

Data Storage Group, Inc.

Computer System Recovery

Walkthrough: Using DATASTOR Shield™ to protect and recover a computer system.

Contents

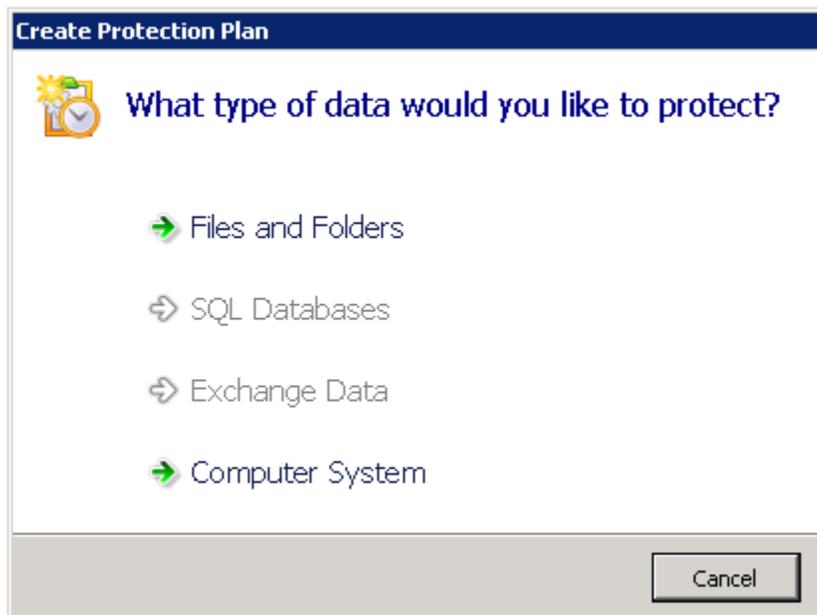
Introduction	2
Computer System Protection Plan.....	2
Running the Protection Plan	9
Saving the System Recovery Environment to Media	10
Copy to a USB drive.....	12
Copy SRE .iso file	13
Burn to CD or DVD	14
Restoring Data from a Computer System Protection Plan	15
Bootting a Computer for Recovery	15
Restoring your Computer System.....	17

Introduction

DATASTOR Shield introduces the ability to recover a complete computer system. There are two basic elements for protecting and restoring a complete computer system using DATASTOR Shield. The first element is creating and running a Computer System Protection plan. This plan type is available for local plans and plans for Remote Computers with proper licensing. A wizard for creating the Computer System type plan steps the user through drive selection, store selection, and creation of a schedule for when the protection plan runs. The second element is the System Recovery Environment (SRE). When recovering a complete system, the computer needs to use a bootable device to bootstrap the recovery process. The System Recovery Environment is a custom Microsoft Windows 7 Pre-installation Environment image that can run from a CD/DVD drive, bootable USB drive and, in the case of a virtual machine recovery, mounted as an ISO formatted bootable CD/DVD. Once the computer has been booted with the SRE, the process of recovering the system is only a few steps away.

Computer System Protection Plan

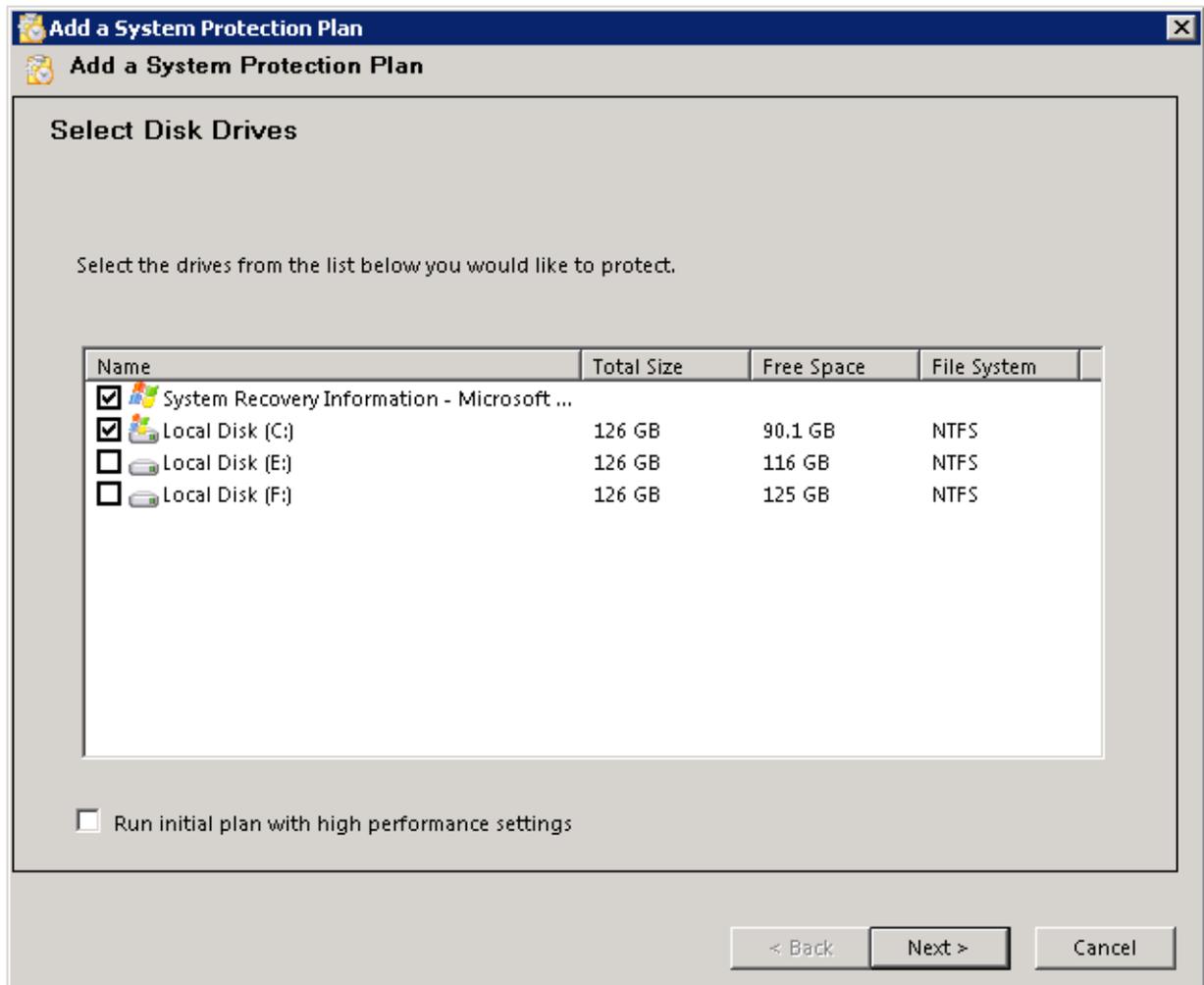
The Computer System Protection Plan saves both the system configuration information, including volume information and sizes, and the data that represents an entire computer system. You can create a Computer System Protection Plan for Windows Vista, 7, 2008 and 2008 R2 operating systems. To start the “Add a System Protection Plan Wizard” click “Create Protection Plan...” from the Actions for a Local Plan or a Remote Computer you have added into the system. Then, choose Computer System from the enabled plan types.



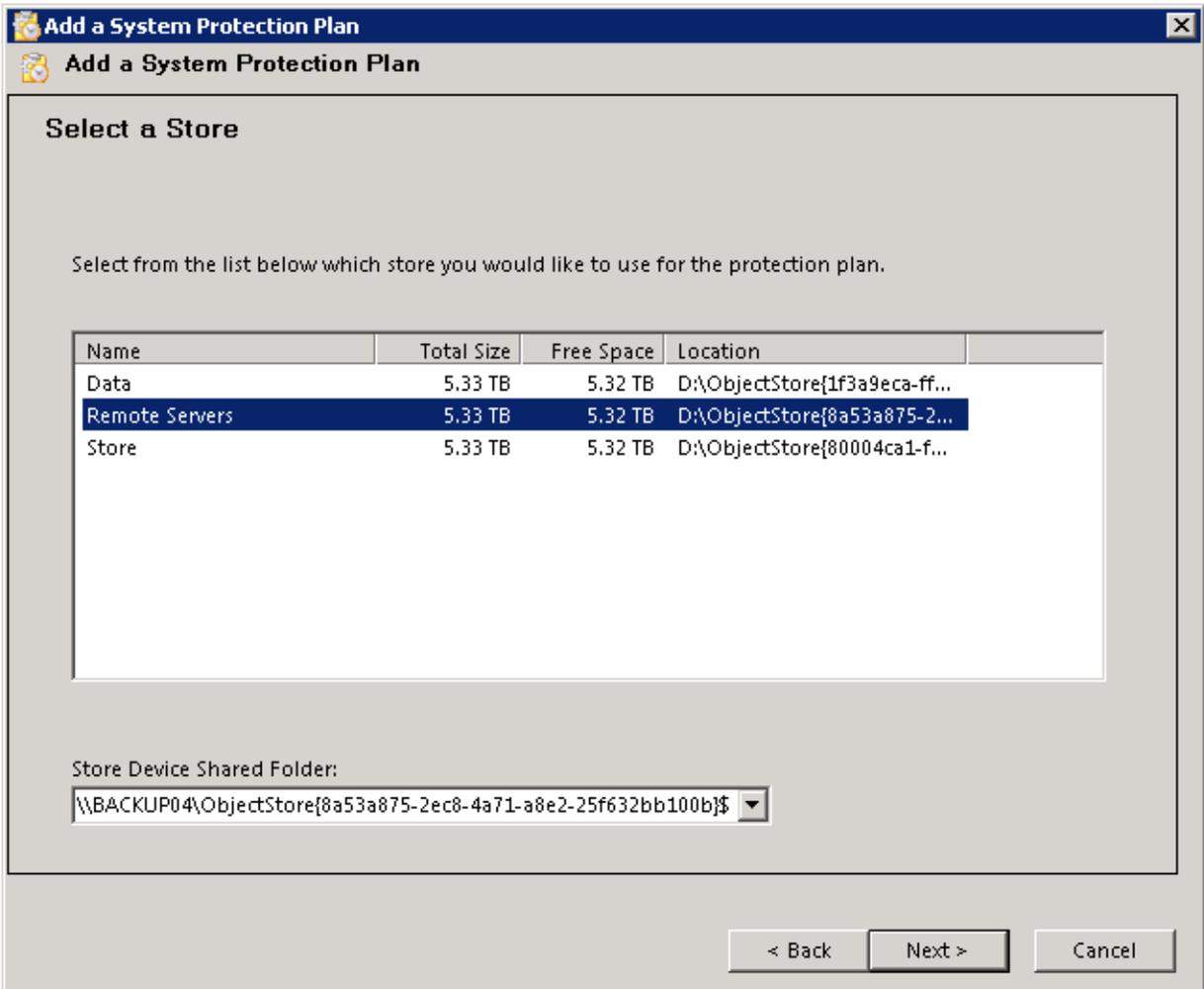
First, the “Add a System Protection Plan” wizard displays the disk drives to select for protection by the plan. There are three elements to choose in this view: System Recovery Information, System Drives and Data Drives. When the System Recovery Information is checked all System Drives must be checked as well. A system drive will be indicated with an icon of a disk with a Windows Logo overlaid in the upper left of the screen. The Data Drives are not required to be selected as part of the plan, where it may be

preferable to protect data on those drives with a different plan type. For example the data on a Data Drive might contain database and or log files for Microsoft Exchange, and in this case an Exchange Data Protection Plan would be a better candidate for protection of the data on this Data Drive, since only an Exchange Data type plan truncates logs..

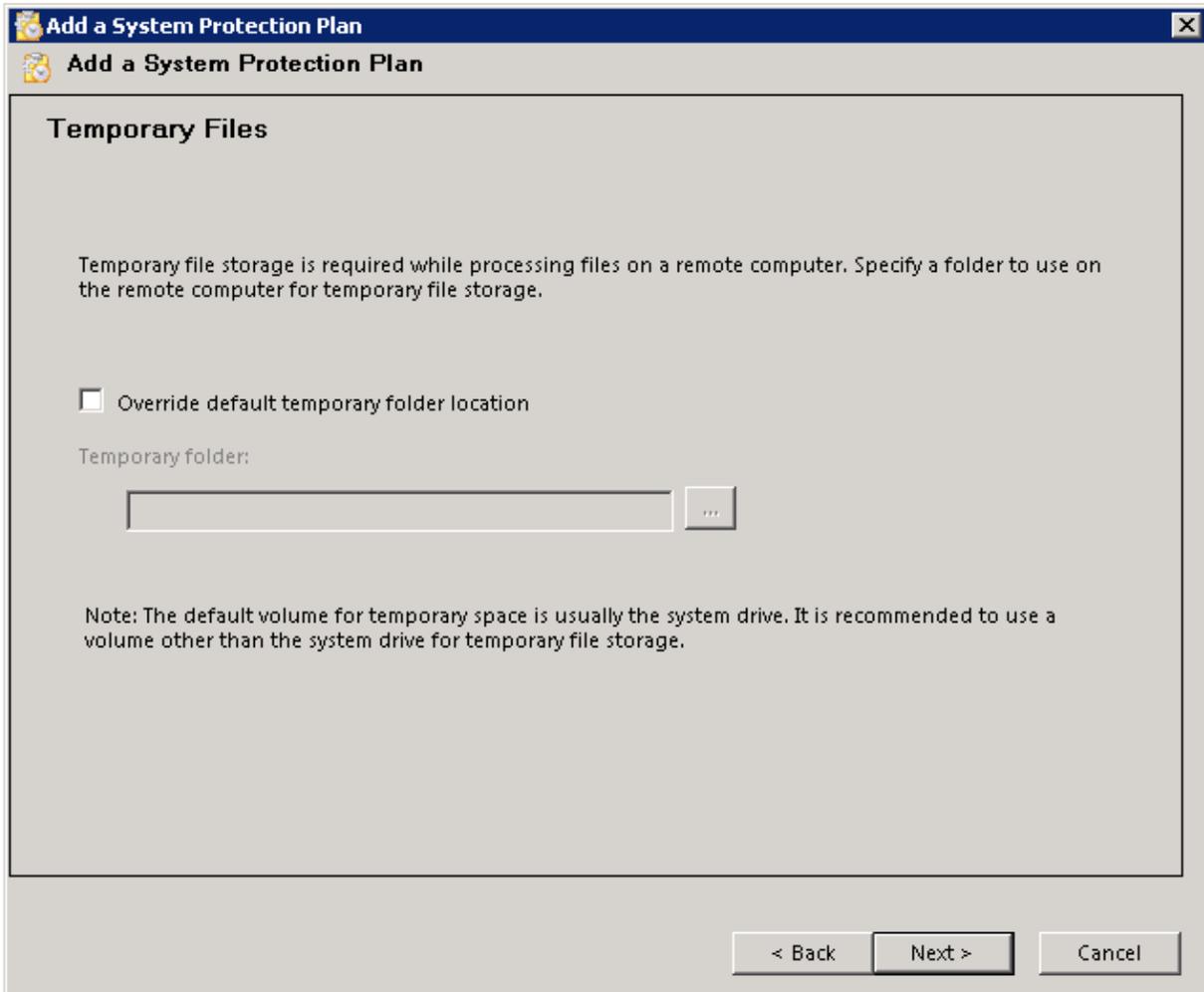
NOTE: Using the setting “Run initial plan with high performance settings” launches multiple backups assigning each sub-backup a portion of the work based on the number of CPUs in the system.



Next, select a store for the system plan to use to store the backup data and catalogs. A good practice would be to use a store created specifically for Computer System type protection plans, as deduplication of data across servers is a big benefit when backing up several Windows computers.



Next, select whether or not to override the Temporary Files location.



Next, provide a name for the protection plan. Protection plan names must be unique throughout the DATASTOR Shield system. A good practice for a Computer System Protection Plan is to use the computer name as part of the plan name, for example “Seligman System Plan”, where Seligman is the name of the computer being protected.

Add a System Protection Plan

Add a System Protection Plan

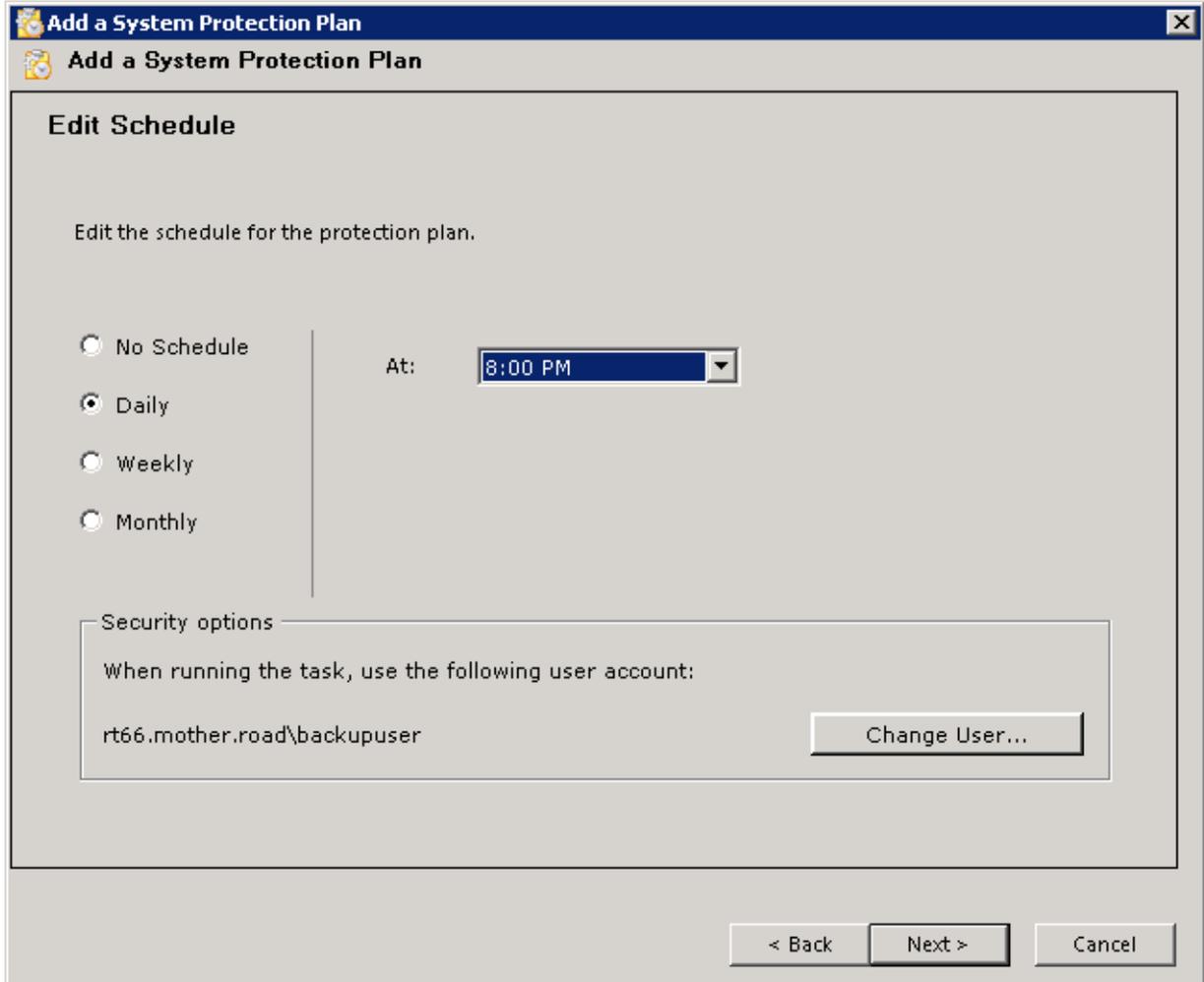
Enter Plan Name

Specify the name for the protection plan

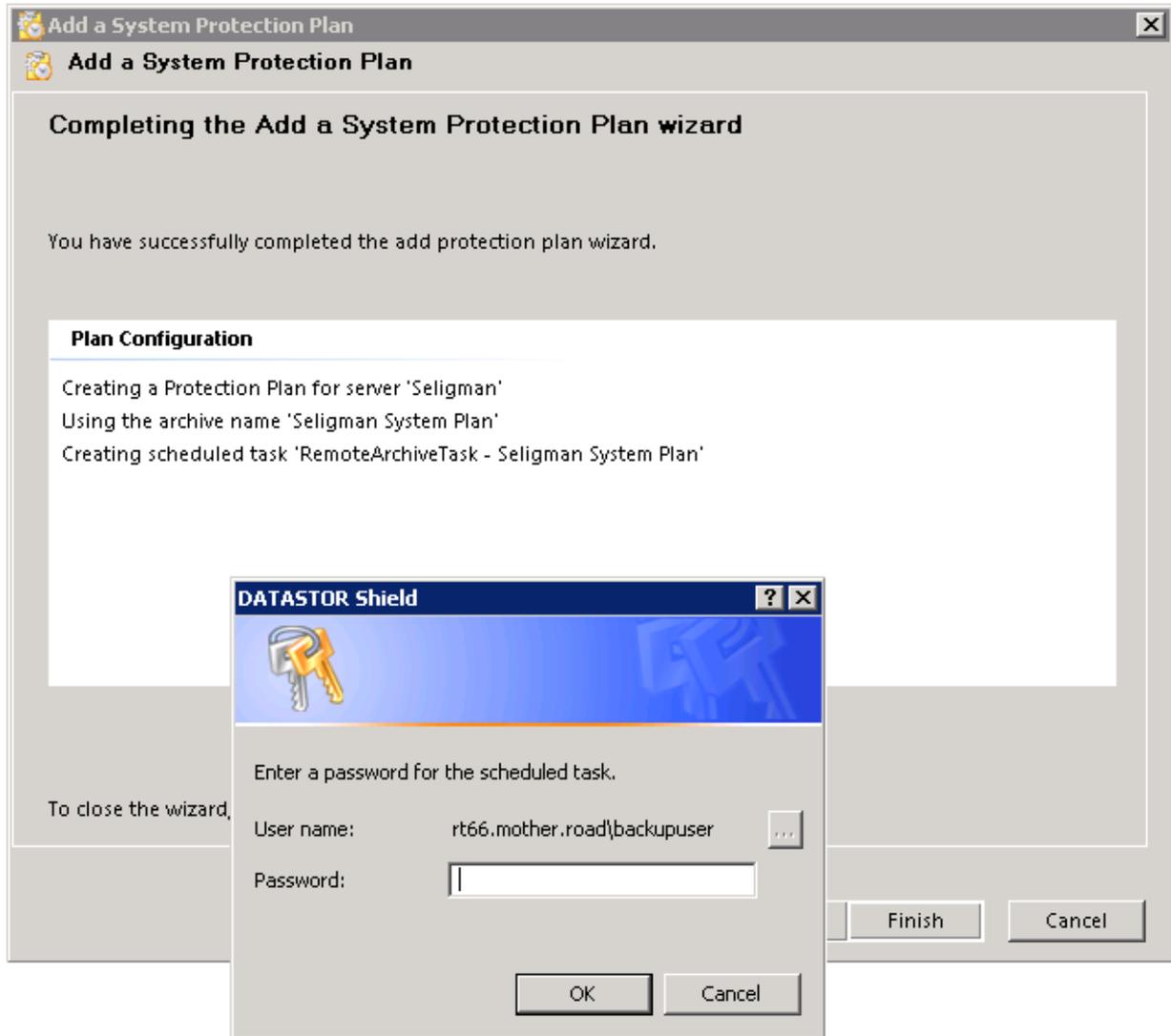
Seligman System Plan

< Back Next > Cancel

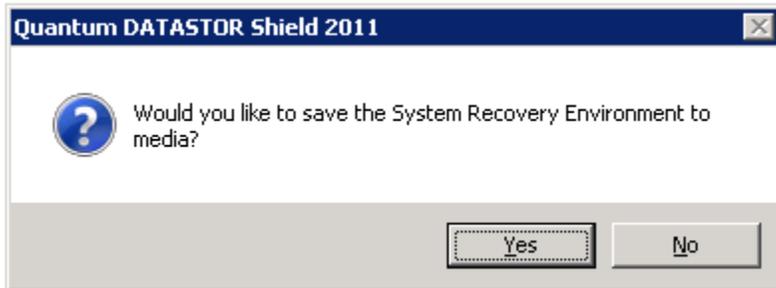
Next, select a schedule for running the protection plan. A typical schedule for a system protection plan is to run daily or weekly after business hours. The security options section specifies a user account to use to run the plan. A good practice is to create a single domain administrator account to run all of the protection plans in the environment.



Finally, click “Finish” to complete the wizard or “Back” to review or change any of the plan settings before saving the plan. Note: You will be prompted for a password to save for the plan “run as” user before the plan is saved to the system. Enter the password and click OK to save the plan.

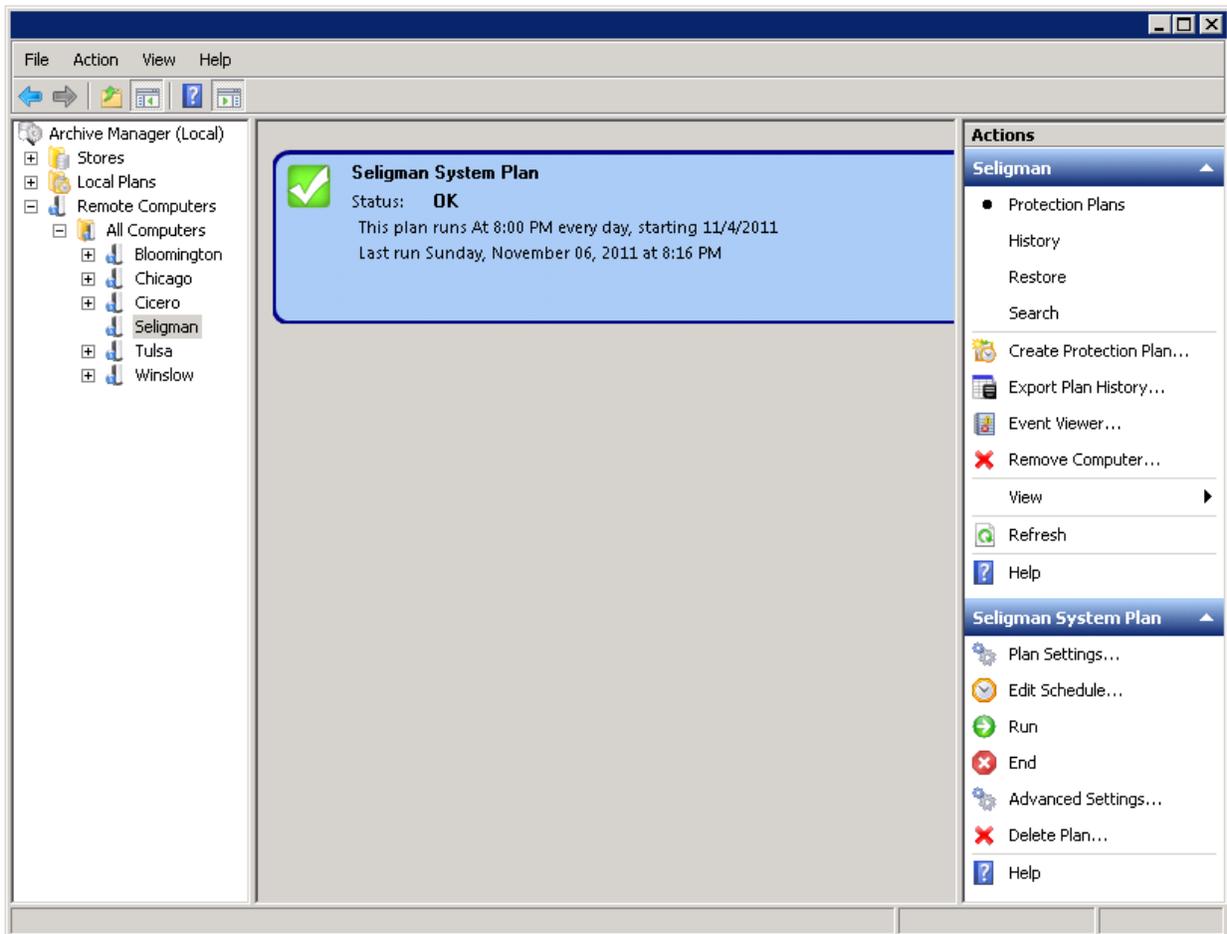


After the plan is saved a dialog box appears asking if you would like to save the System Recovery Environment (SRE) to media. This dialog serves as a reminder to save the SRE before it is needed.



Running the Protection Plan

When creating a protection plan you can schedule the plan to run Daily, Weekly or Monthly at a specific time. A summary of the schedule and most recent run status is visible from the Protection Plans view when either "Local Plans" or a remote computer is selected in the Archive Manager console.

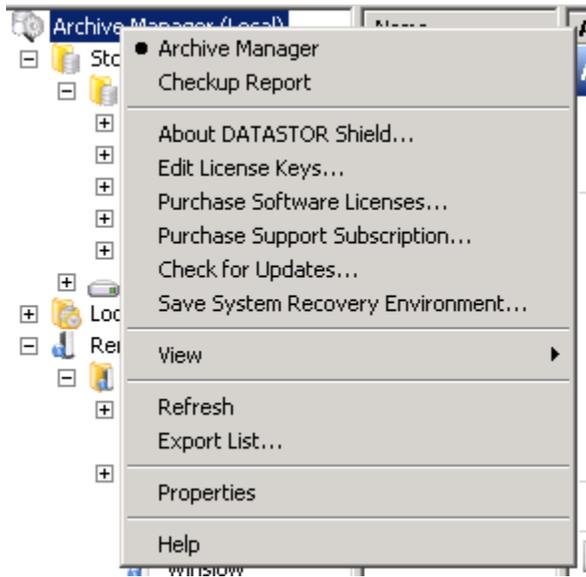


After the plan is created you can choose one of the following actions to review or modify how and when the plan runs; "Plan Settings", "Edit Schedule", "Run", "End", "Advanced Settings" or "Delete Plan". You

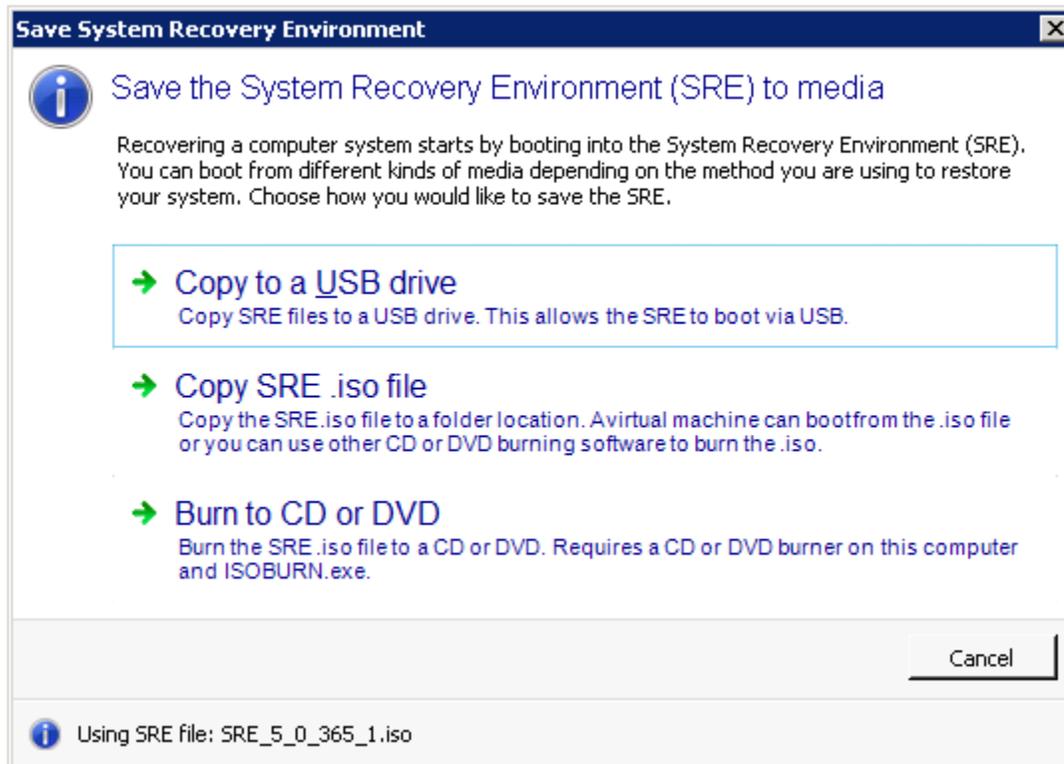
can always run the manually plan, without a schedule, using the Run action. For more information on these actions select the “Help” action for the selected plan.

Saving the System Recovery Environment to Media

Bootable System Recovery Environment media must be prepared for use with a System Recovery Protection Plan restore point during a system recovery. There are two ways to save the System Recovery Environment (SRE) to media. First, at the end of the Add a System Protection Plan wizard the user is prompted whether or not to save the SRE to media. Second, a “Save System Recovery Environment” action on the Archive Manager node of the console launches the Save System Recovery Environment dialog.

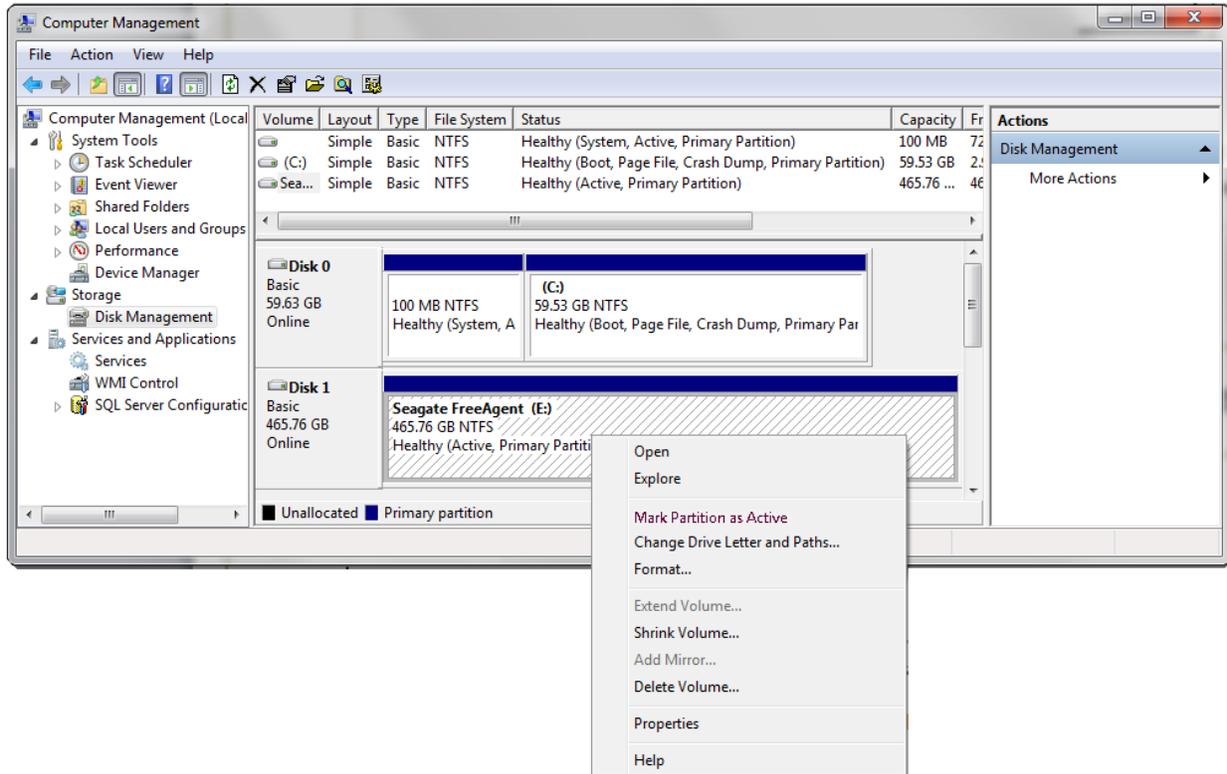


Using either method, the user is presented with a dialog with options to save the SRE to different types of media: USB, ISO formatted file, or CD/DVD.



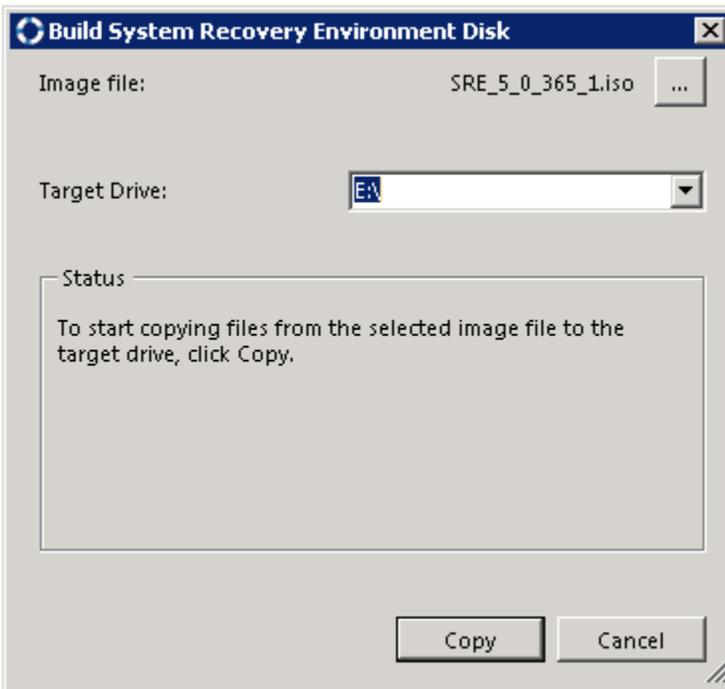
Copy to a USB drive

Selecting “Copy to a USB drive” presents a dialog with the image file to copy and a list of USB drives connected to the system to use as a target for the copy. Only the first partition on a USB drive can be used and the partition on that drive should be set to active using disk manager or the DISKPART utility to allow the USB drive to boot a system



When copying to a USB drive the existing data is preserved, the drive is not formatted. The required files to make the drive bootable with the SRE are copied to the drive.

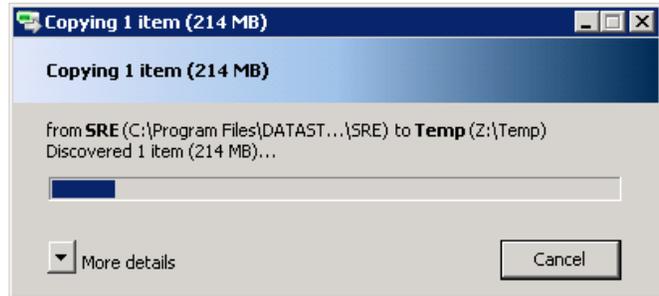
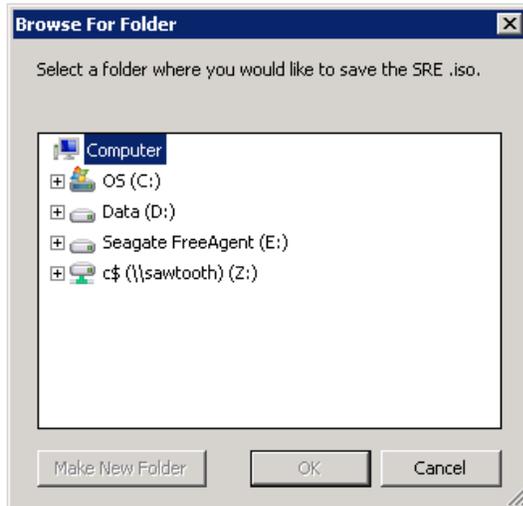
Click Copy when you are ready to copy the information to the target drive. When the copy completes click “Cancel” to close the dialog.



Copy SRE .iso file

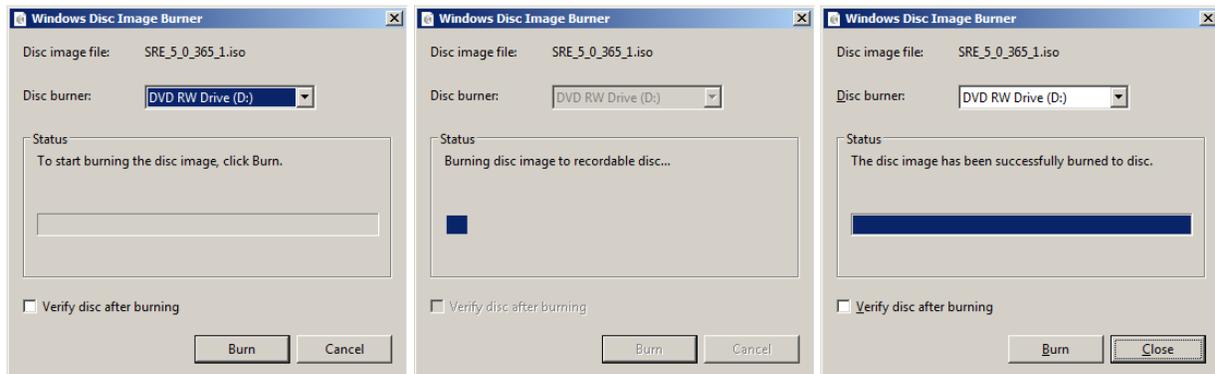
Selecting “Copy SRE .iso file” presents a “Browse For Folder” chooser dialog allowing you to specify a location to save the SRE .iso file. You can choose a folder on a local or mapped drive. Once you choose a folder and click “OK” the copy starts with a progress bar.

The SRE .iso file is an ISO formatted file that can be used for booting virtual machines. Most virtual machine hypervisors allow a user to configure a virtual machine to boot from CD/DVD devices or ISO formatted files. Another use for copying the SRE .iso file to a folder is to use a CD/DVD burner on another computer using 3rd party burning software or isoburn.exe on a Windows 7 or Windows 2008 R2 computer.



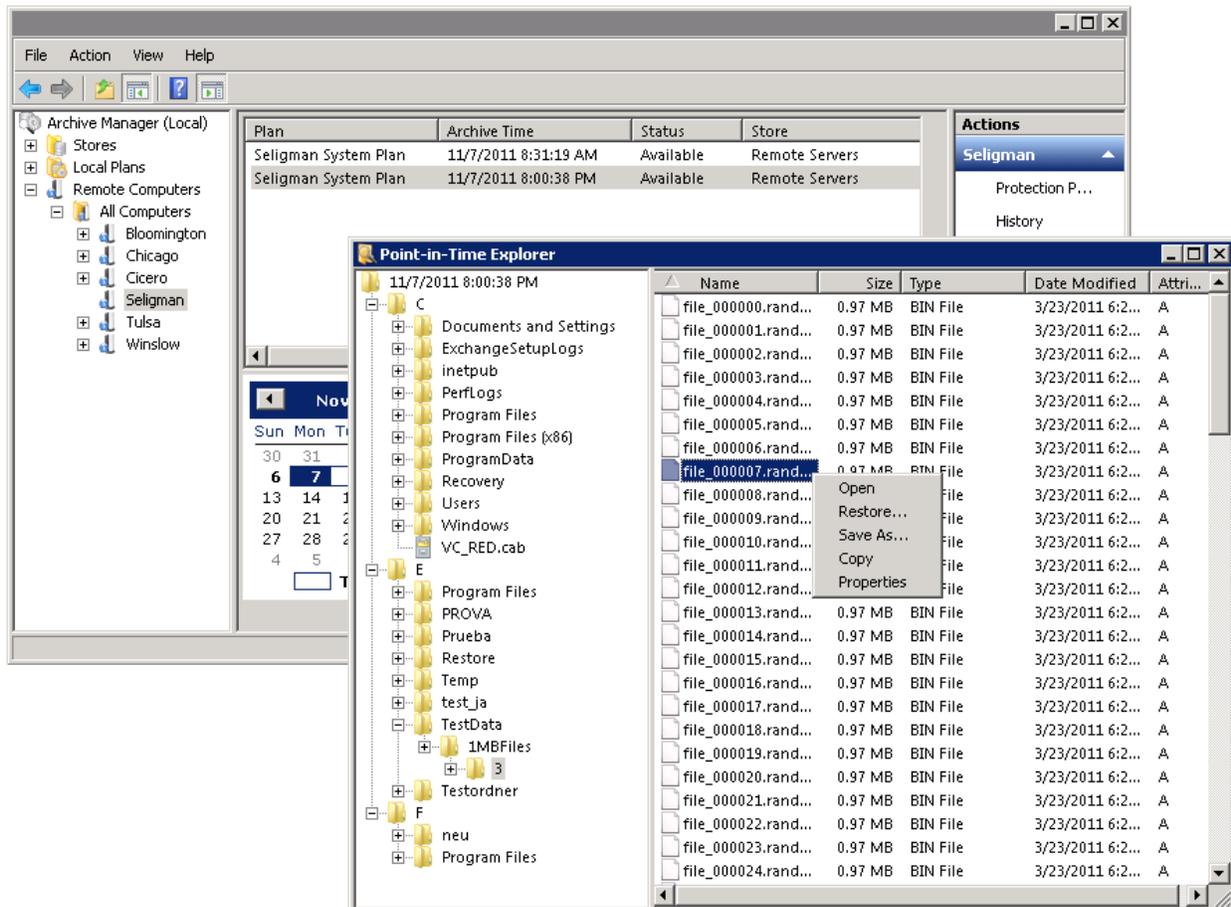
Burn to CD or DVD

Selecting “Burn to CD or DVD” presents the Windows Disc Image Burner dialog box allowing you to burn a bootable CD or DVD using one of the installed CD or DVD burners on your computer. This option is only available if the program Windows Disc Image Burner (isoburn.exe) is installed on your computer. Isoburn.exe is installed by default on Windows 7 and on Windows 2008 R2 systems that have the Desktop Experience feature installed.



Restoring Data from a Computer System Protection Plan

The Computer System Protection Plan stores all of the system information to restore a computer, as well as the system data and, optionally, some or all of any attached Data disk volumes. This plan type is not limited to full system recovery, however. You can restore individual files or folders from the plan from the Restore view for “Local Plans” or a remote computer by selecting a recovery point in the list and selecting either “Explore” to view a familiar files and folders listing of the recovery point or “Restore” to restore all of the data from the recovery point to an alternate location. These two methods only restore the data from the backup. You must use the System Recovery Environment to restore an entire system.

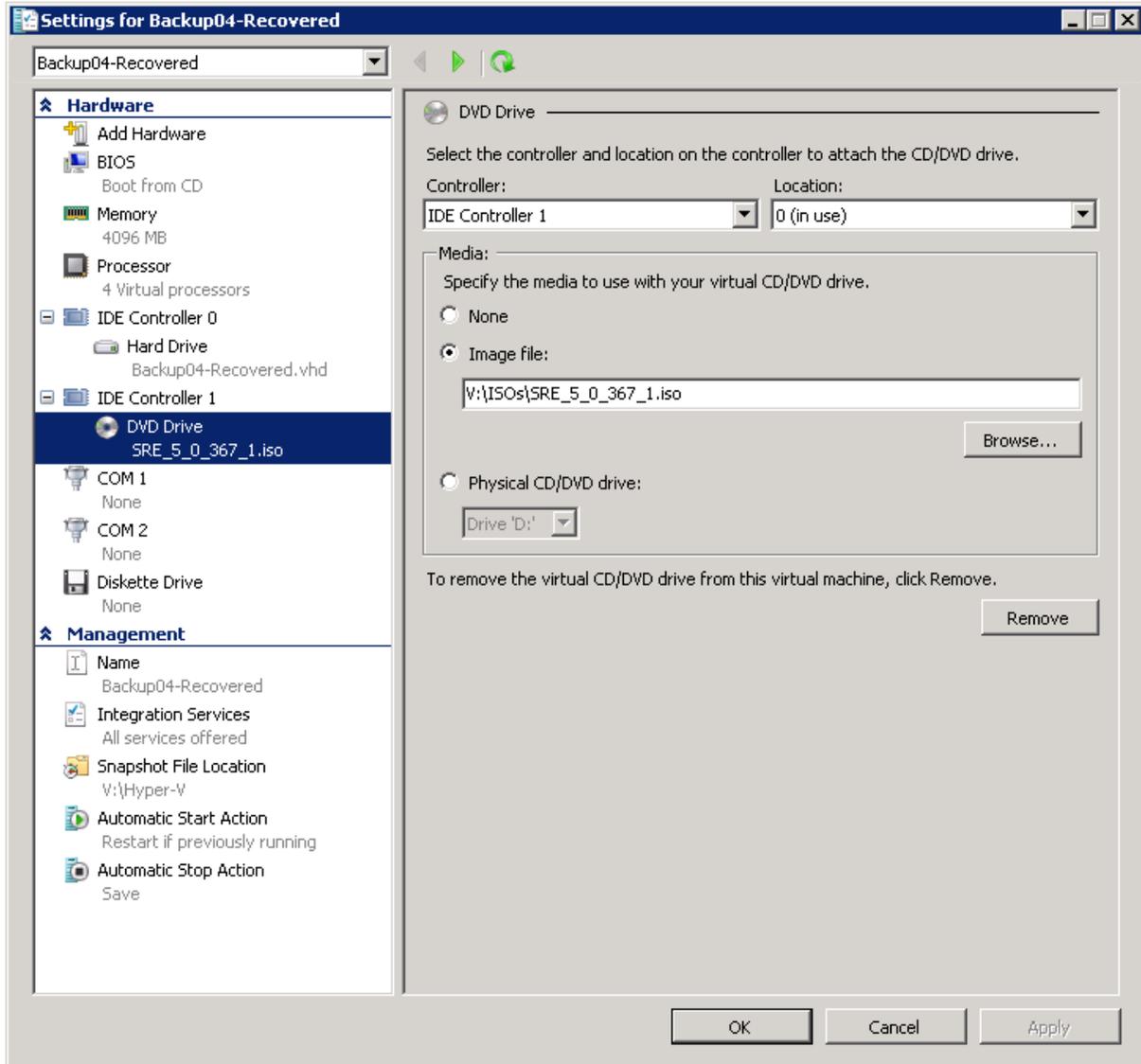


Booting a Computer for Recovery

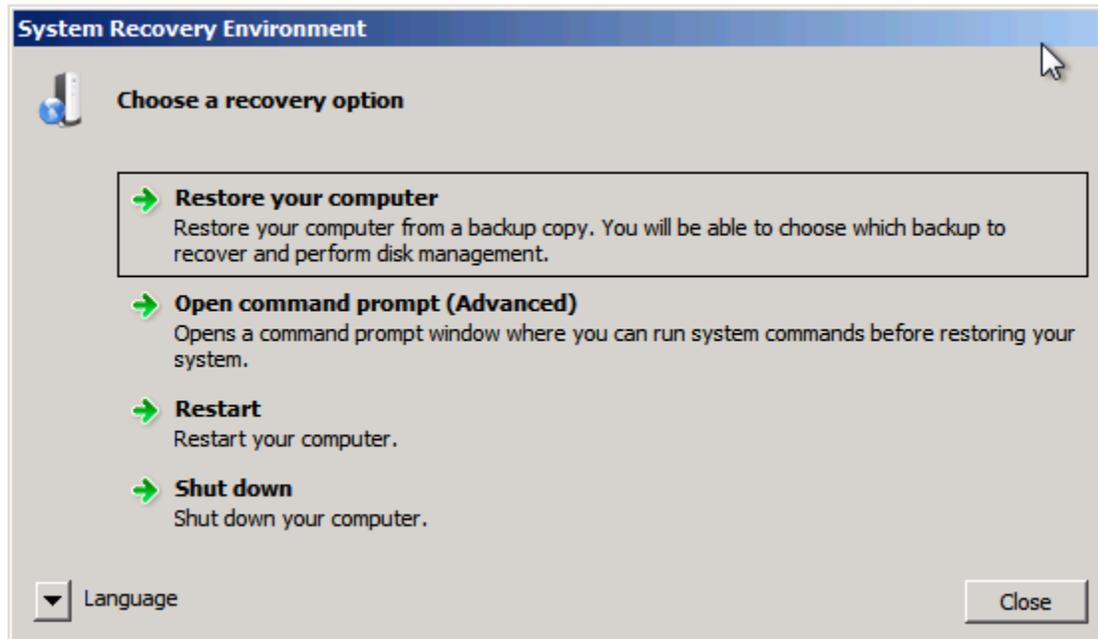
The System Recovery Environment (SRE) is used to boot a computer that needs to be recovered. Most modern computer systems can boot from CD/DVD or USB drives. Check your computer specifications and BIOS support for booting from CD/DVD or USB drives. You may have to select the boot drive from a boot menu at start up or adjust the BIOS to have the system choose to boot from a CD/DVD or USB drive.

Virtual machine hosts, sometimes referred to as hypervisors, allow a virtual machine (VM) to be configured to boot from a physical CD/DVD drive with bootable media inserted or a virtual CD/DVD drive linked to an ISO image file (.iso extension). To recover a VM using the SRE, configure the VM to boot

from CD/DVD media or copy the SRE ISO file to the hypervisor and configure the system to boot from an ISO file as a CD/DVD drive. The picture below is an example of configuring a VM with Microsoft Hyper-V to boot from an ISO file.



Once you boot the SRE you are presented with the SRE Launch screen. This screen is the home screen for the SRE and allows the user to initiate restoring a system with a step-by-step system recovery wizard, use advanced tools to change system configuration through the command prompt, shut down or restart the computer.



Most system restores can be run without requiring the use of the command prompt. There are several reasons for using the command prompt, for example you can set an IP address for a network adapter using the netsh command, if a DHCP server does not provide one.

Restoring your Computer System

From the SRE Launch screen, select “Restore your computer” to start a step-by-step wizard to specify which system you would like to restore and execute the system restore.

The first step is to help the wizard find stores and archives that contain recovery points produced by running Computer System Protection Plans. There are two locations the wizard can search to find recovery points--local disks and network locations. Local disks could range from USB drives (e.g. RDX) to direct attached storage (DAS), to iSCSI connected disks. Network locations are shares on an Archive Manager computer that have stores shared for remote access.

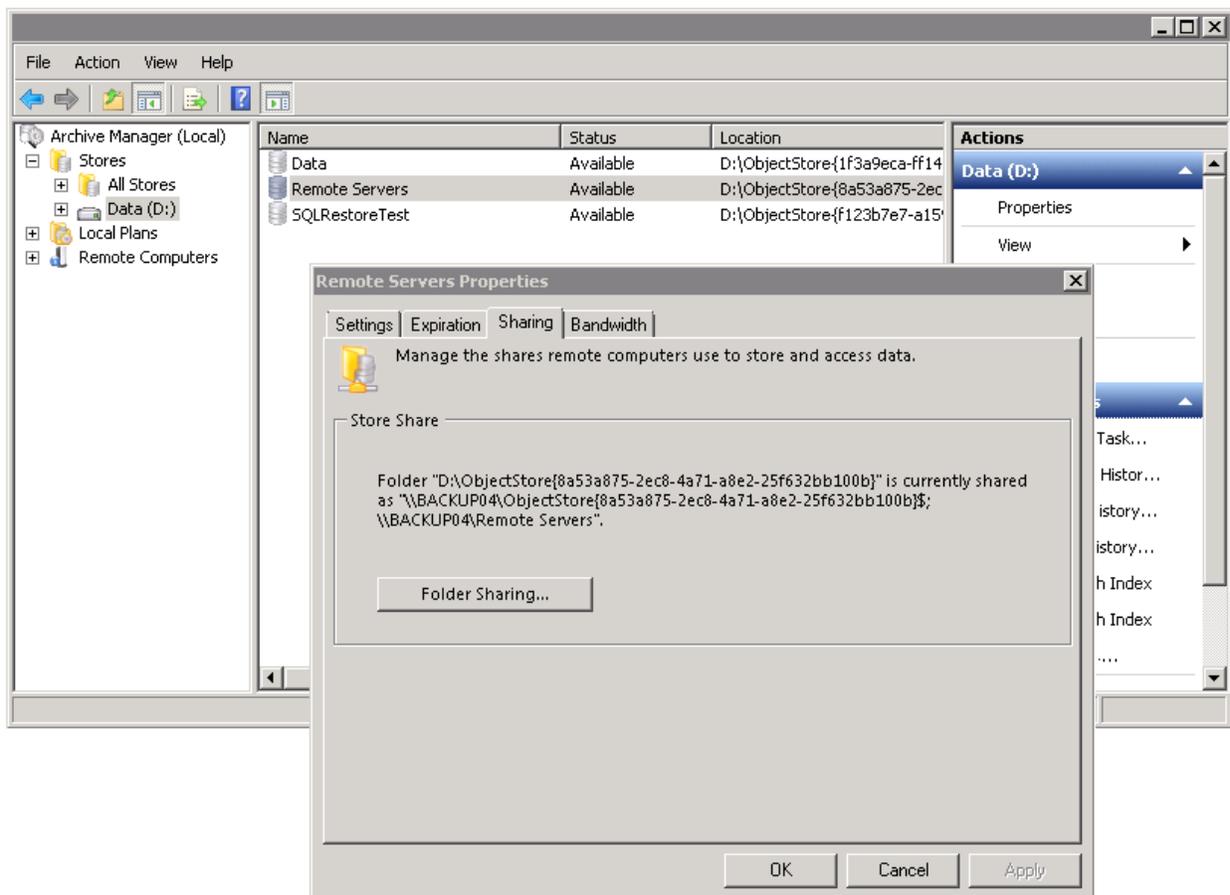
NOTE: To search network locations, the SRE has to be able to bind to a network adapter. At boot time the SRE searches all of the network drivers to find a match for your hardware. If a network driver is available and compatible with your system it is loaded and attempts to obtain an IP address using DHCP. If a network driver cannot be loaded by the SRE you can click “Load Driver” to browse for a 32-bit

network adapter driver compatible with your system. Once the network adapter driver is loaded, the driver attempts to obtain an IP address using DHCP.

If you click “Search local disks”, the disk drives attached to the system are scanned for possible systems to recover.

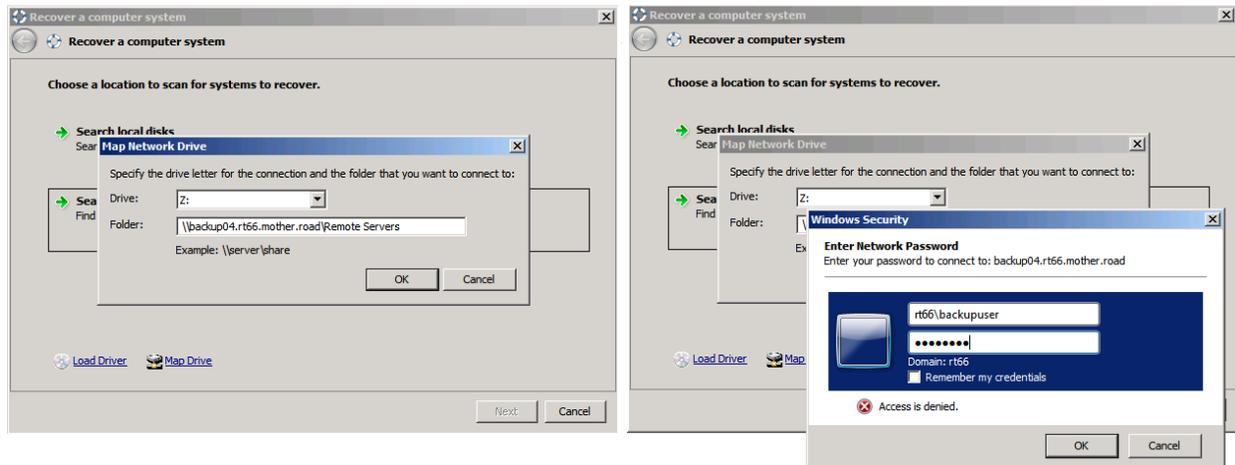
If you click search network locations you are prompted to map a network drive letter to a UNC path. There are two ways to connect to the shares on an Archive Manager server, a specific store share or the administrative share for a drive where one or more stores reside. The simplest way is to use the administrative share, because the wizard searches all stores on the drive for possible systems to recover. For example, if your stores are on the D drive of your archive manager server you can specify \\<archive manager>\D\$ as the folder.

Otherwise, you can see the share name for an object store by right-clicking the object store in the Archive Manager console and selecting the “Properties” action. The “Sharing” tab has a list of the possible shares you can use for the store.

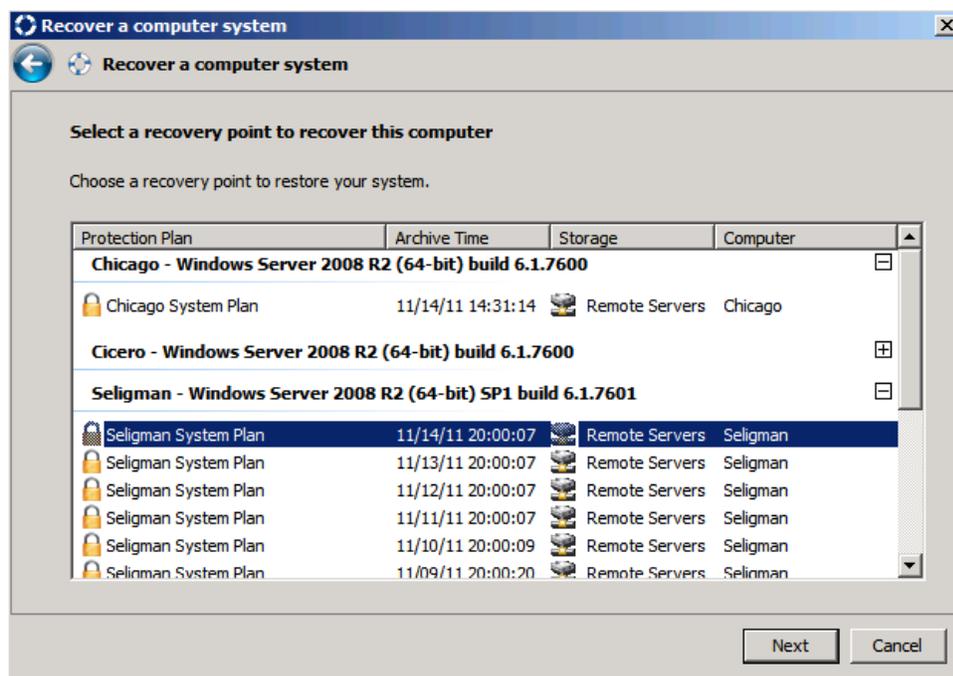


Once you find which share to map enter the path to the shared folder and click “OK” and enter the credentials for the user account that can access the store and click “OK”.

Note: Use the same account for accessing the store through a network folder that you use for your protection plans.



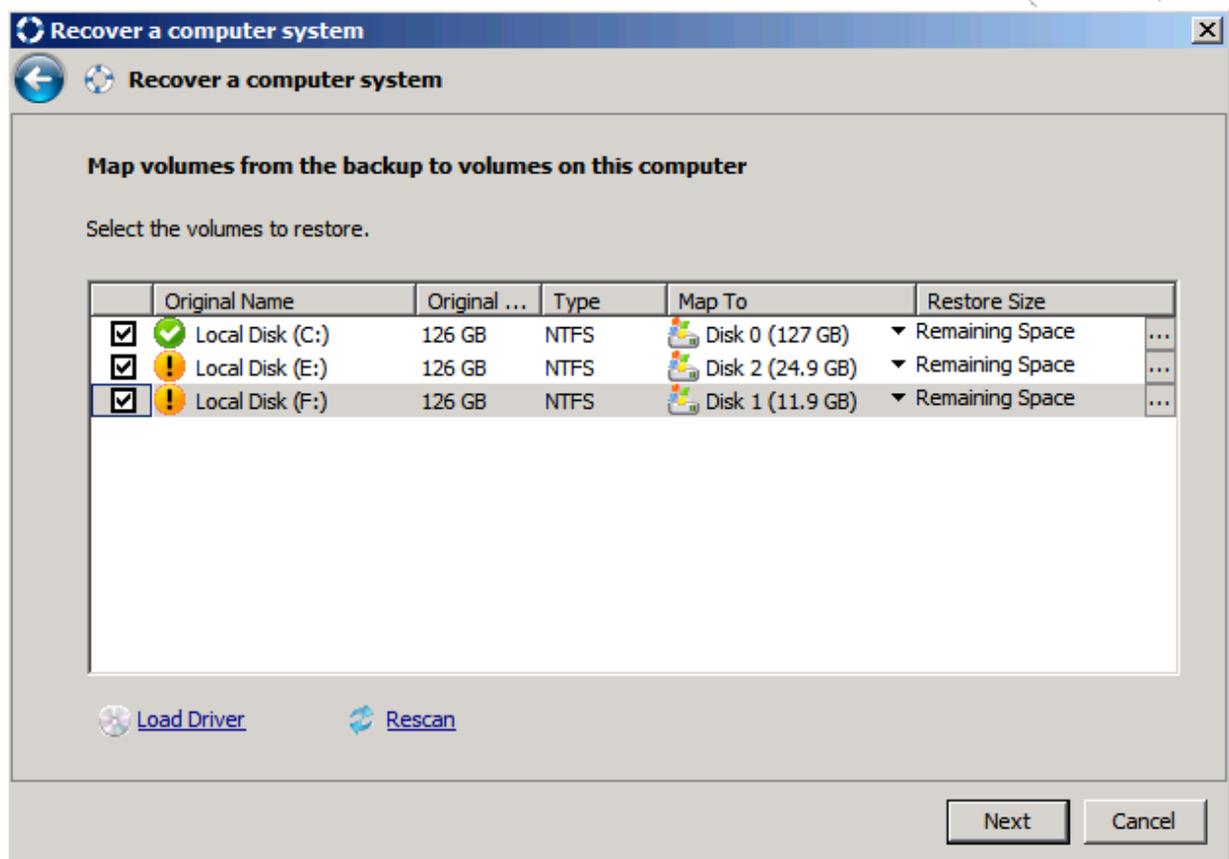
Next, choose the system, system plan and the recovery point to use for recovery. Each system that has recovery points available in the stores that were found is displayed in the list as a group. The system name, OS version and build are displayed. Clicking the + symbol to the right of each group displays the available recovery points for the server. Each recovery point lists the name of the protection plan that created the recovery point and the time the protection plan ran. Select the recovery point you would like to restore to the computer and click “Next”.



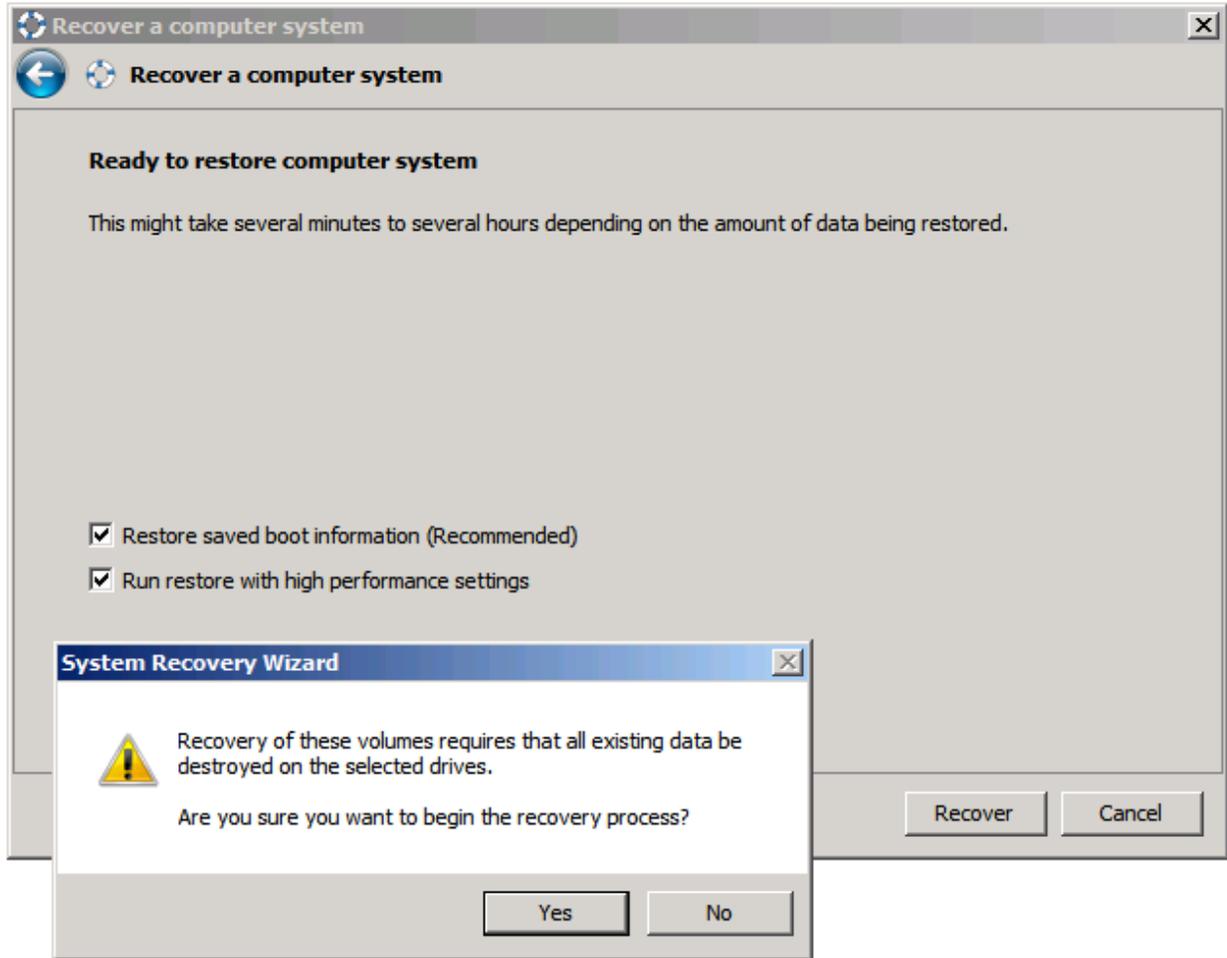
Next, configure the volume-to-drive mapping for the restore. The volumes that were selected by the protection plan are displayed with the original drive letter, label, capacity, and file system type. Check the first drive you would like to restore. The “Map To” column will automatically choose the first disk drive attached to the system and specify to use the “Remaining Space” on the drive. If this is not the desired mapping you can change the disk you would like to map the volume to from the drop-down menu in the “Map To” column. You can change the size of the volume that will be created on the drive by selecting the ... button in the “Restore Size” column. A good volume-to-drive mapping will have a checkmark icon. If the volume mapping you have specified is smaller than the original capacity, the mapping will have a warning icon.

Note: if no drives are displayed in the window for volume mapping you may need a driver for a storage controller installed in your computer. If you need to load a driver click “Load Driver” and browse to a location containing a compatible 32-bit driver. Once the driver is installed, click “Rescan” to scan for drives to map to volumes.

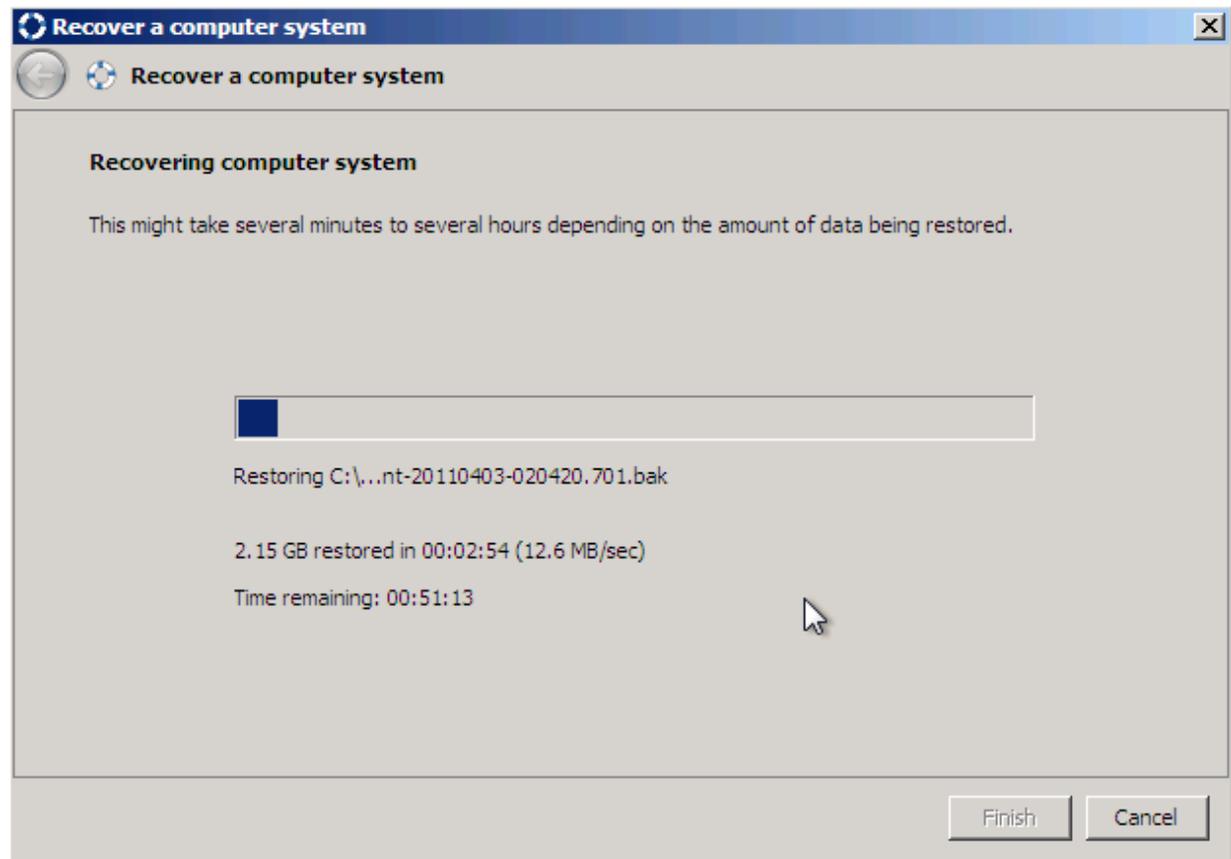
Once you are satisfied with your mappings click “Next”.



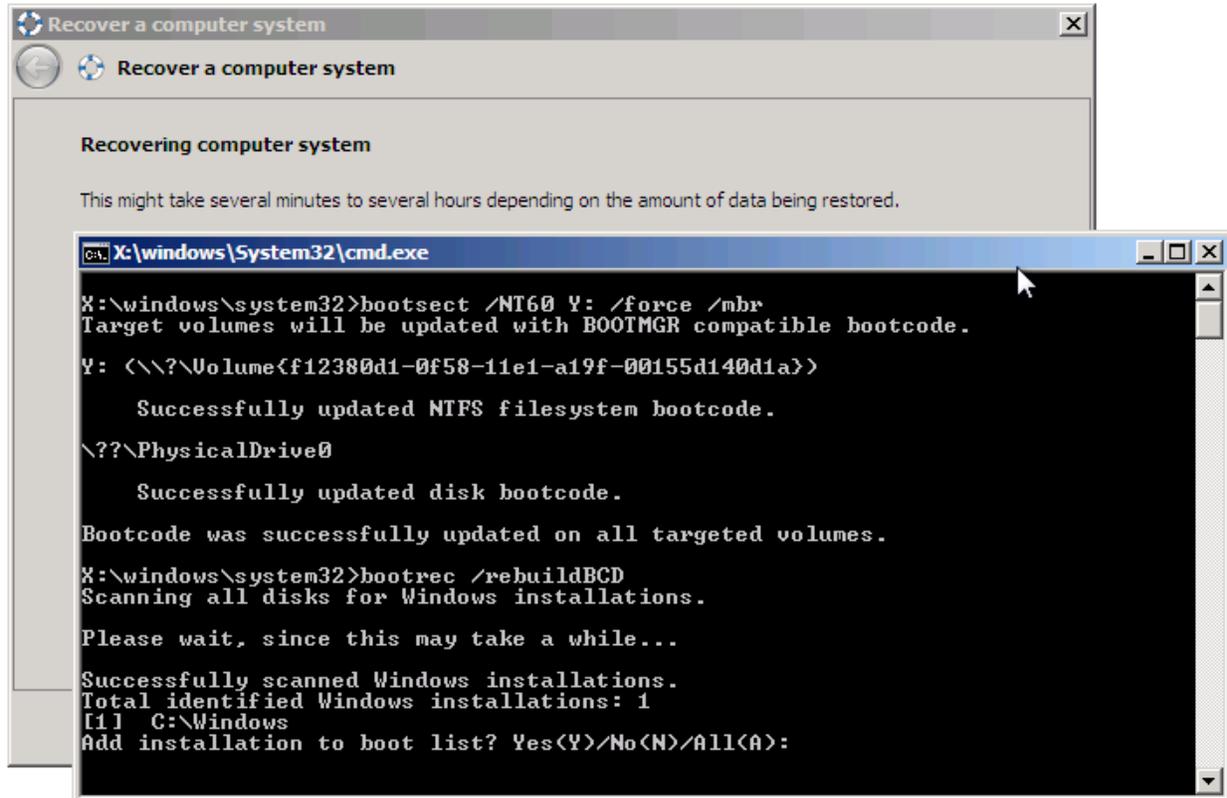
Next confirm that you are ready to start the restore. There are two options on this page, whether or not to restore the boot information and whether or not to restore with high performance settings. When you are ready to begin the restore, click “Next”. You will be warned that the data on the existing volumes will be destroyed, click “Yes” to continue or “No” to return and change your settings.



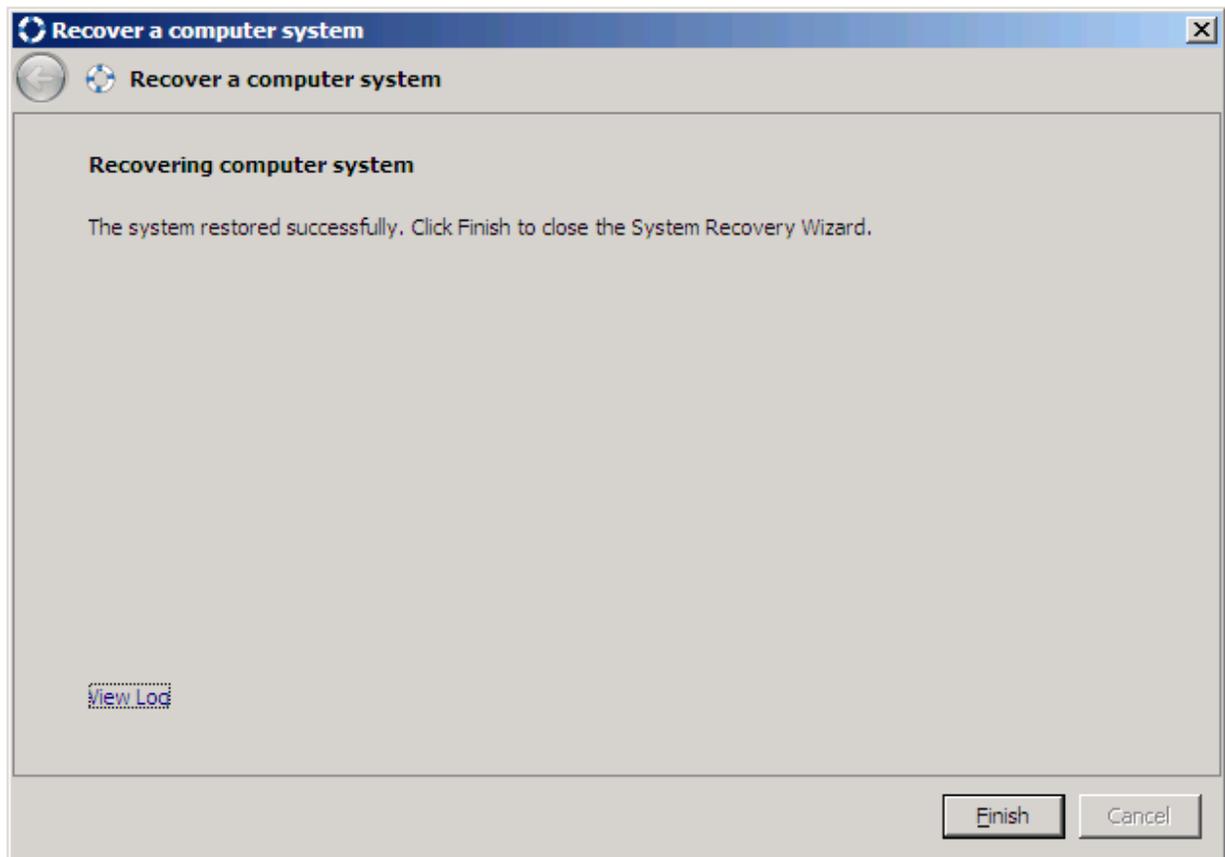
While the restore is running, you can monitor the throughput and an estimate when the restore will finish based on throughput.



After the files are restored for the operating system a command prompt window opens. You will be prompted to restore the boot information for each Windows installation found on the disk drives of the computer. Respond with "Y" or "A" in the window to complete repairing the boot device on the system. If you do not repair the boot device the restored system may not boot.



When the restore is finished you can view the restore log or click Finish to return to the SRE Launch screen.



Once back at the launch screen, you can choose to restart the computer and boot into the restored OS.

Note: You may need to adjust your BIOS boot menu if you changed it during the recovery process.

