STORAGECRAFT®

StorageCraft Recovery Environment User Guide

StorageCraft Copyright Declaration

Table of Content

StorageCraft Recovery Environment User Guide

Welcome to the StorageCraft® *Recovery Environment User Guide*. It describes the ShadowProtect technology, and how to derive maximum benefit from the StorageCraft Recovery Environment. It also describes using the ShadowProtect IT Edition. The IT Edition is identical to the Recovery Environment except that it is distributed as a USB key with a distinct license.

Note: This Guide covers the Recovery Environment-Windows (RE-WIND). Refer to the Recovery Environment-Crossplatform (RE-X) User Guide for details of that software.

This Guide covers Recovery Environment v5.2.5 and REBuilder v1.1.7. New to this release is a 64-bit Recovery Environment that should support native UEFI booting and those with Secure Boot enabled. The 64-bit version does not need to run in Compatibility Mode with UEFI.

This guide includes these major sections:

Additional Information

For emerging issues and other resources, see the following:

- The ShadowProtect ReadMe and StorageCraft Recovery Environment ReadMe files available online.
- The Recovery Environment forum at www.storagecraft.com/support/forum.
- The StorageCraft technical support Web site at www.storagecraft.com/support.html.
- The StorageCraft Glossary of technical terms.

Documentation Conventions

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

1 ShadowProtect Overview

StorageCraft Recovery Environment is a critical component of the overall ShadowProtect disaster recovery solution. You should be familiar with how Recovery Environment fits in this solution and when to use it:

1.1 Features and Components

Component	Features

ShadowProtect Console

This console manages the disaster recovery configuration on your Windows system. The console can:

- Configure wizard-based backup jobs that run unobtrusively in the background using Microsoft VSS (Volume Shadow Copy Service).
- Store backups on 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 data integrity.
- Create compressed and encrypted backup image files for efficiency and security.
- Run 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.
- Mount any backup image file as a virtual disk using VirtualBoot.
- Remotely manage system backup and recovery operations.

ShadowProtect Backup Agent

The engine that creates a system's point-in-time backup images. The ShadowProtect console manages the operation of the backup agent.

StorageCraft Recovery Environment

A bootable environment for disaster recovery. This environment installs no software. It can:

- Load from a bootable CD or a USB stick.
- Mount any backup image file as a virtual disk using VirtualBoot.
- Access all the features of the ShadowProtect Console from a standalone disaster recovery environment.
- 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.

StorageCraft ImageManager

ImageManager controls your backup image files using policy-driven services. ImageManager can:

- Consolidate incremental backup image files into daily, weekly, monthly or rolling monthly consolidated files that greatly reduce the number of files and the space required in an image chain.
- Verify and re-verify backup image files, including consolidated files, to ensure their integrity.
- Replicate backup image files to a local drive, a network share, or an off-site location.
- Rapidly restore images using Head Start Restore (HSR) while ShadowProtect continues to add incremental backups to it. This greatly reduces the downtime associated with hardware failure or hardware migration tasks.

⚠ **Note:** For a complete version history of product updates, see the Recovery Environment ReadMe.

1.2 Recovery Environment Usage Scenarios

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

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.

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 9 and their Converter tool.

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 the three days it takes to migrate the data to new hardware.

Solution: Keep the old server running, generate incremental backups, and begin a HeadStart Restore of the same backup image chain to 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 the off hours, apply the final incremental backup to the new server, and bring the new system online. 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.

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 these 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 online as a replacement for the failed production server.

2 How ShadowProtect Works

ShadowProtect creates backup image files that are an exact 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. In the event that you need to recover data, you can mount a backup image file (using the ShadowProtect Mount utility) and view its contents as if it were a regular volume. You can then recover specific files and folders from the image or you may recover the entire volume to that exact point in time that the backup image was taken.

ShadowProtect performs two primary tasks:

- Create a Backup Image
- Restore a Backup Image

using a variety of image file types.

2.1 Create a Backup Image

Creating a backup image using the installed version of ShadowProtect involves two key processes:

Create a Snapshot

Using 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 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	• VSS-aware applications 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	• VSS-aware applications achieve best backups. • Use script files (before and after the snapshot) to manage non-VSS-aware applications and improve backups. • Cannot create incremental image files
StorageCraft VSM direct	Windows 2000 Server Family Windows 2003/2008 Server Family	Fast	Good	• 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. ImageManager and the ShadowProtect image conversion tool simplify image management by consolidating files in an image set, modifying password encryption and compression, and merging or splitting image files.

Save the 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 details, see Creating a Backup Image File in the ShadowProtect User Guide.

Create a backup using Recovery Environment

The Recovery Environment can create a single full backup image of a system. It can also create a later, differential image of the system if it can access the system's base image on an external drive. However, it cannot schedule a backup job.

2.2 Restore a Backup Image

Once you create a backup image, you can restore this data in two different ways:

Restore individual files and folders

Use the ShadowProtect Mount utility to open an image file as a volume either as a drive letter or a mount point. The Mount utility can efficiently mount hundreds of backup images simultaneously, if needed. These mounted files preserve the Windows volume properties of the original. Users can access the backup image file just as if the volume were on a hard disk. This includes modifying and then saving any changes to the temporary volume as an incremental backup file.

For details on mounting backup image files, see Mounting Backup Image Files in the ShadowProtect User Guide.

Restore an entire volume

Use the ShadowProtect Restore Wizard to restore an entire *data* volume from a backup image file. Use the StorageCraft Recovery Environment to restore a *system* (boot) volume.

2.3 Backup Image Files

The Recovery Environment's Explore Backup Image utility can mount a backup image file as if it were a regular volume. You can then recover specific files and folders from this mounted image. (You recover the entire volume to the exact point in time that ShadowProtect captured the backup image using the Restore Volume function.)

ShadowProtect creates the following types of files:

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 made since a previous 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.
Spanned (.sp#)	Image files that belong to a spanned image set. ShadowProtect makes spanned image sets 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.
-cr	A rolling file used by ImageManager consolidation
.spk	A password key file used to encrypt backup image files.

.spwb	A temporary "write-back" file used to save changes for a mounted image file volume.
.bitmap	A data file used in optimizing ImageManager consolidation

File Naming Conventions

ShadowProtect naming convention identifies the file and its relationship to, and dependencies on, other backup image files. The syntax is:

```
<volume-identifier>-b_<base-seq>-d<diff-seq>-i<inc-seq>.<extension>
```

This syntax uses the following variable components:

Component	Description
volume identifier	Identifies the volume that the backup image file represents.
base-seq	The **Base** backup image file sequence number. This either identifies: • the sequence number of this file or • 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 • 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 • the incremental image file upon which this file is dependent.

Extensions

ShadowProtect uses various file extensions to identify if the file is a Full, Incremental, or Spanned backup image file:

File Type Extension	Description
`C_Vol-b001.spf`	**Full image** of the C:\ volume.
`C_Vol-b001-d001-i000.spi` or `C_Vol-b001.d001.spi`	**Differential image** of the C:\ volume with a dependency on the full backup image file `C_Vol-b001.spf` **Note:** This type of backup is not available in ShadowProtect IT Edition.
`C_Vol-b001-d000-i001.spi` or `C_Vol-b001-i001.spi`	**Incremental image** of the C:\ volume with a dependency on the full backup image file `C_Vol-b001.spf` **Note:** The only time ShadowProtect IT Edition creates a .spi file is when you mount a backup image as writeable and then save the changes to an incremental file.
`C_Vol-b001-d001.i001.spi`	**Incremental 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`. **Note:** This type of backup is not available in ShadowProtect IT Edition.

⚠ **Note:** A backup image filename that has a "`-d000`" or "`-i000`" segment uses this segment only as a placeholder. This segment indicates that a differential backup image or an incremental backup image is not part of the image chain. It also indicates that the backup image file has no dependency on a previous differential or incremental backup image file.

File Dependencies

By examining the name of a backup file image, ShadowProtect users can 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.

3 Using ShadowProtect IT Edition

StorageCraft distributes both the ShadowProtect IT Edition and the ShadowProtect IT Edition PRO software. These two products::

- Provide volume backup and restore services
- Run from a StorageCraft USB key
- Use an annual subscription model
- Install no software on a system to do a volume backup or restore

The IT Edition PRO differs in that it includes the ShadowProtect Granular Recovery for Exchange software. This IT Edition GRE recovers mailboxes, folders, and messages from Exchange backups from an unlimited number of servers.

This section contains the following topics:

- Requirements
- Launching the IT Edition
- Creating an IT Edition CD
- Updating USB Key Source Files

which apply to both IT Editions. The GRE software has its own user guide to describe using the package.

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

3.1 IT Edition Requirements

ShadowProtect IT Edition has the same requirements as Recovery Environment and supports the same systems and media as ShadowProtect does as targets for restoration. The one major difference is that the IT Edition requires an available USB port (either USB 2 or 3) unless using a license server (in which case, the IT Edition runs from a CD and requires a CD-ROM drive).

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

Hardware Requirements

ShadowProtect IT Edition requires:

- All minimum operating system requirements.
- At least 1GB of RAM (or the minimum required by the operating system).
  Note: The IT Edition requires at least 1GB of RAM. If the target system has less than this amount, the IT Edition may fail to boot. Increase the amount of RAM as required to provide 1GB. If this is not an option, use the 32-bit version of the Recovery Environment.
- Available USB 2.0 or 3.0 port.
  Note: Most versions of Microsoft Hyper-V lack USB passthrough or have limited USB support. This may impede license verification or running GRE with the IT Edition.
- Available optical drive if using a ShadowProtect IT Edition CD.
- Port 20248 open on the firewall if using a ShadowProtect IT Edition CD on another system.

Note: To launch the Recovery Environment on a UEFI motherboard, the UEFI must support BIOS emulation.

Supported Operating Systems

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

- Windows 2012
- Windows 8 family
- Windows Server 2008 (including R2)
- Windows 7 family
- Windows Vista family, including:
  - Vista Home Basic
  - Vista Home Premium
  - Vista Business
  - Vista Ultimate
- Windows XP family, including:
  - XP Home
  - XP Professional
- Windows Server 2003 family, including:
  - Server 2003 Standard Edition
  - Server 2003 Standard Edition R2
  - Server 2003 Advanced Edition
  - Server 2003 Advanced Edition R2
  - Server 2003 Enterprise Edition
  - Server 2003 Enterprise Edition R2
  - Server 2003 Datacenter Edition
  - Server 2003 Datacenter Edition R2
  - Server 2003 Web Edition
  - Small Business Server 2003
- Windows 2000 Server SP4

Note: Most versions of Microsoft Hyper-V lack USB passthrough or have limited USB support. This may impede IT Edition license verification or running GRE from the IT Edition USB key. This also means that the IT Edition cannot run "hot" on virtual machines on a booted Hyper-V hypervisor (Type 1 or Type 2). If necessary, run an IT License Server in order to perform license verification.

Supported File Systems

ShadowProtect IT Edition supports the following file systems:

- FAT16
- FAT16X
- FAT32
- FAT32X
- NTFS
- MBR disks
- GPT disks
- Basic and Dynamic volumes and disks
- 4K/AF drives with 4096-byte sectors

Note: ShadowProtect does not support the exFAT or ReFS file systems. It also does not support Windows Storage Spaces storage pools.

Supported Storage Media

The IT Edition supports these storage media:

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

The Image Conversion feature of the IT Edition supports these virtual disks:

- VMware VMDK
- Microsoft VHD

Note: Image Conversion does not support Microsoft's VHDx.

3.2 IT Edition Licensing Scenarios

The IT Edition features that require an IT Edition license include:

- Hot Backup
- Disk Copy
- Multi‑Volume Restore

Users running the regular Recovery Environment for Windows also see these options in the interface. However, selecting any of them displays a message that the option requires a valid IT Edition license.

The following table describes the various licensing scenarios available to IT Edition:

License Option	License Status	Features available
IT Edition USB Key	Valid	Enables all functionality
	Unlicensed/Invalid/Expired	Disables these licensed features: • Hot Backup • Disk Copy • Multi‑Volume Restore
IT Edition CD	Licensed by IT Edition license server	Enables all functionality
	Cannot access license server	Disables licensed features: • Hot Backup • Disk Copy • Multi‑Volume Restore
IT Edition 3‑day ISO	Valid	Enables all functionality
	Expired	Disables licensed features: • Hot Backup • Disk Copy • Multi‑Volume Restore
IT Edition Recovery Environment (CD or USB)		Disables licensed features: • Hot Backup • Disk Copy • Multi‑Volume Restore

3.3 Creating the IT Edition USB Key

Note: Previous editions of the IT Edition USB key included a pre-built Windows environment. Microsoft discontinued the distribution of this product, requiring users to create this environment manually.

StorageCraft provides the Recovery Environment Builder (REBuilder) to create the Recovery Environment for Windows IT Edition (also known as REWIND-IT) either in the Standard or PRO version. The resulting IT Edition works as previous editions with tools to restore system volumes.

IT Edition USB Key

StorageCraft ships a USB key for the IT Edition which includes:

- Recovery Environment CrossPlatform (RE-X)--for use in cold boot systems
- Recovery Environment for Windows (REWIND)--for use in hot systems
- ShadowProtect Granular Recovery for Exchange (GRE)--runs in Demo mode
- Configuration files to support REWIND-IT

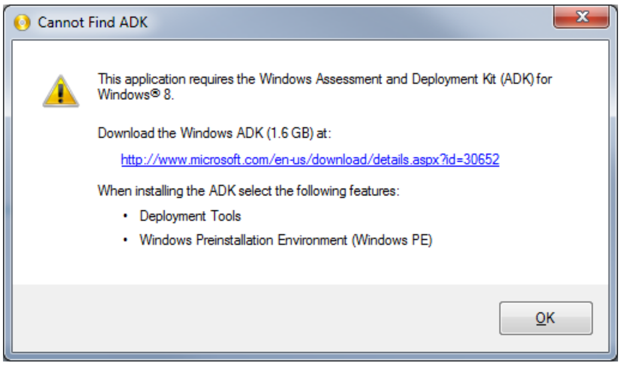
The USB key can boot a system into RE-X for backing up or restoring system volumes. The REBuilder tool adds REWIND-IT to the key to create the familiar IT Edition. Once the tool adds REWIND-IT to the key, the key can perform two operations:

- Insert the key into a live system to run ShadowProtect without installing any software.
- Boot a system using the key displays a menu to run either REWIND-IT or RE-X.

To create the IT Edition

Warning: The dual-boot capability of the IT Edition requires using the assigned volume name on the USB drive as shipped. Do not change this. Doing so prevents the dual boot option.

1. Download and run the Setup executable (or insert the REBuilder disc) into a working Windows 7 or newer system.
   Note: If this system is a VM, verify that the CD-ROM settings for the VM do not use *Legacy Emulation*. Otherwise, the VM cannot burn the ISO to a CD or DVD disc, Also, on ESXi systems, verify that the client uses *Passthrough IDE* and not *Emulate IDE*.
2. Select the REBuilder's language then click **Next**.
   Note: This language selection only applies to dialogs in the REBuilder, *not* to the IT Edition that it builds.
3. Follow the wizard to install the REBuilder.
4. Once the install completes, select Start\All Programs\StorageCraft\Recovery Environment Builder to run the program (if it is installed using the default location of Program Files\StorageCraft\ReBuilder.
5. If the software does not detect an install of the Windows Assessment and Deployment Kit (ADK), it displays this error message:



This application requires the Windows Assessment and Deployment Kit (ADK) for Windows® 8.

Download the Windows ADK (1.6 GB) at:

http://www.microsoft.com/en-us/download/details.aspx?id=30652

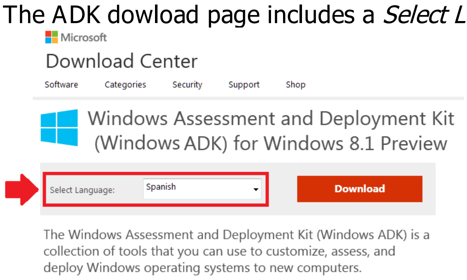
When installing the ADK select the following features:

- Deployment Tools
- Windows Preinstallation Environment (Windows PE)

6. Do not click **OK**. Doing so runs the REBuilder but without the needed components. (These are the Deployment Tools and Windows Preinstallation Environment (Windows PE).) If necessary, close the REBuilder and re-run it to return to the error message.

7. Use the link in the message to open a browser window to the Microsoft Download Center.

8. Close the REBuilder program.
9. The ADK dowload page includes a *Select Language* option:



Windows Assessment and Deployment Kit (Windows ADK) for Windows 8.1 Preview

Select Language: Spanish

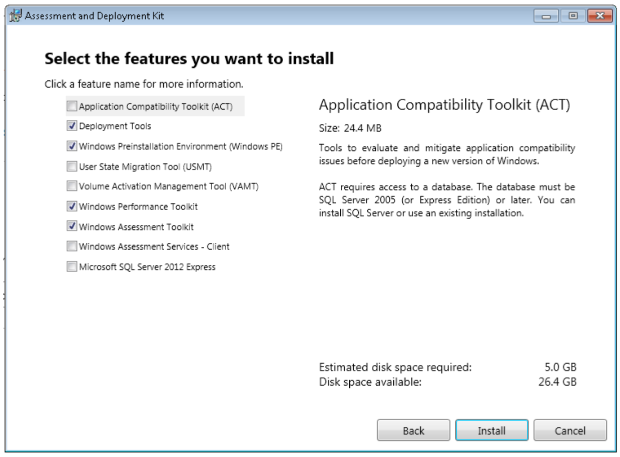
The Windows Assessment and Deployment Kit (Windows ADK) is a collection of tools that you can use to customize, assess, and deploy Windows operating systems to new computers.

   Ignore this option. This only selects the language for this Download Center webpage, *not* the language of the ADK. The ADK includes its own language support.

10. Click **Download** to download the ADK setup program (it is 1.2MB in size).
    NOTE: Although the dialog states that the ADK is for Windows 8, these components also run on Windows 7.

11. Run the ADK setup program. Follow the wizard prompts to begin the install.

12. At the *Select Features* page, the program lists all of the available components for download:



Assessment and Deployment Kit

Select the features you want to install

Click a feature name for more information.

- □ Application Compatibility Toolkit (ACT)
- ☑ Deployment Tools
- ☑ Windows Preinstallation Environment (Windows PE)
- □ User State Migration Tool (USMT)
- □ Volume Activation Management Tool (VAMT)
- ☑ Windows Performance Toolkit
- ☑ Windows Assessment Toolkit
- □ Windows Assessment Services - Client
- □ Microsoft SQL Server 2012 Express

Application Compatibility Toolkit (ACT)

Size: 24.4 MB

Tools to evaluate and mitigate application compatibility issues before deploying a new version of Windows.

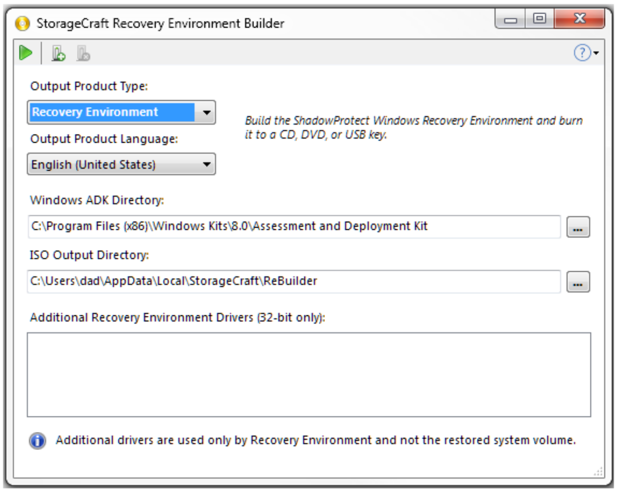
ACT requires access to a database. The database must be SQL Server 2005 (or Express Edition) or later. You can install SQL Server or use an existing installation.

Estimated disk space required: 5.0 GB
Disk space available: 26.4 GB

13. Select only *Deployment Tools* (39.6MB) and *Windows Preinstallation Environment (Windows PE)* (1.6GB). Uncheck any others marked by default.
14. Click **Install**.

15. Close the installer when it completes.

16. Rerun the REBuilder. The software displays its main dialog:



StorageCraft Recovery Environment Builder

Output Product Type: Recovery Environment

Build the ShadowProtect Windows Recovery Environment and burn it to a CD, DVD, or USB key.

Output Product Language: English (United States)

Windows ADK Directory: C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit

ISO Output Directory: C:\Users\dad\AppData\Local\StorageCraft\ReBuilder

Additional Recovery Environment Drivers (32-bit only):

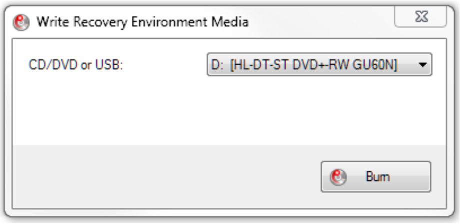
Additional drivers are used only by Recovery Environment and not the restored system volume.

17. Select the Output Product Type as *IT Edition.*
Note: The list includes *IT Edition 3-Day ISO* as well as this ISO is no longer available from StorageCraft directly.

18. Select the appropriate language.
Note: This language selection only applies to the IT Edition, *not* to any OS being restored. The default is the language selected with the REBuilder Setup program.

19. Keep the default paths for the ADK and the ISO output unless necessary.
20. (Optional) The IT Edition may need additional drivers to view specific storage devices. Adding these drivers here means that these drivers are included on the USB stick. To install these drivers, click on the menu bar.
Note: These drivers must be 32-bit even if the restored target OS is 64-bit. The IT Edition's Recovery Environment is a 32-bit application. This means that the IT Edition requires 32-bit drivers to access storage devices. The IT Edition also supports adding these drivers later on during each individual install.
Important: The IT Edition Recovery Environment created by REBuilder does not currently support iSCSI.
21. Locate each needed .inf driver file to include in the Recovery Environment.
Note: REBuilder displays an error message if the driver is 64-bit only. Confirm that the driver SYS file is 32-bit and that it is correctly referenced in the driver .inf file.
Warning: Do not delete any of the listed driver files or move them to a different folder until after using the REBuilder to burn the last required copy of the ISO. (Which may be later on.) If the REBuilder cannot find the driver file(s), it fails. If this occurs, restart the program and recreate the list with the correct driver location(s).
22. To remove a listed driver, select the driver and click .

23. Click ▶ to build the IT Edition Recovery Environment.
24. When finished, REBuilder stores the IT Edition ISO in the selected path. REBuilder then asks if you want to burn the ISO to a CD, DVD, or to USB:



Write Recovery Environment Media

CD/DVD or USB: D: [HL-DT-ST DVD+-RW GU60N]

Note: REBuilder displays an error if the system has no recorder.

If you don't want to burn an ISO, simply close the dialog.

25. To burn the ISO later, rerun the REBuilder tool.
NOTE: You can also use the ShadowProtect ISOTool to burn this ISO to a CD.
26. Click ● to open the Burn dialog.
27. Select the destination in the dropdown box.
28. Click **Burn**.

The program burns the ISO to the disc or USB key.

You can now use the disc (or insert the USB key) to boot a PC and recover a system volume. If this is an IT Edition PRO, you can also run ShadowProtect Granular Recovery for Exchange (GRE) to restore mailboxes, folders, or messages.

3.4 Launching IT Edition

The IT Edition USB key can:

- Run ShadowProtect without installing it on a system
- Boot the Recovery Environment (REWIND-IT or RE-X) to backup or restore a system volume

To start ShadowProtect from the USB key

1. (Conditional) If this is the first time using the IT Edition, remove the write lock on the USB key.
2. Insert the USB key into an available USB 2.0 or 3.0 port.
3. Use Windows Explorer to browse the USB key and execute the `START SHADOWPROTECT` command script. ShadowProtect IT Edition displays.
4. (Conditional) If prompted after selecting an option, enter a valid license code to activate the ShadowProtect IT Edition.
Note: When you purchase ShadowProtect IT Edition, StorageCraft provides you a license code to activate the software. Additionally, you must reactivate the USB key on a quarterly basis. To do this, plug the USB key into a system with Internet access and repeat these steps.

To load StorageCraft Recovery Environment from the USB key

1. Shutdown the system.
2. Insert the USB key into an available USB port, then restart the system.
If necessary, configure the system boot manager or BIOS to boot from a USB drive before the system's hard disk.
Note: When using the Recovery Environment on a UEFI motherboard, the UEFI must support BIOS emulation.
3. Select the option to run the IT Edition Recovery Environment for Windows.
4. Follow the on-screen instructions to load the IT Edition.
Refer to Starting Recovery Environment for details.

Write Lock Protection

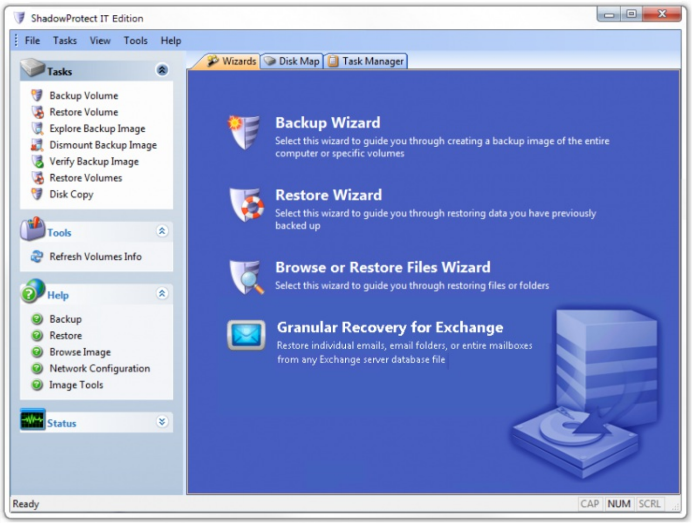
The IT Edition USB key includes a write lock that prevents data writes to the device. StorageCraft recommends keeping the write lock enabled except when:

- Activating or updating the product licensing.
- Updating ShadowProtect IT Edition source files.

3.5 Using the IT Edition Interface

The ShadowProtect IT Edition interface differs depending on the state of the system:

Boot from the IT Edition key	The IT Edition interface is identical to the Recovery Environment for Windows interface.
Run ShadowProtect from the IT Edition key on a live system	The IT Edition ShadowProtect offers a slightly different main dialog (shown here) when run on a system with a Windows operating system running.



Backup Wizard

Select this wizard to guide you through creating a backup image of the entire computer or specific volumes

Restore Wizard

Select this wizard to guide you through restoring data you have previously backed up

Browse or Restore Files Wizard

Select this wizard to guide you through restoring files or folders

Granular Recovery for Exchange

Restore individual emails, email folders, or entire mailboxes from any Exchange server database file

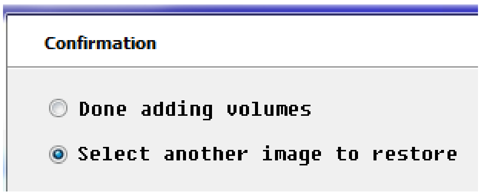
This dialog offers a simplified set of tools useful for working with volumes while the OS is loaded. All the major functions and wizards perform as they do in Recovery Environment. The differences are:

Restore Volumes option in Tasks	Restores two or more volumes at the same time.
Disk Copy option in Tasks	Copies either volumes or disks in real time without requiring a backup image file.
Tools dropdown menu	Limited to two options: • Enable Logging • Refresh Volumes Info
Tools menu at the left	Limited to one option: • Refresh Volumes Info
Help dropdown menu	Includes a Contents link to online documentation.
Granular Recovery for Exchange wizard	If this key is licensed as the IT Edition PRO, this wizard launches the ShadowProtect Granular Recovery for Exchange software. If this key has the IT Edition standard license, the wizard launches the software in demo mode only. (This means that the software displays Exchange mailboxes, folders, and messages from a backup file but cannot restore them.)

Restore Volumes

The IT Edition's Restore Volumes option in the Tasks menu performs in the same way as the Restore Volume option does. The difference is that the Restore Volumes option can restore two or more volumes automatically while the Restore Volume option only does one volume at a time.

The wizard-based restore process is exactly the same for both options except at the Confirmation page. There, the Restore Volumes option displays a selector for choosing to complete the one-volume restore or to add another volume to the restore queue:



Confirmation

○ Done adding volumes

● Select another image to restore

Choose either:

Done adding volumes	Runs the restore on the queued volume(s).
Select another image to restore	Adds another volume to the restore queue.

When you choose *Select another image*, the wizard returns you to the *Backup Image to Restore* dialog at the start of the wizard. You can then select another image file. The wizard continues to guide you through the restore configuration and then asks if you want to add further image files.

Important: Add each volume to the restore queue in the order of their Recovery Environment drive letter assignment: C, D, E, and so forth. Ignore the order in which the partitions appear on the volume. For example, if Recovery Environment assigns the Windows System Reserve volume the drive letter "D" and the System volume the drive letter "C", begin the Restore Volumes process by selecting the System volume first, then adding the System Reserve volume to the queue.

When you have finished configuring the restore jobs, select *Done adding volumes* on the confirmation page to proceed with the restorations.

Disk Copy

The IT Edition's Disk Copy option in the Tasks menu creates a copy of:

- Single Partition
- Entire Disk

and places the copied partitions unto a selected drive. ShadowProtect's Restore Volume function can also create copies but only from existing backup images. Disk Copy creates the copy in realtime.

To copy a disk or partition

1. Confirm that the destination drive or partition is the same size or larger than the source drive or volume.
2. Select *Disk Copy* in the Tasks menu.
3. Choose to copy either a volume or a disk.
4. Select the source disk or partition.
   Note: Drive letters represent assignments made by the IT Edition, not what Windows assigned in the original source volume.
5. Select the destination disk or partition.
6. (Optional) Choose to include or not include unused sectors.
   Note: This could reduce the size of the copied volume on the destination.
7. Click **Finish**.

ShadowProtect creates an exact copy of the partition or disk on the destination drive.

Copying Windows Boot Volumes

After Disk Copy clones a disk with a Windows Vista or newer boot volume on it, the Windows PE component of the Recovery Environment automatically attempts to mount ALL available volumes. This includes the duplicate Windows boot volume. When it does so, Windows PE detects that the Disk Signature in the MBR of both disks is identical and automatically changes the signature of the duplicate boot volume. This may cause the duplicate volume to not boot.

To fix this:

1. Install the duplicate drive into a new system (or remove the original boot drive in the original system).
2. Boot up this new system using the IT Edition.

3. Run the Boot Configuration Utility (BCU) against the duplicate Windows boot volume. The BCU automatically fixes the issue with the duplicate.
4. Reboot the new system using the new boot drive.

3.6 Creating an IT Edition CD

Use the REBuilder tool to create a ShadowProtect IT Edition CD. You can then use this CD to run ShadowProtect or load the StorageCraft Recovery Environment on systems without a USB port. The tool automatically creates an ISO as part of creating the IT Edition USB key.

Note: An IT Edition CD requires an active License Server on the same network to run.

To create a ShadowProtect IT Edition CD

1. Run the REBuilder tool. The tool automatically creates an ISO as part of creating the IT Edition USB key.
2. Note the destination directory where the REBuilder stored the IT Edition ISO.
3. Use a CD/DVD burning software of your choice to burn the ISO image to CD or DVD media.

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

To start ShadowProtect in Windows

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

ShadowProtect IT Edition loads into memory and does not install software on the hard drive.

To load StorageCraft Recovery Environment

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

The Recovery Environment runs directly from the IT Edition CD/DVD). Again, the IT Edition does not install software on the hard drive.

Using the Licensing Server

The ShadowProtect IT Edition includes a licensing server used to run its applications from a CD on another system. The software on the CD locates its required license from this server to successfully run.

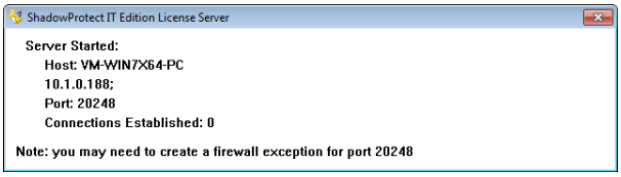
The IT Edition first checks locally for the USB key when it loads. If it does not detect the USB key, it then looks for the ShadowProtect Licensing Server on the network to confirm its license.

Note: The license server must be on the same network subnet as the system running the IT Edition software on a CD.

To start the license server

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

The Licensing Server utility loads onto the system.



```
Server Started:
    Host: VM-WIN7X64-PC
    10.1.0.188;
    Port: 20248
    Connections Established: 0

Note: you may need to create a firewall exception for port 20248
```

Systems running the IT Edition software from a CD can now confirm their licensing and run.

3.7 Updating the IT Edition Software or License

ShadowProtect® IT Edition™ expires quarterly both to ensure that all ShadowProtect® IT Edition™ subscriptions are current, and also to provide regular updates to the software. Near the end of each quarter, the ShadowProtect® IT Edition™ will notify the user that the IT Edition license is about to expire.

Download and use the REBuilder tool to update the IT Edition USB key so it contains the latest application files. This upgrade can be applied to any valid, licensed copy of ShadowProtect IT Edition 4.x.

Note: The upgrade package does NOT update the "Legacy" Windows 2003-based recovery environment. That environment will remain unchanged on the key. The REBuilder tool can also create an IT Edition 5.0.5 ISO for use on systems without an available USB port.

To update the USB key

WARNING: NEVER DELETE OR OVERWRITE the StorageCraft.id file on your IT Edition USB key. This renders the drive useless. Follow these instructions to avoid this error.

1. Perform a full backup of your IT Edition USB key.
2. Remove the write lock from the USB key.

   If you want to use an installed version of ShadowProtect from the workstation to make the backup, perform Steps 3-5. If you want to use the version of ShadowProtect on the USB key, skip to Step 6. (The IT Edition software automatically checks on its license status.)

3. Verify your IT Edition license is active by connecting the USB key to a computer with internet access. Run this test especially if you haven't used your USB Key for a while. Verifying the license ensures the update process completes properly.
4. Force a call home to the StorageCraft licensing server by:
   a) Executing `START SHADOWPROTECT` at a command prompt. With ShadowProtect running, select *Backup* or *Restore*.
   b) Executing `Start_LicenseServer` from the USB Key.
5. Abort the test once you confirm that your license is active. If it is not, contact StorageCraft Support.
6. After you verify the license, open a Web browser to the StorageCraft Upgrade page (http://www.storagecraft.com/release/sprelease.asp).
7. Enter your ShadowProtect serial number. Click **Submit.**
   Note: You must enter a valid serial number to get access to the download file.
8. On the Technician License Agreement page, scroll to the bottom and click **I Accept.**
9. The system presents one or more product download options based on your license. Select the REBuilder option.
   Note: The system then attempts to download the file directly. This is a large (700MB) file and may cause bandwidth and processing issues on some networks. In those cases, use the optional Download Manager which allows you to pause or restart a download.
10. Download and run the REBuilder Setup program. Follow the onscreen instructions to complete the install.
11. Select Start > All Programs > StorageCraft > REBuilder to launch the program.
12. Follow the steps on the Creating the IT Edition to complete the update.
13. Re-enable the Write Protection on the USB key.

The ShadowProtect IT Edition USB key is now updated.

3.8 Launching GRE from the IT Edition

The IT Edition Pro includes support for launching the StorageCraft Granular Recovery for Exchange (GRE) utility.

To run GRE from the IT Edition ISO when attached to booted Windows VM:

1. Attach a licensed IT Edition Pro USB key to a machine on the same network as the target system.
2. Launch the IT Edition license server.
3. Attach the IT Edition ISO (not the 3-day ISO) to the target machine intended to run GRE.
4. Launch the ShadowProtect UI from this ISO.
5. Temporarily select *Disk Copy*. This prompts the user for the IP address of the IT Edition license server.
6. Enter the IP address of the license server.
7. Click **OK**.
8. Open the GRE option. GRE displays and is now an active licensed version.

4 Starting Recovery Environment

Recovery Environment loads automatically when you boot from:

- The ShadowProtect IT Edition USB key
- A ShadowProtect Product CD which includes the Recovery Environment
- A custom CD or USB key created using the downloadable Recovery Environment Builder (REBuilder)

Before you run the Recovery Environment, make sure your system meets the minimum hardware and software requirements.

Note: NETGEAR-stored VHDX files are GPT format. However, they do not include two hidden volumes needed to attach the VHDX volume directly to a VM. Instead, follow the instructions in Step 12 to initialize a disk as a GPT System Disk, restore the NETGEAR VHDX to a volume on the VM.

To load the StorageCraft Recovery Environment

1. If the backup image chain to restore is located on a USB drive, attach that drive to the computer.
2. Attach the IT Edition USB key into a USB port or Insert the Recovery Environment CD or USB key into the computer.
3. Restart the computer.

   Note: You might need to modify the boot options to have the computer boot from a USB or a CD drive.
4. Select which language to use. The default is English.
5. (Optional) In the Network Support dialog box, click **Yes** to start networking. For example, Recovery Environment could use a network connection to access or save image files stored on another device on the network.

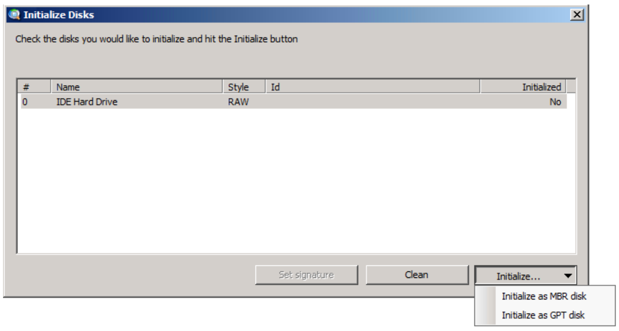
   Note: For details, see Using the Network Configuation Utility.

6. Select your time zone. Click **OK**.

If Recovery Environment detects no initialized disks, it displays the *Initialize Disks* dialog with a list of available drives. Otherwise, skip to the finish.

7. Select a disk(s) to initialize. You need to initialize at least one disk for the System/boot volume.

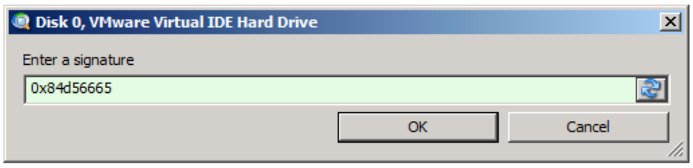
8. Click **Initialize**. Recovery Environment presents two options: MBR or GPT.



Check the disks you would like to initialize and hit the Initialize button

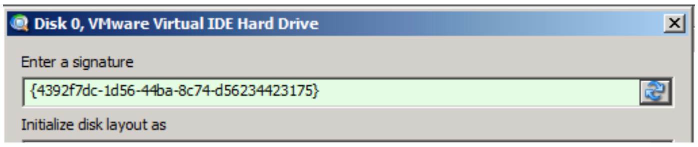
#	Name	Style	Id	Initialized
0	IDE Hard Drive	RAW		No

9. To use MBR, click **Initialize as MBR disk**. Recovery Environment displays a preconfigured signature for the drive:



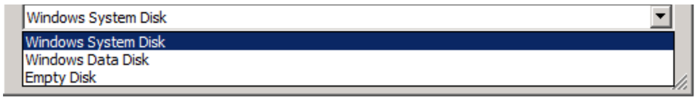
Enter a signature: 0x84d56665

10. Click **OK**.The Recovery Environment displays the Initialize dialog again.
11. Click **Close**. Recovery Environment displays its main screen. Skip to the finish.
12. To use GPT, click **Initialize as GPT disk** and Recovery Environment displays a preconfigured signature and disk layout options:



Enter a signature: {4392f7dc-1d56-44ba-8c74-d56234423175}

Initialize disk layout as

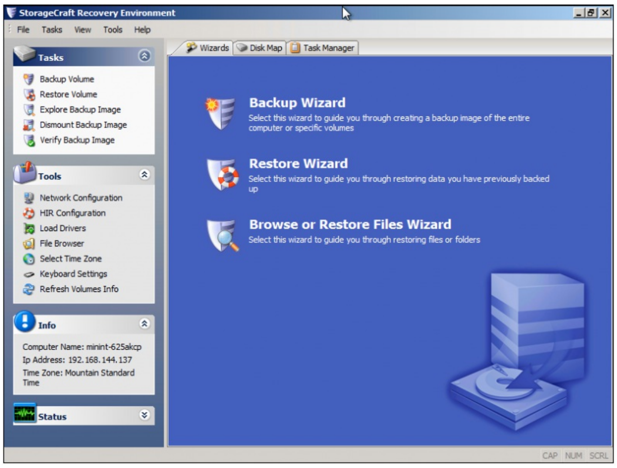


The three GPT options are:

- **Windows System Disk**--Select this option to format the drive as a boot/system drive.
  Note: You must choose System Disk at this point if you plan to use a GPT drive as a system volume with a UEFI motherboard. This option installs the necessary hidden components to make it a boot volume. Without these components, the volume will not boot. These cannot be installed later using the Disk Map options for a GPT drive.
- **Windows Data Disk**--Select this to format the drive for data volumes. You can use the partition options in the Disk Map tab or in the Restore Wizard to reconfigure a data volume later.
- **Empty Disk**--Select this option to initialize the drive as GPT but without creating a partition on it. Use the Disk Map tab or Restore Wizard options to create partitions later. This may be useful when the actual size of the partition needed for the recovery is not clear. Again, you cannot use Disk Map options to make a GPT disk initialized as an Empty Disk to become a bootable drive.

Note: The system must have UEFI firmware to boot a GPT system disk.

13. Click **OK** after selecting the disk layout type. Recovery Environment displays its main screen:



Computer Name: minint-625akcp
Ip Address: 192.168.144.137
Time Zone: Mountain Standard Time

Backup Wizard: Select this wizard to guide you through creating a backup image of the entire computer or specific volumes

Restore Wizard: Select this wizard to guide you through restoring data you have previously backed up

Browse or Restore Files Wizard: Select this wizard to guide you through restoring files or folders

This screen is similar to the installed version of ShadowProtect. To perform these ShadowProtect tasks, see Understanding the User Interface in the ShadowProtect Users Guide.)

4.1 Requirements

ShadowProtect Recovery Environment has these minimum software and 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)
Memory	1GB minimum **Note:** The Recovery Environment requires at least 1GB of RAM. If the target system has less than this amount, the Recovery Environment may fail to boot. Increase the amount of RAM as required to provide 1GB. If increasing memory is not an option, use the 32-bit version of the Recovery Environment.
Motherboard	Requires UEFI firmware to support GPT disks as bootable drives. When using a UEFI motherboard, the UEFI must support BIOS emulation to support Recovery Environment for Windows.
Hard Drive space	N/A
CD-ROM or DVD drive	Required for if the Recovery Environment is stored on a CD/DVD.
USB Port	Required if using the ShadowProtect IT Edition, REWIND on a USB key, or if the backup image chain is stored on an external attached USB drive. Supports USB 2.0 and USB 3.0.
Monitor	VGA or higher resolution

Network Connectivity	Configure VMs to use an identified OS option (such as Windows) and not "Other" in order for RE to automatically load the correct network driver.
Operating System	Bootable GPT drives require the boot OS to be a 64-bit Windows OS (Windows Vista and later). REBuilder requires Windows 7 or newer to run. (Older versions do not support the Windows ADK required to run REBuilder.)
Anti-virus	Anti-virus programs may conflict with REBuilder creating a Recovery Environment. Temporarily turn off the anti-virus program to successfully use REBuilder.
Windows ADK	REBuilder, which creates the Windows Recovery Environment, requires a clean install of Windows ADK v8.0 or v8.1. Note that Windows does not support installing both the 8.0 version of the ADK and the 8.1 version on the same system. Although Windows does support "upgrading" an existing ADK v8.0 install to a v8.1 install, this upgraded version does not support REBuilder. If necessary, uninstall an existing v8.0 install of the ADK, then install the v8.1 of the ADK before completing the REBuilder setup.
Drivers	USB drive or CD/DVD with any additional required 32-bit drivers not included with the Recovery Environment. (See Testing the Recovery Environment for details.)
Windows Deduplication	Recovery Environment for Windows does not support hot backups or restores from volumes with Windows Dedup enabled.
iSCSI	Recovery Environment for Windows also does not support iSCSI.

Hardware Independent Restore (HIR) Licensing

Recovery Environment for Windows allows HIR to run in the following situations. In all other cases, REWIND users must have a valid activation code to use HIR.

- ShadowProtect is installed *and* activated in the selected image file.
- ShadowProtect is installed *and* activated but is expired.
- ShadowProtect MSP is installed and activated, and its license is still within the subscription period.

Supported Sector Sizes

Contemporary hard drives and SSDs ship with a 4096-byte *physical* sector size. Most also support the 512-byte *logical* sector size. (These drives are often labeled 512e for "512 Byte Sector Size Emulation".) ShadowProtect supports backing up both 4096- and 512-byte logical sector sizes.

In the unusual situation of restoring a partition/volume from one logical sector size to another:

- 512 bytes per logical sector -> 4096 bytes per logical sector (and the destination does not support 512e)
- 4096 bytes per logical sector -> 512 bytes per logical sector

ShadowProtect will issue an error message during the restore if it encounters a mis-matched sector size.

4.2 Creating the Recovery Environment

Note: Previous editions of Recovery Environment and the IT Edition included a pre-built Windows environment. Microsoft discontinued the distribution of this product, requiring users to create this environment manually using the Recovery Environment Builder (REBuilder).

REBuilder is a simple tool to create a Windows-based Recovery Environment ISO (called the Recovery Environment for Windows). Once created, this ISO works as previous editions of the ShadowProtect Recovery Environment with tools to restore system volumes.

Requirements

REBuilder requires:

- Windows 7 or newer OSes
- Windows ADK v8.0 or v8.1

to build the Recovery Environment. Note that if the REBuilder setup program does not detect that the ADK is installed, the program displays a link to download it. (Earlier versions of Windows do not support the Windows ADK options needed to create the Recovery Environment.) Refer to the Requirements page for details.

There is no difference between the Recovery Environments created with ADK 8.0 or with ADK 8.1. However, If the ADK is not installed, use v8.0 as it is a significantly smaller download.

Important: REBuilder requires a *clean* install of Windows ADK v8.1. Although Windows does support "upgrading" an existing ADK v8.0 install to v8.1, this upgraded version does not support REBuilder. If necessary, uninstall an existing v8.0 install of the ADK, then install the v8.1 of the ADK before completing the REBuilder setup.

To create the Recovery Environment for Windows

1. Download and run the Setup executable (or insert the REBuilder disc) into a working Windows 7 or newer system.
   Note: If this system is a VM, verify that the CD-ROM settings for the VM do not use *Legacy Emulation*. Otherwise, the VM cannot burn the ISO to a CD or DVD disc, Also, on ESXi systems, verify that the client uses *Passthrough IDE* and not *Emulate IDE*.
2. Select the REBuilder's language then click **Next**.
   Note: This language selection *only* applies to dialogs in the REBuilder, *not* to the Recovery Environment ISO that it builds.
3. Follow the wizard to install the REBuilder.
4. Once the install completes, select REBuilder from the Start Menu.
5. If the software does not detect an install of the Windows Assessment and Deployment Kit (ADK), it displays an error message. This message includes a link to download the Windows ADK v8.0. (Use this version as it is a smaller download than the v8.1.)
6. Do not click **OK**. Doing so runs the REBuilder but without the needed components. (These are the Deployment Tools and Windows Preinstallation Environment (Windows PE).) If necessary, close the REBuilder and re-run it to return to the error message.

7. Instead, use the link in the message to open a browser window to the Microsoft Download Center.

8. Close the REBuilder program.

9. Caution: The ADK dowload page includes a *Select Language* option. Ignore this option. This only selects the language for this Download Center webpage, *not* the language of the ADK. The ADK includes its own language support.

10. Click **Download** to download the ADK setup program.
    NOTE: Although the dialog states that the ADK is for Windows 8, these components also run on Windows 7.

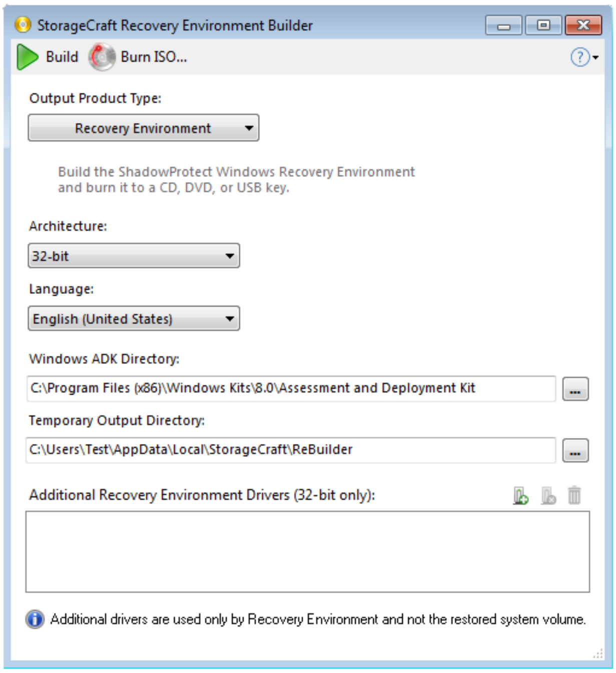
11. Run the ADK setup program. Follow the wizard prompts to begin the install.
    Note: If the setup program does not detect the required .NET Framework components installed, it installs those first. This may require a reboot prior to complete the ADK setup.

12. At the *Select Features* page, the program lists all of the available ADK components for download. Select only:

    - *Deployment Tools* (8.0 = 39.6MB; 8.1 = 54MB) and
    - *Windows Preinstallation Environment (Windows PE)* (3.0GB).
13. Uncheck any other features marked by default.
14. Click **Install**.

15. Close the installer when it completes.

16. Rerun the REBuilder. The software displays its main dialog:



Output Product Type: Recovery Environment

Build the ShadowProtect Windows Recovery Environment and burn it to a CD, DVD, or USB key.

Architecture: 32-bit

Language: English (United States)

Windows ADK Directory: C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit

Temporary Output Directory: C:\Users\Test\AppData\Local\StorageCraft\ReBuilder

Additional Recovery Environment Drivers (32-bit only):

Additional drivers are used only by Recovery Environment and not the restored system volume.

17. Keep the default Output Product Type as *Recovery Environment*.

18. Select the appropriate language.
    Note: This language selection only applies to the Recovery Environment, not to any OS being restored. The default is the language selected with the REBuilder Setup program.

19. Select the appropriate architecture: 32- or 64-bit. Note that either architecture can restore both 32- and 64-bit operating systems. The 32-bit version is smaller in size, and useful for copying onto CD. The 64-bit version supports native Secure Boot and UEFI.
20. Keep the default paths for the ADK and the ISO output destination unless necessary to change them.
21. (Optional) Recovery Environment may need additional drivers to view specific storage devices. (These devices might include specialized RAID or other subsystems or newer versions of a device.) Adding these drivers using this function means that REBuilder includes them on the Recovery Environment ISO. To add drivers, click on the menu bar.
    Note: For most situations, the Recovery Environment does not require additional drivers. It includes many drivers for existing hardware to allow the Recovery Environment to run. However, manufacturers may release new hardware or new versions of drivers or a site may use custom hardware with unique drivers. In those cases, use this option to include these drivers. These drivers must be 32-bit when building a 32-bit Recovery Environment. even if the restored target OS is 64-bit. (The Recovery Environment is a 32-bit application and requires 32-bit drivers, particularly to access storage devices.) The Recovery Environment ISO also supports adding these drivers later on during each individual restore.
    Important: The Recovery Environment created by REBuilder does not currently support iSCSI.
22. Locate each needed .inf driver file to include in the Recovery Environment.
    Note: REBuilder displays an error message if the driver is 64-bit only. Confirm that the driver SYS file is 32-bit and that it is correctly referenced in the driver .inf file.
    Warning: Do not delete any of the listed driver files or move them to a different folder. This should only be done after using REBuilder to burn the last required copy of the ISO. (Which may be later on.) If the REBuilder cannot find the driver file(s), it fails. If this occurs, restart the program and recreate the list with the correct driver location(s).
23. To remove a listed driver, select the driver and click .
24. Click ▶ to build the Recovery Environment ISO.
25. When finished, REBuilder stores the Recovery Environment ISO in the Temporary Output Directory. REBuilder then asks if you want to burn the ISO to a CD, DVD, or to USB. Select the appropriate destination then click **Burn**.

    Note: REBuilder displays an error if the system has no CD/DVD recorder.

    If you don't want to burn an ISO, simply close the dialog.

26. To burn the ISO later, rerun the REBuilder tool.
    NOTE: You can also use the ShadowProtect ISOTool to burn this ISO at a later time.
27. Click to open the Burn dialog.
28. Select the destination in the dropdown box.
29. Click **Burn**.

The program burns the ISO to the disc or USB key.

You can now use the disc (or insert the USB key) to boot a PC and recover a system volume.

Note: After creating the Recovery Environment, the ADK is not required. If conserving hard disk space is a priority, uninstall the ADK.

4.3 Testing the Recovery Environment

Test the StorageCraft Recovery Environment to:

- Ensure that it runs properly on your computer
- Confirm you have the correct drivers needed to access devices.

To test this, boot your computer with the ShadowProtect Recovery Environment CD or USB key.

If Recovery Environment boots and runs as expected, you are ready to restore from backup files in the event of a hardware failure, system volume corruption, or to attempt to save data running a cold backup.

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

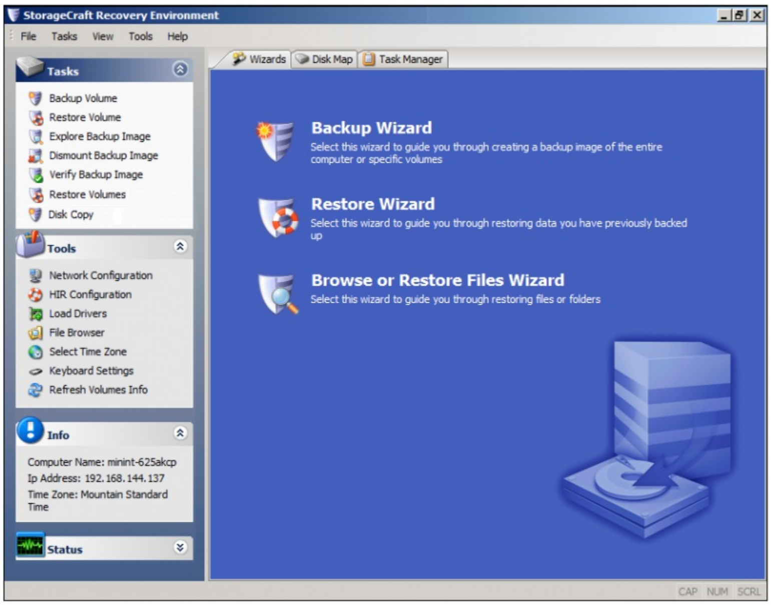
- You do not have the necessary network interface card (NIC) drivers to access the network. You can dynamically load NIC drivers from within Recovery Environment (click **Load Drivers** in the Tools menu).
- You do not have the necessary storage drivers to access a storage device on the computer. To resolve this:
    1. In the Tools menu, click **Load Drivers**.
    2. Browse to the appropriate storage driver files.

Once you identify the needed drivers, copy them to a readily accessible CD or USB drive to use with Recovery Environment.

⚠ **Note:** 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.

5 Understanding the User Interface

Once you initialize the disk, the Recovery Environment screen appears:



Computer Name: minint-625akcp
Ip Address: 192.168.144.137
Time Zone: Mountain Standard Time

Backup Wizard
Select this wizard to guide you through creating a backup image of the entire computer or specific volumes

Restore Wizard
Select this wizard to guide you through restoring data you have previously backed up

Browse or Restore Files Wizard
Select this wizard to guide you through restoring files or folders

This main screen includes three sections:

- **Menu Bar**--Located at the top of the screen. The Menu Bar provides access to additional tools for working with volumes.
- **Tasks**--Located at the left of the screen. The Task Panel is a navigation panel and gives access to information, tools and action wizards.
- **Main Dialog**--Located in the center of the screen. The Main Dialog has three tabs and the dialog's contents change to reflect which tab is active.

The Main dialog's three tabs include:

- **Wizards**--Launches the *Backup*, *Restore*, or *Files* wizard.
- **Disk Map**--Provides partition tools that function similar to the Windows Disk Management utility.
- **Task Manager**--Displays the status of an active task. To view task details, click **Show Details**. To abort an active task, click **Cancel**.

Wizards is the default tab displayed.

5.1 Menu Bar

The Recovery Environment menu bar provides these options:

Menu	Description	Options
File	Accesses application-level options	**Exit**: Closes the Recovery Environment.
Tasks	Access ShadowProtect wizards	**Backup Volumes:** Launches the Backup Wizard. **Restore Volume**: Launches the Restore Wizard. **Explore Backup Image**: Launches the Explore Backup Image Wizard. **Dismount Backup Image:** Launches the Backup Image Dismount Wizard. **Image Conversion Tool**: Launches the Image Conversion Tool. **Verify Image**: Launches the Verify Image Wizard.

View	Manages toolbar visibility	status information. **Task Panel**: Toggles the Task Panel. This enlarges the Tabs display for easier operation. **Show Details Tab:** Toggles the Details tab for each active backup or restore operation.
Tools	Accesses Recovery Environment tools.	**Network Configuration**: Launches the Network Configuration utility. This utility configures the computer's network access settings. **HIR Configuration:** Launches the Hardware Independent Restore (HIR) utility. This utility restores a backup image to a different environment from which the image was created. **Load Drivers:** Opens the Load Drivers dialog. This dialog configures storage drivers for use in Recovery Environment. **File Browser:** A simple file browser, similar to Windows Explorer, for viewing files and folders in a backup image file. **Text Editor:** A simple text editor similar to Notepad. **Boot Configuration Utility**: Launches the Boot Configuration Utility. This utility manages the boot configuration repair process for those situations where the automated process does not work. **Partition Table Editor**: A simple MBR partition table editor. NOTE: Use only at the request of StorageCraft Support. **UltraVNC Service:** Launches the Remote Management utility. This utility configures remote access to systems running Recovery Environment. **Select Your Time Zone**: Launches the Time Zone utility. This utility selects the system's time zone. **Display Settings**: Opens the Display Settings dialog. This dialog configures the resolution and color mode for the Recovery Environment UI. **Keyboard Settings**: Opens the Keyboard Settings dialog. This dialog selects and then test international keyboard layouts. **iSCSI**: Opens the iSCSI Initiator utility. Refer to these two articles for details on using this Microsoft utility: Initiator Overview and iSCSI Initiator User's Guide. **Enable Logging**: Opens the Log Destination dialog. This dialog specifies the location for ShadowProtect log files. This also activates the Recovery Environment's logging. **Refresh Volumes Info**: Interrogates the operating system to refresh the Volume List information. **Disk Partitioning:** Launches the Windows DiskParrt utility to view and configure partitions on a hard drive. **Command Shell:** Launches a command prompt.
Help	Displays general Recovery Environment information	**About:** Displays the Recovery Environment version and copyright information.

5.2 Task Panel

The ShadowProtect Task panel on the left side of the dialog provides navigation to Recovery Environment tasks and tools. The panel is organized into menus and options:

Menu	Description	Options
Tasks	Access ShadowProtect wizards	**Backup Volume**: Launches the Backup Wizard. **Restore Volume:** Launches the Restore Wizard. **Explore Backup Image:** Launches the Explore Backup Image Wizard. **Dismount Backup Image:** Launches the Backup Image Dismount Wizard. **Verify Backup Image**: Launches the Verify Image Wizard. ***Additional IT Edition Options*** **Restore Volumes**: Launches a modified version of the Restore Wizard which allows for setting up two or more volumes for restoration. **Disk Copy**: Copies either volumes or entire disks in realtime without requiring a backup image file.

Tools	Access Recovery Environment tools	**Network Configuration**: Launches the Network Configuration utility. This utility configures the system's network access settings. **HIR Configuration**: Launches the Hardware Independent Restore (HIR) utility. This utility restores a backup image to a different environment from which it was created. **Load Drivers**: Opens the Load Drivers dialog, This dialog configures storage drivers for use in Recovery Environment. **File Browser**: Loads a simple file browser (similar to Windows Explorer) to locate and view files and folders while in the Recovery Environment. **Text Editor**: Loads a simple text editor for editing files or Registry entries. **Select Your Time Zone**: Displays the Time Zone selector. Use this to adjust the system's time zone. **Refresh Volumes Info:** Refreshes the Volume List in ShadowProtect. **Keyboard Settings**: Specifies which keyboard layout the system uses. It also provides a test window where entered text appears.
Info	Display system information	Provides a quick reference to the Computer Name, IP Address and Time Zone.
Status	Displays current ShadowProtect task status	**Queued Tasks:** Shows the number of queued tasks waiting to run. **Running Tasks:** Shows the number of tasks currently running.

5.3 Tabs

The Main dialog tabs provide access to Recovery Environment's primary features and application status. These tabs are:

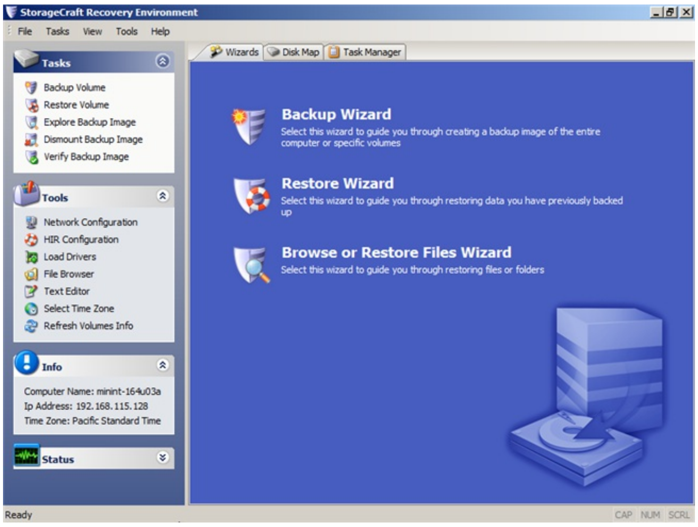
- Wizards
- Disk Map
- Task Manager
- Task Details (A tab which appears only when RE runs a task and you click **Show Details** in Task Manager.

Wizards

The Wizards tab links to three function wizards:

- Backup
- Restore
- Browse or Restore Files

These guide users through the most common Recovery Environment tasks:



Backup Wizard

Select this wizard to guide you through creating a backup image of the entire computer or specific volumes

Restore Wizard

Select this wizard to guide you through restoring data you have previously backed up

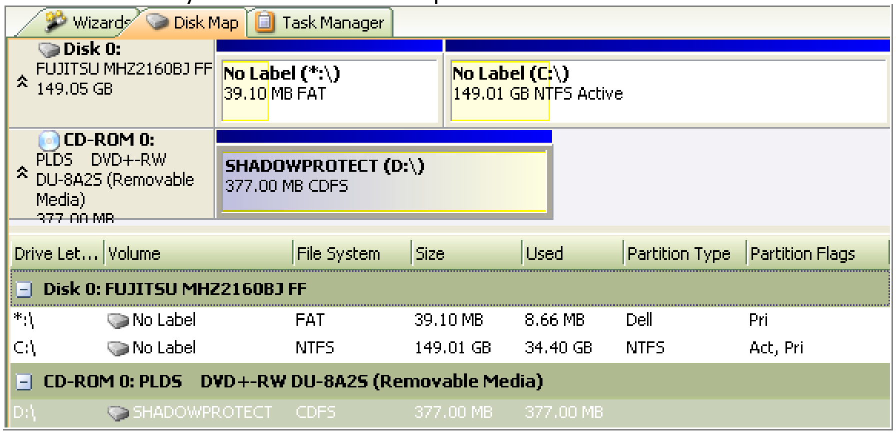
Browse or Restore Files Wizard

Select this wizard to guide you through restoring files or folders

Computer Name: minint-164u03a
Ip Address: 192.168.115.128
Time Zone: Pacific Standard Time

Disk Map

This tab displays a graphical view of the system drives and their partitions.



Drive Let...	Volume	File System	Size	Used	Partition Type	Partition Flags
⊟ Disk 0: FUJITSU MHZ2160BJ FF						
*:\	No Label	FAT	39.10 MB	8.66 MB	Dell	Pri
C:\	No Label	NTFS	149.01 GB	34.40 GB	NTFS	Act, Pri
⊟ CD-ROM 0: PLDS DVD+-RW DU-8A2S (Removable Media)						
D:\	SHADOWPROTECT	CDFS	377.00 MB	377.00 MB		

Use Disk Map to:

- View drive and partition information
- Select a drive or partition to run the Backup or Restore Wizards
- Edit drive parameters. (See Disk Map Options and Partition Restoration Scenarios for details.)
- Run Chkdsk
- Format a drive
- Edit partitions
- Edit the selected disk's parameters of `boot.ini`

Disk Map Options

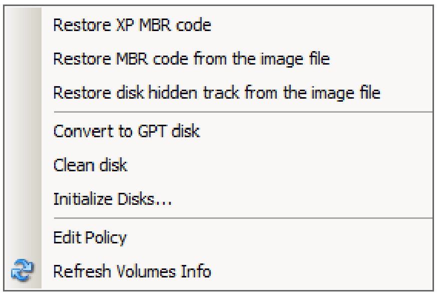
Recovery Environment's Disk Map tab offers four right-click menus depending on which item you select:

- **Disk**: Listed in a column at the left of the tab.
- **Primary Partition:** Each of its primary partitions appears to the right of the disk and is indicated with a blue bar.
- **Extended Partition:** Each extended partition of the disk is indicated with a green outline.
- **Unallocated Space:** This space is indicated with a grey bar.

A new disk begins with all its space as "unallocated". Once you create a partition from the unallocated space, Disk Map labels the unformatted partition with the name "unknown" and the partition type "unrecognized". Format the partition as NTFS or FAT32 and Disk Map includes that text onscreen and changes the grey bar indicator to blue.

Disk

This right-click menu runs these actions on the selected disk:



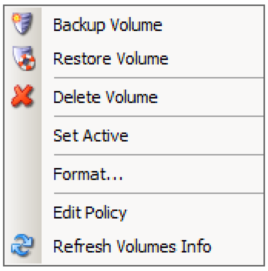
These options include:

Restore XP MBR Code	Recreates the required MBR code needed for a Windows XP system disk. **Note:** Windows Vista and newer OSes do not use this.
Restore MBR code from the image file	Extracts and restores the required MBR info from the backup image file.

Restore disk hidden track from the image file	Restores the hidden track some PC vendors include on their system disks.
Convert to GPT disk	Erases the selected disk's current contents--data and partitions--and lays down the GPT format on the disk.
Clean disk	Erases the selected disk's partitions. Essentially, a reformat of the drive. Use the *Initialize Disks...* option to complete the reformat and partitioning of the drive.
Initialize Disks...	Prepares one or more selected disks for partitioning as either MBR or GPT disks. ⚠ **Warning!** Initializing removes all existing partitions and data from the disks.
Edit Policy	Opens the Partition Creation Policy Editor.
Refresh Volumes Info	Queries the OS and updates the volume information.

Primary Partition

This menu runs these actions on the selected partition:

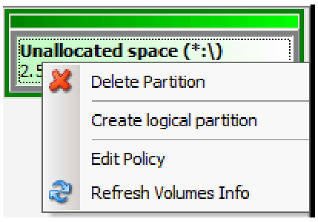


These options include:

Backup Volume	Launches the Backup Wizard (see Create a Backup Image).
Restore Volume	Launches the Restore Wizard (see Restoring a Volume).
Delete Volume	Deletes the selected volume.
Set Active	Makes the selected volume the system's boot volume.
Format...	Opens the Format Volume dialog.
Edit Policy	Opens the Partition Creation Policy Editor.
Refresh Volumes Info	Queries the OS and updates the volume information.

Extended Partition

Disk Map outlines a newly created extended partition in green while retaining the "unallocated space" label. You must create one or more logical partitions within this extended partition. Right-click on the extended partition to display this menu:

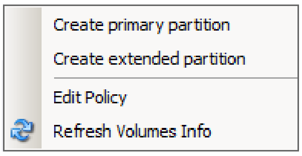


This menu performs these actions on the extended partition:

Delete Partition	Deletes the extended partition. **Warning:** This deletes all data from every logical partition on the extended partition.
Create logical partition	Opens the Create Partition editor. You can create an unlimited number of logical partitions with NTFS. FAT32 limits logical partitions to 23. **Note:** A logical partition cannot be a boot partition.
Edit Policy	Opens the Partition Creation Policy Editor.

Refresh Volumes Info	Queries the OS and updates the volume information.

Unallocated Space



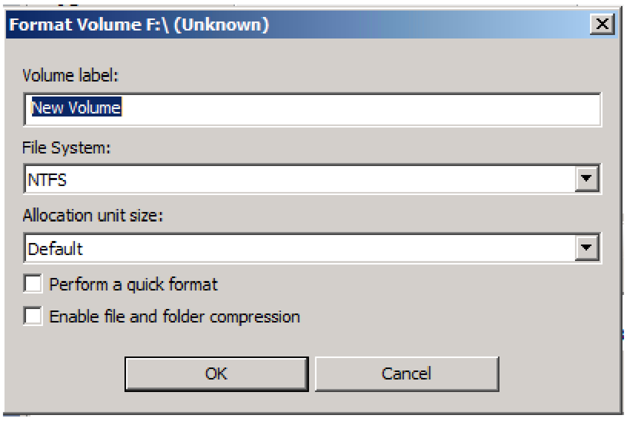
Create primary partition
Create extended partition
Edit Policy
Refresh Volumes Info

This menu performs these actions on unallocated space:

Create primary partition	Opens the Create Partition editor.
Create extended partition	Opens the Create Partition editor. **Note:** The editor automatically inserts "Extended" as the Partition Type.
Edit Policy	Opens the Partition Creation Policy Editor.
Refresh Volumes Info	Queries the OS and updates the volume information.

Format Volume

The Format Volume dialog sets parameters for the new partition:



Format Volume F:\ (Unknown)

Volume label: New Volume

File System: NTFS

Allocation unit size: Default

□ Perform a quick format

□ Enable file and folder compression

OK Cancel

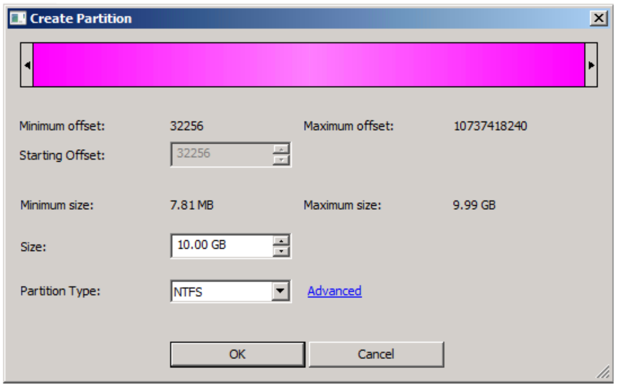
These options include:

Volume Label	A user-defined name. The syntax prohibits these characters in a volume name: \\ \ / [ ] : | < > + ; = . ? "
File System	Default is NTFS. The dropdown box offers FAT, FAT32, and NTFS. Unless restoring an older system volume, keep the NTFS setting.
Allocation Unit Size	The Default setting allows the drive to select its best block size: 512 (typical for MBR disks) or 4096 (4K) (typical for GPT drives). The dropdown box offers a range of settings from 512 to 64KB if needed.
Perform a quick format	Default is to do a standard format and not a quick one. A quick format, while fast, does not test the disk to identify bad sectors. A standard formatting process checks each sector to confirm data retention.
Enable file and folder compression	Default is to not use compression on the new volume. Checking this option lets the OS compress and decompress files in the volume automatically. However, since this uses processor resources, keep the default setting unless required to do so.

In a typical volume format, simply specify a useful name for the volume, keep the default settings, and click **OK**.

Create Partition Editor

The Create Partition Editor modifies the size, offset, and type of the volume to create:



Minimum offset: 32256

Maximum offset: 10737418240

Starting Offset: 32256

Minimum size: 7.81 MB

Maximum size: 9.99 GB

Size: 10.00 GB

Partition Type: NTFS

These options include:

Size Slider Graphically sets the size and offset for the new partition. Click and drag the arrows at either end of the graphic to shrink or increase the partition to the desired size. The editor updates the numeric value in the Size indicator to show the specific dimension selected with the slider.

Minimum Offset This displays the minimum offset for the start of the new partition. If this is the first partition on a disk, the editor bases this offset on the policy set using the Partition Creation Policy Edtior. If the new partition is the second or later on the disk, the offset is the start of the nearest sector in ShadowProtect 5.0.2 and newer or the nearest track in ShadowProtect 5.0.1 and older.

Maximum Offset This displays the maximum offset based on the size of the unallocated space available for this partition. Typically this is the end of the last available sector of the unallocated space.

Starting Offset Selects the starting byte of the new partition.

Minimum Size Size limit set by the OS version and calculated by the policy editor's selection for *Track* or *Sector* as the boundary for partitions.

Maximum Size Size limit of the unallocated space for the partition.

Size Selector for the overall size of the partition. This defaults to the total available unallocated space.

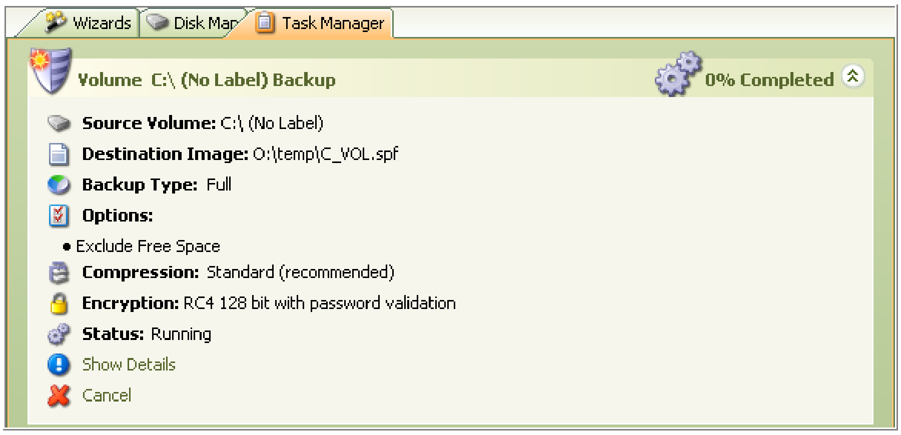
Partition Type Selects NTFS, FAT or FAT32.

Advanced **Note:** This displays a list of partition types available through WindowsPE. However, ShadowProtect only supports the three types available in the *Partition Type* selector.

Task Manager

This tab displays a list of running or completed tasks (such as a backup or verification). To view details of a task, click **Show Details** in that task's section. To abort an active task, click **Cancel**.

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



Volume C:\ (No Label) Backup

0% Completed

Source Volume: C:\ (No Label)

Destination Image: O:\temp\C_VOL.spf

Backup Type: Full

Options:

- Exclude Free Space

Compression: Standard (recommended)

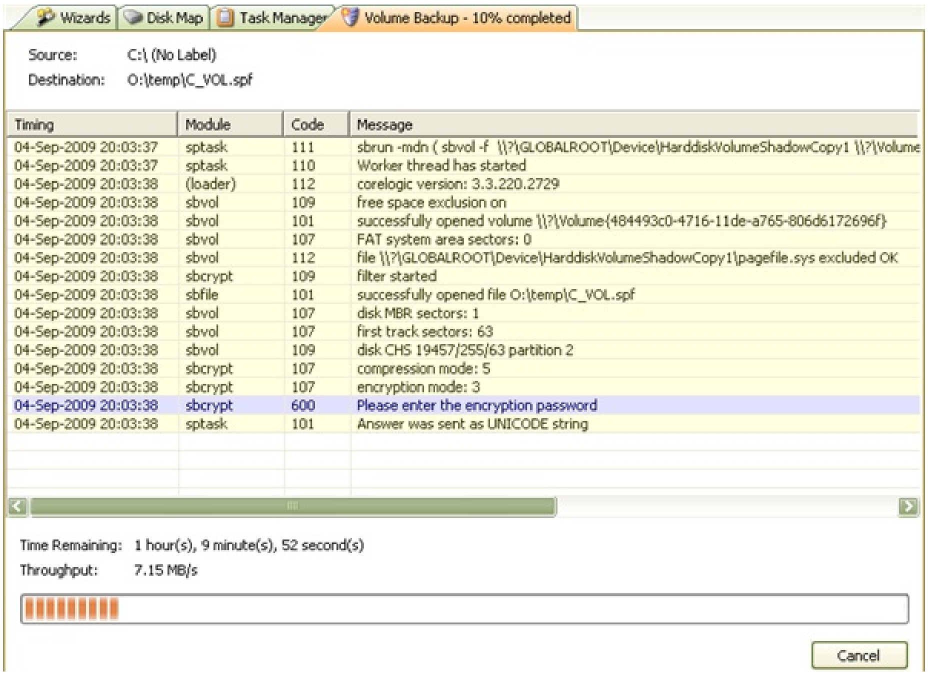
Encryption: RC4 128 bit with password validation

Status: Running

Task Details

Note: This tab only appears after clicking **Show Details** of a task in the Task Manager tab.

The Task Details tab shows status information about a currently running or completed task. (These tasks include a volume backup, volume restore, or verify image.) You can control the display of these tasks by clicking **Show Details / Hide Details** in the Task Manager tab. For example:



Source: C:\ (No Label)
Destination: O:\temp\C_VOL.spf

Timing	Module	Code	Message
04-Sep-2009 20:03:37	sptask	111	sbrun -mdn (sbvol -f \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1 \\?\Volume
04-Sep-2009 20:03:37	sptask	110	Worker thread has started
04-Sep-2009 20:03:38	(loader)	112	corelogic version: 3.3.220.2729
04-Sep-2009 20:03:38	sbvol	109	free space exclusion on
04-Sep-2009 20:03:38	sbvol	101	successfully opened volume \\?\Volume{484493c0-4716-11de-a765-806d6172696f}
04-Sep-2009 20:03:38	sbvol	107	FAT system area sectors: 0
04-Sep-2009 20:03:38	sbvol	112	file \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\pagefile.sys excluded OK
04-Sep-2009 20:03:38	sbcrypt	109	filter started
04-Sep-2009 20:03:38	sbfile	101	successfully opened file O:\temp\C_VOL.spf
04-Sep-2009 20:03:38	sbvol	107	disk MBR sectors: 1
04-Sep-2009 20:03:38	sbvol	107	first track sectors: 63
04-Sep-2009 20:03:38	sbvol	109	disk CHS 19457/255/63 partition 2
04-Sep-2009 20:03:38	sbcrypt	107	compression mode: 5
04-Sep-2009 20:03:38	sbcrypt	107	encryption mode: 3
04-Sep-2009 20:03:38	sbcrypt	600	Please enter the encryption password
04-Sep-2009 20:03:38	sptask	101	Answer was sent as UNICODE string

Time Remaining: 1 hour(s), 9 minute(s), 52 second(s)
Throughput: 7.15 MB/s

Recovery Environment displays a new tab for each selected task when you click **Show Details**.

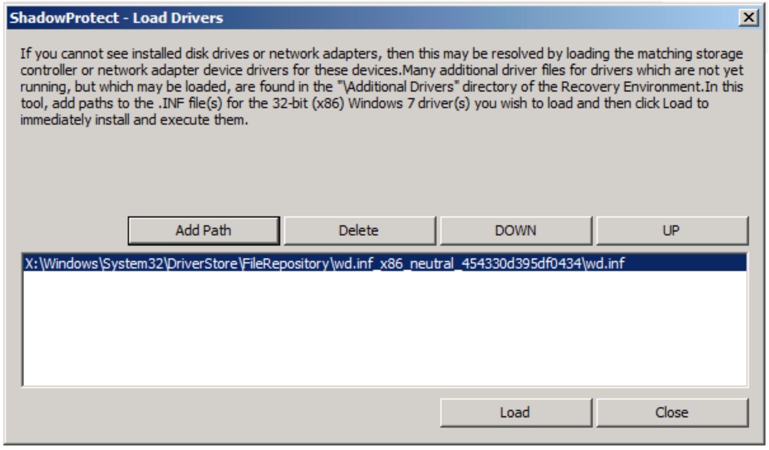
6 Loading Drivers

Recovery Environment lets you dynamically load storage or network drivers so Recovery Environment can access different hardware.

Note: Only Recovery Environment uses these drivers, *not* the restored system volume. When using the 32-bit version of Recovery Environment, these drivers must also be 32-bit. Before loading a driver, verify that the new driver files are actually 32-bit, as some hardware vendors do not clearly distinguish 32-bit versions from 64-bit.

To dynamically load a driver

1. Click **Load Drivers** in the Recovery Environment Tools menu. The *Load Drivers* dialog appears:



If you cannot see installed disk drives or network adapters, then this may be resolved by loading the matching storage controller or network adapter device drivers for these devices.Many additional driver files for drivers which are not yet running, but which may be loaded, are found in the "\Additional Drivers" directory of the Recovery Environment.In this tool, add paths to the .INF file(s) for the 32-bit (x86) Windows 7 driver(s) you wish to load and then click Load to immediately install and execute them.

X:\Windows\System32\DriverStore\FileRepository\wd.inf_x86_neutral_454330d395df0434\wd.inf

2. Click **Add Path** to browse to the INF file you need. Repeat this Add Path process to add all needed INF files.

Click-and-drag the drivers to move them up or down the list in order to establish priority.

3. Click **Load** to immediately load all the listed drivers.

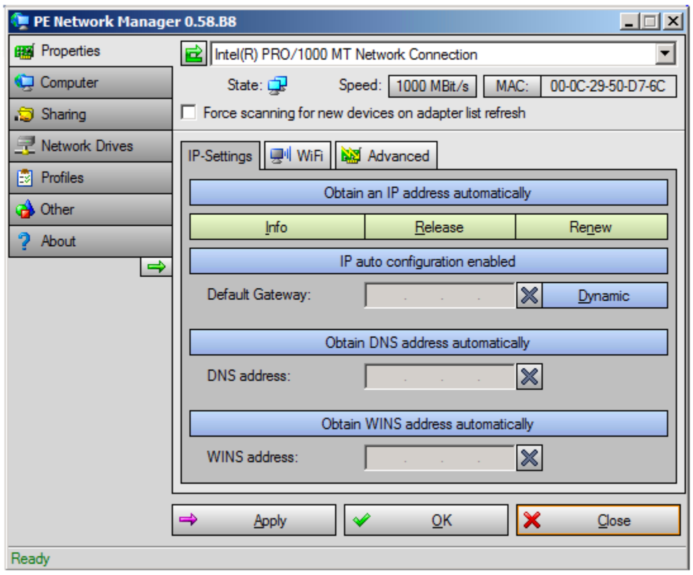
Recovery Environment then provides access to the device(s) or network(s).

Important: The Recovery Environment - Windows (REWIND) created by REBuilder does not currently support iSCSI.

7 Using the Network Configuration Utility

The Network Configuration Utility (NCU) configures a system's Network Interface Card (NIC), TCP/IP settings, and domain information for use in Recovery Environment.

Note: The PE Network Manager provides a comprehensive set of network options. However, most Recovery Environment scenarios work with the default settings.



Intel(R) PRO/1000 MT Network Connection

State: Speed: 1000 MBit/s MAC: 00-0C-29-50-D7-6C

☐ Force scanning for new devices on adapter list refresh

Obtain an IP address automatically

IP auto configuration enabled

Default Gateway:

Obtain DNS address automatically

DNS address:

Obtain WINS address automatically

WINS address:

Ready

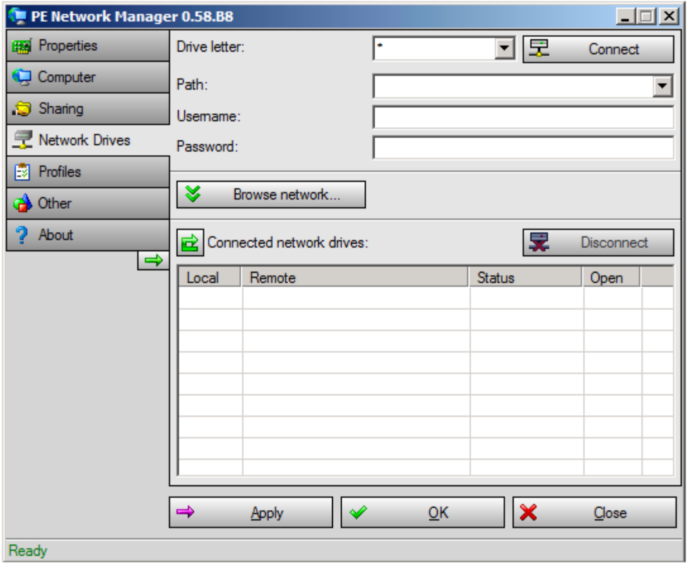
To specify NIC settings

1. Click **Network Configuration** in the Tools menu to open the utility.
2. Select the appropriate Ethernet adapter from the dropdown list.
   If necessary, select the adapter's preferred link speed and specify its MAC address.
3. Modify the adapter settings in the NCU interface. Available settings include:
   IP Settings: The top button in this dialog toggles between:
   Obtain an IP address automatically: Obtains the settings after clicking **OK** or **Apply**.
   Use static IP address: Specify IP address, Subnet mask, and Default gateway. Click the *More* [...] button to specify multiple IP addresses and gateways, if necessary.
   DNS and WINS Settings: These buttons toggle between Dynamic or Static configurations. Click the *More* [...] button to specify two or more IP addresses for the DNS or WINS environment.
   Network Identification: Click **Computer** to specify a computer name, Workgroup, and Primary DNS suffix. Click **Set** to accept the configuration.

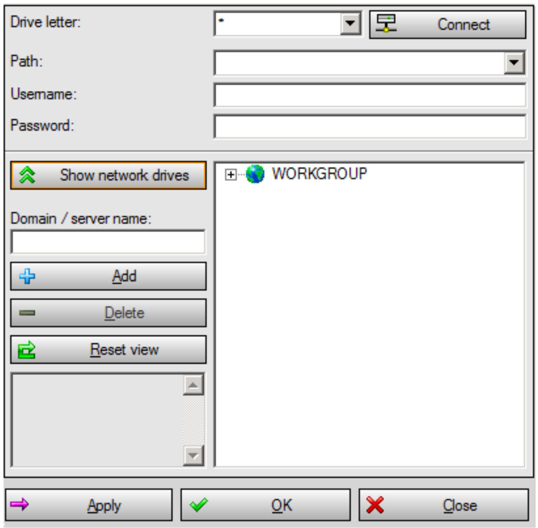
Note: Although PE Network Manager supports WiFi configuration, StorageCraft recommends a wired connection when using the network resource as either a source or target for backup image files.

To specify drive mappings and sharing

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



2. Use the Drive Letter dropdown to select a letter.
3. Click **Browse network** to locate online devices:



a. Enter a name in the Domain/server name 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 the Expand button to view all available resources in the specified Domain or Computer.
c. Select a resource to automatically populate the **Path** field.
d. (Optional) Click **Delete** to remove all network resources from the selected domain or server in the Resources pane.

4. Enter the credentials needed to access the network resource.
5. Click **Connect**. Recovery Environment connects to the drive and maps it.

Additional NCU Options

The NCU includes various additional options which currently are not supported by StorageCraft. Refer to the PENetwork site for further information on these options.

8 Creating a Backup Image File

The Recovery Environment Backup Wizard creates a backup of an entire system or of a specific volume on that system. Unlike the installed version of ShadowProtect, the Recovery Environment creates only cold backups (a backup taken when the system is booted from the Recovery Environment). For further details on creating backups, refer to the ShadowProtect User Guide.

To create a backup image file

1. Open the Backup Wizard:

- In the Wizards tab, click **Backup Wizard.**
- In the Tasks menu, click **Backup Volume.**

2. In the *Volumes to Back Up* page, select the volume(s) to backup. Click **Next.**
   Note: To backup the entire system, select all volumes. However, it is not necessary to backup the Recovery or Hidden Volumes (if they exist).
3. In the *Backup Type* page, select the type of backup to perform:
   Perform a Full Backup: Creates a full backup image file for the selected volume(s).
   Perform a Differential Backup: Creates a backup of all volume changes since the last full backup.
   Note: Recovery Environment needs access to the last full backup to perform the differential.
4. Click **Next.**
5. In the *Backup Name and Destination* page, specify where to store the backup image file:
   a. On a local or network directory or on an optical storage medium (CD/DVD/Blu-ray).
   b. Browse to, or enter, the path to the location. (See Image File Destinations for details.)
   Warning: This destination path cannot be longer than 186 characters or contain any special characters including:

   ` ! @ # $ % ^ & * ( ) | \/ ? > < , { } [ ]

   c. (Optional) Right-click a file name, then click **Rename** to change the name of the backup image file. This renaming is useful to distinguish this particular backup from others that may have been taken of the volume(s) using ShadowProtect.

6. Click **Next.**
7. In the Options page, select compression type, password, or file splitting as needed. Enter a text message in the Backup Comment field to describe this backup if desired.
   Note: Click **Advanced** to display the *Advanced Options* settings. Keep the default settings unless specifically required to.
8. Click **Next** to continue. The Wizard displays a summary of the options for this backup.
   Note: The **Execute Now** option is not needed to run the backup immediately. All backups run from the Recovery Environment occur immediately.
9. Click **Finish** to create the backup image file.
   You can monitor the progress of the backup in the Task Manager tab by clicking **Details**.

Using a Windows Dedup Volume as a Destination

ShadowProtect supports writing backup image files to a Windows Dedup-enabled volume. However, since ShadowProtect compresses image files, Windows Dedup does not yield significant space savings. Also, if any of the dependent backup files in the backup chain are deduped, ShadowProtect cannot:

- Mount the backup file
- Run a VirtualBoot on the backup file.

System Reserve and other Volumes

Hardware vendors may configure their hard drives to include additional partitions:

- *Diagnostic Partition*: Usually a 100MB or less partition, this would include one or more tools specific to that hardware platform. This partition will have no drive letter assigned to it.
- *Recovery Partition*: This stores data existing on the boot partition prior to installing the Operating System.The Recovery Partition is used to restore the system back to factory default status. This partition will have no drive letter assigned to it.
- *System Reserve Volume*: This may include boot information and is of particular value only when using BitLocker.

A ShadowProtect restore typically does not require a backup of any of these volumes. Instead ShadowProtect:

- Recreates the boot information from the System Reserve volume during a restore..
- Does not need the factory content from the Recovery Partition since a typical restore occurs on a new, different vendor-supplied drive.
- Does not need additional hardware-specific diagnostic tools as again a typical restore is to new, different hardware.

However, user-preference may warrant preserving these volumes with additional one-time full backups.

The only exception is in the case of a system which uses Windows BitLocker to encrypt a partition. If a user uses the Recovery Environment to create a full cold backup of the encrypted partition, a one-time full backup of the System Reserve volume is required. This one-time backup preserves the Bitlocker data needed to decrypt the partition.

GPT Disk Volumes

GPT disks also include additional volumes:

- the EFI System partition (ESP)
- the Microsoft Reserved Partition (MSR)

Neither of these require a backup, as ShadowProtect automatically restores the required partitions during recovery. (In fact, the MSR contains no file system to back up.)

8.1 Image File Destinations

Recovery Environment can store backup image files on any disk device, including hard drives, removeable USB/FireWire drives, network drives and NAS (Network Attached Storage) devices. You can also store backup images to optical media such as CDs, DVDs, or Blu-Ray discs if the system has an writeable optical drive.

⚠ **Note:**If you select a destination that does not have enough disk space to save the backup image, the backup job fails.

Location	Advantages	Disadvantages
Local Hard Drive	• Fast backup and restore. • Inexpensive.	• Consumes local disk space. • Vulnerable to loss if the drive fails.
Local USB/FireWire Drive	• Fast backup and restore. • Preserves disk space on local drives. • Inexpensive. • Easy off-site storage.	• More expensive than local hard drives. • Vulnerable to loss if the drive fails.
Network Hard Drive	• Fast backup and restore. • Protection from local hard drive failure. • Off-site storage.	• Must have network interface card drivers supported by Recovery Environment. • Complexity. Users must have network rights to save and access backup images.
CD/DVD/Blu-Ray	• Good media for archiving. • Protection from local hard drive failure.	• Slower backups due to media speeds. • File restrictions due to limited size.

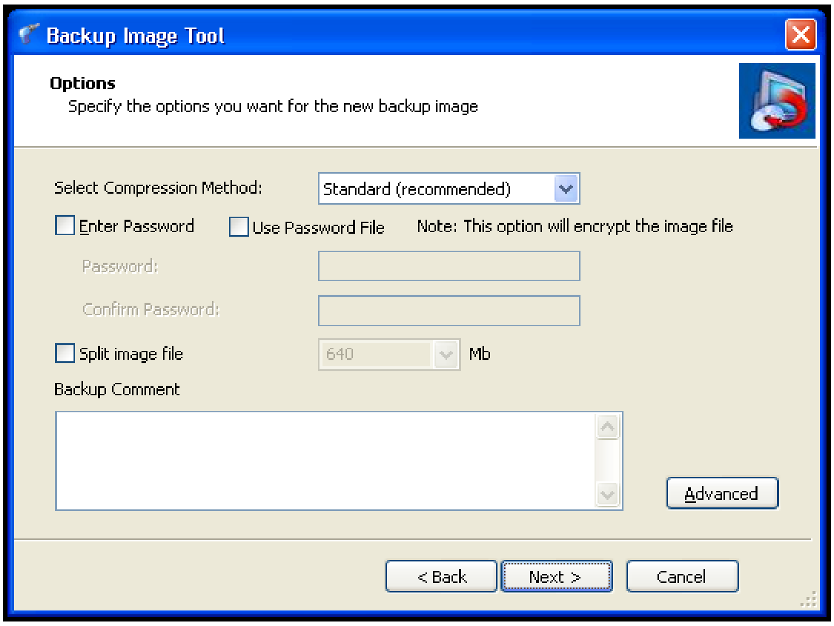
Using a Windows Dedup Volume as a Destination

ShadowProtect supports writing backup image files to a Windows Dedup-enabled volume. However, since ShadowProtect compresses image files, Windows Dedup does not yield significant space savings. Also, if any of the dependent backup files in the backup chain are deduped, ShadowProtect cannot:

- Mount the backup file
- Run a VirtualBoot on the backup file.

8.2 Options

The Backup Wizard's *Options* dialog controls compression, security, and file splitting:



Backup Image Tool

Options
Specify the options you want for the new backup image

Select Compression Method: Standard (recommended)

□ Enter Password □ Use Password File Note: This option will encrypt the image file

Password:

Confirm Password:

□ Split image file 640 Mb

Backup Comment

This section decribes these options:

- File Compression
- Backup File Encryption
- Splitting Backup Image Files
- Backup Comments
- Advanced Options

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. Most contemporary systems can support this level of compression.

Backup File Encryption

ShadowProtect can 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 as StorageCraft cannot bypass the encryption on a backup image files without the password.

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 highest level of backup image file security:

- At least eight characters in length

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

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

Splitting Backup Image Files

Recovery Environment can split backup image files into multiple smaller files, if needed. This splitting allows the program to save large backup files on fixed-length media such as CD, DVD. or Blu-Ray.

You can split backup image files:

- During creation by selecting this option.
- After creation with the Image Conversion tool.

To split a file during creation:

1. Check the *Split Image File* box in the Backup Wizard's *Options* dialog.
2. Specify a size for each of the smaller files (such as 700MB for CD-R discs or 4480MB on DVD-R).
3. Run the backup job.
4. Insert CD or DVD recordable discs as required during the backup.

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

Backup Comments

Use the Backup Comments field to enter any needed text to describe the backup job. ShadowProtect displays these comments when mounting or restoring the backup image file. By default, Recovery Environment adds the time and date stamp as backup comments on all backup files.

Advanced Options

⚠ **Note:** StorageCraft recommends keeping all advanced options at their default settings unless you fully understand the impact of changing these options.

View the advanced backup image file options by clicking **Advanced** in the Backup Image Options page. These options are:

Lock Source Volume

⚠ **Note:** Since the Recovery Environment performs only cold backups, locking the source volume is not relevant. Either setting performs a complete backup.

Default: **On**

On: Instructs Recovery Environment to lock access during the backup of the volume.

Off: Instructs Recovery Environment to use VSS snapshot technology to backup the volume.

Include Free Space

Default: **Off**

On: Backs up all sectors on the volume, including all free space. This creates a larger backup file.

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

IO Throttle

Default: **100**

Specifies the percentage of the system's I/O subsystem that Recovery Environment uses to perform the backup. In most cases, this setting should remain at the default. To change this value, click and drag the slider control to the desired setting.

Enable Write Caching

Default: **Off**

On: Recovery Environment uses caching when writing the backup image file. Caching might slow down the imaging process.

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

9 Restoring a System Volume

The primary purpose of Recovery Environment is to restore a system volume. The Recovery Environment's Restore Wizard supports two types of restore for a system or boot volume:

One Step Restore	This method restores a system volume from a selected backup image file in a single operation. **Note:** Use the Recovery Environment for Windows to restore from a VHD/VHDX formatted image file. The Recorvery Environment CrossPlatform only supports restores from .SPF and .SPI image files, not from VHD or VHDX format files.
HeadStart Restore	The HeadStart Restore (HSR) operation in Recovery Environment breaks up the volume restore process into multiple stages. Doing this is useful when restoring a large volume--a process that can take days.

Note: While similar to the ImageManager HSR, HeadStart Restore in Recovery Environment is a *manual* process. ImageManager's HSR is automated; the Recovery Environment version requires a reboot, using the Backup and then the Restore Wizards to capture and apply the latest changes to the backed up volume prior to finalizing it. The Recovery Environment version of HSR however does not require a license.

Supported Sector Sizes

Contemporary hard drives and SSDs ship with a 4096-byte *physical* sector size. Most support the 512-byte *logical* sector size. (These often are labeled 512e for "512 Byte Sector Size Emulation".) ShadowProtect supports both 4096- and 512-byte sector sizes.

In the unusual situation of restoring a partition/volume from one sector size to another:

- 512 bytes per sector -> 4096 bytes per sector
- 4096 bytes per sector -> 512 bytes per sector

ShadowProtect will issue an error message during the restore if it encounters a mis-matched sector size. To avoid this, reformat the destination drive to have a logical sector size that matches the source volume.

Restoring Windows 8.x System/Boot Volumes with UEFI Secure Boot

Many computers now support Secure Boot, an anti-malware feature available in UEFI . Secure Boot ensures that a system only boots from a safe operating system. However, many safe OSes don't support Secure Boot. Currently, the only Windows operating systems that support Secure Boot are:

- Windows 8.1
- Windows Server 2012 R2
- Windows 8
- Windows Server 2012

Earlier OSes, including Windows 7, Vista, and Windows XP do not support Secure Boot (and therefore do not require enabling Secure Boot).

In addition, there are many other safe OSes and boot environments that do not support Secure Boot. This includes the ShadowProtect Recovery Environment for Windows and Recovery Environment CrossPlatform.

ShadowProtect Recovery Environment for Windows, however, can only be booted on a computer with UEFI when:

- The UEFI either does not support Secure Boot or if Secure Boot is not enabled.

- The UEFI is booted into BIOS Compatibility Mode. (This mode is often referred to as CMS.)

The ShadowProtect CrossPlatform environment *does* support booting in native UEFI mode (with Secure Boot in disabled mode) rather than BIOS Compatibility Mode (CMS). It will not boot, however, when Secure Boot is enabled.

To allow either Recovery Environment to boot, temporarily disable the Secure Boot feature. To do so:

1. Boot the system into the UEFI management screen.
2. If Secure Boot is an option AND enabled, temporarily disable this feature. (Some systems refer to this as UEFI Boot. Verify the option in the system's documentation.)
3. Change the Boot order so that the CD or DVD is the first boot item.
4. If booting the ShadowProtect CrossPlatform Recovery Environment, simply reboot the system to start the CrossPlatform environment.
5. If booting the ShadowProtect Recovery Environment for Windows, verify that the option to boot into BIOS Compatibility Mode (sometimes referred to as CMS) is enabled.
   Note: Some UEFI systems list the same CD or DVD in two ways--one with a "UEFI:" prefix and one without. On these systems, to boot using BIOS Compatibility Mode, select the CD or DVD entry that does NOT have this prefix.
6. Proceed to perform the volume restore.
7. After performing the restore, boot into the UEFI screen again and re-enable Secure Boot (if required).
8. Continue with booting the restored system.

9.1 Restore a Volume in One Operation

When migrating or restoring a system volume to new hardware or to a virtual machine, the volume will likely need new drivers. The Recovery Environment for Windows includes Hardware Independent Restore technology to ensure these new drivers get installed so the new system volume can boot. The Recovery Environment allows HIR to run in the following situations. (Note that in all other cases, REWIND users must have a valid activation code to use HIR)

- ShadowProtect is installed *and* activated in the selected image file.
- ShadowProtect is installed *and* activated but is expired.
- ShadowProtect MSP is installed and activated, and its license is still within the subscription period.

Confirm that the restore meets one of these requirements in order for the volume to boot.

To use the restore feature:

1. Attach a disk with at least as much space as the original drive.
2. (Optional) If the disk is not initialized and you want to add a new MBR partition, you will need to reboot the Recovery Environment to continue the restore. Windows cannot accurately read and refresh the new MBR partition information for this newly initialized drive until after the reboot.
3. Select the *Disk Map* tab to create a partition on the new drive.
4. Select *Create Primary Partition*. The default setting is to use all the available space on the new drive for the new partition. Modify this setting as required for the System partition restore. Click **OK**. The Recovery Environment creates a new primary partition.
5. In Recovery Environment, select one of these:
   - **Tasks** > **Restore Volume**.
   - **Restore Volume** in the left-side Navigation panel.
   - **Restore Wizard** in the Wizards tab.

   The program launches the Restore Wizard. Follow the wizard prompts to complete the restore.

6. On the *Restore Type* page, select *Restore* from the list of types:

Restore	Restores a system volume in one operation or begins an HSR operation. **Note:** NETGEAR ReadyDATA systems do not support HSR operations.
Resume aborted restore	Restarts an earlier cancelled restore.
Restore subsequent incrementals	Adds incremental files to an existing HSR system volume backup. **Note:** This typically requires the source system to have run ShadowProtect earlier to create these incremental backup files. However, it is possible to use Recovery Environment to perform a differential backup to create one or more incrementals.
Finalize an HSR restore	Completes a restore that you chose to finalize later on. The system volume is then ready to boot.

7. Select the backup image to restore. (Use the *Files of type* dropdown box to select either ShadowProtect files or Microsoft

Virtual Hard Disk File (VHDX).)
⚠ **Caution:** On split files, have all the related split files in one folder. Select the initial .SPI file, not the file with the .001 extension. If the split files reside on optical disc, RE will ask to change discs as need to complete the restore.
⚠ **Note:** On NETGEAR ReadyDATA systems, this dialog shows the unallocated space of the volume that is often in the terbyte range (such as 63.77 TB). As the volume is stored on a thin-provisioned drive, this upper limit for the volume allows the NETGEAR device to store any sized backup while only consuming the actual space necessary for the backup file.

8. Select the destination for the restore.
   Note: The drive letters shown in the dialog reflect Recovery Environment assignments. They may or may not match what Windows assigned as the original drive letters. To view these two drive mappings and determine which to use as a source for the backup image:
   a) Run the Boot Configuration Utility.
   b) Select a volume
   c) Click **Drive Letter**. The utility lists both the Windows and the Recovery Environment drive letter assignments for the partition.
9. (Optional) If the target destination drive lacks partitions, refer to Recreate Original Partitions to lay down partitions that match the orginal or Restore Destination Options to create a new layout.
10. On the *Backup Image Dependencies* page, choose to:
    - Keep the selected backup image file.
    - Choose another point in time to restore.

    Note: The left pane displays all backup image files in the previously selected image set. Properties of the selected backup image file appear in the right pane.

11. On the *Finalization Options* page, select *Finalize the volume at the end of this restore* from the list:

Finalize the volume at the end of this restore	Select this option to perform a Standard restore operation, where the restored volume is ready for use after the restore operation completes. ⚠ **Note:** Do *not* select this option if you want to perform a HeadStart Restore operation.
Generate a .HSR file to use in a future finalization	⚠ **Note:** Select this option only for an HSR operation. (Optional) When you select this option, the Restore Wizard begins an HSR volume at the location you specify.

12. (Conditional) On the *Specify the Restoration Options* page, set any boot parameters you need to apply to the restored volume:
    Note: Recovery Environment only displays this page when finalizing an MBR boot volume, not for an HSR operation or for a GPT disk.

Set partition active	Configures the restored volume as the active boot partition.
Restore MBR	Restore the master boot record (MBR) as part of the volume restore job. 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. This utility configures the volume's drivers and properties to interact with the new or changed hardware after the restore.

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

The Restore Wizard completes the volume restore. Remove the Recovery Environment CD/DVD or USB key, then reboot the system to confirm the restore.

Note: After restoring a system volume, some OEM versions of Windows may not reactivate. Windows Activation may intentionally lock some OEM copies of Windows to specific machines. Some OEM licenses may, in fact, not reactivate except on the original machine. In these cases, consult with Microsoft on reactivation options.

Impact of Server Virtual Memory Size

The Windows default setting for server virtual memory size is RAM size. Consider this when restoring to a system with greater RAM than the original machine held, as the new system's virtual memory size will increase.

Restoring Domain Controllers

Network connectivity is essential when restoring a domain controller system. If the restored system uses new or different hardware, Windows may take significant time to reboot in order for each service to test the new environment. Refer to the Knowledge Base article on How to Restore to Dissimilar Hardware for details on domain controller restorations.

9.2 Resuming a Restore Operation

If you need to cancel a restore operation, the Restore Wizard lets you resume this operation later without having to start over.

To resume a restore operation

1. In Recovery Environment, select one of these:
   - **Tasks** > **Restore Volume**.
   - **Restore Volume** in the left-side Navigation panel.
   - **Restore Wizard** in the Wizards tab.

   Recovery Environment launches the Restore Wizard.

2. On the Restore Type page, select **Resume Aborted Restore**. Click **Next**.
3. On the Restore Destination page, select the volume where you previously started the restore operation, then click **Next.**
4. On the Backup Image to Restore page, browse to the backup image that you want to resume restoring, then click **Next.** **Note:** If you encrypted the backup image, you must specify the appropriate password to access it.
5. On the Finalization Options page, select *Finalize the volume at the end of this restore*.
6. (Conditional) On the Specify the Restoration Options page, set any MBR boot parameters you need to apply to the restored volume:

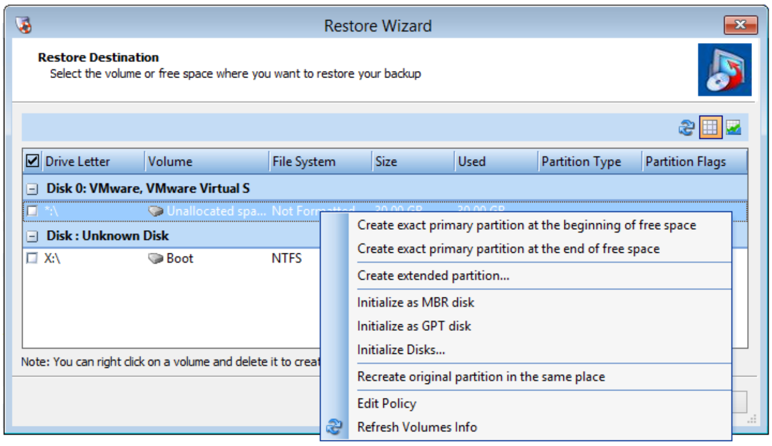
Set partition active	Configures the restored volume as the active partition the system boots from.
Restore MBR	Restores the volume's master boot record (MBR). When selected, you have the following MBR restore options: ◦ **Restore MBR from the image file**: Restores the MBR from the backup image file. ◦ **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. HIR configures drivers and properties of the restored volume to properly interact with the new or different hardware of the system.

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

Recovery Environment resumes the restore operation. Once the restore operation completes, remove the Recovery Environment CD/DVD or USB key and reboot the system to confirm the restored system volume. If necessary, use the Boot Configuration Utility to correct any issues so that the newly restored system volume is bootable.

9.3 Recreate Original Partitions

The Restore Wizard provides a number of options for partitions when you select an unitialized drive:



Restore Wizard

Restore Destination
Select the volume or free space where you want to restore your backup

☑ Drive Letter	Volume	File System	Size	Used	Partition Type	Partition Flags
⊟ Disk 0: VMware, VMware Virtual S						
☐ *:\	Unallocated spa...	Not For	20.00 GB	20.00 GB		
⊟ Disk : Unknown Disk						
☐ X:\	Boot	NTFS				

Note: You can right click on a volume and delete it to creat

Create exact primary partition at the beginning of free space
Create exact primary partition at the end of free space
Create extended partition...
Initialize as MBR disk
Initialize as GPT disk
Initialize Disks...
Recreate original partition in the same place
Edit Policy
Refresh Volumes Info

The Restore Destinations Option page covers each of these in detail. The option most often used is to match the original layout.

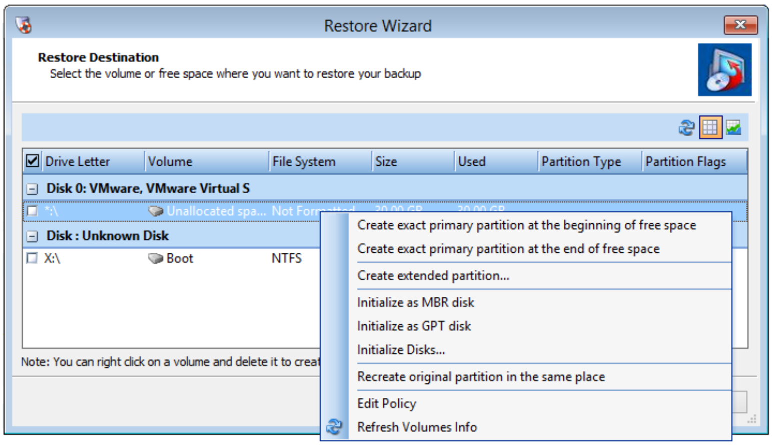
To create a partition layout that matches the original source volume:

1. Select *Clean disk* if needed to remove any existing partitions on the target destination drive.
   ⚠ **Warning:** This erases all data on those partitions.
2. Select *Recreate original partition in the same place* to duplicate the source volume on the destination drive.

Note: If you add a new MBR to an uninitialized drive, you will need to reboot the Recovery Environment to continue the restore. Windows cannot accurately read and refresh the new partition information for the destination drive until after this reboot.

9.4 Destination Partition Options

The Restore Wizard offers various partition options for a selected disk:



Restore Wizard

Restore Destination
Select the volume or free space where you want to restore your backup

☑ Drive Letter	Volume	File System	Size	Used	Partition Type	Partition Flags
⊟ Disk 0: VMware, VMware Virtual S						
☐ *:\	Unallocated spa...	Not For	20.00 GB	20.00 GB		
⊟ Disk : Unknown Disk						
☐ X:\	Boot	NTFS				

Note: You can right click on a volume and delete it to creat

Create exact primary partition at the beginning of free space
Create exact primary partition at the end of free space
Create extended partition...
Initialize as MBR disk
Initialize as GPT disk
Initialize Disks...
Recreate original partition in the same place
Edit Policy
Refresh Volumes Info

These options include:

Create exact primary partition at the beginning of free space	(Available only if unpartitioned disk space exists) Creates a new primary partition on the destination disk of the same size as the source partition. The Wizard creates it at the start of unallocated space. **Note:** You cannot create more than four (4) primary partitions on an MBR disk.
Create exact primary partition at the end of free space	Creates a primary partition of the same size as the source partition in the disk's unpartitioned, unallocated space. The Wizard places the end of the new partition at the end of the unpartitioned space, then moves backwards to create a volume of the exact size as the original.
Create extended partition	(Available only on MBR drives and only if unpartitioned disk space exists on the drive.) Creates a new extended partition on the destination drive. This partition can then be divided into one or more logical drives or partitions. This allows more than four partitions on an MBR drive.
Initialize as MBR disk	Displays a list of available drives. Select one or more disks to initialize as an MBR disk. (Recovery Environment requires at least one initialized disk to restore the system/boot volume.) See Starting Recovery Environment for details.

Initialize as GPT disk	Displays a list of available drives. Select one or more disks to initialize as a GPT disk. (Recovery Environment requires at least one initialized disk to restore the system/boot volume.) See Starting Recovery Environment for details.
Initialize Disks...	Displays a list of available drives. Select one or more disks to initialize as either MBR or GPT. (Recovery Environment requires at least one initialized disk to restore the system/boot volume.) See Starting Recovery Environment for details.
Recreate original partition in the same place	Creates a duplicate of a single partition at the same location as the original on the new drive.
Edit Policy	Runs the *Partition Creation Policy Editor* for changing partition alignment and offsets. For example, use the Editor for restoring a hard disk volume to an SSD for Windows system volumes prior to Vista.
Refresh Volumes Info	Asks the operating system for more current data on the drive volumes.

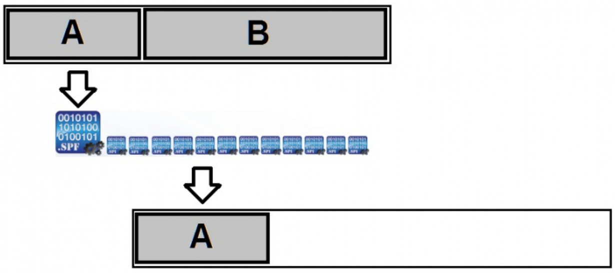
The Partition Restoration Scenarios section illustrates these different configurations.

Partition Restoration Scenarios

ShadowProtect Recovery Environment supports a wide variety of partition restoration scenarios to answer specific user needs.These cover both a single and multiple partitions:

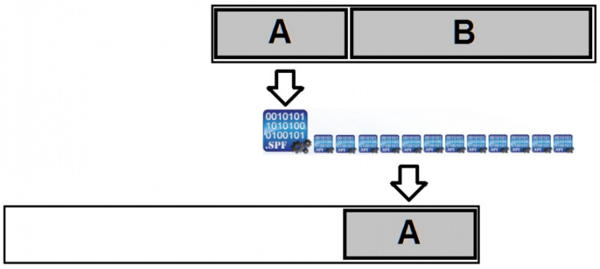
Single Partition

Beginning of Free Space



ShadowProtect uses the "A" source partition's backup image files to restore the original volume to the new drive. This new "A" partition is the same size as the original, and begins at the start of the available free space on the new destination drive.

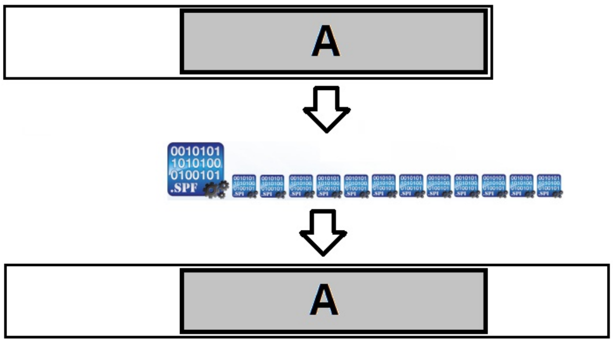
End of Free Space



ShadowProtect restores the original "A" volume to a same size partition on the new drive. This new "A" partition ends at the end of available free space on the destination drive.

Recreate the Original Partition

Select *Recreate original partition in the same place* to restore a volume to the same location as on the source drive.



ShadowProtect restores the original volume "A" to the same physical location on the new drive. Often this leaves free space after the partition on the new drive.

9.5 Partition Policy Editor

A restoration may require matching a partition's previous disk geometry onto the destination drive. The two common scenarios where partition alignment is important are restores to a:

1. SSD
2. RAID Virtual Drives or LUNs

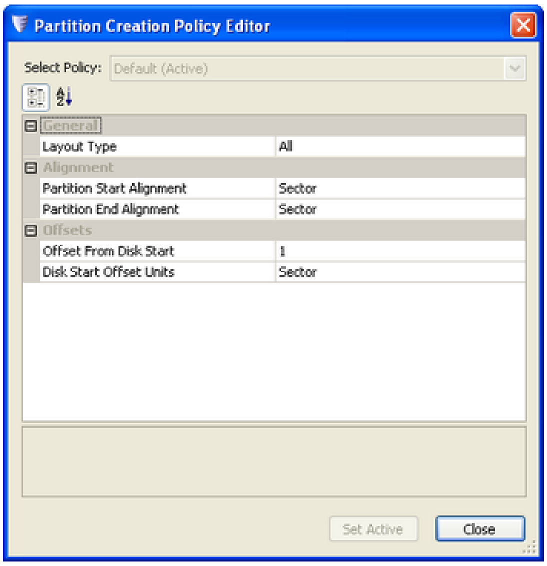
The first primary partition, for example, is normally located at a byte offset of 1,048,576 from the start of the disk. (For a 512byte/sector drive that would be LBA=2048.) When restoring a Windows XP boot partition to an SSD, this offset is not automatic. Without correct alignment and offset, read/write performance is significantly degraded on the SSD.

Note: Windows operating systems from Vista onwards use the correct offset by default for a System Reserved partition. This means that there's no need for any changes for restoration in those environments. Simply restore the partition back to its original location and the partition will be correctly aligned.

The Partition Creation Policy Editor lets you modify basic disk geometry settings used to create a new partition. The editor creates a policy (a template) which it saves for use with restoring to other drives.

NOTE: These policies only work on initialized drives (either MBR or GPT).

You can access the Policy Editor from the Disk Map tab. Right-click on a partition to display the action menu. Select *Edit Policy* to display the Policy Editor dialog:


Partition Creation Policy Editor

Select Policy: Default (Active)

General

Layout Type	All

Alignment

Partition Start Alignment	Sector
Partition End Alignment	Sector

Offsets

Offset From Disk Start	1
Disk Start Offset Units	Sector

To modify partition creation settings

1. Select the *Disk Map* tab.
2. Right-click on the desired partition, then select *Edit Policy*. The Partition Creation Policy Editor displays.
3. To modify a particular setting:
   A. Click in the appropriate field.
   B. Type in the desired value or select it from the drop-down list (if available).

Layout Type	Specifies which type(s) of drive formats this policy applies to. The choices include All, GPT, or MBR.
Partition Start Alignment (Default: Track)	Identifies the partition starting point, which typically occurs at a specific disk boundary. Supported options include: Cylinder, Track, and Sector.
Partition End Alignment (Default: Sector)	Identifies the boundary for the partition's end point. Supported options include: Cylinder, Track, and Sector.
Offset from Disk Start (Default: 1)	Specifies an offset from the start of the disk where you want the partition to begin. This should be a whole number. The next field, Disk Start Offset Units, specifies which unit to use with this number.
Disk Start Offset Units (Default: Sector)	Specifies the units for the specified offset. Supported options include: Cylinder, Track, Sector, and Byte. For example, in a typical restore to an SSD from an MBR volume, the Offset from Disk Start would be 1,048,576 when the Disk Start Offset Units is in bytes. With the offset unit as Sector, the value would be 2048 for restoring to the SSD.

4. Click **Set Active** to adjust the selected partition to match the configured policy.
5. Click **Close.**

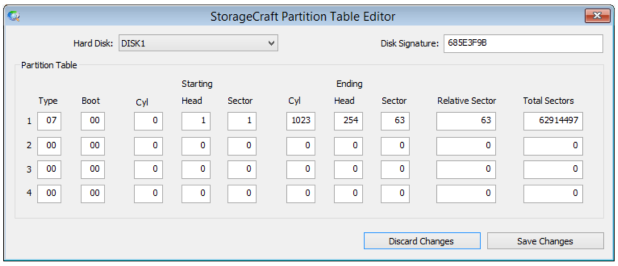
Recovery Environment closes the editor and returns to the Disk Map tab.

9.6 Partition Table Editor

⚠ **WARNING:** The Partition Table Editor should only be used by experienced technicians familiar with MBR partition parameters and in consultation with StorageCraft Support. Modifying these parameters can render a volume unusable and require a restore. Use the Disk Map options and the BCU instead to work with partitions and correct boot problems.

Note: The Total Sectors value may show a minus sign on some occasions. Ignore this incorrect sign.

The Partition Table Editor provides basic configuration control of the MBR partition table. This table lists references to the four potential volumes on an MBR hard disk. Reviewing these parameters can assist in troubleshooting or repairing boot failures or lack of volume access.



Hard Disk: DISK1

Disk Signature: 685E3F9B

Partition Table

			Starting			Ending				
	Type	Boot	Cyl	Head	Sector	Cyl	Head	Sector	Relative Sector	Total Sectors
1	07	00	0	1	1	1023	254	63	63	62914497
2	00	00	0	0	0	0	0	0	0	0
3	00	00	0	0	0	0	0	0	0	0
4	00	00	0	0	0	0	0	0	0	0

The editor displays:

Field	Description	Options
Hard Disk	A designator specific to this partition editor only.	Subtract 1 from the value indicated to determine the Windows numerical designator (for example, DISK1 is DISK0 in Windows).

Type	A numerical designation in the partition table	Typical Windows partition types include 00 (unpartitioned), 07 (NTFS), and 0F (Extended Partition)
Boot	Indicates whether this is a system (boot) volume.	The editor lists the boot volume as 80. Others as 00.
Starting	Displays the values for the three parameters for the start of the partition: Cylinder, Head, and Sector	
Ending	Displays the values for the three parameters for the end of the partition: Cylinder, Head, and Sector	
Relative Sector	Indicates the number of sectors before the start of this volume.	
Sectors	Lists the total number of sectors in the volume.	

Click **Save Changes** to keep any modifications made to the table. Click **Discard Changes** to keep the original MBR values.

10 Mounting a Backup Image File

The Recovery Environment *Explore Backup Image Wizard* guides you through the process of mounting a backup image file to browse and restore files and folders.

Note: For information on types of mounts see Backup Image File Mount Options.

To restore files and folders

1. Open the Explore Backup Wizard by doing one of the following:
   - In the Wizards tab, click **Browse or Restore Files Wizard.**
   - In the Tasks menu, click **Explore Backup Image.**
2. In the Backup Image File Name page, browse to the image file you want to browse, then click **Next.**
   Note: The Mount Wizard supports both ShadowProtect image files as well as Microsoft Virtual Hard Disk (VHDX) files. Use the *Files of type* dropdown box to show and select either VHDX or ShadowProtect files.
3. (Conditional) Provide the appropriate password if the wizard detects the file is encrypted.
4. (Conditional) In the Backup Image Dependencies page, keep the selected point-in-time image or choose another.
   Note: Recovery Environment only displays this Dependencies page if you select an Incremental image (.spi) to explore.
5. In the Explore Options page, select from these 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. Uncheck this option to mount the volume as read/write. You can then make changes to content--add, edit, or delete files or folders--and save them. When you dismount the volume, the utility asks you if you want to save the changes and to name the file. The utility saves this new file to preserve the changes. **Note:** The utility never alters the original backup file.

6. In the Wizard Summary page, review the mount information, then click **Finish.**

The utility mounts the backup image file, then automatically launches an Explorer window and displays the contents of the mounted volume.

Mounting a Windows Dedup Volume

If any of the dependent backup files in the backup chain are stored on a Windows Dedup volume, ShadowProtect cannot:

- Mount the backup file.
- Run a VirtualBoot on the backup file.

10.1 Backup Image File Mount Options

The Recovery Environment Mount utility can open a backup file as:

- A drive letter or as a mount point.
- Read-only or writeable.

Mounting a Backup Image as a Drive Letter

The Mount Utility can mount a backup image file as a drive letter with all the properties of the original volume. For example, if this is an NTFS volume using EFS (Encrypted File System), the security remains intact on the volume once it mounts.

Once mounted as a drive letter, you can perform a variety of tasks on the volume. These include 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.

You can also mount the volume as a shared drive. Users on a network can then connect to the shared drive and restore files and folders from within the backup image. In this way users can recover their own files. The volume remains mounted until you dismount it or restart the system.

Note: You can mount one or more backup images at a time.

Mounting a Backup Image as a Mount Point

The Mount Utility can also mount the volume as a mount point (a directory on an NTFS file system). Mount points overcome the available drive letter limitation and support more logical organization of files and folders.

Mounting a Read-Only Backup Image

By default, the Recovery Environment mounts backup image files as read-only. This lets users access the backup image to:

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

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

Mounting a Writeable Backup Image

The wizard can mount a backup image as a writeable volume. This lets users access the backup image to:

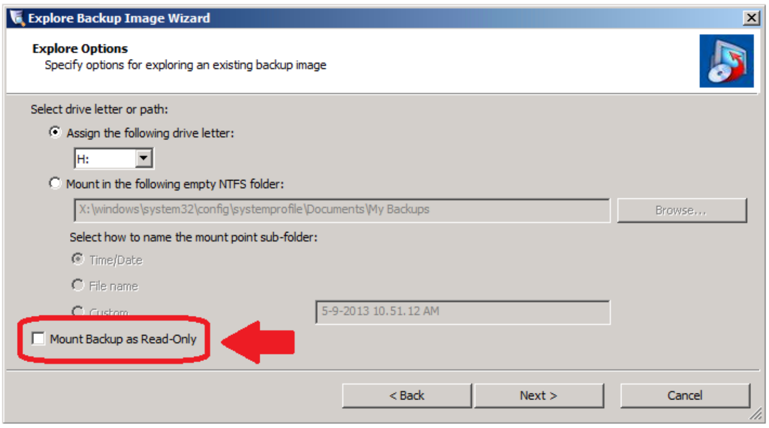
- Remove files from the backup image (viruses, malware, etc.)
- Add files to the backup image.
- Update the backup image security.
- Restore a backup image to a smaller volume (see Dismounting a Backup Image File).

⚠ **Note:** ShadowProtect prevents you from modifying the initial full backup image file to prevent corruption of an entire backup image set. If necessary, create a differential incremental and then mount that volume as writeable in order to make changes.

Also, saving a writeable volume creates a new backup file which is a "branch" to the original chain. It does not change the source file or the image chain.

Enabling a writeable file is a two step process:

1. Uncheck the default *Mount Backup as Read-Only* in the options dialog as shown:



Explore Options
Specify options for exploring an existing backup image

Select drive letter or path:

● Assign the following drive letter: H:

○ Mount in the following empty NTFS folder: X:\windows\system32\config\systemprofile\Documents\My Backups

Select how to name the mount point sub-folder:

● Time/Date

○ File name

○ Custom 5-9-2013 10.51.12 AM

□ Mount Backup as Read-Only

Otherwise, the Mount utility ignores the changes when you dismount the volume.

2. When you dismount the volume, select to Save Changes and specify a name and location for the new image file.

The utility then creates a new incremental file as a branch to the original chain.

10.2 Dismounting a Backup Image File

Once mounted, a backup image file remains mounted until explicitly dismounted or the system reboots. The Backup Image Dismount Wizard guides you through the process of dismounting. As part of the dismount process, you can:

- 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 the 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. 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.**
2. On the Mounted Backup Images page, select the backup image volume to dismount, then click **Next.**
3. (Conditional) On the Backup Image Dismount Options page, select if you want to:

   ⚠ **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.
   Note: This option is only available when dismounting a writeable backup image of an NTFS volume in Windows Vista or Windows Server 2008 (or later).
4. On the Backup Image Dismount Summary page, review the dismount details, then click **Finish.**

The wizard dismounts the volume.

11 Using Image Conversion Tool

The Image Conversion Tool can:

- 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, DVD, or Blu-Ray discs.

- Consolidate a base image file and any incremental files into a new base image file.
- Convert existing image files into either a .vmdk or a .vhd format for use in a virtual environment.

For more details, refer to the Image Conversion Tool section of the ShadowProtect User Guide.

Common tasks for the Image Conversion tool in Recovery Environment include:

- Converting a file
- Checking Dependencies

11.1 Converting a File

To use the Image Conversion Tool to convert a file

1. Click **Tasks** > **Image Conversion Tool** on the menu bar**.**
2. On the Source Image File page, select the backup image file you want to copy to a new format.
   Note: Provide the appropriate password if the backup image is encrypted.
3. (Optional) If you chose an incremental (.spi) file, the wizard presents a dependencies page showing details of this file. You can keep this file for conversion or select a different one. **Note:** The file details fields are read-only.
4. On the Destination Image File page, specify the location and name of the new file, then click **Next.**
5. On the Options page, configure any needed settings (see Options for details.)
6. On the Wizard Summary page, review the job summary, then click **Finish.**

The tool converts the selected file and places it in the destination folder.

11.2 2TB Drive Size Limit on Conversion

The current hypervisor from VMware *only* supports VMDK files converted from partitions of under 2TB in size. Previous versions of Hyper-V also limited VHD files to under 2TB as well. Any ShadowProtect image file converted using the image conversion tool to VHD or VMDK format must come from a source partition that is under 2TB in total size. The actual size of the image file, even if it is under 2TB in size, isn't important. If the source partition is over 2TB then these hypervisors won't mount the file.

A workaround is to partition drives larger than 2TB into volumes smaller than 2TB.

NOTE: In Windows 8/Server 2012, Microsoft introduced a new virtual file format: VHDx. VHDx does support volumes greater than 2TB. However, Recovery Environment and the image conversion tool do not currently support this format.

The conversion tool warns if the source partition is larger than 2TB, depending on which version of ShadowProtect runs:

Warning in ShadowProtect versions 4.1.5 and older

When using the image conversion tool, ShadowProtect 4.1.5 and older will fail to create the converted file. Instead, it displays a -87 error in the event log:

```
14-Oct-2012 10:01:44 sbrest 411 Cannot create new virtual disk file E:\backups\big conversion.vmdk (-87 The
parameter is incorrect.)
```

ShadowProtect version 4.2.x and newer

In ShadowProtect 4.2 and newer, selecting a source partition larger than 2TB in the image conversion tool displays a dialog with the VHD and VMDK options disabled:

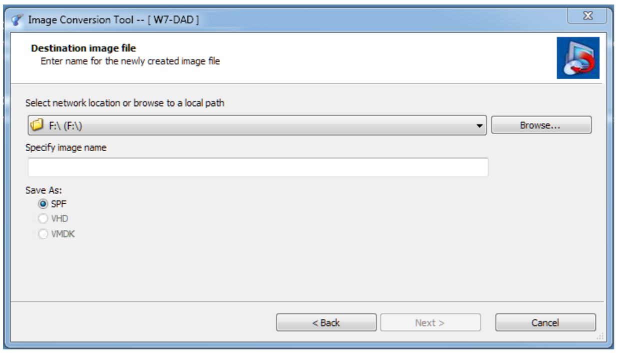


Image Conversion Tool -- [W7-DAD]

Destination image file
Enter name for the newly created image file

Select network location or browse to a local path

F:\ (F:\)

Specify image name

Save As:
● SPF
○ VHD
○ VMDK

11.3 Checking Dependencies

You can use the Image Conversion tool to determine dependencies in a backup image chain. Use this prior to deleting one or more image files to avoid breaking a backup chain and preventing a restoration.

To use the tool to view dependencies:

1. Click **Tasks** > **Image Conversion Tool** on the menu bar**.** The Image Conversion Wizard displays.
2. On the Source Image File page, select the incremental backup image (.spi) file you want to view dependencies for. **Note:** Provide the appropriate password if the backup image is encrypted.
3. The wizard displays a dependencies page showing details of this file. The dependency chain appears on the left side, with the base image at the top and the latest incremental at the bottom of the list. **Note:** The file details fields are read-only.
4. Click **Cancel** after reviewing the dependencies to exit the tool.

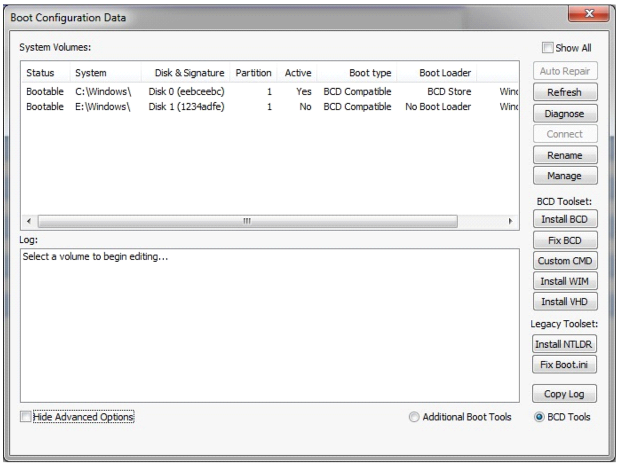
⚠ **Warning:** Do not delete the selected file if it has subsequent incremental files. This breaks the chain and renders the subsequent files useless.

12 Using the Boot Configuration Utility

In most restores, the Recovery Environment's automated boot configuration repair ensures that a system volume is bootable. In cases where this process encounters problems or where the volume is part of a complex multi-boot scenario, the Boot Configuration Utility (BCU) can manage the boot configuration repair process. The utility modifies the configuration data (hence BCD in the interface for "boot configuration data"). The BCU can also test the "bootability" of a system volume while still in Recovery Environment and do an automatic repair even before rebooting the system.

Note: Review the [Windows Boot Process] to better understand the BCU process.

To use the Boot Configuration Utility



System Volumes:

Status	System	Disk & Signature	Partition	Active	Boot type	Boot Loader	
Bootable	C:\Windows\	Disk 0 (eebceebc)	1	Yes	BCD Compatible	BCD Store	Winc
Bootable	E:\Windows\	Disk 1 (1234adfe)	1	No	BCD Compatible	No Boot Loader	Winc

Log:

Select a volume to begin editing...

BCU interface lists:

Available tools	Buttons at the right side of the dialog
Accessible volumes	System Volumes in the top pane

Running event log	Log in the lower pane

It also displays options to:

Show All	(Default: *Not Selected*) Displays either all volumes on the system (Show All) or only system volumes in the top pane.
Hide Advanced Options	(Default: *Selected*) Hides all of the boot configuration tools except *Auto Repair*.
Additional Boot Tools	(Default: *Not selected*) Displays a set of advanced tools for working with the registry and disks. Toggles with the *BCD Tools* option.
BCD Tools	(Default: *Selected*) Displays the BCD toolset. Toggles with the *Additional Boot Tools* option.

To use the BCU:

1. Select **Tools** > **Boot Configuration Utility**.
   The System Volumes pane lists all accessible partitions that contain a Windows installation.
2. 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 advanced boot scenarios). Each *System Volumes*entry includes the following information:

   Status The status of the current boot configuration. Piossible values include `Bootable` and `Broken`.

   System The root and drive letter of the detected Windows installation.

   Disk & Signature The disk number and its signature. Every disk has a unique signature. **Note:** 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.

   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.
3. Click on the desired boot repair action to fix a broken volume:

   ### General Tools

   Auto Repair: Runs the automated boot configuration routine. (This apppears only when the *System Volumes* pane lists the selected volume status as *Broken*.) **Note:** Using **Auto Repair** should be the first course of action when attempting to fix a boot configuration.

   Refresh: Refreshes the volume data in the *System Volumes* pane.

   Diagnose: Runs the same automated boot configuration routine as Auto Repair except it is in read-only mode. This routine displays a description of the boot configuration error and presents possible courses of action.

   Connect: Links additional bootable partition(s) to the active partition for use in dual- or multi-boot environments. Without this connection, the additional boot environments would not be accessible. To link each additional partition, select one partition at a time, click **Connect**, then select the active partition and click **OK**.

   Rename: Opens the *Boot Loader Entry Name* dialog box. Use this dialog to change the selected volume's name at boot time.

   Manage: Opens the *Manage Boot Entries* dialog box. Use this dialog to 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.

   ⚠ **Warning:** Deleting valid entries renders a volume unbootable until repaired.

   Copy Log: Copies the contents of the event Log shown in the lower pane to the clipboard so you can save it to a text file. **Note:** The contents of the log refresh after each action runs. Using **Copy Log** allows you to preserve the results of each action.

   ### BCD Toolset (displayed by selecting *BCD Tools*)

Install BCD: Installs a BCD boot loader. This might be necessary if the Windows installation was not the Active partition on the system where it was created. **Note:** This option only works for post-Windows-Vista OSes.

Fix BCD: Repairs BCD-compatible boot configurations. When migrating a volume to a different disk, information required for startup might be altered or lost. This option repairs or replaces this information. **Note:** This option only works for post-Windows-Vista OSes.

Custom CMD: Opens the `BCDEdit` utility for the BCD store of the selected Windows Vista or later installation.

Install WIM: Selects a Windows Image (WIM) as a boot option.

Install VHD: Selects a Virtual Hard Disk (VHD) image as a boot option.

Legacy Toolset (displayed by selecting *BCD Tools*)

Install NTLDR: Installs a legacy `(NTLDR)` boot loader. This includes the NTLDR, NTDETECT.COM, and BOOT.INI files. This install may be necessary if the Windows installation was not the Active partition on the system where it was created. **Note:** This option only works with pre-Windows-Vista OSes.

Fix Boot.ini: Repairs the `boot.ini` file used by legacy `(NTLDR)` boot configurations. **Note:** This option only works with pre-Windows-Vista OSes.

Registry Toolset (displayed by selecting *Additional Boot Tools*)

Edit Services: Opens the Service Explorer. Use the Explorer to enable or disable services and drivers for the selected volume. This is very helpful to debug a migration compatibility issue or identify a driver or service that is causing a startup failure.

Drive Letter: Opens the Drive Letter editor. Use this editor to assign a specific letter to any drive in the selected volume. This is useful to restore 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 of any changes that resulted 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 selected source: default Legacy (pre-Vista), default Windows Vista, default Windows 7, or fom the volume's corresponding ShadowProtect backup image. This is useful if data from Hidden tracks were not restored.

Set Signature: Opens the Enter New Disk Signature dialog. Use this dialog to manually set a disk signature. Typically, Windows sets the disk signature during installation, but migration and disk duplication can result in two disks having the same signature.

⚠ **Note:** The Boot Configuration Utility warns the user if there is a conflict between two disks.

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

Initialize: Opens the Initialize Disks dialog. Use this dialog to initialize a disk as either MBR or GPT.

⚠ **Note**: Initializing a disk erases all partitions and data from the drive. After initializing a disk, you must reboot before using the disk.

4. Review entries in the Log pane to see the result of each boot configuration action.
   Note: If an action fails, the log information identifies the point of failure.
5. Close the utility.

12.1 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.

Windows System: 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 results in system errors.

13 Working with an HSR Volume

HeadStart Restore (HSR) creates a standby volume for later restoration in the event of a failure. You can create the HSR volume then apply incremental updates to it to keep it current. Typically, HSR is used for large volumes as the HSR process greatly shortens the time needed to do a full restore. This also shortens the time needed to bring a failed server back online.

Note: ImageManager also includes an HSR feature. There are significant differences between the two however. HSR in ImageManager:

- Runs as an automated process to update HSR volumes
- Works only with virtual volumes

HSR in the Recovery Environment:

- Requires manual updates to the HSR volume.
- Requires downing the system and booting into Recovery Environment for each update.
- Works only with physical volumes.

You can use the HSR feature of Recovery Environment to:

- Create a new HSR volume
- Create incremental backups
- Apply incremental updates to an existing HSR volume
- Finalize an existing HSR volume

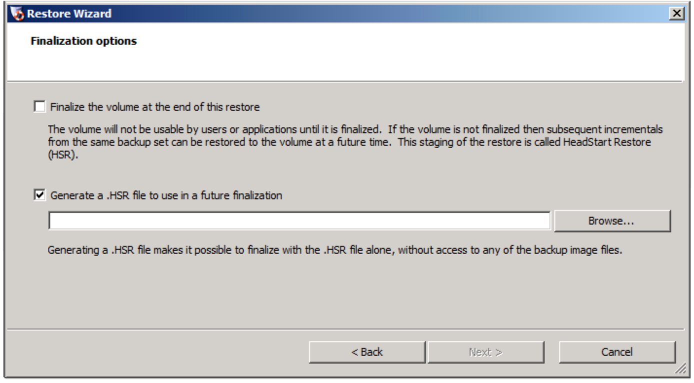
13.1 Create a new HSR Volume

To create a new HSR volume in Recovery Environment:

1. Attach one or more disks or select an existing volume or volumes as the:
   - Destination for the backup files.
   - Target for the future system's restore.
   - Repository for HSR management files.

   Note: The target and destination disks or volumes must have at least the same capacity as the existing volume.

2. If necessary, create a full backup image file of the volume using the Backup WIzard.
   Note: You can also use an existing full backup of the volume as well.
3. Save this file to the backup files destination.
4. Run the Recovery Environment Restore Wizard.
5. Select *Restore*.
6. Select the full backup file of the volume.
   Note: Backup files stored on the NETGEAR ReadyDATA do not support HSR.
7. Select the target for the restored volume. Recovery Environment displays the Finalization Options dialog:



Restore Wizard

Finalization options

☐ Finalize the volume at the end of this restore

The volume will not be usable by users or applications until it is finalized. If the volume is not finalized then subsequent incrementals from the same backup set can be restored to the volume at a future time. This staging of the restore is called HeadStart Restore (HSR).

☑ Generate a .HSR file to use in a future finalization

Generating a .HSR file makes it possible to finalize with the .HSR file alone, without access to any of the backup image files.

8. Select *Generate a .HSR file to use in a future finalization*.
9. Select a destination for the .HSR management files. Note: This cannot be the target for the restore. However, it can be the destination for the backup files.
10. Click **Finish**.

Recovery Environment creates the HSR volume. This volume is not readable by the OS or users. As an HSR volume, however, you can apply future incrementals to the HSR volume (until it is finalized) by using the Restore Wizard.

13.2 Create Incremental Backups

To create an incremental backup of a source volume for use with HSR:

1. Select *Perform a Differential Backup* as the restore type in the Restore Wizard.
2. Select the previous backup file (either a .SPF or a .SPI if this is a subsequent backup incremental).
3. Review the Dependencies page to ensure the selected file is the latest backup.
4. Confirm the destination of the new backup incremental file. This must be in the same folder with the rest of the backup chain.

Restore Wizard executes the backup. Return to the wizard to choose to restore subsequent incrementals to the existing HSR volume.

13.3 Applying Incrementals to an HSR Volume

You can use the Restore Wizard to apply incremental files to update an unfinalized HSR volume. Note these cautions:

- You can only apply later incremental images that are "descendants" of the last Incremental image file used to update 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 when you select one to update the HSR volume, Recovery Environment automatically applies all intervening incremental images up to and including the one you selected.

⚠ **Warning:** The Recovery Environment HeadStart Restore requires you to keep the last incremental file used to update the volume if you want to apply future incrementals. If HSR cannot find the last incremental, the HSR volume effectively closes and can then only be finalized. You cannot add further incrementals to it. This closing can occur when:

- You move the last incremental to a new directory. (HSR expects to find it in the same directory with the rest of the backup chain.)
- You delete this last incremental.
- ShadowProtect deletes the last incremental due to retention policy.
- ImageManager deletes this incremental as part of a consolidation policy.

StorageCraft recommends you turn off consolidation and/or retention policy in both ShadowProtect and ImageManager until you complete the HSR to avoid prematurely closing the HSR volume to further updates.

Encrypted Backup Image Files

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

Incremental Application Options

The Restore Wizard can apply one or more incrementals to an HSR volume:

- Using the wizard interface
- Using the volume's right-click menu

Applying Incrementals using the Wizard Interface

To apply incremental updates to the HSR volume using the Restore Wizard:

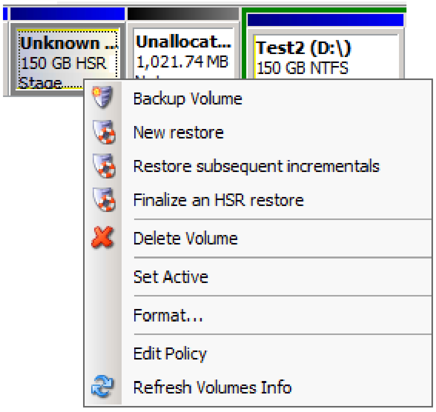
1. Select *Restore subsequent incrementals* as the Restore Type in the wizard.
2. Select the target HSR volume.
3. Browse and select the latest incremental in the backup repository from the source volume.
   Note: This incremental must be a descendent of the backup file used to create the HSR volume. Recovery Environment alerts you if it is not.
4. To keep adding future incrementals to this file, select the *Generate a .HSR file to use in a future finalization* option.
   Note: Select *Finalize the volume at the end of the restore* if you want to complete the restore and boot the target volume.
5. If you select the Generate .HSR file option, browse to and select the existing HSR management file.
6. Follow the wizard's prompts to complete the update.

The Restore WIzard will apply the incremental(s) and update the HSR management file.

Applying Incrementals using the Right-click Menu

To apply incremental updates to the HSR volume using the right-click menu:

1. Right-click on the target HSR volume to display this menu:



2. Click **Restore subsequent incrementals**.
3. Browse and select the latest incremental from the source volume.
   Note: This incremental must be a descendent of the backup file used to create the HSR volume. Recovery Environment alerts you if it is not.
4. The Restore Wizard displays the list of file dependencies for this incremental. Confirm this is the point in time you wish to restore. Note that if you select a later incremental, the Restore Wizard applies all intervening incrementals to reach that point in time.
5. To keep adding future incrementals to this file, select the *Generate a .HSR file to use in a future finalization* option.
   Note: Select *Finalize the volume at the end of the restore* if you want to complete the restore and boot the target volume.
6. If you select the Generate .HSR file option, browse to and select the existing HSR management file.
7. Follow the wizard's prompts to complete the update.

You can return later to this HSR volume to do further updates or to finalize and boot the volume.

13.4 Finalize an HSR Volume

To finalize an existing HSR volume:

1. Run Recovery Environment on a system with access to the backup image repository, the HSR volume, and the HSR management file.
2. Run the Restore Wizard in Recovery Environment.
3. Select the latest incremental for the HSR volume.
4. Select the HSR volume as the destination.
5. Select *Finalize the volume at the end of the restore* in the Finalization Options dialog.
6. If necessary, select the appropriate boot parameter options. In particular, select *Hardware Independent Restore* on the Options page if the target system has new or different hardware.
7. (Optional) If the target is an existing HSR volume, select *Finalize using information from a .HSR file*.
8. (Optional) If this is a new HSR volume (without a saved .HSR file), select *Finalize using information from the backup image set*.
9. Click **Finish**.

Recovery Environment finalizes the HSR volume. Use HIR to complete the recovery and make the system bootable.

Boot Parameter Options

The *Specify the Restoration Options* page in Restore Wizard provides a set of boot parameter options that you can apply as needed to the restored volume**:**
Note: Recovery Environment displays this page only if you selected to finalize the volume.

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

Restore MBR	Restores the master boot record (MBR) as part of the volume restore job. 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. Use this utility to configure the volume to properly interact with the new or different hardware on the target system.

14 Using HIR

The Hardware Independent Restore (HIR) utility restores system images to different hardware or virtual environments. Use HIR to restore:

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

⚠ **Note:** HIR requires an activated copy of ShadowProtect on the source system volume in order to restore that volume to different hardware or to a virtual environment. ShadowProtect IT Edition does not have this limitation.

You can load the HIR utility from the:

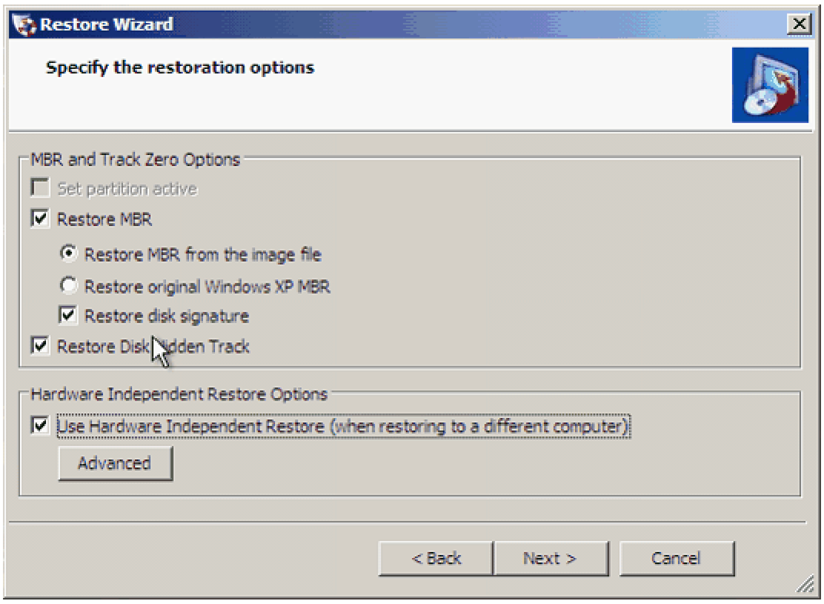
- HIR restore wizard
- HIR standalone utility
- HIR advanced options

⚠ **Note:** The ShadowProtect Restore log may not provided all error messages if there are problems patching boot code or performing HIR. These conditions are extremely rare but may include problems writing data to disk. The result is a restore log with no errors but the restored system fails to boot. The user can run the ShadowProtect Boot Configuration Utility (BCU) to gather more information about the underlying problem.

14.1 Run HIR from the Restore Wizard

To use HIR from the Restore Wizard

1. Run the Restore Wizard.
2. In the Options dialog, select **Use Hardware Independent Restore**.



Restore Wizard

Specify the restoration options

MBR and Track Zero Options

□ Set partition active

☑ Restore MBR

● Restore MBR from the image file

○ Restore original Windows XP MBR

☑ Restore disk signature

☑ Restore Disk Hidden Track

Hardware Independent Restore Options

☑ Use Hardware Independent Restore (when restoring to a different computer)

3. Complete the restore.

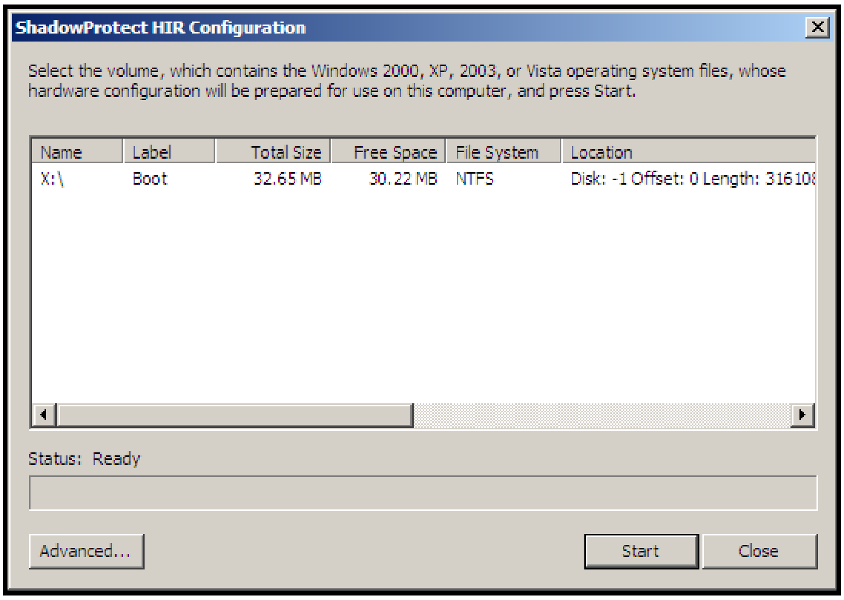
HIR automatically runs as part of the restore. Should HIR not find a needed driver, it displays a dialog asking for the path to the driver in order to contine.

Note: HIR verifies the existing ShadowProtect license from the backup image. If that license isn't current, HIR asks for an authentication code to continue. STC Support can provide this temporary code to perform the HIR. This code expires after 24 hours.

14.2 Run HIR as a Standalone Utility

You can run HIR as a standalone utility:

1. Complete the steps for restoring a backup image (see Restoring a System Volume).
2. In Recovery Environment, select **HIR Configuration** in the Tools menu.
   Note: HIR verifies the existing ShadowProtect license on the restored volume. If this license isn't current, HIR asks for an authentication code to continue. STC Support can provide this temporary code to perform the HIR. This code expires after 24 hours.



ShadowProtect HIR Configuration

Select the volume, which contains the Windows 2000, XP, 2003, or Vista operating system files, whose hardware configuration will be prepared for use on this computer, and press Start.

Name	Label	Total Size	Free Space	File System	Location
X:\	Boot	32.65 MB	30.22 MB	NTFS	Disk: -1 Offset: 0 Length: 31610

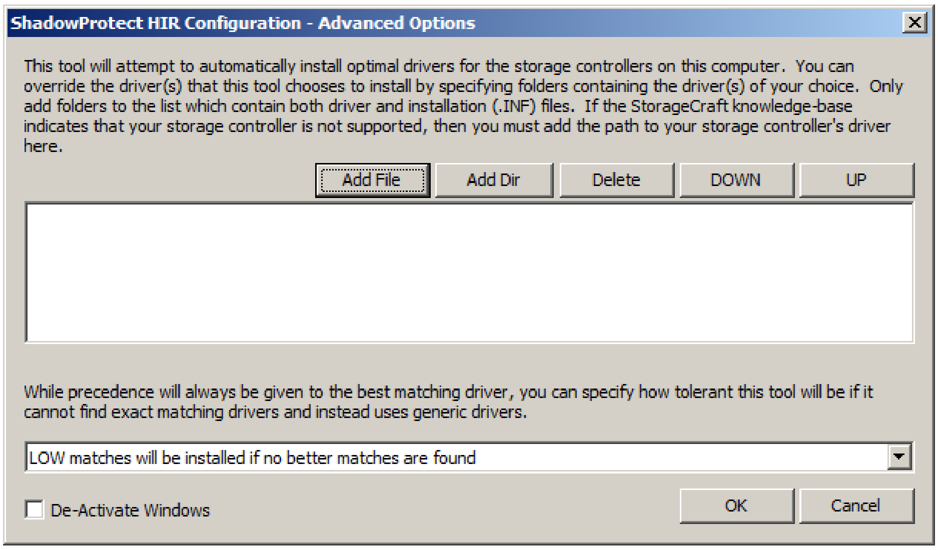
Status: Ready

3. Select the restored boot volume.
4. Click **Start.**

HIR runs and prepares the restored volume to be bootable on the new system.

14.3 HIR Advanced Options

The HIR Advanced options dialog adds files and directories to the HIR storage driver detection process.



This tool will attempt to automatically install optimal drivers for the storage controllers on this computer. You can override the driver(s) that this tool chooses to install by specifying folders containing the driver(s) of your choice. Only add folders to the list which contain both driver and installation (.INF) files. If the StorageCraft knowledge-base indicates that your storage controller is not supported, then you must add the path to your storage controller's driver here.

While precedence will always be given to the best matching driver, you can specify how tolerant this tool will be if it cannot find exact matching drivers and instead uses generic drivers.

LOW matches will be installed if no better matches are found

□ De-Activate Windows

From the HIR Advanced Options dialog, you can:

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	Changes the order in which HIR attempts to use these supplemental drivers or search directories. Select a driver or directory and click **UP** or **DOWN** to move the selected driver or directory up or down in the list.

You can also define how closely a driver must match the actual storage hardware to load. Use the dropdown menu to select to load a driver only when it:

- Matches hardware EXACTLY.
- Is an EXCELLENT match if no better driver is found.
- Is a GOOD match if no better driver is found.
- Is a FAIR match if no better driver is found.
- Is a LOW match if no better driver is found.

Deactivate Windows

The *De-Activate Windows* option instructs HIR to deactivate the existing Windows license found in the backup image file during the restore. You can then reactivate it through normal Windows mechanisms after the restore completes. Sometimes an HIR-restored Windows environment no longer registers as having an active license due to the changes in hardware. Deactivating then reactivating the license after the restore may avoid this issue.

Note: Windows Activation may intentionally lock some OEM copies of Windows to specific machines. Some OEM licenses may, in fact, not reactivate except on the original machine. In these cases, consult with Microsoft on reactivation options.

15 Using Remote Management

Recovery Environment includes the UltraVNC Server and Viewer that let you remotely control, using the UltraVNC Viewer, another computer running Recovery Environment and UltraVNC Server.

To configure the UltraVNC remote management solution

1. Select **UltraVNC** in Tools menu on the computer that you need to manage.
2. Enter a password for remote management. UltraVNC Server then loads.
3. Configure UltraVNC Viewer on the remote computer:
    1. Collect the address and credentials necessary to connect to UltraVNC Server.

2. Load UltraVNC Viewer.
3. Specify the IP address of the computer running UltraVNC Server
4. Click **Connect**.
5. When prompted, specify the remote management password.
6. Once connected to the remote UltraVNC Server, you can operate Recovery Environment as if on the remote system.

For more information about UltraVNC Server and UltraVNC Viewer, visit www.uvnc.com.

16 Other Operations

The StorageCraft Recovery Environment supports the following additional operations:

- Deleting Backup Image Files
- Verifying Backup Image Files

16.1 Deleting Backup Image Files

You can use the File Browser tool to review or 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.

WARNING: Deleting a backup image file that has dependencies renders these newer dependent files useless. If you can delete such a file, you can no longer browse or restore from these files.

Delete using the File Browser tool

1. Click **Tools > File Browser**.
2. Navigate to the file you want to delete.
3. Right-click on the file, select *Delete* and confirm the deletion.

The tool deletes the file.

16.2 Verifying Backup Image Files

Both ShadowProtect and ImageManager provide tools for verifying the integrity of backup image files. If necessary, Recovery Environment also provides a verification tool. This helps ensure that a backup image file is ready when needed.

Note: You can also use the *Explore Backup Image* utility or the *Browse or Restore Files Wizard* to further verify a backup file's integrity. Use either of these to mount the image, browse and view the files and folders, and confirm their integrity. (See Mounting a Backup Image File.)

To use the Verify Image wizard

1. Select *Verify Image* in the Tasks menu. The Verify Image wizard displays.
2. Browse and select the image file you want to verify. Click **Next.**
3. In the Specify the Verify Options page, select:
   - **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.
     Note: If you select this option, specify the file order you want the Verify Image wizard to use.
4. In the Wizard Summary, review the verify job, then click **Finish.**

The tool performs the verification and reports on the success or failure of the test.