



Radix kSafe Encrypted Virtual Drives

Radix kSafe is an easy-to-use personal encryption system, enabling professional and novice users to effectively protect their data.

By using an advanced encryption algorithm (AES 256) and Virtual Drive technology, kSafe prevents unauthorized access to data stored in local and external hard disk drives, as well as on portable storage devices such as flash disks (Disk-On-Key).



Why do you need it?

Laptop computers and portable flash disks are easy targets for thieves and business data spies, especially when left unguarded at hotel rooms, airport security checkpoints, at home, or in a car. With Radix kSafe installed, no one can access your data even if your computer or flash-disk falls into the wrong hands.

How does it work?

Radix kSafe converts pre-determined disk sectors into encrypted files (a 'virtual safe'). Opening a safe or using the files stored in it, is only possible by plugging in a personal coded USB key ("what you have") and/or typing a secret password ("what you know"). Unplugging the USB key, instantly and automatically locks all open virtual safes and hides the encrypted virtual safe files.

Radix

Working with Radix kSafe

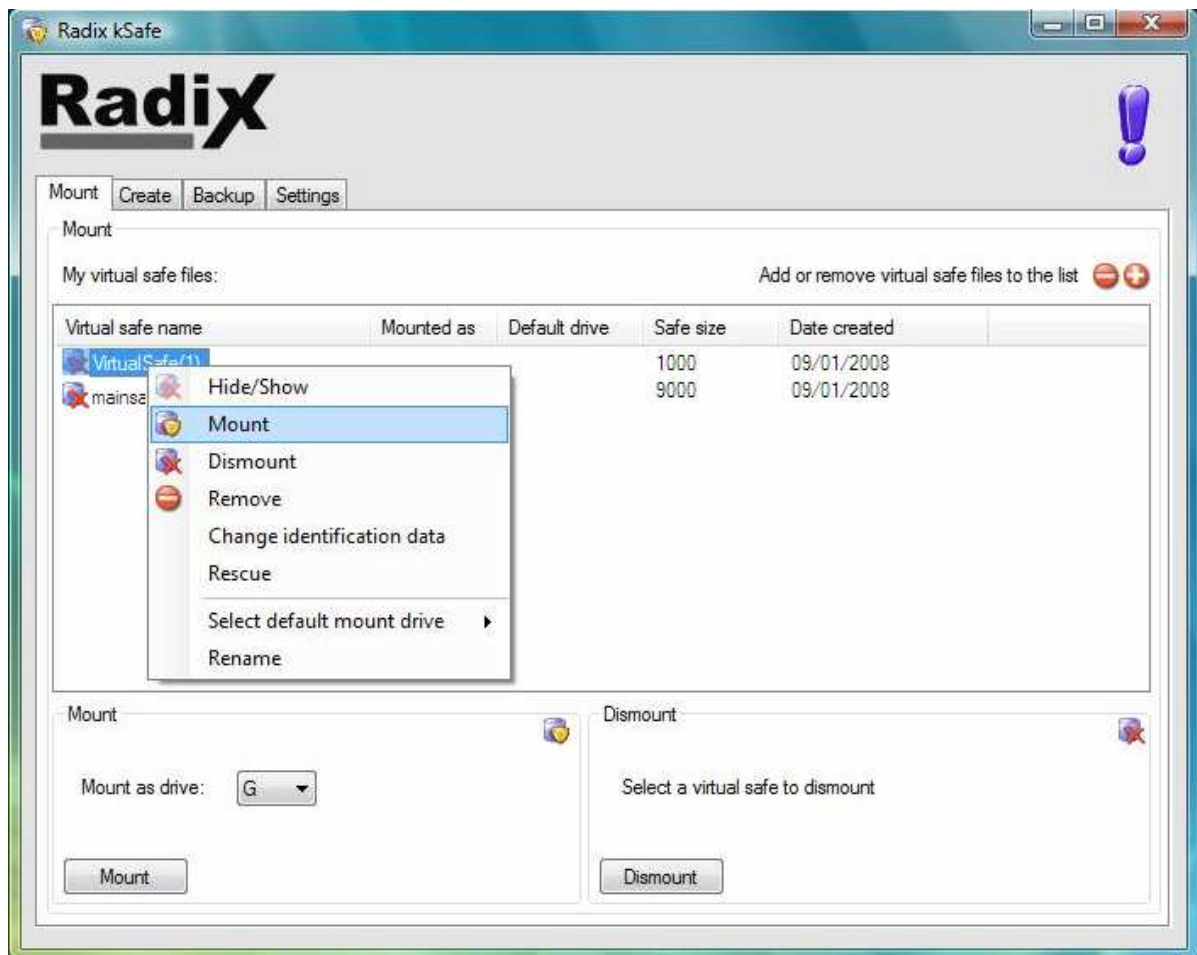
Working with kSafe is similar to working with a regular flash disk (Disk-On-Key).

By plugging in a USB key or alternately hitting a pre-programmed string – the user mounts a virtual drive (open the safe) and can work with it like a regular drive. Unplugging the key, or clicking on an icon, instantly dismounts the virtual drives (lock the safe).

Files stored in a virtual safe are constantly encrypted, even when the safe is open. New files are automatically encrypted 'on-the-fly' when stored in the safe.

User can create unlimited number of safe files, and open and work with up to 20 safes simultaneously.

Virtual safe files are regular files and can be securely stored, saved, backed up, attached to an e-mail message, and are fully compatible with Radix Reload's instant recovery system.

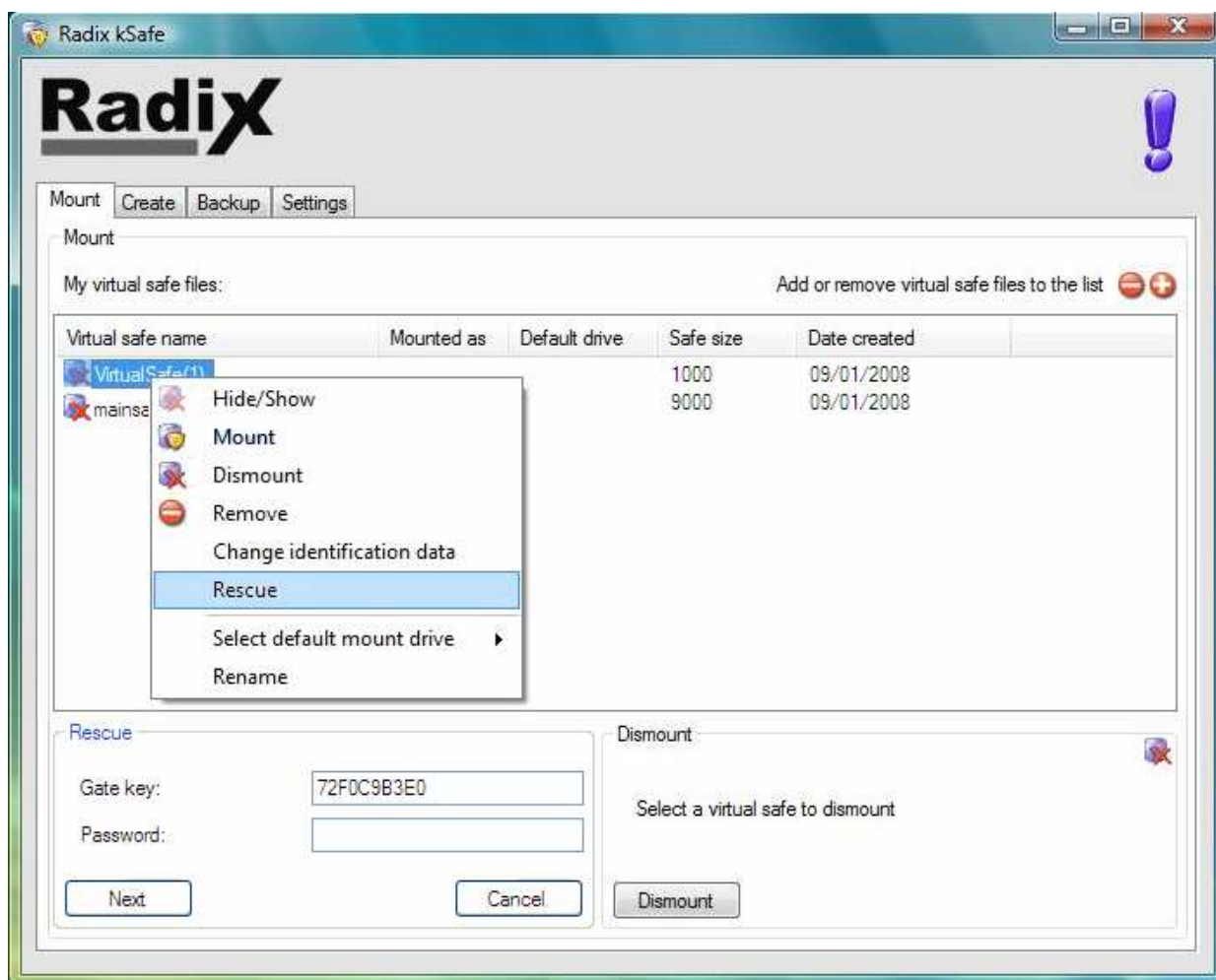


Radix

Lost key recovery

For extra protection, Radix kSafe system does not include 'back doors'. Opening a virtual safe in case of a lost key or forgotten password requires using two keys simultaneously:

- **Backup Key** – backup password (saved by the user during safe creation)
- **Gate Key** – a one-time code received from the help desk center after user's authorization verification process





Advantages over full HDD encryption solutions

Radix kSafe	Full HDD Encryption
Decrypts only the safe in use. All other safes are locked and secured at all times.	Decrypts prior to <u>any</u> operation. Protected data is exposed even when working in an unsecured environment.
Encrypts important data only, without consuming valuable PC resources and without affecting PC performance. Security officer can set the kSafe to force users to store data only within a safe.	Encrypts insignificant applications and non confidential data. Adds a considerable load on PC resources, decreasing performance and increasing PC vulnerability.
Encrypts no system files. Failure in the encryption system, (such as a lost encryption key) does not affect other applications.	Encrypts system files. In case of any failure in the encryption system, the computer is completely disabled.
Random safe formats leave no leads to hackers. Even if one safe has been cracked, all other safes are secured.	Fixed encryption format, makes an easier job for hackers who can compare the (standard) boot sector of the encrypted HDD with non encrypted HDD.
Integrates perfectly with any other applications.	Conflicts with other applications, such as HDD cloning, multi-boot systems and instant recovery software.
Easy implementation and deployment by cloning and distributing the master HDD.	Custom installation for each computer. Makes deployment and implementation processes longer and more complicated.



“Radix proves simple ideas can often be the best” (PC Pro UK)



Features & Specifications

Virtual Safe

- Compatible with Windows Xp, 2000, 2003, Vista
- Create multiple virtual safes within local, external, portable and flash disks
- Store, backup, copy and e-mail virtual safe files as regular files
- Mount up to 20 virtual safes simultaneously
- Auto mount default virtual safe at startup, on a USB key plug-in, or on a pre-set string
- Auto dismounts all safes on key plug-out, on log-out, or after preset time interval
- Unlimited capacity per virtual safe (NTFS); 4GB per virtual safe (FAT)

Encryption

- AES 256bit encryption algorithm
- 64-bit password and/or USB encryption key
- Encrypt data stored in a virtual safe - on-the-fly
- By virtual safe rescue key (users backup password)
- By USB key rescue password (by help desk)

Aladdin eToken (optional)

- Onboard symmetric DES-X challenge-response authentication
- Secure and encrypted EEPROM memory chip
- Standard Crypto API connectivity
- Secured storage of users' private credentials and PKI keys
- Hardened tamper-evident and water-resistant shell
- Compatible implementation with smart cards
- Protected serial ID chip (32-bits length)
- API Support PKCS#11 V2.01, CAPI, PC/CS, X.509 V3, SSL V3, IPSec/IKE
- Compliant with CE, FCC, RoSH

Radix - Your First and Last Lines of Defence!