



ShadowProtect IT Edition User Guide

1. ShadowProtect IT Edition User Guide	3
1.1 ShadowProtect Overview	4
1.1.1 Features and Components	5
1.1.2 What's New	6
1.1.3 Usage Scenarios	7
1.2 How ShadowProtect Works	8
1.2.1 Create a Backup Image	9
1.2.2 Restore a Backup Image	10
1.2.3 Backup Image Files	11
1.2.3.1 File Naming Conventions	12
1.2.3.2 File Dependencies	13
1.3 Starting ShadowProtect IT Edition	14
1.3.1 Requirements	15
1.3.1.1 Hardware Requirements	16
1.3.1.2 Supported Operating Systems	17
1.3.1.3 Supported File Systems	18
1.3.1.4 Supported Storage Media	19
1.3.2 Starting ShadowProtect from the USB Key	20
1.3.3 Creating a ShadowProtect IT Edition CD	21
1.3.3.1 Using the IT Edition Licensing Server	22
1.3.4 Updating USB Key Source Files	23
1.4 Understanding the User Interface	24
1.4.1 Menu Bar	25
1.4.2 Task Panel	27
1.4.3 Tabs	30
1.5 Creating a Backup Image File	31
1.5.1 Options	32
1.5.1.1 Backup Image File Storage Location	33
1.5.1.2 File Compression	34
1.5.1.3 Backup Image File Security	35
1.5.1.4 Splitting Backup Image Files	36
1.5.1.5 Backup Comments	37
1.5.1.6 Advanced Options	38
1.6 Mounting a Backup Image File	39
1.6.1 Dismounting a Backup Image File	40
1.6.2 Backup Image File Mount Options	41
1.7 Restoring a Volume	42
1.7.1 Volume Restore Options	44
1.8 Using Image Conversion Tool	45
1.9 Other Operations	47
1.9.1 Deleting Backup Image Files	48
1.9.2 Verifying Backup Image Files	49
1.10 Best Practices	50
1.11 Product Support	51
1.12 Glossary	52

ShadowProtect IT Edition User Guide

Welcome to the StorageCraft® ShadowProtect® IT Edition User Guide. This Guide describes the ShadowProtect technology, how to use the product, and how to derive maximum benefit from ShadowProtect IT Edition. All references to ShadowProtect in this Guide refer to ShadowProtect IT Edition.

This Guide includes the following major sections:

- ShadowProtect Overview
- How ShadowProtect Works
- Starting ShadowProtect IT Edition
- Understanding the User Interface
- Creating a Backup Image File
- Mounting a Backup Image File
- Restoring a Volume
- Using Image Conversion Tool
- Other Operations
- Best Practices

Additionally, this Guide includes the following general information sections:

- Product Support
- Glossary

Additional Information

- For emerging issues and other resources, see the following:
 - The `readme.txt` file included with the ImageManager product files.
 - The StorageCraft technical support Web site at www.storagecraft.com/support.html.
- This User Guide is also available in the ShadowProtect user interface from the Help menu.

Documentation Conventions

Note or **Warning** text provides important information about the configuration and/or use of ShadowProtect ImageManager.

ShadowProtect Overview

ShadowProtect provides robust and flexible disaster recovery by creating and managing backup image files. Each backup image file represents the exact state of your system at a given point-in-time. ShadowProtect provides tremendous advantages over traditional disaster recovery methods.

Other Methods	Shadow Protect
1. Repair hardware if necessary	1. Repair hardware if necessary
2. Collect all necessary OS media	2. Boot from Recovery CD
3. Reload OS from CD-ROM	3. Restore entire system or selected files
4. Reboot	4. Reboot
5. Apply multiple service packs	FULLY RESTORED IN MINUTES
6. Reboot (this could take several reboots)	
7. Reload backup software from CD-ROM	
8. Patch backup software to the latest support level	
9. Reboot	
10. Load recovery tape and restore	
FULLY RESTORED IN HOURS	

You should be aware of the following information as you prepare to install and use ShadowProtect:

- [Features and Components](#)
- [Usage Scenarios](#)

Features and Components

Component	Features
ShadowProtect Console	<p>An easy-to-use management console that lets you manage the disaster recovery configuration on your Windows system. ShadowProtect console provides the following primary features:</p> <ul style="list-style-type: none"> • Microsoft VSS-aware (Volume Shadow Copy Service) so you can unobtrusively back up changes in the background. • Wizard-based back-up to any accessible hard disk, including network storage (SAN, NAS, iSCSI), removable drives (USB, FireWire), and optical media (CD, DVD, Blu-Ray). • Verify backup images to ensure complete recovery. • Create compressed and encrypted backup image files for efficiency and security. • Wizard-based recovery of files, folders, or a complete data volume, to an exact point -in-time. • View backup images for quick file and folder recovery. • Remotely manage system backup and recovery operations. • VirtualBoot lets you create a mount any backup image file as a virtual disk in the VirtualBox Virtual Machine environment.
ShadowProtect Backup Agent	<p>The engine that creates and manages a system's point-in-time backup images. The Backup Agent also handles mounting of backup image files. You can manage the operation of the Backup Agent from the ShadowProtect Console.</p> <p>To access the ShadowProtect Backup Agent, you must be a user with local administration rights.</p>
StorageCraft Recovery Environment	<p>A bootable Windows environment for disaster recovery without installing software. For more information about the Recovery Environment, see the StorageCraft Recovery Environment Guide.</p> <ul style="list-style-type: none"> • Access all the features of the ShadowProtect Console from a standalone disaster recovery environment. • Loads from the bootable ShadowProtect CD. • Restore a system (bootable) volume quickly and easily. • Back up a non-bootable system before attempting a restore operation. • Use Hardware Independent Restore (HIR) to restore to different hardware, or to virtual environments (P2P, P2V, V2P). • Network configuration tool to manage TCP/IP properties, domains and network resources.
ImageManager	<p>ImageManager provides unprecedented control over your backup image files. It provides policy-driven services for managing backup image files. For more information about ImageManager features, see the ImageManager User Guide.</p> <ul style="list-style-type: none"> • Consolidation of Incremental backup image files into daily, weekly, and monthly consolidated image files that greatly reduce the number of files in an image chain. • Verification and re-verification of backup image files, including consolidated files. • Replication of backup image files to a local drive, a network share, or an off-site location (using FTP) • Head Start Restore (HSR) lets you restore a backup image while ShadowProtect continues to add Incremental backup images to it. This lets you greatly reduce the downtime associated with hardware failure of hardware migration tasks.

What's New

ShadowProtect 4.0.2 provides the following primary features and updates. For a complete version history of product updates, see the Readme.rtf, located in the \StorageCraft\ShadowProtect\ folder of your ShadowProtect installation.

ShadowProtect Console

- ShadowProtect for Managed Services provides a subscription-based licensing option for Managed Service Providers (MSP).
- ShadowProtect SBS Edition (Small Business Server) now supports Windows Server 2008 R2 Foundation.
- VirtualBoot now supports VirtualBox 4.0.2. Due to problems in VirtualBox 4.0.0 related to implementing third-party plug-ins, VirtualBoot cannot work with this particular version. These problems have been resolved in VirtualBox 4.0.1 and later.
- VirtualBoot now automatically pauses (disables) backup jobs when it creates a new VM. Users must manually restart a backup job to have it create backup images from the VirtualBoot VM. This gives users the opportunity to reconfigure the backup job as needed for the VM environment (for example, update the network destination object to ensure backup image files created in the VM are stored in the same location as those created prior to the VirtualBoot).
- The Monthly backup schedule now supports multiple intra-daily Incrementals, similar to the Weekly backup schedule.
- All scheduled backup schedules (Weekly, Monthly, and Continuous Incremental) now automatically generate SPK (Password Key) files for use by ImageManager with encrypted backup image files. Users no longer need to manually generate the SPK file.
- The ShadowProtect snapshot driver (stcvsm.sys) has been enhanced to reduce interoperability issues with third-party storage drivers.
- Includes an SPDiagnostic tool that can gather detailed information about a ShadowProtect installation for the purposes of troubleshooting, and gathering information for StorageCraft Support.
- ShadowProtect 4.1.0 and ImageManager 4.1.0 are released for English, Japanese, French, German, and Portugal-Portuguese.

Recovery Environment

- Includes an option to change the system keyboard layout.
- The Recovery Environment CD no longer contains a directory with the product installers. This was necessary to ensure that the Recovery Environment ISO would fit on a common CD-R. StorageCraft now provides a separate non-bootable ISO file with the installer files.

Image Manager

- Support for VMware ESX and ESXi (when sufficiently licensed) as HeadStart Restore targets.
- Simplified user interface to improve usability.
- ImageManager now automatically deletes backup image files from a local replication target, according to the retention schedule specified in a Weekly or Monthly scheduled backup job.

Usage Scenarios

The following use cases introduce several common usage scenarios for ShadowProtect IT Edition:

Bare Metal Recovery

Problem: Servers, desktops and laptops need to be available and online for employees to stay productive. In the case of a disaster, systems must be restored as quickly and reliably as possible. Manually re-installing operating systems and rebuilding user environments requires multiple reboots and can take considerable time.

ShadowProtect Solution: Using Recovery Environment, available on the bootable ShadowProtect CD, IT personnel can restore an entire system in minutes. The disk-speed restoration process is much faster than restoring from tape, and the ShadowProtect restores the system to its exact state before the failure.

Bare Metal Recovery to a Different System

Problem: Due to hardware failure or other circumstances, IT personnel must restore a system volume to partially, or completely, different hardware, or restore a system to a virtual environment.

ShadowProtect Solution: Using Recovery Environment, available on the bootable ShadowProtect CD, IT administrators can use Hardware Independent Restore (HIR) restore a system to different hardware, or a virtual environment. HIR supports any type of system restore (P2P, P2V, V2P and V2V).

Additionally, VMWare provides support for StorageCraft Image Files in VMWare Workstation 6 and their Converter tool.

Create a Base Image for Every System

Problem: IT personnel need to create "factory" images of new systems so they can restore system to the original factory state, or some other known state. IT departments don't want to have to buy a license to do this for each system in the organization.

ShadowProtect Solution: ShadowProtect IT Edition lets IT personnel take images of as many systems as necessary, throughout the entire organization. IT administrators can image each new system and periodically backup systems without installing software.

Full System Backup without Installing Software

Problem: IT personnel need to get full backups of systems without installing software. Ideally, they want to leverage proven technology that is already deployed throughout the organization.

ShadowProtect Solution: IT personnel can utilize the Microsoft VSS framework to create full backup images of Windows Server 2003 or Windows XP without installing any additional software. ShadowProtect IT Edition supports full system backups using a VSS snapshot.

Live Backup

Problem: When taking system backups, IT personnel cannot afford to stop each system in order to create a backup image.

ShadowProtect Solution: By leveraging disk imaging with existing Windows snapshot technology, ShadowProtect lets IT personnel create live system backups without any system downtime. ShadowProtect creates live backup images that include a system's operating system, critical data and configuration settings.

ExactState Backup Images

Problem: IT personnel need the most reliable and recoverable backup images possible.

ShadowProtect Solution: ShadowProtect includes ExactState backup image technology that lets IT personnel create a backup image file from the StorageCraft Recovery Environment, thereby ensuring that all system files and resources are closed so ShadowProtect can back them up properly. ExactState image technology supports all Windows server and desktop operating systems.

How ShadowProtect Works

ShadowProtect provides robust and flexible disaster recovery by creating and managing backup image files. Each backup image file represents the exact state of your system at a given point-in-time.



There are two primary tasks related to data recovery with ShadowProtect:

- Create a Backup Image
- Restore a Backup Image
- Backup Image Files

Create a Backup Image

Creating a ShadowProtect backup image involves two key processes:

Create a Virtual Volume

Using Microsoft VolSnap and VSS (with Windows Server 2003, Windows XP, or later), ShadowProtect creates a point-in-time snapshot of the volume you want to backup. The entire process of taking a snapshot of a volume and creating a virtual volume takes only seconds and does not interfere with system operation.

Snapshot methods supported by ShadowProtect

Snapshot	Supported OS	Image Speed	Quality	Comments
StorageCraft VSM with VSS	Windows Server 2000 Family	Fast	Best	<ul style="list-style-type: none"> VSS aware applications are managed to achieve best backups. Can use script files to manage applications that are not VSS aware to improve backups.
Microsoft VolSnap with VSS	Windows Server 2003/2008 Family	Slow	Best	<ul style="list-style-type: none"> VSS aware applications are managed automatically to achieve best backups. Use script files (before and after the snapshot) to manage non-VSS-aware applications and improve backups. Cannot create Incremental Image File (see Glossary)
StorageCraft VSM direct	Windows 2000 Server Family Windows 2003/2008 Server Family	Fast	Good	<ul style="list-style-type: none"> Use script files (before and after the snapshot) to manage applications (both VSS and non-VSS) and improve backups.

Additionally, ShadowProtect provides a Backup Scheduler that lets you configure automated backup jobs for protected volumes. You can schedule Full Image, Incremental Images (as often

as every 15 minutes), and manage the retention of backup Image Sets. The ShadowProtect Image Conversion Tool simplifies image management by letting you manage existing image files,

including consolidating files in an Image Set, modifying password encryption and compression, and merging or splitting image files.

Capture the Virtual Volume

To backup the volume, ShadowProtect replicates the virtual volume to create a backup image file. A backup image file is a sector-by-sector representation of the volume at the time the

volume snapshot was taken. For more information about backup image files, see [Backup Image Files](#).

ShadowProtect writes the backup image file to the designated storage media. Options include network storage (SAN, iSCSI, NAS, etc.), removable storage (USB / FireWire), and optical

storage (CD, DVD, Blu-ray). The amount of time it takes to write the backup image file depends upon the system hardware and the size of the image file. For information about configuring

and creating backup image files, see [Creating a Backup Image File](#).

Restore a Backup Image

Once you have created a backup image, you can use a ShadowProtect backup image to restore data in two different ways:

Recover individual files and folders

Use the ShadowProtect Mount utility to mount the backup image file as a volume using either a drive letter or a mount point. The Mount utility can efficiently mount hundreds of backup images simultaneously, if desired. Furthermore, since the mounted backup image files preserve the Windows volume properties, users can share and access the backup image file for emergency access to backup image file data, including modifying and saving changes to the backup image file as an incremental backup file.

For more information about mounting backup image files to recover data, see [Mounting a Backup Image File](#).

Restore an entire volume

Use the ShadowProtect Restore Wizard to restore an entire volume from a backup image file. You can restore system volumes (that contains the system's operating system) using the StorageCraft Recovery Environment, or restore non-system volumes using either Recovery Environment or while running ShadowProtect Console in Windows. For more information about recovering volumes, see [Restoring a Volume](#).


Backup Image Files

A ShadowProtect backup image file is a point-in-time representation of a computer volume. It is not a standard file copy of the volume, but rather a sector-by-sector duplicate of the volume.

Because of this, you can mount a backup image file (using the ShadowProtect Mount utility) and view its contents as if it were a regular volume. In the event that you need to recover data, you

can recover specific files and folders from the image or you may recover the entire volume to the exact point-in-time that the backup image was taken.

ShadowProtect uses the following types of backup image files to provide a complete disaster recovery solution.

Backup Images	Description
Full (.spf)	A stand-alone image file that represents a disk volume at a specific point-in-time. Full backup image files do not rely on any other files.
Incremental (.spi)	<p>An image file that contains volume changes relative to another backup image file. You can create Incremental backup image files relative to Full backup images or other Incremental backup images. ShadowProtect also creates an Incremental image file when an existing image file is mounted as a read/write volume and modified. Incremental backup image files let ShadowProtect offer multiple volume backup strategies, including Differential and Incremental backup options. See Glossary for information about these backup strategies.</p> <div style="background-color: #ffffcc; padding: 10px; border: 1px solid #ccc;"> <p> Note: ShadowProtect IT Edition does not support this type of backup. Use ShadowProtect Server Edition or ShadowProtect Desktop Edition to take advantage of Incremental backup images.</p> </div>
Spanned (.sp_#_)	<p>Image files that belong to a spanned image set. Spanned image sets are made by breaking a backup image file into pieces for increased portability (for example, to save the image file on multiple CDs).</p> <p>The actual Spanned image file replaces the pound sign (#) with a number that indicates the position of the file within the spanned image set.</p>

File Naming Conventions

ShadowProtect backup image files use the following naming convention to help you identify the file and its relationship to, and dependencies on, other backup image files.

`<Volume Identifier>-b<base-seq>-d<diff-seq>-i<inc-seq>.<extension>_`

The ShadowProtect naming convention uses the following variable components:

volume identifier: Identifies the volume that the backup image file represents.

base-seq: The Base Image File sequence number. This either identifies the sequence number of this file, or identifies the Base Image File upon which this file is dependent.

diff-seq: The Differential backup sequence number. This either identifies the sequence number of this file, or identifies the Differential Image File upon which this file is dependent.

inc-seq: The Incremental backup sequence number. This either identifies the sequence number of this file, or identifies the Incremental Image File upon which this file is dependent.

extension: The file extension, which identifies if the file is a Full, Incremental, or Spanned backup image file.

File Type Extension	Description
C_Vol-b001.spf	Full image of the C:\ volume.
C_Vol-b001-d001-i000.spi* or C_Vol-b001.d001.spi	Differential image of the C: volume with a dependency on the full}} backup image file {{C_Vol-b001.spf This type of backup is not available in ShadowProtect IT Edition.
C_Vol-b001-d000-i001.spi* or C_Vol-b001-i001.spi	Incremental image of the C:\ volume with a dependency on the full backup image file {{C_Vol-b001.spf The only time ShadowProtect IT Edition creates a .spi file is when you mount a read/write backup image and save changes made to that volume. Upon dismounting that volume, the changes will be saved out to an incremental file.
C_Vol-b001-d001.i001.spi	Incremental backup image file of the C:\ volume with a dependency on the differential backup image file C_Vol-b001-d001.i000 which in turn has a dependency on C_Vol-b001.spi. This type of backup is not available in ShadowProtect IT Edition.



Note: Backup image file names that have a "-d000" or "-i000" segment use these name segments only as place holders, and indicate that a differential backup image or an

incremental backup image are not part of the image and the backup image file has no dependency on a previous differential or incremental backup image file.

File Dependencies

By examining the name of a backup file image, ShadowProtect users can tell identify the files that it is dependent on. However, it is not possible to determine if other backup image files are dependent on this file. Because of this, it is very important to use the Image Conversion Tool (see [Using Image Conversion Tool](#)) to review dependencies prior to moving, modifying or deleting backup images.



Warning: Deleting a backup image file on which other files depend renders the dependent backup image files useless. You cannot browse or restore files contained by these dependent backup image files.



Note: Deleting a full image file from an active backup image job causes ShadowProtect to create a new Full image during the next scheduled backup and start a new backup image set.

Starting ShadowProtect IT Edition

StorageCraft distributes ShadowProtect IT Edition software and licensing using a USB key, which makes it possible for StorageCraft to more efficiently support its customer base. ShadowProtect IT Edition does not install any software on your system.

This section contains the following topics:

- Requirements
- Starting ShadowProtect from the USB Key
- Creating a ShadowProtect IT Edition CD
- Updating USB Key Source Files



Note: Use of ShadowProtect IT Edition is governed by the ShadowProtect Technician License Agreement (TLA). Before using the Software, review the complete TLA (visit <http://www.storagecraft.com/legal>).

Requirements

ShadowProtect IT Edition has the following requirements:

- [Hardware Requirements](#)
- [Supported Operating Systems](#)
- [Supported File Systems](#)
- [Supported Storage Media](#)

Hardware Requirements

ShadowProtect IT Edition has the following minimum hardware requirements:

- Must meet minimum operating system requirements.
- Memory: At least 512 MB of RAM (or the minimum required by the operating system).
- Available USB port

Supported Operating Systems

ShadowProtect supports the following Windows operating systems (both 32-bit and 64-bit versions, where applicable):

- Windows Server 2008 (including R2)
- Windows 7
 - Windows XP Family, including:
 - XP Home
 - XP Professional
- Windows Vista Family, including:
 - Vista Home Basic
 - Vista Home Premium
 - Vista Business
 - Vista Ultimate*
- Windows Server 2003 Family, including:
 - Server 2003 Standard Edition
 - Server 2003 Standard Edition R2
 - Server 2003 Advanced Edition
 - Server 2003 Advanced Edition R2
 - Server 2003 Enterprise Edition
 - Server 2003 Enterprise Edition R2
 - Server 2003 Datacenter Edition
 - Server 2003 Datacenter Edition R2
 - Server 2003 Web Edition
 - Small Business Server 2003
- Windows 2000 Server SP4



Note: ShadowProtect provides Hot Backup capability only on Windows systems that provide VolSnap/VSS.

Supported File Systems

ShadowProtect supports the following File Systems:

- FAT16
- FAT16X
- FAT32
- FAT32X
- NTFS
- GPT Disks
- Dynamic Disks

Supported Storage Media

ShadowProtect supports the following storage media:

- Locally-connected hard drives
- Removeable hard drives (USB or FireWire)
- Network drives (SAN, NAS, iSCSI)
- Optical media (CD, DVD, Blu-Ray)

Starting ShadowProtect from the USB Key

StorageCraft distributes ShadowProtect IT Edition software and licensing using a USB key. The USB key includes a write lock that prevents data writes to the device. StorageCraft recommends keeping the write lock enabled except when:

- Updating ShadowProtect IT Edition source files (see [Updating USB Key Source Files](#)).
- Booting to the Legacy (Windows 2003/XP) version of ShadowProtect IT Edition.

The first time you start ShadowProtect IT Edition you must activate the USB key with the license code you received from StorageCraft when you purchased ShadowProtect IT Edition.

To start ShadowProtect from the USB key

1. Insert the USB key into an available USB port.
2. If ShadowProtect IT Edition does not start automatically, browse the USB key and execute `START SHADOWPROTECT` command script.
3. (Conditional) If prompted, enter a valid license code to activate the USB Key.

When you purchase ShadowProtect IT Edition, StorageCraft provides you a license code to activate the USB key. Additionally, you must reactivate the USB key on a quarterly basis. To do this, plug the USB key into a system with Internet access.

To load StorageCraft Recovery Environment from the USB key

1. Shutdown the system.
2. Insert the USB key into an available USB port, then restart the system.
Make sure the system BIOS is configured to boot from a USB drive before the system's hard disk drive (HDD).
3. Follow the on-screen instructions to load the Recovery Environment.
For more information about Recovery Environment, see the [StorageCraft Recovery Environment User Guide](#).

Creating a ShadowProtect IT Edition CD

The USB key contains the source files and license necessary to create a ShadowProtect IT Edition CD. You can then use the CD to start ShadowProtect in Windows or load the StorageCraft Recovery Environment.

To create a ShadowProtect IT Edition CD

1. Insert the USB key into an available USB port.
2. Browse the USB key for the ShadowProtect IT Edition image file (`ENU_ShadowProtect_IT_CD_3.5.iso`).
3. Use a CD/DVD burning software of your choice to burn the ISO image to CD or DVD media.

From the CD, you can start ShadowProtect IT Edition in two ways:

To start ShadowProtect in Windows

1. Place the IT Edition CD in the system's CD/DVD drive.
2. If ShadowProtect IT Edition does not start automatically, browse the USB key and execute `START SHADOWPROTECT` command script.
3. When prompted, enter the IP address of the IT Edition license server that contains your activated IT Edition license.

For more information, see [Using the IT Edition Licensing Server](#).

ShadowProtect IT Edition loads into memory only (Windows XP or later). The hard drive is not used to store information.

To load StorageCraft Recovery Environment

1. Shutdown the system.
2. Insert the USB key into an available USB port, then restart the system.
Make sure the system BIOS is configured to boot from the CD/DVD drive before the system's hard disk drive (HDD).
3. Follow the on-screen instructions to load the Recovery Environment.

The Recovery Environment runs directly from the CD/DVD. The hard drive is not used to store information. For more information about the Recovery Environment, see the StorageCraft Recovery Environment User Guide.

Using the IT Edition Licensing Server

Although you can run ShadowProtect IT Edition from a CD, the USB key still provides the license to use the software. IT Edition must be able to locate the activated IT Edition license to successfully load from the CD.

IT Edition automatically looks for the USB key when loading. If it does not detect the USB key locally, it looks on the network. ShadowProtect IT Edition includes a licensing server utility that makes your IT Edition license available on the network when loading IT Edition from a CD.

To start the license server

1. Insert the USB Key into an available USB port.
2. Browse the USB key and execute `Start_LicenseServer` command script.

The license server must be on the same network subnet as the system



Updating USB Key Source Files

When StorageCraft releases updates to ShadowProtect IT Edition, you can update the USB key so it contains the current source files.



Note: In the task below, x.x indicates the product version number.

To update the USB key

1. Before updating your USB Key, make sure your license is active and, if necessary, connect it to a computer and give it the opportunity to "call home".

You can force a call home by executing `START SHADOWPROTECT` or `Start_LicenseServer` from the USB Key. If you haven't used your USB Key for a while, doing this helps ensure the update process completes properly.

2. Open a Web browser to the StorageCraft Upgrade site (<http://www.storagecraft.com/release/sprelease.asp>).
3. Enter your ShadowProtect serial number, then click Submit.
You must enter a valid serial number to get access to the download file.

4. On the Technician License Agreement page, scroll to the bottom and click I Accept.

5. Save `ShadowProtect_IT_USB_x.xdl.exe` to your local drive, then launch the executable.

6. Specify a location to store the compressed update file (`ENU_ShadowProtect_IT_Edition_USB_Key_Update_x.x.zip`), then click Next.

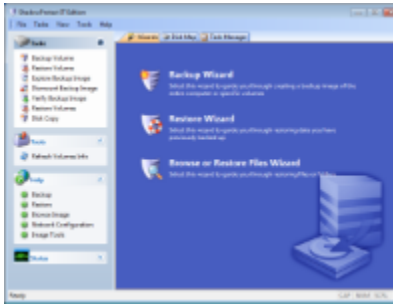
StorageCraft uses a download manager to download the compressed update file. Because of this, you can pause and resume the download, or even cancel the current download and pick up where you left off at a later time.

7. Extract the contents of the `.zip` file to your local drive.
8. Launch the update application (`ENU_ShadowProtect_IT_Edition_USB_Key_Update_x.x.exe`).
9. In the USB Key Update Wizard, follow the steps to install the ShadowProtect IT Edition updates.



Note: When prompted for the destination folder, you MUST select the IT Edition USB key as the location to install the files

Understanding the User Interface




ShadowProtect Main Screen

Menu Bar

The ShadowProtect menu bar provides access to following menus:

ShadowProtect File Menu Options

Menu	Description	Options
File	Access application-level options.	Exit: Close the ShadowProtect UI.
Tasks	Access ShadowProtect wizards.	<p>Backup Volumes: Launches the Backup Wizard (see Creating a Backup Image File).</p> <p>Restore Volume: Launches the Restore Wizard (see Restoring a Volume).</p> <p>Explore Backup Image: Launches the Explore Backup Image Wizard (see Mounting a Backup Image File).</p> <p>Dismount Backup Image: Launches the Backup Image Dismount Wizard (see Dismounting a Backup Image File).</p> <p>Image Conversion Tool: Launches the Image Conversion Tool Wizard (see Using Image Conversion Tool).</p> <p>Verify Image: Launches the Verify Image Wizard (see Verifying Backup Image Files).</p>
View	Create custom toolbars and manage toolbar visibility.	<p>Toolbars: Opens the Customize Tool Bar dialog box, where you can create customized tool bars for the ShadowProtect UI.</p> <p>Status Bar: Toggles a status bar at the bottom of the UI that provides application and environment status information.</p> <p>Task Panel: Toggles the Task Panel (see Task Panel).</p> <p>Show Detail Tabs: Toggles the Details tab for each active backup or restore operation.</p>

Tools	Access ShadowProtect tools.	<div data-bbox="553 159 1230 331" style="background-color: #ffffcc; padding: 10px; border: 1px solid #ccc;">  Note: Several tools are available only in Recovery Environment (RE). For more information about these tools, see the StorageCraft Recovery Environment User Guide. </div> <p>Network Configuration: (RE only) Launches the Network Configuration utility, where you can configure a computer's network access settings.</p> <p>HIR Configuration: (RE only) Launches the Hardware Independent Restore (HIR) utility, where you can restore a backup image to a different environment from which it was created.</p> <p>Load Drivers: (RE only) Opens the Load Drivers dialog box, where you can configure storage drivers for use in Recovery Environment.</p> <p>File Browser: (RE only) A simple file browser that lets you browse files and folders of a backup image file.</p> <p>Text Editor: (RE only) A simple text editor.</p> <p>Vista BCD: (RE only) Launches the Vista BCD editor, where you can edit Boot Configuration Data (BCD) on systems running Windows Vista.</p> <p>Partition Table Editor: (RE only) A simple partition table editor.</p> <p>UltraVNC: (RE only) Launches the Remote Management utility, where you can configure remote access to systems running Recovery Environment.</p> <p>Select Your Time Zone: (RE only) Launches the Time Zone utility, where you can adjust the system's time zone information.</p> <p>Enable Logging: Opens a Logging dialog box, where you can specify a location for ShadowProtect log files.</p> <p>Refresh Volumes Info: Refreshes the Volume List in ShadowProtect.</p>
Help	Access ShadowProtect help resources.	<p>Contents: Launches the ShadowProtect on-line help system. The help is available only when running ShadowProtect in Windows (not Recovery Environment).</p> <p>About ShadowProtect: Displays the ShadowProtect version and copyright information. Click System Info to open the Microsoft System Information dialog box, which contains detailed information about the computer.</p>


Task Panel

The ShadowProtect Task panel provides left-side access to ShadowProtect tasks and tools. The Task panel is organized into the following categories. You can collapse and expand each

category, as desired.

ShadowProtect Task Panel Options

Menu	Description	Options
Tasks	Access ShadowProtect wizards.	<p>Backup Volume: Launches the Backup Wizard (see Creating a Backup Image File).</p> <p>Restore Volume: Launches the Restore Wizard (see Restoring a Volume).</p> <p>Explore Backup Image: Launches the Explore Backup Image Wizard (see Mounting a Backup Image File).</p> <p>Dismount Backup Image: Launches the Backup Image Dismount Wizard (see Dismounting a Backup Image File).</p> <p>Verify Backup Image: Launches the Verify Image Wizard (see Verifying Backup Image Files).</p> <p>Restore Volumes: (Experimental) Launches a modified Restore Wizard where you can restore multiple volumes simultaneously.</p> <p>Disk Copy: (Experimental) Launches the Disk Copy Wizard where you can make exact copies of volumes or disks from one drive to another. You must have multiple disk drives in the system to use Disk Copy.</p>

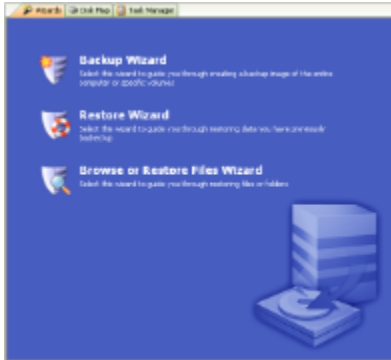
Tools	Access ShadowProtect tools.	<div data-bbox="706 157 1425 424" style="background-color: #ffffcc; padding: 10px; border: 1px solid #ccc;">  Note: Several tools are available only in Recovery Environment (RE). For more information about these tools, see the StorageCraft Recovery Environment User Guide. </div> <p>Network Configuration: (RE only) Launches the Network Configuration utility, where you can configure a computer's network access settings.</p> <p>HIR Configuration: (RE only) Launches the Hardware Independent Restore (HIR) utility, where you can restore a backup image to a different environment from which it was created.</p> <p>Load Drivers: (RE only) Opens the Load Drivers dialog box, where you can configure storage drivers for use in Recovery Environment.</p> <p>File Browser: (RE only) A simple file browser that lets you browse files and folders of a backup image file.</p> <p>Text Editor: (RE only) A simple text editor.</p> <p>Vista BCD: (RE only) Launches the Vista BCD editor, where you can edit Boot Configuration Data (BCD) on systems running Windows Vista.</p> <p>Partition Table Editor: (RE only) A simple partition table editor.</p> <p>UltraVNC: (RE only) Launches the Remote Management utility, where you can configure remote access to systems running Recovery Environment.</p> <p>Select Your Time Zone: (RE only) Launches the Time Zone utility, where you can adjust the system's time zone information.</p> <p>Refresh Volumes Info: Refreshes the Volume List in ShadowProtect.</p>
Help	(Windows only) Access to on-line help topics.	<p>Backup: Opens the on-line help to Creating a Backup Image File.</p> <p>Restore: Opens the on-line help to Restoring a Volume.</p> <p>Browse Image: Opens the on-line help to Mounting a Backup Image File.</p> <p>Network Configuration: Opens the on-line help to "Using the Network Configuration Utility" in the StorageCraft Recovery Environment User Guide.</p> <p>Image Tools: Opens the on-line help to Using Image Conversion</p>
Info	(RE only) Display system information.	A quick reference to basic system information, including Computer Name, IP Address and Time Zone information.

Status	(RE only) Displays current ShadowProtect task status.	Queued Tasks: The number of queued tasks waiting to run. Running Tasks: The number of tasks currently running.
--------	---	---

Tabs

The ShadowProtect tabs provide access to primary features and application status:

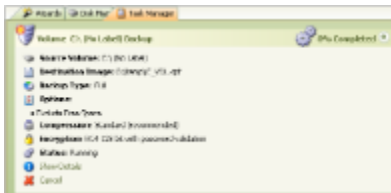
- **Wizards:** Provides access to the three Wizards (Backup, Restore, and Explore Backup Image) that guide users through the most common ShadowProtect tasks.



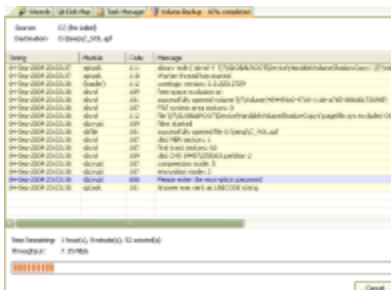
- **Disk Map:** Provides a graphical view of the system drives. The Disk Map tab lets you access the Backup and Restore Wizards, and change partition creation policies for the selected drive. Additionally, in Recovery Environment you can also run Check Disk, format a drive and edit the selected disk's boot . ini



- **Task Manager:** Displays the status of an active task. View task details by clicking Show Details, or cancel the task by clicking Cancel.



- **Volume Backup, Volume Restore, Image Maintenance:** Displays status information about a currently active task. You can control the display of these tabs by clicking Show Details / Hide Details in the Task Manager tab. For example:



Creating a Backup Image File

The ShadowProtect Backup Wizard guides you through the process of creating a backup of an entire system, or a specific volume on a system. The process is the same whether you are making a Hot Backup from Windows, or a Cold Backup from the StorageCraft Recovery Environment. For more information about each of these options, see [Components and Features](#).

To create a backup image file

1. Start the ShadowProtect Console (see [Starting ShadowProtect IT Edition](#)).
2. Open the Backup Wizard by doing one of the following:
 - In the Wizards tab, click Backup Wizard.
 - In the Tasks menu, click Backup Volume.
3. In the Volumes to Back Up page, select the volumes to backup, then click Next.
To backup the entire system, select all volumes.
4. In the Backup Type page, select the type of backup to perform, then click Next.
Perform a Full Backup: Makes a full backup image file for the selected volumes.
Perform a Differential Backup: Makes a backup of volume changes since the last Full Backup.



Note: The ability to make an Incremental backup is available only in ShadowProtect Server Edition and ShadowProtect Desktop Edition.

5. In the Backup Name and Destination page, specify where you want to store the backup image file, then click Next.
 - a. Select whether you want to store the backup image file on a local or network directory, or an optical storage medium (CD/DVD/Blu-ray).
 - b. Browse to, or enter, the path to the location.
 - c. (Optional) Right-click a file name, then select Rename to change the name of the backup image file.
6. In the Options page, select the backup image file options, then click Next.
The Options page lets you set file compression, security (password and encryption), image file size (splitting), and a backup comment. For more information about each of these options, see [Options](#).
7. In the Wizard Summary page, review the backup image file configuration, then click Finish to create the backup image file.
You can monitor the progress of the backup in the Task Manager tab by clicking the Details button.

Options

The following options let you control how ShadowProtect creates a backup image file:

- Backup Image File Storage Location
- File Compression
- Backup Image File Security
- Splitting Backup Image Files
- Backup Comments
- Advanced Options

Backup Image File Storage Location

ShadowProtect lets you store backup image files on any disk device, including hard drives, removeable USB/FireWire drives, network drives and NAS (Network Attached Storage) devices. You can also store backup images to optical media such as CDs, DVDs, or Blu-Ray discs.



Note: If you select a destination that does not have enough disk space to save the backup image, the backup job fails due to lack of destination storage space. ShadowProtect notes the reason for the failure in its log file.

Advantages and Disadvantages for Various Storage Locations

Location	Advantages	Disadvantages
Local Hard Drive	<ul style="list-style-type: none"> • Fast backup and restore. • Inexpensive. 	<ul style="list-style-type: none"> • Consumes local disk space. • Vulnerable to loss if the drive fails
Local USB/FireWire Drive	<ul style="list-style-type: none"> • Fast Backup and restore. • Preserves disk space on local drives. • Inexpensive. • Easy off-site storage. 	<ul style="list-style-type: none"> • More expensive than local hard drives • Vulnerable to loss if the drive fails
Network Hard Drive	<ul style="list-style-type: none"> • Fast backup and restore • Protection from local hard drive failure • Off-site storage. 	<ul style="list-style-type: none"> • Must have network interface card drivers supported by Recovery Environment. • Complexity. Users must have network rights to save and access backup images.
CD/DVD/Blu-Ray	<ul style="list-style-type: none"> • Good media for archiving. • Protection from local hard drive failure. 	<ul style="list-style-type: none"> • Slower backups due to media speeds. • File restrictions due to limited size

File Compression

ShadowProtect offers multiple file compression options when creating backup image files.

Backup Image File Compression Levels

Compression Level	Description
None	No file compression. This option provides faster backup where disk space is not an issue.
Standard	Compresses data by about 40% on average. This option provides a balance between backup speed and disk space consumption.
High	Compresses data by about 50% on average. This option requires the most time and system resources to complete a backup, but is useful when disk space is limited.

Backup Image File Security

ShadowProtect lets you encrypt and password protect backup image files. This is particularly useful when storing backup image files on a network or off-site. To mount or restore a protected backup image file, you must provide the correct password. If you do not enter the correct password, or you forget the password, you cannot access the backup image file. Make sure the password is stored in a secure location. StorageCraft cannot bypass the encryption on a backup image files.

You may select from three methods when encrypting a backup image file.

You may select from three methods when encrypting a backup image file.

- RC 4 128 bit (Fast): Faster but less secure than AES 128-bit.
- AES 128 bit (More Secure): Faster but less secure than AES 256-bit.
- AES 256 bit (Most Secure): Slowest but most secure security option.

In addition to bit strength, the password used to secure the backup image file can affect security. Use the following password guidelines to ensure the best backup image file security:

- At least eight characters
- Random mixture of upper and lower case letters, characters and numbers.
- Do not use words found in the dictionary.
- Change passwords regularly, or if you suspect your password has been compromised.



Note: ShadowProtect passwords are case-sensitive and support alphanumeric characters.

Splitting Backup Image Files

ShadowProtect lets you split backup image files into multiple smaller image files, if desired. Splitting files lets you more easily move backup image files onto fixed length media such as CD or DVD.

You can split backup image files when creating them (either manually or during a scheduled backup job), or after the fact with the Backup Image Utility (see [Using Image Conversion Tool](#)).



Note: A backup image file that has been split into multiple files is known as a Spanned image file. Spanned image files use a special file extension to indicate they are part of a file set (see [Deleting Backup Image Files](#)).

Backup Comments

You can attach backup comments to a backup image file. These comments are available for review when mounting or restoring the backup image file at a later date. By default, the time and date stamp are added as backup comments.

Advanced Options

Advanced backup image file options are available by clicking Advanced in the Options page of the Backup Wizard (see Creating a Backup Image File).



Note: StorageCraft recommends using the default advanced option settings unless you fully understand the impact of changing these features.

Lock Source Volume

Default: Off

On: ShadowProtect does not use snapshot technology to backup the volume. Instead it attempts to gain exclusive access to the volume. If it is unable to gain exclusive access, the backup fails.

Off: ShadowProtect uses snapshot technology to backup the volume so that it does not need to lock volume access. You must use snapshot technology (`Lock Source Volume = Off`) to backup a system volume.

If snapshot technology is not available in the Windows operating system you want to backup, you must set Lock Source Volume = On or run ShadowProtect from the StorageCraft Recovery Environment. When running ShadowProtect from Recovery Environment, ShadowProtect automatically gets exclusive access to volumes, including the system volume.

Include Free Space

Default: Off

On: Backs up all sectors on the volume, including those in the volumes free space.

Off: Backs up only sectors marked as currently containing data.

IO Throttle

Default: 100

Specifies, as a percentage, how much of the system's I/O subsystem you want ShadowProtect to use. To change this value, click-and-drag the slider control to the desired setting.

Enable Write Caching

Default: Off

On: ShadowProtect uses file caching when writing the backup image file, which might slow down the imaging process.

Off: ShadowProtect does not use file caching when writing the backup image file.

Mounting a Backup Image File

The ShadowProtect Explore Backup Wizard guides you through the process of mounting a backup image file to browse and restore files and folders. ShadowProtect automatically associates the files required to browse and restore a specific backup image file. You need only select the backup image you want to explore.

While the process is the same, whether you can restore files and folders in Windows, or need to use the StorageCraft Recovery Environment, depends specifically on what you need to restore:

- Windows: Windows loads, but you have lost data or had undesirable changes to applications or hardware files on a volume (excluding the operating system files).
- Recovery Environment: Windows does not load and you have lost data or operating system files, or had undesirable changes to applications or hardware files on a volume. For more information, see the [_Backup Image File Mount Options](#)

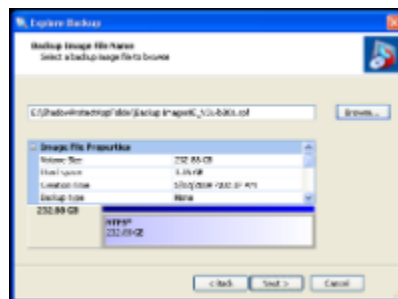
For information about mount options, see [Backup Image File Mount Options](#).

To restore files and folders

1. Start the ShadowProtect Console (see [Starting ShadowProtect IT Edition](#)).
2. Open the Explore Backup Wizard by doing one of the following:
 - In the Wizards tab, click Browse and Restore Files Wizard.
 - In the Tasks menu, click Explore Backup Image.
3. In the Backup Image File Name page, browse to the image file you want to browse, then click Next.



Note: If the backup image is encrypted you must provide the appropriate password. The Explore Backup Image Wizard displays a categorized list of information about the backup image file.



Select Backup Image File to Browse

4. (Conditional) In the Backup Image Dependencies page, select the desired point-in-time image from the selected backup image set, then click Next.
5. In the Explore Options page, select how you want to mount the backup image.
6. Mount the backup image as a Drive Letter or Mount Point. For more information, see [Backup Image File Mount Options](#).
 - Drive Letter: Select Assign the following drive letter, then select the appropriate drive letter from the dropdown list.
 - Mount Point: Select Mount in the following empty NTFS folder, then browse to the appropriate NTFS folder. Select how you want to name the mount point sub-folder:
 - Time/Date: Uses the backup image's creation date and time as the subfolder name (for example, 7-12-2008 10.19.24 AM).
 - File Name: Uses the backup image file name as the subfolder name (for example, E_VOL_b001).
 - Custom: Lets you specify a custom subfolder name.
7. (Optional) Deselect Mount Backup as Read-Only to mount the backup image as a writeable volume, then click Next. For more information, see [Backup Image File Mount Options](#).
8. In the Wizard Summary page, review the mount information, then click Finish. ShadowProtect mounts the backup image file, then automatically launches Windows Explorer and displays the mounted volume.

Dismounting a Backup Image File

Once mounted, a backup image file remains mounted until explicitly dismounted, or the system reboots. The ShadowProtect Backup Image Dismount Wizard guides you through the process of dismounting a previously mounted backup image file (see [Mounting a Backup Image File](#)). As part of the dismount process, you can do the following:

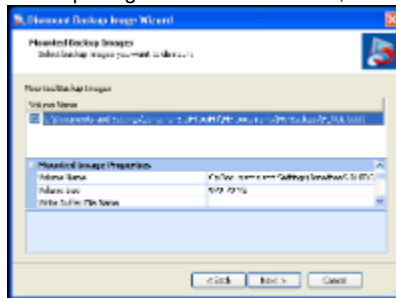
- Save changes to writeable backup images.
- Shrink the volume so you can restore the image to a smaller drive.



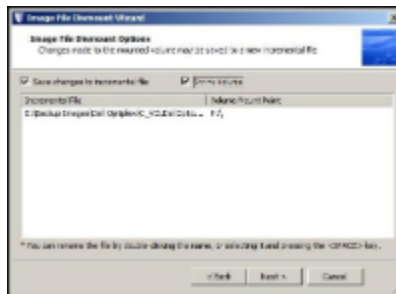
Note: The Shrink Volume feature truncates mounted backup image so that the file system ends at the last currently-allocated cluster. To reduce the backup image size as much as possible, use a disk defragmentation tool on the mounted image to consolidate file distribution within the volume and free up space at the end of the volume.

To dismount a backup image

1. Start the ShadowProtect Console (see [Starting ShadowProtect IT Edition](#)).
2. Open the Backup Image Dismount Wizard by doing one of the following:
 - In the Tasks menu, click Dismount Backup Image. In the Mounted Backup Images page, select the backup image volume to dismount, then click Next.
 - In the Tasks menu, click Dismount Backup Image.
 - In the Disk Map, right-click a mounted backup image, then select Dismount Backup Image.
3. In the Mounted Backup Images page, select the backup image volume to dismount, then click Next.



4. (Conditional) In the Backup Image Dismount Options page, select if you want to Save volume changes, or Shrink the backup Image, then click Next.



These options are available only if the backup image volume is writeable (see [Backup Image File Mount Options](#)).

Save changes to incremental file: Saves changes made to the mounted volume. Right-click the Incremental File to save the modified backup image file using a different name.

Shrink Volume: Lets you shrink the volume so you can restore this image to a smaller hard drive. This option is available in the following situations:

- Dismounting a writeable backup image of an NTFS volume in Windows Vista or Windows Server 2008 (or later).
- Running StorageCraft Recovery Environment using boot option 1 (Recommended), which boots using Windows PE (Vista-based).

5. In the Backup Image Dismount Summary page, review the dismount details, then click Finish.

Backup Image File Mount Options

When mounting a backup image file, consider the following:

- Whether to mount the backup image as a drive letter or at a mount point location.
- Whether to mount the backup image as read-only or writeable.

Mounting a Backup Image as a Drive Letter

The ShadowProtect Mount Utility lets you mount a backup image file as a drive letter on your computer with all the properties of the original volume.

After mounting a backup image as a drive letter, you may perform a variety of tasks, such as running ScanDisk (or CHKDSK), performing a virus check, defragmenting the drive, copying folders or files to an alternate location or simply viewing disk information about the drive such as used space and free space.

When a drive is mounted, you may set it up as a shared drive. Users on a network can connect to the shared drive and restore files and folders from within the backup image if you want end users to recover their own files. You also may mount one or more backup images at a time. The drives will remain mounted until you dismount them or restart the machine. If an NTFS volume uses EFS (Encrypted File System), the security remains intact on the volume when it is mounted.

Mounting a Backup Image as a Mount Point

The ShadowProtect Mount Utility lets you mount a backup image file as a mount point (a directory on an NTFS file system). Mount points overcome the available drive letter limitation and support more logical organization of files and folders.

Mounting a Read-Only Backup Image

By default, ShadowProtect mounts backup image files as read-only. This lets users access the backup image to do the following:

- Recover files from an existing backup image.
- View the contents of a backup image.
- Run other applications that need to access the backup image, such as a storage resource manager or data mining application.



Note: Windows 2000 does not support read-only NTFS volumes.

Mounting a Writeable Backup Image

ShadowProtect can mount a backup image as writeable volume. This lets users access the backup image to do the following:

- Remove files from the backup image (viruses, malware, etc.)
- Add files to the backup image.
- Update the backup image security.
- Restore a backup image to a smaller volume (see [Dismounting a Backup Image File](#)).



Note: ShadowProtect prevents you from modifying a Base Image File to prevent corruption of an entire backup image file set.

Restoring a Volume

The ShadowProtect Restore Wizard guides you through the process of restoring an entire volume from a backup image file. While the process is the same, whether you can restore a volume in Windows, or need to use the StorageCraft Recovery Environment, depends on the type of volume you need to restore:

Windows: Restore a non-system volume. This method does not require you to reboot the system.

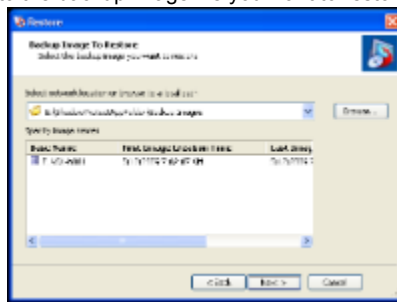
Recovery Environment: Restore any volume (system or non-system). You must reboot the system to start Recovery Environment. For more information, see the StorageCraft Recovery Environment User Guide.



Note: To restore a volume, you must first create a backup image of the volume. For more information, see [Creating a Backup Image File](#).

To restore a volume

1. Start the ShadowProtect Console (see [Starting ShadowProtect IT Edition](#)).
2. Open the Restore Wizard by doing one of the following:
 - In the Wizards tab, click Restore Wizard.
 - In the Tasks menu, click Restore Volume.
3. In the Backup Image to Restore page, browse to the backup image file you want to restore, then click Next



If you have saved backup image files to a network share, you might need to use the Network Configuration tool to map to a network drive. You must have network rights to the backup image file.



Note: If the backup image is encrypted you must provide the appropriate password.

The Explore Backup Image Wizard displays a categorized list of information about the backup image file.

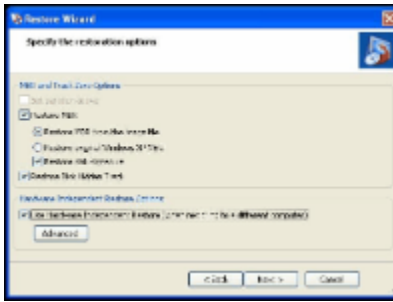
4. In the Backup Image Dependencies page, select the desired point-in-time image from the selected backup image set, then click Next. Select a backup image file to view the following properties about the backup image file set. The image file properties helps you determine the best backup image file to restore.
5. In the Restore Destination page, select the location where you want to restore the backup image, then click Next. Restoring a backup image to a volume overwrites all data currently on the volume. You must have enough space to restore the backup image. For example, you cannot restore a 4GB backup file with only 2GB of free space.

Right-click a volume entry to do the following:

- **Delete Volume:** Deletes the selected volume. The deleted volume will become unassigned space on the disk that can be repartitioned.
- **Set Active:** Set the volume active. Only one partition may be designated as active. By setting a volume active, the computer will boot to the volume.
- **Create an exact primary partition:** (Available only if unpartitioned disk space exists) Create a primary partition on the disk. You cannot create more than four (4) primary partitions on a disk.
- **Create extended partition:** (Available only if unpartitioned disk space exists) Create an extended partition and divide it into one or more logical partitions.
- **Edit boot.ini:** View and modify the `boot.ini` file.
- **Edit Policy:** Opens the Partition Creation Policy Editor.

6. In the Specify the Restoration Options page, select appropriate volume restoration options, then click Next.
For more information, see [Volume Restore Options](#).
7. In the Wizard Summary page, review the volume restore job, then click Finish.
View the progress of the volume restore job in the Volume Restore tab.

Volume Restore Options



The Restore Wizard provides the following options when restoring a volume:

- Set Partition Active: Configures the restored volume as the active partition in the system (the drive the machine boots from).
- Restore MBR: Restore the master boot record (MBR) as part of the volume restore job. The master boot record is stored in the first sector of the first physical hard drive, and contains the master boot program and partition table. The master boot program uses the partition table to determine the active partition, then starts the boot program from the boot sector of the active partition. When selected, you have the following MBR restore options:
 - Restore MBR from the image file: Restores the MBR from the backup image file.
 - Restore original Windows XP MBR: Restores the default MBR that ships with Windows XP.
 - Restore disk signature: Restores the original hard drive physical disk signature. Windows Server 2003, Windows 2000 Advanced Server, and Windows NT Server 4.0 Enterprise Edition (SP3 and later) require disk signatures to use the hard drive.
- Restore Disk Hidden Track: Restores the first 63 sectors of a drive. Some boot loader applications require this for the system to boot.
- Use Hardware Independent Restore: (Recovery Environment only) Lets you restore a volume to a different hardware environment from which it was created, either physical or virtual. For more information, see "Using Hardware Independent Restore" in the StorageCraft Recovery Environment User Guide.

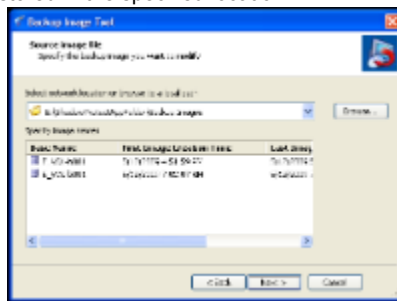
Using Image Conversion Tool

The Image Conversion Tool lets you do the following:

- Change the compression setting on an existing image.
 - Change the encryption setting on an existing image.
 - Split an image into multiple files (a Spanned set) where each file has a maximum file size. This is useful for moving image files to CD or DVD.
 - Consolidate a Base Image File and any Incremental Image Files into a new Base Image File.
- You can access the Image Conversion Tool from either Windows or the StorageCraft Recovery Environment.

To use the Image Conversion Tool

1. Start the ShadowProtect Console (see [Starting ShadowProtect IT Edition](#)).
2. In the Tools menu, click Image Conversion Tool.
3. In the Source Image File page, browse to the location of the backup image files you want to modify.
4. ShadowProtect displays the Base Image Files stored in the specified location

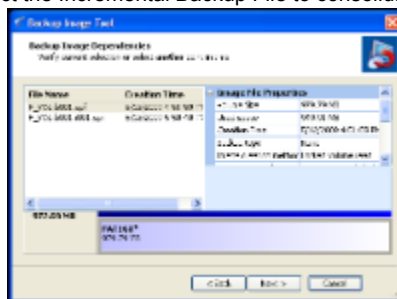


5. Select the Base Image File to work with, then click Next.



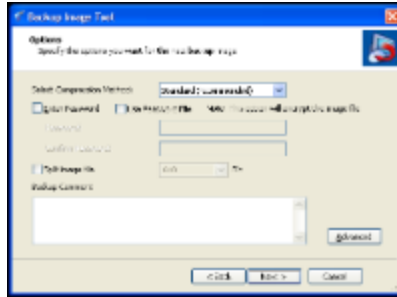
Note: If the backup image is encrypted you must provide the appropriate password.

6. In the Backup Image Dependencies page, select the Incremental Backup File to consolidate with the Base Image File, then click Next



Select a backup image file (left pane) to view its properties (right pane), including:

- Originating machine: The operating system version, the machine name, MAC address and the engine version of ShadowProtect used to create the image file.
 - Disk Information: Disk geometry, disk size and number of the first track sectors. You can view the original disk layout in graphical form at the bottom of the screen.
 - Original Partition Information: Style, number, type, bootable option, starting offset and length.
 - Image File Properties: Volume size, creation time, compression, password protection, comment.
7. In the Destination Image File page, specify the location and name of the new backup image file, then click Next. You can save the new backup image file locally or to a network drive.
 8. In the Backup Wizard Options page, specify the desired backup image file options, then click Next



For information about each of these options, including the Advanced options, see [Options](#).

9. In the Wizard Summary page, review the Image Conversion Tool job summary, then click Finish.
Monitor the progress of the Image Conversion Tool job in the Backup Jobs tab (select the job, then click Details. Review the results of previously executed jobs in the Backup History tab.

Other Operations

ShadowProtect IT Edition supports the following additional operations:

- Deleting Backup Image Files
- Verifying Backup Image Files

Deleting Backup Image Files

You can delete backup image files as you would any other file in the file system. However, before deleting backup image files, make sure that none of them are required for any active backup jobs, or that other backup image files depend on the backup images. Use the Image Conversion Tool to scan for image file dependencies (see [Using Image Conversion Tool](#)).



Warning: Deleting a backup image file that has dependencies ruins the dependent backup image files. You can no longer browse and restore files from the dependent backup image files.

Verifying Backup Image Files

On a regular basis, you should verify the quality and integrity of backup image files. This helps ensure that backup image files are ready when needed. One way to do this is to mount a backup image and confirm that you can browse the files and folders (see [Mounting a Backup Image File](#)). However, ShadowProtect provides a utility for verifying the integrity of backup image files.

To use the verify image wizard

1. Start the ShadowProtect Console (see [Starting ShadowProtect IT Edition](#)).
2. In the Tasks menu, select **Verify Backup Image**.
3. In the **Specify Verify Options** page, browse to the image file you want to verify, then click **Next**.
4. In the **Specify The Verify Options** page, select the appropriate verify option, then click **Next**.
 - **Verify only selected image:** Verifies only the currently selected backup image file.
 - **Verify selected image and all dependent files:** Verifies the currently selected backup image file, and any files dependent on the selected file. If you select this option, specify the file order you want the **Verify Image Wizard** to use.
5. In the **Wizard Summary**, review the verify job, then click **Finish**.

Best Practices

- Test the StorageCraft Recovery Environment. Make sure the ShadowProtect IT Edition CD lets you boot your system and gain access to both any local drives and network devices that you might need.
- Monitor disk space usage where images are stored. Make sure your backup image file storage location has sufficient disk space for new backup image files, or backup jobs will fail.
- Monitor the ShadowProtect log files. Routinely examine the ShadowProtect log files. The log files will provide status of backup jobs, letting you know the backup jobs were completed successfully or if the backup jobs failed. If the backup job failed, the log files will provide details of the failure allowing you to take action to correct the situation.
- Backup the system and data to disk first. Then copy the backup image files to any subsequent storage systems, such as tape backup software.
- Use password encryption to protect backup image files. Since ShadowProtect backup images include all the contents of the disk drive, use password encryption to help protect data security.
- Include multiple volumes in your backup job. If you have databases or applications that span volumes, include all relevant volumes in the backup image file. ShadowProtect snapshots can operate simultaneously on multiple volumes, thereby ensuring cross-volume consistency.
- Periodically save backup image files on a removable hard drive. CD, DVD, and Blue-Ray storage lets you easily store backup image files at an off-site location. This helps ensure available backup images in the case of a disaster.
- Use the Image Conversion Tool to manage backup images. You can consolidate backup images, split backup images for CD or DVD storage, and apply new password encryption to existing backup image files in the event passwords are compromised.
- Specify drivers for Hardware Independent Restore (HIR). If an HIR restore fails, use the Advanced options to add hardware-specific drivers. This improves the likelihood of a successful restore to different hardware.

Product Support

Technical support for StorageCraft products is available beginning with the release of the product and ending six months after the release of the next major version of the product or after StorageCraft discontinues the product line.

Complimentary Technical Support

StorageCraft complimentary technical support consists of self-help support tools that are available at <http://forum.storagecraft.com/Community/> (in English only), and an easy-to-use, powerful knowledge base that helps you find answers to the most frequently asked product questions, as well as "how-to" procedures and technical information about all StorageCraft products.

E-Mail Support

Requests for e-mail support in North America are processed 8:00 am to 5:00 pm MST, Monday through Friday. To obtain e-mail technical support for specific technical questions or issues, fill out the form at <http://forum.storagecraft.com/Community/>. Please provide as much detail as possible to help the technical support engineers understand and diagnose the issue.

In order to ensure efficient service, please provide at a minimum the following information:

- Product name and version number
- Detailed problem description, error code, log file description, etc.
- Hardware and software configuration, operating system version, service pack number, etc.

Telephone Support

StorageCraft support engineers are available Monday through Friday 9:00 A.M. to 5:30 P.M. (MST), except for business holidays. To reach the StorageCraft technical support team, please call: (801) 545-4710. Telephone support is available to all customers with a current maintenance plan or customers who have purchased product maintenance from the StorageCraft Web store. If you are not immediately connected to a support engineer, leave a message and the next available support engineer will return your call.

Glossary

Backup: The activity of copying files, volumes, and databases to preserve them in case of equipment failure or other catastrophe. An important part of a disaster recovery strategy, backup is often neglected, particularly for personal computer users.

Backup Image File: Files that contain the contents of a backup activity, Backup Image Files let you restore the contents of a computer system to a specific point-in-time.

Bare Metal Recovery: The complete restoration of computer data after a catastrophic failure, including the operating system, file system, partitions, volumes and data, from a complete backup image.

Base Image File: Backup files that contain a copy of all used sectors on a disk drive. This image file contains all data on the computer, including the operating system, applications, and data.

Basic Disk: A physical disk drive that can be accessed by MS-DOS* and all Windows* operating systems. Basic disks can contain up to four primary partitions, or three primary partitions and an extended partition with multiple logical drives.

Cold Backup: A backup taken from the Recovery Environment, rather than when the computer's operating system is loaded.

Continuous Incrementals: A backup scheduling model for ShadowProtect that lets you create a base backup file, then create additional incremental backup files that include only changes that occurred since the last backup.

Compression: A technology that reduces the size of a file. Compression lets you save time, bandwidth and storage space.

Differential Image File: Backup files containing the hard drive sectors that have changed since the Base Image File was created. Differential image files take about the same time to create as Base Image Files, but they are smaller. When restoring a drive (or files and folders), you must use the Base Image File with the appropriate Differential Image File to restore the computer to a specific point-in-time.

Disaster Recovery: The ability to recover from the complete loss of a computer, whether due to natural disaster or malicious intent. Typical disaster recovery strategies include replication and backup/restore.

Disk Device: A locally accessible disk drive, including locally attached USB or FireWire disk drives, and network drives such as SAN, NAS, iSCSI, SCSI, USB or FireWire.

Driver: A program that interacts with a particular device or software. The driver provides a common interface to the device, or software, that makes it accessible to other computer systems and the user.

Drive Letter: See Mount as Drive Letter.

Dynamic Disk: A physical disk that provides features that basic disks do not (see Basic Disk), such as support for volumes spanning multiple disks. Dynamic disks use a hidden database to track information about dynamic volumes on the disk and other dynamic disks in the computer.

Encryption: A procedure that renders the contents of a file unintelligible to anyone that cannot present the appropriate decryption key.

ExactState Imaging: The ability to create a backup image at a point where the computer is in the best state for creating a backup (for example, no open files).

Full Image File -- See Base Image File.

Hard Drive: An electromagnetic storage device, also referred to as a "disk drive," "hard drive," or "hard disk drive" that stores and provides access to data on a computer.

Head Start Restore (HSR): The ability to begin the restoration of a large backup image chain while ShadowProtect continues to add Incremental backup image files to the same image chain. This reduces the time necessary to restore a large volume from days or weeks, to minutes or just a few hours.

Hot Backup: A backup image taken when ShadowProtect is loaded on the computer's standard operating system. A hot backup requires the use of a snapshot filter driver (see Snapshot).

Hot Restore: The restoration of a backup image while the computer or server remains up and running. You cannot perform a hot restore of a system volume.

Image or Image File: See Backup Image File.

Image Set: The combination of a Full image and all additional Incremental images necessary to restore a computer to a given point-in-time.

Incremental Image File: Backup files containing the sectors that have changed since the last Incremental backup was taken. Incremental Images are fast to create and smaller than either Base Image Files or Differential Image Files. When restoring a drive (or files and folders), you must use the Base Image File and the appropriate Incremental Image Files necessary to restore the computer to a specific point-in-time.

Lock Volume: A software request to gain exclusive access to a particular drive. Locking the volume prevents other software programs from changing the file system or opening files during the process of writing the image file.

Microsoft VolSnap: The proprietary Microsoft snapshot technology.

Microsoft Volume Shadow Copy Service (VSS): The backup infrastructure for Microsoft Windows XP and Microsoft Windows Server 2003 operating systems, as well as a mechanism for creating consistent point-in-time copies of data. The Volume Shadow Copy Service produces consistent snapshots by coordinating with business applications, file-system services, backup applications, fast-recovery solutions, and storage hardware.

Mount as Drive Letter: The process of assigning volumes (active primary partitions and logical partitions) to specific letter designators in the root namespace of a Microsoft operating system. Unlike mount points (see Mount Point), drive letter assignment permits only letters in the namespace, and they solely represent volumes. In other words, it is a process of naming the roots of the "forest" that represents the file-system (with each volume being an independent tree therein).

Mount Point: A directory on a volume that an application can use to "mount" (set up for use) a different volume. Mount points overcome the limitation of drive letters (see Mount as Drive Letter) and allow for more logical organization of files and folders.

Mounted Volume: The ability to see and use a backup image that is physically located somewhere else on the network. When mounted, the backup image appears as a volume and behaves as if it is a part of the local computer system. Mounted volumes are read/write capable so users can update existing image files, scan for viruses or other malware, and repair the image file.

Operating System: Software that, after being loaded into the computer by a boot program, manages all other programs on a computer. Other programs are called applications or application programs.

Partition: The portion of a physical disk that functions as though it were a physically separate disk. Once created, a partition must be formatted and assigned a drive letter before data can be stored on it. On basic disks, partitions can contain basic volumes, which include primary partitions and logical drives. On dynamic disks, partitions are known as dynamic volumes and come in the following types: simple, striped, spanned, mirrored, and RAID-5 (striped with parity) volumes.

Restoring: The activity of retrieving computer data from a previously saved backup image file.

Snapshot: A type of backup that provides a point-in-time view of a volume. When you perform a backup or scheduled backup, ShadowProtect uses either StorageCraft Volume Snapshot Manager (VSM) or Microsoft Volume Shadow Copy Service (VSS) to take a snapshot of the volume. Any changes that occur to the volume after the snapshot is taken are not included in the backup.

.spf: A file extension representing a ShadowProtect full or base image file.

.spi: A file extension representing a ShadowProtect incremental or differential image file.

.sp(number): A file extension representing a ShadowProtect image file that spans multiple files. The number following .sp is the sequence of the file in the spanned image file group.

Point-In-Time Backup: A backup routine that lets you restore a file, folder, or the entire system to a specific point-in-time. Point-in-time backups are often used to roll-back a computer to a point prior to a computer problem.

Protected Volumes: Volumes that users have selected for backup by ShadowProtect.

RAID: Redundant Array of Independent Disks. A collection of disk drives that offers increased performance and fault tolerance. There are a number of different RAID levels. The three most commonly used are 0, 1, and 5:

- Level 0: striping without parity (spreading out blocks of each file across multiple disks).
- Level 1: disk mirroring or duplexing.
- Level 5: block-level striping with distributed parity.

Real-Time: A level of computer responsiveness that a user perceives as essentially immediate, or that enables the computer to keep up with some external process such as backing up.

Recovery Environment: See StorageCraft Recovery Environment.

Remote Computer (Node): A computer that is physically located somewhere else on a network but is accessible from a local computer.

Service: A program, routine, or process that performs a specific system function to support other programs, particularly at a low (close to the hardware) level.

Scheduled Job: A job created in the ShadowProtect interface. Scheduled jobs let ShadowProtect backup events to occur automatically.

Spanned Image Set: A Backup Image File that has been divided into multiple smaller files for easier management or storage. This lets you save the Backup Image File to removable media such as a CD or DVD.

StorageCraft Recovery Environment: A secondary boot environment (or operating system) that gives a user the functionality necessary to access and restore Backup Image Files on a network. This environment is typically used when a drive cannot be restored from within Windows or when the computer has suffered a catastrophic failure and the entire hard drive must be restored.

System downtime: The amount of time a server or PC is offline and inaccessible to users. This is commonly known as having the system out of production.

System Volume: The volume that stores the boot files necessary to load an operating system. Typically, this is the C:\ volume.

Tray Icon: A graphical representation of a computer program or application. For example, ShadowProtect uses a tray icon for the user to gain information about the program. Tray icons reside in the system tray.

UNC (Universal Naming Convention): A method used to identify folders, files and programs on a network computer. A UNC path begins with two backslashes followed by the server name, share name, directory and filename. For example, \\server_name\share_name\backup_name.spi.

Unprotected Volumes: Volumes not protected by ShadowProtect.

User Interface (UI): The portions of a computer system with which a user interacts (display, keyboard, mouse, etc.) and the portion of a software program that accepts and responds to user interaction.

Virtual Private Network (VPN): A private data network that makes use of the public telecommunication infrastructure. VPNs maintain privacy through the use of tunneling protocols, encryption, and other security procedures.

VirtualBoot: The ability to create a Virtual Machine based on an existing backup image chain. Once started, the VM provides complete access to data, applications, and services provided by the original system, in a state corresponding with the last Incremental image included in the VM.

Virtual Volume: A locally referenced volume that does not physically exist on the system. ShadowProtect uses virtual volumes for the benefit of protecting computer systems.

Volume: An area of storage on a hard disk. A volume is formatted by using a file system, such as file allocation table (FAT) or NTFS, and typically has a drive letter assigned to it. A single hard disk can have multiple volumes, and volumes can also span multiple disks.

VSS Aware: An application designed to work with Microsoft Volume Shadow Copy Services (VSS) framework to ensure consistent data backup.