opentext ™

OpenText™ Server Backup System Restore 9.4

User Guide

Document History

Version	Date	Description
1	January 2025	Initial guide for System Restore 9.4*x*.

Contents

1   Overview: Restore a Windows system

If a Windows computer is protected by a Bare Metal Restore (BMR) backup, you can restore the computer, including its operating system and system state, to the machine where it was backed up or to a different machine.

A BMR backup is created using the Windows Agent or Image Plug-in and contains all volumes necessary for starting the protected system. For information about creating a BMR backup, see the Portal online help or *Windows Agent and Plug-ins Guide*.

To restore a Windows system from a BMR backup, you must:

1. Create recovery media. Recovery media is a USB flash drive or other device with a System Restore ISO image file, and is used to boot destination machines and restore protected computers. See Create recovery media.

    You do not need to create recovery media every time you restore a system. You can use the same recovery media to restore multiple Windows computers.

2. Choose the machine where you will restore the protected system. See Choose a destination machine for a restore.

3. Boot the machine from the recovery media, and restore the protected system. See Restore a Windows system.

4. If required, repair the operating system and drivers for the restored computer. See Repair a restored system.

2 Create recovery media

Before you can restore systems from BMR backups, you must create recovery media. Recovery media is a USB flash drive, CD, DVD or PXE boot server with a System Restore (SR) ISO image file, and is used to boot destination machines and restore protected computers.

You can create recovery media using the Bootable Media Creator utility (BMC).

You can use the same recovery media to restore multiple Windows computers. However, beginning in version 9.40, you must create separate recovery media for restoring systems with Windows Server 2025, Windows Server 2022 or Windows 11, and for restoring systems with Windows Server 2019, Windows Server 2016 or Windows 10.

The Windows Assessment and Deployment Kit (Windows ADK) and the Windows Preinstallation Environment (Windows PE) must be installed on the system where you run BMC. You can download Windows ADK and Windows PE from Microsoft and install them before running BMC or when you run BMC. For required Windows ADK and Windows PE versions, see the *System Restore from Bootable Media Creator* release notes. For more information about Windows ADK and Windows PE, see documentation from Microsoft.

To create recovery media:

1. If the Bootable Media Creator (BMC) is not installed on the machine where you want to create recovery media, do the following:

   - Double-click the BMC installation kit.

   - On the Welcome page, click **Next**.

   - On the License Agreement page, read the license agreement. Click **I accept the terms in the license agreement**, and then click **Next**.

   - On the Ready to Install the Program page, click **Install**.

   - On the installation completed page, click **Finish**.

2. Start BMC.

3. On the Creating Recovery Media page, select the operating system of the systems that you want to recover:

   - **Windows Server 2022, Windows 11 and later**. With recovery media created using this option, you can also restore systems with Windows Server 2025.

   - **Windows Server 2019 and earlier, or Windows 10**

     Note: If you are running BMC on Windows Server 2025 or Windows 11 24H2, this option is unavailable. On Windows Server 2025 or Windows 11 24H2, BMC can only create

recovery media for restoring systems with Windows Server 2025, Windows Server 2022 or Windows 11.

4. Click **Continue**.

5. If a warning message states that the existing version of the Windows Assessment and Deployment Kit must be uninstalled, click **Yes**. The software is then uninstalled.

6. If the Install Windows Assessment and Deployment Kit page appears, you must download and install Windows ADK before you can create the recovery media. Click **Install**. On the Specify Location page, select **Install the Windows Assessment and Deployment Kit to this computer**, and then click **Next**.

   Alternatively, to download the Windows ADK installer for installation on another computer, select **Download the Windows Assessment and Deployment Kit for installation on a separate computer**, and then click **Next**.

7. In the Windows Assessment and Deployment Kit installer, follow the prompts to install the **Deployment Tools** and the **Windows Preinstallation Environment (Windows PE)**. Depending on the version you are installing, Windows PE might be on the Windows ADK feature selection page, or installed in a separate installer.

   When a message states that the installation was successful, click **Continue**.

8. On the Select Your Media Device page, do one of the following:

   - To create recovery media on a USB flash drive, select **USB Flash Drive**, and choose a flash drive from the list. To add a flash drive to the list, insert the flash drive into a USB port, and click **Refresh** when it is ready.

     The flash drive storage capacity must be at least 500 MB.

     Note: Any existing data on the USB drive will be erased.

   - To create an ISO image file, select **ISO Image**, and specify a location for saving the file.

     After creating an ISO image file, burn it to a bootable CD or DVD, set up a PXE boot server, or attach it to a VM and boot the VM from the ISO file to use it as recovery media.

9. Click **Continue**.

10. To add drivers for specialized hardware, click **Add** on the Build Bootable Media Image page. In the Browse for Folder dialog box, browse to the location of driver (.inf) files, and then click **OK**.

11. Click **Continue**.

    When finished, a message states that your recovery media is ready.

12. Click **Close**.

3   Choose a destination machine for a restore

Before restoring a system from a BMR backup, you must choose a destination machine where the system will be restored.

The destination machine can be the machine where the computer was backed up, or can be a different physical or virtual machine. If you restore a system to the machine where it was backed up, files will be restored to their state when the system was backed up.

When restoring a protected computer using recovery media, the destination machine:

- Must have 64-bit hardware. System Restore can only restore a system to 64-bit hardware.

- Can be a physical or virtual machine (VM). You can restore a backup of a physical computer to a physical or virtual machine, and can restore a backup of a virtual computer to a physical or virtual machine.

    When restoring a computer to a VM, ensure that the VM configuration is compatible with the computer that is being restored.

- Can use UEFI or BIOS. You can restore a backup of a BIOS-based computer to a BIOS or UEFI machine. You can restore a backup of a UEFI-based computer to a UEFI machine, but cannot restore a backup of a UEFI-based computer to a BIOS machine. For more information, see Restoring UEFI-based systems and Restoring BIOS-based systems.

- Can have an operating system and files, or can be in a bare metal state. If you restore to a machine that has an operating system and data, the existing files will be overwritten.

- Can have similar hardware to the protected system, or can have dissimilar hardware.

    If the destination machine hardware supports the operating system of the protected system you are restoring, you should be able to restore even if, for example, the disks are different. You might not be able to restore if the destination hardware is incompatible with the source operating system.

    Some non-Intel or non-AMD processors, such as Itanium, might not restore to Intel/AMD processors.

To restore a volume from an Image backup, the disk on the destination machine must have the same sector size as the original disk. For example, a volume that was backed up on a disk with 512 byte sectors cannot be restored to a disk with 4 KB sectors.

Beginning in version 9.40, System Restore can automatically map volumes from a backup to a destination machine. To use this functionality, there are additional system requirements. For more information, see Automatically map volumes to the destination machine.

4   Restore a Windows system

After creating recovery media, you can restore a Windows system from a BMR backup to a destination machine. The destination machine can be the machine where the system was backed up or a different machine. See Choose a destination machine for a restore.

Note: If you are restoring a system to a different destination machine (i.e., not the machine where it was backed up), make sure that the original machine is offline. This will help avoid IP address and name conflicts after the restore.

Beginning in version 9.10, if you are restoring from a backup in a vault where certificate checking is enabled, System Restore checks whether the certificate is valid. For more information, see Vault certificate validation and pinning.

Beginning in version 9.40, System Restore can automatically map volumes from a backup to a destination machine. For more information, see Automatically map volumes to the destination machine.

To restore a Windows system:

1. Boot the destination machine from the recovery media.

    If the recovery media is a bootable USB flash drive, CD or DVD, the device should be the first option in the boot order of the firmware. If another bootable device is listed before the recovery media, System Restore might not launch automatically.

    If the System Restore ISO file is on a PXE server, the PXE option must be enabled in the firmware and the DHCP server must be set up in the network where the system resides.

2. On the System Restore page, specify the time zone and keyboard, and then click **Next**.

    This time zone is used for showing available restore points (i.e., BMR backup start times) in System Restore. The restored machine will have the time zone of the system that was backed up.

3. On the License Agreement page, read the license agreement. Select **I accept the terms and conditions in the license agreement**, and then click **Next**.
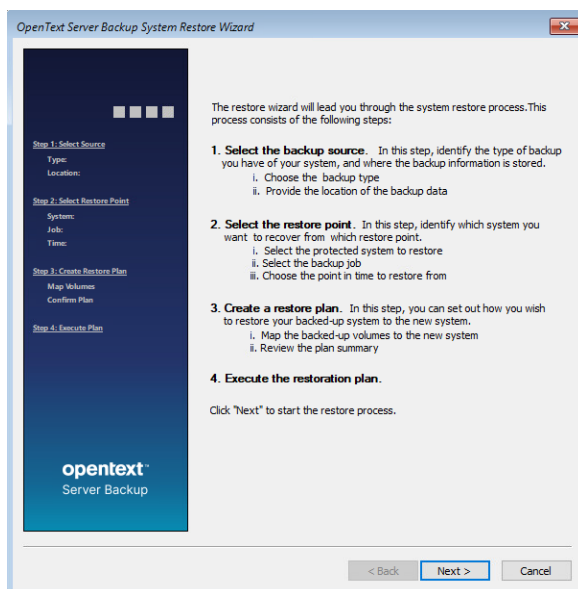
4. On the Main Menu page, click **Restore My System**.

   Note: You can also test a restore without restoring the system. To do this, click the **Restore Test-Run** button, and follow the remaining steps.
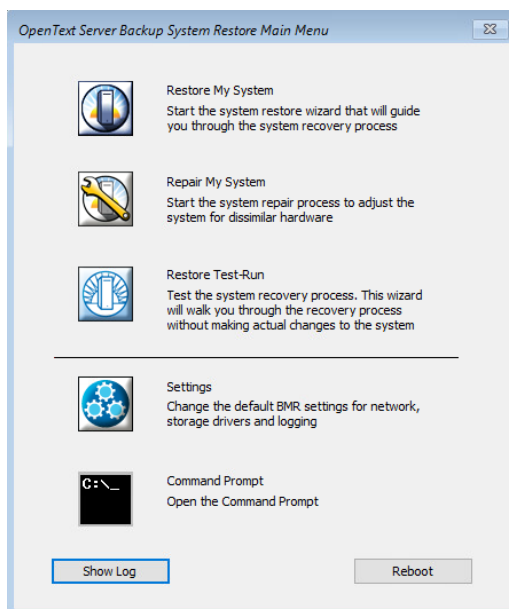
The restore wizard lists steps in the restore process:

- Step 1. Select the backup source

- Step 2. Select the restore point

- Step 3. Create a restore plan

- Step 4. Execute the restore plan

5. Click **Next**.

Step 1. Select the backup source

The backup source is the vault with the BMR backup from which you want to restore.

6. On the Choose Backup Location page, select **Vault**. Specify the IP address or hostname (if DNS is available) of the vault. Specify the vault account, username and password used for the backup.

    To specify port, reconnection and encryption options, click **Advanced Settings**. In the Advanced Settings dialog box, specify settings and then click **OK**.

    Note: If System Restore cannot connect to the vault, open a command prompt and ping the vault server. If you cannot ping the vault server, run the ipconfig command to view network information. You can open Restore Settings and set up your network card IP addresses as described in Step 7.

7. If you are restoring from a backup in a vault and System Restore is not connected to a network, click **Restore Settings**. In the Settings dialog box, configure a network connection for System Restore. See Set up a network connection for System Restore.

    Normally, System Restore connects to a network automatically. However, if DHCP is not configured on your network or network card drivers are not present, you must set up the connection.

    Note: This process does not configure networking for the restored system. You can configure networking for the restored system after you start it.

8. To install or update device drivers, click **Restore Settings**. In the Settings dialog box, install or update drivers on the All Devices tab. See Install or update device drivers.

9. Click **Next**.

    If you are restoring from a vault where certificate pinning is enabled, System Restore checks the vault's TLS certificate. See Vault certificate validation and pinning.

    If the Select Protected System page appears, go to Step 2. Select the restore point.

10. If a Vault Certificate Verification dialog box shows vault certificate information, review the certificate information and then do one of the following:

    - If you do not trust the vault certificate, click **Decline**. You can then select a different backup source or cancel the restore.

    - To connect to the vault and continue the restore, click **Accept**. Go to Step 2. Select the restore point.

Step 2. Select the restore point

The restore point is the start date and time of the BMR backup from which you want to restore.

11. On the Select Protected System page, click the protected system that you want to restore, and then click **Next**.
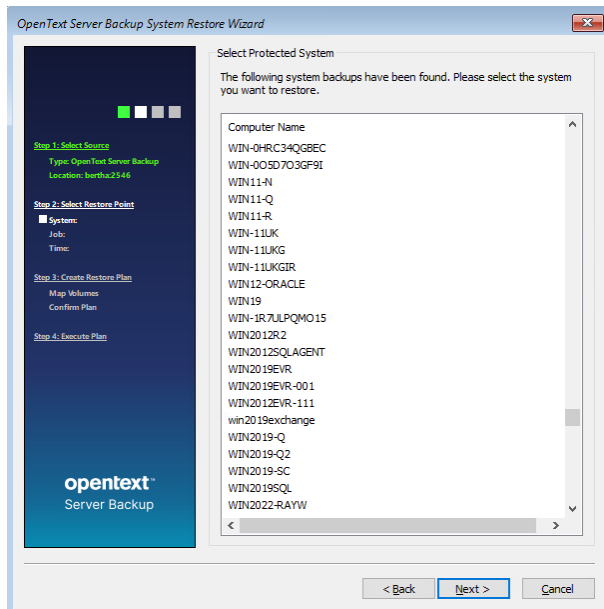

12. On the Select Backup Job page, click the BMR backup job from which you want to restore, and then click **Next**.

13. On the Select Restore Point page, click the start date and time of the BMR backup that you want to restore, and then click **Next**.

    Restore points are shown in the time zone selected in Step 2.

14. In the Password dialog box, enter the encryption password for the backup, and then click **OK**.

    To view a password hint, click the question mark (?) button.

    The Select Source and Destination Volumes page appears. This page shows disks and volumes in the protected (source) system and in the destination machine. Blue rectangles represent volumes that were backed up and can be restored. For more information, see Items on the Select Source and Destination Volumes page.
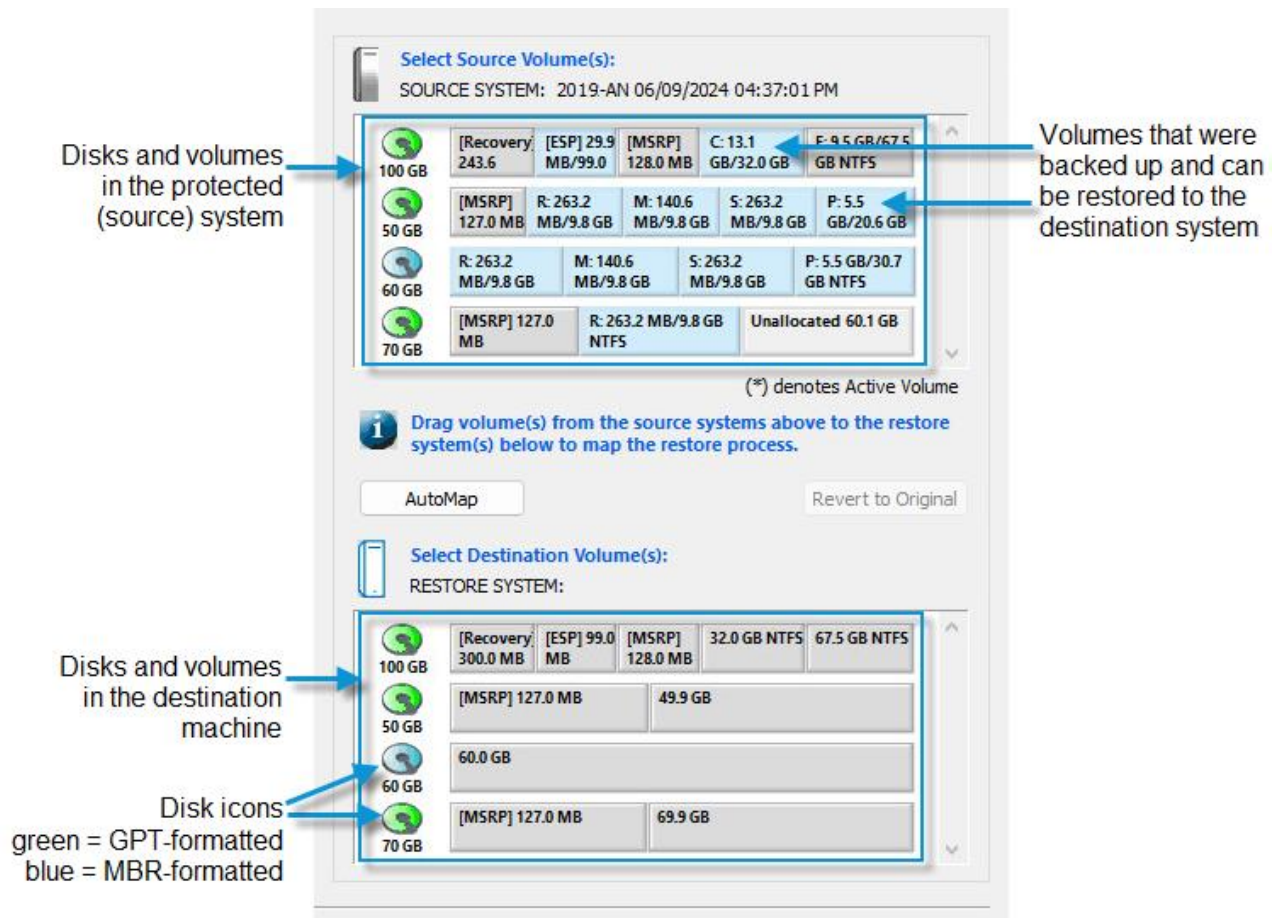
Note: If disks are missing from the destination machine, you might need to add drivers for a RAID controller or other disk device. See Install or update device drivers.

Step 3. Create a restore plan

You can create a restore plan on the Select Source and Destination Volumes page. A restore plan shows which volumes from the backup to restore to the destination machine.

15. To automatically map all protected volumes from the source (protected) system to the destination machine and clear any existing data from the destination machine, click **AutoMap**. For more information and requirements, see Automatically create a restore plan.
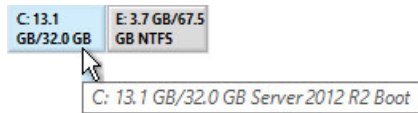
    Do one of the following:

    - To restore volumes as shown in the Destination Volumes area, click **Next**, and go to Step 4. Execute the restore plan.

    - To create a different restore plan, click **Revert to Original**, and continue with the following steps.

16. To make room for volumes that you want to restore by deleting a volume from the destination machine, right-click the volume, and click **Delete Volume**.

    Note: You cannot delete MSRP volumes using this method. To remove an MSRP volume, right-click the disk icon and change the disk format.

17. To view the entire label for a volume, point to the volume. The label appears in a tooltip.

18. Do one or more of the following until the Select Destination Volumes area shows the volumes that you want to restore to the destination machine:

    - To change the format of a disk in the destination machine from MBR to GPT or from GPT to MBR, delete all volumes from the disk (except for any MSRP volume), and then right-click the disk icon and choose **Convert to GPT disk** or **Convert to MBR disk**.
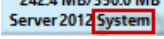
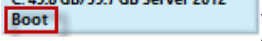   - If the protected (source) system has an "ESP" volume (e.g.,):

        i. Drag the ESP volume from the source system to the start of a GPT-formatted disk in the destination machine.

           If a message states that an EFI partition can only be restored to a UEFI system, you are trying to restore the system to a BIOS machine. You can only restore a UEFI-based system to a UEFI destination machine.

        ii. Drag the "Boot" volume from the source system to the right of the ESP volume in the destination machine.

        iii. Drag other volumes that you want to restore, if any, from the source system to the destination machine.

        Note: A system with an ESP volume is UEFI-based. See Restoring UEFI-based systems.

    - If the protected (source) system has a "System" volume (e.g.,):

        i. Drag the "Boot" volume (e.g.,) from the source system to the start of a GPT-formatted disk in the destination machine.

           If an ESP volume is created automatically in the destination machine, you do not need to restore the System volume.

        ii. If an ESP volume is not created automatically, drag the System volume to the right of the Boot volume.

           If a message states that the volume is an OEM volume, delete the Boot volume from the destination machine disk. Drag the System volume to the start of the

destination machine disk, and then drag the Boot volume to the right of the System volume. See [Restoring OEM partitions](#).

iii. Drag other volumes that you want to restore, if any, from the source system to the destination machine.

Note: A system with a "System" volume is BIOS-based. See [Restoring BIOS-based systems](#).

- To change the size of a volume from a File-based backup in the destination machine, right-click the volume and click **Edit Volume**. Enter a size for the volume, and then click **OK**.

  Note: You cannot change the size of a volume from an Image backup.

- To revert disks in the destination machine to their original state, click **Revert to Original**.

19. Click **Next**.

The Restore Plan Summary page lists changes that will be made in the destination machine if you run the restore.

Step 4. Execute the restore plan

20. Review the restore plan. Do one of the following:

- If you are not satisfied with the restore plan, click **Back** to change the restore plan or **Cancel** to cancel the restore.

- If you are satisfied with the restore plan, select **Click here to confirm the restore plan**, and then click **Next**.

  The restore begins. A message appears when the restore is finished.

21. Click **OK** in the message box, and then click **Next**.

22. Do one of the following:

- If the restore was successful and you want to start the restored system, select **Reboot the system**. Click **Finish**.

- If the system was successfully restored but the destination machine hardware is significantly different than the original machine, click **Next** to proceed to the repair wizard. See [Repair a restored system](#).

- If the restore failed, exit from the wizard.

Notes:

- A restore must finish within 72 hours, or it will fail.

- After you restore a system with more than one disk, you might need to bring the disks online using the Disk Management utility or diskpart command interpreter in Windows.

- After you restore a system, you must synchronize the existing backup job before running it to back up the restored system.

4.1   Vault certificate validation and pinning

Beginning in version 9.10, when System Restore first tries to connect to a Director version 8.6*x* or later vault where certificate pinning is enabled, it checks the vault's TLS certificate.

If System Restore determines that the vault certificate is a valid certificate from a certificate authority (CA), the next restore wizard page appears.

If System Restore cannot validate the vault certificate (e.g., because the certificate is self-signed or expired, or because System Restore does not have internet access), a Vault Certificate Verification dialog box shows the following messages:

> Unable to verify certificate due to: *<reason the certificate cannot be verified>*
> Do you want to accept this certificate and connect to this vault?

You can then review vault certificate information in the dialog box, and accept or decline the vault connection. If you accept the vault connection, the next restore wizard page appears. If you do not accept the vault connection, you can either select a different backup source or cancel the restore.

After a vault certificate is validated or you accept a vault connection, if System Restore tries to connect to the vault again (e.g., after a network interruption), it checks whether the public key of the vault certificate is the same as when System Restore first connected to the vault.

If the public key of the vault certificate is the same, the next restore wizard page appears.

If the public key of the vault certificate is different, System Restore will not connect to the vault and the following message appears: *Pinned certificate changed. Connection not allowed.* If this occurs, you must restart System Restore and try the restore again so that System Restore can try to validate the new vault certificate.

Note: Each time you start System Restore and choose a vault, System Restore tries to validate the vault certificate. System Restore does not "remember" a vault certificate after you restart System Restore.

4.2   Automatically map volumes from backups to destination machines

Beginning in version 9.40, System Restore can automatically map volumes from a backup to a destination machine. This simplifies the restore process, as you do not have to manually drag volumes from the source system to the destination machine in the System Restore wizard.

If you click the **AutoMap** button during a restore, System Restore automatically maps all protected volumes from the source (protected) system to corresponding disks on the destination machine, and clears any existing data from the destination disks. Data is not cleared from disks that are not destinations in the restore. For example, as shown in the following diagram, volumes from Disk 0 and

Disk 2 in a source system are mapped to Disk 0 and Disk 2 in the destination machine, and existing data remains on Disk 1 in the destination machine.
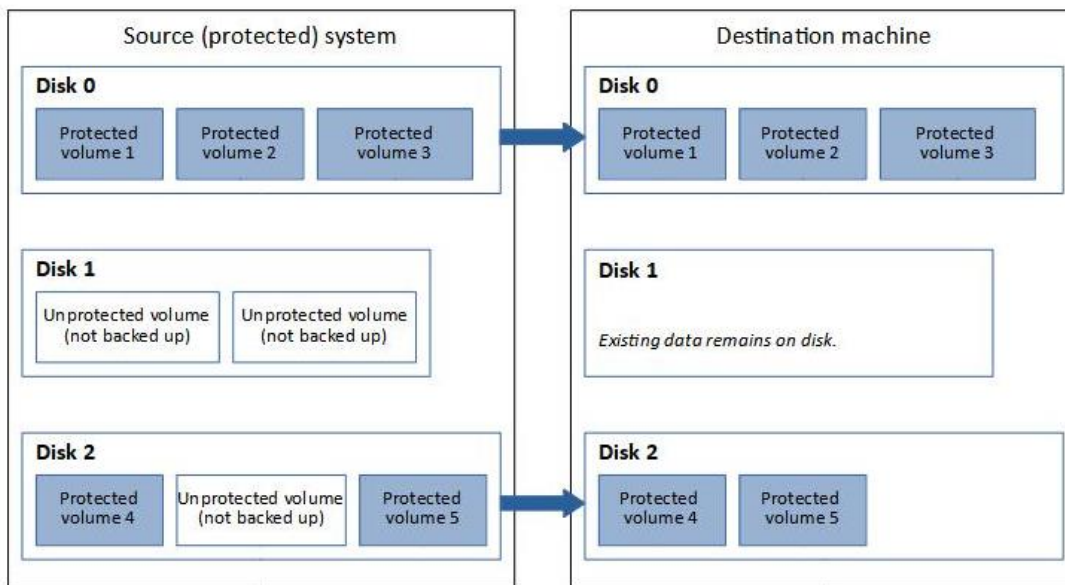
The AutoMap feature is available when the source and destination systems meet the following requirements:

- The source and destination systems use the same firmware: either UEFI or BIOS.

- The source (protected) system has a maximum of four disks. None of the protected disks can be dynamic disks.

- The destination machine has a maximum of four disks. None of the disks can be larger than 2 TB.

- The destination machine has the same number or more disks than in the source system. For example, if volumes are backed up on the first three disks in a source system, the destination machine must have three or more disks. If volumes are backed up on the first, third and fourth disk in the source system, the destination machine must have four disks.

- Disks where volumes will be restored on the destination machine are the same size or larger than the corresponding disks on the source (protected) system.
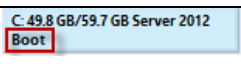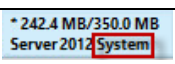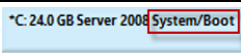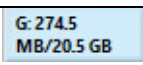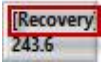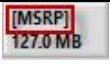
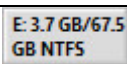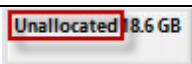*Note:* These conditions are usually met if you restore a system to the same hardware where it was backed up.

To automatically create a restore plan, click the **AutoMap** button during a restore. See Step 3. Create a restore plan.

If the **AutoMap** button is not available, check the restore log to determine the reason. If the log does not state why the AutoMap feature is not available, set the logging to a lower level. See Configure restore log settings.

4.3 Items on the Select Source and Destination Volumes page

As described in Step 3. Create a restore plan, the Select Source and Destination Volumes page shows disks and volumes in the protected (source) system and destination machine. The following table describes items on the page.

Item	Example	Description
Blue rectangles		**Volumes that are backed up and can be restored**
ESP/EFI partition	[ESP] 29.9 MB/99.0	An Extensible Firmware Interface (EFI) System Partition. A UEFI-based system must have an EFI system partition or the system will not boot up. See Restoring UEFI-based systems.
Boot volume	C: 49.8 GB/59.7 GB Server 2012 Boot	A boot volume. A BIOS-based system must have a boot volume or the system will not boot up. See Restoring BIOS-based systems.
System volume	* 242.4 MB/350.0 MB Server 2012 System	A system volume. A BIOS-based system must have a system volume or it will not boot up. See Restoring BIOS-based systems. A volume with the "System" label can also be an OEM partition. See Restoring OEM partitions.
System and Boot volume	*C: 24.0 GB Server 2008 System/Boot	A volume that is both a system and boot volume. See Restoring BIOS-based systems.
Optional volume	G: 274.5 MB/20.5 GB	Volume that was backed up and can be restored, but is not required for the destination machine to boot up.
Gray rectangles		**Volumes that are not backed up and cannot be restored**
Recovery volume	[Recovery] 243.6	A recovery volume that contains system files, drivers and factory default setup information. Recovery volumes are not backed up.
MSR partition	[MSRP] 127.0 MB	Microsoft Reserved (MSR) partition. An MSR partition is disk space reserved for Windows use on a GPT disk. If one is required in the destination machine, it is created automatically.
Volume	E: 3.7 GB/67.5 GB NTFS	In a source system, a volume that was not backed up. In a destination machine, an existing volume on the disk. You can delete, change or overwrite an existing volume.
Unallocated space	Unallocated 18.6 GB	Unallocated space on a disk.
Free space	FREE 9.8 GB	Free space on a disk.

Item	Example	Description
Disk icons		**One icon for each disk. The icon color represents the disk format.**
		GPT-formatted disk. If you drag a volume to an uninitialized disk on a UEFI destination machine, the disk type automatically changes to GPT.
		MBR-formatted disk
		Uninitialized disk

## 4.4 Set up a network connection for System Restore

To connect to a vault during a restore, System Restore requires a network connection. Normally, System Restore sets up a network connection automatically. However, if DHCP is not configured on the network or you want to use a static IP address, you can set up the connection manually.

Note: This process sets up a network connection for System Restore, not the restored system. You can configure networking for the restored system after you start it.

To set up a network connection for System Restore:

1. In the System Restore wizard, do one of the following:

    *   To set up a default network connection, click **Settings** on the System Restore main menu page.

    *   To set up a network connection for a specific restore, click **Restore Settings** on the Choose Backup Location page.

    The Settings dialog box shows recognized network adapters in the destination machine. The Device Properties area shows driver information for the selected adapter.
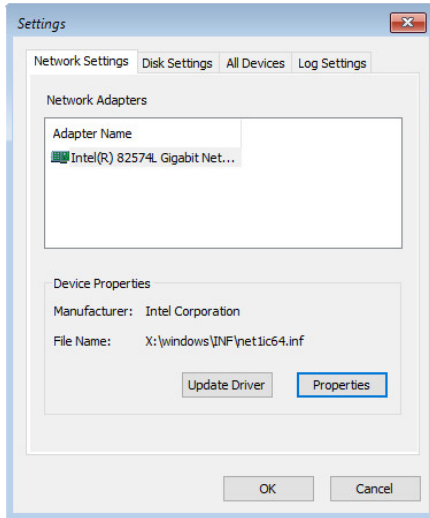
2. To install or update the driver for a network adapter, select the adapter, and then click **Install** or **Update Driver**. In the Install Driver dialog box, do one of the following:

    *   To install the driver from a local disk, select **Local Disk.** Browse to the .inf file location, or enter the path to the driver manually.

    *   To install the driver from a network share, select **Network Share**, and enter the path to the .inf file. You cannot browse to a network share.

3. Select the network adapter to use for the network connection.

4. Click **Properties**. If a driver is installed for the adapter, a LAN is connected, and a port is enabled, the Network Configuration dialog box appears.
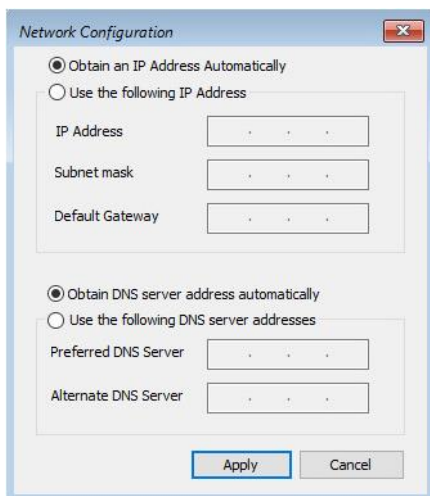
5. In the Network Configuration dialog box, select **Use the following IP Address**.

6. Enter the IP address, subnet mask, and default gateway for the network adapter.

7. If you have DHCP and want to access other systems using domain names instead of IP addresses, select **Use the following DNS server addresses**. 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.

8. Click **Apply**.

4.5 Install or update device drivers

System Restore includes commonly-used recovery-critical drivers. You can install other drivers for destination machine devices. For example, if you cannot see all available storage devices in the destination machine when restoring a system, you might need to add a driver for a RAID controller or other disk device. You can also update existing drivers.

To install or update a device driver:

1. In the System Restore wizard, do one of the following:

   - To change the default network settings, click **Settings** on the System Restore main menu page.


   - To change network settings for a specific restore, click **Restore Settings** on the Choose Backup Location page.

   The Settings dialog box shows recognized network adapters in the destination machine. The Device Properties area provides driver information for the selected adapter.

2. In the **Settings** dialog box, do one of the following:

   - To install or update a network adapter driver, click the **Network Settings** tab.

   - To install or update a storage device driver, click the **Disk Settings** tab.

   - To install or update another device (e.g., PCI device) driver, click the **All Devices** tab.

   The tab lists devices in the destination machine.
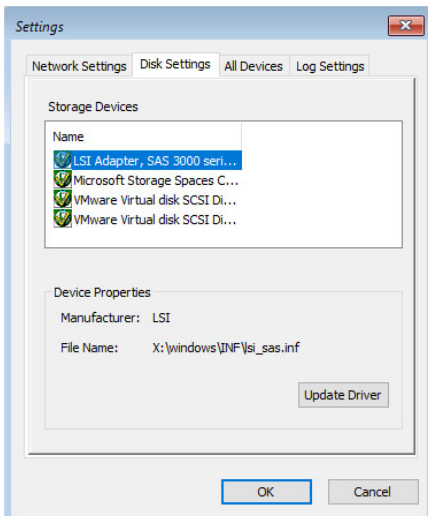
3. Select the device for the driver installation or update.

   If there is no driver for the device, the Install button will appear. If there is a driver, the Update Driver button will appear.

4. Click **Install** or **Update Driver**. In the driver dialog box, do one of the following:

   - To install the driver from a local disk, select **Local Disk.** You can then browse to the .inf file location, or enter the path to the driver manually, and click OK.

   - To install the driver from a network share, select **Network Share**. You can then enter the path to the .inf file manually, and click OK. You cannot browse to a network share.

5. Click **OK**.

4.6 Configure restore log settings

You can configure the following settings for System Restore restore logs:

- Level of detail. You can include error messages only, warning and error messages, or all messages in the logs. You can also disable logging.

- Maximum log file size. When the maximum log file size is reached, the log starts overwriting the file from the beginning. By default, the maximum log file size is 100 MB.

- Log file location. By default, the log file is saved on the X: RAM drive, which is lost after reboots. We recommend saving logs on a separate device.

To configure restore log settings:

1. On the System Restore main menu page, click **Settings**.

2. In the **Settings** dialog box, click the **Log Settings** tab.
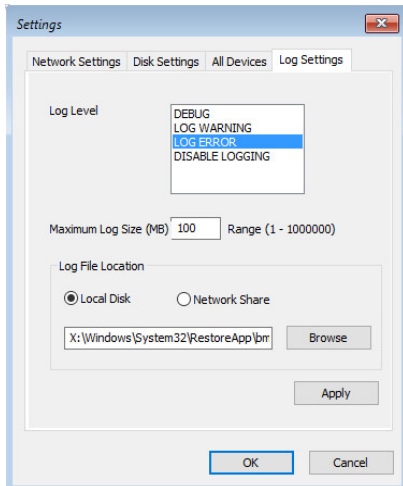
3. In the **Log Level** list, do one of the following:

   - To record all messages in the log, select **Debug**.

   - To record warning and error messages, select **Log Warning**.

   - To only record error messages, select **Log Error**.

   - To not generate a log, select **Disable Logging**.

4. To change the maximum log file size, enter the size in MB in the **Maximum Log Size** field.

5. To change the log file location, do one of the following:

   - To specify a log file location on a local disk, select **Local Disk.** Browse to the location, or enter the path manually.

   - To specify a log file location on a network share, select **Network Share**, and enter the path manually. You cannot browse to a network share.

6. Click **Apply**.

7. Click **OK**.

4.7   Run Windows utilities from a command prompt

You can open a command prompt from System Restore and run Windows utilities that are available in the Windows Preinstallation Environment (WinPE). For example, you could open a command prompt and use ping to check for network connectivity to the vault.

To run Windows utilities from a command prompt:

1. On the System Restore main menu page, click **Command Prompt**.

The command prompt window opens.

2. Run Windows utilities from the command prompt.

5   Repair a restored system

If you restore a system to a destination machine with significantly different hardware, the restored system might not be able to boot. Drivers might be missing for boot-critical devices, and the Hardware Abstraction Layer (HAL) and kernel might not be optimal for the destination machine. You can repair boot-critical devices and perform HAL and kernel repairs using System Restore.

Some drivers, such as network drivers, are not necessary for booting a system. After starting a restored system, Windows can update drivers for devices that are not boot-critical.

Windows Server 2012 and later can repair drivers at boot if the drivers are provided with Windows.

To repair a restored system:

1. If System Restore detects that system repairs are necessary after a restore, the repair wizard starts automatically at the end of a restore.

    To start the repair wizard manually, click **Repair My System** on the Main Menu page.

2. In the operating system list, select the operating system to repair.

    The repair wizard shows information about the operating system, hardware, and boot-critical devices. Status icons appear for the operating system and device drivers. For more information, see Items in the repair wizard.
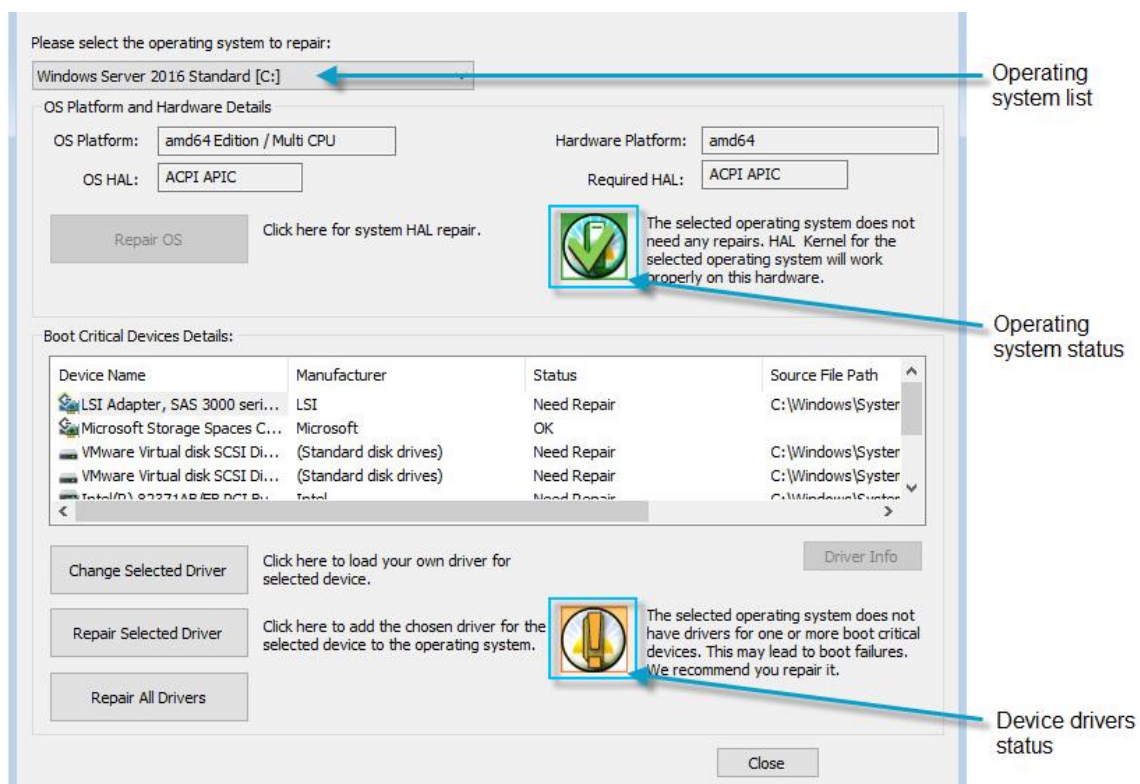
3. If a yellow operating system status icon appears in the OS Platform and Hardware Details area, the operating system needs to be repaired. Click **Repair OS**.

4. If a yellow status icon appears in the Boot Critical Devices Details area, at least one boot-critical driver needs repair. Do one or more of the following:

   - To repair drivers for all boot-critical devices that need repair, click **Repair All Drivers**.

   - To repair the driver for one boot-critical device that needs repair, click the device name and then click **Repair Selected Driver**.

     If System Restore cannot automatically repair the driver, a **Browse for Folder** dialog box appears. If you added the driver when you created the recovery media (see Create recovery media), you can find the driver (.inf) files in the Boot drive (usually X:\) in ..\Windows\System32\RestoreApp.

   - To install a specific driver for a device, click the device name and then click **Change Selected Driver**. In the Browse for Folder dialog box, select the folder that contains the .inf file. If System Restore cannot find a matching .inf file in the selected folder, a message appears.

   Note: If System Restore does not find the best driver for a device, it might use a more generic driver. Ideally, provide the latest driver (from the vendor) for your specific hardware.

5. Click **Close** to exit from the repair wizard.

5.1 Items in the repair wizard

As described in Repair a restored system, the repair wizard shows status icons for the operating system and boot-critical device drivers. The following table describes possible icons and statuses.

Icon	Description
OS Platform and Hardware status icons	
	Repair is not required. The HAL or kernel does not need to be adjusted for the current hardware.
	Repair is required. The operating system might not be able to boot with the current HAL. This can occur, for example, if you restore a single-CPU operating system to hardware with multiple CPUs or cores. In this instance, you can repair the operating system so that it uses all CPUs.
	Repair is not possible. The selected operating system is not compatible with the current hardware. For example, you cannot restore a non-ACPI operating system to ACPI-compatible

| Icon	Description
	hardware.
Boot Critical Devices status icons	
	Device drivers are OK. The selected operating system does not need new drivers for boot-critical devices.
	At least one device driver needs repair. The Status column for each device indicates whether its driver is OK or needs repair.

6   System-specific restore information

This section provides information about restoring specific types of Windows systems, including:

- Restoring UEFI-based systems

- Restoring BIOS-based systems

- Restoring systems with OEM partitions

- Restoring application servers

- Restoring systems with device installation restrictions

- Restoring data to the original volume

- Restores with dynamic disks and spanned volumes

6.1   Restoring UEFI-based systems

If a protected (source) system on the Select Source and Destination Volumes page includes a partition labeled "ESP", the system is UEFI-based. An ESP (EFI system partition) is required for a restored UEFI system to boot into Windows.
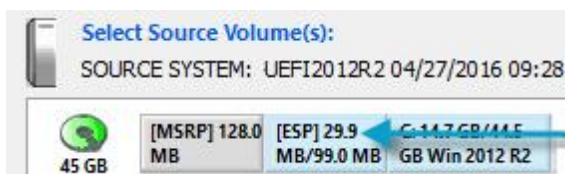
You can only restore a UEFI-based system to a UEFI destination machine. You cannot restore a UEFI-based system to a BIOS destination machine.

Restore the ESP partition from the source system to a GPT-formatted disk in the destination machine. If you drag a volume to an uninitialized disk on a UEFI system, the disk type automatically changes to GPT.

If an ESP volume already exists in the destination machine, the ESP partition from the protected machine should overwrite the existing ESP partition. You can also delete an existing ESP partition if, for example, it is too small to overwrite.

The order of partitions on the GPT disk should be: ESP, OEM (if any) and MSR followed by primary data partition(s). Partition order rules are enforced during a restore.

If required, an MSR (Microsoft Reserved) partition is automatically created on the destination machine during a UEFI system restore.

6.2 Restoring BIOS-based systems

If a protected (source) system on the Select Source and Destination Volumes page includes a partition labeled "System", the system is BIOS-based.

You can restore a BIOS-based system to a UEFI or BIOS destination machine.

Restoring a BIOS-based system to a UEFI destination machine

If you drag the Boot volume from a protected BIOS-based system to a UEFI destination machine, an ESP volume is generated automatically in the destination machine. An ESP (EFI system partition) is required for a UEFI system to boot into Windows.

The ESP partition must be on a GPT-formatted disk in the destination machine. If you drag a volume to an uninitialized disk on a UEFI system, the disk type automatically changes to GPT.
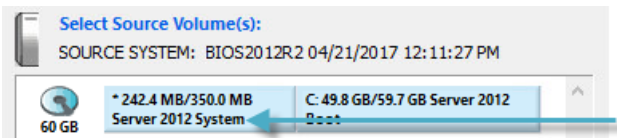
The order of partitions on the GPT disk should be: ESP, OEM (if any) and MSR followed by primary data partition(s). Partition order rules are enforced during a restore.

If required, an MSR (Microsoft Reserved) partition is automatically created in the destination machine.

You do not have to restore the System volume from a protected BIOS-based system to a UEFI destination machine.

When restoring a volume from a BIOS-based system to a UEFI destination machine, there might not be enough space, even if the destination disk is the same size. This problem can occur because an uninitialized UEFI disk defaults to GPT format and additional space is required for a GPT partition table. To prevent this problem, choose a larger destination volume or convert the volume to MBR format.

Restoring a BIOS-based system to a BIOS destination machine

To restore a BIOS-based system to a BIOS destination machine, you must restore both the System volume and the Boot volume from the source to the destination machine. The destination disk must use MBR formatting. A BIOS-based system can have GPT-formatted disks, but cannot boot from a GPT disk.

An active partition is required for booting. The active partition is marked with an asterisk (*).

To avoid losing disk space, initialize all disks larger than 2TB as GPT format. MBR partitioning does not allow to use disk space beyond 2TB.

If the destination machine does not boot after the restore, you may need to go into the BIOS and select the disk for booting. Dragging the System/Active volume to the first disk in the destination machine usually avoids this problem.

6.3 Restoring systems with OEM partitions

You can restore a BIOS-based system with an Original Equipment Manufacturer (OEM) partition to a BIOS or UEFI destination machine.

Note: A "System" label appears on an OEM partition on the Select Source and Destination Volumes page in the restore wizard.

When restoring a protected (source) system with an OEM partition to a BIOS destination machine, the OEM partition must be restored or the system will not boot up. The OEM partition must be restored to the start of a destination machine disk.

When restoring a protected (source) system with an OEM partition to a UEFI destination machine, the OEM volume is not required for booting and does not have to be restored.

If you restore a system with an OEM operating system license to dissimilar hardware, the system might boot but you will not be able to log in to the system without activating Windows. This occurs because OEM licenses are not transferable. When the restore process finishes, contact Microsoft to activate the Windows license.

6.4 Restoring application servers

To fully protect an application server (e.g., a server running Microsoft SQL Server), you must back up the operating system, application binaries, and application data.

If you use an application-specific plug-in (e.g., SQL Server Plug-in) to back up application data, you need a separate BMR job to back up the server operating system and application binaries.

To restore the application server, you can:

1. Use System Restore to restore the operating system and application binaries to a destination machine.

2. If required, install an Agent and required plug-ins on the restored system.

   Note: If an Agent was installed on the protected system, it should have already been restored.

3. Use the appropriate plug-in to recover application data to your system.

   For information about steps 2 and 3, see the Portal online help or *Windows Agent and Plug-ins Guide*.

If you use the Image Plug-in to create a BMR and SQL application aware backup job, you should be able to restore a working SQL Server using System Restore. However, System Restore will not prompt you to restore all SQL Server volumes. It will only require you to restore volumes that are required for booting.

6.5 Restoring systems with device installation restrictions

When device installation restrictions in a system's group policy could prevent a restored system from starting successfully, System Restore tries to change the device installation restrictions during a restore.

You can change the device installation restrictions back after starting the restored system.

To change device installation restrictions on a Windows 7 or Windows Server 2008 R2 system, see Microsoft KB article 2773300.

To change device installation restrictions on a system running Windows 8, Windows Server 2012, or a later Windows version, do the following:

1. Start the restored computer.

2. Install required drivers.

3. Using the Registry Editor, import the HKEY_LOCAL_MACHINE_SYSTEM_DriverDatabase_Policies_Restrictions.reg file from the root of the Windows directory drive (usually drive C) into HKEY_LOCAL_MACHINE\SYSTEM\DriverDatabase\Policies\Restrictions.

4. Using the Group Policy Editor, apply a change to a setting in Local Computer Policy\Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions. The group policy settings will then be applied to the computer.

6.6 Restoring data to the original volume

If you restore a volume from a Local System BMR backup (not an Image BMR backup) to the original simple volume, you might have the option to merge data with existing data.

Merging data is strongly discouraged because:

- The machine can run out of space during the restore.

- The machine might not boot after the restore.

- You could restore from an NTFS volume to a FAT volume and lose security and other streams.

## 6.7 Restores with dynamic disks and spanned volumes

System Restore can only restore volumes to basic disks. It cannot create dynamic disks, and cannot restore volumes to dynamic disks on destination machines. You can convert basic disks to dynamic disks after starting a restored system.

Dynamic disks do not appear to be dynamic on the Select Source and Destination Volumes page of the restore wizard. When a volume in a protected (source) system spans dynamic disks, each portion of the spanned volume appears as a separate volume with the same drive letter. When a destination machine disk has dynamic partitions, one large volume appears for all dynamic partitions on the disk.

As an example, consider the system shown in the following Disk Management screen. This system has three dynamic disks (Disks 1, 2 and 3) and four volumes (R, M, S and P) that span disks.
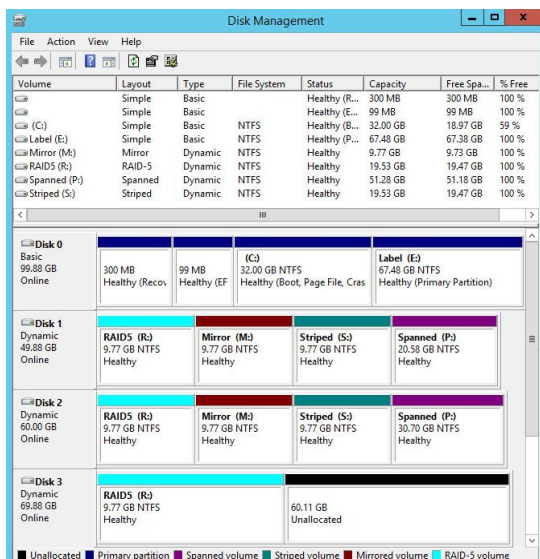

When this system is the protected (source) system in System Restore, each portion of a spanned volume appears as a separate volume with the same drive letter. For example, the R spanned volume is shown as three separate R volumes.
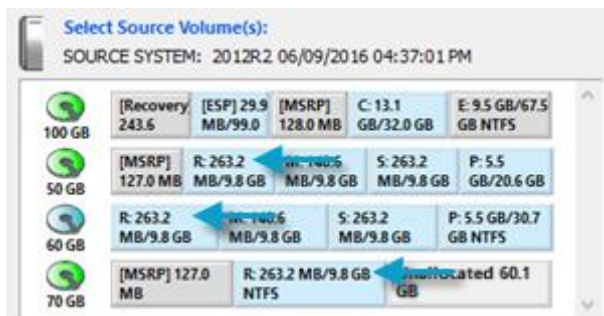

When this system is the destination machine in System Restore, all dynamic partitions on a disk appear as one large volume. For example, a 49.9 GB volume represents the portions of volumes R, M,

S and P on Disk 1. You must delete this volume before you can restore data to the disk. Similarly, you must delete the 60.0 GB and 69.9 GB partitions before you can restore data to them.
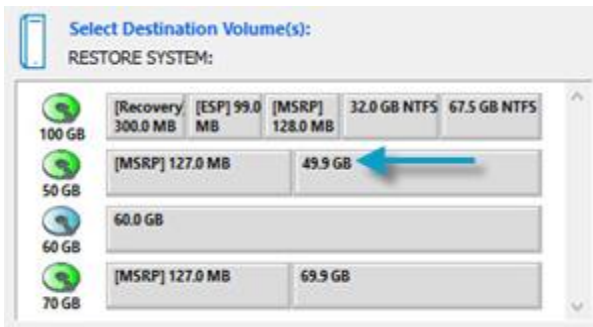
When you restore a spanned volume to a destination machine, one basic volume is created for the contents of the entire spanned volume. The volume contains as much space as the original volume, unless a volume was only partially full and can fit in the destination disk. Volumes can only be restored as simple volumes, not spanned, RAID5, mirrored or striped.

The following screenshot and table show how volumes from the sample system are restored:
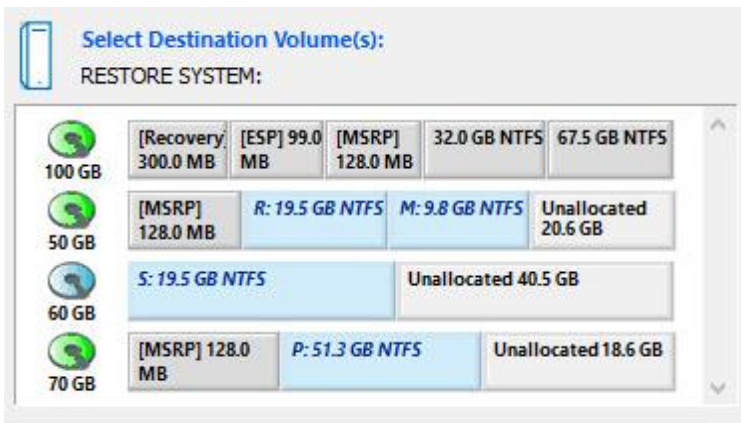
Volume	Original	Restored
P	Spanned volume with two parts: 20.6 GB and 30.7 GB	One 51.3 GB volume (20.6 GB + 30.7 GB)
S	Striped volume with two 9.8 GB parts	One 19.5 GB volume (approx. 2 * 9.8 GB)
M	Mirrored volume with two 9.8 GB parts. Second part for mirroring only.	One 9.8 GB volume
R	RAID5 volume. Three portions; 9.8 GB each. 2/3 of the RAID volume was used for data. The rest was used for parity.	One 19.5 GB volume (approx. 2/3 * (3 * 9.8 GB)

7   Server Backup Support

If you have a question about OpenText Server Backup that isn't covered in this guide, our frequently-updated Knowledge Base contains comprehensive information. The Knowledge Base is your first stop when searching for any OpenText Server Backup solutions you may need. We highly recommend searching here first for the quickest answers to your questions.

7.1 Contacting Support
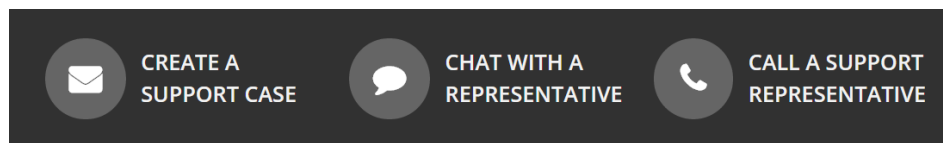
If you need live assistance from a qualified support agent, OpenText Support is here for you 24 hours a day, 7 days a week (excluding US holidays). Please feel free to get in touch with us, and we'll help out any way we can! You can find the contact information for OpenText Support in the Knowledge Base.

Tip: When contacting Support with a technical issue, please have both the program's log files and the store you are having difficulty with ready.

To gather log files, click **File** menu and choose *Open log folder*. Compress the contents of the folder in a .zip file and attach it to your support request.

If the log archive and/or mail store exceeds 10MB, you may not be able to send them as an email attachment. In that case, upload instructions will be provided to you upon request.