

EVault System Restore

Version 8.0

User Guide



Revision: This manual has been updated for version 8.0a (March 2016).

Software Version: 8.0a

© 2016 Carbonite, Inc.

Carbonite makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Carbonite reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Carbonite to notify any person of such revision of changes. All companies, names and data used in examples herein are fictitious unless otherwise noted.

No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval System or translated into any language including computer language, in any form or by any means electronic, mechanic, magnetic, optical, chemical or otherwise without prior written permission of:

Carbonite, Inc.
Two Avenue de Lafayette
Boston, MA 02111
www.evault.com

Carbonite, EVault Software, EVault SaaS, and EVault DeltaPro, are registered trademarks of Carbonite, Inc. All other products or company names mentioned in this document are trademarks or registered trademarks of their respective owners.

Acknowledgements: Two encryption methods, DES and TripleDES, include cryptographic software written by Eric Young. The Windows versions of these algorithms also include software written by Tim Hudson. Bruce Schneier designed Blowfish encryption.

“Part of the software embedded in this product is gSOAP software. Portions created by gSOAP are Copyright 2001-2006 Robert A. van Engelen, Genivia Inc. All Rights Reserved. THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.”

The EVault Software Agent, EVault Software CentralControl, and EVault Software Director applications have the encryption option of AES (Advanced Encryption Standard). Advanced Encryption Standard algorithm (named Rijndael, pronounced “Rain Doll”) was developed by cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen. This algorithm was chosen by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce to be the new Federal Information Processing Standard (FIPS).

The EVault Software Agents and EVault Software Director applications also have the added security feature of an over the wire encryption method.

Contents

1	Introduction	5
1.1	Features.....	5
2	Requirements and Support	6
2.1	Supported Operating Systems	6
2.2	Supported File Systems	6
2.3	Supported Storage Types	6
2.4	Supported Disk Layouts.....	6
2.5	Supported OEM Partitions	6
2.6	Limitations.....	7
3	Creating a Bootable Image	8
3.1	BMC Installation and Requirements	8
3.2	Obtain a Windows Assessment and Deployment Kit (ADK).....	8
3.3	Specify Drivers for the Image	9
3.4	Build the Image	10
4	Creating a Bare Metal Restore Backup.....	11
5	Launching and Running EVault System Restore.....	12
5.1	Running the Application.....	13
5.2	EVault System Restore - Main Menu	13
6	Restore My System.....	15
6.1	Restore Wizard.....	15
6.2	Basic Disks and Dynamic Disks	27
6.3	Recovering a Dynamic Disk to a Basic Disk	28
7	Repair My System.....	29
7.1	HAL and Kernel Repair	30
7.2	Boot-Critical Device Repair	30

8	Restore Test-Run	32
9	Configuring Settings.....	33
9.1	Network Settings.....	33
9.2	Disk Settings	36
9.3	All Devices Tab	37
9.4	Driver Installation.....	38
9.5	Log Settings	38
10	Appendix.....	40
10.1	Configuring Advanced Vault Settings.....	40
10.2	Restoring Operating Systems with OEM Licenses.....	40
10.3	Restoring to UEFI Systems	40
10.4	Creating BMR Backups	41
10.5	Restoring Applications such as SQL Server and Oracle.....	41

1 Introduction

The EVault System Restore (ESR) application provides disaster recovery for Windows-based computers. ESR can restore your entire system, including the operating system, applications, System State, and data. You can restore from Bare Metal Restore (BMR) backups to dissimilar hardware, and even virtual machines. ESR can help you avoid a manual bare metal recovery process, which can be time consuming and error-prone.

Protected System: This is the source system, which needs to be protected from catastrophic failures. On this system, a backup application must be installed, and backups created.

Target System: This is the receiving system, which might be in a “bare metal” state, or might contain existing information that will be lost (overwritten) on a restore. You need to run ESR on this target system. It will restore the backed up image, and then the system can be started (rebooted).

Note: In some cases, you might not be able to restore if the target hardware is incompatible with the source OS.

EVault System Restore enables you to:

- Restore your system to similar, dissimilar or virtual environments
- Restore your system to a selected point in time
- Restore from file-based backups
- Restore from local backups or backups stored on the vault
- Choose your boot media. You can boot from CD, DVD, USB, or a network.

This user guide is intended for IT administrators who are responsible for performing backup and recovery operations.

1.1 Features

- Ability to restore from BMR backups created using the Windows Agent or the Image Plug-in
- Ability to restore volumes from non-BMR backups created using the Image Plug-in
- Bootable Media Creator (BMC) utility for creating an ESR ISO image
- Support for Unified Extensible Firmware Interface (UEFI)
- UEFI to UEFI restores
- BIOS to UEFI restores

Details about restoring to UEFI systems are available in the [appendix](#) of this guide.

2 Requirements and Support

EVault System Restore requires CPU and RAM to meet the basic requirements of your operating system, as prescribed by Microsoft.

You might also need specific hardware:

- Network interface card (required if you will use a network to restore from a vault)
- USB port (required if you will restore from data that has been exported from a vault)

For detailed information about requirements, please refer the latest release notes.

2.1 Supported Operating Systems

Please refer to the latest release notes.

2.2 Supported File Systems

This version of ESR supports NTFS for recovery of Windows and data volumes.

The application also supports FAT and FAT32 for volumes that are required for the boot process.

2.3 Supported Storage Types

- Vault
- SAN
- USB drives
- NAS
- DAS

2.4 Supported Disk Layouts

- MBR
- GPT

2.5 Supported OEM Partitions

- 0x12 // EISA partition (Compaq)
- 0x84 // Hibernation partition for laptops
- 0xA0 // Diagnostic partition on some Hewlett-Packard notebooks
- 0xDE // Dell partition
- 0xFE // IBM IML partition

Note: Encrypted volumes (BitLocker, TrueCrypt, etc.) are not supported for BMR jobs.

2.6 Limitations

ESR is not supported on 32-bit hardware.

ESR is not supported on VMware ESX 4.x.

You cannot restore UEFI backups to Generation 1 Hyper-V virtual machines. Generation 1 Hyper-V virtual machines do not have support for UEFI.

3 Creating a Bootable Image

Before you start using EVault System Restore, you need to create an ISO (.iso) image. You can then use the image to start (“boot”) a computer and restore from a BMR backup.

To create the ISO image, use the Bootable Media Creator (BMC) utility. This utility allows you to create a new ISO image, or inject drivers into an existing image.

BMC produces an image whose file name is:

System-Restore-`<version number>`.iso

where `<version number>` is the version number of the ESR application that is included in the image.

3.1 BMC Installation and Requirements

For supported operating systems and detailed requirements, please refer to the latest release notes.

BMC is available as a self-extracting installation (.exe) file. You can obtain this file from your service provider. To install BMC, run the .exe file.

BMC requires the Windows Preinstallation Environment (WinPE), which is a component of the Windows Assessment and Deployment Kit (ADK). The ADK must be installed before you can create an image using BMC.

For supported ADK versions, see the EVault System Restore release notes.

3.2 Obtain a Windows Assessment and Deployment Kit (ADK)

A supported ADK version must be installed before you can create an image using BMC.

You can download the ADK from Microsoft. When you launch the BMC utility, the software detects whether or not your system has a supported ADK version. If a supported ADK version is not found, a screen opens for ADK installation.

- To download the ADK from Microsoft, simply click the **Download** button.
- To use an existing version of the kit, click the **Browse** button. Navigate to the location of the kit, select the **ADKSetup.exe** file, and click **Open**. You are then returned to the BMC screen.

Click the **Install** button. The **Specify Location** screen opens.

- To install the ADK in the default location, click **Next**. The Microsoft **Downloading features** screen opens, showing you the download progress.
- Otherwise, click one of the **Browse** buttons to either install the kit on your computer, or download the kit to a separate computer. Navigate to a folder for the installation, select it, and click **OK**. Click **Next**.

On the **License Agreement** screen, read the terms of the agreement. To accept the terms of the agreement, click **Accept**. Otherwise click **Decline** or **Back**.

If you click **Accept**, a feature selection screen might open. If this screen opens, select **Windows Preinstallation Environment (Windows PE)**, and click **Install**.

Next, the Microsoft **Installing features** screen opens, showing you the installation progress.

3.3 Specify Drivers for the Image

When you have a supported ADK version installed and open, you can start to create a bootable ESR image. The image should include Original Equipment Manufacturer (OEM) drivers for the devices that are present in the target system (but not devices that are included in the *Windows Hardware Compatibility List*).

On the BMC **Build Bootable Media Image** screen, you need to choose between these options:

- **Create new image**
- **Modify existing image**

To create a new image:

1. Click **Create new image**.
2. Click **Add**. Navigate to the location of a driver that you want to include, select its folder, and click **OK**.
3. Using the **Add** and **Remove** buttons, continue to add or delete driver locations until the **Folder path** lists all of the drivers that you want.

To modify an existing image:

1. Click **Modify existing image**. The **Mounted image drive** box opens.
2. Enter the location of the image that you want to modify. Alternatively, click **Browse**, navigate to the location of the existing image, select its folder, and click **OK**.
3. Use the **Add** and **Remove** buttons to add or delete driver locations until the **Folder path** lists all of the drivers that you want.

Note that the folders you include can only contain **.inf** files. Also note that you only need to supply the drivers that are required to boot your system.

Here is a sample procedure to follow if you have several systems from Company A:

1. Download the driver files from Company A's website.
2. *Extract* the files to a folder called **Company_A** on your network.
3. When you create the image, include the **Company_A** folder.

3.4 Build the Image

In the **ISO image destination** box, enter the location where you want to build the image. Alternatively, click **Browse** so that you can find and select a destination for the image.

Click **Build Image**. The **Building Bootable Media Image** screen opens, showing a progress bar.

To stop building the image, click **Cancel**. An automatic cleanup operation begins. After the cleanup operation finishes, you can click **Cancel** or **Back**.

4 Creating a Bare Metal Restore Backup

Using EVault System Restore, you can restore from Bare Metal Restore (BMR) backups created using the Windows Agent or Image Plug-in. You can also use ESR to restore volumes from non-BMR backups created using the Image Plug-in.

For information about creating BMR backups using the Windows Agent or Image Plug-in, see the Portal online help, the *Agent for Microsoft Windows User Guide*, or the *Image Plug-in Guide*.

Note: To restore your system, you must have already created a backup image.

5 Launching and Running EVault System Restore

EVault System Restore is bundled as a bootable image. First you need to build an ESR ISO image using the [BMC utility](#). Then you use the image to start (“boot”) the target system and run the restore.

The types of bootable media that you can use include:

- CD/DVD – Burn the ISO image to a CD and make it bootable.
- USB – Similarly, a bootable USB device with the ESR application can be created by applying the ISO image to a USB device and making it bootable.
- Network boot – The ISO image can also be used to set up a PXE boot server.

To launch ESR using a CD/DVD:

- 1) Obtain the ESR CD/DVD that you have burned, and insert it into the drive of the machine that you want to restore.
- 2) Power on the system to automatically launch the ESR application.

Note: Make sure that the CD/DVD device is the first option in the boot order of the firmware (i.e., UEFI or BIOS). If you have another bootable device that is listed prior to the CD/DVD drive, ESR might not launch automatically.

To launch ESR using a USB boot:

- 1) Plug your USB device into the port on the system to automatically launch the ESR application.
- 2) Restart the computer.

Note: Make sure that the USB is the first option in the boot order of the firmware. The firmware must have built-in support for booting USB devices. If you have another bootable device that is listed prior to the USB drive, ESR might not launch automatically.

To launch ESR using a network boot:

- 1) Reboot the system that is being restored from the PXE boot ROM.

Note: Make sure the PXE option is enabled in the firmware. It is the user’s responsibility to take the WIM image and create a PXE server to enable network boot functionality. You must also provision the necessary hardware and software to enable the PXE server.

- 2) Press F12 to start the network service boot wizard when prompted.
F12 might not work on all systems. Follow the instructions on the screen.

Note: Before launching the application from the network, make sure that the DHCP server is set up in the network where the system being restored resides.

Note: A network card must be present in the system when the backup is taken and connected (by a network) to one in the remote system.

It might be helpful to refer to the appropriate Microsoft documentation describing how to enable PXE boot servers.

5.1 Running the Application

When you launch the application, a welcome screen appears.

- 1) Choose a time zone from the **Time zone selection** list. The restore points for backups are stored in UTC. When these restore points appear on screens, they are translated to the selected (local) time zone.
- 2) Choose a language from the **Keyboard selection** list.
- 3) Click **Next** to proceed. The **License Agreement** screen appears.
- 4) Read the license agreement for the EVault System Restore software.
- 5) Select the **I accept...** check box, or click **Reboot** if you do not wish to accept the terms/conditions specified in the license agreement. This will reboot the system, allowing you to exit properly from the ESR application.
- 6) If you accept the terms of the agreement, click **Next** to open the ESR main menu.

5.2 EVault System Restore - Main Menu



The **Main Menu** screen has two sections. The three options in the upper section allow you to perform restores and repair tasks. The options in the lower section allow you to configure settings, view logs, and reboot the system.

Restore/Repair Options



Restore My System: Allows you to initiate the process of restoring your system from its bare-metal state.



Repair My System: Allows you to repair your system by adjusting for dissimilar hardware configurations. Typically you would use **Restore My System** first, to copy the system volume and possibly other volumes to local disks. Then, if needed, you would be directed to run a repair. Optionally, if the system does not need to be restored (again), you can go directly to the repair wizard.



Restore Test-Run: Allows you to test the system recovery process without making actual changes to the system. It demonstrates that you can restore the system when necessary.

Additional Options



Settings: Allows you to configure settings for network devices, storage devices and logs on your system if they are not already correctly configured.

Show Log

Show Log: Allows you to view or save logs during the restore process.

Reboot

Reboot: Allows you to exit from the ESR application. You can then return to the restored system.

6 Restore My System

EVault System Restore allows you to restore your system after a crash. You can restore to a different system and adjust for differential hardware. If the target hardware supports the operating system of the system you are restoring, you should be able to restore (even, for example, if the disks are different).

You might need to configure some settings before you start restoring or repairing your system. For more information, please refer to [Configuring Settings](#).

You might not be able to restore if the target hardware is incompatible with the source OS. Some non-Intel or non-AMD processors, such as Itanium, might not restore to Intel/AMD processors.

Using EVault System Restore, you can only restore systems on 64-bit hardware. You can restore a supported 32-bit operating system on 64-bit hardware. To restore a system with a 32-bit operating system to a virtual machine, prepare a virtual machine with a 64-bit operating system. After the restore, switch the machine to the 32-bit operating system you restored.

When restoring a BMR backup to a destination in a virtualized environment (Hyper-V or ESXi), ensure that the VM configuration is compatible with the system that is going to be restored. Issues could arise when restoring to a mismatched destination. As well, ensure that your destination's BIOS/UEFI selection type matches what you intend to restore.

Use the **Restore My System** option from the main menu to start following the steps to restore the system to its previous, usable state, or to any point in time for which you have a backup.

Note: A restore must complete within 72 hours, or EVault System Restore will restart and the restore will fail.

6.1 Restore Wizard

Using the restore wizard, you can recover your system to:

- **Similar hardware**
- **Dissimilar hardware**
- **Virtual hardware**

To initiate the process of restoring, click **Restore My System** on the [main menu](#). The **System Restore Wizard** opens.

The wizard screen has two panes:

- **Left pane:** The left side of the restore wizard displays a quick view of the current stage in the restore process.

A *gray* area denotes a step that has not run yet.

A *black* area denotes the current step you are working on.

A *green* area denotes a step that has finished.

- **Right pane:** The right side of the restore wizard describes the steps of the restore process.

Click **Next** to start the restore process.

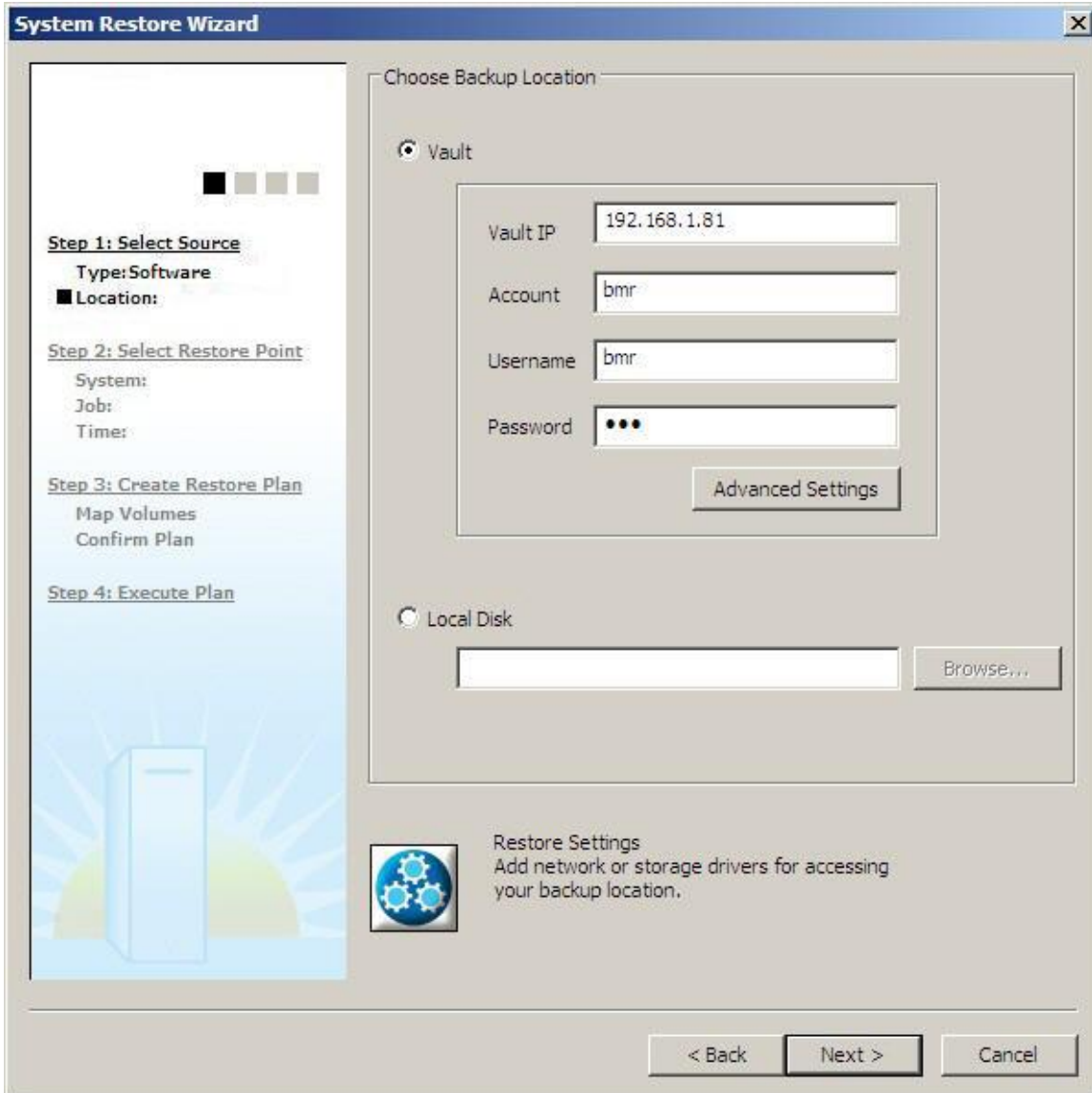
Step 1: Select Backup Source

The first step in the EVault System Restore process is **Select Source**. This step allows you to choose the backup type that was used to create your system backup, and the location where the backup is stored. You can restore your system from backups located on directly attached storage, or a vault, depending on your backup type. See [Creating BMR Backups](#) for more information about backup types.

To perform **Step 1: Select Source**

- 1) Select the required backup source type.

Note: The vault software backup service supports restoring from a local backup or a remote vault on the network.



The available backup locations are:

Local Disk: Choose **Local Disk** if the location of the backup image and the system that is restored are on the same locally attached device, such as a USB drive.

Vault: Choose **Vault** if the location of the backup image is a vault. (This is only enabled if you have chosen **EVault Software** as a backup source.)

- 2) Select **Local Disk** or **Vault**, depending on the location of the backup. If you choose **Local Disk**, click **Browse** to locate the image to be restored.

If the backup is located on a vault, choose the **Vault** option. To connect to the vault, enter these attributes:

Vault IP: Vault IP is the host IP address. (Or you can use the host name, if DNS is available.)

Account: Your account, created in the vault for accessing the backup image.

Username: User name for logging into the vault to access the backup image.

Password: Password for logging into the vault to access the backup image.

To configure settings for the vault, click **Advanced Settings**. Refer to [Configuring Advanced Vault Settings](#) for details.

3) Click **Next** to proceed with the restore process.

Step 2: Select a Restore Point

The second step in the system restore process is to select a restore point.

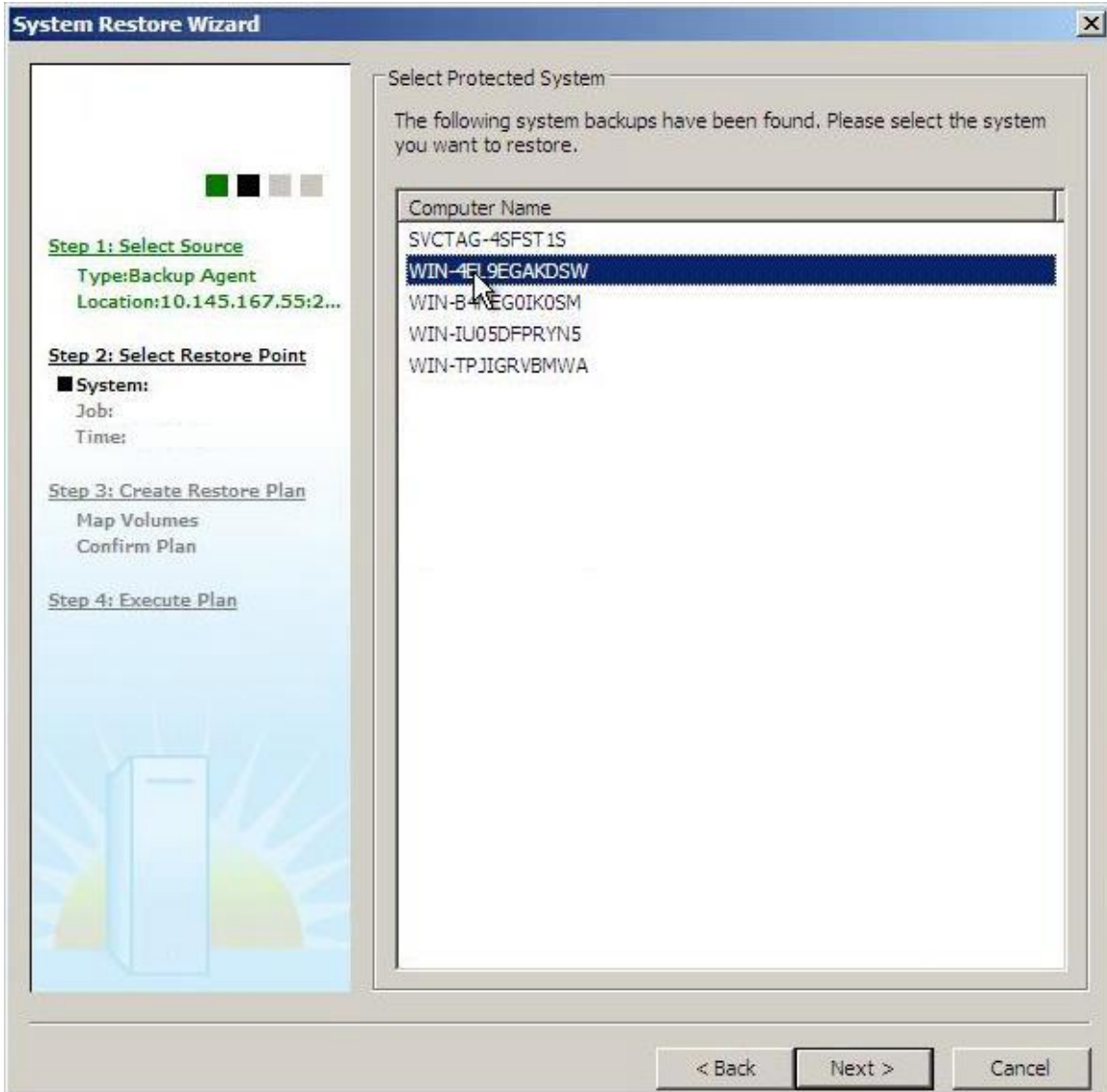
Click **Next** on the **Select Source** screen to access the **Select Restore Point** screen.

This step comprises the following:

Select Protected System: Select the protected system that you want to restore. You will only be able to see computers for which BMR backups have been created. Other backups that are not BMR will not be shown.

Select Backup Job: Select the backup job that you want to restore from the list of available backup jobs.

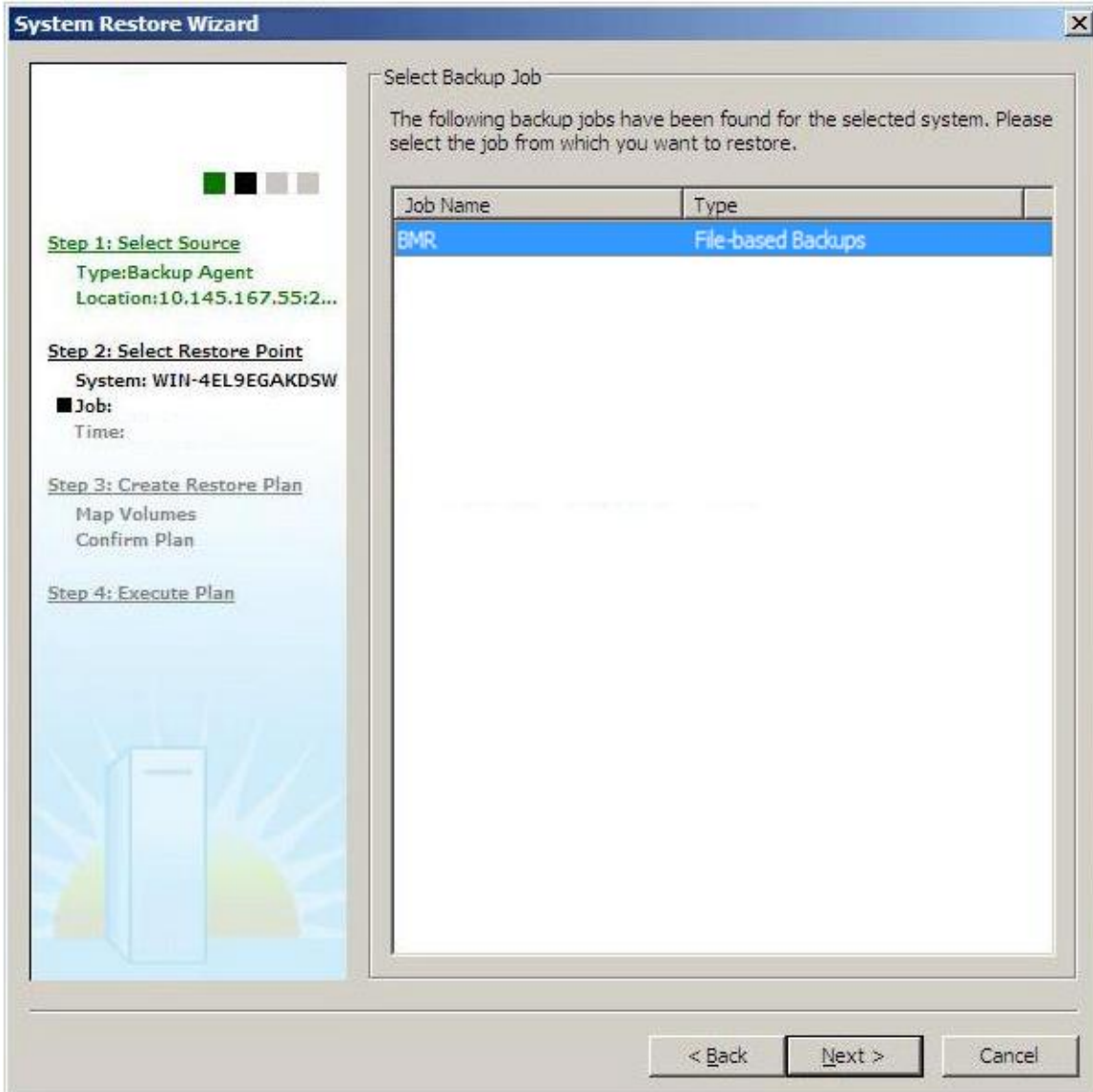
Select Restore Point: Select the restore point date and time from the list of recent restore points or a list of restore points for a specific period.



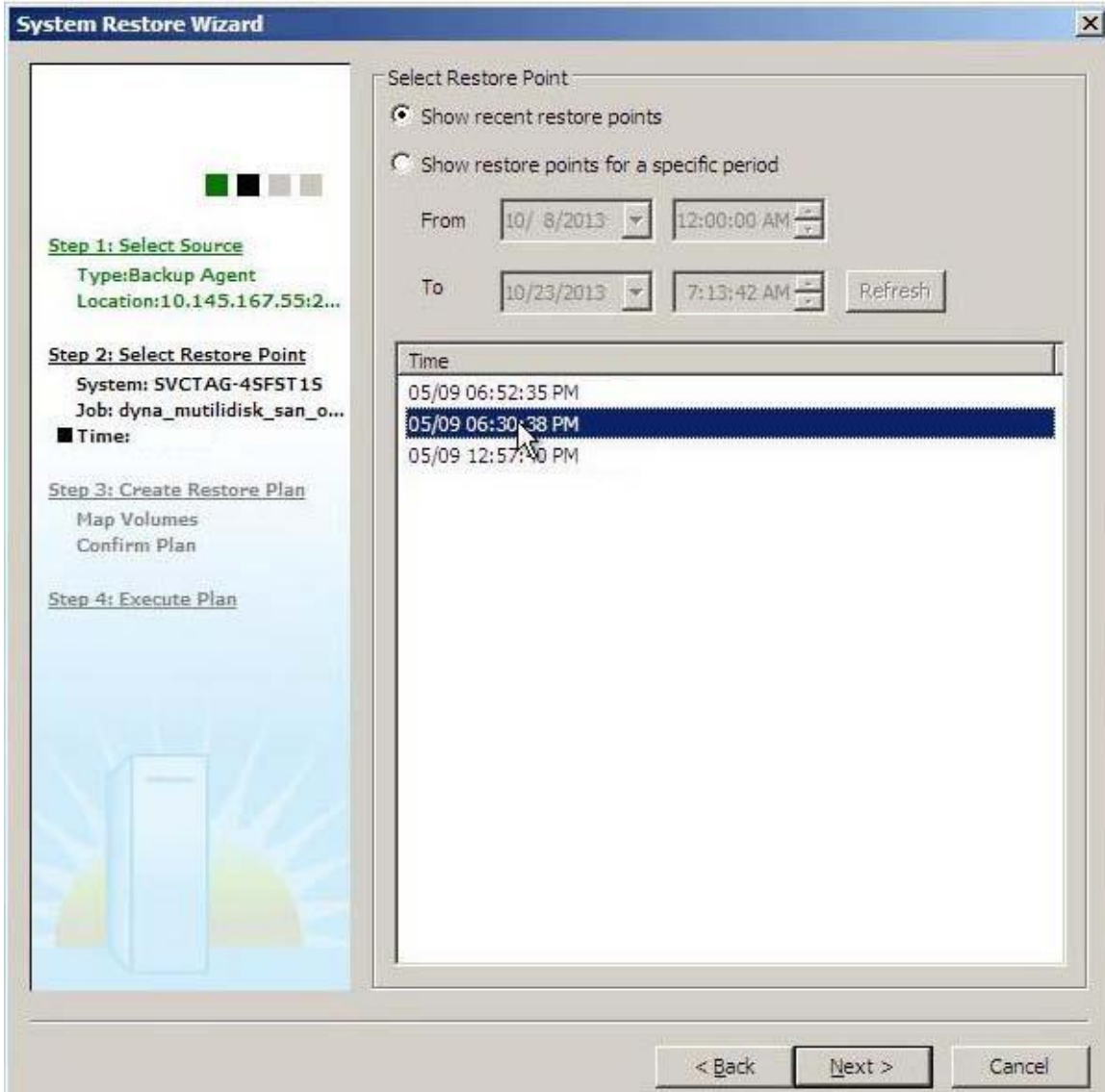
To perform **Step 2: Select Restore Point**

- 1) Select the system from the list of computers displayed in the **Select Protected System** section.
- 2) Click **Next** to continue.

Note: The original system should be offline. This can help you to avoid IP and name conflicts after the restore.



- 3) Select the backup job from which you want to restore your system. The **Select Backup Job** screen shows the following.
 - Job Name:** The list of jobs that have been backed up.
 - Type:** Specifies the type of backup job.
- 4) Click **Next** to select the restore point.



- 5) Select one of the two buttons for **Select Restore Point**.
 Select **Show recent restore points** to list the recent restore points. This displays the most recent restore points (up to ten, if available), listed in reverse order, with the most recent restore point appearing first in the list.
 or
 Select **Show restore points for a specific period** to list the restore points created within a specific period of time.
 If you select this option, you must also choose the start date and time of the backup from the **From** field, and the end date and time of the backup from the **To** field.

If trailing dots (such as ...) appear next to a field, you can pause your mouse over that field to see the complete description (e.g., Job – dyna_multidisk_san_o...).

6) Click **Next** to proceed with the restore process.

Note: *Restore point* denotes the point in time at which the backup was created, or the snapshot was taken. The number of restore points depends on the number of times the backup is created over a specific period of time.

Remember to select the correct time zone when the backup was taken during the beginning of the restore process. Note that the restore points listed are the date/time of the backup, at the time it was in your current (local) time zone.

Step 3: Create Restore Plan

The third step in the system restore process is to create a restore plan. This is where you map your volumes, produce a summary and confirm your plan before it actually executes.

Click **Next** on the **Select Restore Point** screen to access the **Create Restore Plan** screen. This screen displays the following:

Select Source Volume(s) section: Displays all of the disks and volumes on your system (including OEM partitions). The disks that have been backed up are shown in a blue or green color. Select the volumes that you want to restore to your new system.

Select Destination Volume(s) section: Displays all of the disks and volumes in the destination system where the backup can be restored. It also displays all volumes or partitions that might pre-exist on a disk.

Each disk in the source and destination volume is represented in a row. And each volume in a disk is represented as a cell in a row.

The colors of the volumes denote the following:

- Blue icon in the Source Volume: Volumes that are backed up
- Light Grey in the Source Volume: Unused free space
- Dark Grey in the Source Volume: Volumes that are not backed up
- Light Grey in the Destination Volume: Unused free space
- Dark Grey in the Destination Volume: Volume exists
- Blue icon in the Destination Volume: Volumes that are mapped
- Green icon in the Source/Restore Systems: GPT drives
- Blue icon in the Source/Restore Systems: MBR drives

Notes about restoring: You can drag a volume to a disk (i.e., free space on the disk) or a volume. Dragging a volume onto a volume overwrites and formats the destination volume.

You can convert from MBR disks to GPT disks (or GPT disks to MBR disks) by dragging the desired source volume to the desired destination volume or disk. You can restore to a smaller or larger GPT drive partition.

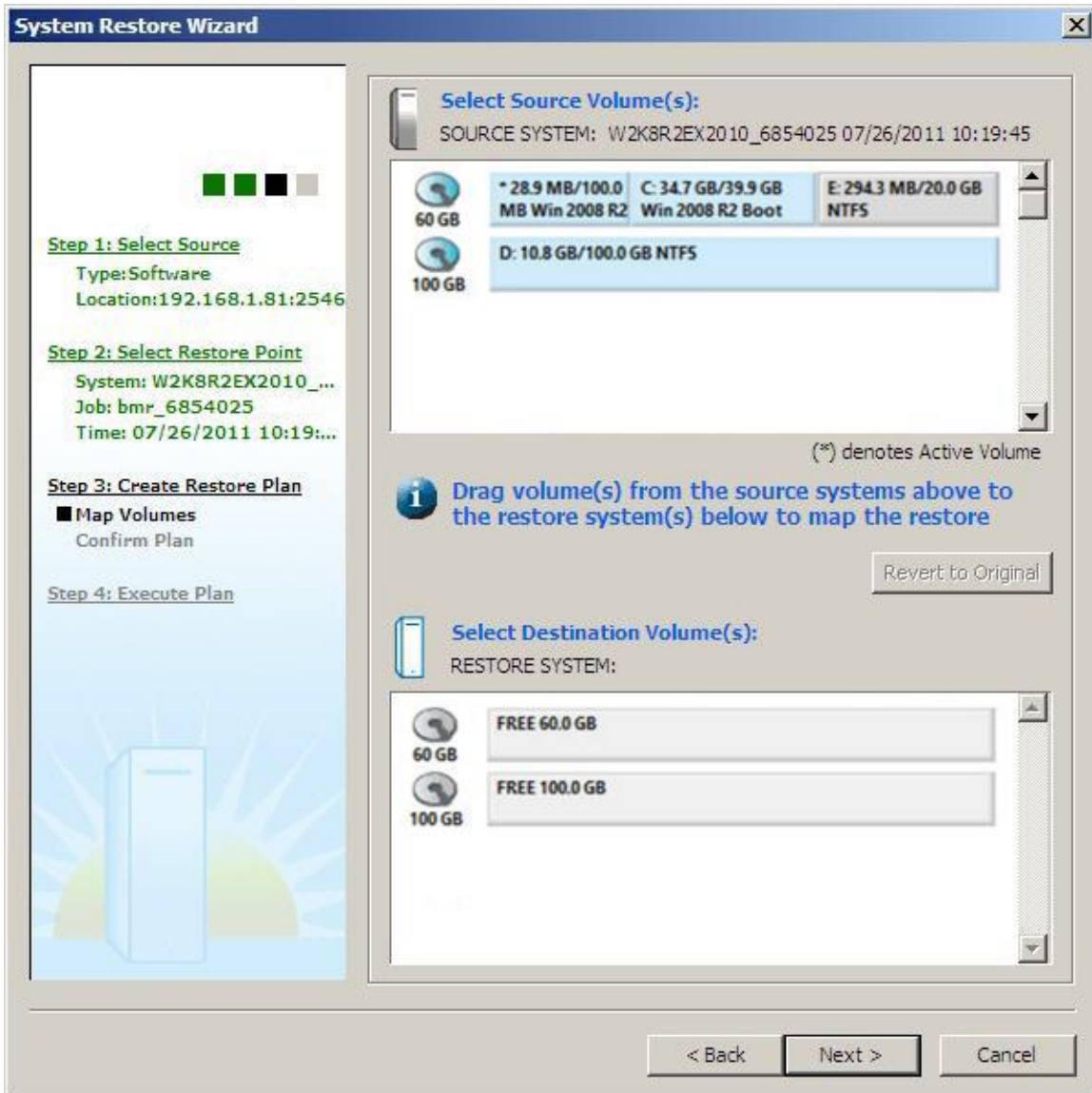
If you drag a volume to an uninitialized UEFI disk, the disk type automatically changes to GPT.

Note: If you restore a volume from a BIOS-based system to a UEFI system, the following error might appear, even if you map a volume to a destination disk of the same size: *“The source volume cannot be mapped. There is not enough space available.”* This problem occurs because an uninitialized UEFI disk defaults to GPT, and an additional 16,384 bytes + 128 bytes is required for the partition table for a GPT partition. To prevent this problem, you can choose a larger destination volume or convert the volume to MBR. If you are restoring from a UEFI-based system to a UEFI-based system, this problem does not occur.

Note: In the destination area, if you have existing partitions that could contain data, they will be shown as dark grey volumes. You can remove them, but this will delete the data in those volumes.

To prepare to restore your system, map the volumes in the source section to the volumes in the destination section. Do this by selecting volumes from the source section and dropping them onto the chosen destination disk.

The volume marked with an asterisk (*) is the active volume. It contains information about the OS location, as well as boot parameters.



OEM volumes: Dragging and dropping are handled differently, depending on the nature of the target (i.e., BIOS versus UEFI).

For BIOS to BIOS recoveries, dragging an active OEM volume (needed for booting) from the source to a destination volume requires the OEM volume to be the first partition on the destination disk.

For a recovery to a UEFI target system, the OEM volume is not required for booting. Because of this, the OEM volume is treated as a regular data volume.

To perform **Step 3: Create Restore Plan**

- 1) Select a volume from the **Select Source Volume(s)** section.
Drag the selected volume in the **Select Source Volume(s)** and drop it into any of the existing destination disk volumes. The application will ask whether you want to **Merge**, **Format** or **Cancel**. If you want to drop it in free space, there must be enough space available, or else you will get an error message. If you select **Format**, all existing files will be deleted. If you select **Merge**, the restore process will write its files from the backup to the destination volume, overwriting any files that have the same path and file name.

Note: Each disk can have a maximum of 4 primary volumes, or 3 primary volumes and 1 extended volume.

There are partitioning limitations that could prevent a volume from being mapped. The restore will attempt to find the best way to do the mapping, but in some rare cases, it might not be possible to create a partitioning scheme that allows the requested mapping of volumes. In this case, the mapping will be rejected, and an error message will appear.

Destination Disk Format: When you drag and drop a volume onto an uninitialized destination disk, a **Disk Type Selection** pop-up will appear. This allows you to choose the format type to apply (**GPT** or **MBR**).

Convert Destination Disk Partition Format: You can also right-click on a grey destination disk icon to choose the format to apply (**GPT** or **MBR**).

- 2) (Optional) Right-click the selected disk volume in the **Select Destination Volume(s)** and choose the required option:

Remove: Removes the mapping of the volume in the destination disk volume.

Edit Volume: Edits the disk volume details.

- 3) Optionally, you can edit a volume to change the size of the volume that is mapped.

To restore the disk volumes to the original state, click **Revert to Original** at any time. (All of the previous mapping will be reset to the original state.)

To edit the volume details, under **Select Destination Volume(s)**, right-click the selected disk volume, and select **Edit Partition**.

- 4) Enter the required size for the volume in the **Select the amount of space in MB** field. Click **OK** to confirm your entry.

- 5) Click **Next** to continue. (Otherwise, to select a different restore point, click **Back** to return to the previous screen.)

If you only mapped the C: drive or the system partition, a warning message will appear. You need to restore BOTH the system and the boot volumes to ensure a full system recovery.

- 6) On the **Restore Plan Summary** screen inside the restore wizard, you can view the steps that will be taken to execute your restore plan.

Generally, a restore plan consists of:

Partitioning: List the plan for the modifications to the disk's partitioning scheme to be made.

Restoring: List the volumes that you plan to restore from the backup.

Generating Boot Configuration: List the plan for updating the boot configuration on the disk.

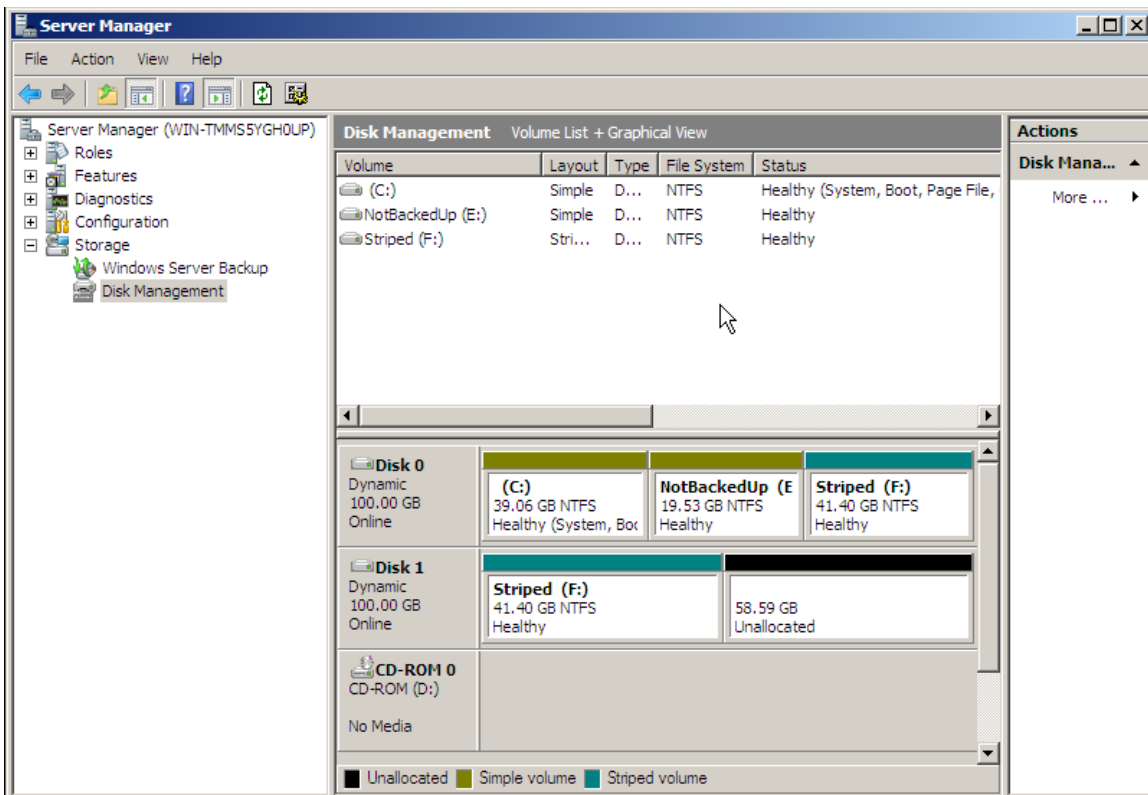
- 7) Select the **Click here to confirm the restore plan** check box.
- 8) Click **Next** to proceed with the restore process. The restore operation for the selected backup volumes will begin.

6.2 Basic Disks and Dynamic Disks

A basic disk is a physical disk with primary and extended partitions. Provided that you use an appropriate format, all Windows versions can access basic disks.

Dynamic disks are a Microsoft proprietary format. Basic disks and dynamic disks differ in their ability to extend storage beyond one physical disk. Basic partitions are confined to one disk, and their size is fixed.

Dynamic disks are created in the Microsoft **Disk Management** console. They allow you to adjust their size and add more free space (from the same disk or another physical disk). Dynamic disks can span different physical disks. They also permit RAID-5 configurations (e.g., striped or mirrored).



6.3 Recovering a Dynamic Disk to a Basic Disk

This is similar to recovering a basic disk, but if you have a dynamic disk that consists of multiple volumes (e.g., mirrored or RAID-5 volumes), you will see multiple backed-up volumes with the same drive letter. When you map one of them, it creates a mapped basic disk for the contents of the dynamic disk.

Note that EVault System Restore does not create dynamic disks. You can convert to dynamic disks after booting into the restored OS.

Follow the steps as before, in section 6.1:

- Select **EVault Software** for the **Source Type**, and specify the location of your backup.
- Select a restore-point **System, Job** and **Time**.
- Create a restore plan and map the volumes.
- Confirm and execute the restore plan.

Step 4: Execute Plan

The fourth step in the system restore process is to execute the restore plan.

In the **Restore Progress** pane, when you execute the plan, different status values can appear: **Pending, Restoring, Reconnecting, Failed, and Completed**.

To perform **Step 4: Execute Plan**

- 1) Go to the **Execute Plan** screen by clicking **Next** on the **Confirm Restore Plan** screen.
- 2) By the time the **Overall progress** reaches 100%, the source volumes should have finished being copied to the destination disk. Click **Next** to complete the restore process.
- 3) The final screen displays messages that are similar to these:
 - Successful:** The restore process has completed successfully, and no repair is needed. In this case, the **Finish** button will appear so that you can exit the restore wizard.
 - Successful but repair needed:** Restore process has completed successfully, but the restored system contains hardware that is significantly different from before. You should repair the system. In this case, the **Next** button will appear so that you can proceed to the repair wizard.
 - Failed:** The restore process has failed.
- 4) Click **Next** to proceed to the repair wizard, or if repairs are not required, click **Finish** to complete the restore process and exit from the wizard.

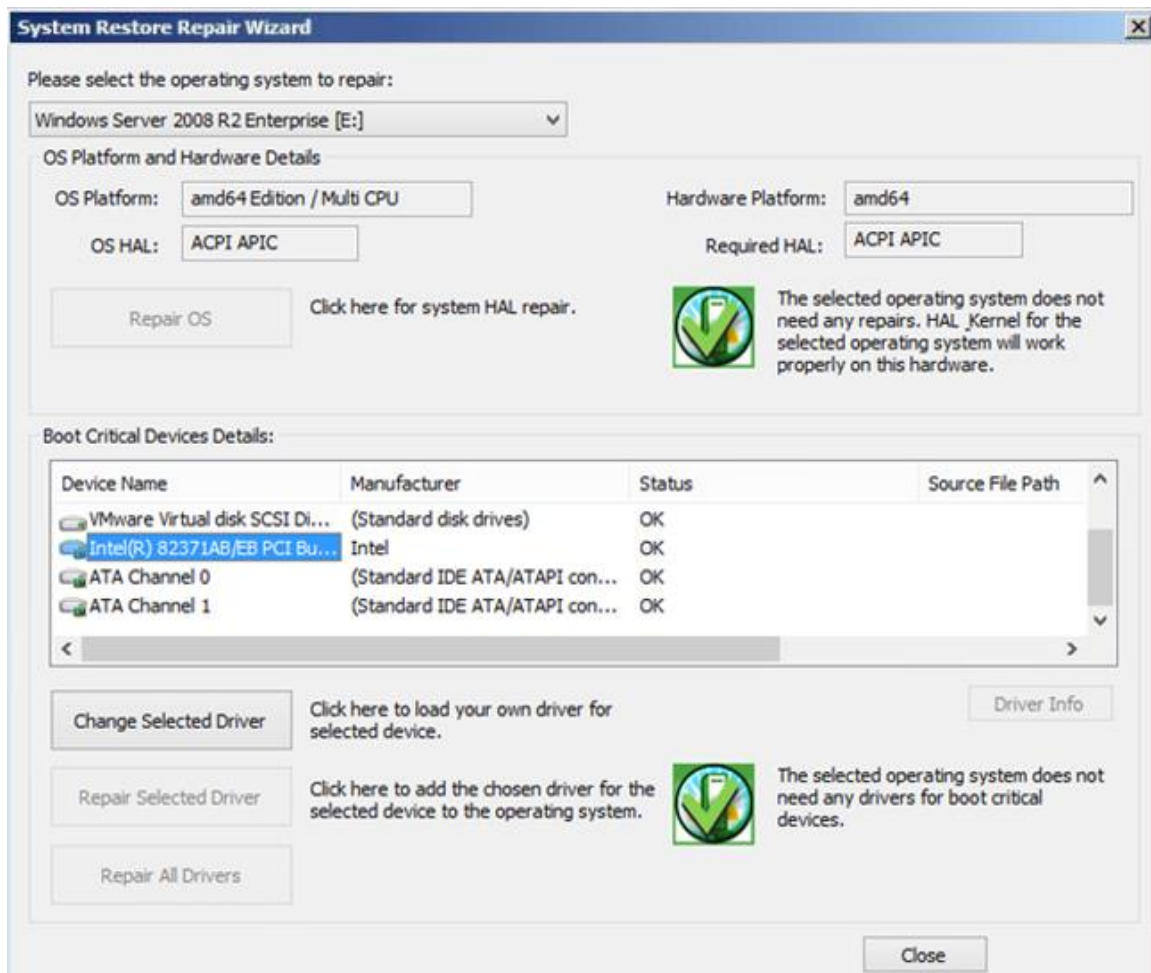
7 Repair My System

If you have restored your failed system to hardware that is significantly different from the system that was backed up, the restored system might not be able to boot. This is due to boot-critical devices that are not configured for the new hardware in the OS you have restored. You can repair the OS by repairing the drivers necessary for it to boot.

After Windows has successfully started, it will recognize the non boot-critical devices, and start the driver update process for them. You can repair the OS by installing or updating the missing boot-critical drivers.

The ESR repair wizard allows you to perform:

- Hardware Abstraction Layer (HAL) and kernel repair
- Boot-critical device repair



7.1 HAL and Kernel Repair

If a system is being restored to dissimilar hardware, the HAL and kernel that have been stored in the backed-up operating system might not be optimal for the new hardware. You can choose to repair the OS, selecting HAL and kernel versions that are better matches for the new hardware. The OS should then boot and work properly, unless it is incompatible.

The status icons are as follows:



The selected OS does not need to have its HAL or kernel adjusted for the current hardware.



The selected OS will work with the current hardware, but it is recommended that you repair it for optimal performance.

As an example, you might have restored a single-CPU OS to hardware with multiple CPUs or cores. In this instance, you might wish to repair the OS so that it takes advantage of all CPUs.



The selected OS is incompatible with the current hardware.

For example, it is not possible to restore a non-ACPI OS to ACPI-compatible hardware.

To complete HAL and kernel repair:

- 1) Click **Repair My System** on the main menu.
The repair wizard opens.
- 2) Select the required operating system from the dropdown list.
Details for the selected OS appear.
- 3) Click **Repair OS**.
- 4) Click **Close** to exit from the repair wizard.

7.2 Boot-Critical Device Repair

After a restore, the system might find that the boot drives are not correct for the new hardware. It will then search for an appropriate driver on the ESR boot media, or on the restored OS.

If the system is unable to find a good driver for your specific hardware, you must install your own.

The **Boot Critical Devices Details** pane provides details about devices that might require changes or repairs to their drivers:

- **Device Name:** Name of the device
- **Manufacturer:** Name of the manufacturer of the device
- **Status:** Status of the device. If the status is **Needs Repair**, a driver will need to be installed. If the status is **OK**, a driver for the device is already installed on the operating system.
- **Source File Path:** Location of the suggested driver for the device. If the suggested drivers are not present in the driver repository, you can install your own driver.

Note: ESR will suggest the closest matching driver for the device. If no driver is found that matches well, a more generic driver might be suggested. It is always best to provide the latest driver (from the vendor) for your specific hardware.

Again, the status icons are:



The selected OS does not need new drivers for boot-critical devices.



The selected OS does not have the necessary drivers for all of the boot-critical devices. You should install them.

To complete the boot-critical device repair:

- 1) Click **Repair My System** on the main menu.
The repair wizard opens.
- 2) Select the required boot-critical devices from the list.
- 3) Click **Change Selected Driver** if you want to load a driver that is not present in the driver's repository for the selected device.
If the system locates the driver that is required for the repair, you can skip this step.
- 4) Click **Repair Selected Driver** if you want to repair the driver for the selected device, or click **Repair All Drivers** to repair all drivers for all of the devices.
- 5) Click **Close** to exit from the repair wizard.

8 Restore Test-Run

Restore Test-Run allows you to test the system recovery process without making actual changes to the system. It provides you with a simulation of the process – it does not actually restore the system.

You can then have a level of assurance that in case of disaster, you will be able to connect to the backup, select your restore point, do the mapping, and complete the recovery.

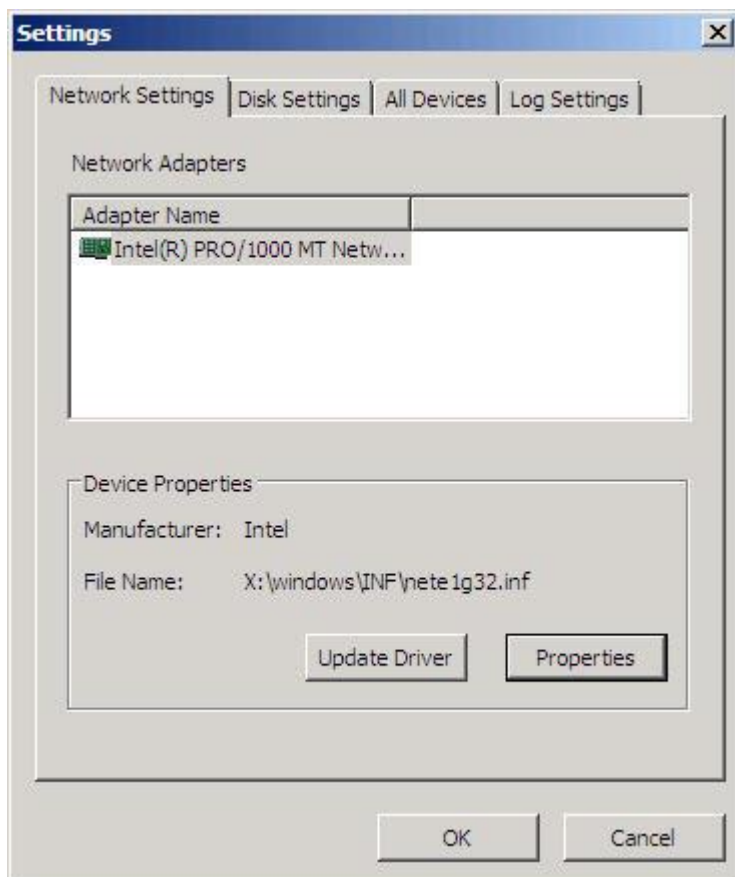
To start the Restore Test-Run wizard, click **Restore Test-Run** on the main menu, and follow the instructions in the wizard.

9 Configuring Settings

You might need to configure some settings before you start restoring or repairing your system. The network settings allow you to configure the network devices of the system that you are restoring to if they are not already automatically configured correctly. Network connectivity is required for restoring from backups stored on a NAS, SAN, or vault.

You can configure the disk settings to add disk drivers to use disks for the restore process that are not automatically recognized and configured. It is possible to configure your settings during the restore or repair process.

To configure the settings, click the **Settings** icon on the main menu. The **Settings** screen appears:



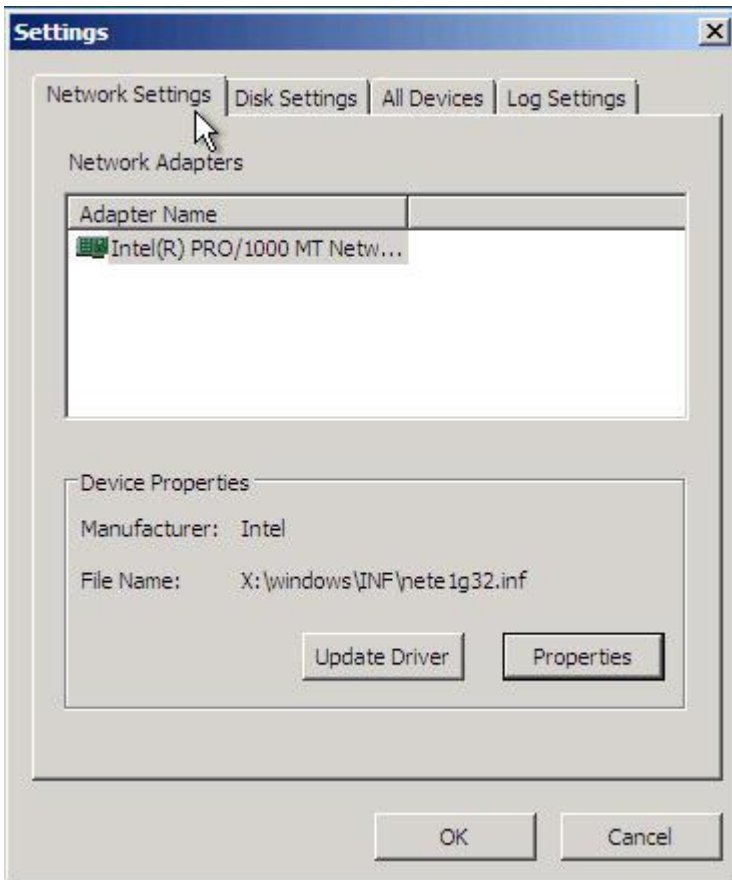
9.1 Network Settings

The **Network Settings** tab displays all network adapters that are connected to the system. The **Device Properties** section provides information about the driver for the selected network adapter. The **Properties** button allows you to configure the IP address, gateway and DNS details. The **Update Driver** button allows you to install a driver in case the driver for the selected network adapter is not available.

If you do not configure the network settings before you start the restore or repair process, network connectivity might not be available, and you won't be able to restore your system over the network.

To configure the network settings:

- 1) On the **Settings** screen, click the **Network Settings** tab.



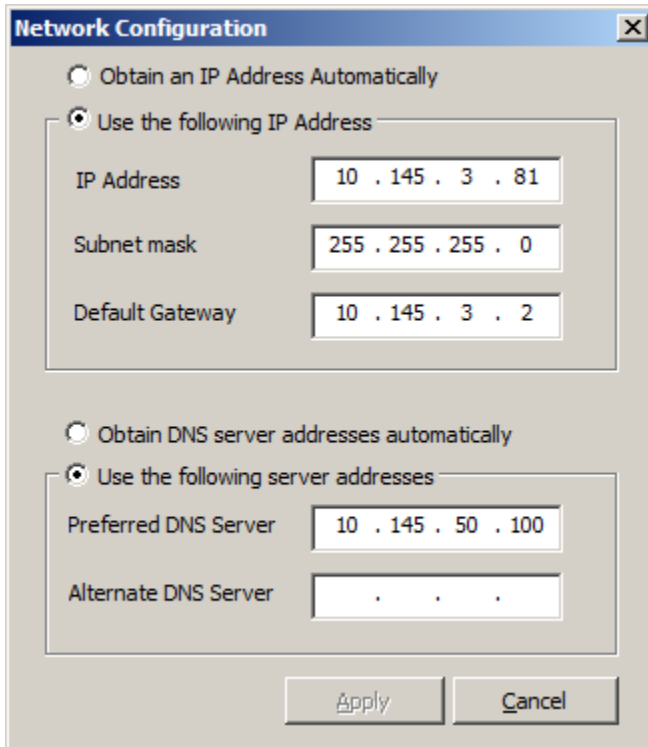
- 2) Select the required network adapter.
Note: If there are no drivers for the device, the **Install** button will appear. If there is a driver (but perhaps the wrong one), the **Update Driver** button will appear.
- 3) Click **Install** to install the driver required for the selected network adapter if the required driver is not already available. Or click **Update Driver** if the driver is already available, but requires updating.
- 4) Click **Properties** to configure the IP address, DNS, and gateway for the selected network adapter if the required driver is already available.
- 5) Click **OK** to apply the settings.

Network Configuration

The **Network Configuration** screen allows you to set the IP address, gateway and other DNS details for the selected network adapter. This screen is available only if the network adapters are configured appropriately with the drivers, a LAN is connected, and the port is enabled.

To open the **Network Configuration** screen, make these selections:

Main Menu > Settings > Network Settings > Properties



By default, an IP address will be automatically assigned using DHCP. If you do not have DHCP, or you wish to assign a specific IP address, you will need to set a static IP address.

Static IP Configuration

To set a static IP address for the selected network adapter:

- 1) On the **Network Configuration** screen, select **Use the following IP Address**.
- 2) Enter the IP address, subnet mask, and default gateway for the network adapter in the respective fields.
- 3) Select **Use the following server addresses**.
- 4) In the **Preferred DNS Server** field, enter the primary DNS IP address for the network adapter. You can also provide an IP address for an alternate DNS server.
- 5) Click **Apply** to apply the specified IP address to the network adapter.

Note: DNS server details are optional. They are required only for accessing other systems through computer domain names instead of IP addresses.

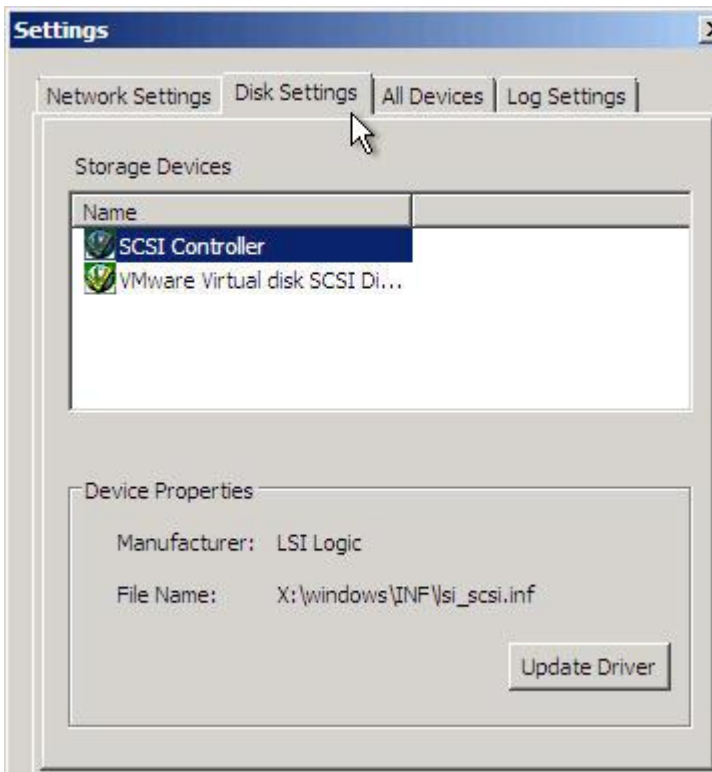
DHCP Configuration

To set the dynamic IP address for the selected network adapter:

- 1) On the **Network Configuration** screen, select **Obtain an IP Address Automatically**.
- 2) Select **Obtain DNS server addresses automatically**.
- 3) Click **Apply** to apply the specified IP address to the network adapter.

9.2 Disk Settings

The **Disk Settings** tab lists all of the storage devices that are connected to the system.



To configure the disk settings:

- 1) On the **Settings** screen, click the **Disk Settings** tab.
- 2) Select the required storage device.

Note: If there are no drivers for the device, the **Install** button will appear. If there is a driver (but perhaps the wrong one), the **Update Driver** button will appear.

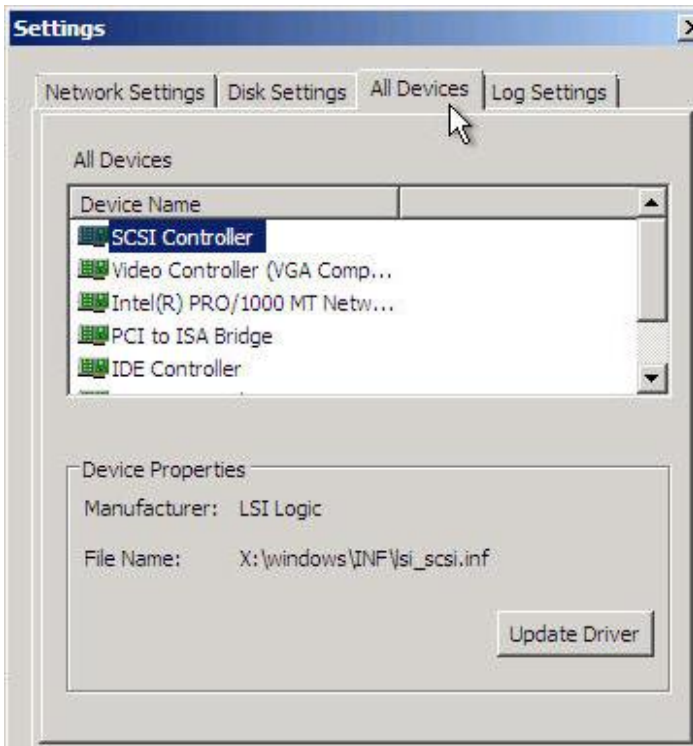
- 3) Click **Install** to install the driver required for the selected storage device if the required driver is not available. Or, click **Update Driver** if the required driver is already available, but you wish to replace it.

Installing Disk Drivers

Refer to [Driver Installation](#) for information about installing drivers.

9.3 All Devices Tab

The list for the **All Devices** tab includes devices that are not listed for the **Network Settings** or the **Disk Settings** tab. Depending on your specific hardware configuration, you might need to install the required drivers for selected PCI devices. You can do so through this tab.



To configure the **All Devices** settings:

- 1) On the **Settings** screen, click the **All Devices** tab.
- 2) Select a device.
Note: If the storage devices do not have drivers already installed, the **Install** button will appear. Otherwise, the **Update Driver** button will appear.
- 3) Click **Install** to install the driver required for the selected storage device if no driver is available. Or, click **Update Driver** if a driver is already available.
- 4) Click **OK** to apply the settings.

Installing drivers for the items in the All Devices list

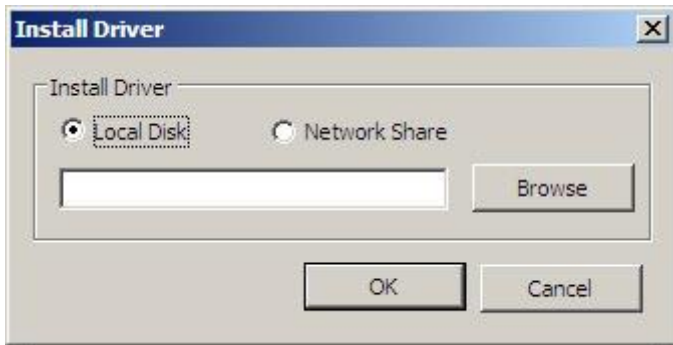
Refer to [Driver Installation](#) for information.

9.4 Driver Installation

The EVault System Restore CD comes preloaded with commonly used recovery-critical drivers.

You might need to restore critical drivers if the hardware to which you are restoring and running ESR includes hardware that is not recognized by ESR. In this case, you need to manually install the required driver as follows.

When you click **Update Driver** in the **Device Properties** pane of one of the preceding tabs, the **Install Driver** screen appears.



To install a driver for the selected network adapter:

- 1) Choose **Local Disk** to install the driver from a local disk. Or, choose **Network Share** to install the driver from a network share.
- 2) If you select **Local Disk**, you can use the **Browse** button, or enter the path name manually. If you select **Network Share**, the **Browse** button is disabled, and you must enter the full path name for the location of the driver.

Click **OK** to start the driver installation process.

9.5 Log Settings

You can choose to create a log file for each restore job. This file can include error messages, failure messages, and warnings encountered during a restore process. The **Log Settings** tab allows you to configure the following details for your log file.

- **Log Level** settings:
 - a) **DEBUG**: Records all of the log messages
 - b) **LOG WARNING**: Logs only warnings and error messages
 - c) **LOG ERROR**: Logs only errors
 - d) **DISABLE LOGGING**: No log is generated
- **Maximum Log Size**: You can restrict the log size to conserve disk space. Otherwise, the log size is set to the default. The maximum log file size is set initially to 100 MB. It is

recommended that detailed logs be placed on a separate device because the default X: drive is a RAM drive, which is lost after reboots.

- **Log File Location** pane: This specifies where to save the log file.

Note: To configure the log settings, click the **Settings** icon on the main menu. The **Settings** screen will open. This is the only way to configure log settings.

To return to the **Settings** screen, once again, click the **Settings** icon on the main menu.

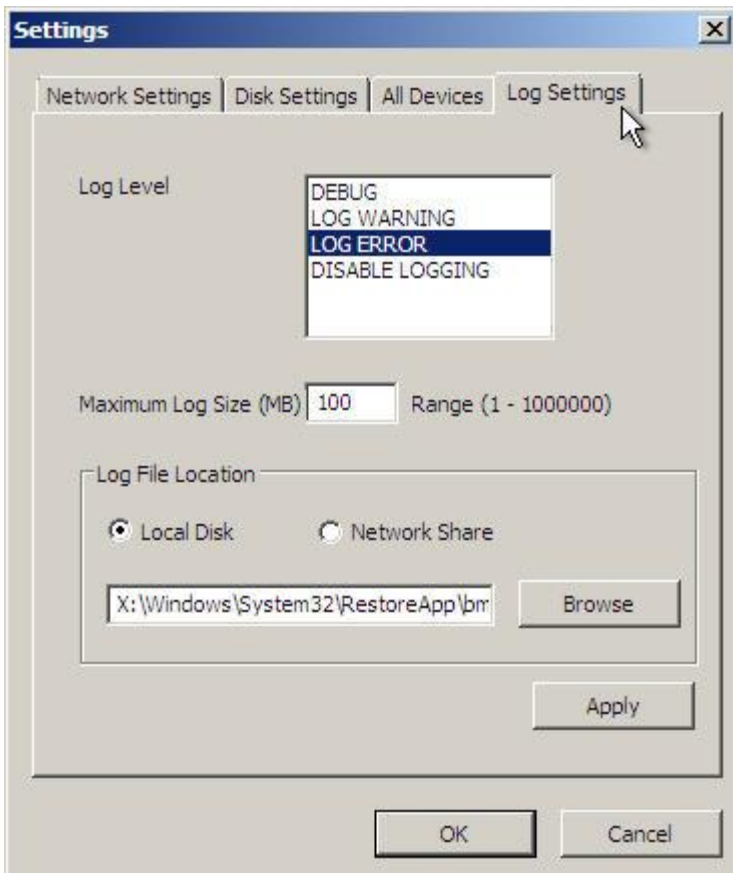


Figure 1. Log Settings

To configure log settings:

- 1) On the **Settings** screen, choose **Log Settings**.
- 2) Select a level from the **Log Level** list.
- 3) Use the **Maximum Log Size** field if you want to restrict the size of the log file. When the maximum size is reached, the log wraps around and starts to overwrite the file from the beginning.
- 4) For **Log File Location**: Choose **Local Disk** if you want to save the log file on a local disk. Choose **Network Share** if you want to save the log file on the network, and enter the full address for the log file location.
- 5) Click **Apply** to apply the settings. Click **OK** to continue.

10 Appendix

10.1 Configuring Advanced Vault Settings

You can use over-the-wire (OTW) encryption for transmissions to and from the vault. You can also configure the following settings.

Port: Enter the port number at which the vault should listen.

Try to reconnect every: Enter the maximum number of seconds over which your system should try to reestablish connection with the server before terminating/failing the job.

Stop reconnection attempts after: Enter the number of minutes after which you want to stop trying to reconnect. This value (entered in minutes) must be greater than the value (entered in seconds) in the **Try to reconnect every** field.

10.2 Restoring Operating Systems with OEM Licenses

When you back up operating systems with Original Equipment Manufacturer (OEM) licenses, and then try to restore to dissimilar hardware, the system might boot, but you will not be able to log on without activating Windows. This is because the OEM licenses are not transferable.

When the restore process finishes, you must contact Microsoft to activate your Windows license before you can log back into the system.

10.3 Restoring to UEFI Systems

The Extensible Firmware Interface System Partition (ESP) is a required component of UEFI-based systems. This volume is important for the boot process – it contains system information used solely by the UEFI boot process.

The ESP volume replaces the OEM/system volumes used by BIOS-based systems for the boot process.

UEFI to UEFI Restores

UEFI to UEFI restores are different from BIOS to BIOS restores because of the ESP component.

First you need to apply the ESP from the source system to the destination system. If an ESP already exists on the destination system, drag the source ESP and drop it so that you *overwrite the destination ESP*.

Then you can drag the Windows volume to restore it to the destination system.

BIOS to UEFI Restores

A BIOS to UEFI restore is similar to data migration.

The OEM volume does not need to be mapped to the destination. An ESP volume will be generated automatically to accommodate the BIOS-based backup. You only need to drag the Windows volume, as well as data volumes from the source to the destination.

10.4 Creating BMR Backups

You can create a BMR backup of a system using the Windows Agent or Image Plug-in. For procedures, see the Portal online help, the *Agent for Microsoft Windows User Guide*, or the *Image Plug-in Guide*.

The Agent will check for an EVault System Restore license during the backup operation. If you have created a BMR backup job, but do not have the appropriate license, the job will fail when it attempts to perform the corresponding backup operation.

Note: You cannot run BMR restores from Portal or CentralControl. You must use the ESR application for this.

Upgrading an Existing Job to a BMR-Type Job

CentralControl allows you to upgrade an existing **Local System** job to a BMR-type job without reseeding. When you select **Bare Metal Restore**, the following selections become unavailable:

- **System State**
- **System files**
- **RSM database**
- **Event logs**

Upgrading your job to a BMR-type backup will not cause reseeding, and it will not alter existing data selections. It will identify all volumes that need to be backed up to help ensure a recoverable system at restore time.

10.5 Restoring Applications such as SQL Server and Oracle

Restoring applications such as SQL Server and Oracle can be multistep processes. For SQL you need to restore:

- a. Operating system
- b. SQL Server binaries
- c. SQL Server data

If you use SQL or Oracle Plug-Ins to back up your database application data, you will require two separate jobs to completely back up. The first job will back up the OS and application binaries. The second job will use the appropriate Plug-In to back up the database data.

If you only use ESR for ordinary backups and restores, you will not see the second job in the job list for restores. This is because the second job does not have an associated OS backup.

Restoring the application entirely (binaries and data) is a multistep process:

1. Use ESR to restore the OS and SQL binaries to the new/fixed machine. Follow the steps from Chapter 6 of this manual.
2. Install the EVault Agent on the system, and start the database server there.

Note: If the Agent was previously installed on the system, ESR will have recovered it already, so you should not need to install/reinstall it.

3. Recover the database application data to your system.

Note: Details for steps 2 and 3 here do not appear in this guide. They are described in the Windows Agent and plug-in guides which are available from your service provider.