



StorageCraft Recovery Environment CrossPlatform User Guide

StorageCraft Copyright Declaration

StorageCraft ImageManager, StorageCraft ShadowProtect, StorageCraft Cloud, and StorageCraft Cloud Services, together with any associated logos, are trademarks of StorageCraft Technology Corporation in the United States and elsewhere. All other brands and product names are or may be trademarks or registered trademarks of their respective owners.

Table of Content

Table of Content	2
1 ShadowProtect Overview	3
1.1 Features and Components	3
1.2 Recovery Environment Usage Scenarios	4
2 How ShadowProtect Works	5
2.1 Create a Backup Image	5
2.2 Restore a Backup Image	6
2.3 Backup Image Files	6
3 Starting Recovery Environment	8
3.1 Requirements	8
3.2 Using Network Settings	10
3.3 Testing the Recovery Environment CD	11
4 Understanding the User Interface	12
4.1 Menu Bar	12
4.2 Task Panel	13
4.3 Tabs	14
4.4 Task Bar	18
5 Creating a Backup Image File	19
5.1 Image File Destinations	19
5.2 Options	20
5.3 Create Differential Backups	21
6 Using the Disk Utility	22
7 Restoring a System Volume	24
7.1 Recreate Original Partitions	25
7.2 Using the Restore Wizard	25
8 Mounting a Backup Image File	26
8.1 Dismounting a Backup Image File	26
9 Using Image Conversion Tool	27
9.1 Converting a File	28
9.2 2TB Drive Size Limit on Conversion	28
9.3 Checking Dependencies	29
10 Using HIR	29
10.1 Run HIR as a Standalone Utility	29
11 Using Boot Repair	30
12 Using Remote Management	31
13 Other Operations	31
13.1 Deleting Backup Image Files	31
13.2 Verifying Backup Image Files	32

StorageCraft Recovery Environment CrossPlatform User Guide

Welcome to the StorageCraft® *Recovery Environment CrossPlatform User Guide*. This Guide describes the ShadowProtect technology, and how to derive maximum benefit from the StorageCraft Recovery Environment CrossPlatform (RE-X).

RE-X is an innovative environment based on a Linux OS. It provides unique benefits for recovering system volumes:

- Restores all Linux and Windows environments supported by ShadowProtect and SPX.
- Supports both formatting and partition actions on MBR and GPT drives.
- Runs as a full 64-bit environment with significant contemporary 64-bit driver support.
- Supports conversion of an image chain into the new Microsoft .vhdx virtual drive format.
- Prevents saving a new incremental using the same name as an existing one.

This Guide includes the following major sections:

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

Additional Information

- For emerging issues and other resources, see the following:
 - The [StorageCraft Recovery Environment ReadMe](#) file available online.
 - 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 CrossPlatform 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:

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

1.1 Features and Components

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

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

ShadowProtect Console

- 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.

[ImageManager](#) controls your backup image files using policy-driven services. ImageManager can:


StorageCraft ImageManager

- 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.

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

StorageCraft Recovery Environment - CrossPlatform

- Load from a CD or a USB stick.
- Mount any backup image file as a virtual disk.
- Access essential 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).
- Export backup files as VMware .vmdk and Hyper-V .VHD or .VHDX.

 **Note:** For a complete version history of product updates, see the [online ReadMe files](#).

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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Use script files (before and after the snapshot) to manage applications (both VSS and non-VSS) and improve backups.

Additionally, ShadowProtect provides a Backup Scheduler that lets you configure automated backup jobs for protected volumes. You can schedule full image, incremental images (as often as every 15 minutes), and manage the retention of backup image sets. 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	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.
-cw.spi	
-cm.spi	
-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 backup image files use the following naming convention to help you identify the file and its relationship to, and dependencies on, other backup image files.

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

The ShadowProtect naming convention uses the following variable components:

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

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

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

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

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

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

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

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

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 Starting Recovery Environment

Recovery Environment - CrossPlatform (RE-X) loads automatically when you boot from:

- A custom CD created with the downloadable Recovery Environment ISO.
- Using the RE-X ISO in a VM.

Note: Although built on Linux, RE-X fully supports all Windows restorations as well as Windows partition and drive operations.

Before you run RE-X, make sure your system meets the minimum [hardware and software requirements](#).

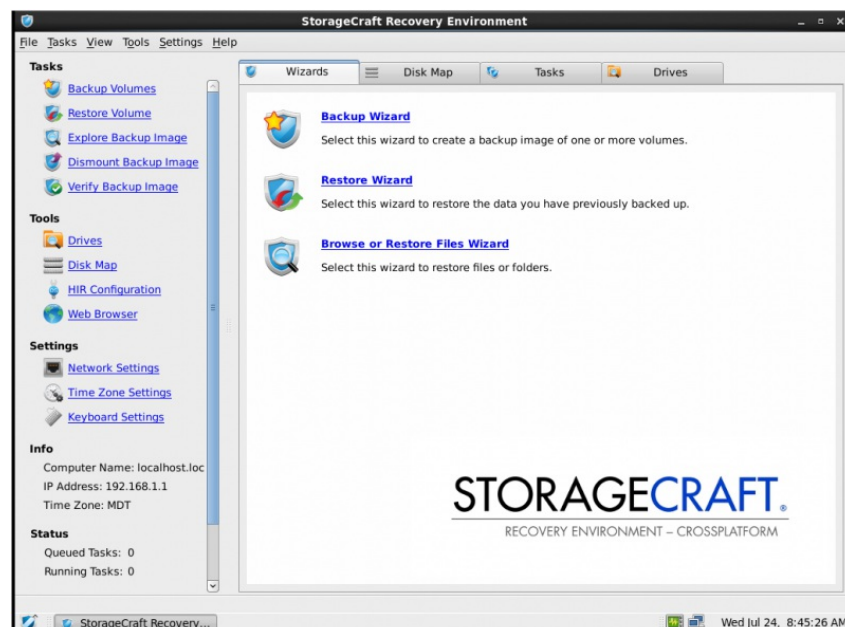
Note: StorageCraft recommends downloading a fresh copy of RE-X at least every six months. StorageCraft continually updates the RE-X ISO with new drivers--network, video, and storage--to keep pace with updated hardware.

To load the StorageCraft Recovery Environment

1. If necessary, [download the RE-X ISO](#) from the StorageCraft website and either burn it to a CD or make it available to the hypervisor host.
2. If the backup image chain to restore is located on a USB drive, attach that drive to the computer.
3. Insert the RE-X CD into the computer or create a VM using the ISO.
4. Restart the computer.

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

5. Select which language to use. The default is English.
6. Click **OK**. Follow the prompts to launch RE-X. Recovery Environment displays its main screen:



This screen and the wizards are similar to the installed version of ShadowProtect. For additional details on how to use the wizards, see [Understanding the User Interface](#) in the ShadowProtect Users Guide.

3.1 Requirements

ShadowProtect Recovery Environment has these minimum hardware requirements:

Hardware	Recovery Environment CrossPlatform (RE-X)
CPU	1 GHz or faster 64-bit processor
Memory	512 MB minimum
Motherboard	Requires UEFI firmware to support GPT disks as bootable drives. When using a UEFI motherboard, the UEFI must support BIOS emulation.
Hard Drive space	N/A
CD-ROM or DVD drive	Required
USB Port	Required if the image chain is stored on an external USB drive
Monitor	VGA or higher resolution

Using a Japanese Keyboard

The Recovery Environment CrossPlatform supports using a Japanese keyboard. Note that selecting Japanese as the language for RE-X does not automatically enable Japanese keyboard support. To enable this support:

- Select Settings > Keyboard Settings.
- Select the Layouts tab
- Click **Add**.
- In the Country tab, choose *Japan* as the country. Keep the default *Japanese* in the Variants field.
- Select the English (US) keyboard layout then click **Remove**.
- To use Japanese characters, right-click on the Keyboard icon at the bottom right of the screen and select Anthy:



- To toggle between Japanese and Latin characters, press the 半角/全角キー (Hankaku/Zenkaku key) on the Japanese keyboard:



Supported Operating Systems

The Recovery Environment CrossPlatform supports restoring the following operating systems:

Windows

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

Linux Operating Systems

StorageCraft is committed to providing backup and restore features for distributions of Linux with long-term support (LTS). It does not support self-compiled or short-term releases. The 64-bit version of RE-X is designed to backup and restore Ubuntu 12.04 (64-bit) and CentOS/RHEL 6 (64-bit) with EPEL repositories enabled.

Supported File Systems

The Recovery Environment - CrossPlatform 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: RE-X and ShadowProtect do not support the exFAT or ReFS file systems. It also does not support Windows Storage Spaces storage pools.

Supported Storage Media

The Recovery Environment - CrossPlatform 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)

Note: RE-X supports iSCSI which the Windows Recovery Environment does not.

The Image Conversion feature supports these virtual disks:

- VMware VMDK
- Microsoft VHD
- Microsoft VHDX

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.

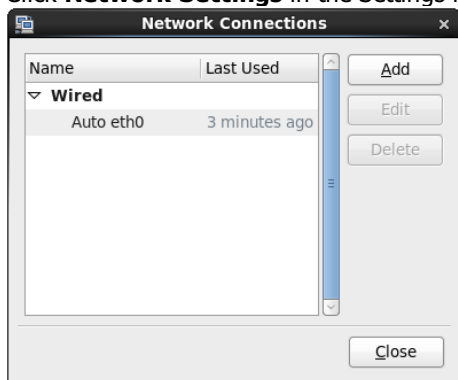
3.2 Using Network Settings

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

Note: While RE-X can support wireless network cards, StorageCraft recommends only using a wired connection when restoring files from a network repository to the destination system or for backing up volumes to a network repository.

To specify NIC settings

1. Click **Network Settings** in the Settings menu to open the utility:



2. Select the appropriate network adapter from the list.
3. Click **Edit** to modify the adapter settings. The Network Details dialog displays:



The dialog's tabs include:

Wired: Specifies the MAC address for the adapter.

802.1x Security: Specifies credentials used when running security on this connection.

IPv4 and v6 Settings: These tabs display configuration details for each of these.

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.

3.3 Testing the Recovery Environment CD

Test the StorageCraft Recovery Environment CrossPlatform to ensure that it runs properly on your computer and that you have the correct drivers needed to access devices. To do this, boot your computer with the Recovery Environment CD.

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

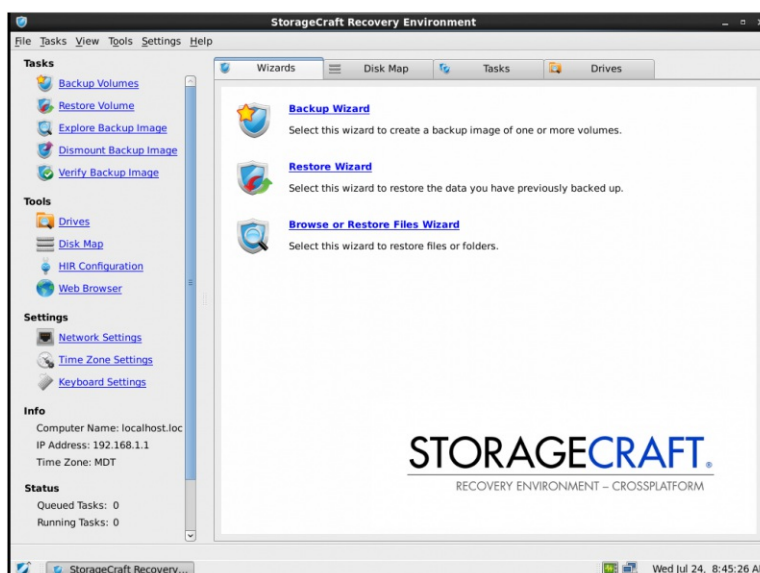
- You do not have the necessary network interface card (NIC) drivers to access the network.
- You do not have the necessary storage drivers to access a storage device on the computer.

If this is the case, try the [Recovery Environment for Windows](#) available from the StorageCraft website.

Note: If you find the Recovery Environment CrossPlatform lacks certain drivers, contact StorageCraft Technical Support or send an e-mail to support@storagecraft.com so StorageCraft can include these drivers in future releases of RE-X.

4 Understanding the User Interface

Once the Recovery Environment CrossPlatform loads, the main dialog appears:



This main screen includes four 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.
- **Task Bar**--Located at the bottom of the screen. The [Task Bar](#) includes tabs to running applications, calendar, and a "Start" menu with similar options to those on the menu bar or Tasks panel.

The Main dialog's four [tabs](#) include:

- **Wizards**--Launches the *Backup*, *Restore*, or *Files* wizard.
- **Disk Map**--Provides partition tools that function similar to the Windows Disk Management utility.
- **Tasks**--Displays the status of an active task in the upper panel, details from the task in the lower panel. To abort an active task, click **Cancel**.
- **Diagnostics**--Shown only after running a Diagnostic test, this tab shows the resulting log from the test.

Wizards is the default tab displayed.

Note: Holding down the right mouse button on a dialog in RE-X behaves differently than it does in REWIND. In RE-X, holding down the right button on a dialog which includes a pop-up menu not only displays the menu but also automatically selects the first option in the menu. This may result in unexpected actions so note which option is selected before releasing the right mouse button.

4.1 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	<p>Backup Volumes: Launches the Backup Wizard.</p> <p>Restore Volume: Launches the Restore Wizard.</p> <p>Explore Backup Image: Launches the Explore Backup Image Wizard.</p> <p>Dismount Backup Image: Launches the Backup Image Dismount Wizard.</p> <p>Image Conversion Tool: Launches the Image Conversion Tool.</p> <p>Verify Image: Launches the Verify Image Wizard.</p> <p>Restore Disk Layout from Image: Opens the Restore Wizard and instructs the system to duplicate the partition layout based on the layout of the selected backup image file. Note: The destination drive must be formatted first using the Disk Utility as either GPT or MBR.</p>
View	Manages toolbar visibility	<p>Task Panel: Toggles the Task Panel. This enlarges the Tabs display for easier operation.</p> <p>Wizards: Redisplays the Wizards tab if that tab is closed or another tab is currently displayed.</p> <p>Disk Map: Redisplays the Disk Map tab if that tab is closed or another tab is currently displayed.</p> <p>Tasks: Redisplays the Tasks tab if that tab is closed or another tab is currently displayed.</p> <p>Drives: Redisplays the Drives tab if that tab is closed or another tab is currently displayed.</p>
Tools	Accesses Recovery Environment tools.	<p>HIR Configuration: Launches the Hardware Independent Restore (HIR) utility. This utility assists in restoring restores a backup image to a different environment from which the image was created. In particular, the HIR dialog allows the user to specify a source directory of drivers for use on the new platform.</p> <p>Text Editor: A simple text editor similar to Notepad.</p> <p>Configure LVM: Opens a standard Linux <i>Logical Volume Manager</i> utility. Use this utility to configure LVM partitions as part of restoring a Linux server.</p> <p>VNC Settings: Launches the Remote Management utility. This utility configures remote access to systems running Recovery Environment.</p> <p>Manage iSCSI Targets: Opens the iSCSI utility to specify the host name or IP address and the port used by iSCSI.</p>
Settings	Manages the system configuration	<p>Network Configuration: Launches the Network Configuration utility. This utility configures the computer's network access settings.</p> <p>Proxy Settings: Specifies the proxy configuration if the system's network uses a proxy. Most Recovery Environment operations do not require network access unless the backup image file repository is on a server.</p> <p>Display Settings: Opens the <i>Display Settings</i> dialog. This dialog configures the resolution and color mode for the Recovery Environment UI.</p> <p>Keyboard Settings: Opens the Keyboard Settings dialog. This dialog selects and then test international keyboard layouts.</p> <p>Time Zone Settings: Launches the Time Zone utility. Use this utility to select the system's time zone and to set the date and time for RE-X.</p>
Help	Displays general Recovery Environment information	<p>About: Displays the Recovery Environment version and copyright information.</p> <p>Collect Diagnostics: Generates an onscreen report of installed hardware and software for use by StorageCraft Support.</p>

4.2 Task Panel

The Task panel on the left side of the dialog provides navigation to RE-X tasks and tools. The panel is organized into menus and options:

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

Tasks	Access ShadowProtect wizards	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 .
Tools	Access Recovery Environment tools	HIR Configuration: Launches the Hardware Independent Restore (HIR) utility . This utility assists in restoring restores a backup image to a different environment from which the image was created. In particular, the HIR dialog allows the user to specify a source directory of drivers for use on the new platform.
		Drives: Selects the <i>Drives</i> tab in the main panel to select or mount local or network drives or to mount a backup image file.
		Web Browser: Opens a browser. If one is not installed, RE-X asks to install one. (Requires network connectivity.)
Settings	Manages system configuration	Network Configuration: Launches the Network Configuration utility . This utility configures the system's network access settings.
		Time Zone Settings: Launches the Time Zone utility. Use this utility to select the system's time zone and to set the date and time for RE-X.
		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.

4.3 Tabs

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

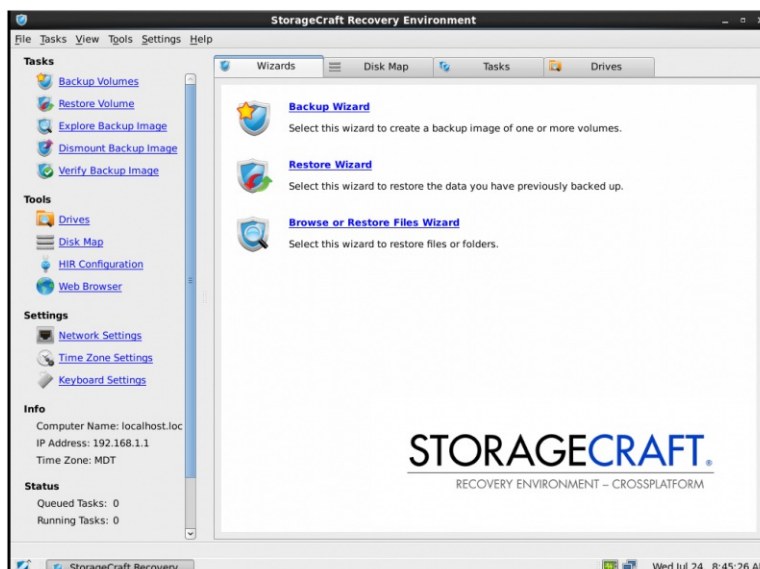
- [Wizards](#)
- [Disk Map](#)
- [Tasks](#)
- [Drives](#)
- [Diagnostics](#) (A tab which appears only when RE-X runs a report using the Help/Collect Diagnostics menu option.)

Wizards

The Wizards tab links to three function wizards:

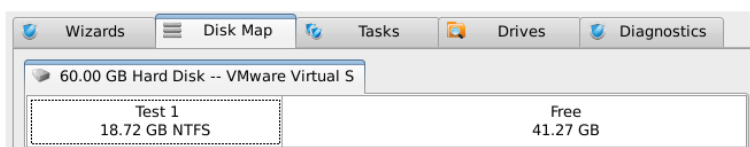
- [Backup](#)
- [Restore](#)
- [Browse or Restore Files](#)

These guide users through the most common Recovery Environment tasks:



Disk Map

This tab displays a graphical view of the available system drives, mounted image files, and their partitions:



Use Disk Map to:

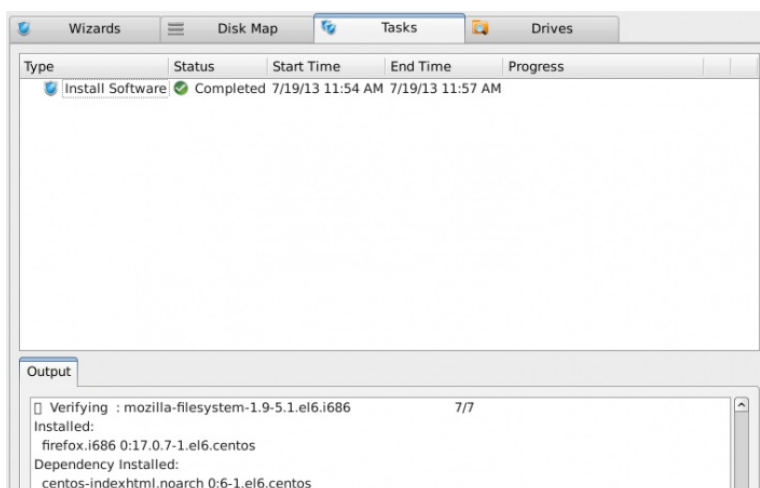
- View drive and partition information
- Select a drive or partition to run the Backup or Restore Wizards
- Restore a disk and duplicate the partition layout of the image file
- Run the [Disk Utility](#) to format disks or to create or modify partitions

Warning: The Disk Map right-click menu includes the option to *Initialize a drive as a GPT disk*. This option is the same as re-formatting the drive and removes any existing partitions and their data. Use the steps in the [Disk Utility](#) instead to format a drive.

Tasks

This tab displays a list of running or completed tasks (such as a backup or verification). Details of a completed task appear in the Output panel at the bottom of the dialog. To abort an active task, click the X at the end of the task line.

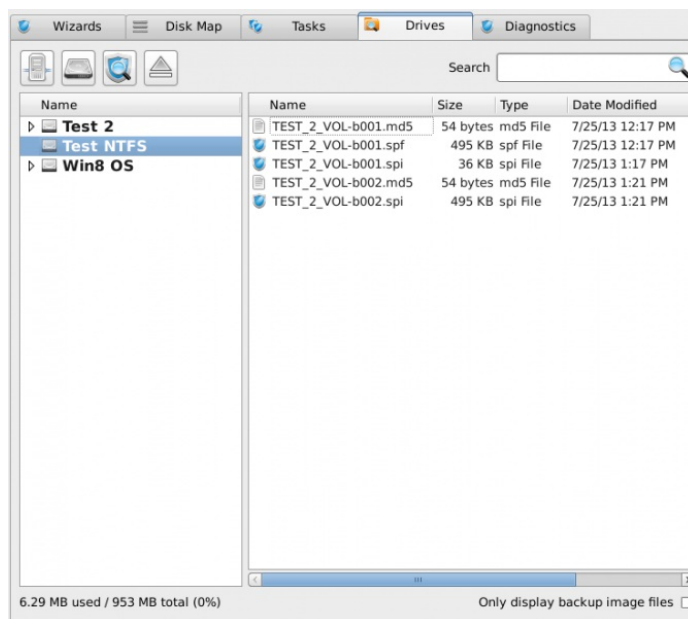
Note: If you abort an operation, you must restart the process from the beginning.





Drives

The Drives tab displays a list of available storage devices and mounted image files, the contents of those devices, and various options for working with drives:







Drives Menu Icons

The Drives main menu has four icons:



when working with drives. These include:

Icon	Title	Action
	Add Network Location	Opens a dialog to specify the UNC path and credentials needed to access a network storage device. This device then is mounted and available to RE-X.
	Add Local Drive	Opens a list of available locally attached drives. Note: Geryed-out items in the list are already mounted and accessible.
	Explore a Backup Image File	Mounts a backup image file to view or restore files or folders. Select an image file to mount by selecting the location in the Drives list or by clicking the Explorer icon and RE-X opens a box to choose the image file.
	Dismount the Selected Destination	Dismounts the selected drive or mounted image file. Once dismounted, the drive is not accessible to RE-X functions.

Search Box

This functions as a current directory filter to list only those files which match the criteria entered in the search box. For example, to display only those backup files with the string "b029", enter "b029" and click the search icon.

Only Display Backup Image Files Option

The Drives tab offers this option to simplify the file list to show only ShadowProtect backup files: .SPF and .SPI. This is useful when the source folder contains a large number of files in the chain with their associated .md5 files as well as any other non-ShadowProtect files.

Image File Right-Click Menu

Select a ShadowProtect .SPF or .SPI file and right-click on it to display a menu of options:

Open File	Attempts to open the file if RE-X has an application which can open it.
Copy	Saves a copy of the file to the clipboard.
Paste	Pastes the copy of the file from the clipboard.
Delete	Deletes the file. Warning: Do not delete backup image files without first checking dependencies . Doing so renders any subsequent backup files useless.
Restore Image	Opens the Restore Wizard .
Verify Image	Opens the Verify Wizard .
Explore Image	Mounts the selected file similar to the Mount Wizard .
Convert Image	Opens the Image Conversion utility .
Rename	Edits the file name.

Drives vs. Disk Map vs. Disk Utility

RE-X provides three tools for working with storage devices: the Drives tab, the Disk Map tab, and the Disk Utility. While all display a list of currently mounted disks and images, they offer distinct functions in working with these drives:

Tool	Description	Unique Capability
Drives tab	Selecting a drive displays a file/folder listing and works similar to Explorer. Can also mount accessible storage devices using the Add Network Drive and Add Local Drive functions to make them available to RE-X.	Provides file explorer functions
Disk Map tab	Displays the list of currently mounted disks and images along with their partitions. Provides options for working with the partitions including formatting and restoring images.	Can backup and restore volumes
Disk Utility	Provides options for working with disk hardware, including formatting the drive and creating or deleting partitions.	Formats drives as MBR or GPT. Adds, edits, or deletes partitions

Checking Dependencies

You can delete a selected file using the Drives dialog right-click menu. However, prior to deleting any .SPF or .SPI, it is critical to determine if any subsequent files depend on this file. This avoids breaking a backup chain and preventing a restoration.

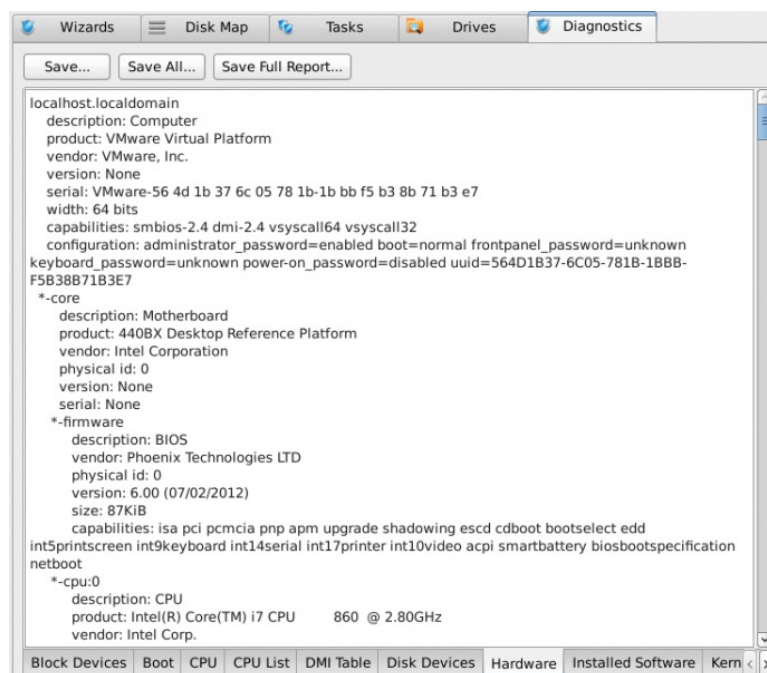
To view dependencies:

1. Select Restore Volume in the Tasks menu.
2. Select the base image file for the chain with the file that is targeted for deletion. Click **Next**.
Note: Provide the appropriate password if the backup image is encrypted.
3. The wizard displays a dependencies page showing details of the highlighted 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 an image file if it has subsequent incremental files. This breaks the chain and renders the subsequent files useless.

Diagnostics

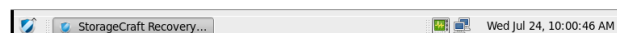
The Diagnostics tab display a set of reports on installed hardware and software in the system. Click Help\Collect Diagnostics to generate the report set. The set automatically displays in the new Diagnostics tab:



Use this information when contacting StorageCraft Support.

4.4 Task Bar

The Task Bar sits at the bottom of the RE-X main dialog:



These options are not necessary to perform ShadowProtect activities. They include:

- | | |
|---------------------------------|---|
| "Start" Menu | Click on this to open a list of options. The relevant ones to RE-X are duplicated in the main dialog. |
| Running Application Tabs | RE-X displays one or more tabs for currently running applications. By default, StorageCraft Recovery Environment always appears. Click on a tab to redisplay the application. |
| Disk Usage Icon | Right-click on this icon to display current disk usage. Since RE-X is a temporary environment, any disk activity is largely informational only. |
| Network Icon | Click on this icon to display the current network connections. The Network Settings option provides the same functionality in the RE-X dialog. |

Date/Time Indicates the current system time.

5 Creating a Backup Image File

The Recovery Environment Backup Wizard creates a backup of an entire system or a specific volume on that system. Unlike ShadowProtect, the Recovery Environment creates only cold backups. For 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 Volumes**.
 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.

Warning: Do NOT perform a differential backup of multiple drives and volumes that do not have a common full backup. The Wizard assumes that all the selected volumes have a common full image backup when creating the differentials. Attempting to do so results in a failure to perform the backup.
 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.
 6. Click **Next**.
 7. In the [Options](#) page, select compression type, password, and file splitting, then click **Next**.

Note: Keep the default settings shown in Advanced Options unless specifically required to make changes.
 8. Click **Finish** to create the backup image file.
- You can monitor the progress of the backup in the Tasks tab.

Note: When creating a cold backup of a system which uses Windows BitLocker to encrypt a partition, include the System Reserve partition as well in a backup. This one-time snapshot of System Reserve preserves Bitlocker data needed to decrypt the partition.

5.1 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.

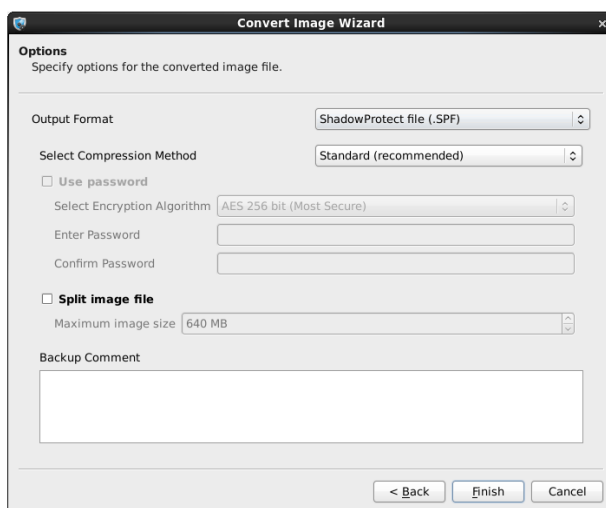
 **Note:** If you select a destination that does not have enough disk space to save the backup image, the backup job fails.

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

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

5.2 Options

The Backup Wizard's (and the Image Conversion tool's) *Options* dialog controls compression, security, and file splitting:



This section describes these options:

- [File Compression](#)
- [Backup File Encryption](#)
- [Splitting Backup Image Files](#)
- [Backup Comments](#)

File Compression

RE-X offers multiple file compression options when creating (or converting) 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

RE-X 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.

Warning: Make sure the password is stored in a secure location as StorageCraft cannot bypass the encryption on a backup image files without the password.

Note: The Image Conversion utility cannot encrypt files when output to a new .SPF file.

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

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

In addition to bit strength, the password used to secure the backup image file can affect security. Use the following password guidelines to ensure the 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 with the Backup Wizard.
- After creation with the [Image Conversion tool](#).

To split a file either during creation or conversion:

1. Check the *Split Image File* box in the Backup Wizard's (or Image Conversion tool'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. RE-X stores the resulting split files into the same folder as the source image file.
4. Copy the resulting split files onto CD or DVD recordable discs for archiving.

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.

5.3 Create Differential Backups

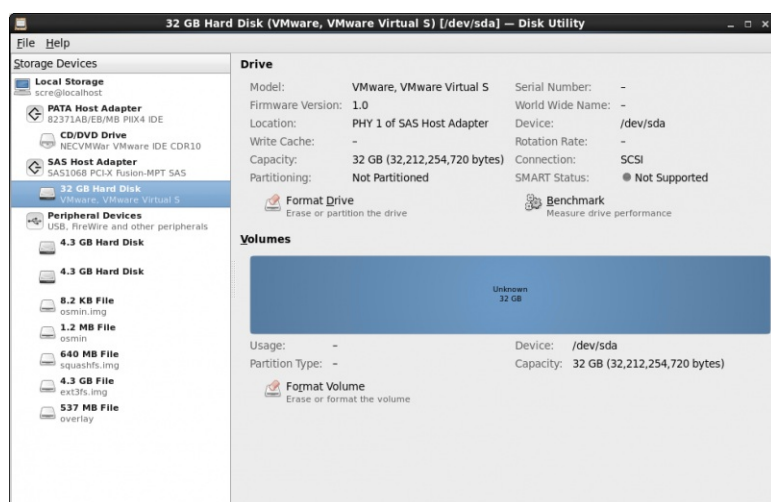
To create a differential backup of a source volume:

1. Run the Restore Wizard from the Tasks menu option or from the Wizards tab.
2. Select *Perform a Differential Backup* as the restore type in the Restore Wizard.
3. Select the previous backup file for that volume (either a .SPF or a .SPI if this is a subsequent backup incremental).
4. Review the Dependencies page to ensure the selected file is the latest backup.
5. Confirm the destination of the new backup incremental file. This must be in the same folder with the rest of the backup chain.
6. Click **Finish**.

Restore Wizard executes the backup.

6 Using the Disk Utility

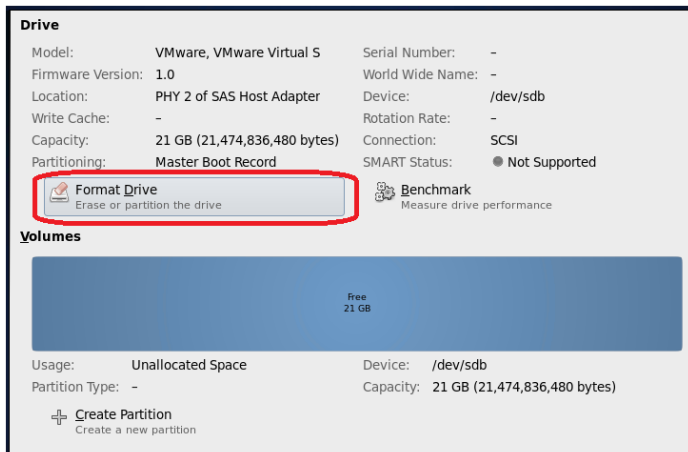
The Recovery Environment's Disk Utility primary function is to format drives and create partitions. In most restores, use the Disk Utility first to create a partition on a new, unformatted drive.:



While the tool itself has many options, most restores only require the use of the Format and the Create Partition features.

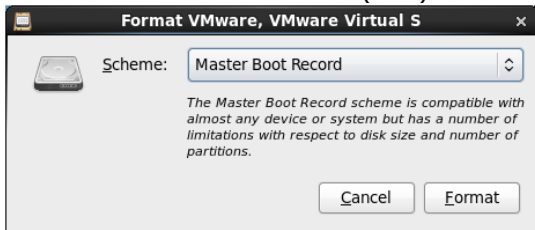
To Format a New Drive

1. Select the Drives tab. Locate the new drive in the list.
2. If the drive does not appear, click the [Add Local Drive icon](#) and mount the drive.
3. Click **Tools > Disk Utility**.
4. Select the drive from the list at the left.
5. Click Format Drive:



Note: Although the option says "Partition the drive", this option only formats the drive.

6. Select either Master Boot Record (MBR) or GUID Partition Table (GPT) from the dropdown list for the drive:

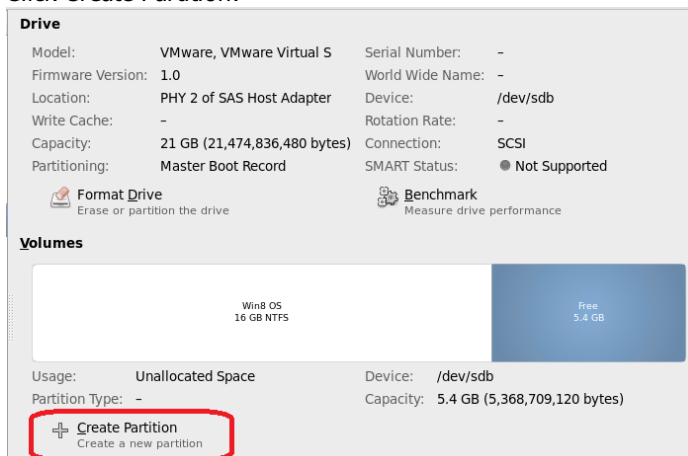


Note: Do not select either *Don't Partition* or *Apple Partition*.

The Disk Utility formats the drive.

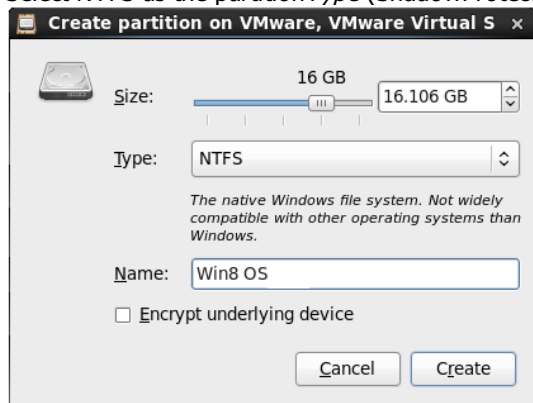
To Partition the Drive

1. Select newly formatted drive image in the center of the dialog.
2. Click Create Partition:



The Create Partition dialog appears.

3. Select NTFS as the partition *Type* (ShadowProtect does not support the others):



Warning: Do not select Encrypt underlying device. This prevents ShadowProtect from correctly reading the partition.

4. Click **Create**.

The Disk Utility adds the partition to the drive. Click on the Drives tab > Add Local Drive to mount this drive for a restore.

7 Restoring a System Volume

The primary purpose of Recovery Environment is to restore a system that cannot boot on its own. RE-X supports two methods to restore a system volume:

[Restore Disk Layout from Image](#)

This option in the Tasks menu restores both a system volume and/or any other volumes contained in the selected backup image file. It automatically restores these volumes to the same partition layout as on the source drive. It does this all in a single operation, rather than requiring separate operations to create the partitions and then restore the backup image.

[Restore Wizard](#)

Runs the wizard to guide the user through the process of restoring a single volume.

Note: RE-X only supports restores from .SPF and .SPI image files, not from VMDK, VHD, or VHDX format files.

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.

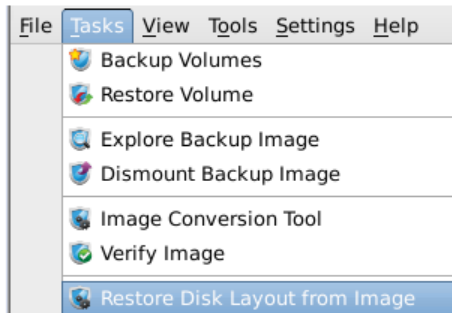
In the unusual situation of restoring a partition/volume from one logical sector size to another:

- 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.

7.1 Recreate Original Partitions

The *Restore Layout from Image* option recreates the partitions of the original drive on the destination drive:



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

1. Select *Format* if needed to:
 - Create a partition on a new, unformatted drive.
 - Remove any existing partitions on the target destination drive.

Warning: This erases all data on those partitions.
2. Select *Recreate layout from image file* to duplicate the source volume on the destination drive.
3. Select the base or incremental file to restore from.
4. Select any [Advanced Restore options](#) needed (for MBR disks).
5. Select the destination drive.

Note: RE-X displays an error message if the destination drive has existing partitions. It will erase these partitions (and any data in them) when it performs the restore.
6. The program displays a representation of the destination drive with the restored partition layout. Click **Finish** to confirm this layout is correct and to execute the restore.

The program restores the volumes onto the drive.

Advanced Restore Options

The Restore Wizard offers additional options when restoring an MBR drive:

Restore MBR Code Section	Restores the master boot record (MBR) from the backup image file. The master boot record is stored in the first sector of the first physical hard drive, and contains the master boot program and partition table. The master boot program uses the partition table to determine the active partition, then starts the boot program from the boot sector of the active partition.
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 Partition Table	Restores the layout of partitions from the backup file.
Restore Hidden Track	Restores the first 63 sectors of a drive. Some boot loader applications require this for the system to boot.

7.2 Using the Restore Wizard

The Restore Wizard guides the user through the restoration of a single volume from a backup image file to a new drive.

To restore a volume:

1. Use the Disk Utility to create a partition on a new, unformatted drive or to remove an existing partition.
2. Open the Restore Wizard using one of these methods:
 - Click **Restore Volume** in the Tasks menu.
 - Right-click on a backup image file in the Drives tab and select Restore Image.
 - Right-click on a partition in the Disk Map and select Restore Volume.

The Restore Wizard displays.

3. Select the backup image to restore. If necessary use the Add Network or Add Local drive options to access the drive with the image files.
Note: RE-X only supports restores from .SPF and .SPI image files, not from VMDK, VHD, or VHDX format files.
4. If the image file is a full backup image, the Wizard displays a list of subsequent incremental files as an option to restoring just the base image.
5. Select the appropriate partition to restore the volume.
Note: The Wizard displays an error if the partition selected is too small for the size of the volume on the backup file.
6. Choose whether to use Verify Image Before Restore to do one last check on the image file before the restore. The Wizard alerts if the image file fails the test.
7. Click **Finish**.

The Restore Wizard completes the restoration of the volume.

If this is a system volume restored on new hardware or on a virtual machine, [use the HIR feature](#) to ensure the disk is bootable.

8 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.

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**.
 - In the Drives tab, locate the file you want. Right-click on it to select *Explore Image*.
2. In the Backup Image File Name page, browse to the image file you want to browse, then click **Next**.
Note: Provide the appropriate password if the file is encrypted.
3. (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.
4. Click **Finish**. The utility mounts the backup image file.
5. Select the mounted image in the Drives window to display the contents of the mounted volume.
6. Right-click on a file or folder, then select *Copy* to restore the file or folder to another volume or drive.

8.1 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.

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 or Drives tab, right-click a mounted backup image, then select **Dismount Destination**.
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:

Save Changes to Incremental File the modified backup image file using a different name.
Note: StorageCraft recommends customizing the name to indicate this new branch of an existing backup chain. Otherwise, the default name for the incremental is the next available number in the existing backup chain. Although that chain ignores the new branch incremental file, users may be confused when trying to select a point in time from a long list of numbered backups if the branch isn't clearly identified.

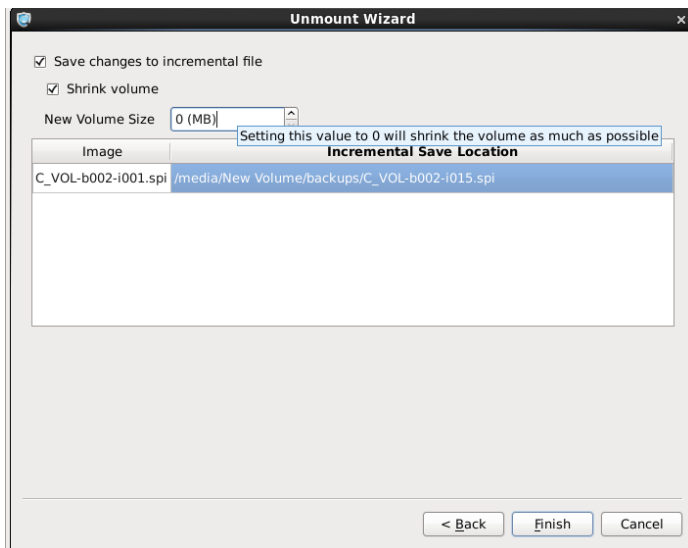
Shrink Volume Shrinks the volume so you can restore the image to a smaller partition.

4. Click **Finish**.

The wizard dismounts the volume.

Using Shrink Volume

Check the box labeled Shrink volume in the Dismount wizard to select the size you want to shrink the volume to:



The default value, 0, instructs the program to shrink the volume as much as possible.

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 prior to performing the shrink operation. This consolidates file distribution within the volume and frees up space at the end of the volume.

This option can also shrink the volume to a user-defined value. RE-X attempts to shrink the volume to the specified size but may not be able to do so due to environmental reasons. If the shrink operation fails, or if the resulting image does not restore, try specifying a larger value then re-run the shrink operation.

For example, if a 100GB volume has only 9GB of used space, and the user-selected value to shrink the volume to is 10GB, the shrink operation may fail. In that case, try selecting a value of 15GB and re-run the shrink operation.

9 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, a .vhd or .vhdx 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](#)

9.1 Converting a File

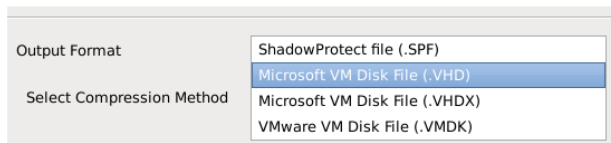
To use the Image Conversion Tool to convert a file

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 to convert 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 Converted Image Directory page, specify the location for the converted file. Click **Next**.
5. Edit the name of the new file as needed then click **Next**.
6. On the Options page, configure any needed settings (see [Output Format](#) and [Options](#) for details).
7. 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.

Output Format

The Image Conversion tool presents four options for output format:



These options are:

Output Type	Description
ShadowProtect file (.SPF)	Creates a single backup file from a chain of image files. This consolidation may be to conserve disk space or to simplify archiving of older chains.
Microsoft .VHD	Creates a virtual disk usable on the Hyper-V platform. Note: Limited to partitions smaller than 2TB.
Microsoft .VHDX	Creates a virtual disk usable on the Hyper-V platform. Note: Supports partitions greater than 2TB.
VMware .VMDK	Creates a virtual disk usable on VMware platforms. Note: Limited to partitions smaller than 2TB.

9.2 2TB Drive Size Limit on Conversion

Contemporary drive sizes now exceed 2TB in size. However, the current hypervisor from VMware *only* supports VMDK virtual disk files converted from partitions of under 2TB in size. Previous versions of Hyper-V also limited VHD files to under 2TB as well. This meant that 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 drive's contents or 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.


To answer this need, in Windows 8/Server 2012 Microsoft introduced a new virtual file format: VHDX. VHDX does support volumes greater than 2TB. With the introduction of RE-X, the StorageCraft Recovery Environment and the image conversion tool now support this contemporary format.

9.3 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.

10 Using HIR


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

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

 **Note:** You must install and activate ShadowProtect on the system volume before making a backup image of the volume in order to restore this image to different hardware using Recovery Environment. Use the ShadowProtect IT Edition instead to perform such restores.

The HIR function runs from:

Restore Wizard	Runs automatically as part of the restore process. Note: If the restore needs additional drivers, run the standalone HIR utility to apply them to the restored system volume.
Tools menu	Opens the standalone HIR utility .

 **Note:** Although the standalone HIR dialog displays a "Connect to Driver Service" option, this option is not active in this version.

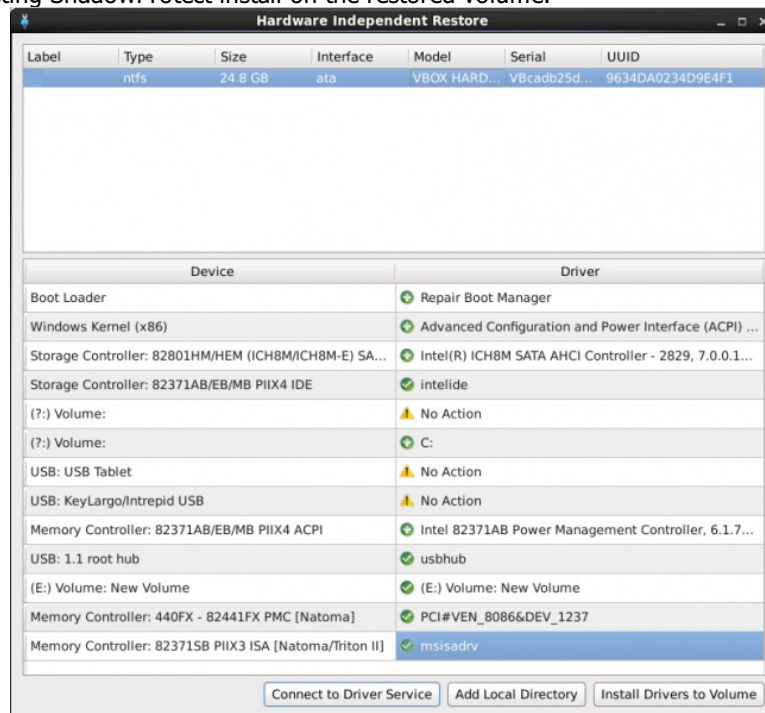
Caution: Unlike the Windows Recovery Environment, the StorageCraft CrossPlatform Recovery Environment does not support requesting an HIR decode key. If the image to be restored does not contain a current license, the HIR fails.

10.1 Run HIR as a Standalone Utility

Run HIR as a standalone utility after restoring a system volume on new hardware or as a new virtual machine. To do so:

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 install on the restored volume.



3. Select the restored boot volume.
4. Click **Add Local Directory** to select the location of additional drivers needed for the new hardware. HIR automatically populates the available device driver list next to each storage item in the Device list.
5. Select the correct device driver for each listed storage controller in the Device list.
6. Click **Install Drivers to Volume**.

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

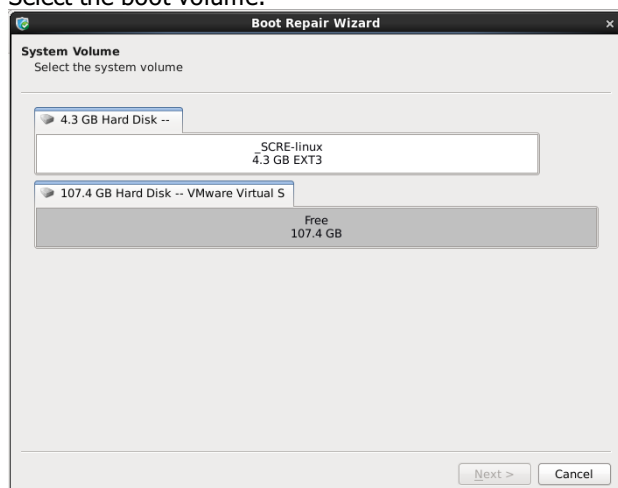
Note: StorageCraft recommends downloading a new copy of the Recovery Environment CrossPlatform ISO at least every six months. StorageCraft is continually updating the ISO with new device drivers to maintain compatibility with the latest hardware.

11 Using Boot Repair

Recovery Environment CrossPlatform (REX) includes the Boot Repair utility for use with restored Linux system volumes. (Boot Repair performs a similar function to HIR on Windows.)

To use Boot Repair:

1. Perform a Linux system volume restore.
2. Select **Tasks > Boot Repair**.
3. Select the boot volume:



Note: SPX also supports Linux systems with both a Boot and Root partitions,

4. Click **Next**.

- Click **Finish** to finalize the repair.

REX performs the repair to the system volume.

12 Using Remote Management

Recovery Environment includes VNC support to allow remote management of the system running RE-X..

To configure VNC remote management

- Select **VNC Settings** in the Tools menu on the system running RE-X:



- Check *Allow other users to view your desktop*.
- Enter a password for remote management.
- Click **Close**.
- Configure and run a VNC viewer on the remote computer:
 - Enter the address and credentials necessary to connect to the system running RE-X.
 - Click **Connect**.
 - When prompted, specify the remote management password.
 - Once connected, you can operate RE-X as if it were running at the console of the remote system.


13 Other Operations

The StorageCraft Recovery Environment CrossPlatform supports the following additional operations:

- [Deleting Backup Image Files](#)
- [Verifying Backup Image Files](#)

13.1 Deleting Backup Image Files

You can use the Drives tab (or the File Browser tool) to review or delete backup image files as you would any other file in the file system. However, do not delete any image file before verifying that none of them are required for any active backup jobs or that other backup image files depend on the backup images. Use the Restore Wizard 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 Drives Tab

- Click on the Drives tab.
- Navigate to the file you want to delete.
- Right-click on the file and select *Delete*.
- Confirm the deletion.

The tool deletes the file.

Checking Dependencies

You can delete a selected file using the Drives dialog right-click menu or the File Browser. However, prior to deleting any .SPF or .SPI, it is critical to determine if any subsequent files depend on this file. This avoids breaking a backup chain and preventing a restoration.

To view dependencies:

1. Select **Restore Volume** in the Tasks menu.
2. Select the base image file for the chain with the file that is targeted for deletion. Click **Next**.
Note: Provide the appropriate password if the backup image is encrypted.
3. The wizard displays a dependencies page showing details of the highlighted 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 an image file if it has subsequent incremental files. This breaks the chain and renders the subsequent files useless.

13.2 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 Backup Image* in the Tasks menu. The Verify wizard displays.
2. Browse and select the image file you want to verify.
3. Click **Next**.
4. Click **Finish**.

The tool performs the verification and reports on the success (green mark) or failure (red mark) in the Tasks tab..