ShadowProtect User Guide

Table of Content

ShadowProtect User Guide

Welcome to the StorageCraft® *ShadowProtect® User Guide*. This Guide describes the ShadowProtect technology, how to use the product, and how to derive maximum benefit from ShadowProtect. ShadowProtect comes in multiple editions. While most differences between ShadowProtect editions relate to the associated user license, this Guide specifically identifies information that applies to a specific edition.

Edition	Description
ShadowProtect Desktop	Provides volume backup and restore options for a single desktop system. This edition is most suitable for home use.
ShadowProtect Server	Provides backup and restore options for server operating systems. A separate license is required for each installed Windows OS.
ShadowProtect SBS	Provides backup and restore options for Microsoft Small Business Server (SBS). A separate license is required for each installed Windows OS.
ShadowProtect MSP	Provides a subscription-based licensing model for Managed Service Providers (MSP) that want to provide disaster recovery solutions for their clients.
ShadowProtect Virtual	Provides a VM-based licensing model for disaster recovery in a virtualized environment.

This Guide includes the following major sections:

Additionally, this Guide includes the following general information sections:

Additional Information

- For emerging issues and other resources, see the following:
  - The `readme.txt` file included with the ShadowProtect 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

⚠ This symbol designates **Note** or **Warning** text that highlights important information about the configuration and/or use of ShadowProtect.

1 ShadowProtect Overview

ShadowProtect provides robust and flexible disaster recovery by creating, managing and restoring from backup image files. A 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	ShadowProtect
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	

Review these topics as you prepare to install and use ShadowProtect:

- Features and Components
- Usage Scenarios

1.1 Features and Components

For a complete version history of product updates, refer to the online ReadMe document.

Component	Features
ShadowProtect Console	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: • 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 mount any backup image file as a virtual disk in the Oracle VirtualBox virtual machine environment.
ShadowProtect Backup Agent	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. ⚠ **Note:** To access the ShadowProtect Backup Agent, you must be a user with local administration rights.
StorageCraft Recovery Environment	A bootable Windows environment for disaster recovery which doesn't require installing software. For more information about the Recovery Environment, see the *StorageCraft Recovery Environment User Guide*. • 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	ImageManager provides policy-driven services for managing backup image files. For more information about ImageManager features, see the *ShadowControl ImageManager User Guide*. • 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, intelligentFTP, or ShadowStream). • 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 or hardware migration tasks.

1.2 Usage Scenarios

ShadowProtect offers a variety of backup and recovery solutions, depending on your needs. This section includes several usage scenarios organized into the following types:

- ShadowProtect Console Scenarios
- VirtualBoot Scenarios

ShadowProtect Console Scenarios

Here are several common use cases for ShadowProtect:

Live Backup

Problem: I don't want to shutdown a system every time I want to create a system backup image.

ShadowProtect Solution: By leveraging disk imaging with existing Windows snapshot technology, ShadowProtect lets you 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.

Create Full and Incremental Backup Images

Problem: Making a full backup image every time I backup a system is very time consuming. I need to be able to make incremental backup images to save time and space.

ShadowProtect Solution: ShadowProtect uses a sector-based backup strategy that lets it backup just the changes to a file in an Incremental backup image. Sector-based incremental backup is the quickest and most efficient way to take an incremental backup. Once you have an initial Full backup, you can create regular Incremental backup images from that point forward to support an accurate restoration.

Individual Folder and File Restore

Problem: Restoring individual files and folders traditional backup systems, such as a tape drive, can be very difficult and time-consuming...assuming I can even find the necessary data in the first place. I need a quick and easy method to recover lost files or folders.

ShadowProtect Solution: Use the ShadowProtect Backup Explore Wizard to mount a backup image file as a volume using a Drive letter or mount point. Once mounted, you can explore and recover individual files and folders from the backup image. Disk-based backup images provide fast file access, and you can even share backup images so Since the backups are disk-based, the process is very fast and easy and uses Windows Explorer. The IT administrator can mount a backup image and share this with end users who can select the files and folders they need to restore.

Update an Existing Backup Image

Problem: I have an existing backup image, but need to update a driver in that image, or clean a virus or other malware from the backup image before restoring files. I don't want to have to clean the system, then re-create the backup image before using it to restore a system.

ShadowProtect Solution: Because you can mount ShadowProtect backup image files as read/write volumes, you can modify and repair backup images as needed. ShadowProtect saves these backup image changes as a separate Incremental image file.

VirtualBoot Scenarios

The following scenarios introduce several possible use cases for VirtualBoot:

Historical Data Access

Problem: After transitioning to a new financial management system, you are audited. To satisfy the audit, you need access to historical tax records stored in the proprietary format of the old financial software. Unfortunately, you no longer have the old software, so you cannot access your historical tax records.

VirtualBoot Solution: Rather than trying to restore a complete backup image that contains the old financial software, use VirtualBoot to boot the backup image, which gives you access to both the application and the data from your system at the time of the backup. By preserving the applications with the data, you can greatly extend the lifespan of your data.

Software Testing

Problem: You need to find out how some new software performs on your production system, but you don't want to risk having any problems.

VirtualBoot Solution: VirtualBoot the latest backup of your production system, then install the software in the virtual machine. You can evaluate the software performance using your system's actual production environment without any risk to your production system.

Backup Image Testing

Problem: You need to confirm that your backup images restore properly and that they provide access to all your mission critical applications and data.

VirtualBoot Solution: VirtualBoot a recent backup image and you can verify that the restored applications and data perform as expected..

Hardware Failure

Problem: You have a database server and the 20TB disk array crashes. You need to get the system back on-line and replace the disk subsystem.

VirtualBoot Solution: This solution is a three-step process:

1. VirtualBoot the latest backup image of your database server so users can continue using the database. The interim VM solution performs well because there is no file conversion required. StorageCraft provides native support for its backup image files in the VirtualBox environment.
   As part of this process, configure ShadowProtect to continue creating Incremental backups in the VM, preferably every 15 minutes. These Incremental backups are part of the original backup image chain. ShadowProtect has VirtualBox store the VM-generated Incremental backups in native VDI files. While these files are relatively tolerant of VM host crashes, or VirtualBox.exe or VBoxSvc.exe process crashes, they might become corrupt and prevent the VM from restarting. If this happens, create a new VirtualBoot VM, using as the VM source the latest Incremental backup created in the prior VM.

   Warning: To continue uninterrupted Incremental backups in a VirtualBoot VM, the ShadowProtect backup job that creates the backup image files must use a ShadowProtect Destination Object of type Network Share (see Destinations).
2. Start a HeadStart Restore (HSR) on the database server's new disk subsystem (For more information, see the *ShadowProtect ImageManager User Guide*).
3. Once the HSR catches up to the most current Incremental, created in the VM, take the VM offline and finalize the HSR installation on the new disk subsystem (a quick operation), then bring the database server hardware back on-line.

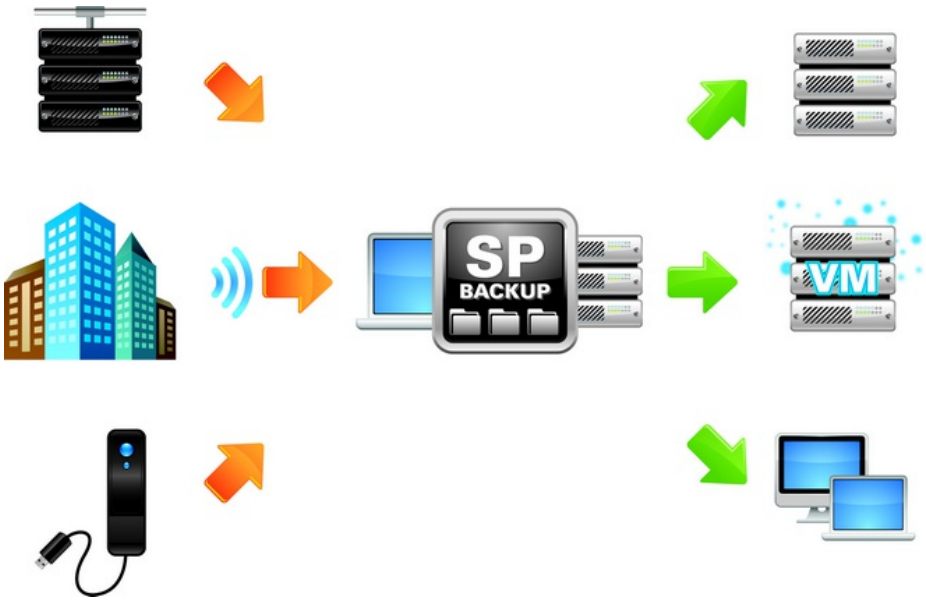
Note: Once the replacement VM is on-line and continuing the Incremental backup image chain, you can recover from a hardware failure in several different ways, including:

- Restore to the original hardware, once repaired.
- Restore to new hardware (using StorageCraft Recovery Environment's Hardware Independent Restore (HIR)).
- Restore permanently to a VM environment by using HSR to restore to a VHD or VMDK virtual machine hard disk file.

2 How ShadowProtect Works

ShadowProtect Backup and Restore - How it 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.



This section includes the following topics:

2.1 Create a Backup Image

Creating a ShadowProtect backup image involves two key processes:

Capture Snapshot of the Volume

Using Microsoft VolSnap and VSS (used 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 takes only seconds and does not interfere with system operation.

Snapshot	Supported OS	Image Speed	Quality	Comments
StorageCraft VSM with VSS	Windows XP / 2003 and later	Fast	Best	• 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 XP / 2003 and later	Slow	Best	• 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 files (see Glossary).

StorageCraft VSM direct	Windows 2000	Fast	Good	applications and improve backups. ⚠ **Note:** Windows 2000 does not support VSS.

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 Backup Image Files.

2.2 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 Backup Image Files.

Restore an entire volume

Use the ShadowProtect Restore Wizard to restore an entire volume from a backup image file. You can restore a system volume (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.

2.3 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 and does not rely on any other files.
Incremental .spi	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.

Spanned .sp_#_	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). The actual Spanned image file name replaces the pound sign (#) with a number that indicates the position of the file within the spanned Image Set.
ImageManager -cd.spi -cw.spi -cm.spi	Image files that have been automatically collapsed by ShadowProtect ImageManager. The suffix before the file extension indicates if the file is a daily, weekly or monthly collapsed backup files.
.spk	A password key file used to encrypt backup image files.
.spwb	A temporary "write-back" file used to save changes for a mounted image file volume.

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>_`

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`
`C_Vol-b001-d000-i000.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`
`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`.

*Backup image file names that include the "-d000" or "-i000" segment identifier indicate that the backup image file does not rely on any other Differential or Incremental backup image files.

File Dependencies

By examining the name of a backup image file, ShadowProtect users can identify the files on which it depends. 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 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.

3 Installing ShadowProtect

Before installing ShadowProtect, review the Requirements and the License and Install Options.

To Install ShadowProtect

1. If you have a ShadowProtect CD, insert the disc into the system's CD drive.
   If the installation does not start automatically, browse the ShadowProtect CD and run AUTORUN from the root of the CD.
2. If you have downloaded the ShadowProtect installer, click on the .EXE file to launch the program.
3. In the Setup Wizard, select the language you wish to install and click **Next**.
   Note: To register ShadowProtect, you must install the language that matches the license key you purchase.
4. On the Welcome page, click **Next**.
5. On the License Agreement page, select **I accept the terms of the license agreement**, then click **Next**.
   You must accept the license agreement to install ShadowProtect. Click **Print** to print out the License Agreement.
6. On the Installation Type page, select which type you want:

Complete	This installs all the ShadowProtect components
Custom	This option allows you to select which components to install.

7. In the Installation Location page, accept the default path or specify a new path to install ShadowProtect. Click **Next**.
8. If you chose the Custom install option, select the ShadowProtect components to install, then click **Next**.

Management Console	Installs the ShadowProtect management interface, which lets you manage ShadowProtect operations for this system, and remote systems if desired.
Backup Agent	Installs the ShadowProtect Backup agent, which lets you manage ShadowProtect operations on this system remotely.
Snapshot Driver	Installs the ShadowProtect VSS driver. This is required for optimal performance and data protection. It should only be deselected if the system needs to run non-VSS compliant software, such as some versions of Intuit QuickBooks.
Mount Services	Installs the ShadowProtect mount driver and adds the ability to mount and dismount a backup image file using the right-click menu in Windows Explorer.
VirtualBoot	Installs Windows Explorer integration for VirtualBoot.
SPDiagnostic Tool	Installs a tool that gathers detailed information about a ShadowProtect installation for use in troubleshooting issues for StorageCraft Support.

9. On the Ready to Install the Program page, click **Install**.The program completes the installation of ShadowProtect.
10. Click **OK** on the Reboot reminder page.
11. In the Installation Complete page, select **Yes, I want to restart my computer now**, then click **Finish**.
    If you cannot restart the computer immediately, select **No, I will restart my computer later**. However, you must restart the computer before attempting to use ShadowProtect.
12. Remove the ShadowProtect CD from the system's CD drive.

3.1 Requirements

ShadowProtect has the following hardware and software requirements:

- Hardware Requirements
- Supported Operating Systems
- Supported File Systems
- Supported Storage Media

Hardware Requirements

Hardware	ShadowProtect	Recovery Environment (RE)
CPU	300 MHz or higher Pentium-compatible CPU.	**Windows 2008 RE:** 1 GHz or faster. **Windows 2008 RE (Japan only):** 1.4 GHz (x64 processor) or 1.3GHz (Dual Core). **Windows 2003 RE:** 550 MHz or faster. Supports up to four processors per system.
Memory	The greater of 256 MB or the Operating System minimum.	**Windows 2008 RE:** 512 MB minimum. **Windows 2003 RE:** 256 MB minimum.
Hard Drive space	50 MB free disk space.	N/A
CD-ROM or DVD drive	Required.	Required.
Monitor	VGA or higher resolution.	VGA or higher resolution.

Supported Operating Systems

Specific Operating System support is dependent upon the edition of ShadowProtect that you have purchased. However, ShadowProtect supports both 32-bit and 64-bit versions of the operating system, where applicable.

Edition	Description

ShadowProtect Desktop Edition	• Windows XP Family, including:
	  ◦ XP Home
	  ◦ XP Professional
	• Windows Vista Family, including:
	  ◦ Vista Home Basic
	  ◦ Vista Home Premium
	  ◦ Vista Ultimate
	• Windows 7
	• Windows 2000 Workstation SP4 (Support for Hot Backup of the booted OS and Cold Backup from Recovery Environment.)

ShadowProtect Server Edition	• Window Server 2000 SP4 (Support for Hot Backup of the booted OS and Cold Backup from Recovery Environment.)
	• 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 Server 2008 (including R2) 32-bit x86 and 64-bit x64
	• Windows Server 2008 R2 Foundation
	• Windows Server 2008

ShadowProtect SBS Edition (Small Business)	• Small Business Server 2003 • Small Business Server 2008

Supported File Systems

ShadowProtect supports the following File Systems:

- FAT16
- FAT16X
- FAT32
- FAT32X
- NTFS
- 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)

Multi-Boot Environments

If your system has multiple boot partitions, install ShadowProtect on each of the bootable Windows partitions to guarantee that ShadowProtect recognizes changes to ShadowProtect-managed volumes from these secondary Windows environments. You do not need to activate ShadowProtect, but the snapshot driver (stcvsm.sys) must be available in each Windows partition.

The *snapshot driver* manages the fast incremental tracking in ShadowProtect. If you boot to an alternate OS environment where the snapshot driver is not loaded, ShadowProtect cannot track volume updates from that OS boot session. This means that your next Incremental backup misses any changes made from the alternate OS.

If one or more of non-Windows operating systems, such as Linux, can write to a ShadowProtect-managed volume, you can make sure ShadowProtect recognizes those changes by creating a script. This script should execute during the startup/logon phase of the non-Windows OS, and delete all VSM000.IDX (case-sensitive) files from the root directory of each ShadowProtect-managed volume. Removing these files forces stcvsm.sys, when your primary Windows volume boots, to use a Full Differential/Comparison backup, which captures any changes made to the volume from the non-Windows OS.

3.2 License and Install Options

StorageCraft provides the following ShadowProtect license options to help you in your decision-making process:

Purchased License: StorageCraft licenses ShadowProtect on a per-system basis (based on the number of systems for which you are making backups. For example, using ShadowProtect to backup 100 computers requires 100 licenses. Before using the Software, review the complete End User License Agreement (see http://www.storagecraft.com/legal).

Evaluation Version License: StorageCraft provides an Evaluation version of the ShadowProtect Software as a CD or ISO image file. With the Evaluation version, you can create backup image files of system and data volumes. You can also restore system and data volumes or specific files and folders. The Evaluation version includes the StorageCraft Recovery Environment, so you can restore system volumes with the Evaluation version. The Evaluation version expires and ceases to operate when the Evaluation period ends. Images created during the Evaluation period are fully compatible with the registered (purchased) version of the Software.

Trial Version License: StorageCraft provides a Trial version of the ShadowProtect software as a free download. With the Trial version, you can create backup image files of system and data volumes. You can also restore system and data volumes or specific files and folders. However, the Trial version expires and ceases to operate when the trial period ends. Images created during the trial period are fully compatible with the registered (purchased) version of ShadowProtect. However, you cannot restore the system volumes because StorageCraft Recovery Environment is not included with the Trial version.

ShadowProtect Virtual

ShadowProtect Virtual is a licensing model specifically designed for virtual environments. It allows you to purchase VM licenses for ShadowProtect in single- or multi-license bundles (3-pack, 6-pack, 12-pack, 24-pack, or 50-pack).

ShadowProtect Virtual offers the same features and functionality available in ShadowProtect at a price point more conducive to a virtualized environment.

Note: ShadowProtect Virtual licenses allow you to migrate or restore to a physical environment. However, once restored the virtual license does not permit ShadowProtect to continue making backups. You must use a standard ShadowProtect license to make backups in a physical environment.

ShadowProtect for Managed Service Providers

ShadowProtect for Managed Services Providers (SPMSP) is a subscription-based licensing option for Managed Service Providers (MSP) that want to provide disaster recovery services to their clients. MSPs should be aware of the following features related to ShadowProtect for Managed Services:

- SPMSP supports all types of Windows installations (Desktop, Server, SBS, etc.) using a single product installer.
- On a daily basis, SPMSP licenses "call home" to StorageCraft servers to confirm that these licenses are still active. Because of this, SPMSP requires Internet connectivity.
- An SPMSP license activation is valid for 30 days. As part of the "call home" process, SPMSP licenses auto-renew every 30 days unless one of the following occurs:
  - The MSP or StorageCraft explicitly deactivates the license.
  - The license stops calling home, in which case it automatically deactivates.
  - The StorageCraft MSP Licensing Console (http://msp.storagecraft.com) lets MSPs create and manage SPMSP licenses, including remotely deactivating licenses when needed.

3.3 Starting ShadowProtect

You can access ShadowProtect in two ways:

From Windows: Select **Start** > **All Programs** > **ShadowProtect** > **ShadowProtect.**

From Recovery Environment: Put the ShadowProtect CD in the system's CD-ROM drive, then boot the system. Make sure your system boot sequence is set to boot from the CD before the hard drive. For more information about loading and using Recovery Environment, see the *StorageCraft Recovery Environment User Guide*.

3.4 Activating ShadowProtect

When you purchase ShadowProtect, StorageCraft will provide you with both a product serial number and an Evaluation version of the purchased product. This Evaluation version is the same as other Evaluation versions of StorageCraft products. It provides you with 30 days of product access, during which time you must activate the product with the product serial number. If you do not activate the product within 30 days of installation, the product times out and stops functioning. (You can still activate the product after the end of the 30 days. However, any backup jobs you created will not run again until after you activate the product.) We recommend you activate the product upon installation.

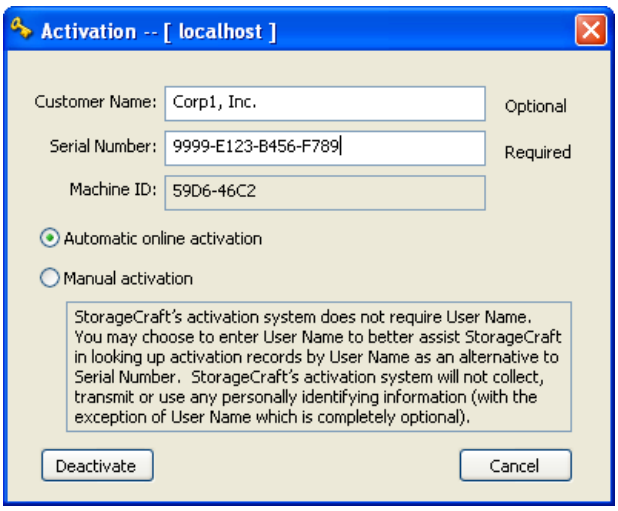
You can activate ShadowProtect in two ways:

- Automatic Activation
- Manual Activation

Note: You can also deactivate a previously activated ShadowProtect installation to free that product license for use on another system (see Deactivating ShadowProtect).

Automatic Activation

StorageCraft provides an activation server that you can use to quickly and easily activate your ShadowProtect installation.



To activate ShadowProtect automatically

1. Start ShadowProtect.
   For more information, see Starting ShadowProtect.
2. From the Menu Bar select **Help** > **Product Activation**.
3. In the Product Activation dialog box, provide the requested information, then click **OK**.
   Customer Name: (Optional) Specify the name of the product purchaser, either person or organization.
   Product Serial Number: Enter the serial number that you received when purchasing ShadowProtect.
4. ShadowProtect notifies you if the activation process was successful.
   1. If the activation is successful, click **Close**.
   2. If the activation was not successful, review the message to determine why the activation was unsuccessful. To correct the problem, do one of the following:
      1. Review the information in the Product Activation dialog box for accuracy. Correct any errors, then **OK** to resubmit the activation request.
      2. If your computer cannot successfully communicate to the activation server or the Internet, wait for a while and try the activation process again.. You can also try using a manual activation option.
      3. If you exceed the number of allowed activations for the serial number, you must purchase additional licenses. If you feel you received this message in error, contact StorageCraft Support (see Product Support.)

For all other activation issues, also contact StorageCraft Support (see Product Support.)

Manual Activation

If for some reason you are unable to use the automated activation method, StorageCraft provide the following manual options for activating your ShadowProtect installation. These manual options require you to receive the activation key and manually apply it to your ShadowProtect installation.

To get an activation key

1. Use one of the following methods to contact StorageCraft and request an activation key.
   Online: Open a Web browser to http://www.storagecraft.com/product_activation.php.
   Email: Request an activation key from StorageCraft Support (support@storagecraft.com).
   Phone: Call StorageCraft Support (see Product Support).
2. Provide the information required to generate an activation key.
   Product Serial Number: Enter the serial number that you received when purchasing ShadowProtect.
   Machine ID: ShadowProtect generates the Machine ID during the installation process. You can view the Machine ID in the ShadowProtect Activation dialog box (select **Help** > **Product Activation**).
   Version: The ShadowProtect version you installed. You can view this by selecting **Help** > **About**.
   Language: The product language you are using (English, Japanese, French, or German).
3. When you receive the activation key, continue with **To activate ShadowProtect manually**.
   Depending on the method used to request the activation key, StorageCraft will deliver it to you either in a Web form or via an Email where you can copy and paste it into your ShadowProtect installation.

To activate ShadowProtect manually

1. Start ShadowProtect.
   For more information, see Starting ShadowProtect.
2. From the Menu Bar select **Tools** > **Product Activation**.
3. In the Activation dialog box, select **Manual activation**.
4. In the Activation Key field, type or copy the activation key, then click **Activate**.

Deactivating ShadowProtect

When retiring a system, you can deactivate the ShadowProtect license to make the license available for use on another system.

To deactivate a ShadowProtect license

1. Start ShadowProtect.
   For more information, see Starting ShadowProtect.
2. From the Menu Bar select **Help** > **Product Activation**.
3. Click **Deactivate**.
   ShadowProtect displays a message stating you can no longer use this product key on this machine
4. Click **OK**.

3.5 Uninstalling ShadowProtect

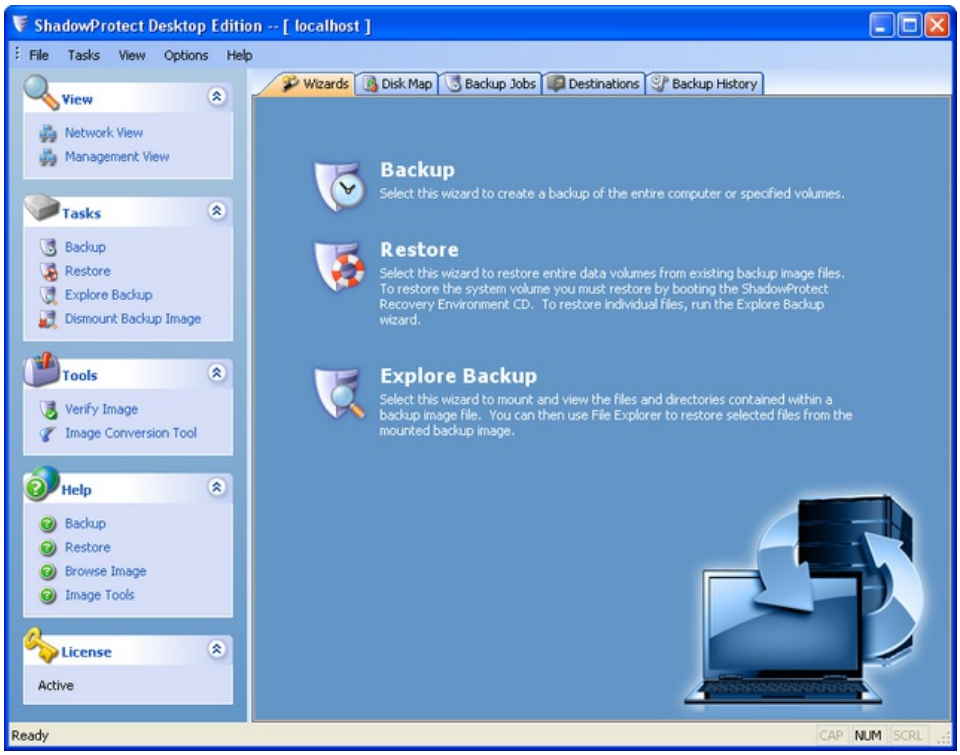
Use the standard Windows application removal tool to uninstall ShadowProtect.

To uninstall ShadowProtect

1. In Windows, select **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**.
2. Select ShadowProtect 4.x, then click **Remove**.
3. Click **Yes** to complete the uninstall.
   After uninstalling ShadowProtect, you must reboot the computer for the changes to take effect.

4 Understanding ShadowProtect Console

ShadowProtect Console provides access to most configuration and operation controls for ShadowProtect:



The console is divided into three panels:

Navigation Panel: Located on the left side of the console, the Navigation panel provides access to the tasks and tools necessary to configure and operate ShadowProtect. For more information, see Navigation Panel.

Main Panel: Located in the center of the console, the Main panel contains tabbed views of ShadowProtect tasks and information. For more information, see Tabs.

Network Panel: Located on the right side of the console, the Network panel, or Network View, provides access to the remote management features in ShadowProtect. For more information, see Remote Management.

4.1 Menu Bar

ShadowProtect Console has a menu bar that includes the following menus:

Menu	Description	Options
File	Access application-level options.	**Exit:** Close the ShadowProtect UI.
Tasks	Access ShadowProtect Wizards.	**Backup:** Launches the Backup Wizard (see Create a Backup Image). **Restore:** Launches the Restore Wizard (see Restoring a Volume). **Explore Backup:** Launches the Explore Backup Image Wizard (see Mounting Backup Image Files). **Dismount Backup Image:** Launches the Backup Image Dismount Wizard (see Dismounting Backup Image Files). **Verify Image:** Launches the Verify Image Wizard (see Verifying Backup Image Files). **Image Conversion Tool:** Launches the Image Conversion Tool Wizard (see Image Conversion Tool). **Add Destination:** Opens the Destination dialog box where you can create named destinations for backup image files (see Destinations). **Refresh Volume Info:** Refreshes the ShadowProtect volume list for the current system.
View	Manage toolbar visibility.	**Status Bar:** Toggles a status bar at the bottom of ShadowProtect Console that provides application and environment status information. **Task Panel:** Toggles visibility of the Navigation Panel (see Navigation Panel).
Options	Access ShadowProtect Agent options.	**Client Options:** Opens the Client Options dialog box where you can configure visual notifications for backup job success or failure. **Agent Options:** Opens the Agent Options dialog box where you can configure Email notification settings for the current system. You can choose to send Email notifications for both failed and successful backup jobs.
Help	Access ShadowProtect help resources.	**Contents:** Launches the ShadowProtect on-line help system. The help is available only when running ShadowProtect Console in Windows (not in the Recovery Environment). **Product Activation:** Opens the Activation dialog box, where you can activate (or deactivate) the ShadowProtect installation (see Activating ShadowProtect). **Check for Latest Version:** Queries the StorageCraft Web site for updates to the current ShadowProtect installation. If there is an update available, a message displays the URL where you can get the update. **Register:** Opens a browser to https://register.storagecraft.com/register/regstart.jsp where you can manually request an product activation key (see Manual Activation). **About:** 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.

4.2 Navigation Panel

The left-side Navigation panel provides quick access to ShadowProtect tasks and tools. You can toggle the Navigation panel on or off by selecting **View** > **Task Panel**. The Navigation panel is organized into the following categories. You can collapse and expand each category, as desired.

Category	Description	Options

View	Display or hide the Network View.	**Network View:** Toggles to display the list of nodes running the ShadowProtect Backup Agent (see Remote Management).
Tasks	Access ShadowProtect Wizards.	**Backup:** Launches the Backup Wizard (see Creating Backup Image Files). **Restore:** Launches the Restore Wizard (see Restoring a Volume). **Explore Backup:** Launches the Explore Backup Image Wizard (see Mounting Backup Image Files. **Dismount Backup Image:** Launches the Backup Image Dismount Wizard (see Dismounting Backup Image Files). ⚠ Note: Several tools are available only in the Recovery Environment (RE). For more information about these tools, see the *StorageCraft Recovery Environment User Guide*.
Tools	Access ShadowProtect tools.	**Verify Image:** Launches the Verify Image Wizard (see Verifying Backup Image Files). **Image Conversion Tool:** Launches the Image Conversion Tool Wizard (see Image Conversion Tool). **Network Configuration:** (RE only) Launches the Network Configuration utility, where you can configure a computer's network access settings. **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. **Load Drivers:** (RE only) Opens the Load Drivers dialog box, where you can configure storage drivers for use in the Recovery Environment. **File Browser:** (RE only) A simple file browser that lets you browse files and folders of a backup image file. **Text Editor:** (RE only) A simple text editor. **Vista BCD:** (RE only) Launches the Vista BCD editor, where you can edit Boot Configuration Data (BCD) on systems running Windows Vista. **Partition Table Editor:** (RE only) A simple partition table editor. **UltraVNC:** (RE only) Launches the Remote Management utility, where you can configure remote access to systems running the Recovery Environment. **Select Your Time Zone:** (RE only) Launches the Time Zone utility, where you can adjust the system's time zone information. **Enable Logging:** (RE only) Opens the Logging dialog box, where you can configure ShadowProtect event logging.
Help	(Windows only) Access to on-line help topics.	**Backup:** Opens the on-line help to Create a Backup Image. **Restore:** Opens the on-line help to Restoring a Volume. **Browse Image:** Opens the on-line help to Mounting Backup Image Files in Windows. **Image Tools:** Opens the on-line help to Image Conversion Tool.
License	(Windows only) Displays current licensing information for this ShadowProtect installation.	**Trial or Evaluation version:** Displays the number of days before the ShadowProtect installation expires. **Licensed version:** Displays "Active", meaning that the product is fully licensed and activated.
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 the current state of the system, including:	Queued Tasks: The number of queued tasks waiting to run. Running Tasks: The number of tasks currently running.

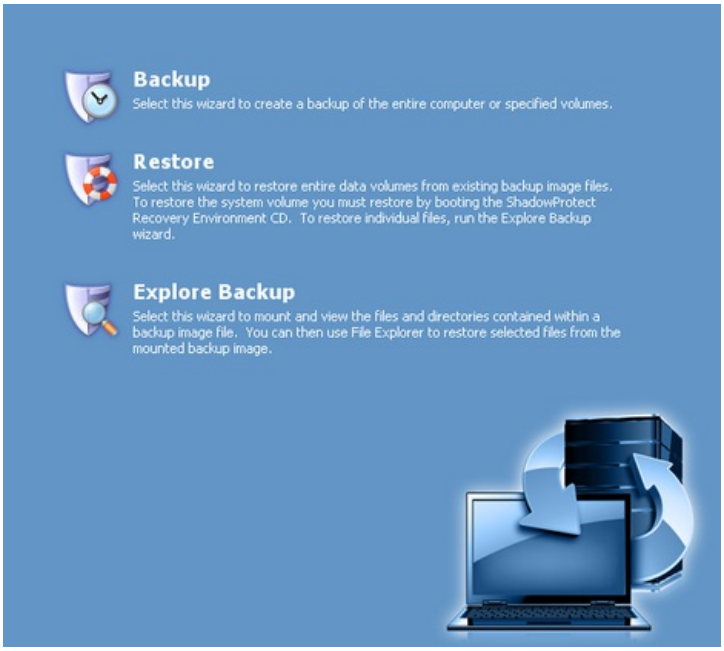
4.3 Tabs

The ShadowProtect Console provides the following pages in the Center panel:

- Wizards Tab
- Management View Tab
- Disk Map Tab
- Backup Jobs Tab
- Destinations Tab
- Backup History Tab

Wizards Tab

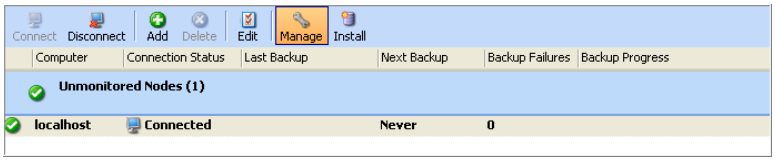
The Wizards tab is the default page in the Main panel. It provides access to three Wizards that guide users through the most common ShadowProtect tasks.



- **Backup:** Starts the Backup Wizard, which guides you through the creation of a backup job. For more information, see Create a Backup Image.
- **Restore:** Starts the Restore Wizard, which guides you through the process of restoring a volume from a backup image file. For more information, see Restoring a Volume for additional information.
- **Explore Backup:** Starts the Explore Backup Wizard, which guides you through mounting a backup image file as a volume so you can restore individual files and folders. For more information, see Mounting Backup Image Files.

Management View Tab

The Management View tab is one way to access the remote management capabilities of ShadowProtect. It is the preferred management view for users of ShadowProtect Server and ShadowProtect SBS because it lets you easily manage many nodes from a single location.



The Management View tab is divided into two panes:

Node Controls Pane: The upper Node Controls pane lets you manage connected nodes. Select a node from the Node Information pane to manage it. The Node Controls pane includes the following controls:

Control	Description
Connect	Connects a previously added managed remote node to the ShadowProtect user interface.
Disconnect	Disconnects a managed remote node from the ShadowProtect user interface.
Add	Adds a system that has the ShadowProtect Backup Agent installed to the node list.
Delete	Deletes a remote node from the managed node list.

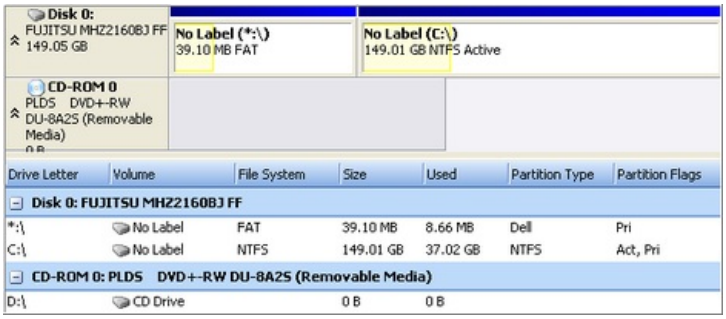
Edit	Opens the Server Details dialog box of the currently selected node (see Mgmt View - Modifying Remote Node Properties).
Manage	Opens the ShadowProtect tabs (Disk Map, Backup Jobs, Destinations, Backup History) for the currently selected node.
Install	Opens the ShadowProtect Push Wizard, which lets you push the ShadowProtect agent out to other systems that you want to manage from this Management View. For more information, see Installing the Backup Agent Remotely.

Node Information List: The Node Information pane displays a list of nodes currently managed by this management console.

Component	Description
Basic Properties	Displays information about the currently selected backup job in three panes: **Job Status:** Displays information about the current backup job, including the destination backup image file, and status (queued, running, completed), and the time remaining (running job) or total time (completed job). Click **View Details** to view the Volume Backup tab. **Backup Job:** Displays information about the backup job configuration, including Compression, Encryption, and the backup job options. **Schedule:** If the selected backup job is a recurring job, the Basic Properties tab displays the job schedule for both Full backup images, and Incremental backup images, where applicable.
Volume Backup	Displays detailed information about the currently running backup job, including time remaining, throughput, and an Event log. If no backup job is running, the Volume Backup tab displays details from the most recent backup job.

Disk Map Tab

The Disk Map tab provides a graphical view of system drives. Disk Map lists each physical disk drive with the partitions available on that drive.



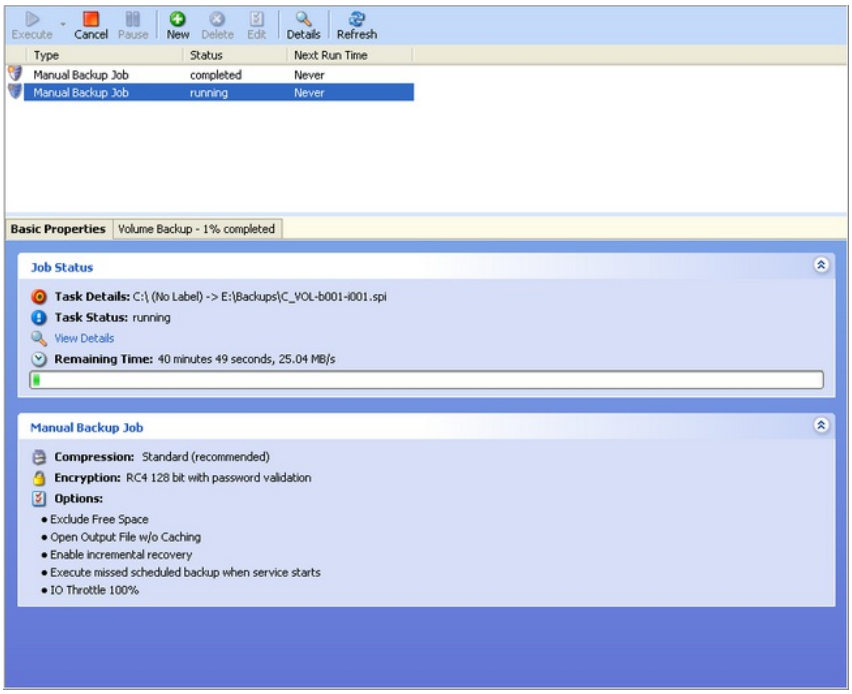
ShadowProtect Disk Map tab
Right-clicking an entry in the Disk Map opens an actions menu for that entry.

Entry	Right-click Actions
Physical Drive	**Edit Policy:** Opens the Partition Creation Policy Editor dialog box. **Refresh Volumes Info:** Refreshes the ShadowProtect volume list for the current system.
Partition	**Backup:** Launches the Backup Wizard (see Creating Backup Image Files). **Restore:** Launches the Restore Wizard (see Restoring a Volume). **Delete Partition:** Deletes the selected partition. **Set Active:** Sets the selected partition as the active (bootable) partition on the physical drive. **Edit Policy:** Opens the Partition Creation Policy Editor dialog box. For more information, (see Changing Partition Creation Policy). **Refresh Volumes Info:** Refreshes the ShadowProtect volume list for the current system.

The Disk Map tab lets you access the Backup and Restore Wizards, and change partition creation policies for the selected drive. Additionally, in the Recovery Environment you can also run Check Disk, format a drive and edit the selected disk's `boot.ini`.

Backup Jobs Tab

The Backup Jobs tab displays scheduled backup jobs. From this tab, you have complete control over the ShadowProtect jobs configured for the current system.



The Backup Jobs tab is divided into two panes:

Job Controls Pane: The upper Job Controls pane lets you manage backup jobs. Select a backup job from the job list to manage it, and view job information in the Job Information pane. The Job Controls pane includes the following controls:

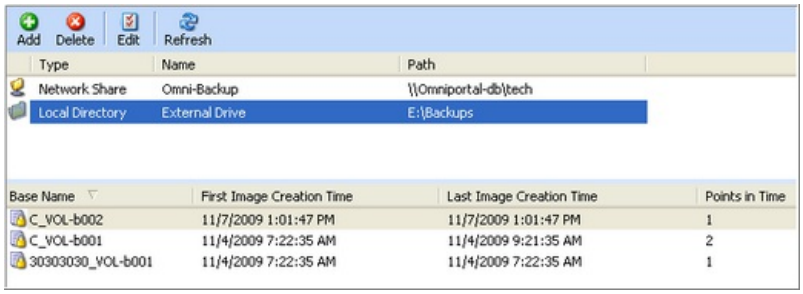
Control	Description
Execute	Executes the selected backup job.
Cancel	Cancels the selected backup job. This terminates a currently running job, but keeps the job status as enabled (the job executes at its Next Run Time).
Pause	Toggles the selected job status between enabled and disabled. A disabled job is suspended and will not run until re-enabled.
New	Launches the Backup Wizard (see Create a Backup Image).
Delete	Deletes the selected job from the Job Scheduler.
Edit	Launches the Backup Wizard, where you can edit the selected job's configuration (see Create a Backup Image).
Details	Opens the Volume Backup tab in the Job Information pane so you can see details about the currently selected backup job.
Refresh	Refreshes the volume information in the Backup Job Information pane.

Job Information: Displayed in the lower pane, the Job Information pane includes two tabs that provide information about the currently selected backup job.

Component	Description
Basic Properties	Displays information about the currently selected backup job in three panes: **Job Status:** Displays information about the current backup job, including the destination backup image file, and status (queued, running, completed), and the time remaining (running job) or total time (completed job). Click **View Details** to view the Volume Backup tab. **Backup Job:** Displays information about the backup job configuration, including Compression, Encryption, and the backup job options. **Schedule:** If the selected backup job is a recurring job, the Basic Properties tab displays the job schedule for both Full backup images, and Incremental backup images, where applicable.
Volume Backup	Displays detailed information about the currently running backup job, including time remaining, throughput, and an Event log. If no backup job is running, the Volume Backup tab displays details from the most recent backup job.

Destinations Tab

The Destinations tab displays information about the configured storage locations for backup image files. From this tab, you create or modify the destinations used by ShadowProtect backup jobs. For more information see Destinations.



The Destinations tab includes the following panes:

Destinations List: The upper pane displays a list of currently defined Destinations for the system. To delete or edit a destination location, highlight the destination location in the list and then select the operation to perform. Information about backup Image Sets stored at the destination location is presented for the highlighted entry in the Destination Information.

Destination Usage: The lower pane displays information about the backup Image Sets stored in the currently selected Destination, including Base Name, First Image Creation Time, Last Image Creation Time and number of "point-in-time" image files in the backup Image Set.

Additionally, the Destinations tab includes the following icons for working with Destinations:

Add: Opens the Destination dialog box (see Destinations for additional information).

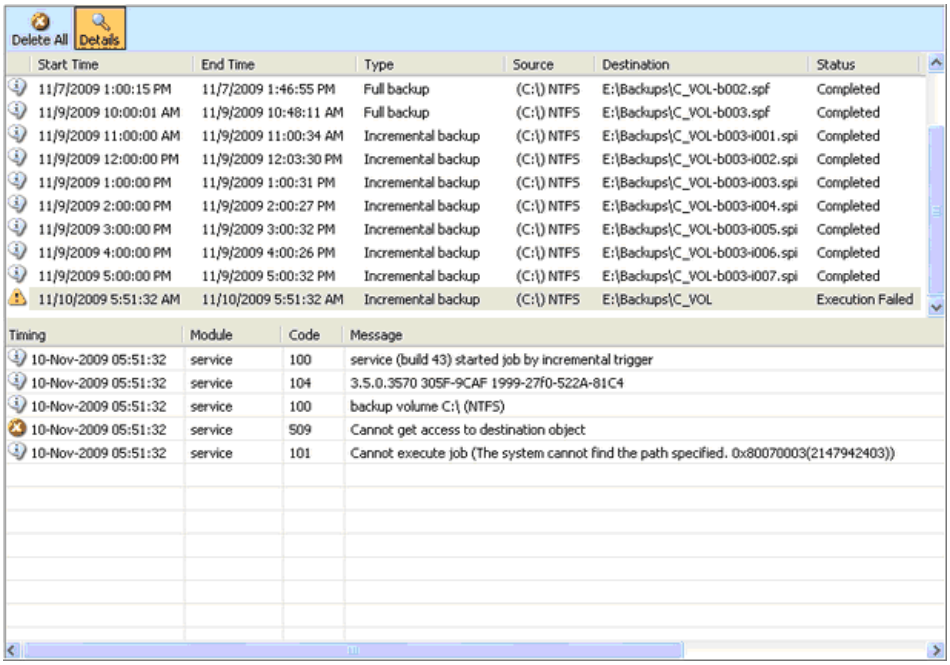
Delete: Deletes the currently selected Destination.

Edit: Opens the Destinations dialog box so you can modify an existing Destination configuration (see Editing Destinations).

Refresh: Updates the Destination Objects List and the Destination Objects Information List.

Backup History Tab

The Backup History tab displays log information for completed backup jobs. The Backup History lets you analyze ShadowProtect backup activity over time, including failed jobs, if any.



The Backup History tab includes the following panes:

Job History: The upper pane displays a list of completed backup jobs. Select a job to view job details in the Job Log.

Job Log: The lower pane displays the log entries for the selected job. This is the same information available in the Volume Backup tab (see Backup Jobs Tab.)

You can sort the backup history lists by clicking on the column headers. You can also adjust the column width by dragging the column header borders.

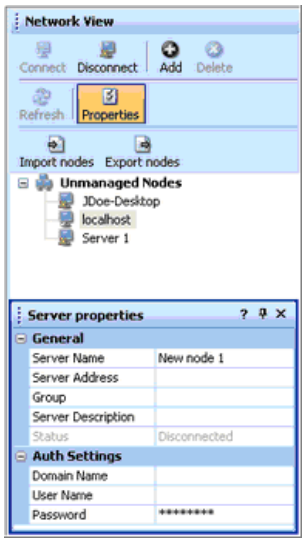
Additionally, the Backup History tab includes the following icons:

Delete All: Clears the Job List.

Details: Displays or hides the Job Log pane.

4.4 Network View

The Network view displays information for managing ShadowProtect on remote systems (see Remote Management). Select Network View from the Navigation panel to see this pane.



The Network View includes the following controls:

Control	Description
Connect	Connects a previously added managed remote node to the ShadowProtect user interface.
Disconnect	Disconnects a managed remote node from the ShadowProtect user interface.
Add	Adds a system that has the ShadowProtect Backup Agent installed to the node list.
Delete	Deletes a remote node from the managed node list.
Refresh	Refreshes the remote node list.
Properties	Toggles the Server Properties table on and off.
Import Nodes	Imports a previously exported node list into your Network View.
Export Nodes	Exports your node list into an XML file.

5 Creating Backup Image Files

Note: For information about creating a backup image file in Recovery Environment, see the *StorageCraft Recovery Environment User Guide*.

ShadowProtect provides two ways to create backup image files:

One-Time Backup: The Backup Wizard guides you through creating a backup image file immediately. Consider the following when creating a one-time backup job:

- To create a one-time backup job, you must be a member of the Administrator group on the system where you are creating a backup.
- One-time backup jobs do not affect scheduled backup jobs.
- ShadowProtect supports one-time backup images from both Windows and Recovery Environment. For more information about each of these options, see Features and Components.

Scheduled Backup: The Backup Wizard guides you through the process of creating a recurring backup job. Consider the following when creating a scheduled backup job:

- A volume can belong to no more than one scheduled backup job that includes Incremental backups. This limitation does not include one-time backup images or Differential backup images, as long as they do not disrupt sector tracking for the Incremental backup.
- If ShadowProtect is currently running a backup job, or the computer is turned off and unavailable, ShadowProtect skips any scheduled backup jobs during that time.
- ShadowProtect supports scheduled backup images only from Windows (not the Recovery Environment).

To create a backup image file

1. Start the ShadowProtect Console (see Starting ShadowProtect).
2. Start the Backup Wizard, then click **Next**.
   There are several ways to start the Backup Wizard, including:
   - In the Wizards tab, click **Backup**.
   - In the Tasks menu, click **Backup**.
   - In the Menu Bar, select **Tasks** > **Backup**.
3. On the *Volumes to Back Up* page, select the volumes to backup, then click **Next**.
   ShadowProtect creates a separate backup file for each volume.
4. On the *Backup Name and Destination* page, specify the following information about the backup image file, then click **Next**.

Location	You can select either a local drive or network location to store the backup image file: **Local Drive:** Click Browse. In the Open Folder dialog box, select the local drive and folder to store the backup image file. **Network Share:** In the drop-down list, select <Network Locations>. This opens the Destinations dialog box where you can define the network share. For more information, see Destinations
Name	The File Name table displays the volumes (with default file names) selected for the backup job. Double-click a table row to modify the file name.

5. On the *Specify the Backup Schedule* page, specify the schedule and backup image type, then click **Next**.

   Note:The selected backup schedule determines the available backup image types. For more information about the backup image types, see Glossary.

Now	Creates Full or Differential backup images. Creates a one-time backup job that starts as soon as the Backup Wizard closes.
Later	Creates Full backup images. Creates a one-time backup job at the specified date and time. By default, the Start Time fields display the current date and time. To change the date and time settings, click on an element of the date/time (month, day, year, hour minute, second, AM/PM), then type or use the up/down buttons to set the desired value.
Weekly	Creates Full and Incremental backup images. Creates a recurring backup job based on a weekly schedule. You select the weekdays and time of day to start a Full backup. Optionally, you can specify a schedule for Incremental backups. a. Select the weekdays to create Incremental backups. b. Specify times of day to start and stop creating Incremental backups. c. Specify the Incremental backup frequency (minutes between Incremental backups).
Monthly	Creates Full and Incremental backup images. Creates a recurring backup job based on a monthly schedule. You select the days of the month and time of day to start a Full backup. Optionally, you can specify a schedule for Incremental backups. a. Select the weekdays to create Incremental backups. b. Specify times of day to start creating Incremental backups

	Creates Full and Incremental backup images. Creates a single Full backup, then creates recurring Incremental backups from that point forward. This option requires ShadowProtect ImageManager (see the *ShadowProtect ImageManager User Guide*).
Continuous Incrementals	To specify the Incremental backup schedule: a. Select the weekdays to create Incremental backups. b. Specify times of day to start and stop creating Incremental backups. c. Specify the Incremental backup frequency (minutes between Incremental backups).

6. (Conditional) On the *Previous Backup Image* page, select the existing backup image file to use as a basis for creating the Differential backup image, then click **Next**.
   This page displays only when you specified a Differential backup in the *Backup Schedule* page.
7. On the *Options* page, select the desired backup image file options, then click **Next**.
   The *Options* page lets you set both basic and advanced backup image options. For more information about each of the available options, see Options.
8. On the *Wizard Summary* page, review the backup job configuration, then click **Finish**.
   Select Execute Now to run the backup job immediately in addition to the schedule defined in the job.

You can monitor the progress of the backup in the Backup Jobs tab (see Backup Jobs Tab).

5.1 Backup Image File Storage Locations

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. ShadowProtect notes the reason for the failure in its log file (and in the Backup History tab).

Location	Advantages	Disadvantages
Local Hard Drive	• Fast backup and restore. • Inexpensive.	• Consumes local disk space. • Vulnerable to loss if the drive fails.
Local USB/FireWire Drive	• Fast backup and restore. • Preserves disk space on local drives. • Inexpensive. • Easy off-site storage.	• More expensive than local hard drives. • Vulnerable to loss if the drive fails.
Network Hard Drive	• Fast backup and restore. • Protection from local hard drive failure. • Off-site storage.	• 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	• Good media for archiving. • Protection from local hard drive failure.	• Slower backups due to media speeds. • File restrictions due to limited size.

5.2 Configuring a Weekly/Monthly Backup Job

To configure a weekly or monthly ShadowProtect backup job:

1. Start the ShadowProtect Console (see Starting ShadowProtect).
2. Start the Backup Wizard, then click **Next**.
   There are several ways to start the Backup Wizard, including:
   - In the Wizards tab, click **Backup**.
   - In the Tasks menu, click **Backup**.

- In the Menu Bar, select **Tasks** > **Backup**.

3. On the *Volumes to Back Up* page, select the volumes to backup, then click **Next**.
   ShadowProtect creates a separate backup file for each volume.
4. On the *Backup Name and Destination* page, specify the following information about the backup image file, then click **Next**.

Location	You can select either a local drive or network location to store the backup image file: **Local Drive:** Click **Browse**. In the Open Folder dialog box, select the local drive and folder to store the backup image file. **Network Share:** In the drop-down list, select <Network Locations>. This opens the Destinations dialog box where you can define the network share. For more information, see Destinations
Name	The File Name table displays the volumes (with default file names) selected for the backup job. Double-click a table row to modify the file name.

5. On the *Specify the Backup Schedule* page, specify the schedule and backup image type, then click **Next**.

   Note:The selected backup schedule determines the available backup image types. For more information about the backup image types, see Glossary.

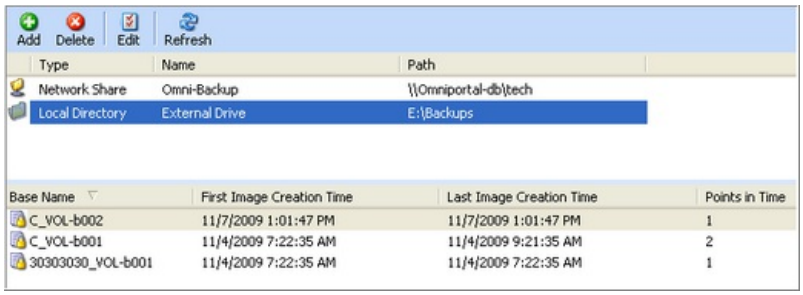
Now	Creates Full or Differential backup images. Creates a one-time backup job that starts as soon as the Backup Wizard closes.
Later	Creates Full backup images. Creates a one-time backup job at the specified date and time. By default, the Start Time fields display the current date and time. To change the date and time settings, click on an element of the date/time (month, day, year, hour minute, second, AM/PM), then type or use the up/down buttons to set the desired value.
Weekly	Creates Full and Incremental backup images. Creates a recurring backup job based on a weekly schedule. You select the weekdays and time of day to start a Full backup. Optionally, you can specify a schedule for Incremental backups. a. Select the weekdays to create Incremental backups. b. Specify times of day to start and stop creating Incremental backups. c. Specify the Incremental backup frequency (minutes between Incremental backups).
Monthly	Creates Full and Incremental backup images. Creates a recurring backup job based on a monthly schedule. You select the days of the month and time of day to start a Full backup. Optionally, you can specify a schedule for Incremental backups. a. Select the weekdays to create Incremental backups. b. Specify times of day to start creating Incremental backups
Continuous Incrementals	Creates a recurring backup job. See *Configuring a Continuous Incremental Backup Job* for details.

6. (Conditional) On the *Previous Backup Image* page, select the existing backup image file to use as a basis for creating the Differential backup image, then click **Next**.
   This page displays only when you specified a Differential backup in the *Backup Schedule* page.
7. On the *Options* page, select the desired backup image file options, then click **Next**.
   The *Options* page lets you set both basic and advanced backup image options. For more information about each of the available options, see Options.
8. On the *Wizard Summary* page, review the backup job configuration, then click **Finish**.
   Select Execute Now to run the backup job immediately in addition to the schedule defined in the job.

You can monitor the progress of the backup in the Backup Jobs tab (see Backup Jobs Tab).

5.3 Destinations

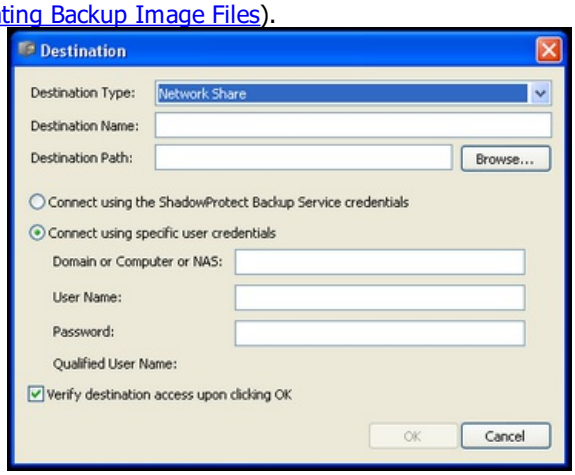
Backup destinations let you create pre-defined storage locations for backup image files, either locally or on a network. You can then select these destinations when creating backup jobs. Then, if you need to modify the destination, you can do so by editing the destination object rather than deleting and recreating new backup jobs.



Note: ShadowProtect requires that every system has a unique Destination for its backup image files. Multiple systems should not save files to the same folder. However, you can use the same folder to save backup jobs from the same system which has multiple volumes (such as a boot volume and a data volume).

To create a backup job destination

1. Open the ShadowProtect Console, then select **Tasks** > **Add Destination**.
   This opens the Destinations dialog box. You can also open the Destinations dialog box from the Backup Name and Destination page of the Backup Wizard (see Creating Backup Image Files).



2. Specify the settings for the new destination, then click **OK**.

Destination Type	Select the type of destination to create: **Local Directory:** The destination is on a locally connected storage device (HDD, USB drive, etc.) **Network Share:** The destination is on the network.
Destination Name	Specify the path to the a descriptive name for this destination.
Destination Path	Specify the details of the destination. The information you need to provide depends on the Destination Type. **Local Directory:** Click **Browse**, then select the local drive and folder to store backup images. **Network Share:** Click **Browse**, then select the network location to store backup images. You must also specify the network credentials that ShadowProtect should use to access the specified network location: **ShadowProtect Backup Service credentials:** Use the same stored credentials used by the ShadowProtect backup service to access your system. **Specific User credentials:** Provide the Container (Domain, Computer name, or NAS device name), Username and Password that ShadowProtect should use to access this network share.
Verify Destination Access	Instructs ShadowProtect to verify the destination path and access credentials, if necessary, before creating the Destination object. If the destination access verification is not successful the program alerts you that the destination could not be created as requested. If this happens, check the path and credentials used to make sure they are accurate, then re-create the destination.

Editing Destinations

To edit a backup job destination

1. Start the ShadowProtect Console (see Starting ShadowProtect).
2. Select the Destinations tab.
3. Select the destination to edit, then click **Edit**.
   This open the Destination dialog box, which displays the current destination configuration. From this dialog box, you can edit

all Destination properties except the Destination Type (Network Share or Local Directory).

Deleting Destinations

To delete a backup job destination

1. Start the ShadowProtect Console (see Starting ShadowProtect).
2. Select the Destinations tab.
3. Select the destination to delete, then click **Delete**.

   Note: Before deleting a Destination, make sure to modify or delete any backup jobs that use the Destination or the jobs will fail. For information about editing backup jobs, (see Backup Jobs Tab.)

5.4 Options

When creating a backup job, ShadowProtect provides the following backup image file options. The Backup Wizard provides access to these options when you are creating a backup job (see Creating Backup Image Files).

- Compression Method
- Encryption
- Split Image File
- Backup Comment

Compression Method

ShadowProtect provides the following file compression options when creating a backup image file:

None	No data compression. This option uses the fewest CPU resources but uses the most disk space.
Standard	Typically compresses data by about 40%. Standard compression provides an optimal balance between CPU usage and disk space usage.
High	Typically compresses data by about 50%. This option requires the most CPU resources, but is useful when disk space is limited.

File Protection

ShadowProtect provides the following file protection mechanisms when creating a backup image file. This is particularly useful when storing backup image files on a network, or off-site, to help prevent unauthorized access and use of your backup image files. If you select to protect the backup image file, you must specify the correct password in order to mount or restore the backup image.

Password Protection: Assigning a password requires you to enter the correct password before using the backup image file (for example, to restore a volume or create a Differential backup image based on the password-protected file. ShadowProtect supports passwords comprised of alphanumeric characters. Use the following guidelines when creating a password for the greatest security with password encrypted backup image files.

- Use at least eight characters.
- Use a random mixture of characters, upper and lower case and numbers.
- Don't use a word found in the dictionary.
- Change your password regularly or if you suspect your password has been compromised.

  Warning: If you forget the password, you cannot access the backup image file. StorageCraft cannot access an encrypted backup image file.

File Encryption: ShadowProtect uses the password as an encryption key when encrypting the backup image file. You can select one of three encryption methods in the Advanced Options dialog box. For more information,see "Encryption" in Advanced Options.

Use Password File: You can use password file, also known as a Key File, to encrypt a backup image. This is helpful if you are not managing your own backups and you don't want other users to have access to the password used to protect the backup image files. For information about creating a Key File, see Creating Key Files.

Split Image File

ShadowProtect lets you split a backup image file into multiple smaller files, creating a *Spanned Image Set*. This is useful when you need to move a backup image file onto fixed-length media such as CDs or DVDs.

To split a backup image file:

1. Select **Split Image File** in the Backup Wizard's *Options* page.

2. Specify the maximum file size (in MB) for each of the smaller files in the set the **Split Image File** field.

For more information about the Backup Wizard, see Creating Backup Image Files.

You can also split an existing backup image file using the Image Conversion Tool (see Image Conversion Tool).

Note: If a backup image file is divided into multiple files, the filename suffix will change to `.sp1, .sp2, ..., .spN`, where *N* represents the file's sequence within the Spanned Image Set.

Backup Job Name

The Backup Job Name field lets you specify a name for the backup job. ShadowProtect uses this name as a prefix for each backup image file created as part of this backup job. For example, you can specify a backup job with the name "Server1" to quickly identify just those backup image files that are related to Server1.

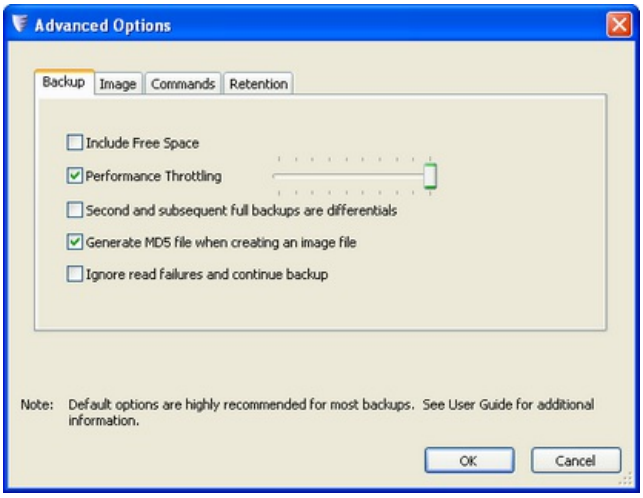
Backup Comment

The Backup Comment option lets you attach a comment 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 to the backup image.

Advanced Options

ShadowProtect supports the following advanced options when creating a backup image job. You can access these options by clicking **Advanced** on the Options page of the Backup Wizard (see Creating Backup Image Files).

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



ShadowProtect organizes its advanced options into four tabs:

Backup

The Backup tab includes the following advanced options:

Option	Default	Description
Include Free Space	OFF	Backs up all sectors on the volume, including those sectors marked as free space. This can result in a much larger image file, but can help preserve previously deleted files.
Performance throttling	ON, 100% I/O usage	Specifies how much I/O bandwidth that ShadowProtect can use when creating a backup image file. Use the slider bar to adjust this setting. Reducing (throttling) ShadowProtect I/O usage increases the time it takes to create a backup image file, but can reserve I/O bandwidth for other processes.
2nd and subsequent full backups are differentials	OFF	Instructs ShadowProtect to create Differential images rather than Full images for second and subsequent scheduled backup jobs. For example, if you have a weekly backup schedule that creates a new Full image each Monday, selecting this option instructs ShadowProtect to create Differential images each Monday that are based on the initial Full image created when the backup job ran for the first time. This reduces storage needs for the backup image files over time.
Generate MD5 file when creating an image file	ON	Instructs ShadowProtect to create an MD5 (Message Digest 5) checksum file when creating a backup image file. The checksum lets you confirm the file integrity of backup image files.
Ignore read failures and continue backup	OFF	Instructs ShadowProtect to ignore disk read errors that occur during the creation of backup image files. StorageCraft does not recommend using this option because you might back up disk corruption that might prevent a restored volume from working properly.

Image

The Image tab includes the following advanced options:

Option	Default	Description
Enable write caching	OFF	Enables or disables using file caching when writing the backup image file. When writing to a network location, this might slow down the the backup process.
Enable concurrent task execution	OFF	Enables or disables creating backup images simultaneously for multiple volumes rather than creating only one backup images at a time. When using this option, you should have hardware capable of supporting a high disk load.

Enable self-healing incremental recovery	ON	Determines how ShadowProtect reacts to a system error that interrupts the ShadowProtect incremental tracking feature. When set to Off, ShadowProtect recovers by generating a new Full image and starting a new Image Set. When set to On, ShadowProtect recovers by creating an Incremental image as planned, along with a Differential image based on the most recent Incremental image and the current volume. This prevents disruption of the Incremental backup schedule, but can result in increased CPU and network bandwidth when compared to creating a new backup Image Set.
Auto-execution of unexecuted task	ON	Enables or disables executing the last scheduled backup job if it was missed (for example, because the system was powered off). This option executes only the last unexecuted backup job if ShadowProtect misses more than one scheduled backup job.

Commands

The Commands tab lets you specify command files (.exe, .cmd, .bat) to execute at key points in the backup image file creation process. The command files cannot rely on any user interaction, so you should test each command file before using them with ShadowProtect. ShadowProtect allows 5 minutes at each stage (Pre-snapshot, Post-snapshot, and Post-backup) for command files to complete. If the command files do not complete in 5 minutes, ShadowProtect proceeds while the command files continue executing.

To use a command file for a particular stage, either:

- Use **Browse** to locate and open an existing command file or
- Enter the full file name, including path, into the appropriate field:

Pre-Snapshot: Executes the specified command file before taking the image snapshot (see "Snapshot" in Glossary). For example, you might execute a pre-snapshot command file that places non-VSS aware applications or databases into a backup state.

Note: It takes only a few seconds to create a snapshot, so non-VSS databases or applications are out of production only briefly before they can be returned to normal operating mode with a post-snapshot command .

Post-Snapshot: Executes the specified command file after taking the image snapshot (see "Snapshot" in Glossary). For example, you might execute a post-snapshot command file to return non-VSS-aware applications or databases to normal operating mode.

Post-Backup: Executes the specified command file after creating the backup image file. For example, you might execute a post-backup command file to automatically copy the backup image file to an off-site location or FTP server.

Note: To avoid the 5 minute execution limit for post-backup command files, you can call a command file that simply executes another command file and then finishes. This lets you complete the ShadowProtect-associated command file in the 5-minute allotment while the secondary command file performs tasks that take longer to complete (synchronizing or copying the backup image files to an alternate location, scanning the backup image file for viruses, etc.).

Encryption

The Encryption tab lets you select the algorithm used to encrypt the backup image file. The Encryption tab is displayed only when you have selected **Enter Password** on the Options page of the Backup Wizard (see File Protection).

- **RC4 128-bit**: This encryption option is the fastest, but least secure, of the algorithms.
- **AES 128-bit**: This encryption option strikes a balance between speed and security.
- **AES 256-bit**: This encryption option is the most secure, but slowest, of the algorithms.

Retention

The Retention tab lets you specify a policy for automatically managing the retention of backup Image Sets (see "Image Set" in Glossary. The Retention tab is not available if you are using the Continuous Incremental backup schedule, which leverages ShadowProtect ImageManager to manage backup Image Sets. For more information, see the *ShadowProtect ImageManager User Guide*.

The Retention tab includes the following advanced options:

Option	Default	Description
Enable a retention policy	OFF	Enables or disables an automatic image set retention policy.
Number of backup Image Sets to retain	3	Specifies the maximum number of image sets to retain. When the specified maximum (M) is reached, ShadowProtect deletes the oldest image set. By default, ShadowProtect enforces the retention policy after creating an image set, meaning that ShadowProtect creates the M+1 image set, then deletes the oldest Image Set, thereby retaining M image sets.
Delete both Full and Incremental backup images in the set	OFF	Instructs ShadowProtect to delete the all files, both Full and Incremental, when removing an old image set.
Delete only Incremental backup images (retain Full backup images)	ON	Instructs ShadowProtect to delete only Incremental backup images when removing an old image set.
Enforce policy before starting the next Full backup	OFF	Instructs ShadowProtect to "make room" for a new image set by deleting the oldest image set before creating the new image set that will replace it. This reduces the amount of disk space needed to adhere to the specified retention policy.

For more information about the benefits of retention policies, see Retention Policy Configurations.

5.5 Deleting Backup Image Files

You can delete backup image files using any process you normally use to delete a file in Windows. However, before deleting a backup image file, be certain of the following:

- If this is a full backup image file, that this file is not required for any active backup job. If you delete this file, and it is the start of an active backup job, ShadowProtect will create a new full backup image file at the next scheduled backup and start a new Image Set. All existing incremental files that depended on the deleted full image will not be accessible.
- If this is an incremental file, that no later incremental files depend on this one. If you delete a backup image file that other (later) point-in-time backup image files depend on, all the later dependent backup image files become useless. You will then not be able to mount or restore files from these dependent backup image files.

Use the Image Conversion Tool to check for any file dependencies (see Image Conversion Tool).

5.6 Configuring a Continuous Incremental Backup Job

A continuous incremental backup job creates a single full backup, then creates recurring incremental backups from that point forward at set intervals. This option requires ShadowProtect ImageManager (see the *ShadowProtect ImageManager User Guide*) to manage the amount of disk space used by the files as well as to maintain the integrity of the backup files.

To configure a continuous incremental backup job:

1. Start the ShadowProtect Console (see Starting ShadowProtect).
2. Start the Backup Wizard, then click **Next**.

There are several ways to start the Backup Wizard, including:
- In the Wizards tab, click **Backup**.
- In the Tasks menu, click **Backup**.
- In the Menu Bar, select **Tasks** > **Backup**.

3. On the *Volumes to Back Up* page, select the volumes to backup, then click **Next**. ShadowProtect creates a separate backup file with a default name for each volume.
4. On the *Backup Name and Destination* page, specify the following information about the backup image file, then click **Next**.

Location	You can select either a local drive or network location to store the backup image file: **Local Drive:** Click **Browse**. In the Open Folder dialog box, select the local drive and folder to store the backup image file. **Network Share:** In the drop-down list, select <Network Locations>. This opens the Destinations dialog box where you can define the network share. For more information, see Destinations.
Name	The File Name table displays the volumes (with default file names) selected for the backup job. Double-click a table row to modify the file name.

5. On the *Specify the Backup Schedule* page, select *Continuous Incrementals*.

   Note: For more information about the continuous incremental backup image type, see the Glossary.

6. In the *Additional Incremental Backups* section, specify on which days you want to create incremental backups.
7. Specify the time of the first and last incremental backup for each day.
8. Specify the interval (in minutes) between each incremental using the arrow buttons. (The Wizard does not accept numbers typed in.) The minimum is every 15 minutes. The maximum is every 1440 minutes. The Wizard will display the number of backups ShadowProtect will do each day based on the start/stop times and the interval.
9. Leave the *Use VSS* option and the *Sunday* option under *VSS Incremental Backups* section checkmarked. (See *Using VSS* for details on when to not use VSS.) Click **Next**.
10. On the *Options* page, select the desired backup image file options, then click **Next**. The *Options* page lets you set both basic and advanced backup image options. For more information about each of the available options, see Options.

    Note: Provide a name for the backup job. A unique name allows quick identification of related backup files. ShadowControl CMD also can display the backup job name--again making it easier to determine which job applies to which EndPoint.

11. On the *Wizard Summary* page, review the backup job configuration, then click **Finish**.
12. Select *Execute Now* to run the backup job immediately in addition to the schedule defined in the job.

You can monitor the progress of the backup in the Backup Jobs Tab.

Using VSS

ShadowProtect uses the Windows VSS framework to provide consistent backups of SQLServer, Exchange, Active Directory, Oracle or other database systems. VSS also ensures that all cached data is written to disk prior to taking the snapshot. Using VSS, ShadowProtect simplifies a system restore--whether on a server or a workstation. For these reasons, using VSS is the default for all ShadowProtect backup jobs.

There are, however, a few uncommon scenarios where taking a non-VSS backup may be an option:

- One or more VSS components fail, causing the backup job to fail
- Limited disk space requires smaller incremental file sizes.
- Limited server resources (RAM or CPU) requires a simpler backup operation.

The preferred solution is to either resolve the failure issue or provide additional storage or processor resources. However, it is also possible to configure a backup job to run wthout VSS or to only use VSS on set occasions.

Note: The option to use or not use VSS is only available when configuring a Continuous Incremental backup job.

This table summarizes strategies for various backup issues:

Issue	Possible Resolutions
VSS component failure	Some VSS writers do not fully or correctly comply with the VSS spec. This may cause VSS to halt. This type of error will be noted in the backup job's log file.
Limited disk space	This may occur for example with a NAS destination for multiple systems' backup files. Rather than have a backup fail for lack of space, configure ShadowProtect to take a non-VSS backup. The resulting non-VSS incremental file typically gives a modest decrease in size compared to a full VSS backup. This decrease may be useful then for multiple devices to continue to backup to a single volume.
Limited server resources	A server may host multiple processor-intensive applications (such as may occur with Windows SBS). Adding the task of executing an incremental backup every 15 minutes may result in poor performance. Opting for a non-VSS backup could limit the impact of each snapshot on the server. Rather than execute non-VSS backups only, the recommendation is to configure the job for non-VSS backups during business hours, then executing a VSS backup after hours.

Non-VSS-Aware Applications

Some applications, such as Intuit QuickBooks, remain non-VSS-aware. These applications may seem like a good case to configure a non-VSS backup. However, it is not. Instead, ShadowProtect supports both pre- and post-backup scripts which can run commands to stop and restart these non-VSS-aware apps. (See Commands for details on running scripts.)

Non-VSS Options

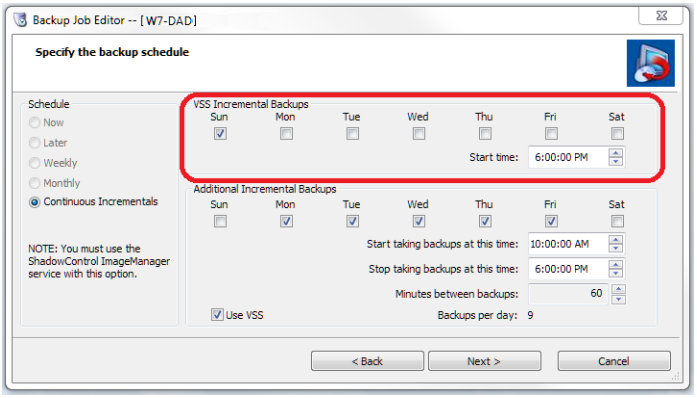
ShadowProtect can configure either a:

- Scheduled VSS and Non-VSS incremental backups
- Non-incremental backups

The linked sections explain these options.

Configuring a Scheduled VSS Backup Job

The Backup Job wizard can configure a scheduled backup job using VSS on one or more days. Use the *VSS Incremental Backups* section of the **Backup Schedule** dialog:



To configure this job:

1. Mark the day(s) to perform the VSS backup.
2. Use the combo box to specify the time to run the VSS job.

   Note: If the aim is to reduce the workload on a server, select a time after business hours.

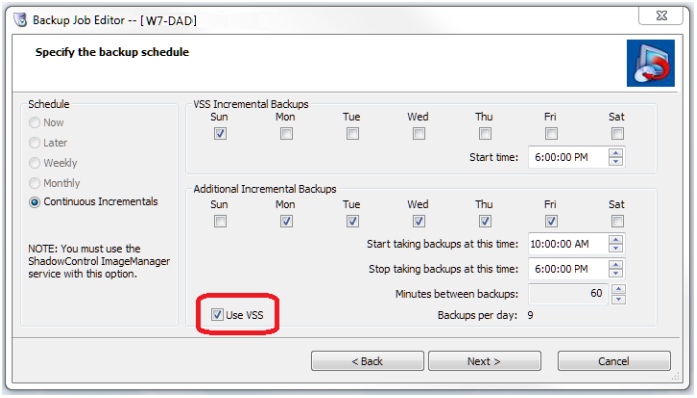
3. Uncheck **Use VSS** in the lower *Additional Incremental Backups* section.

   Note: Leaving the **Use VSS** checkbox marked will cause ShadowProtect to ignore the scheduled VSS backup settings and then to use VSS for all incremental snapshots.

This VSS backup incremental file will be kept in the correct time sequence of the backup job's chain along with the non-VSS backups. In the event of a system restore, select the VSS backup file if possible to ensure a clean restore of the volume.

Configuring a Non-VSS Backup Job

Use the Backup Schedule dialog to configure a non-VSS backup job:



1. Uncheck **Use VSS** in the lower *Additional Incremental Backups* section.

2. Uncheck **Sun** (and any other marked days) in the upper *VSS Incremental Backups* section.

Warning: Consider carefully before executing a non-VSS continuous incremental backup job. Without VSS, there is the potential for lost data and corrupted files particularly with VSS-aware apps. In the event of a restore, these applications may require an extended recovery using the application's tools to repair these losses--the same as would occur to recover from a power failure and without a proper shutdown of the application.

6 Mounting Backup Image Files

The ShadowProtect Explore Backup Wizard guides you through the process of mounting a backup image file. If the selected image file is part of a chain, ShadowProtect automatically associates the needed files required to browse and restore this specific backup image file. You only need to select the backup image you want to explore. Once mounted, you can treat the backup image file as you would any other Windows volume:

- Browse the backup image file.
- Share the backup image file.

- Copy individual files and folders from the backup image file.
- Modify the backup image file (if the volume is configured as writeable).
- Use standard Windows security and file properties.

The restore process is the same whether you restore files and folders in Windows or need to use the StorageCraft Recovery Environment. Which you use depends specifically on the state of your system and what you need to restore:

Restore in 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).
Restore in 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 *StorageCraft Recovery Environment User Guide*.

Note: To restore data from an Incremental image, you must have all previous incremental backup image files and the initial full backup image. If any of these files is missing or corrupt, mounting the backup image to that point in time is not possible. ShadowProtect does not let you modify full images to prevent corrupting an entire image set.

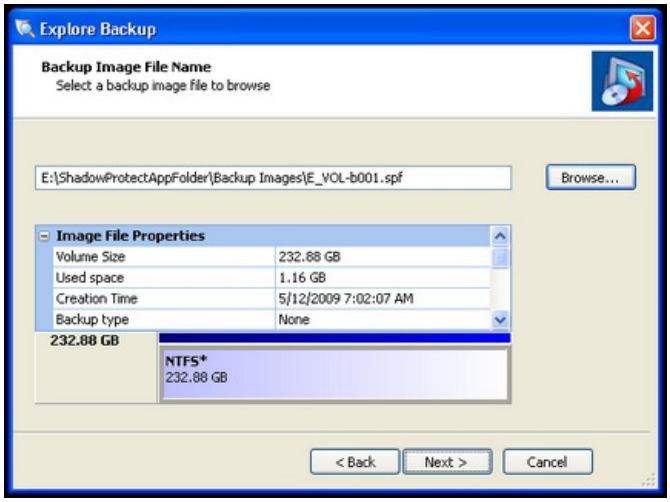
For information about mount options, see Backup Image Mount Options.

To mount a backup image file

1. Start the ShadowProtect Console (see Starting ShadowProtect).
2. Open the Explore Backup Wizard by doing one of the following:
   - In the Wizards tab, click **Explore Backup**.
   - In the Tasks menu, click **Explore Backup**.
   - In the Menu bar, select **Tasks** > **Explore Backup**.
3. On the Backup Image File Name page, browse to the backup image file you want to mount, then click **Next**.
   For information about backup image file naming conventions, see File Naming Conventions.

   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. (Conditional) In the Backup Image Dependencies page, select the desired point-in-time image from the selected backup image set, then click **Next**.
5. On the Explore Options page, select how you want to mount the backup image, then click **Next**.
   For more information about mount options, see Backup Image Mount Options.
   a.To mount the backup image file as a drive letter, select **Assign the following drive letter**, then select the appropriate drive letter from the drop-down list.
   b.To mount the backup image file as a mount point, select **Mount in the following empty NTFS folder**, then browse to the appropriate NTFS folder. You must also specify how to name the mount point sub-folder:
   Time/Date: Uses the backup image's creation date and time as the sub-folder name (for example, 7-12-2008 10.19.24 AM).
   File Name: Uses the backup image file name as the sub-folder name (for example, E_VOL_b001).

Custom: Lets you specify a custom sub-folder name.
c.(Optional) Deselect **Mount Backup as Read-Only** to mount the backup image as a writeable volume.
If you mount the backup image file as a writeable volume, you can choose to save the changes to an Incremental image file when you dismount the volume (see Dismounting Backup Image Files in Windows).

6. On 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.
7. With the backup image mounted, you can browse the contents of the volume as you would any Windows volume.
To restore individual files or folders, simply copy them from the backup image file volume to your production volume.

> **Note**: Once mounted, select Refresh Volumes Info to get an accurate view of the mounted system volumes from the Disk Map tab.

6.1 Mounting Backup Image Files in Windows

ShadowProtect adds two options to the Context menu (the right-click menu) of backup image files:

Mount	Launches the Image File Mount Wizard to guide you through the process of mounting the selected backup image file. For information about the various options in the Image File Mount Wizard, see Mounting Backup Image Files, starting in Step 3. You can simultaneously mount multiple backup image files, but you must mount each backup image file individually with the Image File Mount Wizard.
Quick Mount	Mounts the backup image file as read-only using the next available drive letter. You can select multiple backup image files, then "Quick Mount" them simultaneously, with each backup image file receiving the next available drive letter.

For information about dismounting a backup image file, see Dismounting Backup Image Files.

6.2 Backup Image 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 a 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 Backup Image Files).

Note: ShadowProtect prevents you from modifying a Full image file to prevent corruption of an entire Image Set. ShadowProtect, however, will track changes to the data and can preserve these as a new image file when you dismount the image.

6.3 Dismounting Backup Image Files

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 Backup Image Files). As part of the dismount process, you can do the following:

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

  Note:The Shrink Volume feature truncates mounted backup image files 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).
2. Open the Backup Image Dismount Wizard by doing one of the following:
   - In the Tasks menu, click **Dismount Backup Image**.
   - In the Menu bar, select **Tasks** > **Dismount Backup Image**.
3. In the Mounted Backup Images page, select the backup image volume to dismount, then click **Next**.
   When selecting a mounted backup image, this page also displays the volume properties.
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 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: Shrinks the volume so you can restore the image to a smaller hard drive. This option is available only 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 (based on Windows 7).
5. In the Backup Image Dismount Summary page, review the dismount details, then click Finish.

   Note: Once dismounted, select Refresh Volumes Info to get an accurate view of the mounted system volumes from the Disk Map tab.

Dismounting Backup Image Files in Windows

ShadowProtect adds two options to the Context menu (the right-click menu) of mounted backup image files. (For information about mounting backup image files, see Mounting Backup Image Files.) These options are:

Dismount	Launches the Backup Image Dismount Wizard to guide you through the process of dismounting the selected backup image file. This is most useful to save data changes made to the volume to an incremental file. (For information about the various options in the Backup image Dismount Wizard, see Dismounting Backup Image Files, starting in Step 3.)
Quick Dismount	Dismounts the backup image file without any further user interaction. ShadowProtect dismounts the backup image file without saving any changes made to data on the mounted image.

7 Restoring a Volume

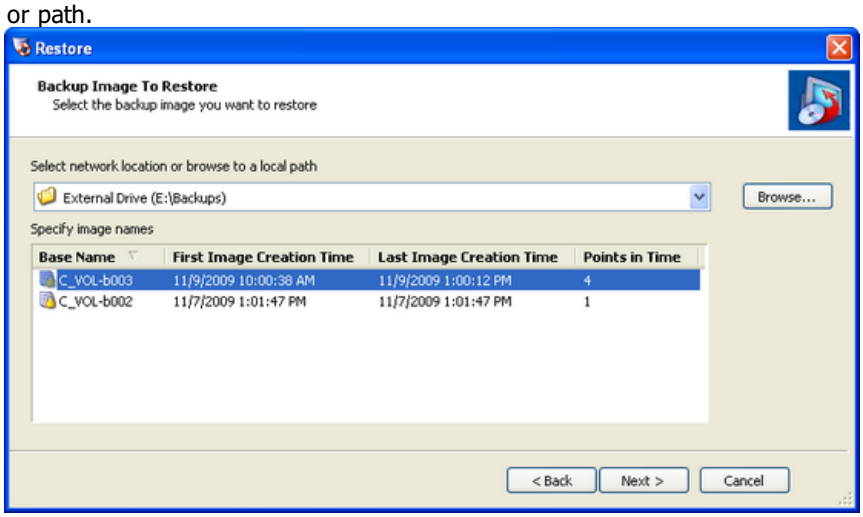
ShadowProtect provides two ways to restore volumes from backup image files:

Restore in Windows	Restore a non-system volume using the ShadowProtect Restore Wizard. This method does not require you to reboot the system.
Restore in Recovery Environment	Use the bootable Recovery Environment when restoring a system volume where the operating system resides. For information about restoring a system volume from the Recovery Environment, see the *StorageCraft Recovery Environment User Guide*.

Warning: Restoring a backup image to an existing volume overwrites all data currently on the volume.

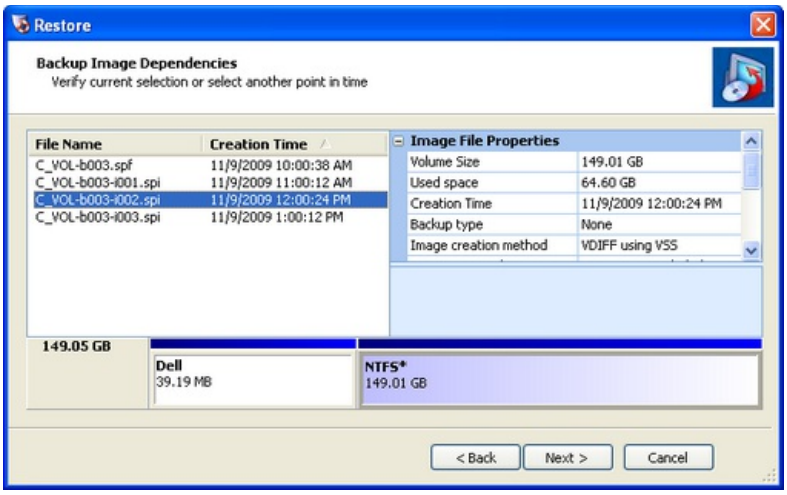
To restore a non-system volume

1. Start the ShadowProtect Console (see Starting ShadowProtect).
2. Open the Restore Wizard by doing one of the following:
   - In the Wizards tab, click **Restore**.
   - In the Tasks menu, click **Restore**.
   - In the Menu bar, select **Tasks** > **Restore**.
3. On the Backup Image to Restore page, select the Image Set to restore, then click **Next**.
   In the drop-down menu, select the Destination (see Destinations) that contains the backup Image Set to restore, or click **Browse** to locate the desired backup image set. The Specify Image Names field displays the backup Image sets available at the selected destination or path.



Note: To restore a volume from a backup image set stored on a network share, you must have the proper network credentials.

4. On the Backup Image Dependencies page, select the point-in-time to restore, then click **Next**.



This page displays all Incremental backup image files associated with the selected Image Set. Select a specific backup image file to view the following image file properties:
Image File Properties: Volume size, creation time,compression, password protection, comment.
Original Partition Information: Style, number, type, bootable option, starting offset and length.
Disk Information: Disk geometry, disk size and number of the first track sectors. You can also view the disk layout graphically at the bottom of the screen. This represents what the disk looked like at the time of backup.
Originating machine: Operating system version, the machine name, MAC address and the ShadowProtect engine version used to create the image file.

5. On the Restore Destination page, select the partition where you want to restore the backup image, then click **Next**.

   Note: The selected partition must have sufficient space for the selected Image Set. For example, you cannot restore a 4GB backup file with only 1GB of free space.

   Right-click a volume to see the following actions in the context menu:
   Delete Volume: Deletes the selected volume. The deleted volume becomes unassigned space on the disk that can be repartitioned.
   Set Active: Sets the selected volume as Active (bootable). Only one partition per drive can be designated as Active.
   Create an exact primary partition: (Available only if unpartitioned disk space exists) Defines and creates 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) Extends the selected partition, then subdivide the extended partition into one or more logical drives.
   Edit Policy: Launches the Partition Creation Policy Editor.

6. On the Specify the Restoration Options page, select the appropriate volume restore options, then click **Next**.
   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.
7. On the Wizard Summary page, review the details of the volume restore operation, then click **Finish**.

You can view the progress of the restore volume operation in the Backup Jobs tab.

8 Image Conversion Tool

ShadowProtect includes the Image Conversion Tool so you can manage existing backup image files, and provides the following primary features:

- Consolidate a point-in-time backup image (Full + Incremental images) into a new Full image.
- Change the compression setting on an existing image.

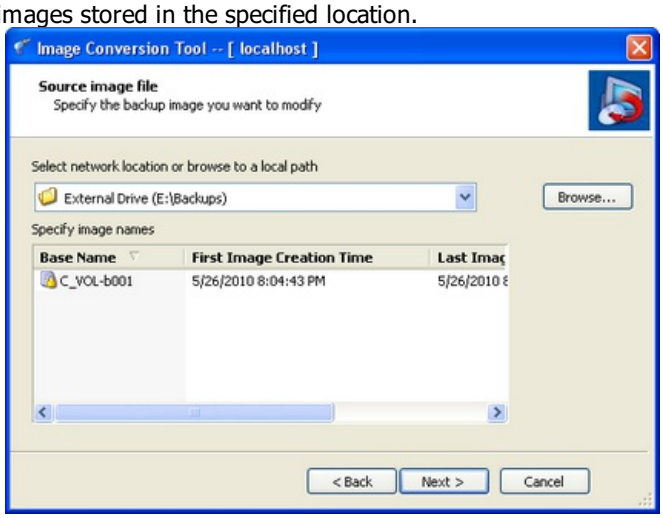
- Change the encryption setting on an existing image.
- Split an backup image file into a Spanned Set where each file has a maximum file size. This is useful for moving backup image files to CD or DVD.
- Convert a backup image into a virtual machine format (VMDK or VHD).

Note: Current hypervisors, including Hyper-V and VMware, limit the size of a VMDK or VHD to under 2 TB.

You can access the Image Conversion Tool from either Windows or the StorageCraft Recovery Environment.

To use the Image Conversion Tool

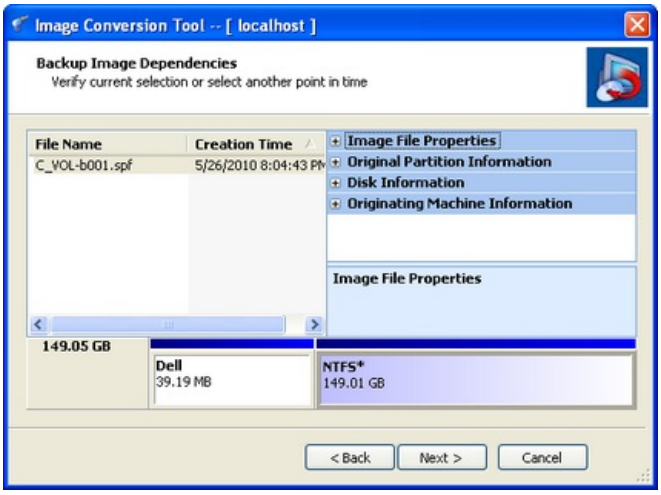
1. Start the ShadowProtect Console (see Starting ShadowProtect).
2. In the Tools menu at the left (or in the Tasks dropdown menu), click **Image Conversion Tool**.
3. The Image Conversion Tool wizard appears. Click **Next**.
4. On the Source Image File page, browse to the location of the backup image files you want to modify. ShadowProtect displays the Full images stored in the specified location.



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

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

6. In the Backup Image Dependencies page, select the Incremental image that represents the point-in-time to consolidate with the Full image, then click **Next**.



   Select a backup image file in the left pane to view its properties in the right pane. ShadowProtect groups backup image file properties into four groups:

   - **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 required information, then click **Next**.

Select network location or browse to a local path	From the drop-down menu, select the Destination (see Destinations) where you want to store the destination image file, or **Browse** to the desired location.
Specify image name	Specify a name for the destination image file.

Save As	Select the type of image file you want to create. Supported options include: **SPF:** Create a new Full (Base) image file. **VHD:** Create a Microsoft Virtual Hard Disk file compatible with Microsoft and Hyper-V virtual environments. **VMDK:** Create a Virtual Machine Disk file compatible with VMWare virtual environments.

8. In the Options page, specify the desired backup image file options. 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 Backup job in the Backup Jobs tab (select the job, then click **Details**). Review the results of previously executed jobs in the Backup History tab.

   Note: After converting a backup image to VHD/VMDK, and assigning it to a VM, make sure to load Recovery Environment in the VM and run Hardware Independent Restore (HIR) on the system volume created by the Image Conversion Tool. You must do this before the operating system will boot successfully. If you still have boot problems after doing this, use Recovery Environment's Boot Configuration Utility (BCU) to auto-fix any problems it encounters. For more information, see "Using HIR" and "Using the Boot Configuration Utility" in the *StorageCraft Recovery Environment User Guide*.

9 Remote Management

ShadowProtect provides two ways to remotely manage ShadowProtect Backup Agents installed on remote servers and desktops (known as remote nodes), as long as these systems are accessible through the local area network or a virtual private network (VPN). By connecting to a remote node through one of these tools, you have full access to ShadowProtect features and functionality on the remote node.

- Remote Management with the Management Console
- Remote Management with the Network View

Note: You must have administrative rights to the remote node in order to manage it. However, with the proper administrative rights, you can remotely manage both ShadowProtect Server Edition and ShadowProtect Desktop Edition nodes using either the Management View or the Network View.

9.1 Remote Management with the Management Console

The Management View tab is designed specifically for ShadowProtect Server and ShadowProtect SBS users that need to manage a larger number of remote ShadowProtect installations from a central location.

Although the functionality is very similar to the Network View, the Management View organizes it in a way to make it more friendly to administrators with many remote nodes to manage. You can open and close the Management View by selecting **Management View** in the View menu (see Management View Tab).

You can do the following from the Management View:

- Installing the Backup Agent Remotely
- Mgmt View - Adding and Deleting Remote Nodes
- Mgmt View - Modifying Remote Node Properties
- Mgmt View - Connecting and Disconnecting Remote Nodes

Installing the Backup Agent Remotely

Using the Push Agent, Management View lets you remotely install the ShadowProtect Backup agent so you can configure ShadowProtect operations on the remote system.

To remotely install the backup agent

1. Start the ShadowProtect Console (see Starting ShadowProtect).
2. In the Management View tab, click **Install**.
3. The Push Install Wizard so you can configure the remote installation.
4. On the Specify Installer Package page, browse to the ShadowProtect Installer Package that you want to use for the remote installation, then click **Next**.
   There must be an associated installation setup file (.iss) with the selected installer package. For more information, see Creating an Install Setup Package.

5. In the Choose Search Options and Proper Credentials dialog box, provide the required information, then click **Next**.

System Name	The name of the system where you want to install the ShadowProtect Backup agent. Select either **Domain name** or **Host name** according to the type of system name you are providing, then type the system name in the field. Note: If you leave the field blank, Push Install uses your current domain or workgroup to locate a list of available systems.
Use Active Directory Search	Instructs ShadowProtect to search Microsoft Active Directory for the desired system. To use this parameter, click **options** (at the bottom of the Push Install dialog box when **Use Active Directory search** is selected) to refine the Active Directory search characteristics.
Use Specified Credentials	The authentication credentials that Push Install uses to gain access to the remote system. **Note:** If you do not provide credentials, Push Install uses your current credentials to attempt to access the remote system.
Discover Services	Push Install attempts to identify existing ShadowProtect services running on remote systems. When successful, it displays the information it gathers about agent version.
Automatically activate installed agents	Push Install automatically activates the Backup agent it installs. To use this parameter, click **settings** (at the bottom of the Push Install dialog box when **Automatically activate installed agents** is selected) to specify the Username and Serial # of the ShadowProtect license you want to use on the remote system.
Reboot after install	Following a successful Backup agent install, ShadowProtect automatically re-boots the remote system so the Backup agent is active. To use this parameter, click **settings** (at the bottom of the Push Install dialog box when **Reboot after install** is selected) to specify the details of the reboot operation. You can instruct the remote system to reboot at a specific date/time; specify a message to display before rebooting; and specify a delay before the reboot occurs (in seconds).

6. (Conditional) On the Computers Overview page, select the systems where you want to install the Backup agent, then click **Next**.
   If you didn't specify a system name, you can select the systems where you want to install the Backup agent here.
7. On the Install Overview page, wait until the install finishes, then click **Next**.
8. (Optional) On the Post Install Overview page, specify a Group name for each system where you installed the Backup agent, then click **Next**.
   Click in the **Group name** field, then type of select the group where you want to add this system. For more information about Groups, see Mgmt View - Modifying Remote Node Properties.
9. On the Summary page, click **Finish**.
   The newly installed remote nodes appear in the Management View node list.

Mgmt View - Adding and Deleting Remote Nodes

Before managing a remote node, you must add it to your Management View.

To add a remote node

1. Start the ShadowProtect Console (see Starting ShadowProtect).
2. In the Management View tab, click **Add** .
3. In the Server Details dialog box, specify the appropriate connection information for the remote node.
   For information about remote node properties, see Mgmt View - Modifying Remote Node Properties.
   You can now connect to the remote node to manage ShadowProtect.

To delete a remote node

1. In the Management View tab, select the remote node in the node list.
2. Click **Delete** .
   Deleting a remote node does not delete ShadowProtect or any of its configurations from the remote node, or remove the remote node from the Management View of any other system that might be configured to remotely manage that node.

Note: You cannot delete the local node from the Management View.

Mgmt View - Modifying Remote Node Properties

The properties table displays the properties of the currently selected remote node. You can edit remote node properties as long as the remote node is not connected.

To modify the properties of a remote node

1. Start the ShadowProtect Console (see Starting ShadowProtect).
   If the Network View is not visible, select **Network View** from the View menu.
2. In the node list, select a remote node to modify.
   If the Server Properties pane is not visible, click **Properties**.
3. In the Server properties pane, modify the remote node properties as needed.
   Select a field to make it active. You can also use the Tab key to move from field to field. Remote Node properties include the following:

Server Name	A remote node name used to identify it in the node list.
Server Address	The IP address or machine name of the remote node. To browse the network for a particular system so you can find the IP address, click **Browse**.
Group	The group that you want to associate with the remote node. You can create groups to help organize remote nodes and make management easier.
Server Description	A description of the remote node. This is for your information only.
Status	(Informational) The remote node status (Connected or Disconnected).
Domain Name	The domain name used to access the remote node.
User Name	A user name with Administrator rights to the remote node.
Password	The user name's associated password.
Agent Version	(Informational) The version of the Backup Agent installed on the remote node.
Last Connected	(Informational) The date and time you last connected to the remote node.

Mgmt View - Connecting and Disconnecting Remote Nodes

To connect to a remote node

1. Start the ShadowProtect Console (see Starting ShadowProtect).
2. In the Management View tab, select the remote node in the node list.
3. Click Connect.

   You can be connected to only one node at a time. If you connect to another remote node, ShadowProtect automatically disconnects you from the previously connected node.

   Note: You must add a remote node in order to connect to it (see Mgmt View - Adding and Deleting Remote Nodes).

To disconnect a remote node

1. In the Management View tab, select the remote node in the node list.
2. Click **Disconnect**.

   Disconnecting a remote node does not stop the ShadowProtect Backup Agent or affect any of ShadowProtect operations on the remote node.

9.2 Remote Management with the Network View

When open, the Network View appears as a right panel in the ShadowProtect Console. You can open and close the Network View by selecting **Network View** in the View menu (see Network View).

You can do the following from the Network View:

- Mgmt View - Adding and Deleting Remote Nodes
- Mgmt View - Modifying Remote Node Properties
- Mgmt View - Connecting and Disconnecting Remote Nodes
- Exporting and Importing Node Settings

Network View - Adding and Deleting Remote Nodes

Before managing a remote node, you must add it to your Network View.

To add a remote node

1. Start the ShadowProtect Console (see Starting ShadowProtect).
   If the Network View is not visible, select **Network View** from the View menu.
2. In the Network View, click Add .
   This creates a new node in the Network View named *New Node 1* and opens a Server Properties pane where you can configure the remote node.
3. In the Server Properties pane, specify the appropriate connection information for the remote node.
   For information about remote node properties, see Network View - Modifying Remote Node Properties.

You can now connect to the remote node and manage ShadowProtect.

To delete a remote node

1. In the Network View, select the remote node in the node list.
2. Click Delete .
   Deleting a remote node does not delete ShadowProtect or any of its configurations from the remote node, or remove the remote node from the Network View of any other system that might be configured to remotely manage that node.

Note: You cannot delete the local node from the Network View.

Network View - Modifying Remote Node Properties

The properties table displays the properties of the currently selected remote node. You can edit remote node properties as long as the remote node is not connected.

To modify the properties of a remote node

1. Start the ShadowProtect Console (see Starting ShadowProtect).
   If the Network View is not visible, select **Network View** from the View menu.
2. In the node list, select a remote node to modify.
   If the Server Properties pane is not visible, click **Properties** .
3. In the Server properties pane, modify the remote node properties as needed.
   Select a field to make it active. You can also use the Tab key to move from field to field. Remote Node properties include the following:

Server Name	A remote node name used to identify it in the node list.
Server Address	The IP address or machine name of the remote node. To browse the network for a particular system so you can find the IP address, click Browse .
Group	The group that you want to associate with the remote node. You can create groups to help organize remote nodes and make management easier.
Server Description	A description of the remote node. This is for your information only.
Status	(Informational) The remote node status (Connected or Disconnected).
Domain Name	The domain name used to access the remote node.
User Name	A user name with Administrator rights to the remote node.

Password	The user name's associated password.
Agent Version	(Informational) The version of the Backup Agent installed on the remote node.
Last Connected	(Informational) The date and time you last connected to the remote node.

Network View - Connecting and Disconnecting Remote Nodes

To connect to a remote node

1. Start the ShadowProtect Console (see Starting ShadowProtect).
   If the Network View is not visible, select **Network View** from the View menu.
2. In the Network View, select the remote node in the node list.
3. Click Connect.

   You can only be connected to a single node at a time, so if you connect to another remote node, ShadowProtect automatically disconnects you from the previously connected remote node.

   Note: You must add a remote node in order to connect to it (see Network View - Adding and Deleting Remote Nodes).

To disconnect a remote node

1. In the Network View, select the remote node in the node list.
2. Click **Disconnect**.

   Disconnecting a remote node does not stop the ShadowProtect Backup Agent or affect any of ShadowProtect operations on the remote node.

Exporting and Importing Node Settings

ShadowProtect lets you transfer remote node configurations from one ShadowProtect Console to another.

To export remote node configurations

1. Start the ShadowProtect Console (see Starting ShadowProtect).
   If the Network View is not visible, select **Network View** from the View menu.
2. In the Network View, click **Export nodes**.
3. Specify the name for the XML file that contains the exported remote node configurations, then click **Save**.

To import remote node configurations

1. In the Network View, click Import nodes.
2. Browse to the XML file that contains the previously exported remote node configurations, then click **Open**.

9.3 Using an Install Setup Package

The ShadowProtect Install Setup Package contains the recorded selections and settings for a ShadowProtect push installation. You can use these recorded configurations to automate push installs. ShadowProtect includes two setup package files: one for a full and one for an agent-only install.

Note: An Install Setup package file must have the same name as the Installer package but with a .iss extension.

To use a ShadowProtect Install Package

1. Determine the path to the appropriate .iss file (Agent or Full) in the ShadowProtect install package.
2. Open a Windows command prompt.
   Click **Start** > **Run**. Enter cmd in the **Open** field, then click **OK**.
3. Browse (using the cd command) to the directory that contains the ShadowProtect installer to use for the remote install.

4. Execute the ShadowProtect installer using command-line parameters. For example:

   ```
   c:\Install\ShadowProtectSetup.exe /s /f1c:\storagecraft\ShadowProtectSetup.iss.
   ```

   where the path in the /fl switch points to the appropriate .iss file (agent or full). The Setup program proceeds to do the install.

Note: Avoid directory names with spaces for .iss installs. The install may fail as the command line attempts to interpret paths with spaces in directory names.

Command Line Switches

The remote install command includes these switches:

/s	Runs InstallShield Silent to execute a silent setup.
/f1	Specifies where to locate the install package. Do *not* put a space between the parameter and the path information. For example, the parameter `/fl c:\storagecraft` is *incorrect*. The correct syntax is `/f1c:\storagecraft`.

10 Using VirtualBoot

VirtualBoot lets ShadowProtect users boot a system volume backup image in a Virtual Machine (VM) environment. VirtualBoot leverages the open source Oracle VirtualBox software so you can quickly boot the backup image without performing a time-consuming restore operation, and without converting backup image files to a different format.

VirtualBoot provides tremendous value in the following situations:

System Fail-over: When you're dealing with Terabytes of storage, restoring a failed system can take days. However, VirtualBoot lets you quickly recreate your failed system in a VM while you rebuild the failed system. Users have full access to the system during this time, with only a brief downtime to cut-over to the new system once it is ready. Downtime drops from days to just minutes.

Backup Test: Disaster recovery is all about having system data stored in a way that is readily accessible should it be needed. But can you be confident that your stored data is valid? VirtualBoot lets you mount any backup image in a VM so you can test it to make sure a restored system would function properly. In just minutes you can feel confident that your backup images are ready for use when needed.

Application-specific Data: While backing up system data is a critical operation, sometimes the data files alone aren't useful without their associated applications. VirtualBoot lets you mount an entire system, both applications and data, in a VM where you have access to data from its associated application.

For information about VirtualBoot usage scenarios, see VirtualBoot Scenarios.

This section includes the following topics:

Note: DeveloperNotes_VirtualBoot.txt contains developer-level information related to VirtualBoot. You can find this file in the *<install_folder>*\StorageCraft\ShadowProtect\ folder. This file gives troubleshooting and advanced technical details for using VirtualBoot.

Warning: If you want to power off a VM created with VirtualBoot, do *not* select *Restore current snapshot VirtualBoot *as a shutdown option, or you will lose all Incremental backup data written in the VM since its creation. Select this option *only* if you want to revert the VM back to its original state.

10.1 VirtualBoot Requirements

VirtualBoot requires you to install the following software to use it:

Software Requirements

ShadowProtect 4.*x* or later: VirtualBoot supports backup image files created by any version of ShadowProtect, but you must have ShadowProtect 4.*x* or later to run the application. ShadowProtect 4.*x* includes VirtualBoot as a core component of the console installation.

Note: Although VirtualBoot can generate a VM from backup image files created with any version of ShadowProtect, StorageCraft recommends using VirtualBoot with backup image files created by ShadowProtect 3.3 and later to get full access to the benefits of VirtualBoot.

VirtualBox: VirtualBox is an open source VM environment from Oracle. VirtualBoot provides native support for ShadowProtect files in a VirtualBox VM. For information about VirtualBox, and to download the software, visit www.virtualbox.org.

ShadowProtect supports various versions of VirtualBox, up through v4.1.6. Please refer to the VirtualBoot Developer Notes found in the ShadowProtect directory for details on the latest supported versions.

Warning:VirtualBoot will not support VirtualBox 4.0.0 as that version does not properly use third-party plugins.

Hardware Requirements

VirtualBoot hardware requirements are driven primarily by the hardware requirements necessary to run VirtualBox (see VirtualBox End-User Documentation).

Processor: Reasonably powerful x86 processor (either Intel or AMD), including AMD/Intel x64 processors. VirtualBoot does not support Itanium (IA64).

Note: When using VirtualBoot to boot an image of an x64 operating system, make sure that your host hardware supports AMD-V or VT-x, and that AMD-V, or VT-x, is enabled in the host machine's hardware BIOS settings.

Memory: At least 1GB.

Hard Drive: At least 10 GB. This is dependent upon the Operating System you want to load in the VM.

Host OS: VirtualBoot supports the same Host operating systems as VirtualBox 1.6; namely Windows XP or later. Windows 2000 is not supported.

Guest OS: VirtualBoot supports backup image files that contain backups of the following operating systems (This is the OS that runs in the VM):

- Windows 2000
- Windows XP (32- and 64-bit)
- Windows 2003 (32- and 64-bit)
- Windows Vista (32- and 64-bit)
- Windows 2008 (32- and 64-bit)
- Windows 2008 R2 (32- and 64-bit)
- Windows 7 (32- and 64-bit)

10.2 Limitations

This release of VirtualBoot has the following limitations:

- Supports boot volumes up to 2TB. However, VirtualBoot supports data volumes (non-bootable) of any size.
- Does not support LBD hard disk volumes, which report 4096-byte sector size to the OS. However, Advanced Format hard disks, which have 4096-byte sectors but report 512-byte sectors to the OS, are supported.
- If the host crashes while running a VirtualBoot VM, you must create a new VM using the latest Incremental backup image file created in the VM. For more information, see the VirtualBoot Scenarios.
- VirtualBoot does not work in a Windows 2000 Terminal Services session.

10.3 Creating a VM

Important: Before using VirtualBoot to create a VM, review the VirtualBoot Requirements and Limitations.

To create a virtual machine

1. Start VirtualBoot, then click **Next** on the VirtualBoot Wizard welcome page.
   There are three ways to start VirtualBoot:

Executable:	In Windows, select **Start** > **ShadowProtect** > **VirtualBoot**.
Command Line:	From a Windows command prompt, type VirtualBoot *<backup image file>*, where *<backup image file>* is the name, including full path, of the ShadowProtect backup image file that you want to use to create a VM. For example: `VirtualBoot e:\backups\C_VOL-b005.spi`
Right-Click Menu:	In Windows Explorer, right-click the ShadowProtect backup image file that you want to use to create a VM, then select **VirtualBoot**.

2. In the Backup Image List page, provide the required information, then click **Next**.
   If you start VirtualBoot using the command line or right-click menu option, VirtualBoot populates the Backup Image list with all files that are part of the backup chain for the specified backup image file.

Add Image File	Lets you add a backup image file to the VM. Use this if you have a separate data volume you want to add to the boot volme. If the selected backup image file is encrypted, you must provide a valid password to access it.
Remove Image File	Lets you remove a backup image file from the VM.
Specify Boot Volume	Lets you designate the boot volume in the VM. Typically, VirtualBoot detects this automatically, but if you include multiple bootable volumes in the VM, you can select the volume that VirtualBoot designates as the boot volume.

   Note: If you specified a backup image file when starting VirtualBoot, this page lists the related backup image file information.

3. In the Options page, provide the required information, then click **Next**.

Specify the operating system for the new virtual machine	From the dropdown menu, select the Windows OS contained in the boot volume of the backup image file.
Automatically create the new virtual machine	Select this option to have VirtualBoot automatically create the VM as part of the configuration process. If you do not select this option, you must manually configure the VM in VirtualBox. In either case, VirtualBoot creates the XSP files that VirtualBox uses to define the virtual disk drives in the VM. Note: VirtualBoot ALWAYS places the boot volume in the Disk_0 XSP file. For more information, see Creating a VM Manually.
Automatically start the new virtual machine	Select this option to launch VirtualBox automatically after the VM is complete and load it for use.
Specify the name of the new virtual machine	Specify a name for the VM. By default, VirtualBoot creates a name based on the machine name.
Specify the amount of memory to allocate to the new virtual machine	Specify the amount of memory, in MB, that VirtualBox should allocate for use by the VM when it loads.
Specify the VM network adapter type	Select whether to include a network adapter in the VM. Supported options include: **NAT PRO/1000 MT Desktop:** Adds a generic network adapter to the VM that uses Network Address Translation (NAT). **No Network Adapter:** Excludes a network adapter from the VM.

4. (Optional) On the Options page, click **Advanced** to open the Advanced Options dialog box.
   The Advanced Options dialog box provides the following options:

Import only one volume per hard disk drive within the virtual machine	Instructs VirtualBoot to include only one volume per VirtualBox XSP file. By default, VirtualBoot assigns four volumes per XSP file. **Note:** VirtualBoot ALWAYS places the boot volume in the Disk_0 XSP file.

Deactivate Windows within the virtual machine	number of reactivations, this options lets you use the activation grace period to accomplish your purposes with the VM. **Note:** If the host hardware where you start the VM is sufficiently different, Windows might deactivate automatically.
Store write buffers in a different directory than the image files	Lets you specify a location to store the write buffers used when creating the VM. By default, VirtualBoot stores write buffers in the same location as the backup image files used to create the VM.
Override personality used to configure the virtual machine OS volume	For use only by StorageCraft technical support.

5. On the Wizard Summary page, click **Finish**.
   VirtualBoot generates the files necessary to support the new VM and, if specified in the VM configuration, creates the VM and launches it for use.
   Note: For information about manually creating a VM in VirtualBox, see Creating a VM Manually.
6. You may need to do further configuration on the VM if, for example, you want to use the VM as a temporary replacement for a server. If so, continue with Configuring a VM and refer to the VirtualBox documentation for details.

To Restart an existing Virtual Machine

You can also restart an existing VM manually from VirtualBox:

1. Launch VirtualBox.
2. In the left-side VM list, select the VM, then click **Start**.

Continuing Incremental Backups

To use VirtualBoot in a hardware failure scenario, you must configure Incremental backups to continue in the VM. For more information, see the VirtualBoot Scenarios. When working with a VirtualBoot VM, remember the following important considerations:

- To prevent performance problems in the VM, use backup jobs that use Incremental backups (preferably Creating Backup Image Files). Do not use Differential imaging.
- Any ShadowProtect backup jobs in the VirtualBoot VM are Paused/Disabled state. After starting the VM, manually re-start the backup job (in the Backup Jobs tab) to continue making backups.
- If you power off a VM created with VirtualBoot, DO NOT select **Restore current snapshot VirtualBoot** as a shutdown option, or you will lose all Incremental backup data written in the VM since its creation. Select this option only if you want to revert the VM back to its original state.

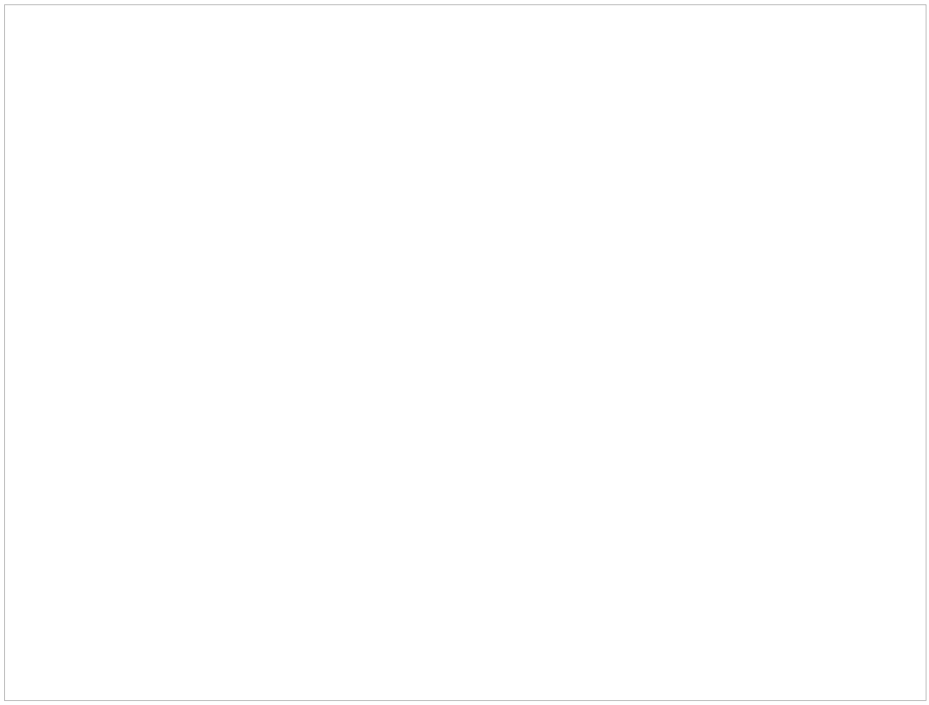
To continue incremental backups in the VM

1. Launch your VM using either VirtualBoot (by selecting the relevant image file in Windows Explorer) or VirtualBox (by selecting the appropriate pre-existing VM).
2. Once the VM loads, log in, then start ShadowProtect in the VM.
3. In ShadowProtect, select the Destinations tab.
4. In the Destinations tab, select the destination object used to store the VM's source backup image files, then click **Edit**.
   - **Warning:** Do not delete the destination object or you will break the backup image chain. Rather, modify the destination object as needed to point to the current location of the backup image files used to create the VM.
5. In the Destination dialog box, modify the Destination Path to point to the location of the backup image files used to create the VM, then click **OK**.
   You might need to modify the network credentials (Domain, User, Password) in the destination object to access the backup image files in their new location. If you have problems with name resolution in the VM environment, try using the IP address of the host machine rather than its Host name.
   When editing the Destination Object path, use only real SMB/CIFS network share paths. Do not use share paths provided in the VM-to-Host file sharing facility of the VirtualBox "Guest Additions".
6. In the ShadowProtect main page, select the Backups tab.
7. Select the appropriate backup job, then click **Execute**.
   ShadowProtect starts an incremental backup job. The naming of incremental backup files in the VM starts where the last Incremental image file used to create the VirtualBoot VM left off. The new incremental image file depends on the Incremental image file chain used to create the VM. This maintains a single backup image chain and makes it possible to provide Head Start Restore (HSR) capabilities.
   - **Warning:** When continuing Incremental backups in the VM and using VirtualBox's Virtual Media Manager to Remove managed XSP files, make sure to specify that you want to keep the storage unit of the XSP disks for the VM where you continued creating Incremental backups. Otherwise, VirtualBox deletes the XSP file and all other associated files, including the Incremental backup image file created by VirtualBoot (You can identify this file because the file name includes a GUID value). Any Incremental backups created in the VM are dependent upon the VirtualBoot Incremental backup image file. By deleting it, VirtualBox renders all Incrementals created in the VM unusable.

Creating a VM Manually

If you elect not to have VirtualBoot create the VM for you (see Creating a VM), you can use VirtualBox to create it. Unlike VirtualBoot, however, you will need to manually configure the virtual machine and then restore the desired image files to the new VM. We strongly recommend using the automated VirtualBoot process instead.

Note: The following task is based on VirtualBox v 4.1.12. Task details might vary slightly with different versions of VirtualBox.



To manually create a virtual machine

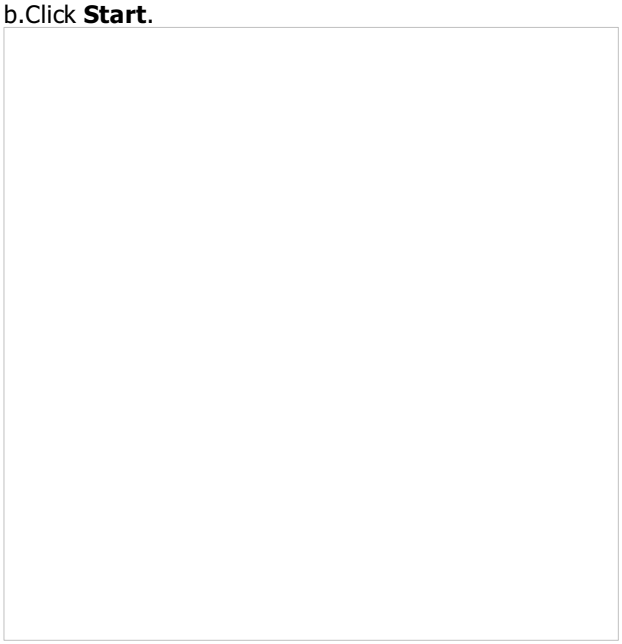
1. Launch VirtualBox.
2. In VirtualBox, select **File** > **Virtual Media Manager**., then select the **Hard Disks** tab.
3. Review the listed .xsp files to see if your required boot volume is listed. (VirtualBoot virtual hard disk files have a .xsp extension.These XSP files contain lists of the backup image files that will constitute the virtual hard drive used by the VM.)
4. If your boot volume .xsp file isn't listed, but has been created, click **Add.**
5. Browse to and select the required XSP file previously created by VirtualBox.
   This adds the selected XSP file as a managed hard disk that you can assign to any VirtualBox VM.

   Note: Make sure you select the _Disk_0 XSP file as the VM's first disk, as this disk always contains the boot volume.
6. Click **New**. The New Virtual Machine Wizard appears.
7. Click **Next**.
8. On the VM Name and OS Type page, specify the required information, then click **Next**.

Name	The name of the virtual machine. You should make the name descriptive of the OS and environment used in the VM.
Operating System	The model of operating system used in the VM. VirtualBoot supports only Microsoft Windows.
Version	The specific Windows operating system used in the VM.

9. On the Memory page, specify the amount of system memory (RAM) to allocate for use by the VM.
   More memory makes the VM faster and more efficient. StorageCraft recommends at least 512MB.
10. On the Virtual Hard Disk page, select **Use existing hard disk**, then select the bootable virtual disk created by VirtualBoot.

    Note: If your desired virtual hard disk does not exist, you will need to do a restore of your selected image files to a fresh virtual disk using ShadowProtect.
11. On the Summary page, click **Finish**.
    VirtualBox creates the VM.
12. Once created, you can start the VM manually from VirtualBox.
    a.Select the VM In the left-side list.
    b.Click **Start**.



13. Continue with Configuring a VM Manually.

Configuring a VM Manually

Once you have used VirtualBox to manually create and launch a VM, you must configure it for use, much like you might configure a new Windows installation. This process involves the following tasks:

- Configuring Drivers
- Installing Guest Additions
- Configuring a Network Adapter
- Continuing Incremental Backups

Note: When working with a VM, you must be able to switch keyboard/mouse focus between the VM and your system environment. To switch focus to the VM, simply click the mouse in the VM window. To switch focus out of the VM, press the right Ctrl button.

Configuring a Network Adapter

If you choose not to have VirtualBoot create a network adapter (NIC) in the VM, you can add it after the fact. For the following reasons, this might be a good idea if you want to boot a backup image while the source system is still operational, which can cause the following issues:

- Two systems on the network with the same network ID can cause routing problems, particularly at the Domain controllers.
- Both the VM and the source system might save Incremental backup images to the same network location. This does not affect data integrity, but can lead to confusing backup image file names, with Incremental backup image files from both branches of the chain intermixed.

Keeping the VM off the network lets you resolve these types of issues before they cause any problems. For example, once the VM loads you can pause ShadowProtect backup operations in the VM.

To add network support to the VM

1. Launch VirtualBox.
2. On the VirtualBox main page, select the VM where you want to add a NIC, then click **Settings**.
   The VM must be powered off to modify the VM settings.
3. On the Settings page, select **Network** in the left-side navigation.
4. Select the Adapter 1 tab, then select **Enable Network Adapter**.
5. In the **Attached To** field, select how you want the virtual NIC to communicate with your host.
   By default, VirtualBox uses Network Address Translation (NAT), but it supports other connection options. For more information, see the VirtualBox documentation. A Bridged Adapter is necessary if you want VM services to be visible to other network hosts. For example, during a failover scenario for an Microsoft Exchange server.
6. Click **Advanced**, then select the virtual adapter type to use in the VM.
   In testing, the "Intel Pro/1000 MT Desktop" appears to be a good generic driver for the VirtualBoot environment.
7. Click **OK** to modify the network adapter settings.

Configuring Drivers

After starting a VM for the first time, you must allow Windows to detect and configure drivers for the VM environment.

To configure a virtual machine for use

1. In the VM window, click **Machine** > **Insert Ctrl-Alt-Delete** to launch the Windows login, then log in to the VM.
   Click in the VM window to transfer mouse and keyboard control to the VM.
2. Allow Windows to identify hardware and install drivers in the VM.
   Windows goes through it's initial boot sequence, identifying hardware and attempting to load drivers for those devices. This process is similar to performing a Hardware Independent Restore (HIR) in ShadowProtect. Follow the on-screen prompts and allow Windows to reboot as needed to load the necessary drivers.
3. After rebooting, log in to the VM.

Note: Because of hardware changes detected by Windows as part of the transition to the VM environment, you will likely be prompted to reactivate Windows when you log in to the VM. However, you typically have a three-day grace period for doing this. Because Microsoft restricts the number of hardware reactivations for each Windows license, you might want to leave Windows deactivated if you can get the production system ready to restore within the three day grace period. If this is not possible, activate Windows in the VM using the standard Microsoft activation process, and your Windows VM is licensed for as long as you need it.

If your Windows installation does not grant a login grace period and requires immediate reactivation, try booting into Safe Mode, or Safe Mode with Networking, to log in.

Installing Guest Additions

After Windows has installed drivers for the VM environment, you can install VirtualBox additions that provide enhanced interaction with, and control over, the VM environment.

To install VirtualBox guest additions

1. From the VM menu bar, select **Devices** > **Install Guest Additions**.
   This loads a virtual CD into the VM that has extra software designed to make the VM run quickly and smoothly. If the CD does not auto-run, browse the CD drive in the VM and execute one of the following:
   - `VBoxWindowsAdditions-x86.exe`: 32-bit Windows VM.

- `VBoxWindowsAdditions-amd64.exe`: 64-bit Windows VM.

2. Follow the directions in the Guest Additions Wizard, then reboot the VM.
3. Log in to the VM.

11 Other Operations

ShadowProtect provides the following features to help you manage and maintain your backup environment:

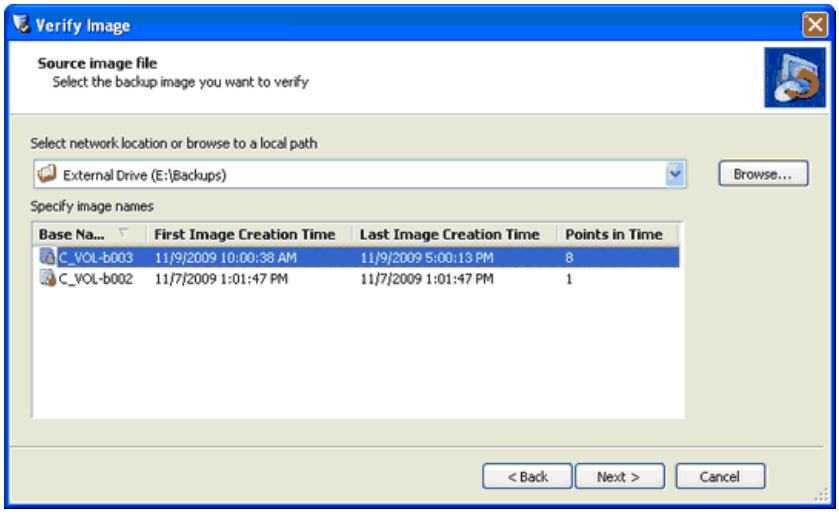
11.1 Verifying Backup Image Files

It is important to verify the quality and integrity of backup images on a routine basis to ensure that a backup image is ready should you need it.

One way to do this is to mount a backup image and browse the files and folders. If you can do this successfully, you know the backup image is healthy. However, you can also use the Verify Image tool to test the integrity of a specific backup image.

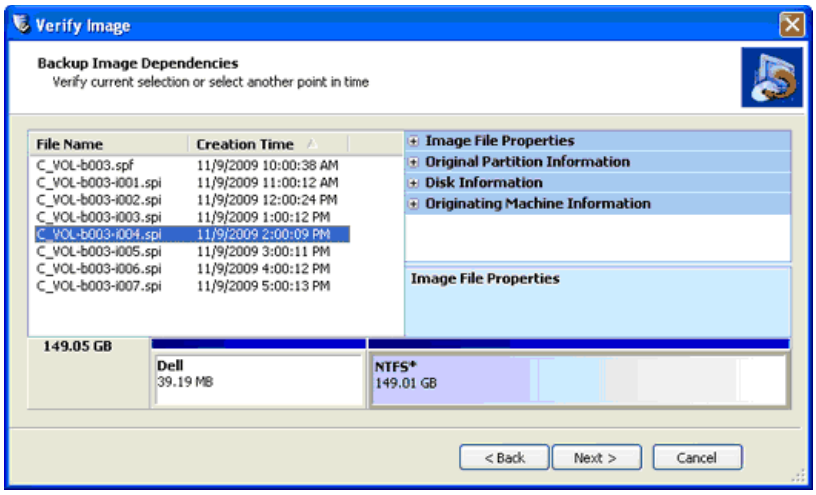
To test a backup image with the Verify Image tool

1. Start the ShadowProtect Console (see Starting ShadowProtect).
2. Open the Verify Image Wizard by doing one of the following:
   - In the Tools menu, click **Verify Image**.
   - In the Menu bar, select **Tasks** > **Verify Image**.
3. On the *Source Image File* page, select the Image Set to verify, then click **Next**.



Note: To verify a backup Image Set stored on a network share, you must have the proper network credentials.

4. On the *Backup Image Dependencies* page, select the point-in-time to verify.



This page displays all Incremental backup image files associated with the selected Image Set. Select a specific backup image file to view the following image file properties:

Image File Properties:	Volume size, creation time, compression, password protection, comment.
Original Partition Information:	Style, number, type, bootable option, starting offset and length.
Disk Information:	Disk geometry, disk size and number of the first track sectors. You can also view the disk layout graphically at the bottom of the screen. This represents what the disk looked like at the time of backup.
Originating machine:	Operating system version, the machine name, MAC address and the ShadowProtect engine version used to create the image file.

5. Once you select the point-in-time you want to verify, click **Next.**
6. On the *Specify the Verify Options* page, select what you want to verify, then click **Next:**

Verify only selected image:	The Verify Image tool checks only the selected backup image file.
Verify selected image and all dependent files:	Verifies the selected backup image file and all files that it depends on. This verifies the integrity of the full point-in-time backup. If you select this option, specify the order to verify the files (Newest to Oldest or Oldest to Newest).

7. On the *Wizard Summary* page, review the details of the verify operation, then click **Finish**.

You can view the progress of verify operations in the Backup Jobs tab.

11.2 Configuring Email Notifications

ShadowProtect can be configured to send Email notifications on the success or failure of a backup job. The Email notification includes the following information:

- **Email Subject:** Indicates that this notification is for a successful or unsuccessful back up job.
- **Email Body:** Contains the following information about the backup job.
  - Start time
  - Finish time
  - Source volume
  - Destination path

To configure email notifications

Note: When doing this, make sure your external email account has POP/IMAP support enabled.

1. Start the ShadowProtect Console (see Starting ShadowProtect).
2. In the Menu bar, select **Options** > **Agent Options**.

3. On the Agent Options page, provide the details of the Email configuration, then click **OK**.

SMTP Server Name or IP Address	The host name or IP address of the outgoing SMTP server to use when sending Email notifications (for example smtp@gmail.com).
SMTP Port	(default: 25) The port used by the SMTP service. The default port for secure SMTP connections (SSL), is 465.
SMTP Login User Name	The username ShadowProtect uses to access the SMTP server. For example, jdoe@gmail.com.
SMTP Login Password	The password associated with the SMTP user name.
SMTP Authentication Method	The authentication method used by the SMTP server. Select the appropriate authentication method for your SMTP server from the drop-down list. For example, the SMTP authentication method for Gmail is Login.
Use SSL	(Default: Off) Indicates if you want to use a secure connection to communicate with the SMTP server. When using SSL, make sure to set the SMTP Port accordingly.
Email From Address	The Email address that appears in email message's From field.
Email To Addresses	A semi-colon separated list of Email addresses that you want to receive the notification. For example, jdoe@gmail.com;jsmith@gmail.com.
Custom Subject Suffix	(Optional) A text string that appears below the ShadowProtect-generated email content in the Subject field. When creating this content, use /r for carriage return, /n for new line, and /t for tab characters.
Custom Body Prefix	(Optional) A text string that appears in the email Message field. Use /r for carriage return, /n for new line, and /t for tab characters.
Send Email on Success	(Default: Off) Indicates if you want to send notification emails when ShadowProtect successfully completes a job.
Send Email on Failure	(Default: Off) Indicates if you want to send notification emails when ShadowProtect fails to complete a job.
Send daily report	(Default: Off) Indicates if you want to send a daily report of ShadowProtect activities.
Send weekly report	(Default: Off) Indicates if you want to send a weekly report of ShadowProtect activities.

4. (Optional) Click **Test Email** to send a test message and confirm that the Email configuration is working properly.

If you have trouble receiving ShadowProtect email messages on your production email server, try sending emails to an external email account such as Gmail or Hotmail. This lets you isolate the problem to ShadowProtect or the email system.

11.3 Log Files

ShadowProtect creates a log file for each backup job. This log file provides information about the backup job results, including the reason for failure, if any. You can view the log for any backup job in the Backup History tab (see Backup History Tab).

ShadowProtect creates a log file for each backup job. This log file provides information about the backup job results, including the reason for failure, if any. You can view the log for any backup job in the Backup History tab (see Backup History Tab).

Each log entry provides information about the related backup job: Start Time, End Time, Type (Full or Incremental), Source, Destination and Status. Backup jobs that finished successfully have a status of "Completed." ShadowProtect marks jobs that do not complete successfully with a Warning icon . These jobs have a status other than "Completed," such as "Execution Failed" or "Aborted." It is important to review these entries and determine why the job failed.

The Job Log provides information about the events that occurred during that job: Timing (when the event occurred), Module, Code, and Message. Backup jobs that finished successfully have a status of "Completed." ShadowProtect marks events that do not complete successfully with Failed icon.

11.4 Creating Key Files

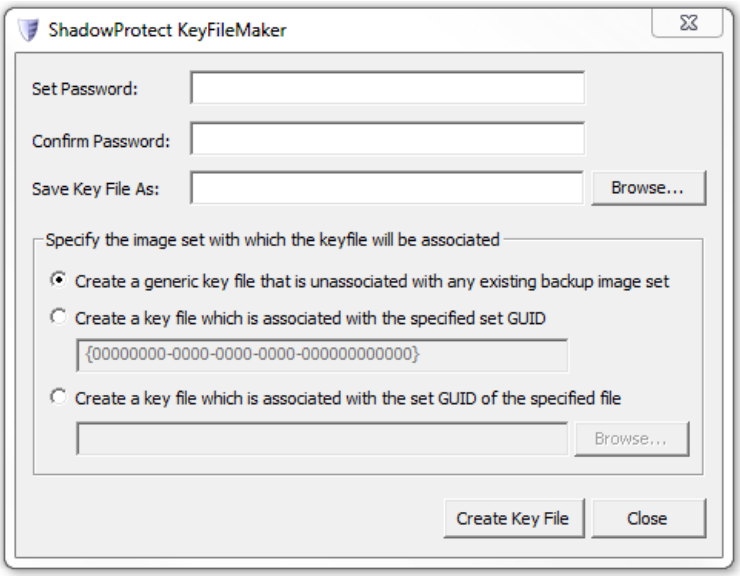
Key Files serve as repositories for passwords used with encrypted backup images. These files let you delegate the creation and storage of encrypted backup image files without losing control of those passwords. These files have a `.spk` file extension with a prefix that matches the name of the associated full backup file.

ShadowProtect includes the KeyFileMaker tool for recreating lost or corrupted Key Files. As these tasks are infrequent, KeyFileMaker is provided on the ShadowProtect CD, but is not installed by default.

Note: When you select to encrypt your backup image files, ShadowProtect automatically creates a new Key File each time it generates a new Full Backup. If you choose a Continuous Incremental backup job, ImageManager will use the resulting Key File when collapsing the encrypted incremental images. For more information about ImageManager, see the *ShadowProtect ImageManager User Guide*.

To install KeyFileMaker

1. Insert the ShadowProtect CD into the system's CD drive.
2. Browse to the \Installers folder, then execute `KEYFILEMAKERSETUP.exe`.
3. Follow the steps in the Installation Wizard to install the KeyFileMaker software.
   Once installed, you can access KeyFileMaker in Windows by selecting Start > Programs > ShadowProtect > ShadowProtect KeyFileMaker.



To create a key file

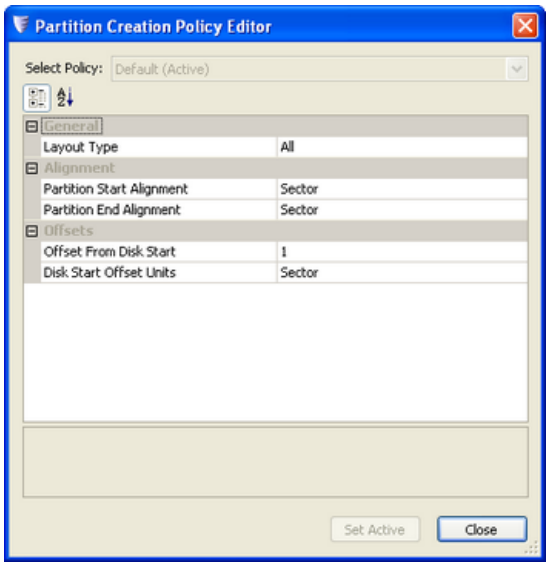
1. Launch KeyFileMaker (**Start** > **Programs** > **ShadowProtect** > **ShadowProtect KeyFileMaker**).
2. In the KeyFileMaker dialog box, provide the following information, then click **Create Key File**.

Set Password / Confirm Password	Specify the password to store in the Key File.
Save Key File As	Specify the name and location for the Key File. You must save the Key File in the same folder as the backup image files that rely on it.

Key File Association	Specify the backup Image Set that you want to associate with this Key File. **Generic Key File:** The key file is not associated with any Image Set. Select *Generic Key File* if all the backup image files in a given folder are part of the same Image Set. **Key File associated with a specific GUID:** Select this option if you have multiple backup image sets in the same directory and you want to manually specify the File Set GUID (Globally Unique ID) for the image set associated with this Key File. You can locate this GUID if you: a. Extracted the File Set GUID from one of the set's image file's header information. (All backup image files in an image set share the same File Set GUID.) b. Viewed the File Set GUID by starting to mount an image file from the relevant set with the Mount wizard (in Windows Explorer), then locating the GUID in the *File set GUID* field on the Image File Name page. **Key File associated with a specified backup image:** Use Browse to locate an image file in the set you want associated with this key file. The tool will automatically extract the GUID for use in creating the key file.

11.5 Changing Partition Creation Policy

The Partition Creation Policy Editor lets you modify basic disk geometry settings used to create a new partition. You can access the Partition Creation Policy Editor from the Disk Map tab action menu (right-click menu) (see Disk Map Tab).



To modify partition creation settings

1. Start the ShadowProtect Console (see Starting ShadowProtect).
2. On the Center panel, select the Disk Map tab.
3. Right-click the desired partition, then select **Edit Policy**.
4. In the Partition Creation Policy Editor, modify the partition creation settings as desired, then click **Set Active**.
   To modify a particular setting, click in the appropriate field, then type the desired value, or select it from the drop-down list (if available).

Layout Type	Specifies a name for the partition creation policy.
Partition Start Alignment	(Default: **Track**) Identifies the partition starting point, which typically occurs at a specific disk boundary. Supported options include: Cylinder, Track, and Sector.
Partition End Alignment	(Default: **Sector**) Identifies the partition end point. Supported options include: Cylinder, Track, and Sector.
Offset from Disk Start	Specifies an offset from the start of the disk where you want the partition to begin. This should be a Whole number.
Disk Start Offset Units	(Default: **Sector**) Specifies the units to use with the specified offset. Supported options include: Cylinder, Track, Sector, Byte.

11.6 Creating a Recovery CD

StorageCraft provides an ISO image file that you can use to create a bootable Recovery Environment disk. For more information about using the StorageCraft Recovery Environment, see the *StorageCraft Recovery Environment User Guide*.

To create a Recovery Environment disk

1. If necessary, download the Recovery Environment ISO image file.
   - a.Open a Web browser to the StorageCraft ISO Download Web page.
   - b.In the Serial Number field, specify the product serial number you received when you purchased ShadowProtect, then click **Submit**.
   - c.Save the Download tool and run it.
   - d.Save the zipped file containing the ISO image to a local drive.
   - d.Use a utility to open the zipped file containing the Recovery Environment ISO image `ShadowProtect_RE_X.iso` (where *X* is the version number of ShadowProtect.)
2. Insert a blank CD/DVD/Blu-Ray in your system's optical drive.
3. From Windows, select **Start** > **ShadowProtect** > **ISO Tool**.
4. Browse to and select the ShadowProtect ISO file, then click **Burn the Disk**.
   Select **Overwrite any existing data...** if you want to replace existing data on the disk.
5. When ISO Tool finishes transferring the ISO image, click **Close**.
   The ISO transfer can take several minutes to complete.

12 Best Practices

Turn off disk defrag software if using incremental backups. When you take an incremental backup, you are writing a file of only the sectors which have changed since the last full or incremental backup image was taken. If you run disk defrag software, you will be changing the sectors on the disk and cause the time and size of the incremental backup image to greatly increase. If you want to run disk defrag software, it is recommended that you do it before you run a Full backup image and then do not run or schedule the disk defrag software to run while ShadowProtect is scheduled to take Incremental backup images.

Test the StorageCraft Recovery Environment. Make sure the ShadowProtect 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.

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. ShadowProtect snapshots can operate simultaneously on multiple volumes, thereby ensuring cross-volume consistency.

Periodically save backup image files to removable storage. External hard drives or optical media let you easily store backup image files at an off-site location. This helps ensure the availability of 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 (see Image Conversion Tool).

Use Email notification. Automatic Emails keep you informed of the operation of your ShadowProtect backup jobs so you can quickly identify and resolve problems that might arise (see Configuring Email Notifications).

Use a retention policy that maximizes point-in-time histories. Review the options available in the ShadowProtect for retaining point-in-time histories, including using Differential images for second and subsequent Full images (see "Retention" in Advanced Options). These options can preserve additional storage capacity while providing a greater number of point-in-time backup image files in the chain.

Working with heavily-stressed servers. When monitoring the operating conditions of critical servers, administrators may note that one or more systems (such as Windows SBS) become heavily-tasked during business hours. This may result in failed VSS backups. Rather than opting for only a crash-consistent backup using a non-VSS driver, ShadowProtect often can successfully

execute a VSS backup of the same server volumes by scheduling the VSS backup outside of normal business hours when the server is less tasked. (See Creating Backup Files for details on scheduling.)

13 Retention Policy Configurations

ShadowProtect employs a unique method for maximizing point-in-time backup images while minimizing storage consumption that results in the ability to store more point-in-time histories in substantially less storage space. The following two tables present four common retention policies for a scheduled backup job, and the resulting performance of each. For more information about creating scheduled backup jobs and retention policies, see Creating Backup Image Files.

	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Use Differentials	X	X		
Delete Only the Incrementals	X		X	
Delete the Full and Incrementals		X		X
Image Set 1	C_Vol-b001	C_Vol-b001	C_Vol-b001	
Image Set 2	C_Vol-b001-d001		C_Vol-b002	
Image Set 3	C_Vol-b001-d002		C_Vol-b003	
Image Set 4	C_Vol-b001-d003		C_Vol-b004	
Image Set 5	C_Vol-b001-d004		C_Vol-b005	
Image Set 6	C_Vol-b001-d005 C_Vol-b001-d005-i001 C_Vol-b001-d005-i002 C_Vol-b001-d005-i003	C_Vol-b001-d005 C_Vol-b001-d005-i001 C_Vol-b001-d005-i002 C_Vol-b001-d005-i003	C_Vol-b006 C_Vol-b006-i001 C_Vol-b006-i002 C_Vol-b006-i003	C_Vol-b006 C_Vol-b006-i001 C_Vol-b006-i002 C_Vol-b006-i003
Image Set 7	C_Vol-b001-d006 C_Vol-b001-d006-i001 C_Vol-b001-d006-i002 C_Vol-b001-d006-i003	C_Vol-b001-d006 C_Vol-b001-d006-i001 C_Vol-b001-d006-i002 C_Vol-b001-d006-i003	C_Vol-b007 C_Vol-b007-i001 C_Vol-b007-i002 C_Vol-b007-i003	C_Vol-b007 C_Vol-b007-i001 C_Vol-b007-i002 C_Vol-b007-i003
Image Set 8	C_Vol-b001-d007 C_Vol-b001-d007-i001 C_Vol-b001-d007-i002 C_Vol-b001-d007-i003	C_Vol-b001-d007 C_Vol-b001-d007-i001 C_Vol-b001-d007-i002 C_Vol-b001-d007-i003	C_Vol-b008 C_Vol-b008-i001 C_Vol-b008-i002 C_Vol-b008-i003	C_Vol-b008 C_Vol-b008-i001 C_Vol-b008-i002 C_Vol-b008-i003

Relative Rank Across Scenarios

CPU Utilization	2[1]	2[1]	1	1
Network Utilization	2[2]	2[2]	1	1
Storage Requirement	2	1	4	3
Point-in-time History	1	2	1	3[3]

1 On machines using local storage the difference between scenarios is minimal. However on machines using network storage, the difference in CPU utilization is more apparent.
2 On machines using local storage this is not a consideration
3 The only difference between Scenario 2 and 4 is the unique information retained in the first full image.

14 Glossary

New Terminology (to be worked into this document) . . . This is per Nisha on 9/25/2012 12:25 pm

Former Name	New Feature Name
Inverse chain technology	StorageCraft Decremental Chain Technology
Raw file format / zfs file	StorageCraft Cloud Backup Image (File Format)
Bare Metal Recovery (BMR) Drive / BMR Process	StorageCraft Bare Metal Recovery (BMR) Drive / Process
Instantly virtualizing in the StorageCraft Cloud	StorageCraft ShadowCloud

For example: Take the legendary reliability of StorageCraft ShadowProtect to the cloud bringing you offsite backup and disaster recoery with immediate file and folder recovery, instant virtuualization of backup images through creation of a StorageCraft Shadow Cloud, and hands-on recovery testing

Roll Forward Consolidation / Rolling Consolidation StorageCraft Rolling Consolidation

This page will be merged with the glossary for all documents. . . work on merging the two as time permits.

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.

Backup Image Set: The Base Image File, plus any Incremental Image Files, that comprise all Backup Image Files for a specific computer system.

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: see *Full Image File*.

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.

Full 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 operating system, applications, and data.

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.

Hardware Independent Restore (HIR): The ability to restore a system volume using ShadowProtect to dissimilar hardware.

HeadStart 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 Full image files or Differential image files. When restoring a drive (or files and folders), you must use the Full 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 available in Microsoft Windows (XP and Windows Server 2003 and later), which includes a mechanism for creating consistent data snapshots. VSS 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.