several key management systems that will allow the trace of lost keys. However, if you are security conscious, you probably would like to have the ability to generate and maintain your own keys distribution. For more information about how to manage the key token, please visit below link:
http://www.enovatech.net/key_management.htm

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.net/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 it is specifically required by customers. 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, you can safely remove the *Secure Key token* for safekeeping after your operating system has fully loaded. Remember that the *Secure Key* token MUST be used again the next time you power up your computer or resume from the hibernation.

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

A: No. the *LX* 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 LX* component, if that ever occurs, and use your original *X-Wall Secure Key* token to access the data on your *X-Walled* hard drive.

Q: What's the likelihood an *X-Wall LX* malfunctions?

A: Very unlikely. Every *X-Wall* family microchip we ship is 100% tested and proven and complies with International quality assurance standards[1]. However, there may be occasions that chip malfunctions after some period of time, or at some unique circumstances. This problem can be resolved by simply replacing the defective *LX* with the same microchip. The contents of the disk drive will NOT be lost as long as you retain the original *X-Wall Secure Key* token intact. 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: Secure USB2.0 to IDE. Please refer to
http://www.enovatech.net/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 Password, Biometrics or Smartcard authentication?

A: Yes, it's possible. This will require system level design effort. You can ask your supplier to work with us to deliver the specific solution you desire to own.

Q: Can I exchange the *X-Wall LX* encrypted files using the public network?

[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.

A: No. the *X-Wall* system was specifically designed to protect **data-at-rest (DAR, stored)** on your PC. The DES/TDES cryptographic engine built inside the *LX* is a symmetric cipher, a **"*Secret Key*"** system that does NOT support the Public Key Infrastructure (PKI). Therefore, you will not be able to exchange *X-Walled* files through public network, as data leaving *X-Wall* interface is the clear text.

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

A: No. DES/TDES is a complicated mathematical 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 LX-40* (DES 40-bit strength). Can I upgrade the same disk drive to an *X-Wall LX-128* (TDES 128-bit strength) or more?

A: Yes, but with two essential steps:

1. You can order the *X-Wall LX-128 (or any strength other than LX-40) circuit* board from your supplier. The package you will receive will have different *Secure Key token*;
2. You must copy the content of your disk drive to a safe location, and then you can install the new *X-Wall LX-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.