



StorageCraft Recovery Environment User Guide

Author: STC Admin

Date: Nov 30, 2011 6:20 AM

URL:

<http://doc.storagecraft.com/wiki/display/enREguide/StorageCraft+Recovery+Environment+User+Guide>



Table of Contents

1	Additional Information	5
2	Documentation Conventions	6
3	ShadowProtect Overview	7
3.1	Features and Components	7
3.2	Recovery Environment Usage Scenarios	9
3.2.1	Bare Metal Recovery	9
3.2.2	Bare Metal Recovery to a Different System	10
3.2.3	Server Migration using HeadStart Restore	10
3.2.4	Standby Server using HeadStart Restore	10
4	How ShadowProtect Works	11
4.1	Create a Backup Image	11
4.1.1	Create a Virtual Volume	11
4.1.2	Capture the Virtual Volume	12
4.2	Restore a Backup Image	12
4.2.1	Recover individual files and folders	13
4.2.2	Restore an entire volume	13
4.3	Backup Image Files	13
4.3.1	File Naming Conventions	14
4.3.2	File Dependencies	15
5	Starting Recovery Environment	17
5.1	Requirements	18
5.2	Testing the Recovery Environment CD	18
6	Understanding the User Interface	20
6.1	Menu Bar	20
6.2	Task Panel	21
6.3	Tabs	22
7	Loading Drivers	25
8	Using the Network Configuration Utility	26
9	Creating a Backup Image File	28
9.1	Options	28
9.1.1	Backup Image File Storage Location	29
9.1.2	File Compression	30
9.1.3	Backup Image File Security	30
9.1.4	Splitting Backup Image Files	31
9.1.5	Backup Comments	31
9.1.6	Advanced Options	31
10	Restoring a System Volume	33
10.1	Resuming a Restore Operation	35
10.2	HSR Volume Options	37
10.2.1	Adding Incrementals to an HSR Volume	37
10.2.2	Finalizing an HSR Volume	40
11	Mounting a Backup Image File	42



- 11.1 Dismounting a Backup Image File _____ 42
- 11.2 Backup Image File Mount Options _____ 43
 - 11.2.1 Mounting a Backup Image as a Drive Letter _____ 44
 - 11.2.2 Mounting a Backup Image as a Mount Point _____ 44
 - 11.2.3 Mounting a Read-Only Backup Image _____ 44
 - 11.2.4 Mounting a Writeable Backup Image _____ 44
- 12 Using Image Conversion Tool _____ 46
- 13 Using the Boot Configuration Utility _____ 47
- 14 Using HIR _____ 51
 - 14.1 HIR Advanced Options _____ 51
- 15 Using Remote Management _____ 53
- 16 Other Operations _____ 54
 - 16.1 Deleting Backup Image Files _____ 54
 - 16.2 Verifying Backup Image Files _____ 54
- 17 Windows Boot Process _____ 55
- 18 Product Support _____ 56
 - 18.1 Complimentary Technical Support _____ 56
 - 18.2 E-Mail Support _____ 56
 - 18.3 Telephone Support _____ 56
- 19 Glossary _____ 57



Welcome to the StorageCraft® *Recovery Environment User Guide*. This Guide describes the ShadowProtect technology, and how to derive maximum benefit from the StorageCraft Recovery Environment.

This Guide includes the following major sections:

- [ShadowProtect Overview](#)
- [How ShadowProtect Works](#)
- [Starting Recovery Environment](#)
- [Understanding the User Interface](#)
- [Loading Drivers](#)
- [Using the Network Configuration Utility](#)
- [Creating a Backup Image File](#)
- [Restoring a System Volume](#)
- [Mounting a Backup Image File](#)
- [Using Image Conversion Tool](#)
- [Using the Boot Configuration Utility](#)
- [Using HIR](#)
- [Using Remote Management](#)
- [Other Operations](#)

Additionally, this Guide includes the following general information sections:

- [Windows Boot Process](#)
- [Product Support](#)
- [Glossary](#)



1 Additional Information

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



2 Documentation Conventions

Note or **Warning** text provides important information about the configuration and/or use of StorageCraft Recovery Environment.



3 ShadowProtect Overview

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

Other Methods	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	

StorageCraft Recovery Environment is a critical component of the overall ShadowProtect disaster recovery solution. You should be aware of the following information before using Recovery Environment:

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

3.1 Features and Components

Component	Features
-----------	----------



<p>ShadowProtect Console</p>	<p>An easy-to-use management console that lets you manage the disaster recovery configuration on your Windows system. ShadowProtect console provides the following primary features:</p> <ul style="list-style-type: none">• Microsoft VSS-aware (Volume Shadow Copy Service) so you can unobtrusively back up changes in the background.• Wizard-based back-up to any accessible hard disk, including network storage (SAN, NAS, iSCSI), removable drives (USB, FireWire), and optical media (CD, DVD, Blu-Ray).• Verify backup images to ensure complete recovery.• Create compressed and encrypted backup image files for efficiency and security.• Wizard-based recovery of files, folders, or a complete data volume, to an exact point-in-time.• View backup images for quick file and folder recovery.• Remotely manage system backup and recovery operations.• VirtualBoot lets you create a mount any backup image file as a virtual disk in the VirtualBox Virtual Machine environment.
<p>ShadowProtect Backup Agent</p>	<p>The engine that creates and manages a system's point-in-time backup images. The Backup Agent also handles mounting of backup image files. You can manage the operation of the Backup Agent from the ShadowProtect Console. To access the ShadowProtect Backup Agent, you must be a user with local administration rights.</p>



StorageCraft Recovery Environment	<p>A bootable Windows environment for disaster recovery without installing software. For more information about the Recovery Environment, see the StorageCraft Recovery Environment User Guide.</p> <ul style="list-style-type: none">• Access all the features of the ShadowProtect Console from a standalone disaster recovery environment.• Loads from the bootable ShadowProtect CD.• Restore a system (bootable) volume quickly and easily.• Back up a non-bootable system before attempting a restore operation.• Use Hardware Independent Restore (HIR) to restore to different hardware, or to virtual environments (P2P,P2V,V2P).• Network configuration tool to manage TCP/IP properties, domains and network resources.
ImageManager	<p>ImageManager provides unprecedented control over your backup image files. It provides policy-driven services for managing backup image files. For more information about ImageManager features, see the ShadowProtect ImageManager User Guide.</p> <ul style="list-style-type: none">• Consolidation of Incremental backup image files into daily, weekly, and monthly consolidated image files that greatly reduce the number of files in an image chain.• Verification and re-verification of backup image files, including consolidated files.• Replication of backup image files to a local drive, a network share, or an off-site location (using FTP).• Head Start Restore (HSR) lets you restore a backup image while ShadowProtect continues to add Incremental backup images to it. This lets you greatly reduce the downtime associated with hardware failure or hardware migration tasks.



Note: For a complete version history of product updates, see the `Readme.rtf`, located in the `\StorageCraft\ShadowProtect` folder of your ShadowProtect installation.

3.2 Recovery Environment Usage Scenarios

The following scenarios introduce several possible use cases for Recovery Environment:



3.2.1 Bare Metal Recovery

Problem: When a failure occurs, I need to be able to restore server, desktop and laptop volumes as quickly as possible to minimize user downtime. Manually re-installing operating systems and rebuilding user environments takes too much time.

Solution: Use StorageCraft Recovery Environment to restore an entire system in minutes, and ShadowProtect restores the system to its exact state before the failure.

3.2.2 Bare Metal Recovery to a Different System

Problem: Due to hardware failure or other circumstances, I need to restore a system volume to partially (or completely) different hardware, or to a virtual environment.

Solution: In the StorageCraft Recovery Environment, use Hardware Independent Restore (HIR) to restore a system to different hardware, or a virtual environment. HIR supports any type of system restore (P2P, P2V, V2P and V2V). Additionally, VMWare provides support for StorageCraft Image Files in VMWare Workstation 6 and their Converter tool.

3.2.3 Server Migration using HeadStart Restore

Problem: You need to migrate a database server with 20TB of data to a new hardware platform, but you cannot afford to have the server offline for three days it takes to migrate the data to new hardware.

Solution: Keep the old server running, and generating incremental backups, while you begin a HeadStart Restore of the same backup image chain on the new hardware. Over time, the HSR catches up to the most current incremental from the old server, at which point you can take the old server down in off hours, apply the final incremental backup to the new server, and bring the new system on-line very quickly. You can even migrate the operating system volume by doing a Hardware Independent Restore (HIR) to make sure the migrated OS boots properly on the new server hardware.

3.2.4 Standby Server using HeadStart Restore

Problem: You want to have a stand-by server that can take over should your primary server fail, but you can't afford the high-priced server mirroring technology.

Solution: Your production server generates continuous incremental backups. Configure an HSR solution to automatically apply those incremental backup images to a secondary "standby" server. If your production server fails, use HSR to finalize to the last incremental to the standby server (a matter of minutes), then bring it on-line as a replacement for the failed production server.



4 How ShadowProtect Works

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



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

- [Create a Backup Image](#)
- [Restore a Backup Image](#)

4.1 Create a Backup Image

Creating a ShadowProtect backup image involves two key processes:

4.1.1 Create a Virtual Volume

Using Microsoft VolSnap and VSS (with Windows Server 2003, Windows XP, or later), ShadowProtect creates a point-in-time snapshot of the volume you want to backup. The entire

process of taking a snapshot of a volume and creating a virtual volume takes only seconds and does not interfere with system operation.

Snapshot	Supported OS	Image Speed	Quality	Comments
StorageCraft VSM with VSS	Windows Server 2000 Family	Fast	Best	<ul style="list-style-type: none">• VSS aware applications are managed to achieve best backups.• Can use script files to manage applications that are not VSS aware to improve backups.



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

Additionally, ShadowProtect provides a Backup Scheduler that lets you configure automated backup jobs for protected volumes. You can schedule Full Image, Incremental Images (as often as every 15 minutes), and manage the retention of backup Image Sets. The ShadowProtect Backup Image 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.

4.1.2 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" in the ShadowProtect User Guide.

4.2 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:

4.2.1 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" in the ShadowProtect User Guide.

4.2.2 Restore an entire volume

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

4.3 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 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 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.

4.3.1 File Naming Conventions

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

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

The ShadowProtect naming convention uses the following variable components:

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

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

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

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

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

File Type Extension	Description
C_Vol1-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 <i>This type of backup is not available in ShadowProtect IT Edition.</i>
C_Vol-b001-d000-i001.spi or C_Vol-b001-i001.spi	Incremental image of the C:\ volume with a dependency on the full backup image file C_Vol-b001.spf The only time ShadowProtect IT Edition creates a .spi file is when you mount a read/write backup image and save changes made to that volume. Upon dismounting that volume, the changes will be saved out to an incremental file.
C_Vol-b001-d001.i001.spi	Incremental backup image file of the C:\ volume with a dependency on the differential backup image file C_Vol-b001-d001.i000 which in turn has a dependency on C_Vol-b001.spi. <i>This type of backup is not available in ShadowProtect IT Edition.</i>



Note: Backup image file names that have a “-d000” or “-i000” segment use these name segments only as place holders, and indicate that a differential backup image or an incremental backup image are not part of the image and the backup image file has no dependency on a previous differential or incremental backup image file.

4.3.2 File Dependencies

By examining the name of a backup file image, ShadowProtect users can identify the files that it is dependent on. However, it is not possible to determine if other backup image files are dependent on this file. Because of this, it is very important to use the Backup Image 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.



5 Starting Recovery Environment

Recovery Environment loads automatically when you boot from the ShadowProtect CD. Before you run ShadowProtect, make sure your system meets the minimum hardware and software requirements (see [Requirements](#)).



To load the StorageCraft Recovery Environment

1. If the backup image you wish to restore is located on a USB drive, attach that to the computer.
2. Insert the ShadowProtect CD into the computer.
3. Restart the computer.



Note: You might need to modify the boot options to have the computer boot to a CD drive.

The ShadowProtect CD Boot Options include the following options:

[1] Start Recommended Recovery Environment: Option 1 is the default boot option that contains commonly distributed drivers. It uses Windows 7 PE, which lets you dynamically load drivers and hot plug disk devices even after Recovery Environment has started.

[2] Start Legacy Recovery Environment: Option 2 contains all drivers in Option 1 along with other less commonly distributed drivers. Option 2 uses Windows Server 2003. Select Option 2 if you know Option 1 does not provide the necessary storage or network drivers, or you are unable to dynamically load the drivers from Option 1.

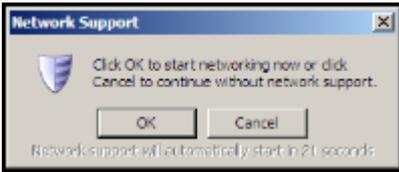
[3] Boot from Hard Disk: Option 3 boots the system from the primary hard drive.

[4] Reboot: Option 4 restarts the system.

Because of the extended driver options and operating system, Option 2 takes significantly longer to boot into Recovery Environment than Option 1. Additionally, Option 2 requires that the ShadowProtect CD remain loaded at all times. You cannot remove the ShadowProtect CD to restore a backup image file.

4. In the Network Support dialog box, click OK to start networking.

For information about using the Network Configuration utility, see (enREguide:Using the Network Configuration Utility).



Once Recovery Environment loads, you can perform ShadowProtect tasks as needed.

5.1 Requirements

ShadowProtect Recovery Environment has the following minimum hardware requirements:

Hardware	Recovery Environment (RE)
CPU	Windows 2008-based RE: 1 GHz or faster. Windows 2008-based RE (Japan only): 1.4 GHz (x64 processor) or 1.3GHz Dual Core). Windows 2003-based RE: 550 MHz or faster. Supports up to four processors per system.
Memory	Windows 2008-based RE: 512 MB minimum. Windows 2003-based RE: 256 MB minimum.
Hard Drive space	N/A
CD-ROM or DVD drive	Required.
Monitor	VGA or higher resolution.

5.2 Testing the Recovery Environment CD

You should test the StorageCraft Recovery Environment to ensure that it runs properly on your computer. To do this, boot your computer with the ShadowProtect CD.

If the StorageCraft Recovery Environment boots and runs as expected, you are ready to perform ShadowProtect operations from Recovery Environment in the event of a hardware failure, system volume failure, or to create a cold backup.

If the StorageCraft Recovery Environment does not boot or run as expected, investigate the following issues:

- You do not have the necessary network interface card (NIC) drivers to access the network. You can dynamically load NIC drivers from within Recovery Environment (Load Drivers in the Tools menu).
- You do not have the necessary storage drivers to access a storage device on the computer. To resolve this, do one of the following:

Load storage drivers during boot time

1. When prompted during Recovery Environment boot sequence, press F6 to add storage drivers.



2. Browse to the appropriate storage driver files.

Load storage drivers after loading Recovery Environment

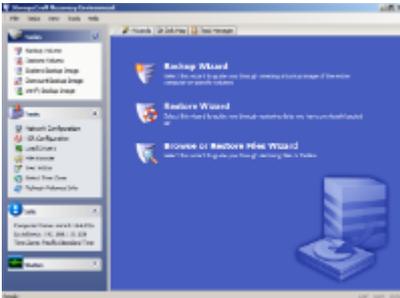
1. In the Tools menu, select Load Drivers.
2. Browse to the appropriate storage driver files.

Keep necessary storage drivers on a diskette that is available in the event you need to load Recovery Environment.

If you find it necessary to load drivers for Recovery Environment, contact StorageCraft Technical Support or send an e-mail to support@storagecraft.com so StorageCraft can include these drivers in future releases of ShadowProtect.



6 Understanding the User Interface



Recovery Environment Main Screen

6.1 Menu Bar

The Recovery Environment menu bar provides access to following menus:

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



Tools	Access Recovery Environment tools.	<p>Network Configuration: Launches the Network Configuration utility, where you can configure a computer's network access settings.</p> <p>HIR Configuration: Launches the Hardware Independent Restore (HIR) utility, where you can restore a backup image to a different environment from which it was created.</p> <p>Load Drivers: Opens the Load Drivers dialog box, where you can configure storage drivers for use in Recovery Environment.</p> <p>File Browser: A simple file browser that lets you browse files and folders of a backup image file.</p> <p>Text Editor: A simple text editor.</p> <p>Boot Configuration Utility: Launches the Boot Configuration Utility, where you can manage the boot configuration repair process for those situations where the automated process does not work (see Using the Boot Configuration Utility).</p> <p>Partition Table Editor: A simple partition table editor.</p> <p>UltraVNC Service: Launches the Remote Management utility, where you can configure remote access to systems running Recovery Environment.</p> <p>Select Your Time Zone: Launches the Time Zone utility, where you can adjust the system's time zone information.</p> <p>Display Settings: Opens the Display Settings dialog box, where you can configure the resolution and color mode used to display the Recovery Environment UI.</p> <p>Enable Logging: Opens the Logging dialog box, where you can specify a location for ShadowProtect log files.</p> <p>Refresh Volumes Info: Refreshes the Volume List information.</p>
Help	Display general Recovery Environment information.	About: Displays the Recovery Environment version and copyright information.

6.2 Task Panel

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

each category as needed.

Menu	Description	Options
------	-------------	---------



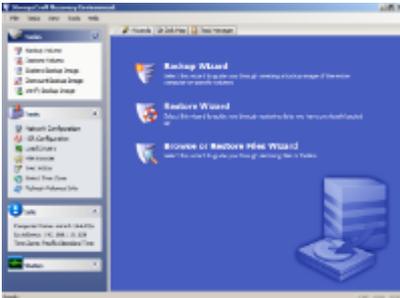
Tasks	Access ShadowProtect wizards.	Backup Volume: Launches the Backup Wizard (see Creating a Backup Image File). Restore Volume: Launches the Restore Wizard (see Restoring a System Volume). Explore Backup Image: Launches the Explore Backup Image Wizard (see Mounting a Backup Image File). Dismount Backup Image: Launches the Backup Image Dismount Wizard (see Dismounting a Backup Image File). Verify Backup Image: Launches the Verify Image Wizard (see Verifying Backup Image Files).
Tools	Access Recovery Environment tools.	Network Configuration: Launches the Network Configuration utility, where you can configure a computer's network access settings. HIR Configuration: 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: Opens the Load Drivers dialog box, where you can configure storage drivers for use in Recovery Environment. File Browser: A simple file browser that lets you browse files and folders of a backup image file. Text Editor: A simple text editor. Select Your Time Zone: Launches the Time Zone utility, where you can adjust the system's time zone information. Refresh Volumes Info: Refreshes the Volume List in ShadowProtect.
Info	Display system information.	A quick reference to basic system information, including Computer Name, IP Address and Time Zone information.
Status	Displays current ShadowProtect task status.	Queued Tasks: The number of queued tasks waiting to run. Running Tasks: The number of tasks currently running.



6.3 Tabs

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

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



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



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

 **Note:** If you abort a restore operation, you can restart it again if necessary (see [Resuming a Restore Operation](#)).



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



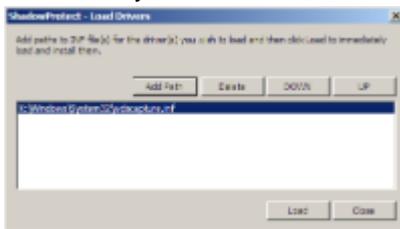
7 Loading Drivers

Recovery Environment lets you dynamically load storage or network drivers.

 The ability to dynamically load drivers is available only if you loaded Recovery Environment using Option 1 (see [Starting Recovery Environment](#)).

To dynamically load a driver

1. In Recovery Environment, click **Load Drivers** in the Tools menu.



2. Click **Add Path** to browse to the INF files you need.
Click-and-drag the drivers to move them up and down the list in order to establish priority.
3. Select the proper driver, then click **Load**.
Recovery Environment loads the driver and automatically provides access to that device.



8 Using the Network Configuration Utility

The Network Configuration Utility (NCU) lets you configure a computer's Network Interface Cards (NICs), TCP/IP settings, and domain information for use in Recovery Environment.



To use the Network Configuration Utility

1. Open the Network Configuration Utility.

You can load the NCU in the following ways:

While booting Recovery Environment: Click OK when asked to start networking (see [Starting Recovery Environment](#)).

After loading Recovery Environment: Click Network Configuration in the Tools menu.

2. (Optional) Select an alternate UI language from the Language dropdown menu.
3. Select the appropriate Ethernet adapter from the dropdown list.

If necessary, select the adapter's preferred link speed and duplex mode.

4. Modify the adapter settings in the NCU interface. Available settings include:

IP Addresses: Select either Dynamic or Static IP address settings:

Obtain an IP address automatically: Specify DHCP settings, including Releasing and Renewing DHCP leases.

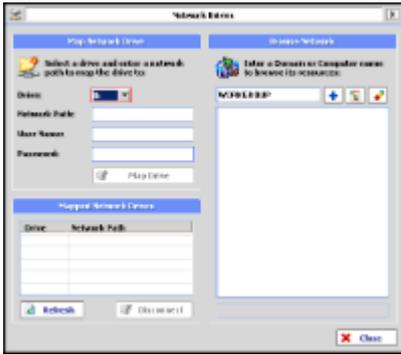
Use the following IP address: Specify IP address, Subnet mask, and Default gateway. You can specify multiple IP addresses and gateways, if necessary.

DNS and WINS Servers: Select either Dynamic or Static DNS and WINS configurations. When using a static configuration, click More to specify one or more IP addresses for the DNS or WINS environment.

Network Identification: Specify a computer name, Workgroup, and Primary DNS suffix. To do this, type a value in the appropriate field, then click Set. The Full Computer Name field displays the current computer name.



5. Click **Network Drives** to configure drive mappings and file sharing.



You can configure drive mappings manually (under Map Network Drive), or search for network resources by Domain or Computer Name (Browse Network). To browse the network, do the following:

- a. Enter a domain or computer name in the field, then click Add .
The NCU browses the network and locates all resources in the specified Domain or Computer, displaying them in the Resources pane.
- b. Click **Expand All** to view all available resources in the specified Domain or Computer.
- c. Select a resource to automatically populate the **Network Path** field in Map Network Drive.
- d. (Optional) Click **Clear All** to remove all network resources from the Resources pane.



9 Creating a Backup Image File

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

To create a backup image file

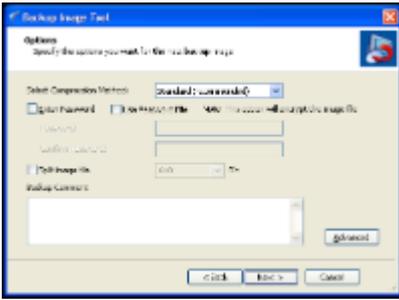
1. Start the ShadowProtect Console (see [Starting Recovery Environment](#)).
2. Open the Backup Wizard by doing one of the following:
 - In the Wizards tab, click **Backup Wizard**.
 - In the Tasks menu, click **Backup Volume**.
3. In the Volumes to Back Up page, select the volumes to backup, then click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



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

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

9.1 Options



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

- [Backup Image File Storage Location](#)
- [File Compression](#)
- [Backup Image File Security](#)
- [Splitting Backup Image Files](#)
- [Backup Comments](#)
- [Advanced Options](#)

9.1.1 Backup Image File Storage Location

ShadowProtect lets you store backup image files on any disk device, including hard drives, removable USB/FireWire drives, network drives and NAS (Network Attached Storage) devices.

You can also store backup images to optical media such as CDs, DVDs, or Blu-Ray discs.

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

Location	Advantages	Disadvantages
Local Hard Drive	<ul style="list-style-type: none">• Fast backup and restore.• Inexpensive.	<ul style="list-style-type: none">• Consumes local disk space.• Vulnerable to loss if the drive fails.
Local USB/FireWire Drive	<ul style="list-style-type: none">• Fast backup and restore.• Preserves disk space on local drives.• Inexpensive.• Easy off-site storage.	<ul style="list-style-type: none">• More expensive than local hard drives.• Vulnerable to loss if the drive fails.



Network Hard Drive	<ul style="list-style-type: none">• Fast backup and restore.• Protection from local hard drive failure.• Off-site storage.	<ul style="list-style-type: none">• Must have network interface card drivers supported by Recovery Environment.• Complexity. Users must have network rights to save and access backup images.
CD/DVD/Blu-Ray	<ul style="list-style-type: none">• Good media for archiving.• Protection from local hard drive failure.	<ul style="list-style-type: none">• Slower backups due to media speeds.• File restrictions due to limited size.

9.1.2 File Compression

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

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

9.1.3 Backup Image File Security

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

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

- **RC 4 128 bit (Fast):** Faster but less secure than AES 128-bit.
- **AES 128 bit (More Secure):** Faster but less secure than AES 256-bit.



- **AES 256 bit (Most Secure):** Slowest but most secure security option.

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

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

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

9.1.4 Splitting Backup Image Files

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

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

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

9.1.5 Backup Comments

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

9.1.6 Advanced Options

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

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



Lock Source Volume

Default: **Off**

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

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

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

Include Free Space

Default: **Off**

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

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

IO Throttle

Default: **100**

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

Enable Write Caching

Default: **Off**

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

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



10 Restoring a System Volume

The primary purpose of Recovery Environment is to let you restore a system that cannot boot on its own. The Restore Wizard guides you through the process of restoring a system volume. Recovery Environment offers two ways to manage the restore of a system volume:

Finalized Restore: The finalized restore operation restores a system volume from a selected backup image file and prepares the volume for use in a single operation.

HeadStart Restore: HeadStart Restore (HSR) lets you break up the volume restore process into multiple stages. Doing this is particularly useful for large volumes where the volume restore process can take days. HSR lets you start the restoration process before a problem occurs. Then, when a restore is needed, you can finish restoring the latest Incrementals and finalize the restoration for use. Instead of days of downtime, you have just a few hours.

Regardless of the type of restore you want to perform, the initial configuration of a restore operation is nearly identical.

To restore a system volume

1. Load Recovery Environment.

For more information, see [Starting Recovery Environment](#). If you need to use Remote Management, load the UltraVNC Server (see [Using Remote Management](#)).

2. In Recovery Environment, select **Tasks > Restore Volume** to launch the Restore Wizard. You can also select **Restore Volume** in the left-side Navigation panel or select **Restore Wizard** in the Wizards tab.

3. On the Restore Type page, select **Restore**, then click **Next**.

4. On the Backup Image to Restore page, browse to the backup image that you want to restore, then click **Next**.

If the backup image is encrypted, you must specify the appropriate password to access the backup image file.

The Backup Image to Restore page displays information about the selected backup image.

5. On the Backup Image Dependencies page, select the backup image file (the specific point-in-time) that you want to restore, then click **Next**.

The left pane displays all backup image files in the previously selected image set. Select a backup image file to display information about that file in the right pane.

6. On the Restore Destination page, select the hard disk where you want to restore the system volume, then click **Next**.

7. On the Finalization Options page, specify whether to finalize the restored volume for use, then click **Next**.



Finalize the volume at the end of this restore	<p>Select this option to perform a Standard restore operation, where the restored volume is ready for use when the restore operation completes.</p> <div data-bbox="466 324 1430 421" style="border: 1px solid #ccc; background-color: #ffffcc; padding: 5px;"> <p> Note: Do not select this option to perform a HeadStart Restore.</p> </div>
Generate a .HSR file to use in a future finalization	<div data-bbox="466 524 1430 620" style="border: 1px solid #ccc; background-color: #ffffcc; padding: 5px;"> <p> Note: This option is available only for HSR operations.</p> </div> <p>(Optional) When selected, the Restore Wizard generates an HSR file, at the location you specify, that contains metadata about the HSR volume. With this file, you can finalize the HSR volume without accessing the source backup image files.</p>

8. (Conditional) On the Specify the Restoration Options page, select the boot parameters you want to apply to the restored volume, then click **Next**.

Recovery Environment displays this page only when finalizing the volume.

Set partition active	Configures the restored volume as the active partition in the system (the drive the machine boots from).
Restore MBR	<p>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:</p> <p>Restore MBR from the image file: Restores the MBR from the backup image file.</p> <p>Restore original Windows MBR: Restores the default MBR for the version of Windows you are restoring.</p> <p>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.</p>
Restore Disk Hidden Track	Restores the first 63 sectors of a drive. Some boot loader applications require this for the system to boot.
Use Hardware Independent Restore*	Instructs Recovery Environment to launch the Hardware Independent Restore (HIR) utility when finalizing the volume for use so you can configure the restore operation to properly interact with the hardware where you want to restore the volume. For more information, see Using HIR .



9. On the Summary page, review the details of the restore operation, then click **Finish**.
Recovery Environment begins the restore operation and opens the Task Manager so you can view its progress. Once the restore operation completes, you have the following options, depending on the type of restore operation:
 - **Finalized Restore:** Optionally, use the Boot Configuration Utility to ensure that the newly restored system volume is "bootable" (see [Using the Boot Configuration Utility](#)). You can now reboot the system to the restored system volume.
 - **HeadStart Restore:** Because the volume is not finalized, an HSR volume is not available to users or applications, but you can continue to restore additional Incremental images to the HSR volume. When ready, you can Finalize the HSR volume to make it ready for use. At this point, the HSR volume becomes a standard system volume, and you can have the same post-restore options as described above for a Standard Restore.

10.1 Resuming a Restore Operation

If a restore operation is interrupted for any reason, the Restore Wizard lets you resume the interrupted restore operation.

To resume a restore operation

1. Load Recovery Environment.
For more information, see [Starting Recovery Environment](#). If you need to use Remote Management, load the UltraVNC Server. For more information, see [Using Remote Management](#).
2. In Recovery Environment, select **Tasks > Restore Volume** to launch the Restore Wizard.
You can also select **Restore Volume** in the left-side Navigation panel or select **Restore Wizard** in the Wizards tab.
3. On the Restore Type page, select **Resume Aborted Restore**, then click **Next**.
4. On the Restore Destination page, select the hard disk where you previously started the restore operation, then click **Next**.
5. On the Backup Image to Restore page, browse to the backup image that you want to resume restoring, then click **Next**.
If the backup image is encrypted, you must specify the appropriate password to access the backup image file. The Backup Image to Restore page displays information about the selected backup image.
6. On the Finalization Options page, specify whether to finalize the restored volume for use, then click **Next**.

Finalize the volume at the end of this restore	Select this option to perform a standard volume restore, where the restored volume is ready for use when the restore operation completes. Do not select this option to perform a HeadStart Restore.
---	--



Generate a .HSR file to use in a future finalization	Note: This option is available only for HSR restore operations. (Optional) When selected, the Restore Wizard generates an HSR file, at the location you specify, as part of the HSR restore operation that contains metadata about the HSR volume. With this file, you can finalize the HSR volume without accessing the source backup image files.
---	--

7. (Conditional) On the Specify the Restoration Options page, select the boot parameters you want to apply to the restored volume, then click **Next**.

Recovery Environment displays this page only if you are finalizing the volume as part of the restore operation.

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 MBR: Restores the default MBR for the version of Windows you are restoring. Restore disk signature: Restores the original hard drive physical disk signature. Windows Server 2003, Windows 2000 Advanced Server, and Windows NT Server 4.0 Enterprise Edition (SP3 and later) require disk signatures to use the hard drive.
Restore Disk Hidden Track	Restores the first 63 sectors of a drive. Some boot loader applications require this for the system to boot.



Use Hardware Independent Restore	Instructs Recovery Environment to launch the Hardware Independent Restore (HIR) utility when finalizing the volume for use so you can configure the restore operation to properly interact with the hardware where you want to restore the volume. For more information, see Using HIR .
---	---

8. On the Summary page, review the details of the restore operation, then click **Finish**. Recovery Environment resumes the restore operation using your configuration. Once the restore operation completes, you have the following options, depending on the type of restore operation:
 - **Finalized Restore:** Optionally, use the Boot Configuration Utility to ensure that the newly restored system volume is "bootable" (see [Using the Boot Configuration Utility](#)). You can now reboot the system to the restored system volume.
 - **HeadStart Restore:** Because the volume is not finalized, an HSR volume is not available to users or applications, but you can continue to restore additional Incremental images to the HSR volume. When ready, you can Finalize the HSR volume to make it ready for use. At this point, the HSR volume becomes a standard system volume, and you can have the same post-restore options as described above for a Standard Restore.

10.2 HSR Volume Options

Once you have created an HSR volume (see [Restoring a System Volume](#)), you can either add Incremental images to the volume or finalize the volume for use.

- [Adding Incrementals to an HSR Volume](#)
- [Finalizing an HSR Volume](#)

10.2.1 Adding Incrementals to an HSR Volume

If you have an HSR volume that is not finalized, you can add Incremental images to the HSR volume. Consider the following when adding files to an HSR volume:

- You can only add Incremental images that are "descendants" of the last Incremental image file in the HSR volume. Descendant image files are newer Incremental images that are part of the same Image Set used to create the HSR volume.
- If you skip Incremental images in the Image Set, Recovery Environment automatically applies all Incremental images necessary to add the selected Incremental image to the HSR volume.

To add incremental images to an existing HSR volume



1. Load Recovery Environment.
For more information, see [Starting Recovery Environment](#). If you need to use Remote Management, load the UltraVNC Server. For more information, see [Using Remote Management](#).
2. In Recovery Environment, select **Tasks > Restore Volume** to launch the Restore Wizard.
You can also select Restore Volume in the left-side Navigation panel or select **Restore Wizard** in the Wizards tab.
3. On the Restore Type page, select **Restore Subsequent Incrementals**, then click **Next**.
4. On the Restore Destination page, select the hard disk where you previously created the HSR volume, then click **Next**.
5. On the Backup Image to Restore page, select the Incremental image to add to the HSR volume, then click **Next**.
If the backup image is encrypted, you must specify the appropriate password to access the backup image file. The Backup Image to Restore page displays information about the selected backup image.
Note: Make sure you follow the conditions, listed at the beginning of this section, for adding an Incremental backup image to an HSR volume.
6. On the Backup Image Dependencies page, select the backup image file (the specific point-in-time) that you want to restore, then click **Next**.
The left pane displays all backup image files in the previously selected Image Set. Select a backup image file to display information about that file in the right pane.
7. On the Finalization Options page, specify whether to finalize the volume for use now, then click **Next**.

Finalize the volume at the end of this restore	Select this option to finalize the HSR volume after adding the selected Incremental image file. Once finalized, the HSR volume is ready for use. Note: Do not select this option if you want to add additional Incremental images to the HSR volume in the future.
Generate a .HSR file to use in a future finalization	Note: This option is available only if you are not finalizing the volume. (Optional) When selected, the Restore Wizard generates an HSR file, at the location you specify, that contains metadata about the HSR volume. With this file, you can finalize the HSR volume without accessing the source backup image files. If you previously created an HSR file for the HSR volume, you must select the same HSR file.

8. (Conditional) On the Specify the Restoration Options page, select the boot parameters you want to apply to the restored volume, then click **Next**.
Recovery Environment displays this page only if you are finalizing the volume as part of the restore operation.

Set partition active	Configures the restored volume as the active partition in the system (the drive the machine boots from).
-----------------------------	--



Restore MBR	<p>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:</p> <p>Restore MBR from the image file: Restores the MBR from the backup image file.</p> <p>Restore original Windows MBR: Restores the default MBR for the version of Windows you are restoring.</p> <p>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.</p>
Restore Disk Hidden Track	<p>Restores the first 63 sectors of a drive. Some boot loader applications require this for the system to boot.</p>
Use Hardware Independent Restore	<p>Instructs Recovery Environment to launch the Hardware Independent Restore (HIR) utility when finalizing the volume for use so you can configure the restore operation to properly interact with the hardware where you want to restore the volume.</p> <p>For more information, see Using HIR.</p>

9. On the Summary page, review the details of the restore operation, then click **Finish**. Recovery Environment begins the restore operation and opens the Task Manager so you can view its progress. Once the restore operation completes, you have the following options, depending on the type of restore operation:
 - **Finalized Restore:** Optionally, use the Boot Configuration Utility to ensure that the newly restored system volume is "bootable" (see [Using the Boot Configuration Utility](#)). You can now reboot the system to the restored system volume.



- **HeadStart Restore:** Because the volume is not finalized, an HSR volume is not available to users or applications, but you can continue to restore additional Incremental images to the HSR volume. When ready, you can Finalize the HSR volume to make it ready for use. At this point, the HSR volume becomes a standard system volume, and you can have the same post-restore options as described above for a Standard Restore.

10.2.2 Finalizing an HSR Volume

If you previously created an HSR volume, the Restore Wizard lets you finalize it for use when you are ready to let users and applications access the restored volume.

To finalize an HSR volume

1. Load Recovery Environment.
For more information, see [Starting Recovery Environment](#). If you need to use Remote Management, load the UltraVNC Server. For more information, see [Using Remote Management](#).
2. In Recovery Environment, select **Tasks > Restore Volume** to launch the Restore Wizard.
You can also select **Restore Volume** in the left-side Navigation panel or select **Restore Wizard** in the Wizards tab.
3. On the Restore Type page, select **Finalize an HSR Restore**, then click **Next**.
4. On the Restore Destination page, select the hard disk where you previously created the HSR volume, then click **Next**.
5. On the Specify Finalization File page, select how you want to finalize the HSR volume, then click **Next**.

Finalize using information from the backup image file set	Uses the original Image Set files to finalize the HSR volume. The source Image Set must be accessible to Recovery Environment to finalize the volume.
Finalize using information from a .HSR File	Uses a previously created HSR file to finalize the HSR volume. The source Image Set files are not needed to finalize the HSR volume. You must specify that you want to create an HSR file when creating the HSR volume (see Restoring a System Volume).

6. On the Specify the Restoration Options page, select the boot parameters you want to apply to the restored volume, 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	<p>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:</p> <p>Restore MBR from the image file: Restores the MBR from the backup image file.</p> <p>Restore original Windows MBR: Restores the default MBR for the version of Windows you are restoring.</p> <p>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.</p>
Restore Disk Hidden Track	<p>Restores the first 63 sectors of a drive. Some boot loader applications require this for the system to boot.</p>
Use Hardware Independent Restore	<p>Instructs Recovery Environment to launch the Hardware Independent Restore (HIR) utility when finalizing the volume for use so you can configure the restore operation to properly interact with the hardware where you want to restore the volume.</p> <p>For more information, see Using HIR.</p>

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

Recovery Environment displays a "Success" message when the volume is finalized.

Optionally, you can use the Boot Configuration Utility to ensure that the newly restored system volume is "bootable". For more information, see [Using the Boot Configuration Utility](#).



11 Mounting a Backup Image File

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

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

To restore files and folders

1. Start Recovery Environment (see [Starting Recovery Environment](#)).
2. Open the Explore Backup Wizard by doing one of the following:
 - In the Wizards tab, click **Browse and Restore Files Wizard**.
 - In the Tasks menu, click **Explore Backup Image**.
3. In the Backup Image File Name page, browse to the image file you want to browse, then click **Next**. 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**. Recovery Environment displays this page if you select an Incremental image (.spi) to explore.
5. In the Explore Options page, select how you want to mount the backup image. You can mount the backup image as a Drive Letter or Mount Point. For more information about these options, see [Backup Image File Mount Options](#).

Assign the following Drive Letter	Mounts the backup image as the selected drive letter.
Mount in the Following Empty NTFS Folder	Mounts the backup image as a Mount Point. You must specify how you want 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.
Mount Backup as Read-Only	Mounts the backup image as read-only.

6. In the Wizard Summary page, review the mount information, then click **Finish**. ShadowProtect mounts the backup image file, then automatically launches an Explorer window and displays the mounted volume.



11.1 Dismounting a Backup Image File

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

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

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

To dismount a backup image

1. Start the ShadowProtect Console (see [Starting Recovery Environment](#)).
2. Open the Backup Image Dismount Wizard by doing one of the following:
 - In the Tasks menu, click **Dismount Backup Image**.
 - In the Disk Map tab, right-click a mounted backup image, then select **Dismount Backup Image**.
3. On 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's properties.
4. (Conditional) On the Backup Image Dismount Options page, select if you want to Save volume changes, or Shrink the backup Image, then click **Next**.

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

Save Changes to Incremental File	Saves changes made to the mounted volume. Right-click the Incremental File to save the modified backup image file using a different name.
Shrink Volume	Shrinks the volume so you can restore this image to a smaller hard drive. This option is available only when: <ol style="list-style-type: none"> a) Dismounting a writeable backup image of an NTFS volume in Windows Vista or Windows Server 2008 (or later); b) Running StorageCraft Recovery Environment using boot option 1 (Recommended), which boots using Windows PE (Windows 7-based).

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



11.2 Backup Image File Mount Options

When mounting a backup image file, consider the following:

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

11.2.1 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.

11.2.2 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.

11.2.3 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.



11.2.4 Mounting a Writeable Backup Image

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

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



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



12 Using Image Conversion Tool

The Image Conversion Tool lets you do the following:

- Change the compression setting on an existing image.
- Change the encryption setting on an existing image.
- Split an image into multiple files (a Spanned set) where each file has a maximum file size. This is useful for moving image files to CD or DVD.
- Consolidate a Base Image File and any Incremental Image Files into a new Base Image File.
- Convert existing image files into either .vmdk or .vhd format for use in a virtual environment.

To use the Image Conversion Tool

1. Start Recovery Environment (see [Starting Recovery Environment](#)).
2. In the Tasks menu, click **Image Conversion Tool**.
3. On the Source Image File page, select the Base image file you want to modify, then click **Next**.
If the backup image is encrypted you must provide the appropriate password.
4. On the Backup Image Dependencies page, select the Incremental backup image file to consolidate with the Base image file, then click **Next**.

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

- **Originating machine:** The operating system version, the machine name, MAC address and the engine version of ShadowProtect used to create the image file.
 - **Disk Information:** Disk geometry, disk size and number of the first track sectors. You can view the original disk layout in graphical form at the bottom of the screen.
 - **Original Partition Information:** Style, number, type, bootable option, starting offset and length.
 - **Image File Properties:** Volume size, creation time, compression, password protection, comment.
5. On the Destination Image File page, specify the location and name of the new backup image file, then click **Next**.
You can save the new backup image file locally or to a network drive.
 6. On the Backup Wizard Options page, specify the desired backup image file options, then click **Next**.
Information about each of these options, including the Advanced options, is available in [Options](#).
 7. On the Wizard Summary page, review the Image Conversion Tool job summary, then click **Finish**.



13 Using the Boot Configuration Utility

By default, ShadowProtect performs an automated boot configuration repair to help ensure that a system volume remains bootable once restored by ShadowProtect. The Boot Configuration Utility (BCU) lets you manage the boot configuration repair process for those situations where the automated process does not work, or for complex multi-boot scenarios not supported by the default process.

To effectively use the BCU and help ensure seamless migration and backup image restoration, you should understand the Windows boot process. For more information, see [Windows Boot Process](#).



BCU tools are accessible as buttons on the right-side of the UI. Additionally, the BCU includes the following UI-related options that help you organize and access BCU tools and data:

Hide Advanced Options: (Default: Selected) Hides all of the boot configuration tools except "Auto Repair".

To use the Boot Configuration Utility

1. Load Recovery Environment, then select **Tools > Boot Configuration Menu**.

The System Volumes pane lists all partitions that contain a Windows installation. Select Show All to display all detected volumes on the system, even if they do not contain a Windows Installation (this might be necessary for some Advanced boot scenarios). Each System Volumes entry includes the following information:

Status	The status of the current boot configuration. Options include <code>Bootable</code> , and <code>Broken</code> .
System	The root of the detected Windows installation.
Disk & Signature	The disk number and its signature. Every disk has a unique signature (Duplicate disk signatures can cause boot failures).
Partition	The disk partition where this volume resides.
Active	Indicates if the partition is configured as a Boot Partition. Although each disk in the system can have a defined Boot Partition, when using the Boot Configuration Utility it is best to have only a single Boot Partition in the system.



Boot Type	The type of boot loader required by the Windows Installation. Possible values include: Legacy: Uses the pre-Windows-Vista boot loader. BCD Compatible: Uses the BCD boot loader introduced with Windows Vista.
Boot Loader	The Boot loader installed on the partition, if any.

2. Select the desired boot repair action by clicking the appropriate button.

The BCU organizes its tools into groups so you can view only those that you need.

General Tools	
Auto Repair:	Run the automated ShadowProtect boot configuration routine. This action is available when the Status of the selected Windows installation is Broken This should be your first course of action when attempting to repair a boot configuration.
Refresh:	Refreshes the volume data in the <code>System Volumes</code> field.
Diagnose:	Run the automated ShadowProtect boot configuration routine in read-only mode so you can display a description of the boot configuration error and review possible courses of action.
Connect:	Connects the Windows installation to an existing Boot Partition. This is necessary if a partition is not mark as a Boot Partition.
Rename:	Opens the Boot Loader Entry Name dialog box, where you can change the name displayed for the selected volume at boot time.
Manage:	Opens the Manage Boot Entries dialog box, where you can delete unwanted boot entries from the selected volume. Each entry displays the technical name and the listed name. Use this option to remove unwanted boot entries at startup time.
 Note:	Deleting valid entries renders a volume unbootable until repaired.
Copy Log:	Copies the contents of the <code>Log</code> field to the clipboard so you can save it to a text file.
BCD Toolset (displayed by selecting BCD Tools)	
Install BCD:	Install a BCD boot loader. This might be necessary if the Windows installation (Windows Vista or later) was not the Active partition on the system where it was created.
Fix BCD:	Repair BCD-compatible boot configurations. When migrating a volume to a different disk, information required for startup might be altered or lost. <code>Fix BCD</code> repairs or replaces this information.
Custom CMD:	Open the <code>BCDEdit</code> utility for the BCD store of the selected Windows installation.
Install WIM:	Select a Windows Image (WIM) as a boot option.
Install VHD:	Select a Virtual Hard Disk (VHD) image as a boot option.



Legacy Toolset (displayed by selecting BCD Tools)

Install NTLDR: Install a legacy (NTLDR) boot loader. This might be necessary if the Windows installation (pre-Vista) was not the Active partition on the system where it was created.

Fix Boot.ini: Repair the `boot.ini` file used by legacy (NTLDR) boot configurations.

Registry Toolset (displayed by selecting Additional Boot Tools)

Edit Services: Opens the Service Explorer, where you can enable or disable services and drivers for the selected volume. This is very helpful if you need to debug a migration compatibility issue or identify a driver or service that is causing a start-up failure.

Drive Letter: Opens the Drive Letter editor, where you can assign a specific letter to any drive in the selected volume. This lets you set drive letters as they were before the migration.

Undo: Loads the registry backups for the selected volume. The BCU makes a backup of the registry whenever you use the Drive Letter Editor or the Service Explorer. This lets you back-out any changes that result in unexpected behavior.

 **Note:** This registry backup is the same one used by the Hardware Independent Restore (HIR), so any HIR changes are lost when you use Undo.

Disk Toolset (displayed by selecting Additional Boot Tools)

Patch MBR: Replaces the currently selected MBR and Hidden tracks with the MBR and Hidden Tracks from the volume's corresponding ShadowProtect image. This is useful if data from Hidden tracks were not restored.

Set Signature: Opens the Enter New Disk Signature dialog box, where you can manually set a disk signature. Typically, Windows sets the disk signature during installation, but migration and disk duplication can result in two disks with the same signature.

 **Note:** The Boot Configuration Utility will warn the user if there is a conflict.

Toggle Active: Sets the active partition flag for the selected partition. There can only be one active partition per disk. If there is an active partition set, Toggle Active disables it.



Initialize: Opens the Initialize Disks dialog box, where you can initialize disks in the system. This process installs an MBR and configures the disk for use by Windows.



Note: After initializing a disk, you must reboot before using the disk.

3. Review the entries in the Log pane to view the status of the boot configuration action.

The Log field displays a summary of the most recent log action. If an action fails, the log information identifies the point of failure. Click **Copy Log** to copy the contents of the Log field to the clipboard so you can paste it into a text file for more extended storage.



14 Using HIR

The Hardware Independent Restore (HIR) utility lets you restore system images to different hardware, or virtual environments. You must use HIR to restore backup image files in the following scenarios:

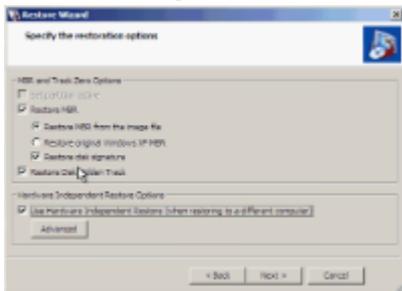
- Restoring to a different physical computer (P2P)
- Restoring from a physical computer to a virtual environment (P2V)
- Restoring from a virtual environment to a physical computer (V2P)
- Restoring from one virtual environment to another (V2V)

You can load the HIR utility from the Restore Wizard as part of a restore or as a stand-alone utility.

Note: To restore a backup image file of a system volume to different hardware with Recovery Environment, you must install ShadowProtect on the system volume before making a backup image of the volume. ShadowProtect IT Edition does not have this limitation.

To use HIR from the Restore Wizard

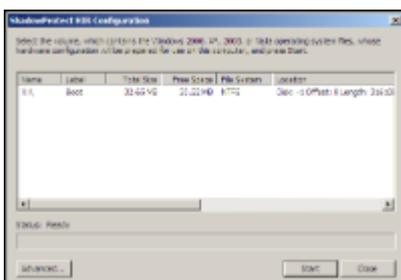
1. When finalizing a volume restore, click **Use Hardware Independent Restore**.



To use HIR as a stand-alone utility

1. Complete the steps for restoring a backup image (see [Restoring a System Volume](#)).
2. In Recovery Environment, click **HIR Configuration** in the Tools menu.
3. Select the volume that contains the Windows operating system, then click **Start**.

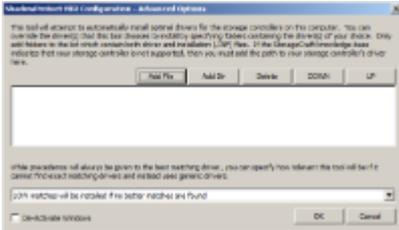
This prepares the restored volume to be bootable on the new system.





14.1 HIR Advanced Options

The HIR Advanced options dialog box lets you add files and directories to Recovery Environment's driver detection process.



From the HIR Advanced Options dialog box, you can do the following:

Add File: Adds a driver to the HIR driver list. You must have both the .sys and the .inf file for any driver you want to add.

Add Dir: Adds a directory to the driver search path. Any directory added to the driver search path must contain both the .sys and the .inf files for any driver that you want HIR to include in its driver analysis.

Delete: Deletes the selected driver or directory from the HIR driver list.

DOWN/UP: Move the selected driver or directory up or down in the HIR driver list. Recovery Environment attempts to use supplemental drivers in the order listed in the driver list.

De-activate Windows: De-activates the Windows installation so you can subsequently activate it through normal Windows mechanisms. Sometimes, an HIR-restored Windows environment is no longer active due to the changes in hardware.

Additionally, you can select how closely a driver must match the actual storage hardware to load. Options include:

- Driver must match hardware EXACTLY.
- Load drivers that are an EXCELLENT match if no better driver is found.
- Load drivers that are a GOOD match if no better driver is found.
- Load drivers that are a FAIR match if no better driver is found.
- Load drivers that are a LOW match if no better driver is found.



15 Using Remote Management

The ShadowProtect CD includes the UltraVNC Server and Viewer that let you remotely control, using the UltraVNC Viewer, a computer running Recovery Environment and UltraVNC Server.

To configure the UltraVNC remote management solution

1. Load UltraVNC Server on the computer that you need to manage.
 1. Load Recovery Environment (see [Starting Recovery Environment](#)).
 2. In Recovery Environment, click **UltraVNC** in Tools menu.
UltraVNC Server prompts you to set the remote management password. Once UltraVNC Server loads, you can remotely manage the computer with UltraVNC Viewer.



2. Configure UltraVNC Viewer on the remote computer
 1. Collect the information necessary to connect to UltraVNC Server.
 2. Load UltraVNC Viewer.
 3. Specify the IP address of the computer running UltraVNC Server, then click Connect.
 4. When prompted, specify the remote management password.
Once connected to the remote UltraVNC Server, you can operate ShadowProtect and Recovery Environment as normal.

For more information about UltraVNC Server and UltraVNC Viewer, visit <http://www.ultravnc.com/>.



16 Other Operations

The StorageCraft Recovery Environment supports the following additional operations:

- [Verifying Backup Image Files](#)

16.1 Deleting Backup Image Files

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

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

16.2 Verifying Backup Image Files

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

To use the verify image wizard

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



17 Windows Boot Process

The Boot Process can be complicated, with several different systems playing a part in it. To effectively migrate or restore bootable volumes, you should be familiar with some of these components. The systems that take part in the boot process include, in order of participation, the following:

BIOS -> MBR -> Boot Sector -> Boot Loader -> Boot Loader Configuration -> Windows System
(Splash Screen)

BIOS: The Basic Input Output System (BIOS) initiates the boot process. The BIOS configuration determines the boot order for the bootable disks in the system. For example: CD Drive, then Hard disk 0, then USB Storage Device. It is important to understand a system's boot order, because there is no way for Windows to query the BIOS to find out the disk used to boot the system.

MBR: The first sector of a bootable disk is the Master Boot Record (MBR). The MBR contains the disk partition information for the bootable disk. Each disk has one "Active" partition. The Active partition contains a boot sector, which is the next step in the boot process. If the disk does not have an Active partition, it is not bootable and the BIOS moves to the next disk in its boot order, or displays an error if no disk has an active partition.

Boot Sector: The boot sector of an active partition is located in the first 16 sectors of the partition. The boot sector contains the boot loader (NTLDR or BOOTMGR). If there is not a valid boot sector in the active partition, the BIOS displays an error, or a blank screen with a cursor.

Boot Loader and Configuration: The boot loader takes control of the boot process and reads its configuration file (boot.ini or BOOT\BCD), which directs the boot process to a Windows installation located on a specific disk and partition in the system wide. If the configuration file is valid, Windows starts loading and you see the Windows Splash screen appear on the system display. If the Windows installation includes multiple boot options, the user can select the specific Windows installation to use. Any problems with the configuration file result in system errors.



18 Product Support

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

18.1 Complimentary Technical Support

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

18.2 E-Mail Support

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

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

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

18.3 Telephone Support

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



19 Glossary

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

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

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

Base Image File: 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.

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

Full Image File – 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.

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

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

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

Image or Image File: See Backup Image File.

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

Incremental Image File: Backup files containing the sectors that have changed since the last Incremental backup was taken. Incremental images are fast to create and smaller than either 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.