



Q: Is there a "Quick Start Guide" or some tutorial for beginners?

A: Yes. The first chapter, **Beginner's Tutorial**, in the [GuardShip User Guide](#) contains screenshots and step-by-step instructions on how to create, mount, and use a GuardShip volume.

Q: Can GuardShip encrypt a partition/drive where Windows is installed?

A: Yes, see the chapter [System Encryption](#) in the [GuardShip User Guide](#).

Q: I forgot my password – is there any way to recover the files from my GuardShip volume?

A: GuardShip does not contain any mechanism or facility that would allow partial or complete recovery of your encrypted data without knowing the correct password or the key used to encrypt the data. The only way to recover your files is to try to "crack" the password or the key, but it could take thousands or millions of years depending on the length and quality of the password/keyfiles, on software/hardware efficiency, and other factors.

Q: Can I directly play a video (.avi, .mpg, etc.) stored on a GuardShip volume?

A: Yes, GuardShip-encrypted volumes are like normal disks. You provide the correct password (and/or keyfile) and mount (open) the GuardShip volume. When you double click the icon of the video file, the operating system launches the application associated with the file type – typically a media player. The media player then begins loading a small initial portion of the video file from the GuardShip-encrypted volume to RAM (memory) in order to play it. While the portion is being loaded, GuardShip is automatically decrypting it (in RAM). The decrypted portion of the video (stored in RAM) is then played by the media player. While this portion is being played, the media player begins loading next small portion of the video file from the GuardShip-encrypted volume to RAM (memory) and the process repeats.

The same goes for video recording: Before a chunk of a video file is written to a GuardShip volume, GuardShip encrypts it in RAM and then writes it to the disk. This process is called on-the-fly encryption/decryption and it works for all file types, not only for video files.

Q: Will GuardShip be open-source and free forever?

A: Yes, it will. We will never create a commercial version of GuardShip, as we believe in open-source and free security software.

Q: Is it possible to donate to the GuardShip project?

A: Yes. For more information, please visit <http://www.GuardShip.org/donations/>

Marcus Ltd, 62 Bagley Lane Farsley Leeds LS28 5LY
tel: 0113 236 2626 fax: 0113 236 2828

email: sales@tomorrows-office.co.uk web: www.tomorrows-office.co.uk

VAT: 372 0159 72 Co. reg: 1649844

Q: Does GuardShip also encrypt file names and folder names?

A: Yes. The entire file system within a GuardShip volume is encrypted (including file names, folder names, and contents of every file). This applies to both types of GuardShip volumes – i.e., to file containers (virtual GuardShip disks) and to GuardShip-encrypted partitions/devices.

Q: How can I use GuardShip on a USB flash drive?

A: You have two options:

1. Encrypt the entire USB flash drive. However, you will not be able run GuardShip from the USB flash drive.
Note: Windows does not support multiple partitions on USB flash drives.
2. Create a GuardShip file container on the USB flash drive (for information on how to do so, see the chapter [Beginner's Tutorial](#), in the [GuardShip User Guide](#)). If you leave enough space on the USB flash drive (choose an appropriate size for the GuardShip container), you will also be able to store GuardShip on the USB flash drive (along with the container – not *in* the container) and you will be able to run GuardShip from the USB flash drive (see also the chapter [Traveler Mode](#) in the [GuardShip User Guide](#)).

Q: Is it possible to install an application to a GuardShip volume and run it from there?

A: Yes.

Q: Is it possible to boot Windows installed in a hidden GuardShip volume?

A: Yes, it is (as of GuardShip 6.0). For more information, please see the section [Hidden Operating System](#) in the [documentation](#).

Q: Will I be able to mount my GuardShip volume (container) on any computer?

A: Yes, virtual [GuardShip volumes](#) (in contrast to [GuardShip-encrypted physical system partitions/drives](#)) are independent of the operating system. You will be able to mount your GuardShip volume on any computer on which you can run GuardShip (see also the question "[Can I use GuardShip on Windows if I do not have administrator privileges?](#)").

Q: Can I unplug or turn off a hot-plug device (for example, a USB flash drive or USB hard drive) when there is a mounted GuardShip volume on it?

A: Before you unplug or turn off the device, you should always dismount the GuardShip volume in GuardShip first, and then perform the '*Eject*' operation if available (right-click the device in the '*Computer*' or '*My Computer*' list), or use the '*Safely Remove Hardware*' function (built in Windows, accessible via the taskbar notification area). Otherwise, data loss may occur.

Q: What is a hidden operating system?

See the section [Hidden Operating System](#) in the [documentation](#).

Q: Will I be able to mount my GuardShip partition/container after I reinstall or upgrade the operating system?

A: Yes, [GuardShip volumes](#) are independent of the operating system. However, you need to make sure your operating system installer does not format the partition where your GuardShip volume resides.

Note: If the system partition/drive is encrypted and you want to reinstall or upgrade Windows, you need to decrypt it first (select *System > Permanently Decrypt System Partition/Drive*).

Q: Can I upgrade from an older version of GuardShip to the latest version without any problems?

A: Generally, yes. However, before upgrading, please read the [release notes](#) for all versions of GuardShip that have been released since your version was released. If there are any known issues or incompatibilities related to upgrading from your version to a newer one, they will be listed in the [release notes](#).

Q: Can I upgrade GuardShip if the system partition/drive is encrypted or do I have to decrypt it first?

A: Yes, generally, you can upgrade to the latest version without decrypting the system partition/drive (just run the GuardShip installer and it will automatically upgrade GuardShip on the system). However, before upgrading, please read the [release notes](#) for all versions of GuardShip that have been released since your version was released. If there are any known issues or incompatibilities related to upgrading from your version to a newer one, they will be listed in the [release notes](#). Note: You cannot *downgrade* GuardShip if the system partition/drive is encrypted.

Q: I use pre-boot authentication. Can I prevent a person (adversary) that is watching me start my computer from knowing that I use GuardShip?

A: Yes (as of GuardShip 6.1). To do so, boot the encrypted system, start GuardShip, select *Settings > System Encryption*, enable the option '*Do not show any texts in the pre-boot authentication screen*' and click *OK*. Then, when you start the computer, no texts will be displayed by the GuardShip boot loader (not even when you enter the wrong password). The computer will appear to be "frozen" while you can type your password. It is, however, important to note that if the adversary can analyze the content of the hard drive, he can still find out that it contains the GuardShip boot loader.

Q: I use pre-boot authentication. Can I configure the GuardShip Boot Loader to display only a fake error message?

A: Yes (as of GuardShip 6.1). To do so, boot the encrypted system, start GuardShip, select *Settings > System Encryption*, enable the option '*Do not show any texts in the pre-boot authentication screen*' and enter the fake error message in the corresponding field (for example, the "*Missing operating system*" message, which is normally displayed by the Windows boot loader if it finds no Windows boot partition). It is, however, important to note that if the adversary can analyze the content of the hard drive, he can still find out that it contains the GuardShip boot loader.

Q: How do I mount a hidden volume?

A: A hidden volume can be mounted the same way as a standard GuardShip volume: Click *Select File* or *Select Device* to select the outer/host volume (important: make sure the volume is *not* mounted). Then click *Mount*, and enter the password for the hidden volume. Whether the hidden or the outer volume will be mounted is determined by the entered password (i.e., when you enter the password for the outer volume, then the outer volume will be mounted; when you enter the password for the hidden volume, the hidden volume will be mounted).

Note: GuardShip first attempts to decrypt the standard volume header using the entered password. If it fails, it loads the area of the volume where a hidden volume header can be stored (i.e. the bytes 65536–131071, which contain solely random data when there is no hidden volume within the volume) to RAM and attempts to decrypt it using the entered password. Note that hidden volume headers cannot be identified, as they appear to consist entirely of random data. If the header is successfully decrypted (for information on how GuardShip determines that it was successfully decrypted, see the section [Encryption Scheme](#) in the [documentation](#)), the information about the size of the hidden volume is retrieved from the decrypted header (which is still stored in RAM), and the hidden volume is mounted (its size also determines its offset).

Further information may be found in the section [Hidden Volume](#) in the [documentation](#).

Q: Can I save data to the decoy system partition without risking damage to the hidden system partition?

A: Yes. You can write data to the decoy system partition anytime without any risk that the hidden volume will get damaged (because the decoy system is *not* installed within the same partition as the hidden system). For more information, see the section [Hidden Operating System](#) in the [documentation](#).

Q: Can I use GuardShip on Windows if I do not have administrator privileges?

See the chapter '[Using GuardShip Without Administrator Privileges](#)' in the [documentation](#).

Q: Does GuardShip save my password to a disk?

A: No.

Q: Is some hash of my password stored somewhere?

A: No.

Q: How does GuardShip verify that the correct password was entered?

See the section [Encryption Scheme](#) (chapter [Technical Details](#)) in the [documentation](#).

Q: Does GuardShip support hardware/software RAID and Windows dynamic volumes?

A: Yes. However, if you use Windows XP/2000/2003, please read the following notes on dynamic volumes (the notes do not apply to Windows Vista and later). If you intend to format a Windows dynamic volume as a GuardShip volume, keep in mind that after you create the Windows dynamic volume (using the *Windows Disk Management* tool), you must restart the operating system in order for the volume to be available/displayed in the 'Select Device' dialog window of the GuardShip Volume Creation Wizard. Also note that, in the 'Select Device' dialog window, a Windows dynamic volume is not displayed as a single device (item). Instead, all volumes that the Windows dynamic volume consists of are displayed and you can select *any* of them in order to format the *entire* Windows dynamic volume.

Q: Is it possible to mount a GuardShip container that is stored on a CD or DVD?

A: Yes. However, if you need to mount a GuardShip volume that is stored on a read-only medium (such as a CD or DVD) under Windows 2000, the file system within the GuardShip volume must be FAT (Windows 2000 cannot mount an NTFS file system on read-only media).

Q: What is the maximum possible size of a GuardShip volume?

A: The maximum possible size of a GuardShip volume is 8589934592 GB. However, due to security reasons, the maximum allowed volume size is 1 PB (1,048,576 GB), as the amount of data that is considered secure to be encrypted using a single key depends, among other factors, on the block size of the encryption algorithm. In addition, you need to take into account other limiting factors. For instance, file system constraints, limitations of the hardware connection standard and of the operating system, etc.

Q: Can I run GuardShip if I don't install it?

A: Yes, see the chapter [Traveler Mode](#) in the [GuardShip User Guide](#).

Q: Why does Windows Vista ask me for permission to run GuardShip every time I run it in 'traveler' mode?

A: When you run GuardShip in traveler mode, GuardShip needs to load and start the GuardShip device driver. GuardShip needs a device driver to provide transparent on-the-fly encryption/decryption, and users without administrator privileges cannot start device drivers in Windows. Therefore, Windows Vista asks you for permission to run GuardShip with administrator privileges.

Note that if you install GuardShip on the system (as opposed to running GuardShip in traveler mode), you will *not* be asked for permission every time you run GuardShip.

Q: Do I have to dismount GuardShip volumes before shutting down or restarting Windows?

A: No. GuardShip automatically dismounts all mounted GuardShip volumes on system shutdown/restart.

Q: Which type of GuardShip volume is better – partition or file container?

A: [File containers](#) are normal files so you can work with them as with any normal files (file containers can be, for example, moved, renamed, and deleted the same way as normal files). [Partitions/drives](#) may be better as regards performance. Note that reading and writing to/from a file container may take significantly longer when the container is heavily fragmented. To solve this problem, defragment the file system in which the container is stored (when the GuardShip volume is dismounted).

Q: What's the recommended way to backup a GuardShip volume?

See the chapter [How to Back Up Securely](#) in the [documentation](#).

Q: What will happen if I format a GuardShip partition?

See the question "[Is it possible to change the file system of an encrypted volume?](#)"

Q: Is it possible to change the file system of an encrypted volume?

A: Yes, when mounted, GuardShip volumes can be formatted as FAT12, FAT16, FAT32, NTFS, or any other file system. GuardShip volumes behave as standard disk devices so you can right-click the device icon (for example in the '*Computer*' or '*My Computer*' list) and select '*Format*'. The actual volume contents will be lost. However, the whole volume will remain encrypted. If you format a GuardShip-encrypted partition when the GuardShip volume that the partition hosts is not mounted, then the volume will be destroyed, and the partition will not be encrypted anymore (it will be empty).

Q: Can I configure GuardShip to start, prompt me for password(s), and mount my volume(s) automatically whenever Windows starts?

A: Yes. To do so, follow these steps:

1. Mount the volume(s) and then select '*Volumes*' -> '*Save Currently Mounted Volumes as Favorite*'.
2. Select '*Settings*' -> '*Preferences*'. In the '*Preferences*' window in the section '*Actions to perform upon log on to Windows*', enable the option '*Mount favorite volumes*'.
3. In the '*Preferences*' window, click '*OK*'.

Alternatively, if the volume(s) is/are partition/device-hosted and if you do not need to mount it/them to particular drive letter(s) every time, you may skip step 1 and in the '*Preferences*' window in the section '*Actions to perform upon log on to Windows*' enable the option '*Mount all devices-hosted GuardShip volumes*' (instead of '*Mount favorite volumes*').

Q: Is it possible to change the password for a hidden volume?

A: Yes, the password change dialog works both for standard and [hidden volumes](#). Just type the password for the hidden volume in the 'Current Password' field of the 'Volume Password Change' dialog.

Remark: GuardShip first attempts to decrypt the standard [volume header](#) and if it fails, it attempts to decrypt the area within the volume where the hidden volume header may be stored (if there is a hidden volume within). In case it is successful, the password change applies to the hidden volume. (Both attempts use the password typed in the 'Current Password' field.)

Q: When I use HMAC-RIPEMD-160, is the size of the header encryption key only 160 bits?

A: No, GuardShip never uses an output of a hash function (nor of a HMAC algorithm) directly as an encryption key. See the section [Header Key Derivation, Salt, and Iteration Count](#) in the [documentation](#) for more information.

Q: Can I change the header key derivation algorithm (for example, from HMAC-RIPEMD-160 to HMAC-SHA-512) without losing data stored on the volume?

A: Yes. To do so, select *Volumes* -> *Set Header Key Derivation Algorithm*.

Q: How do I burn a GuardShip container larger than 2 GB onto a DVD?

A: The DVD burning software you use should allow you to select the format of the DVD. If it does, select the UDF format (ISO format does not support files larger than 2 GB).

Q: The Windows file selector remembers the path of the last container I mount or the path of the last selected keyfile. Is there a way to prevent this?

A: Yes, there is. If you have not done so yet, upgrade to GuardShip 4.2a or later. Run GuardShip and make sure the option '*Never save history*' in the [main window](#) is enabled. If you do not want to enable the option '*Never save history*', you can avoid using the Windows file selector by dragging the icon of the container onto the '*GuardShip.exe*' icon (GuardShip will be automatically launched then), or dragging it onto the GuardShip program window. Likewise, a keyfile can be selected by dragging its icon onto the *Keyfiles* window or onto the password entry window.

Q: Can I encrypt a partition/drive without losing the data currently stored on it?

A: Yes, but the following conditions must be met: If you want to encrypt an entire system drive (which may contain multiple partitions) or a system partition (in other words, if you want to encrypt a drive or partition where Windows is installed) you can do so provided that you use GuardShip 5.0 or later and that you use Windows XP or a later version of Windows (such as Windows Vista). If you want to encrypt a non-system partition in place, you can do so provided that it contains an NTFS filesystem, that you use GuardShip 6.1 or later, and that you use Windows Vista or a later version of Windows (such as Windows 2008).

Q: Can I use tools like *chkdsk*, Disk Defragmenter, etc. on the contents of a mounted GuardShip volume?

A: Yes, GuardShip volumes behave like real physical disk devices, so it is possible to use any filesystem checking/repairing/defragmenting tools on the contents of a mounted GuardShip volume.

Q: Is it possible to use GuardShip without leaving any 'traces' on unencrypted Windows?

A: Yes. This can be achieved by running GuardShip in [traveler mode](#) under [BartPE](#). BartPE stands for "Bart's Preinstalled Environment", which is essentially the Windows operating system prepared in a way that it can be entirely stored on and booted from a CD/DVD (registry, temporary files, etc., are stored in RAM – hard drive is not used at all and does not even have to be present). The freeware [Bart's PE Builder](#) can transform a Windows XP installation CD into BartPE. As of GuardShip 3.1, you do not need any GuardShip plug-in for BartPE. Just boot BartPE, download the GuardShip self-extracting package to the RAM disk (which BartPE creates), run it, extract its content to the RAM disk, and then run the file 'GuardShip.exe' from the RAM disk.

Note: You may also want to consider creating a hidden operating system (for more information, see the section [Hidden Operating System](#) in the [documentation](#)).

Q: Can I mount a GuardShip volume stored in another GuardShip volume?

A: Yes, GuardShip volumes can be nested without any limitation.

Q: Can I run GuardShip with another on-the-fly disk encryption tool on one system?

A: We are not aware of any on-the-fly encryption tool that would cause problems when run with GuardShip, or vice versa.

Q: Does GuardShip support Windows Vista?

A: Yes.

Note: Full support for Windows Vista was introduced in version 4.3. Therefore, we strongly recommend that you do not run GuardShip 4.2a or earlier versions under Windows Vista (those versions were not designed to run on Windows Vista).

Q: Does GuardShip support Windows Vista x64 (64-bit) Edition?

A: Yes. Note: All .sys and .exe files of GuardShip are digitally signed with the digital certificate of the GuardShip Foundation, which was issued by the certification authority GlobalSign.

Q: Does GuardShip run on Mac OS X?

A: Yes.

Q: Does GuardShip run on Linux?

A: Yes.

Q: Can I mount my GuardShip volume under Windows, Mac OS X, and Linux?

A: Yes, GuardShip volumes are fully cross-platform.

Q: Is there a list of all operating systems that GuardShip supports?

A: Yes, see the chapter [Supported Operating Systems](#) in the [GuardShip User Guide](#).

Q: What will happen when a part of a GuardShip volume becomes corrupted?

A: In encrypted data, one corrupted bit usually corrupts the whole ciphertext block in which it occurred. The ciphertext block size used by GuardShip is 16 bytes (i.e., 128 bits). The [mode of operation](#) used by GuardShip ensures that if data corruption occurs within a block, the remaining blocks are not affected. See also the question '*What do I do when the encrypted filesystem on my GuardShip volume is corrupted?*'

Q: What do I do when the encrypted filesystem on my GuardShip volume is corrupted?

A: File system within a GuardShip volume may become corrupted in the same way as any normal unencrypted file system. When that happens, you can use filesystem repair tools supplied with your operating system to fix it. In Windows, it is the '*chkdsk*' tool. GuardShip provides an easy way to use this tool on a GuardShip volume: First, make a backup copy of the GuardShip volume (because the '*chkdsk*' tool might damage the filesystem even more) and then mount it. Right-click the mounted volume in the main GuardShip window (in the drive list) and from the context menu select '*Repair Filesystem*'.

Q: We use GuardShip in a corporate/enterprise environment. Is there a way for an administrator to reset a volume password or pre-boot authentication password when a user forgets it (or loses a keyfile)?

A: Yes. Note that there is no "back door" implemented in GuardShip. However, there is a way to "reset" volume passwords/[keyfiles](#) and [pre-boot authentication](#) passwords. After you create a volume, back up its header to a file (select *Tools* -> *Backup Volume Header*) before you allow a [non-admin user](#) to use the volume. Note that the [volume header](#) (which is encrypted with a [header key](#) derived from a password/keyfile) contains the [master key](#) with which the volume is encrypted. Then ask the user to choose a password, and set it for him/her (*Volumes* -> *Change Volume Password*); or generate a user keyfile for him/her. Then you can allow the user to use the volume and to change the password/keyfiles without your assistance/permission. In case he/she forgets his/her password or loses his/her keyfile, you can "reset" the volume password/keyfiles to your original admin password/keyfiles by restoring the volume header from the backup file (*Tools* -> *Restore Volume Header*).

Similarly, you can reset a [pre-boot authentication](#) password. To create a backup of the master key data (that will be stored on a [GuardShip Rescue Disk](#) and encrypted with your administrator password), select '*System*' > '*Create Rescue Disk*'. To set a user [pre-boot authentication](#) password, select '*System*' > '*Change Password*'. To restore your administrator password, boot the GuardShip Rescue Disk, select '*Repair Options*' > '*Restore key data*' and enter your

administrator password.

Note: It is not required to burn each [GuardShip Rescue Disk](#) ISO image to a CD/DVD. You can maintain a central repository of ISO images for all workstations (rather than a repository of CDs/DVDs). For more information see the section [Command Line Usage](#) (option `/noisochek`).

Q: It is possible to access a single GuardShip volume simultaneously from multiple operating systems (for example, a volume shared over a network)?

Please see the chapter '[Sharing over Network](#)' in the [GuardShip User Guide](#).

Q: Can a user access his or her GuardShip volume via a network?

Please see the chapter '[Sharing over Network](#)' in the [GuardShip User Guide](#).

Q: I encrypted a non-system partition, but its original drive letter is still visible in the 'My Computer' list. When I double click this drive letter, Windows asks if I want to format the drive. Is there a way to hide or free this drive letter?

A: Yes, to free the drive letter follow these steps:

1. Right-click the '*Computer*' (or '*My Computer*') icon on your desktop or in the Start Menu and select *Manage*. The '*Computer Management*' window should appear.
2. From the list on the left, select '*Disk Management*' (within the *Storage* sub-tree).
3. Right-click the encrypted partition and select *Change Drive Letter and Paths*.
4. Click *Remove*.
5. If Windows prompts you to confirm the action, click *Yes*.

Q: How do I remove or undo encryption if I do not need it anymore? How do I permanently decrypt a volume?

Please see the chapter '[How to Remove Encryption](#)' in the [GuardShip User Guide](#).

Q: What will change when I enable the option 'Mount volumes as removable media'?

A: You can enable this option, for example, to prevent Windows from automatically creating the '*Recycled*' and/or the '*System Volume Information*' folders on GuardShip volumes (in Windows, these folders are used by the Recycle Bin and System Restore facilities). However, there are some disadvantages. For example, when you enable this option, the '*Computer*' (or '*My Computer*') list will not show free space on the volume (note that this is a Windows limitation, not a bug in GuardShip).

Q: Is the online documentation available for download as a single file?

A: Yes, the documentation is contained in the file *GuardShip User Guide.pdf* that is included in all official GuardShip distribution packages. Note that you do *not* have to install GuardShip to obtain the PDF documentation. Just run the self-extracting installation package and then, on the second page of the GuardShip Setup wizard, select *Extract* (instead of *Install*). Also note that when you *do* install GuardShip, the PDF documentation is automatically copied to the folder to which GuardShip is installed, and is accessible via the GuardShip user interface (by pressing F1 or choosing *Help > User's Guide*).

Q: Do I have to "wipe" free space and/or files on a GuardShip volume?

Remark: to "wipe" = to securely erase; to overwrite sensitive data in order to render them unrecoverable.

A: If you believe that an adversary will be able to decrypt the volume (for example that he will make you reveal the password), then the answer is yes. Otherwise, it is not necessary, because the volume is entirely encrypted.

Q: Is it secure to create a new container by cloning an existing container?

A: You should always use the Volume Creation Wizard to create a new GuardShip volume. If you copy a container and then start using both this container and its clone in a way that both eventually contain different data, then you might aid cryptanalysis (both volumes would share a single key set). See also the chapter [How to Back Up Securely](#) in the [documentation](#).

Q: How does GuardShip know which encryption algorithm my GuardShip volume has been encrypted with?

Please see the section [Encryption Scheme](#) (chapter [Technical Details](#)) in the [documentation](#).