

Frequently Asked Questions

General Product Questions

Q: What does SAFE PSD stand for?

A: Secure Access For Enterprises Personal Storage Device

Q: Why does Lexar offer multiple secure USB solutions?

A: Lexar JumpDrive® Secure II is designed for retail consumers, while SAFE PSD S1100 is specifically engineered for enterprise users who require enterprise – class security and central device management features.

Q: What is the difference between Lexar SAFE PSD S1100 and Lexar JumpDrive Secure II USB flash drive?

A: Three levels of security features distinguish the SAFE PSD S1100 from JumpDrive Secure II:

- Off-Line Defenses within the device include 256-bit AES encryption and tamper – evident housing
- PSD-Lock provides device-access control technology to manage device locking, passphrases, and dictionary defenses
- Enterprise Manageability Features enhance security using unique serial numbers and digital asset tags

These features offer enterprise protection at every level and are not typically required for a consumer-class product.

General Use Questions

Q: Where do I obtain the driver for SAFE PSD S1100?

A: A digitally signed and certified driver for Windows XP SP2 and Windows Vista x86 and x64 is available through Microsoft Windows Update. The driver can be automatically downloaded via the Found New Hardware wizard. See the SAFE PSD S1100 installation guide for details.

Q: How long can the passphrase be? How does it differ from a password?

A: A passphrase is a longer-and thus more secure-form of password. Lexar SAFE PSD S1100 supports passphrase lengths up to 40 bytes. The passphrase places no restrictions on spaces or special characters.

Data Security Questions

Q: How do the off-line defenses of SAFE PSD S1100 protect my data?

A: The encryption key, the firmware, and all other drive contents are ciphered with very strong algorithms to deter and deflect data attacks. The device's tamper-evident housing clearly shows if anyone has attempted to disassemble the drive to access the flash memory. Removal of the flash is possible, but the flash content is completely encrypted. Without knowledge of the encryption key, the NIST standard encryption algorithm is designed to withstand years of attacks.

Q: How does SAFE PSD S1100 behave if it comes under a password dictionary attack?

A: The device has built-in password dictionary attack defenses. SAFE PSD S1100 only allows a limited number of passphrase attempts per second. After several unsuccessful attempts in a row, the drive locks down and rejects all requests until it is unplugged from the USB port and reinserted. These simple security measures are virtually transparent to the user but provide a solid defense against automated password attacks.

Q: Are copies of the passphrase kept on the host machine?

A: No. By default, the encrypted passphrase is kept on the drive for added security. The SAFE PSD S1100 driver transfers the passphrase to the drive and does not store a copy on the host machine.

Data Security Questions – *continued*

Q: Are any copies of the encryption key kept on the host machine?

A: No, the encryption key is stored solely on the drive.

Q: What happens if I forget my passphrase? Do I have to throw away the drive?

A: The drive can be recovered and reset to factory defaults. Doing so erases all stored data and the old passphrase. A new passphrase must also be set. The erase operation permanently deletes all stored data so that it cannot be retrieved by anyone.

Q: Does SAFE PSD S1100 perform any operations that leave traces on the host machine if the drive is not ejected properly?

A: No. All operations are contained within the drive, so even if the drive is not ejected properly, no trace is left behind on the host machine.

Questions for IT Managers

Q: I'd like to manage SAFE PSD S1100 driver installations for my company to provide a seamless experience for employees. What method do you recommend?

A: The SAFE PSD S1100 driver can be distributed to multiple client computers via Microsoft Update Catalog. For details, see the Microsoft Update Catalog site (<http://catalog.update.microsoft.com/v7/site/home.aspx>).

Q: I want to implement a device – access control and policy enforcement solution. I'm considering pairing SAFE PSD S1100 with SecureWave Sanctuary® centrally managed, end-to-end software. What additional capabilities will this solution provide?

A: Lexar SAFE PSD S1100, in conjunction with SecureWave Sanctuary device control, will enable enterprises to set policies that discover, monitor, control, and audit device usage. Sanctuary policies can be paired with the SAFE PSD S1100 onboard AES encryption features to significantly reduce the risks of using removable mass storage devices within the enterprise.

Q: Does drive performance become diminished because all contents, including the passphrase, data, and firmware, are encrypted?

A: No, the hardware-based 256-bit AES engine performs the encryption on-the-fly and does not impact performance.

Q: Does SAFE PSD S1100 use "spoofing" (i.e. enumerate itself as a removable drive and a CD-ROM) to enable Autorun and launch its passphrase software?

A: No, the device does not represent itself in Windows as a removable drive and CD-ROM. This sort of spoofing is a questionable workaround that takes advantage of a Windows XP defect that is likely to be fixed in Vista. Lexar SAFE PSD S1100 requires a digitally signed driver, which is available via Windows Update.

For additional product information not addressed in this document, please visit www.lexar.com/enterprise.

Note: Security safeguards, by their nature, are capable of circumvention. While the SAFE PSD is designed to offer enterprise-class security, Lexar cannot guarantee data will be 100% secure from unauthorized access, alteration or destruction.