

## Frequently Asked Questions

*-Internal use*

Note: This document assumes the client application of Cryptainer SE is installed on a PC with Windows XP SP2.

**Q: What does UC Merced IT recommend for file/folder data protection?**

*UC Merced Information Technology (UCMIT) recommends a strong level of data protection for those individuals who carry any sensitive data. There are a couple of ways to do this.*

- *Folder and Files are stored on a Server that is protected with enhanced*
  - *Firewall*
  - *Anti-Virus*
  - *Protected VLAN*
  - *Daily Snapshots*
  - *Backup and Recovery*
  - *And more*
- *Folder and Files are stored on a Local PC that is protected with enhanced security*
  - *Cryptainer SE*
  - *Firewall*
  - *Anti-Virus*

*UCMIT recommends that client PCs store sensitive data on protected Server storage space. However, there are cases where this is not possible. At UC Merced, we have a large number of mobile-laptop users that require the need for data to be made easily accessible from their local system. Cryptainer SE will empower the user to store their sensitive data locally onto the PC with its very strong encryption software.*

**Q: How safe is Cryptainer SE for protecting my data?**

*"We use strong encryption algorithms that are statistically uncrackable: the mean time to break Cypherix™'s encryption is estimated at 10<sup>32</sup> years - in comparison, the estimated age of the Universe is 10<sup>18</sup> years."*

*-Cypherix™*

**Q: How do I obtain a copy of Cryptainer SE?**

*Call the IT Help Desk so that a Work Order may be generated and assigned to the Software Acquisition Coordinator. The WO will have a standard priority flag. The WO will then be assigned to a User Services Technician for software installation.*

Software Coordinator: Gabe Edwards ([software@ucmerced.edu](mailto:software@ucmerced.edu))

**Q: How much does a single copy of Cryptainer SE cost?**

*The first real price break is at 20 licenses for \$39.99 each. Below is additional pricing information.*

*1-3 licenses = \$50 ea.*

*4-5 licenses = \$60 ea.*

*6-10 licenses = \$50 ea.*

*11-20 licenses = \$40 ea.*

*21-25 licenses = \$40 ea.*

*25-50 licenses = \$40 ea. (etc)*

**Q: Why should I pay for Cryptainer SE when I can download Cryptainer LE/PE for free?**

*UC Merced IT has selected Cryptainer SE as the recommended application for file/folder data protection with key escrow benefits (as opposed to LE or PE versions).*

**Q: What are those benefits?**

*Cryptainer SE is a clone of Cryptainer LE/PE except it allows for password recovery. This is targeted at Corporate Users.*

*Cryptainer SE has an integrated administrative module. This module logs user passwords in an encrypted log file. This feature is useful in corporate environments where sometimes there is a necessity to recover the password/phrase which may have been lost/forgotten or other contingencies. The end-user interface is identical to that of Cryptainer.*

*Cryptainer SE is useful in resolving issues listed under*

- *Access Control*
- *Command Line Feature (DOS)*
- *Information Security*
- *Minimizing Downtime*
- *Cost Effectiveness*
- *Familiar Windows Environment*
- *No Training*
- *Ease of Deployment and Installation*
- *No Monitoring*
- *Zero maintenance*

*Note: For details on these special features see Section A.*

**Q: What are the differences between Cryptainer SE and LE/PE?**

*The difference is only in the size of volumes allowed (Cryptainer PE allows for multiple 25GB volumes, while Cryptainer 6.0/SE allow for multiple 250GB volumes.*

**Q: What steps should be taken if the computer's hard drive fails?**

*Call the IT Help Desk so that a Work Order may be generated and assigned to a User Services Technician. The WO will have an emergency priority flag. Technician response time will be 30 minutes - 1 hour.*

*Emergency contact: Jose Magana.*

Tech notes: In the event of a hard drive failure, it is imperative to recover the Cryptainer data file to regain access to the encrypted data. The name of this file is **cxid1705** and **admin.crptlog**—the location is **c:\windows\system32**. Once that file has been recovered, the data can be transferred to another computer that has the Cryptainer client installed—the encrypted files can then be accessed.

**Important:** This will only work if the Cryptainer client on the new computer was installed, using the same install files as the client on the old computer. If the password is lost/forgotten, the file **admin.crptlog** must be retrieved and copied to Mongoose, where password recovery can take place.

## **Section A. Special Features**

Cryptainer SE features as an integrated administrative module for **password recovery**. This module logs user passwords in an encrypted log file. This feature is useful in corporate environments where sometimes there is a necessity to recover the password/phrase which may have been lost/forgotten or other contingencies.

Cryptainer SE creates an encrypted volume file that is, when mounted, visible under window as a drive on access with a password. On dismounting, the data is encrypted. To contrast, copying encrypted files to any other file system type (FAT, FAT32, earlier versions of NTFS) using the Windows EFS will save the file in decrypted form. Cryptainer Files remain encrypted and there is no way that the contents are visible.

Cryptainer SE offers **command line** processing for encrypting and decrypting files at the dos prompt. You can group a series of encryption and decryption

commands in a single or multiple batch files and run it to get the desired results.

Cryptainer SE command line enables organizations to integrate encryption into batch processes to ensure the security of corporate data at rest or in transit. You can use it to encrypt or decrypt any file, using simple syntax.

The Cryptainer SE Command Line lets you use encryption from batch files, scripts, and other situations when you have a specific task and would prefer to accomplish the process automatically and quickly, without using the usual Cryptainer graphical user interface.

Cryptainer SE works with all 32 bit versions of Microsoft Windows (Win 95/98/NT/2000/XP). It encrypts on all file systems such as FAT, FAT12, FAT32, NTFS or NTFS with EFS.

Cryptainer SE provides you with single point control and monitoring of the distributed security system, while retaining the privacy of end users who set their own passwords. This ensures the integrity of your data and at the same time gives you flexibility and overall control. Cryptainer SE allows the end users to act independently. To illustrate, users can set any type of password as they please. They can even create as many volumes as they need without any "monitoring". In such a case, the data can be accessed by the administrator(s) without any intervention of any kind by Cypherix or any back doors of any kind.

The administrative module also allows physical recovery of data sector by sector in an event of an absolute disaster.