



CoBMR For Windows

Bare Machine Recovery for Cohesity DataProtect

User Guide

Version 9.6.1 released April 2024

Copyright © 2019-2024 Cristie Software Ltd.
All rights reserved.

The software contains proprietary information of Cristie Software Ltd.; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between Cristie Software Ltd. and the client and remains the exclusive property of Cristie Software Ltd. If you find any problems in the documentation, please report them to us in writing. Cristie Software Ltd. does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Cristie Software Ltd.

- *IBM Tivoli Storage Manager (TSM), AIX and TIVOLI are trademarks of the IBM Corporation.*
- *IBM Spectrum Protect is a trademark of the IBM Corporation.*
- *IBM Virtual I/O Server (VIOS) is a trademark of the IBM Corporation.*
- *NetWorker and Avamar are trademarks of the Dell EMC Corporation.*
- *vSphere, vCenter and vCloud are trademarks of VMware Inc.*
- *Hyper-V is a trademark of Microsoft Corporation.*
- *Azure is a trademark of Microsoft Corporation.*
- *Amazon Web Services (AWS) and Amazon Elastic Compute Cloud (EC2) are trademarks of Amazon.com, Inc.*
- *Cohesity DataProtect is a trademark of Cohesity Inc.*
- *Rubrik is a trademark of Rubrik Inc.*
- *CloneManager® is a registered trademark of Cristie Software Ltd.*
- *SysBack is a registered trademark of Cristie Software Ltd.*

PC-BaX, UBax, Cristie P4VM (Protect for VMs), Cristie Storage Manager (CSM), SDB, ABMR (Bare Machine Recovery for EMC Avamar), NBMR (Bare Machine Recovery for EMC NetWorker), TBMR (Bare Machine Recovery for Spectrum Protect/TSM), CBMR (Cristie Bare Machine Recovery), CoBMR (Bare Machine Recovery for Cohesity DataProtect), RBMR (Bare Machine Recovery for Rubrik) and CRISP (Cristie Recovery ISO Producer) are all trademarks of Cristie Software Ltd..

Cristie Software Ltd
New Mill
Chestnut Lane
Stroud
GL5 3EW
UK

Tel: +44 (0) 1453 847009
Email: support@cristie.com
Website: <https://www.cristie.com>



Contents

1	Document Conventions	5
2	Overview	6
	2.1 Prerequisites	6
	2.2 Backup Process	6
	2.3 Recovery Process	7
3	Create The Bootable Recovery Environment	9
4	The CoBMR Create Configuration Tool	10
	4.1 Creating the Configuration Information	10
	4.2 Backup of Boot and Hard-Link Files	12
	4.3 Creating a CoBMRCfg Pre-Schedule	12
5	Using a Cohesity DataProtect Backup for Disaster Recovery	14
6	Multi-factor Authentication	15
7	Restoring your System	17
	7.1 File- or Block-based Recoveries	17
	7.1.1 Booting the WinPE5, WinPE10 or WinPE11 DR Environment	18
	WinPE5, WinPE10 or WinPE11 Based CoBMR Recovery Environment.....	18
	7.1.2 Block Based Recovery Settings	19
	7.2 Begin the Restore Process	20
	7.2.1 CoBMR Recovery Environment Main Menu	21
	7.2.2 Logfile Save Path	24
	7.2.3 Specify Cohesity DataProtect Details and Recovery Date/Time	26
	7.2.4 Storage Pools	27
	7.2.5 Confirm Volume Layout	32
	7.2.6 Select Volumes To Restore	38
	7.2.7 Clone Settings	39
	7.2.8 Dissimilar Hardware	40
	7.2.9 Disk Recovery Status	41
	7.2.10 Disk Scaling	45
	7.3 Tools	46
	7.3.1 Dissimilar Hardware Wizard	48
	7.3.2 Load a Driver	54
	7.3.3 Copy Logfiles	55
	7.4 View Logs	56



7.5	Configure Network	57
7.5.1	Configure NIC Parameters	58
7.5.2	Assign Static or DHCP IP Settings	61
7.5.3	Map a Network Drive	62
7.5.4	Unmap a Network Drive	63
7.5.5	Setup DNS Servers	64
7.5.6	Setup Network Identification	65
7.6	Configure Routing	66
7.6.1	IPv4 Routes	66
7.6.2	Diagnostics	68
7.7	Reboot	70
7.8	Active Directory Recoveries	70
8	Appendices	71
8.1	Storage Space support	71
8.2	UEFI and MBR BIOS support	72
9	Cristie Technical Support	78



1 Document Conventions

The following typographical conventions are used throughout this guide:

<code>/etc/passwd</code>	represents command-line commands, options, parameters, directory names and filenames
<code>Next ></code>	used to signify clickable buttons on a GUI dialogue
Note:	describes something of importance related to the current topic



2 Overview

This document describes the essential elements of **Bare Machine Recovery for Cohesity DataProtect (CoBMR)** and Disaster Recovery based upon a tailored WinPE5, WinPE10 or WinPE11 recovery module. It is based upon version 9.6.1 of the software.

This document describes the steps required to install, configure and use the Bare Machine Recovery for Cohesity DataProtect (CoBMR) product. Refer to the product Readme for installation requirements and late breaking information associated with this release.

2.1 Prerequisites

Note: Please refer to the product Readme for the supported operating systems, RAM and free disk space required. A full list of supported Cohesity DataProtect clients and servers is included in the Readme.

It is recommended that Windows **VSS (Volume Shadow Copy Services)** is enabled for all drives being backed up to ensure that all open files are captured by the Cohesity DataProtect backup process. This will allow important OS and application data files that are normally held open to be successfully and consistently backed up.

Note that by default the Cohesity DataProtect backup client will enable VSS for System State and System Services, but not necessarily all application data files.

2.2 Backup Process

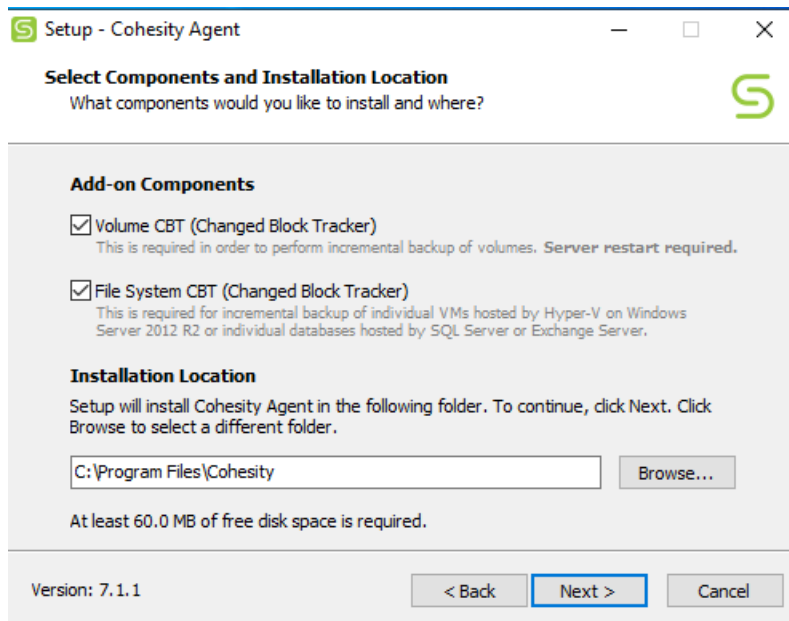
CoBMR allows you to perform a bare machine recovery of your system direct from a Cohesity DataProtect backup.

To do this you must first prepare your system using the process outlined below:

Installation (refer to the CoBMR Installation and Licensing Guide)

- *Install the Cohesity DataProtect agent. Please follow Cohesity recommendations regarding the Component installs: Volume CBT (Change Block Tracker) and/or File System CBT (Change Block Tracker).*





The Volume CBT option will be required when performing block-based backup and disaster recovery. This will require a reboot of the host.

- Install the CoBMR configuration software on the client system to be protected
- License the software (using a Trial or Full license)

Configuration

- Save the configuration parameters.
- Install and run the Cristie Recovery ISO Producer (CRISP) tool on a suitable system to create the CoBMR WinPE5, WinPE10 or WinPE11 based DR environment. This only needs to be done once.

Backup system and user data

- [Perform regular standard](#) Cohesity DataProtect [backups](#) as required

You will then be ready to [Restore the system from the Disaster Recovery Backup](#).

2.3 Recovery Process

In the event of a disaster, having previously taken a Cohesity DataProtect backup of the system and stored the configuration information, Windows WinPE5, WinPE10 or WinPE11 mode DR enables you to restore your system to the state at the last Cohesity DataProtect backup.

The CoBMR recovery console must be created first by using the Cristie Recovery ISO Producer (CRISP) tool. The output from this tool is a bootable WinPE5, WinPE10 or WinPE11 ISO which can be either burnt to physical CD/DVD media, imaged to a USB flash drive or used directly in a virtual environment.

If your machine supports bootable USB flash drives or CD/DVDs, this is the most convenient way to boot the DR module. If the system does not support bootable USB flash drives or CD/DVDs, you can boot from the network. Contact Cristie for details on



how to set this up.

Windows WinPE5, WinPE10 or WinPE11 offers several advantages, namely:

- *a familiar Windows GUI*
- *the ability to inject new mass storage drivers during the boot process*
- *all variations of Windows dynamic disks are supported (ie. mirrored, spanned, striped and RAID-5)*
- *NTFS volumes/partitions are created natively*
- *support for NTFS mounted folders (junctions) and hard links*
- *the restored backup contains the original file security information*
- *BIOS (MBR) to UEFI (GPT) conversion on recovery*

The WinPE5, WinPE10 or WinPE11 recovery process has five main steps:

- 1. Load Configuration data*
- 2. Rebuild storage devices (hard disks)*
- 3. Restore OS files from an Cohesity DataProtect backup*
- 4. Dissimilar Hardware and inject new drivers (if necessary)*
- 5. Boot into the recovered system*



3 Create The Bootable Recovery Environment

The supplied CRISP tool is used to create the CoBMR recovery environment. This environment is based upon a customised version of Microsoft's WinPE version 5 (WinPE5), WinPE10 or WinPE11.

Cristie Software Ltd. recommend using the WinPE10 or WinPE11 based environment if possible. This is based upon Windows 10/11 and is more likely to be compatible with modern hardware. Use the WinPE5 legacy version for Windows 2012R2 or earlier.

Once created the recovery environment is booted on the target system and then manages the restore process.

The CRISP tool should be run in conjunction with the supplied CRISP WinPE5, WinPE10 and WinPE11 Filesets for CoBMR 9.6. The fileset(s) should be installed alongside the CRISP on the same host.

CoBMR requires a specific Cohesity DataProtect client to be added during the creation of the CoBMR recovery environment ISO. You will need to specify or browse to a folder containing the appropriate Cohesity DataProtect 64-bit (WinPE5/WinPE10/WinPE11) client installation executable file (with file extension .EXE). An example of this is Cohesity_Agent_7.1.1_20231128_Win_x64_Installer.exe. **This is important; it will not be possible to create the bootable recovery ISO/USB flash drive without this Cohesity DataProtect client installation file.**

Note: Always use a 64-bit (x64) version for WinPE5/WinPE10/WinPE11 based builds.

You will need to create separate ISOs/USB flash drives for each Cohesity DataProtect client used. Use an ISO/USB flash drive version that corresponds to the client version used for the backup. So, for example, use an ISO/USB flash drive created with the Cohesity DataProtect client version 7.1.1 to match backups made with that version.

A full discussion of how to install and run CRISP is contained in the separate **CRISP User Guide**. Note that CRISP does not need to be installed on the system to be backed up; any suitable host machine will do.

Output from the CRISP tool is either a bootable WinPE5, WinPE10 or WinPE11 ISO file which can then be burnt to physical media (CD or DVD) or mounted directly in a VM environment or a bootable USB flash drive. This media is then booted on the target machine to manage the recovery operation.

Note: Microsoft Powershell is now available in the WinPE5, WinPE10 or WinPE11 DR environments. However this option must be selected when you create the ISO or bootable USB flash drive.



4 The CoBMR Create Configuration Tool

Configuration information is saved by default to the **CoBMRCFG** folder on the Windows system partition. This cannot be changed.

The Cristie tool that provides this function is called **CoBMRCfg.exe** which is located in the CoBMR installation folder (normally **Program Files\Cristie\CoBMR**). This is a command line only tool which is licensed for use for an initial 30 day trial period. A full license is required to use the program beyond the trial period.

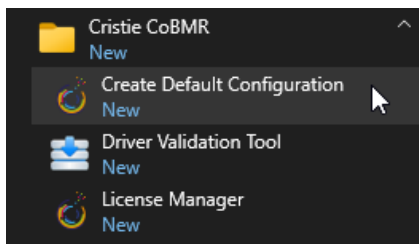
*Note: The **CoBMRCfg.exe** program should be run as part of a Cohesity DataProtect pre-backup script.*

As part of this process, details about the hard disks, operating system, storage controller (s), network adapter(s) and network settings will be queried and stored. You can override some of these details if you wish. The result of the configuration creation (success or failure) is recorded in the Windows Application Event Log.

The next sections discuss this process in more detail.

4.1 Creating the Configuration Information

The easiest way to create the configuration manually is to select the **Create Default Configuration** shortcut provided on the Start menu for CoBMR. Note however that an initial configuration is created during the CoBMR installation process.



This will create a new configuration using the default settings.

```
=====
                CoBMR Configuration Utility Version 9.6 for x64
                Copyright (C) 2009-2024 Cristie Software Limited
=====

Copying the EFI files ...
Successfully copied the EFI files
Created a snapshot of C:\ --> A:\
Searching for files missed under C:\Users ...
Searching for files missed under C:\Windows\ServiceProfiles ...
Saving hard-link information ...
Successfully saved hard-link information
Configuration was stored successfully
```

If you need to select non-default settings, then you will need to create the configuration manually. Run a command window and navigate to the folder where CoBMR is installed.

The CoBMR configuration program is called **CoBMRCfg.exe**. Enter the command **CoBMRCfg.exe /?**, this will display the command line options available.



```

C:\Program Files\Cristie\CoBMR>CoBMRCfg.exe /?

=====
                CoBMR Configuration Utility Version 9.6 for x64
                Copyright (C) 2009-2024 Cristie Software Limited
=====

Usage: CoBMRCFG.EXE [options]

Options are:

/help or /? - Show usage
/format <Drives to format|all> - Format additional volumes during recovery
                             Specify drives separated by comma as in /format D,E,F

                             For a volume that does not have a drive letter but mounted
                             under a folder, enter the mounted folder as in
                             /format D,D:\MountedVolume
                             /format all will format all partitions on all disks

/skiphardlinks - Skip hard-link processing for CoBMR block-based backups
                  and RBMR volume group backups only

The configuration will always be stored in %%SystemDrive%%\CoBMRCFG

```

The command line options are very simple:

/help or **/?**

shows **CoBMRCfg** usage. This displays the command option summary.

/format <Drives to format | all>

The **/format** option allows disk volumes other than the Windows drive to be formatted during the recovery. By default, only the Windows volume will be formatted. There is an exception to this if Windows is not contained within the first partition of the disk. In that case, both the Boot partition and the Windows partition will be configured for formatting. However, regardless of this setting, the WinPE5, WinPE10 or WinPE11 based recovery environment will allow any or all partitions to be formatted.

So, for example, if volumes D:, E: and F: are to be additionally formatted during recovery, enter:

```
CoBMRCfg.exe /format D,E,F (separate the drive letters using a comma)
```

Enter the following to back up all partitions on all drives on the system:

```
CoBMRCfg.exe /format all
```

Volumes mounted on local folders not having a drive letter can be specified like this:

```
CoBMRCfg.exe /format D:\MountedVolume
```

where D:\MountedVolume is the folder mount point. An example using both normal partitions and a mounted volume is:

```
CoBMRCfg.exe /format D,D:\MountedVolume
```

CoBMRCfg stores the configuration in %%SystemDrive%%\CoBMRCFG folder (%%SystemDrive% is



the drive associated with the Windows folder, usually C:\). This location cannot be changed.

Note: it is important to remember that the CoBMR configuration must be created before the Cohesity DataProtect Client backup is made. Cristie suggests using the Cohesity DataProtect pre-script feature which is found in the Advanced Settings section for the protection job.

4.2 Backup of Boot and Hard-Link Files

On all Windows OS's, files additional to the standard Cohesity DataProtect backup dataset must be copied and saved. These include boot files and file hard-link objects which are not normally backed up by the Cohesity DataProtect Client on these OS's.

Some of the additional files backed up are also locked at the time of backup and must be backed up using the Windows Open File Manager **VSS**. So when CoBMRCfg runs, it invokes VSS to take a snapshot copy of these extra files:

```
=====
CoBMR Configuration Utility Version 9.6 for x64
Copyright (C) 2009-2024 Cristie Software Limited
=====

Copying the EFI files ...
Successfully copied the EFI files
Created a snapshot of C:\ --> A:\
Searching for files missed under C:\Users ...
Searching for files missed under C:\Windows\ServiceProfiles ...
Saving hard-link information ...
Successfully saved hard-link information
Configuration was stored successfully
```

4.3 Creating a CoBMRCfg Pre-Schedule

The CoBMR configuration utility (CoBMRCfg) can be triggered pre Cohesity DataProtect backup to run automatically. Generating a fresh configuration makes sure the file is up to date and takes account of any changes to disks/OS patches/hardware etc.

There are two stages required for setup: A script on the source and enabling the setting on the Cohesity DataProtect Console.

First create the script, basic example is shown below:

```
@cd "%ProgramFiles%\Cristie\CoBMR" && cobmrcfg.exe
```

Save as 'cristieCoBMR.bat' and place in 'c:\program files\cohesity\user_scripts'

On the Cohesity DataProtect Console enable and modify the protection job Additional Settings, pre & post scripts, Pre Script to include the script name:



Pre & Post Scripts

Pre and Post scripts will run before and after each object is backed up.

☒ Pre Script

protectionjobs\jobSummary\jobSummary.scriptPath *

cristieCoBMR.bat

Scripts should be located in the 'user_scripts' folder in the agent installation directory on the Server

Script Params

Timeout (mins)

30

☒ Continue Backup if script fails

☐ Post Script

Increase the timeout if required. Due to the nature of Windows systems this can take some time, especially if the system has lots of disks. When deploying through the Cristie Virtual Appliance (VA), these scripts are placed in the correct folders automatically on install. Just set the Coheisty Protection job pre-script option to use.




5 Using a Cohesity DataProtect Backup for Disaster Recovery

CoBMR allows a previously created Cohesity DataProtect backup to be used as a DR backup.

CoBMR supports Cohesity DataProtect backups created in both file-based or block-based form.

As long as the CoBMR configuration has been created (see previous section) and a Cohesity DataProtect backup is performed afterwards, then it will be possible to recover the system using the DR environment.

When running a file-based backup to ensure all files (including system and locked files) get backed up, please enable the setting **Crash Consistent Backups** on the server for the source being backed up. This will be found in the **Protection Group Additional settings** section for the group.



Additional Settings ^	
End Date	Never
QoS Policy	Backup HDD
Abort at Pause Window Start	No
Pre & Post Scripts	None
Crash Consistent Backups	Enabled
Source Side Deduplication	No
Indexing	Enabled - 1 paths included, 18 excluded.
Global Exclude Paths	0 paths excluded.
Alerts	Alert On: Failure
Priority	Medium
SLA	Full Minutes: 240 Incremental Minutes: 120
Pause Future Runs	No
Description	None

Save Cancel

Note: this document does not describe how to create Cohesity DataProtect backups. Please refer to your Cohesity DataProtect Administrator's Guide for details.

Note: When using a CoBMR backup to recover a Windows Domain Controller the recovered system will boot twice.

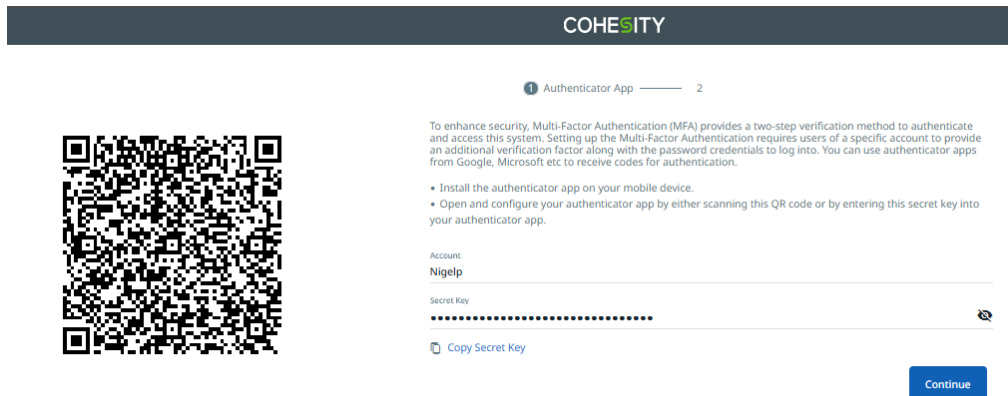


6 Multi-factor Authentication

If your Cohesity DataProtect server is configured to use Multi-factor Authentication (MFA) you will be prompted during an interactive recovery sequence for an MFA code.

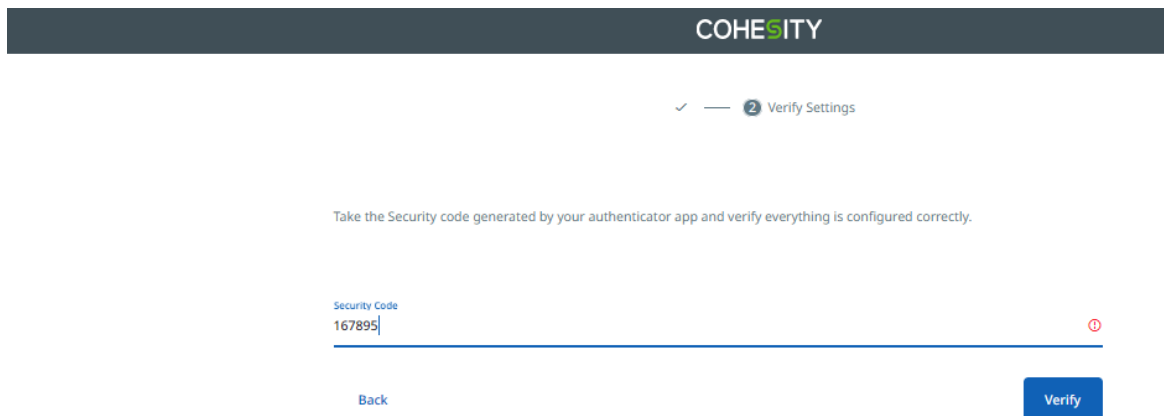
To generate such a code you will need an authentication app installed on a mobile device (e.g. phone or tablet) and an entry added for your server. For example Microsoft and Google provide such Authenticator apps.

When configuring an entry in the app for your server you will need to use the server generated QR code to do this. For example:

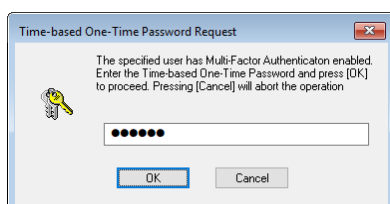


Scan the code with your mobile device to setup an entry for the server in the authenticator app.

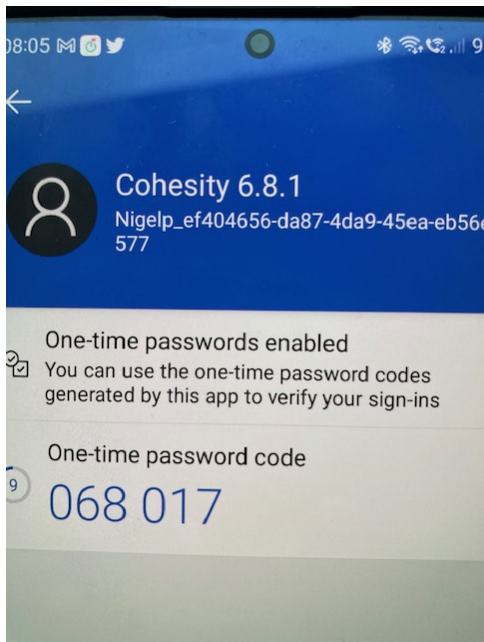
Then to login to the server you will see a prompt like this:



During a recovery operation you will be prompted for an MFA code. Use the entry in your authenticator app to generate an MFA code. For example:



The MFA app will show something similar to this when the code is generated:



Note: The MFA codes are only valid for a short period of time (e.g. 30 seconds). If you take too long to enter the code it will be incorrect. Re-generate the code and re-enter if this occurs.



7 Restoring your System

This section discusses the steps required to run a recover sequence using the CoBMR Recovery Environment. This is booted from the media created by CRISP in conjunction with the CRISP WinPE5, WinPE10 and WinPE11 Filesets for CoBMR 9.6 (see [Create the bootable cloning environment](#) for further details).

The WinPE5, WinPE10 or WinPE11 based recovery environment is booted on the **target** system. This could be the original or a dissimilar system.

A typical CoBMR recovery sequence consists of the following steps.

1. Install and run the **Cristie Recovery ISO Producer (CRISP)** tool on a suitable system to create the CoBMR WinPE5, WinPE10 or WinPE11 based recovery environment either as a CD/DVD ISO image or direct to a USB flash drive. This only needs to be done once per Cohesity DataProtect client used.
2. Boot the CoBMR WinPE5, WinPE10 or WinPE11 recovery environment on the **target** system.
3. Run a restore sequence from the recovery environment on the **target** system using the Cohesity DataProtect backup.
4. When the restore operation is complete and, before booting the system, you may change the hostname and IP address as required. If the target system uses different hardware from the source system inject additional drivers into the system using the hardware wizard tool. This tool will detect any new devices in the target system and prompt for the drivers.
5. Boot the recovered system.

7.1 File- or Block-based Recoveries

This section discusses the steps required to run a recover sequence using the CoBMR Recovery Environment for file-based backups. This is booted from the media created by CRISP in conjunction with the CRISP WinPE5, WinPE10 and WinPE11 Filesets for CoBMR 9.6 (see [Create the bootable cloning environment](#) for further details).

The WinPE5, WinPE10 or WinPE11 based recovery environment is booted on the **target** system. This could be the original or a dissimilar system.

A typical CoBMR recovery sequence consists of the following steps.

1. Install and run the **Cristie Recovery ISO Producer (CRISP)** tool on a suitable system to create the CoBMR WinPE5, WinPE10 or WinPE11 based recovery environment either as a CD/DVD ISO image or direct to a USB flash drive. This only needs to be done once per Cohesity DataProtect client used.
2. Boot the CoBMR WinPE5, WinPE10 or WinPE11 recovery environment on the **target** system.
3. Run a restore sequence from the recovery environment on the **target** system using the Cohesity DataProtect backup.
4. When the restore operation is complete and, before booting the system, you may change the hostname and IP address as required. If the target system uses different hardware from the source system inject additional drivers into the system using the hardware wizard tool. This tool will detect any new devices in the target system and prompt for the drivers.



5. Boot the recovered system.

7.1.1 Booting the WinPE5, WinPE10 or WinPE11 DR Environment

Insert the bootable CoBMR WinPE5 ,WinPE10 DR CD/DVD or USB flash drive and reboot the machine. By default you will be prompted to **Press any key to boot from the CD or DVD** unless you have disabled this feature when creating the ISO/USB flash drive in CRISP.

Press any key to boot from CD or DVD. _

This prompt is only made for a few seconds before the system will attempt to boot the underlying OS, so you will need to react quickly.

Note: It is possible to suppress this prompt completely during the ISO/USB flash drive creation stage. If the prompt is disabled then the DR ISO/USB flash drive image will always boot by default. Please refer to CRISP documentation which describes how to do this.

To support devices (for example a new mass storage controller) not supported in the current DR environment, WinPE5, WinPE10 or WinPE11 allows drivers for any device to be injected at any time post boot. Refer to the section titled [Load a Driver](#) for information on how to do this. Ensure you add the correct driver version; 64-bit for WinPE5/WinPE10/WinPE11.

7.1.1.1 WinPE5, WinPE10 or WinPE11 Based CoBMR Recovery Environment

When the **WinPE5, WinPE10 or WinPE11 CoBMR Environment** is booted, a Windows installation-like boot procedure is started.

During the boot process, WinPE5, WinPE10 or WinPE11 drivers for your **Plug and Play** devices will be loaded - in particular the **Mass Storage** devices and **Network Adapters**. When the WinPE5, WinPE10 or WinPE11 system has fully booted, it is possible to remove the CD/DVD or USB flash drive if you wish.

Note: the DR Console will automatically reboot 72 hours after starting. This is an operating limitation of the Microsoft Windows WinPE5, WinPE10 or WinPE11 environment.



PE10

PE10



COHESITY BMR

Please wait while your PnP devices are loaded...

PE10

PE10

When this sequence completes, the **CoBMR Recovery Environment** will be shown.

7.1.2 Block Based Recovery Settings

When recovering a Block-Based backup with CoBMR, changes are required to be set on the Cohesity DataProtect Cluster to allow full access to the smb shares for recovery. This is due to adjustments in the way Cohesity manages access to smb shares.

Please set the view and gflag options below using the Cohesity **iris_cli**:

1. Start the Cohesity DataProtect CLI remotely or locally as described in Cohesity knowledgebase article: How to access the Cohesity DataProtect CLI (Iris CLI)#: <https://support.cohesity.com/s/article/How-to-access-the-Cohesity-DataPlatform-CLI-Iris-CLI>
2. Enable the option `bridge_smb_portal_auth_local_authentication_enabled` (one line): as per: <https://support.cohesity.com/s/article/How-to-enable-local-user-authentication-to-a-Cohesity-SMB-View>

```
cluster update-gflag gflag-  
name=bridge_smb_portal_auth_local_authentication_enabled  
service-name=bridge effective-now=true reason=KB-3922 gflag-value=true
```

3. Set the view gflag and user access:

Below is an example, please set your own username and password. To do this run `iris_cli` and log in with a suitable Admin User/password.



So for a new user “**blockuser**” with a password of “**P@ssw0rd**”:

```
user add user-name=blockuser password=P@ssw0rd primary-group-  
name=Users  
  
user edit user-name=blockuser password=P@ssw0rd allow-smb-access-  
token=true  
  
user edit user-name=blockuser roles=Admin
```

4. Allow Access to smb shares for the user (on one line):

```
cluster update-gflag service-name=magneto gflag-  
name=magneto_physical_file_restore_try_local_user_for_smb gflag-  
value=true effective-now=true reason=Enable_local_authentication
```

If some of the above commands have already been set e.g. local admin user has already been created or bridge is set, the only requirement is to configure anything new. However, running a command a second time will not break anything.

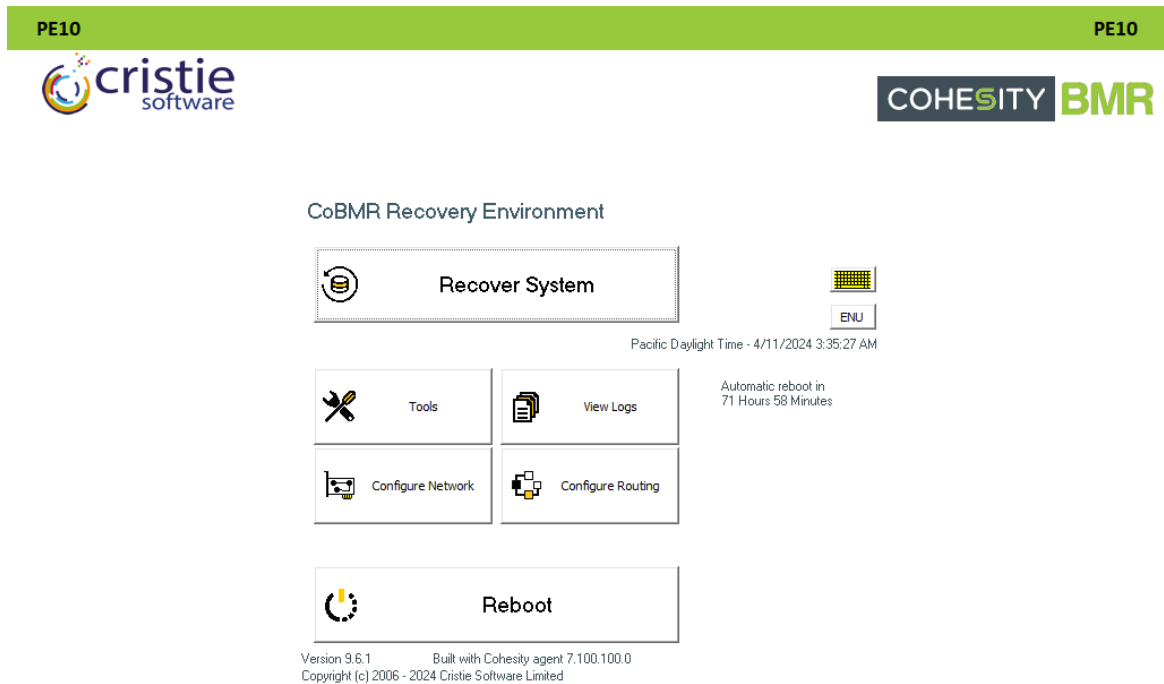
7.2 Begin the Restore Process

Click the **Recover System** option to begin the recovery sequence. This is common for both file- and block-based recoveries.



7.2.1 CoBMR Recovery Environment Main Menu

When you boot the **WinPE5, WinPE10 or WinPE11** DR environment (the WinPE5, WinPE10 and WinPE11 versions are very similar), you will see the **CoBMR Recovery Environment** Main Menu as below:



Prior to beginning the restore operation you may configure the network and/or the network routing as necessary. Click the

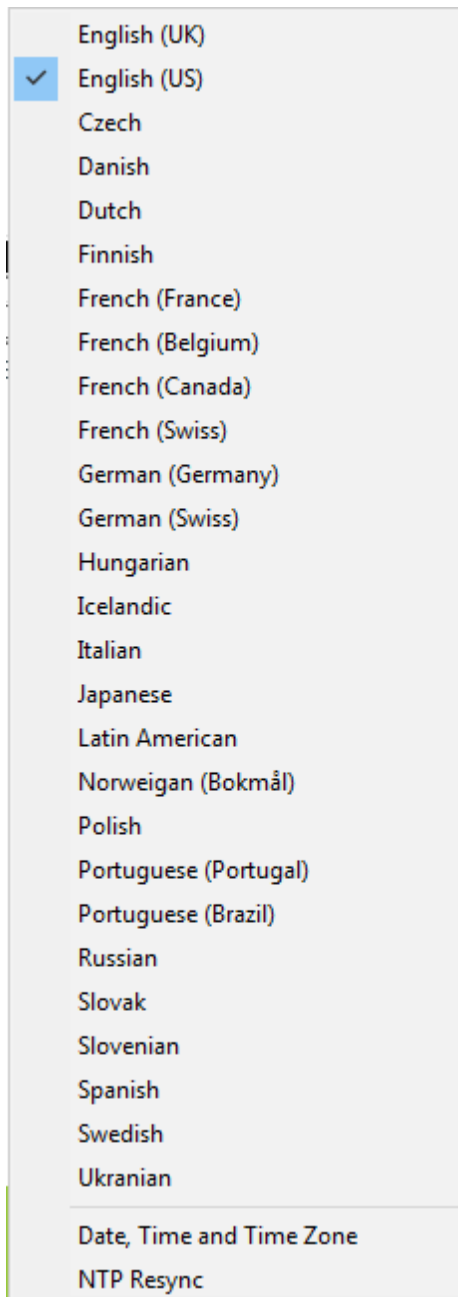


icons to do this.

A reboot countdown clock is shown **Automatic reboot in 68 Hours 14 Minutes**. This indicates how much time is available before the WinPE5 and WinPE10/WinPE11 recovery environment automatically reboots. Note this is a Microsoft constraint for the WinPE environment.

You may configure the format of the displayed date/time and the keyboard layout, by pressing the locale **ENU** icon. Note this icon will be shown according to the locale of the host system used to create the ISO/USB flash drive using the CRISP utility so it may not match the version shown here. So if, for example, the ISO/USB flash drive was built on a machine configured with a UK locale it will be displayed as **ENG**.

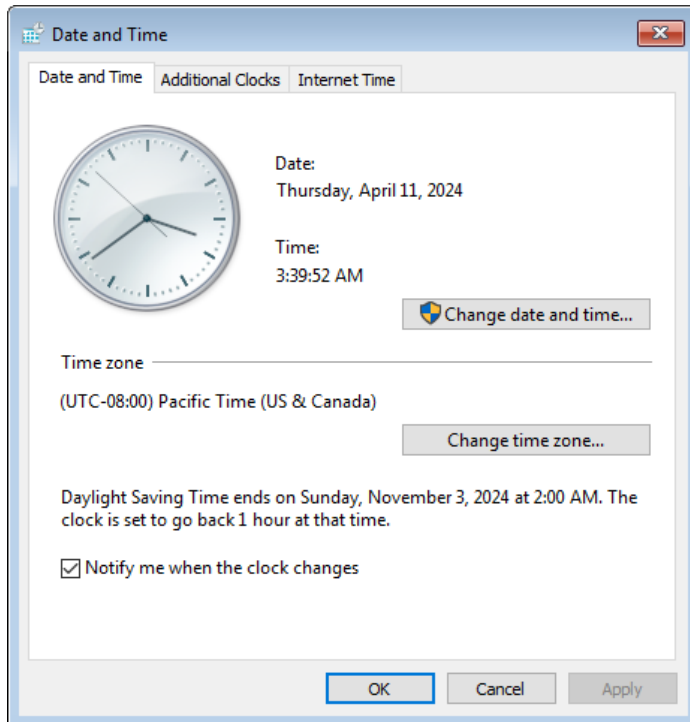





By default the standard display uses a keyboard layout to match the default locale as discussed above. However, this may be changed to one of the listed alternatives. Note that this does not change the display language which is always English.

Select **Date, Time** and **Time Zone** to configure the time zone for the recovery.





Note: the Additional Clocks and Internet Time tabs are operational. In fact it is possible to synchronise the system time with an NTP time server if required.

Finally if your recovery environment does not provide keyboard support (perhaps a driver issue) use the on-screen keyboard which can be displayed by clicking . This then shows a clickable keyboard at the bottom of the screen. The keyboard layout displayed will correspond to the currently selected locale.





CoBMR Recovery Environment



Use this for any data entry.

Note the DR environment requires a working mouse as a minimum.

7.2.2 Logfile Save Path

Before starting the restore process you should configure a location to save the recovery logs. This can be a network location or physical media (such as a USB flash drive). The logs will be automatically saved to the configured location at the end of the restore process without further intervention.


CoBMR - Specify Path To Save Logfiles To At End Of Recovery

☐ Check this box if you do not wish to supply a path to save the log files to

Log Files Path

Enter the path to save the log files to either as a share in UNC format or as a drive letter and path.


Browse...

 Configure Network

< Back Next > Cancel



Configure Network


For example, use the  option to first map a network share location and then **Browse** to select a folder on the share.

Log Files Path

Enter the path to save the log files to either as a share in UNC format or as a drive letter and path.

V:\nigelp\Logs

Browse...

 Configure Network

If you do NOT want to automatically save the the logfiles please check the tick-box to skip this step.



☒ Check this box if you do not wish to supply a path to save the log files to

Click [Next >](#) to continue to the next step.

You will still have the opportunity at the end of the restore process to save the logfiles if you wish.

7.2.3 Specify Cohesity DataProtect Details and Recovery Date/Time

The next step of the restore process identifies the location of the **Cohesity DataProtect Server and Source** used to back up the Client. The Cohesity DataProtect server IP address should be expressed in IPv4 format.

CoBMR - Cohesity Settings

Please enter the Cohesity Appliance and Registered Source details below and select [Next >] to continue.

Cohesity Appliance Details

Cohesity Appliance :

Tenant Id: (optional)

Authentication

Domain:

Username:

Password:

Backup-Type: ☐ Block-Based ☒ File-Based

Registered Source Details

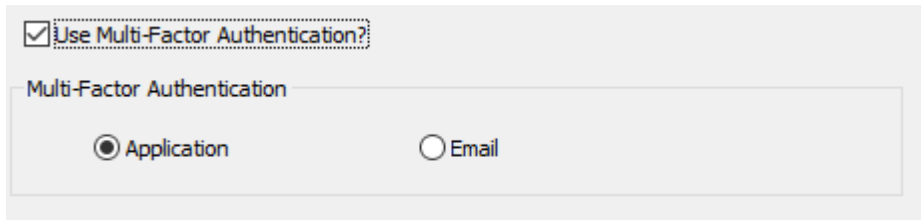
Registered Source

☐ Use Multi-Factor Authentication?

< Back **Next >** Cancel

For **Registered Source** enter the IPv4 address or the name of the registered source, which must match the address or name used to originally register the source on the server. Enter a **Tenant Id** if required.

Click **Use Multi-Factor Authentication** if your Cohesity DataProtect server is configured to use it.



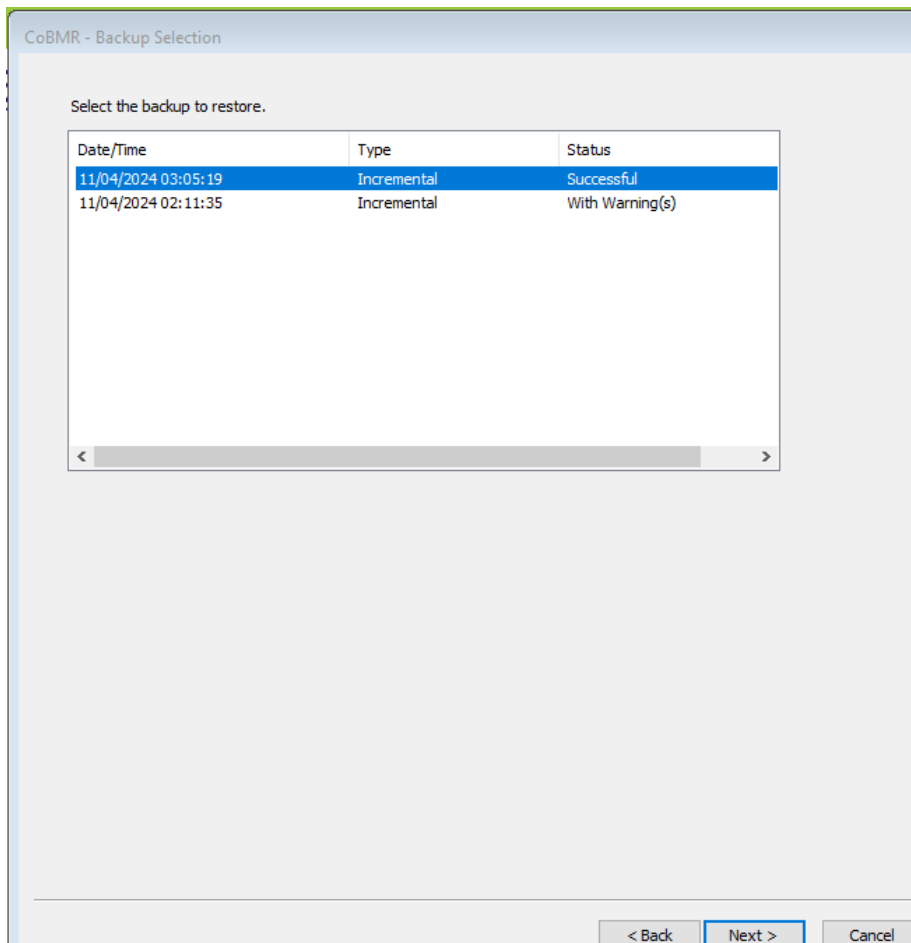
☒ Use Multi-Factor Authentication?

Multi-Factor Authentication

☒ Application ☐ Email

Then choose **Application** or **Email** as appropriate.

Click **Next >** to proceed. If more than 1 recovery point is detected on the server for the source they will then be displayed like this.



CoBMR - Backup Selection

Select the backup to restore.

Date/Time	Type	Status
11/04/2024 03:05:19	Incremental	Successful
11/04/2024 02:11:35	Incremental	With Warning(s)

< Back Next > Cancel

Select the required restore point from the list. Latest is shown at the top. Select **Next>** to continue.

At this point the Source will be accessed on the specified server and the machine configuration extracted.

7.2.4 Storage Pools

If your original source host contained any Windows Storage Pools then this step will be run to allow the pool/disk setup to be configured. If no Storage Pools were configured in your selected backup this step will be skipped.



Note: Storage Pool recovery only works with the WinPE5 version of the CoBMR DR environment. Do not use the WinPE10 version for Storage Pool recovery.

The pool/disk configuration dialogue looks like this:

CBMR - Storage Pools

Stored Storage Pools (2)

Name	Capacity	Free Space
Pool-A	8.97 GB	6.72 GB
Pool-B	18.97 GB	14.97 GB

To configure, select a Virtual Disk from the table below and right-click to assign target Physical Disks to it.

Stored Virtual Disks (1)

Name	Layout	Provisioning	Capacity	Allocated	Volume
Pool-A-Disk0	Simple	Thin	5.00 GB	768.00 MB	E:

Stored Physical Disks (1) Proposed Physical Disks (0)

Name	Capacity	Bus	Usage	Chassis	Media Type
VMware Virtual SATA Hard...	5.00 GB	SATA	Automatic	sata0	SSD

< Back **Next >** Cancel

The pool configuration requires you to map the original pool/virtual disk configuration to the physical disk layout detected on the target. This may have more or fewer disks than the original so this re-mapping needs to be done manually.

There are 3 sections in the dialogue:

- **a list of the original configured pools with their corresponding capacity and the free space at the time of the backup.**
- **a list of the original virtual disks defined for a selected pool together with the corresponding virtual disk layout, provisioning, capacity, size in use and volume letter.**
- **a list of the original physical disks and the proposed physical disks discovered on the target system for the selected virtual disk.**

To assign physical disks to a virtual disk right-click the virtual disk to display the Virtual Disk Layout dialogue.

This is a recovery of a Windows 2019 server with 2 Storage Pools, named Pool-A and Pool-B. Pool-A is currently selected which is showing the Virtual Disk that was in the Storage

Pool on the source system. The screenshot below shows the Physical Disks that the Virtual Disk was built from on the source system. There were 2 of them and they were all SATA (shown as Bus Type SATA).

Note that the **Proposed Physical Disks** has a count of zero, i.e. there are no target Physical Disks selected yet to recreate this Virtual Disk from, where **Stored** = **Source system** and **Proposed** = **Target system**.

Right-click on the virtual disk, to display the disk selection dialogue.

CBMR - Virtual Disk Layout

Storage Pool Virtual Disk

Name: Pool-A-Disk0

Layout: Simple

Provisioning: Thin

Capacity: 5.00 GB

Allocated: 768.00 MB

Volume: E:

Stored Physical Disks (1)

Name	Capacity	Bus	Usage	Chassis	Media Type
VMware Virtual SATA Hard...	5.00 GB	SATA	Automatic	sata0	SSD

Proposed Physical Disks (2)

Name	Capacity	Bus	Usage	Chassis	Media Type
<input type="checkbox"/> PhysicalDisk1	10.00 GB	SAS	Automatic		SSD
<input type="checkbox"/> PhysicalDisk2	10.00 GB	SAS	Automatic		SSD
<input checked="" type="checkbox"/> PhysicalDisk3	5.00 GB	SATA	Automatic		SSD
<input checked="" type="checkbox"/> PhysicalDisk4	5.00 GB	SATA	Automatic		SSD

OK Cancel

In the example above the 2 target physical disks that makeup the original virtual disk are selected. Note the proposed disk count is now non-zero.

Repeat this process for all the remaining virtual disks in each pool. This results in a configuration similar to this:



CBMR - Storage Pools

Stored Storage Pools (2)

Name	Capacity	Free Space
Pool-A	8.97 GB	6.72 GB
Pool-B	18.97 GB	14.97 GB

To configure, select a Virtual Disk from the table below and right-click to assign target Physical Disks to it.

Stored Virtual Disks (2)

Name	Layout	Provisioning	Capacity	Allocated	Volume
Pool-B-Disk0	Simple	Thin	5.00 GB	768.00 MB	F:
Pool-B-Disk1	Simple	Thin	5.00 GB	768.00 MB	G:

Stored Physical Disks (1)

Name	Capacity	Bus	Usage	Chassis	Media Type
VMware, VMware Virtual S	10.00 GB	SAS	Automatic	SCSI0	SSD

Proposed Physical Disks (2)

Name	Capacity	Bus	Usage	Chassis	Media Type
------	----------	-----	-------	---------	------------

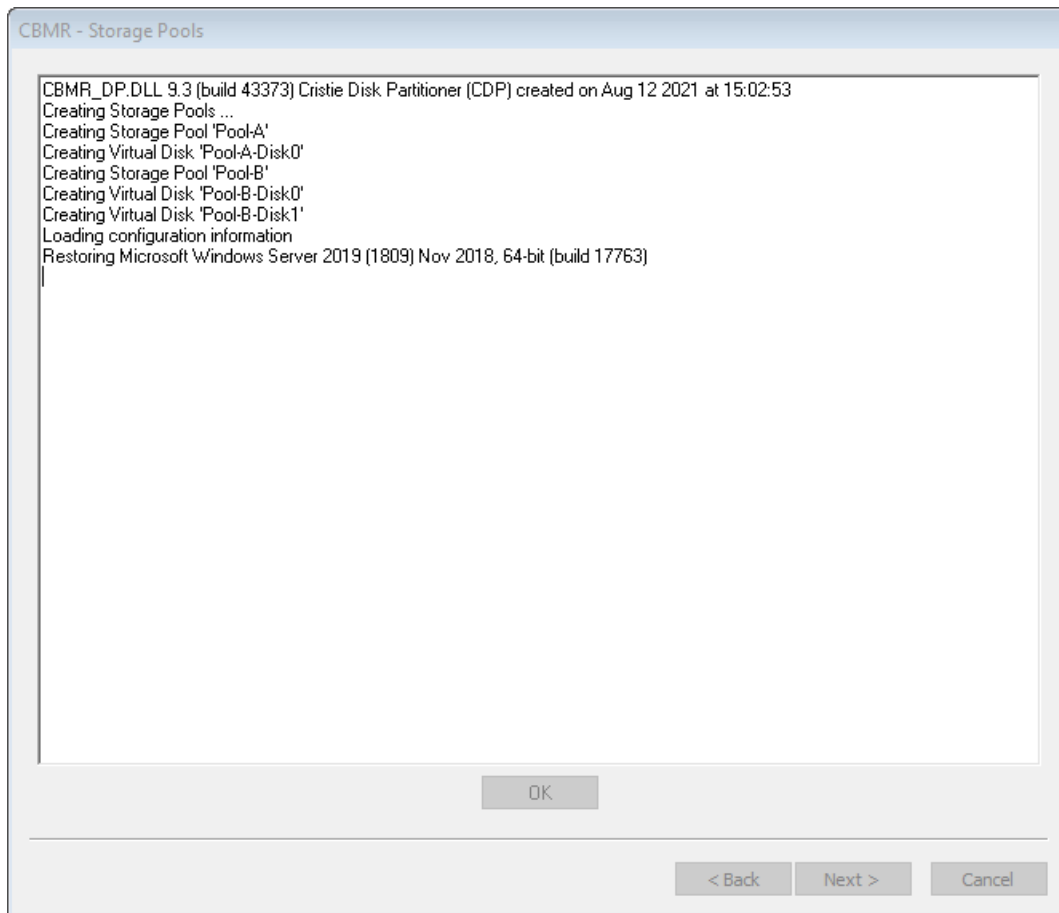
< Back Next > Cancel

Note: There are some constraints on this configuration. For example, it is not recommended to have fewer or more physical disks mapped to your target virtual disk compared with the original source configuration.

Now click **Next >** to continue or **< Back** to return to the previous dialogue.

At this point the Storage Pools and virtual disks will be created.





Note: if no target disks are assigned during the Storage Pool step then recovery will still proceed but no Storage Pools will be restored.

Recovery now runs as normal with no further Storage Pool configuration required.

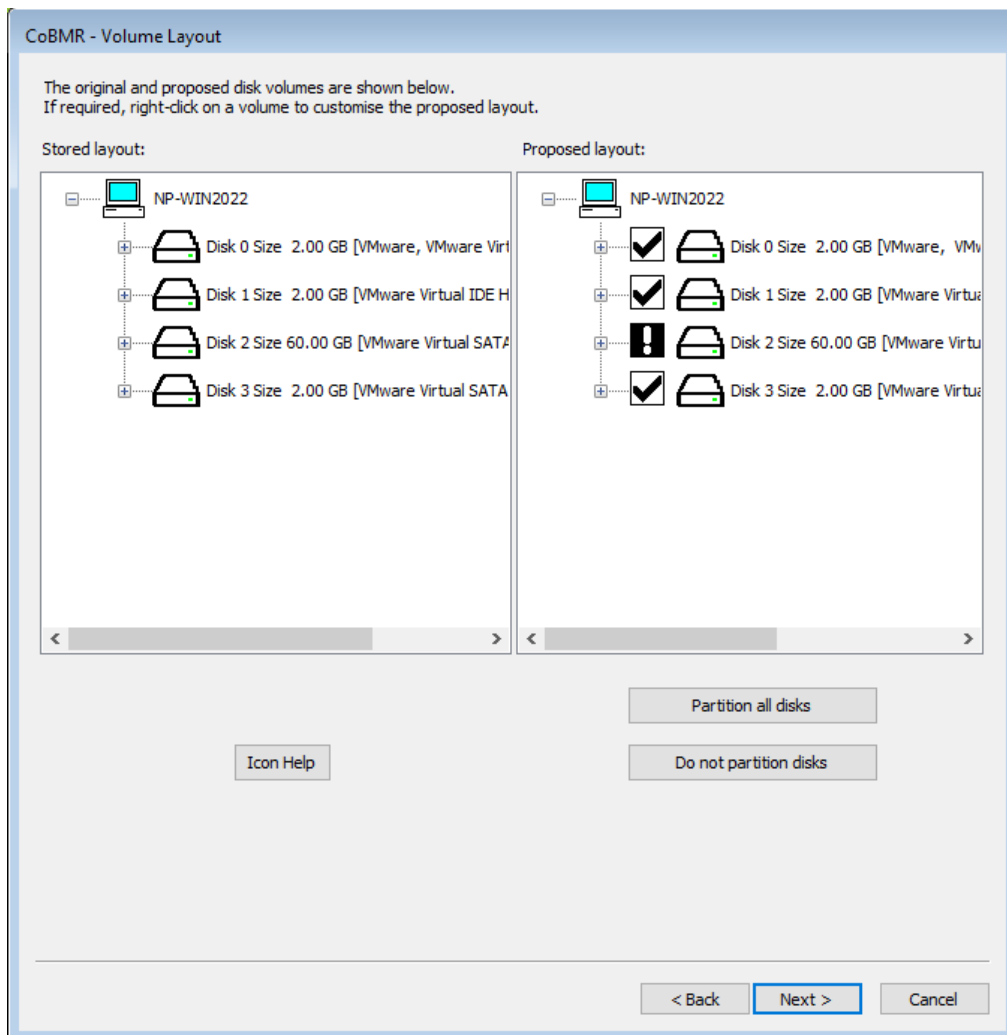
There are certain constraints with this release of Storage Pool support.

- Storage Pools and virtual disks are recognized by CoBMR WinPE5, so if you boot a target system that has them, then WinPE5 will see them and mask out the "real" disks resulting in only the virtual disks being shown.
- The use of NVMe type disks when using VMWare WorkStation is not recommended when using Storage Pools.
- Physical disks used in Storage Pools should have minimum size of at least 8 GB.
- Only the CoBMR WinPE5 DR environment is supported for recoveries of Storage Pools.
- During the Volume Layout phase you can right-click on target disks and swap them etc, but you can't swap a Storage Pool virtual disk with a real disk or vice-versa.

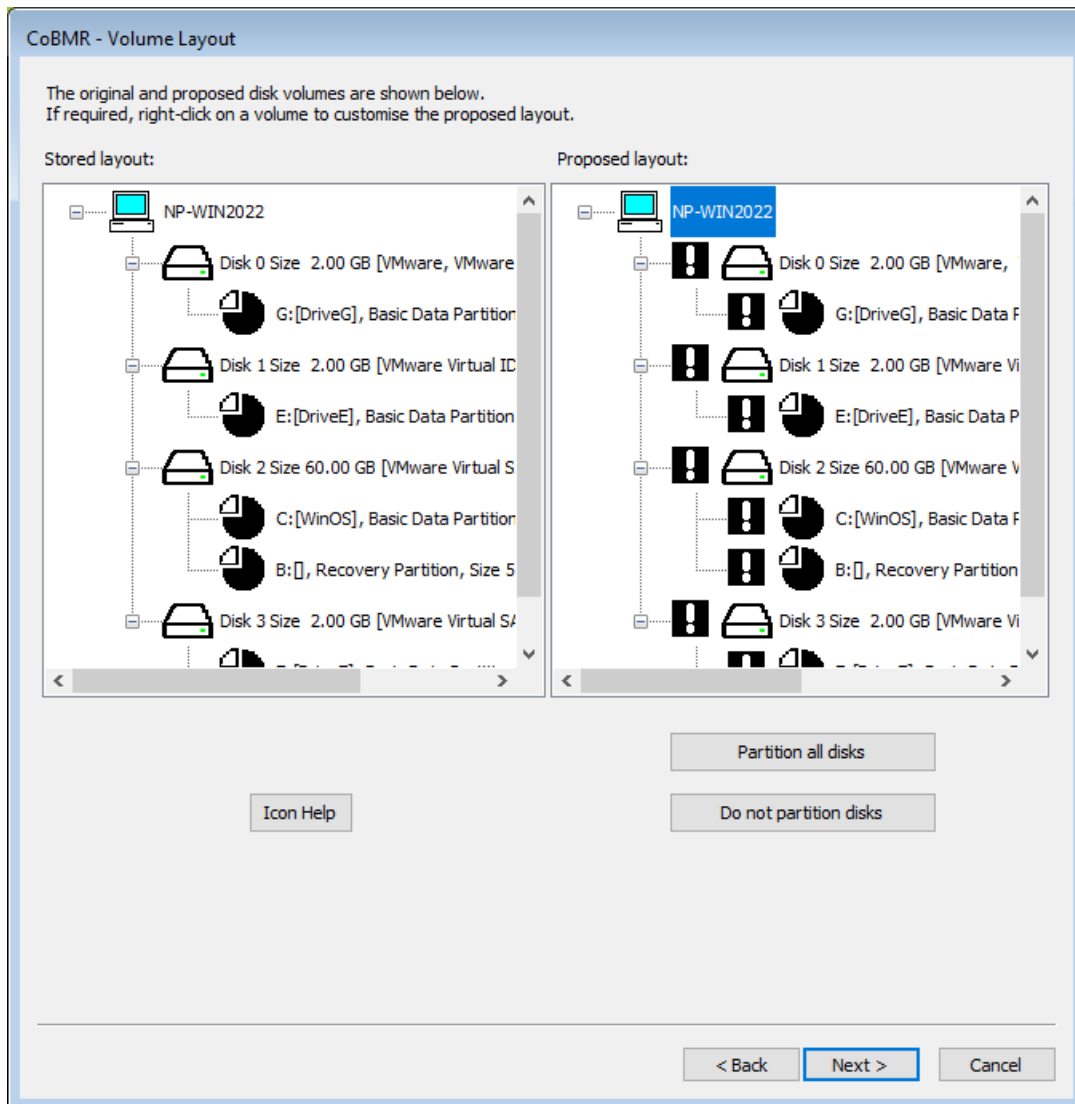


7.2.5 Confirm Volume Layout

The next step in the **Automatic recovery** shows a list of the disks and partitions to be recovered.




For a system with Storage Pools the Volume Layout will resemble this example:




The left-hand panel of the dialogue shows the original disk layout and partitions. The right-hand panel shows how the recovered disks will be partitioned after the recovery.

If you wish to quickly enable the partitioning of all target disks click .


If you wish to quickly disable the partitioning of all target disks click .

A white tick box  next to a disk signifies that the disk and its underlying partitions will be left intact. Placed next to a partition/volume means that the corresponding partition/volume **WILL NOT** be partitioned.

A white exclamation mark  placed next to a disk means it **WILL** be partitioned during recovery. Placed next to a partition or volume means that the corresponding partition/volume **WILL** be partitioned.

A black/white exclamation mark  placed next to a disk means at least one partition/volume **WILL** be partitioned.



A white box  indicates that the disk will be completely ignored during the recovery.

There are 3 disk types available:



indicates a standard disk

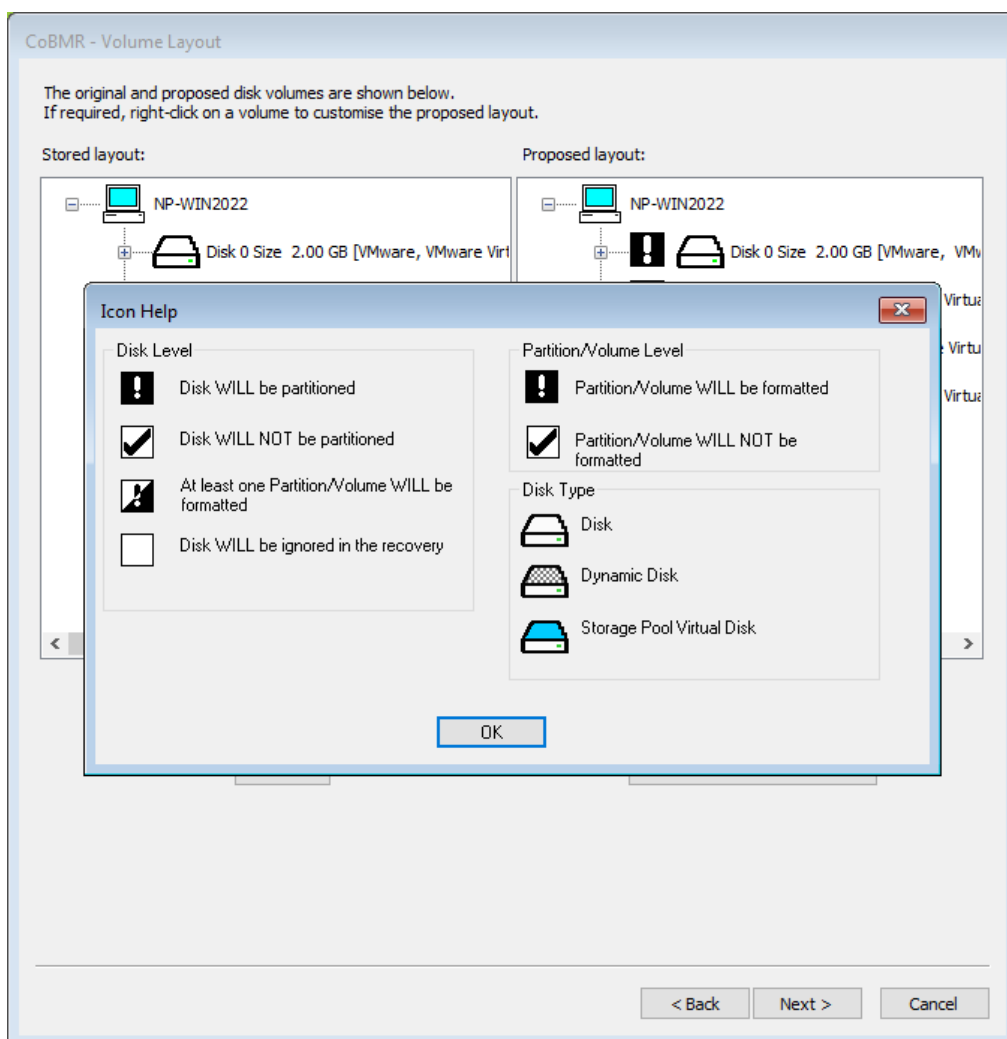


indicates a dynamic disk



indicates a Storage Pool virtual disk

Click on the [Icon Help](#) button to display a summary of this:

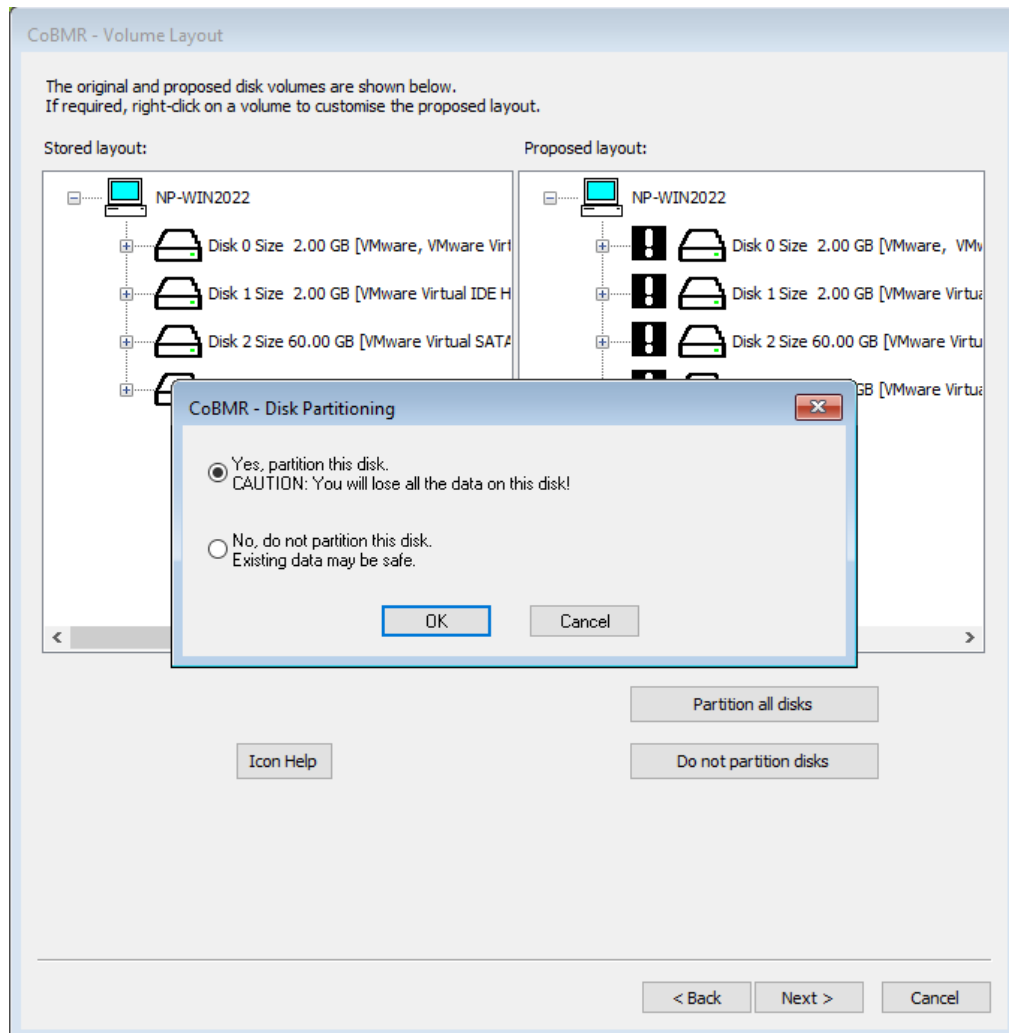


When the recovery is to the original system, the contents of both panels will look similar if the number of disks is the same. Possibly the disk sizes will be different.

When performing a recovery to a dissimilar system, the disk mapping can be much more complex. Some of the criteria used to judge the disk mapping are:

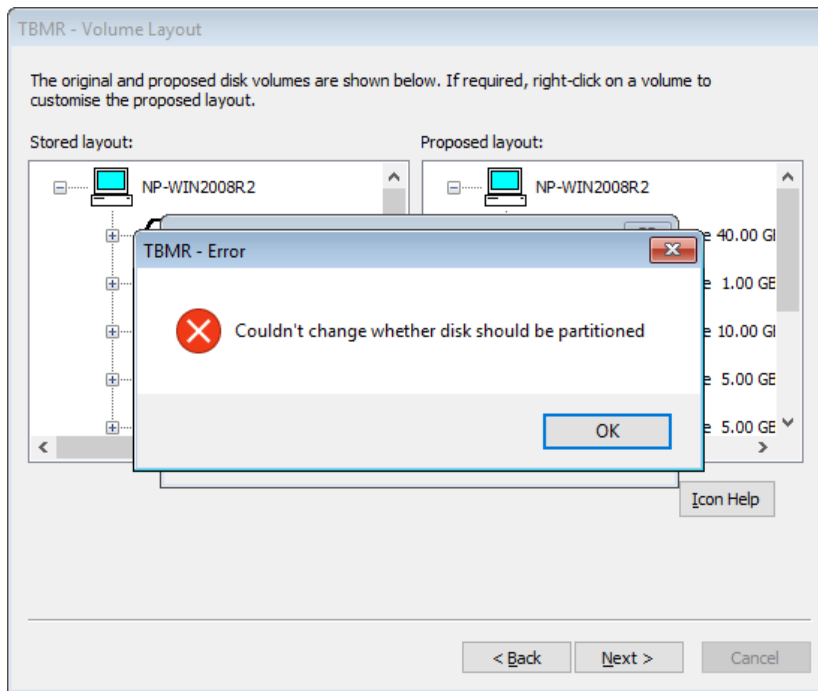
- *disk geometry*
- *disk capacity*
- *if currently formatted, the disk signature*

You may right-click on any disk shown in the right-hand panel to select whether the disk will be partitioned or not.



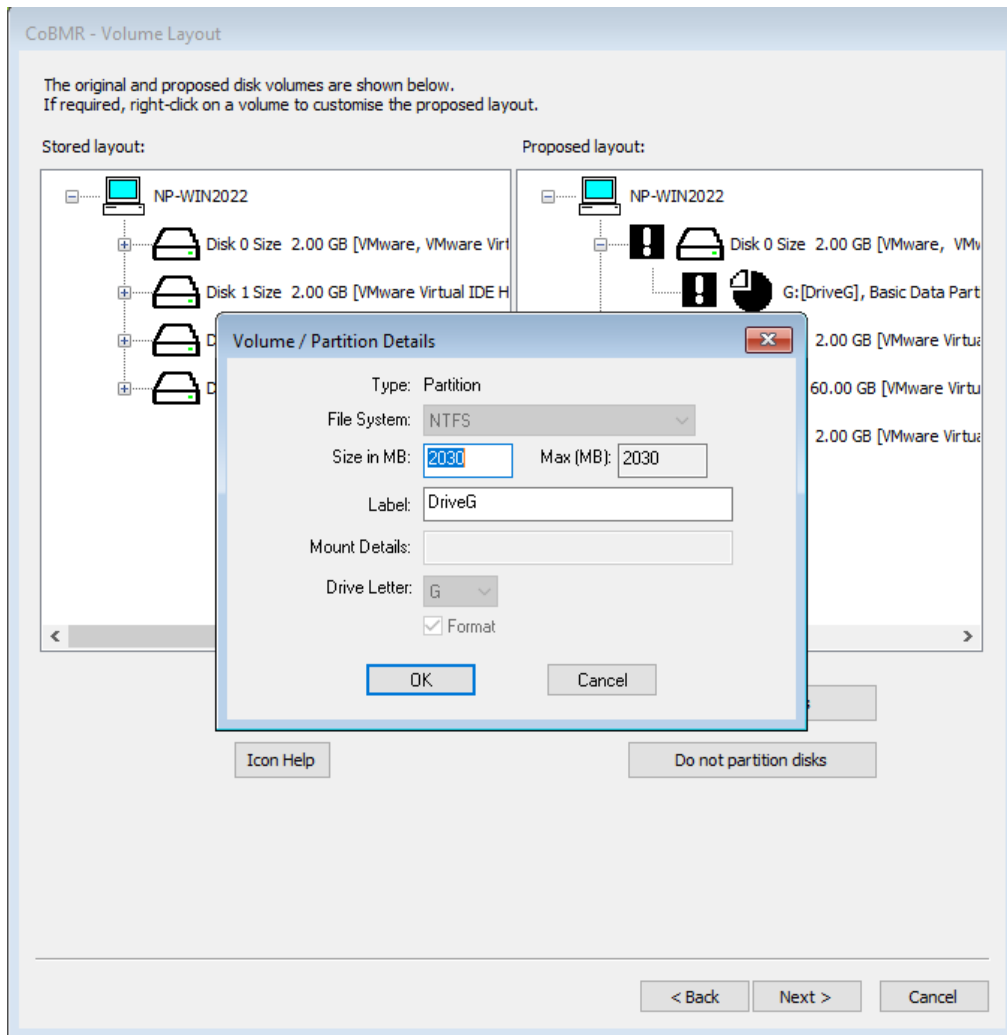
Any attempt to incorrectly turn off formatting will result in this error:






You may also right-click on a partition to allow you to selectively modify the partition parameters.

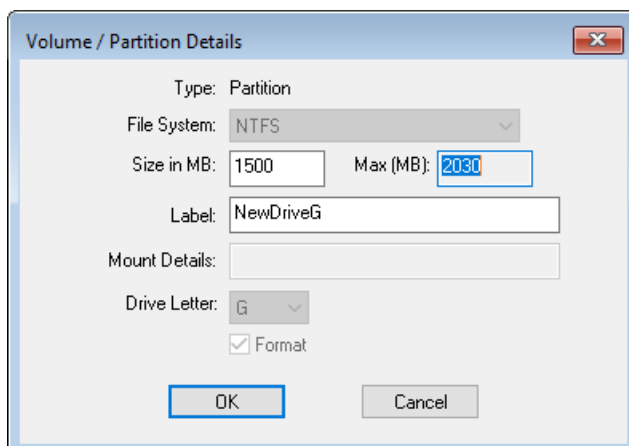




You may **Modify** the following partition parameters:

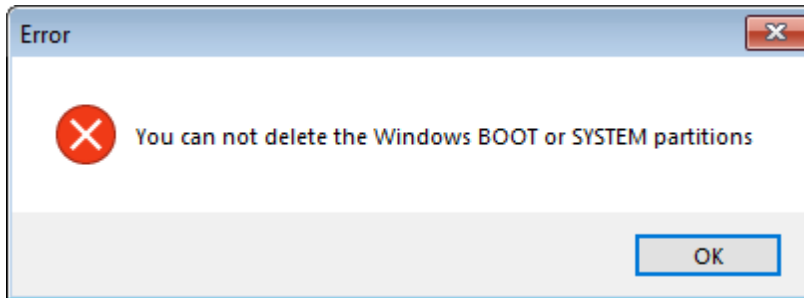
- size in MB (only if disk is shown with a )
- label
- format (yes/no)

The screenshot below shows an example:



If you attempt to either not format or delete a Windows system partition, an error such as this will be displayed:

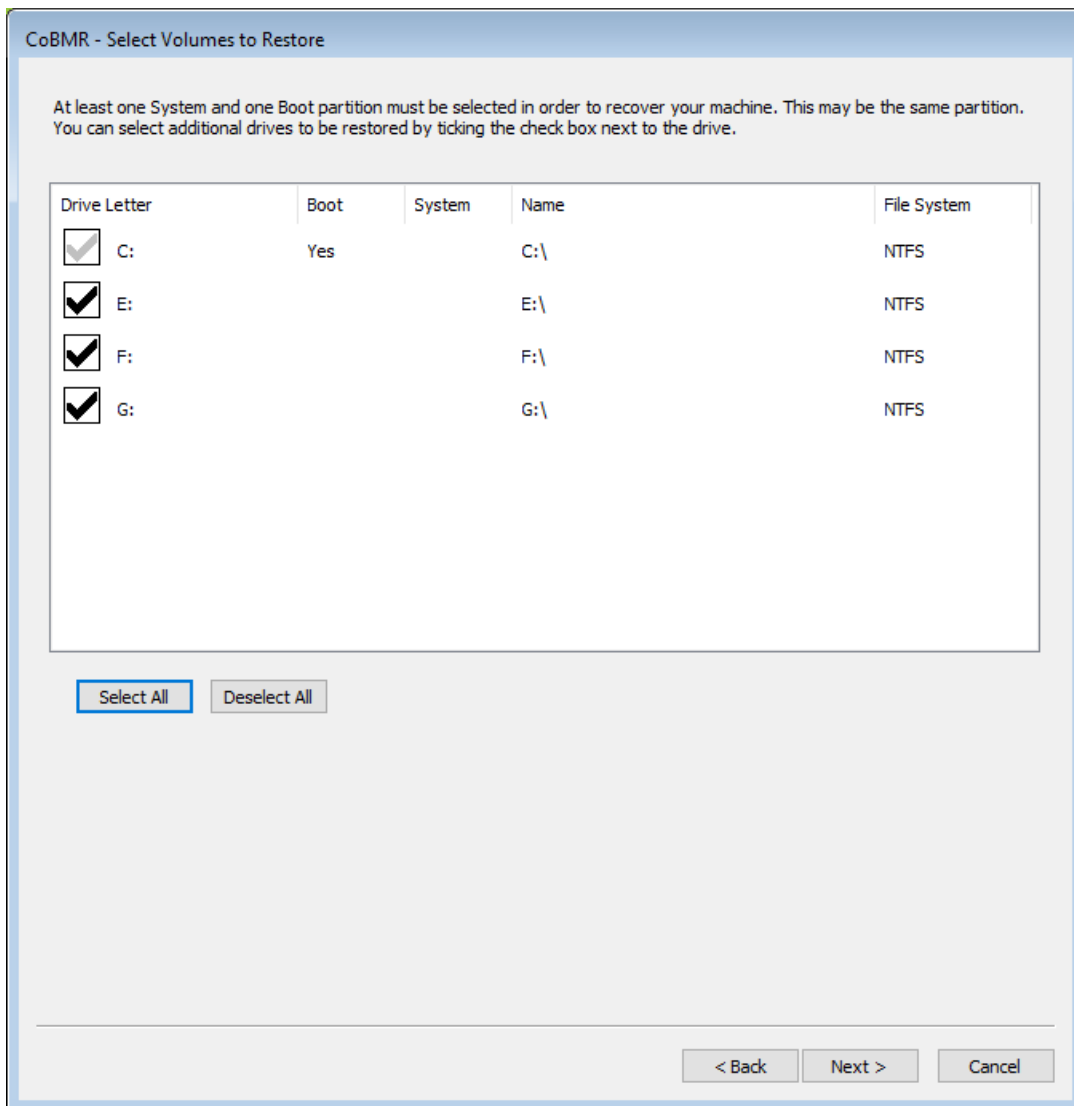




At this stage, nothing has happened to the disks. Press **Next>** to continue with the recovery.

7.2.6 Select Volumes To Restore

The next step prompts for the volumes to restore. Generally, each volume represents a disk partition. Put a tick against each volume that should be restored or **Select All**:



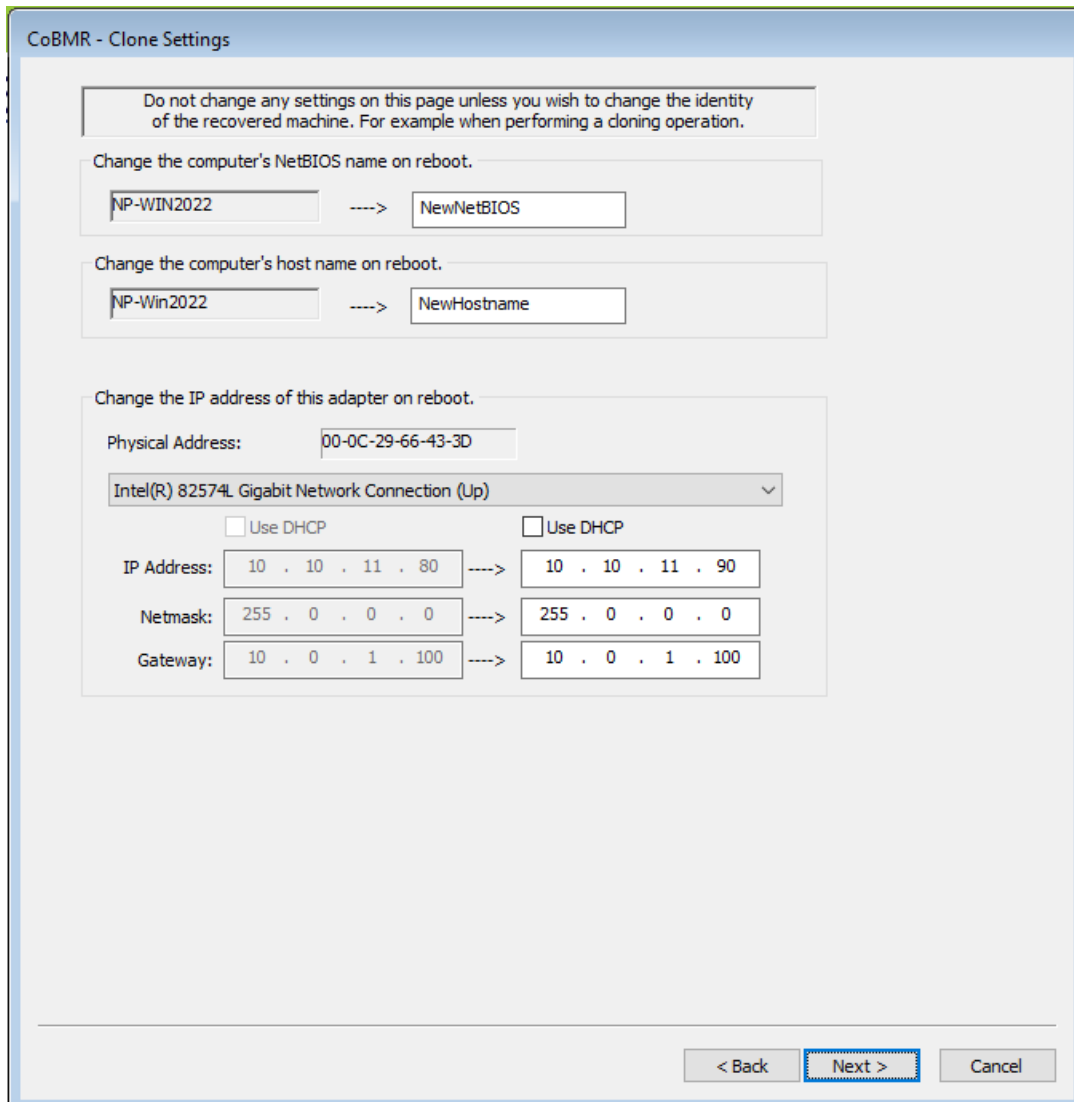
Note: the system and boot partitions (even if on different partitions) will always be restored by default.



Click [Next>](#) to continue to the next step.

7.2.7 Clone Settings

Use this dialogue to change the recovered system's **hostname** and **IP addresses** if required. Select to use either DHCP or enter a valid static IP address.



The image shows a screenshot of the 'CoBMR - Clone Settings' dialog box. It contains three main sections for configuration:

- NetBIOS Name:** A section titled 'Change the computer's NetBIOS name on reboot.' with a text box containing 'NP-WIN2022' and a 'NewNetBIOS' button.
- Host Name:** A section titled 'Change the computer's host name on reboot.' with a text box containing 'NP-Win2022' and a 'NewHostname' button.
- IP Address:** A section titled 'Change the IP address of this adapter on reboot.' containing:
 - A 'Physical Address' field with the value '00-0C-29-66-43-3D'.
 - A dropdown menu showing 'Intel(R) 82574L Gigabit Network Connection (Up)'.
 - Two 'Use DHCP' checkboxes, both currently unchecked.
 - Fields for 'IP Address', 'Netmask', and 'Gateway', each with a current value and a 'New' button to its right. The current values are: IP Address: 10 . 10 . 11 . 80; Netmask: 255 . 0 . 0 . 0; Gateway: 10 . 0 . 1 . 100. The 'New' buttons contain the values: 10 . 10 . 11 . 90; 255 . 0 . 0 . 0; 10 . 0 . 1 . 100.

At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

You may change the IP address for each NIC interface independently. NICs that are currently connected to a network are tagged with **(Operational)**.

Note: The **Use DHCP** tick-box shown on the left side of the dialogue indicates whether DHCP was used on the source system. If its ticked it indicates DHCP was used on the source. If unticked a static IP address was used.

If you wish to retain the current hostname and IP addresses leave the fields at their default values and select [Next>](#) to continue to the next section.

Note: When you click on the [Next >](#) the button will change to [Finish](#), when you click on [Finish](#) the restore will start. If dissimilar hardware is detected, then when you click on [Next>](#) the Dissimilar Hardware dialogue will be displayed instead. Click [Finish](#) on that dialogue to start the restore.

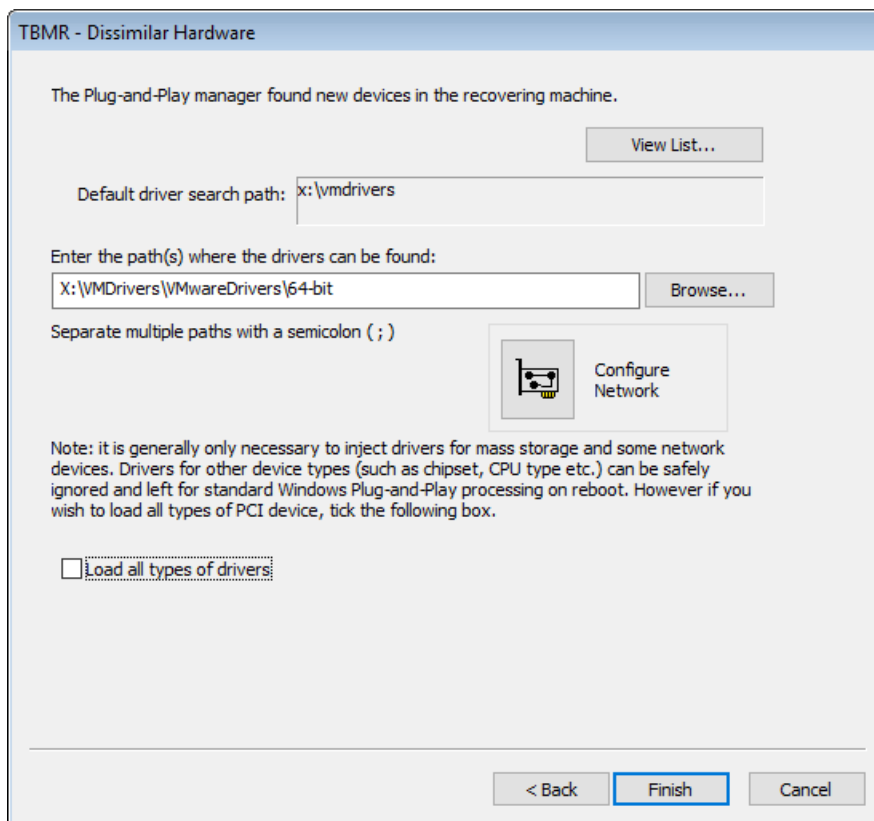


When recovering to a system with a different MAC address (generally during a dissimilar DR), the default IP address settings default to DHCP and not the original IP.

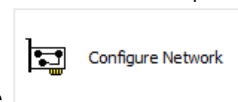
The [Next >](#) button will change to [Finish](#). Click this when ready to continue.

7.2.8 Dissimilar Hardware

Next, the DR process performs a check to determine if there are new devices in the recovering machine that were not present in the original system. If this is true, then this is a 'dissimilar' DR and the following dialogue will be shown to allow the user to specify the location of the new driver files for these devices.

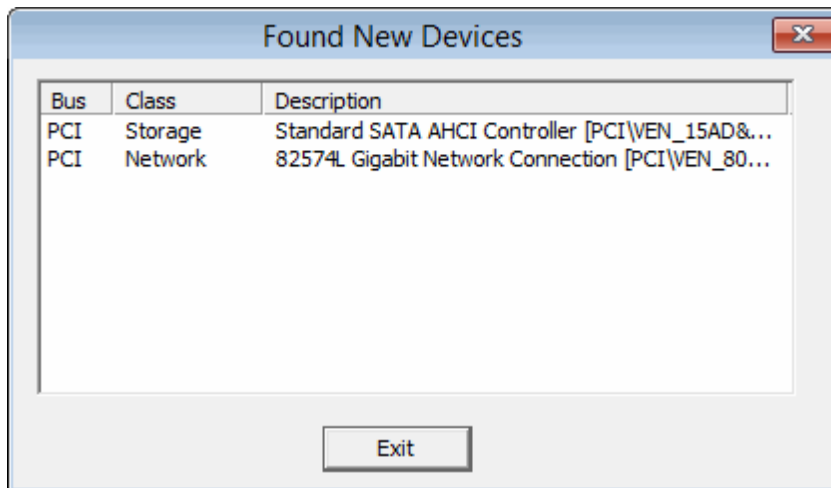


Specify the default path or paths to be searched for the missing driver files. The paths may



be on a local device (eg. a USB disk) or a network share. Use the button if you need to map a network share. In either case, the paths must be accessible to the WinPE5, WinPE10 or WinPE11 environment.

Select [View List...](#) to see a list of the new devices.



Ensure the specified path or paths contain the correct 64-bit drivers for the dissimilar machine. At the end of the DR sequence, the specified paths will be searched for the missing drivers and automatically injected into the recovered system.

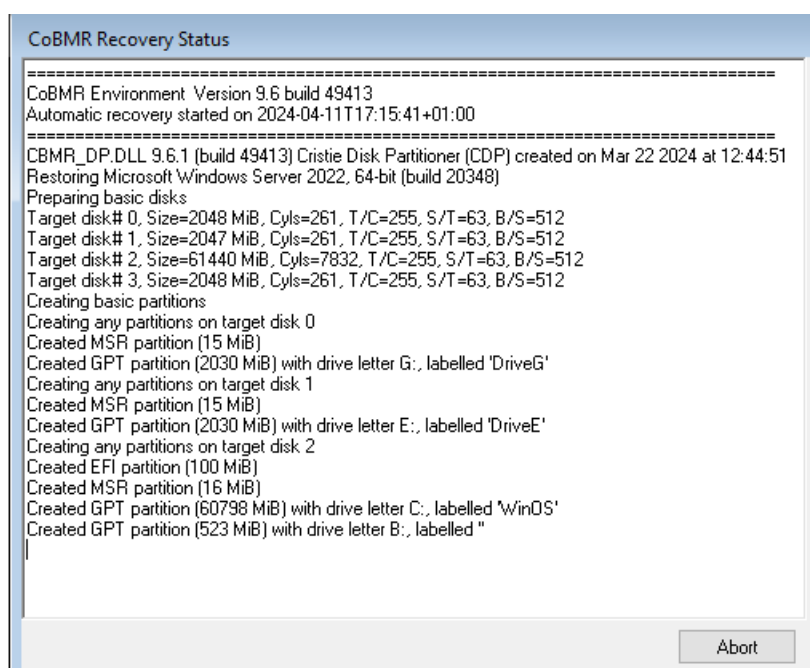
By default, it is only necessary to inject drivers for mass storage devices and, in some some cases, network devices. The 'Load all types of drivers' tick box will force the DR to look for all drivers in addition to mass storage and network devices. For example, this could include graphics cards, USB and chipset devices, but these are rarely required and not recommended.

Note that if drivers are not found for the new boot disk then, although WinPE5, WinPE10 or WinPE11 will be able to recover the files to the disk, there is a good chance that it will not boot correctly.

Press **Finish>** to proceed with the recovery.

7.2.9 Disk Recovery Status

The **Recovery Sequence** begins by preparing the disks selected for the recovery.

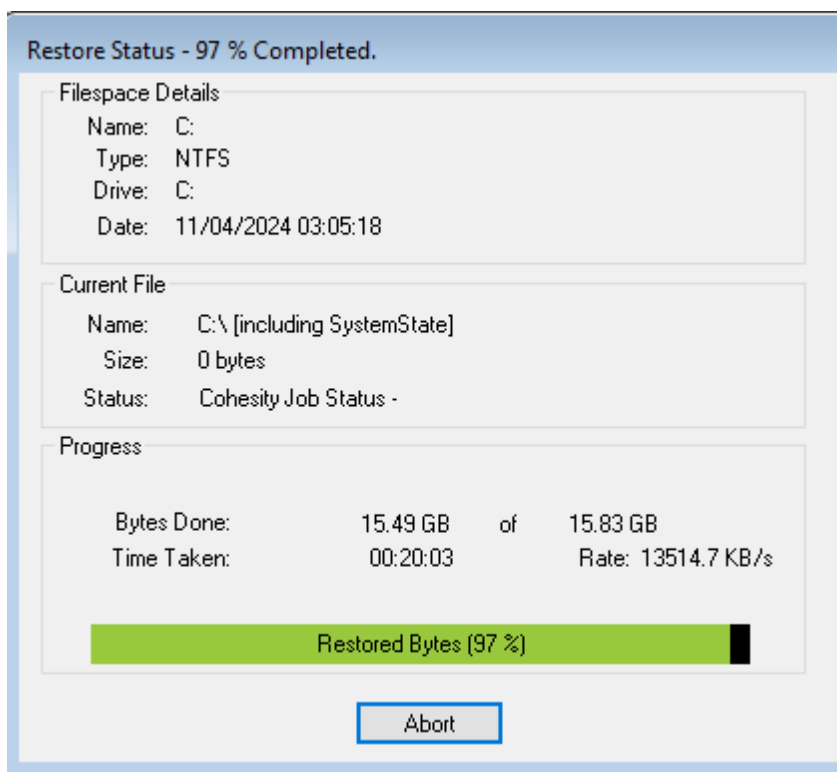


This involves:

- *disk mapping original layout to new*
- *cleaning (removing any existing disk partitions)*
- *removing any existing dynamic volume databases*
- *re-creating the partitions*
- *converting to dynamic volumes if required*
- *formatting to the required partition type*
- *create partition/volume mount points*
- *make bootable volumes active*

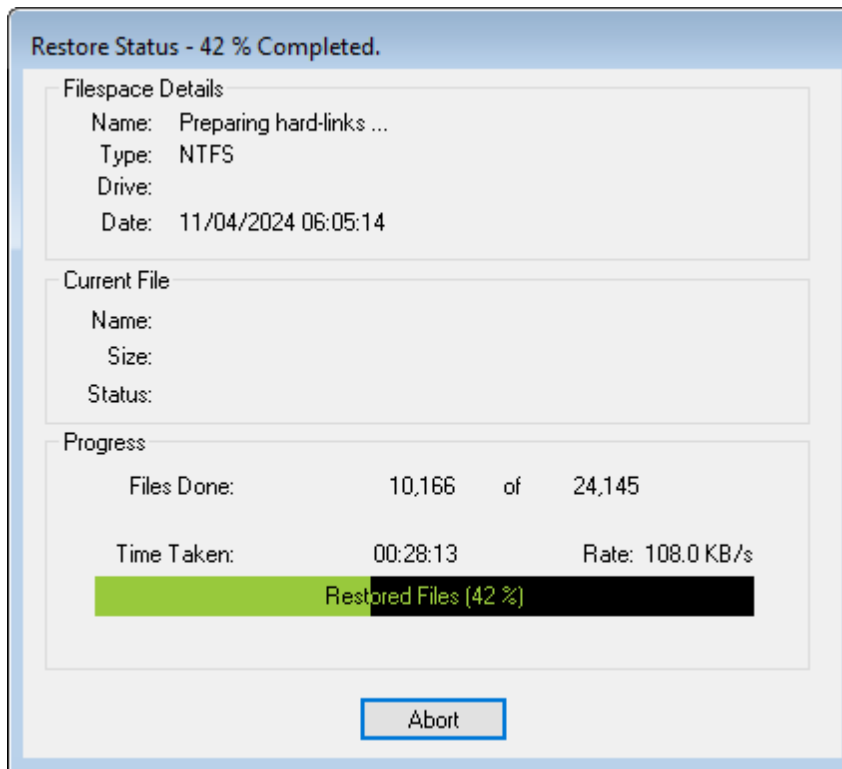
The next step is to recover the volumes to the selected target disks/partitions. A new window appears containing the restore status of recovered files, with a progress bar indicating how much of the backup has been restored. This display also shows the recovery statistics in terms of time, size and throughput.

The recovery is divided into different phases: first the recovery of each selected volume (including **SystemState**),



followed by the restore of **hardlinks**:



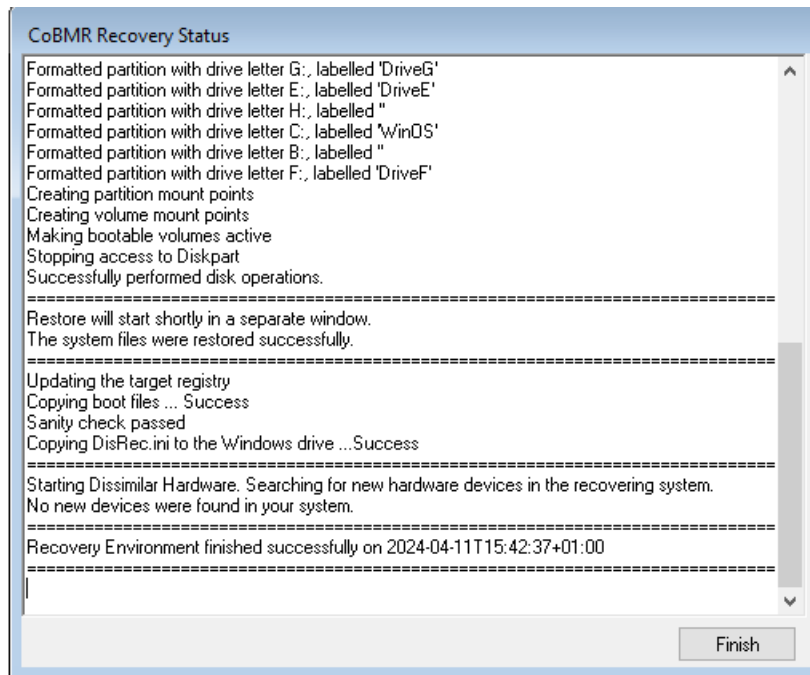


This process may take some time if the backups are large. You may select the [Abort](#) button to terminate the file recovery process, but this may leave a disk or partition in an unpredictable state, which may render it unusable.

If any errors occur during the recovery, an error message will be shown in the window. Refer to the logs post recovery to establish the cause of any error. The final steps of the recovery are to:

- run a sanity check to determine if all the expected boot files are present on the boot volume
- run a dissimilar hardware check to determine if new drivers are required for new boot devices





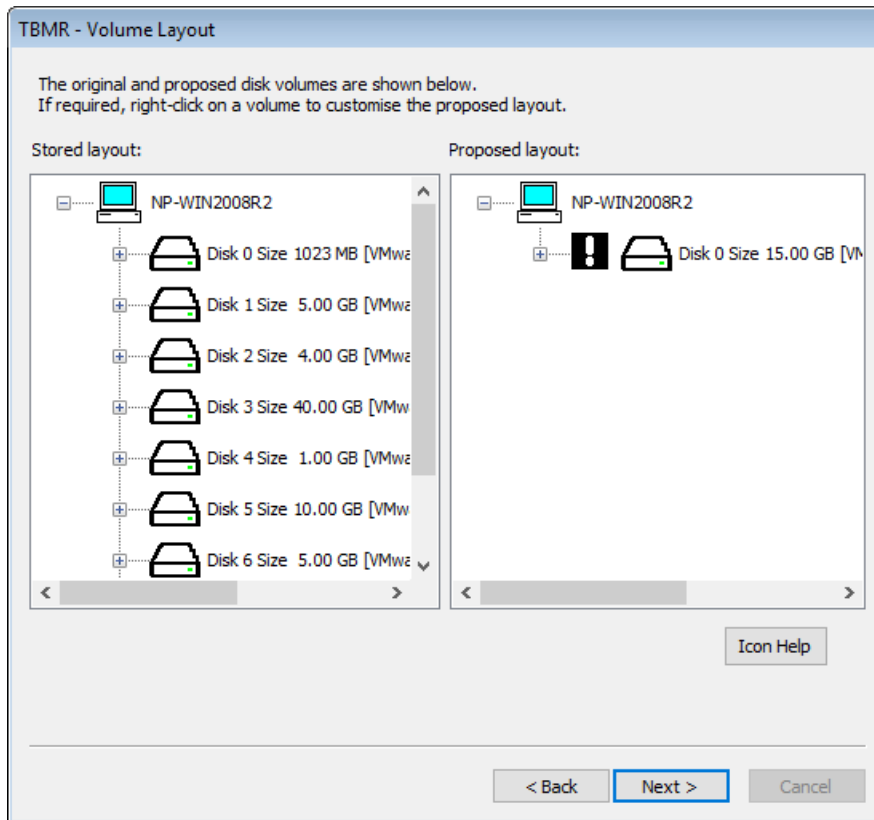
Finally, press **Finish** to return to the **Recovery Environment** main menu. At this point, you may want to view the recovery logs and perhaps copy the logs to a local device or remote share before selecting to reboot. If you have configured the logfile save path from the first step the logfiles will be automatically saved anyway.

Note: recovery logs are also saved to the recovered system to the CoBMR installation sub-folder 'Temp' (e.g. "C:\Program Files\Cristie\CoBMR\Temp")



7.2.10 Disk Scaling

In situations where the target system has fewer or smaller disks than the original system, *Disk Scaling* will come into effect.



The above example shows a recovery from an original system with 8 physical disks, to a target system with only one disk. The target disk is also much smaller than the original system disk.

In this scenario, CoBMR will select as many disks to recover as possible (in this case only one disk - the boot disk). In addition, it will scale the partitions down in proportion to their original size and occupancy. This can be complicated by having, say, mirrored dynamic volumes when the mirror will need to be broken - if only one disk exists on the target (or it has been tagged as not to modify).

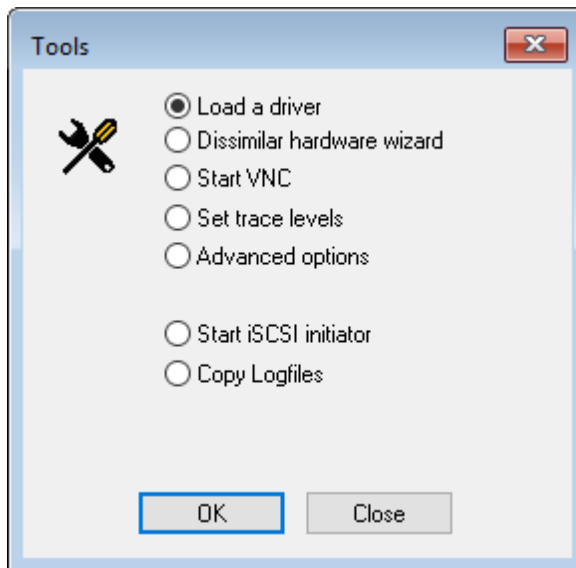
Note 1: the Volume Layout dialogue will only show disks in the left hand panel that can be removed.

Note 2: during a recovery to a system with larger disks, the partition sizes will remain the same as the original by default. However, in this case, it is possible to increase partition size manually during the recovery by right-clicking on the partition icon and selecting [Modify](#).



7.3 Tools

There are a number of tools that can assist with the recovery process. They are all collected under this command button:



The options available are:

- *Load a driver*
- *Dissimilar Hardware Wizard*
- *Start VNC*
- *Set trace levels*
- *Advanced options*
- *Start iSCSI initiator*
- *Copy Logfiles*

Load a driver allows a new mass storage or NIC driver to be injected into the running booted WinPE5, WinPE10 or WinPE11 DR environment. This would be used, for example, to support a mass-storage (disk) device not currently supported out-of-box. This should be done prior to starting the DR sequence.

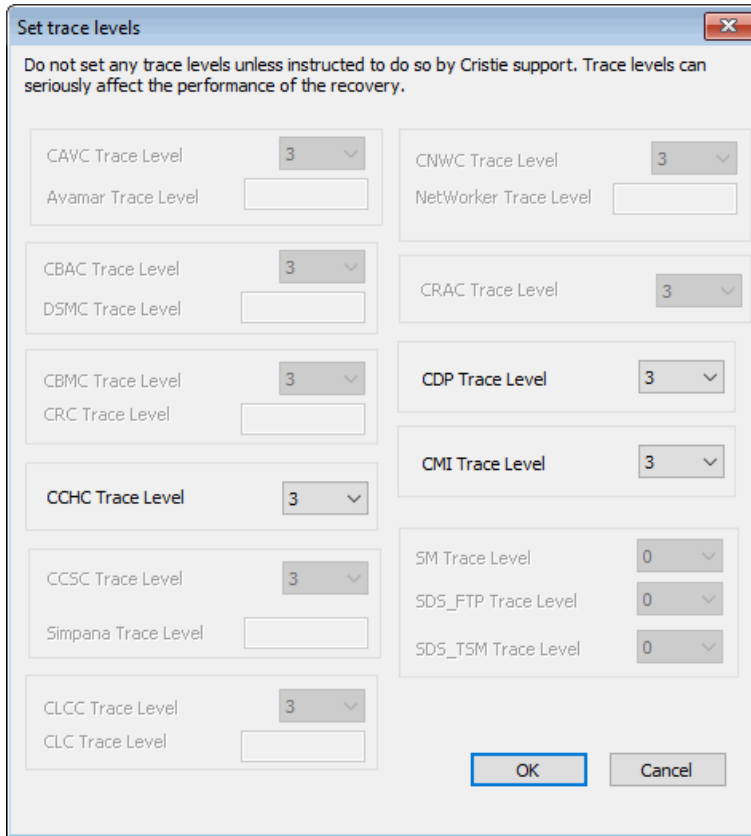
The **Dissimilar Hardware Wizard** will allow drivers to be injected into the recovered system when the target hardware has different devices from the original (eg. RAID controllers). Normally, this will be done automatically as part of the DR sequence and will not need to be run manually.

Start VNC will run a VNC server within the WinPE5, WinPE10 or WinPE11 environment, allowing external VNC clients to remotely connect during the DR session. The start process will provide you with the current IP address of the WinPE5, WinPE10 or WinPE11 environment, which you will need to specify in the VNC client.

Note: the VNC connection is also password protected. The VNC feature is intended for diagnosing DR problems under the guidance of Cristie Support, who will provide the password upon request.



Set trace levels allows the DR log file trace to be increased or decreased as required:

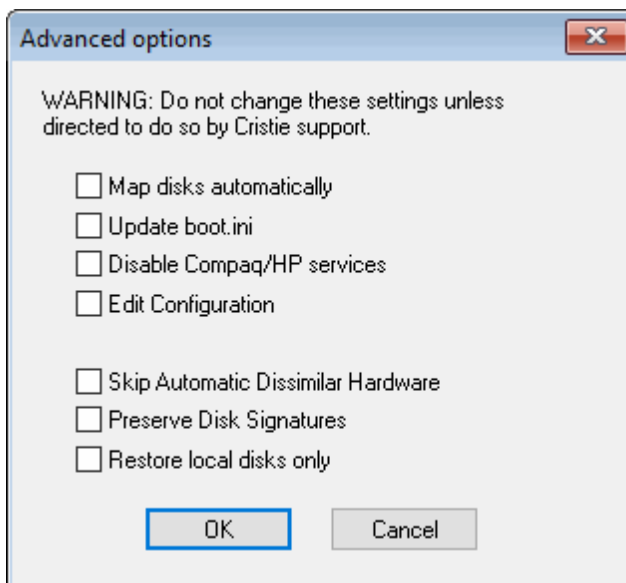


The 'Set trace levels' dialog box contains a warning message: 'Do not set any trace levels unless instructed to do so by Cristie support. Trace levels can seriously affect the performance of the recovery.' Below the warning, there are two columns of trace level settings. Each setting consists of a label and a dropdown menu. The settings are: CAVC Trace Level (3), Avamar Trace Level (empty), CNWC Trace Level (3), NetWorker Trace Level (empty), CBAC Trace Level (3), DSMC Trace Level (empty), CRAC Trace Level (3), CBMC Trace Level (3), CRC Trace Level (empty), CDP Trace Level (3), CCHC Trace Level (3), CMI Trace Level (3), CCSC Trace Level (3), Simpana Trace Level (empty), SM Trace Level (0), SDS_FTP Trace Level (0), SDS_TSM Trace Level (0), CLCC Trace Level (3), and CLC Trace Level (empty). At the bottom right, there are 'OK' and 'Cancel' buttons.

Trace Level	Value
CAVC Trace Level	3
Avamar Trace Level	
CNWC Trace Level	3
NetWorker Trace Level	
CBAC Trace Level	3
DSMC Trace Level	
CRAC Trace Level	3
CBMC Trace Level	3
CRC Trace Level	
CDP Trace Level	3
CCHC Trace Level	3
CMI Trace Level	3
CCSC Trace Level	3
Simpana Trace Level	
SM Trace Level	0
SDS_FTP Trace Level	0
SDS_TSM Trace Level	0
CLCC Trace Level	3
CLC Trace Level	

It is recommended that the trace levels are only changed when advised to do so by Cristie Support staff. This is because they could have a severe impact upon the performance of the backup restore process.

Advanced Options should only be selected when advised to do so by Cristie Support staff.



The 'Advanced options' dialog box contains a warning message: 'WARNING: Do not change these settings unless directed to do so by Cristie support.' Below the warning, there are two groups of checkboxes. The first group includes: 'Map disks automatically', 'Update boot.ini', 'Disable Compaq/HP services', and 'Edit Configuration'. The second group includes: 'Skip Automatic Dissimilar Hardware', 'Preserve Disk Signatures', and 'Restore local disks only'. At the bottom, there are 'OK' and 'Cancel' buttons.

- ☐ Map disks automatically
- ☐ Update boot.ini
- ☐ Disable Compaq/HP services
- ☐ Edit Configuration
- ☐ Skip Automatic Dissimilar Hardware
- ☐ Preserve Disk Signatures
- ☐ Restore local disks only

Start iSCSI initiator - please contact Cristie Support if you wish to use this feature.



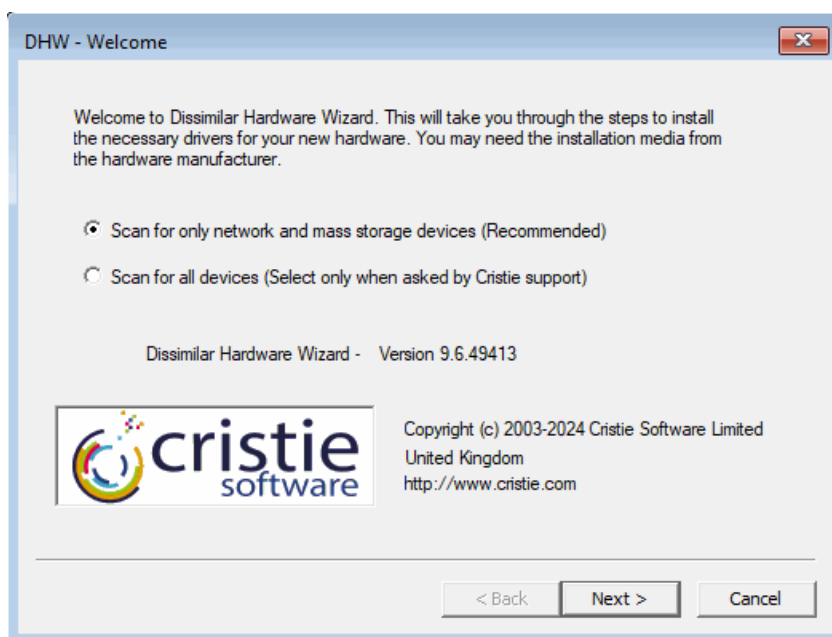
Copy Logfiles allows all the current logfiles created as part of the recovery process to be zipped up and copied to a network share or local device (such as a USB flash drive).

7.3.1 Dissimilar Hardware Wizard

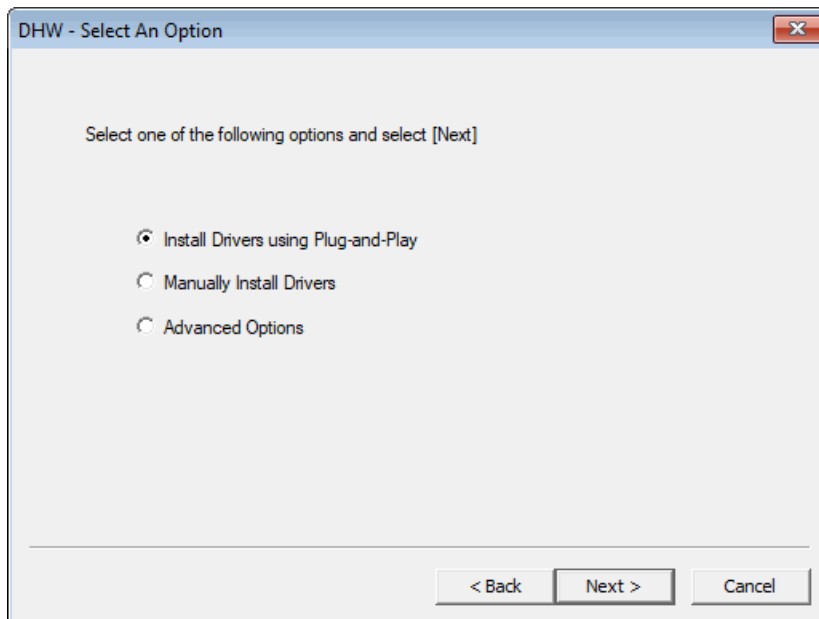
A restore to dissimilar hardware is normally detected during the Automatic or Manual DR sequence. Drivers will be injected automatically at the end of the restore sequence if a source location has been provided. However, if this process has failed for some reason, or additional drivers are required to be injected into the recovering machine, then this **Dissimilar Hardware Wizard** (DHW) tool is provided.

Note: it is only necessary to load the drivers for the hard disk, NIC and, rarely, the HAL. Drivers for the hard disks and NIC can be determined by Plug-and-Play (PnP) and may be readily identified. However, changes required in the CPU model via a change in HAL cannot yet be determined by PnP - these need to be loaded manually.

If you wish to scan for just Mass Storage and Network devices (the minimum required to boot a dissimilar system), select **Next>** to continue to the next step of the Wizard. This is the recommended option. Under the guidance of **Cristie Support**, you may be asked to scan for all devices. In this case, tick the '**Scan for all devices**' box before selecting **Next>**.

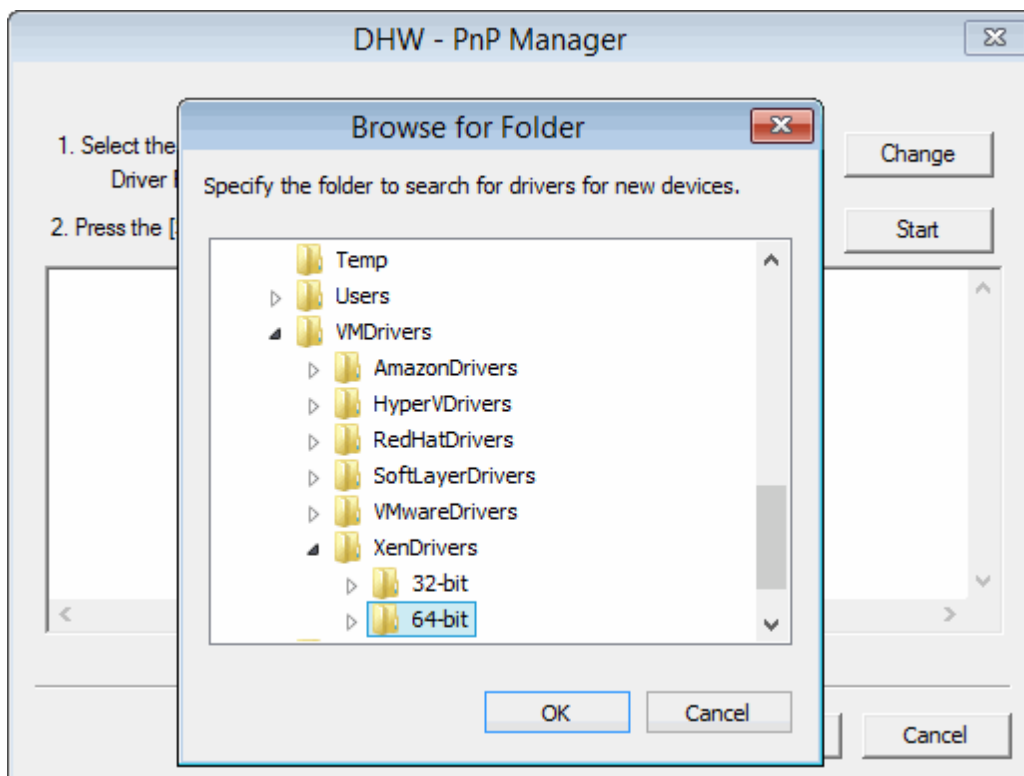


Select the '**Install Drivers using Plug-and-Play**' option:



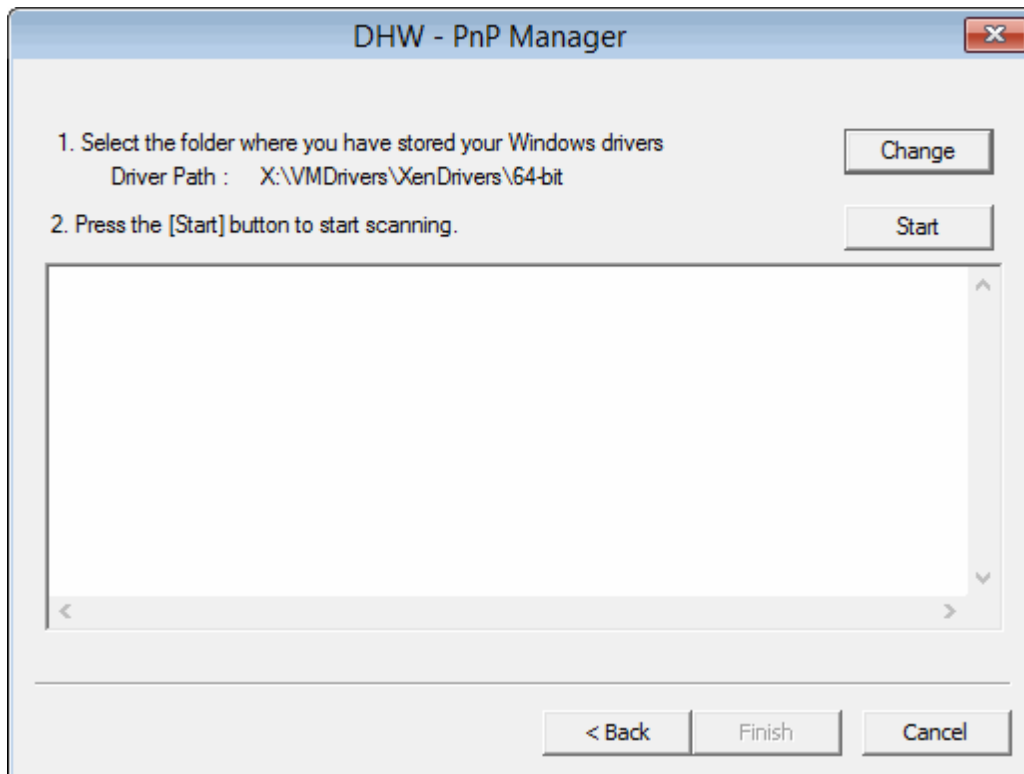
Install Drivers using Plug-and-Play

The window appears empty to start with. The set of drivers located on the recovery CD is the default choice, but in practice they should not be used. Instead, change the driver search path to where you have actually located your drivers (for example, to a network share or another CD) with the **Change** command button.

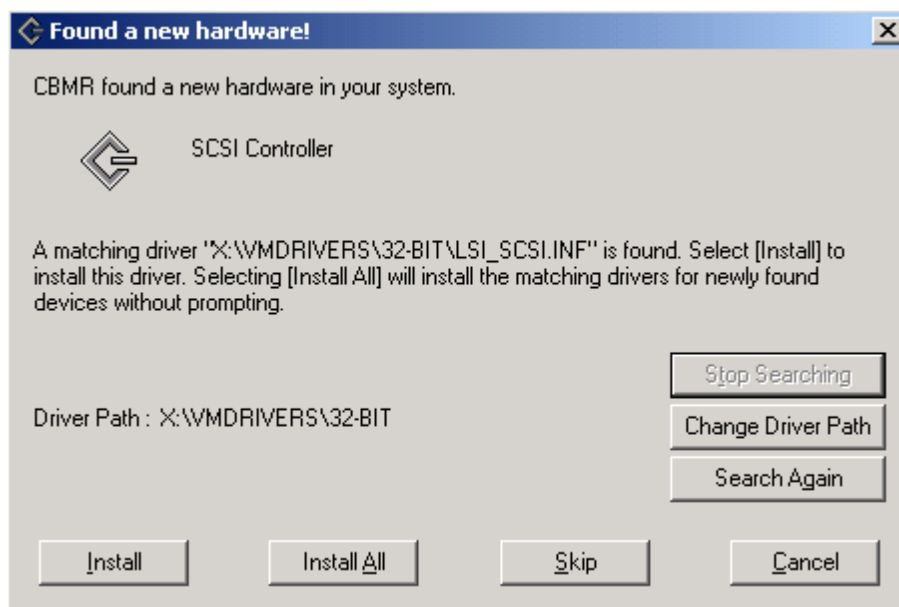


In the example above, the driver search path is changed to the VMware drivers on the WinPE boot CD. Begin the PnP driver detection by clicking **Start**.





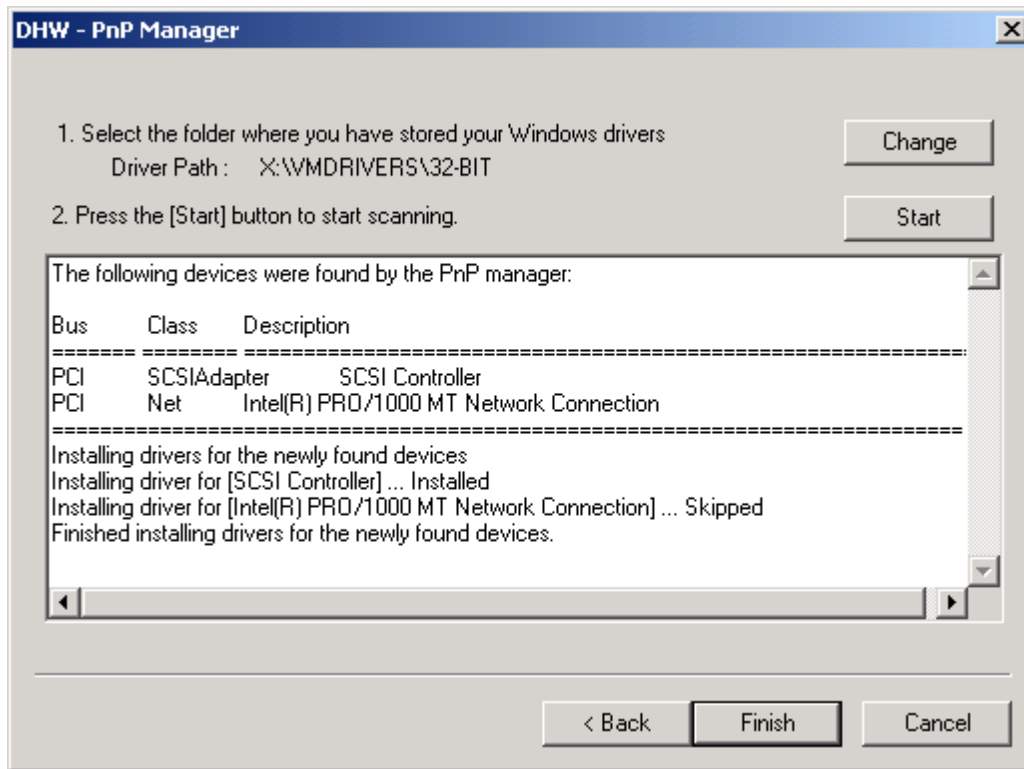
The process checks the devices that it can detect and when it finds one that does not have a driver loaded, it will offer to install it. The example below shows an LSI SCSI device being detected:



If you are satisfied that the found driver path is correct, click on **Install** and the driver will be installed. The device scan will continue and may find, for example, other mass storage or network devices. Follow the steps above to install.

Drivers are usually .sys files. The .inf files define which driver files need to be loaded for a given device. You may need to confirm the location of the driver files for each device, or possibly find the path where they are stored. When you have the correct path, click on **OK** and the Wizard will look for more.

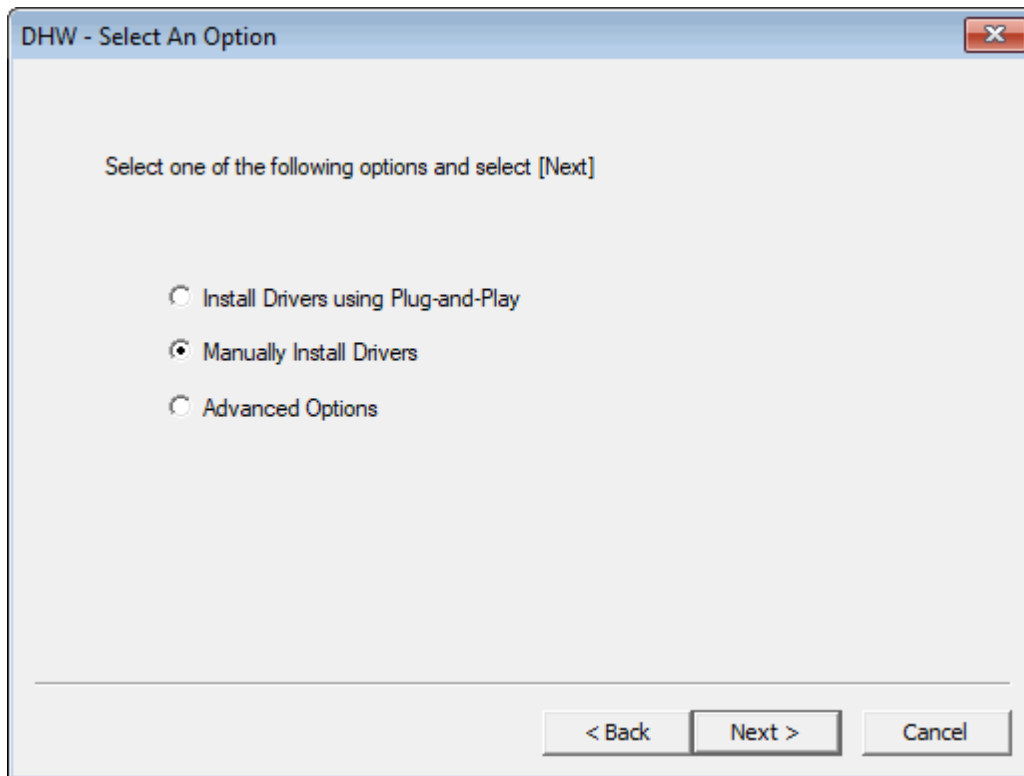
Once all of the drivers of the detected devices have been processed, the Wizard will indicate that the installation has finished. Click on [Finish](#) to proceed.



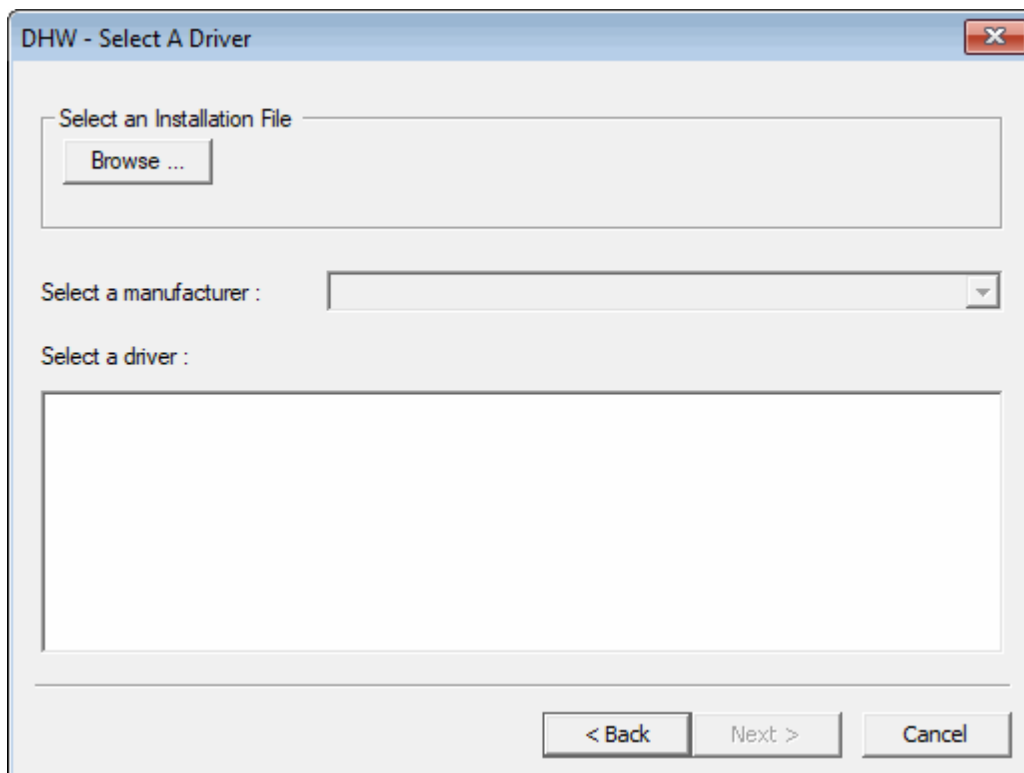
Manual Installation

Typically, you would only manually install a driver for a CPU/HAL change. Select '**Manually Install Drivers**' from the option menu:



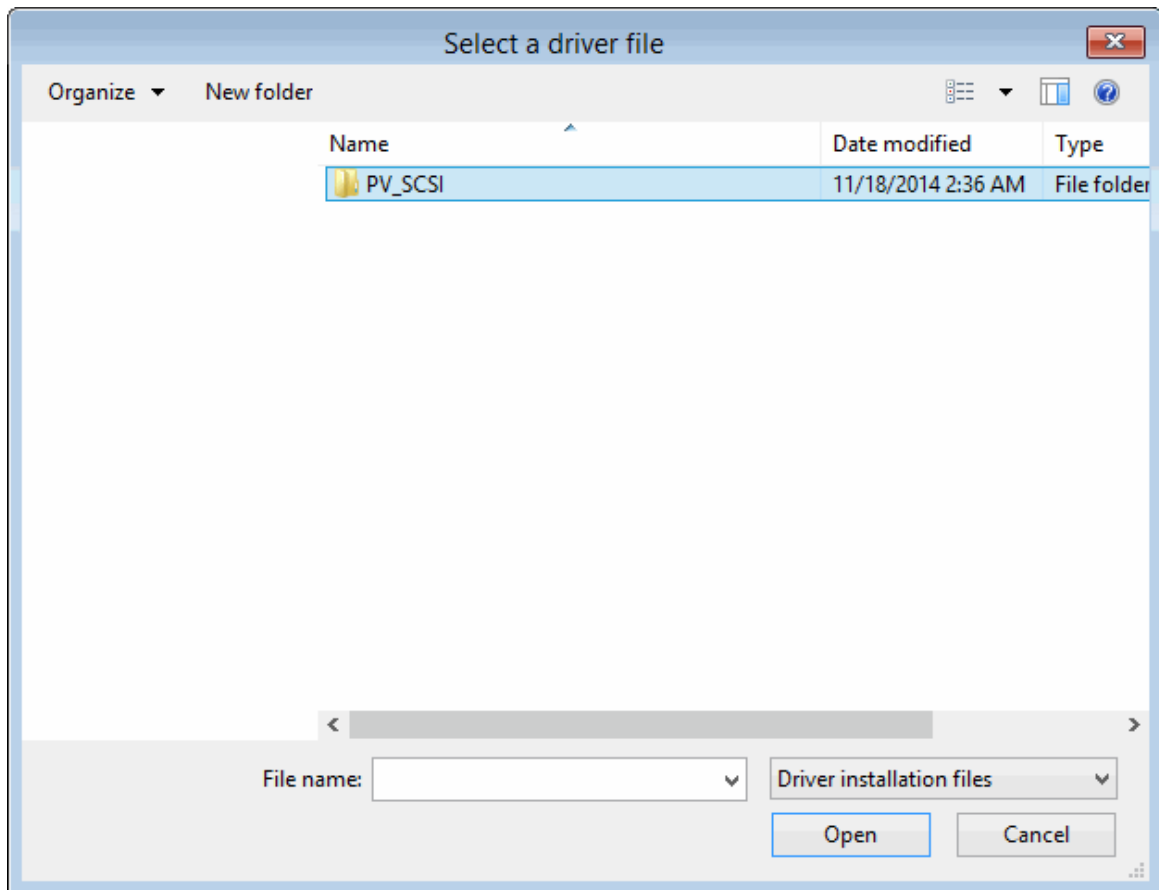


Then select **Next>**.

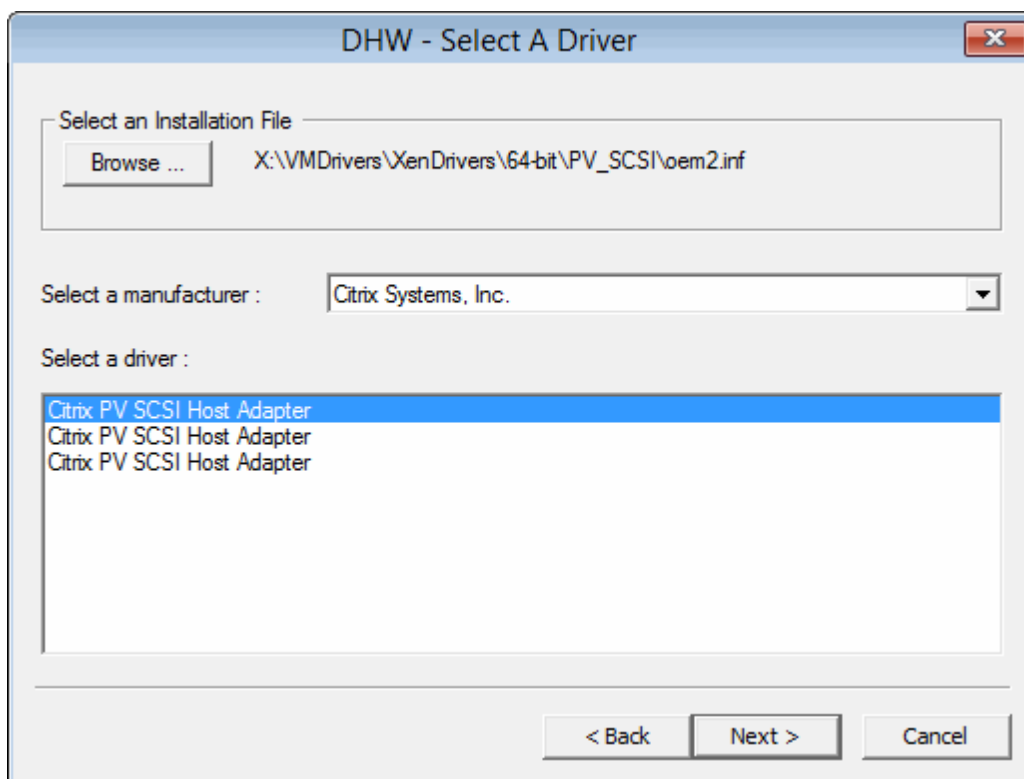


Select **Browse...** to locate the driver or HAL file you need by browsing to the appropriate folder that holds the .inf file. If you need to load the driver from another machine, then you can browse to a share on that machine and then to the appropriate folder.





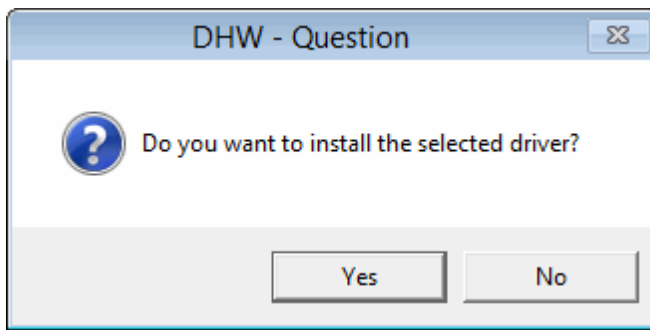
Here we are selecting the Citrix PV SCSI controller driver:



The Wizard allows you to select drivers that are grouped by manufacturer. Select the

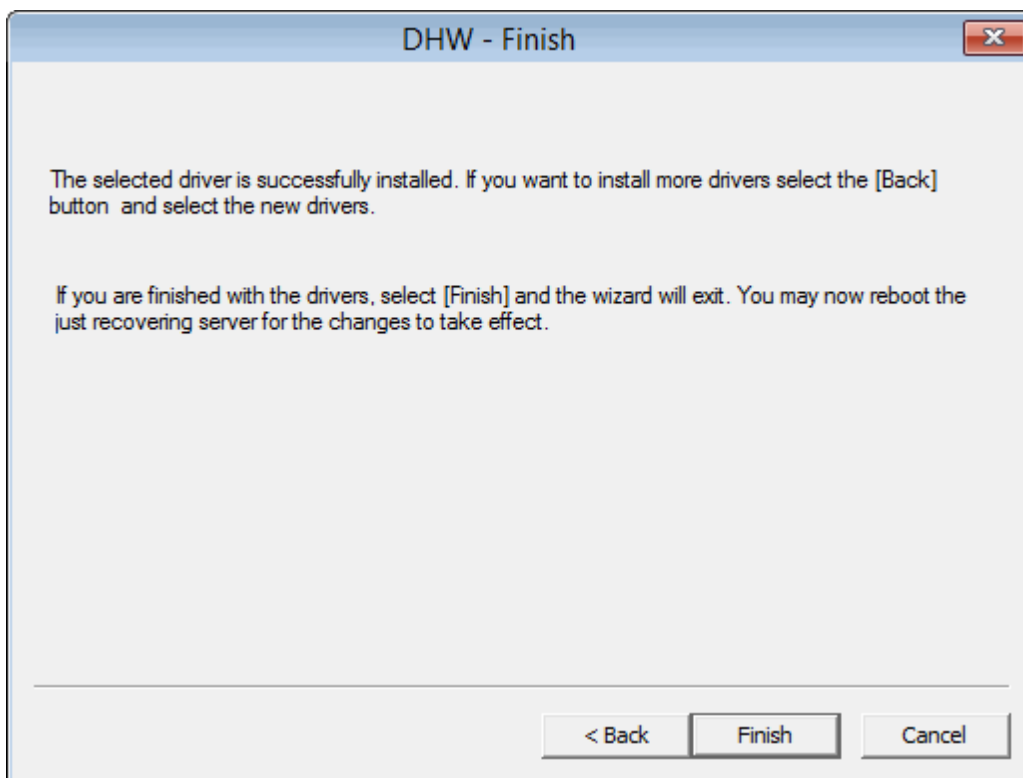


actual driver that you wish to install and click [Next>](#).



After you confirm the selection, the Wizard determines which files need to be installed. You are given the opportunity to change the location from which they are loaded if required..

When the drivers have been installed, the Wizard allows you to go back to install another device driver or [Finish](#) the process.



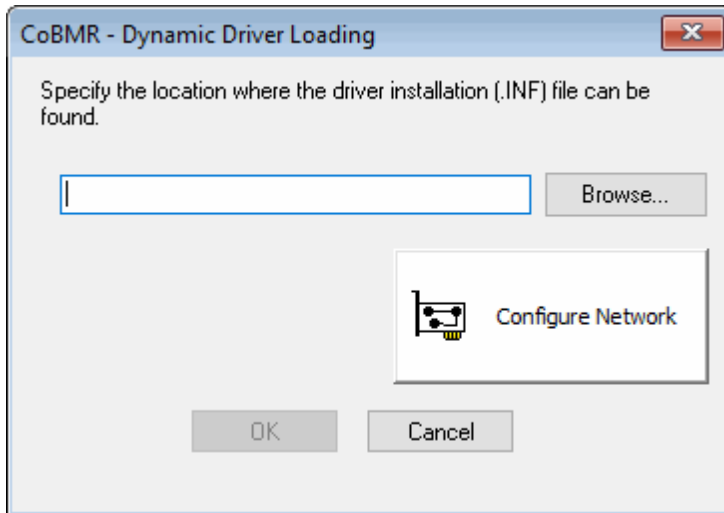
7.3.2 Load a Driver

This option allows a new **Mass Storage** or **Network Interface card** driver to be loaded into the WinPE5, WinPE10 or WinPE11 environment. Use this when WinPE5, WinPE10 or WinPE11 does not have a built-in driver for your hardware.

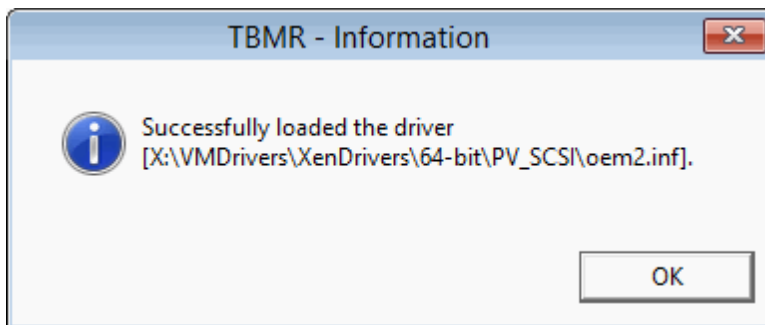
For example, if the DR environment does not show any disks to be recovered, you can inject a new mass storage device driver for the device and retry the DR Wizard.

You will be prompted for the location of the driver INF file. Use the [Configure Network](#) button to map a network share if necessary:





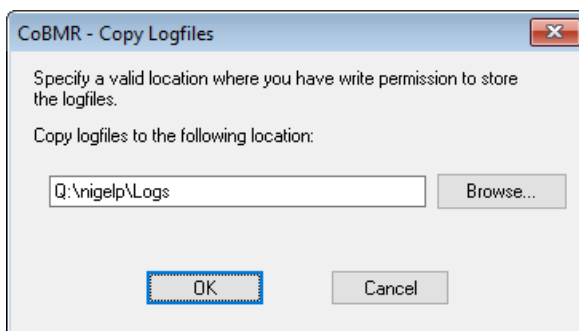
The INF file and other associated driver files (such as the .SYS file) can be located on a CD, USB device or a network share. The following confirmation dialogue is displayed if the driver is loaded successfully:



7.3.3 Copy Logfiles

Since all log and error files generated during the recovery are only transitory (ie. they are lost as soon as the Windows WinPE5, WinPE10 or WinPE11 environment exits), this option allows you to copy the files to a local device or remote network share for permanent record before booting the recovered system.

Use the **Cristie Network Configurator** utility to setup a network share first. All the files are compressed into a single ZIP file so that they can be easily sent to Cristie Support when required.



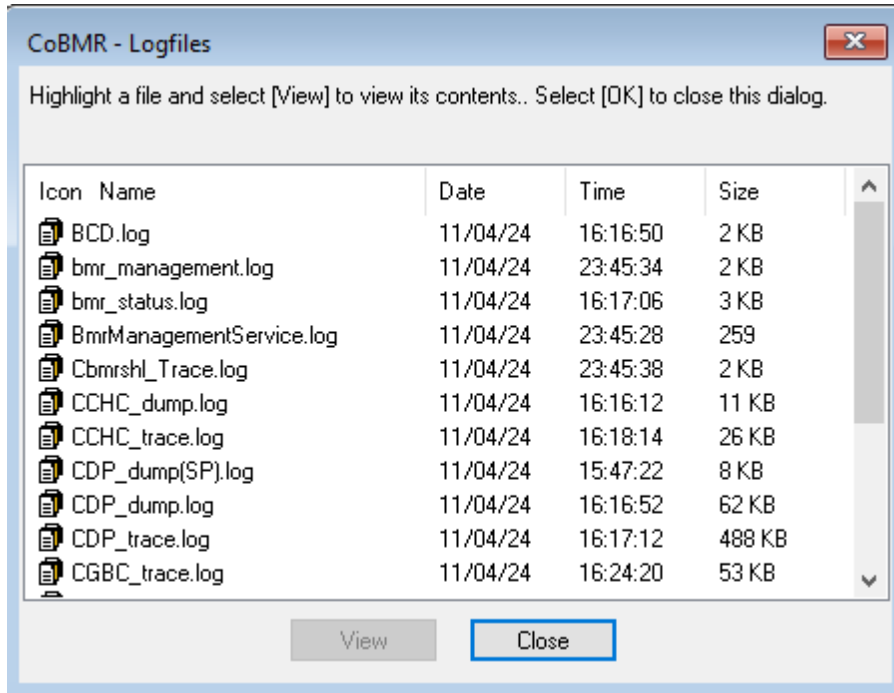
The example shows files being copied to a network share **Q:\nigelp\LOGs**.



Note: the logs are automatically written back to the recovered system after a successful recovery. They are saved to the CoBMR installation sub-folder 'Temp'.

7.4 View Logs

This main menu option allows the log files produced during the recovery to be viewed using Notepad. Normally, viewing this information is only required to diagnose a problem with the recovery.



The important files are (this is not an exhaustive list):

bmr_management.log - remote VA management log, Used by Cristie Support.

bmr_status.log - restored disk and registry configuration log, eg. disks/partitions created summary etc.

BmrManagementService.log - remote VA management log, Used by Cristie Support.

cchc_dump.log - contains a summary of the Cohesity client/server versions and node details.

cchc_trace.log - contains a detailed summary of the Cohesity client/server communications. Used by Cristie Support for diagnosing Cohesity interface problems.

cbmrshl_trace.log - contains a summary of the main menu shell operations. Used by Cristie Support for diagnosing shell operations.

cdp_dump.log - contains general information regarding the system BIOS, disk configuration and timezone details of the original and target system.

cdp_trace.log - contains a detailed summary of how the partitions were restored. Used by Cristie Support for diagnosing disk configuration problems.

CGBC_trace.log - Cristie Generic Backup Client log file.

CRMWizard_trace.log - contains the Recovery Manager log. Used by Cristie Support.

dhw_log.log - contains a summary of Dissimilar Hardware Wizard activities. Used by Cristie Support for diagnosing new driver problems.

discovery_main.log - contains a summary of network discovery activities. Used by Cristie Support for diagnosing network problems.

network.log - contains NIC hardware summary, current network configuration (eg. IP address, gateway IP address etc) and routing table.

PeNetCfg_trace.log - Configure network tool log.

PeRouteCfg_trace.log - Network Routing tool log.

setupapi.log - contains a summary of the Plug and Play devices detected by WinPE5, WinPE10 or WinPE11 as it boots. Used by Cristie Support for diagnosing WinPE5, WinPE10 or WinPE11 driver problems.

Version.log - Used by Cristie Support to determine version of Cristie CoBMR software and DLLs deployed.

7.5 Configure Network

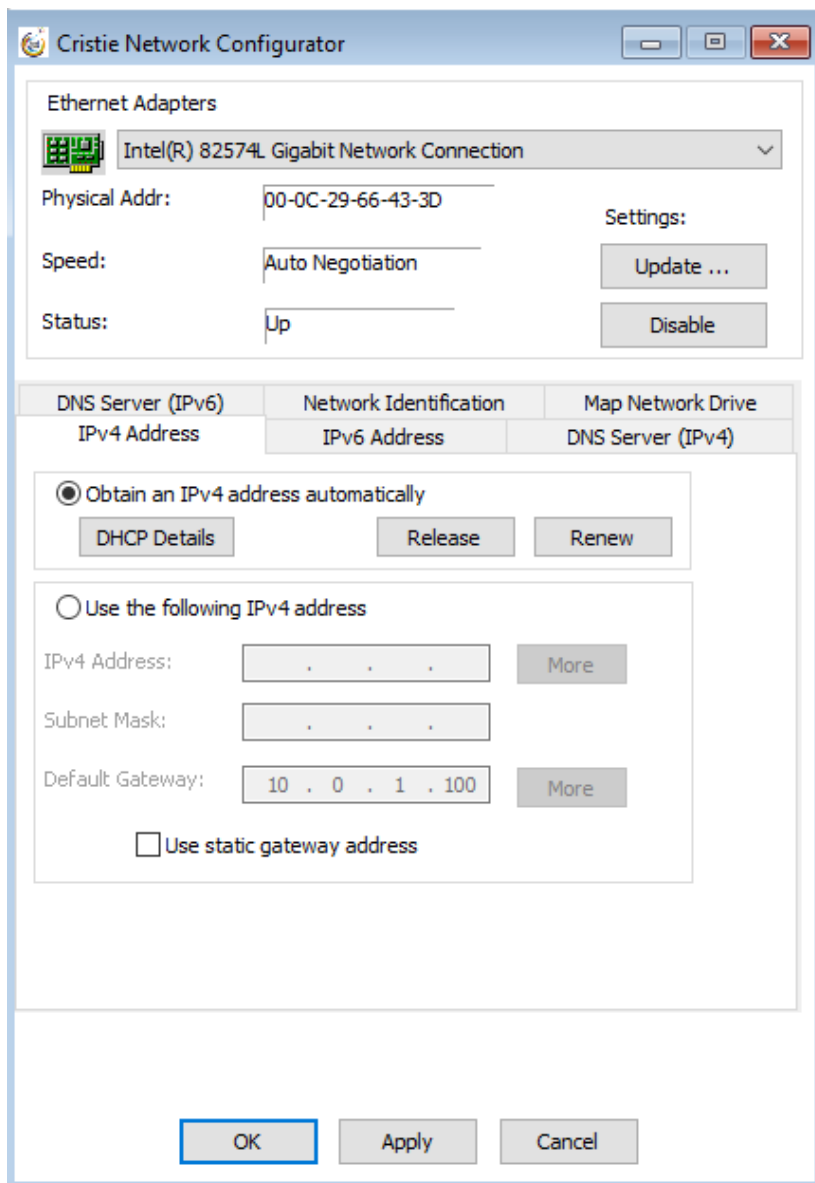
The **Cristie Network Configurator** tool provides extensive facilities to configure the network during the recovery process. It offers the following features:

- supports multiple NICs
- configure individual NIC parameters for duplex mode and link speed
- the ability to select DHCP allocated or static IPv4 IP addresses
- the ability to setup DNS server IPv4 IP addresses
- the ability to setup the Network Identification of the recovering system
- allow file shares to be set on the recovering system (using IPv4 IP addresses)
- map/unmap network drives

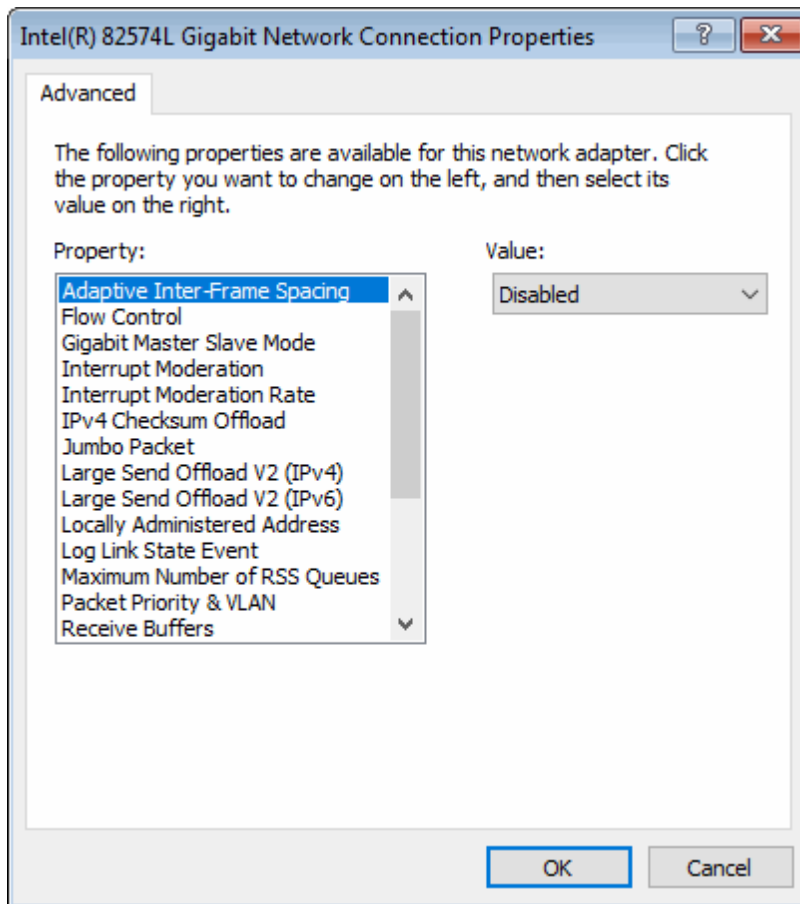


7.5.1 Configure NIC Parameters

It is possible to change both the link speed and duplex mode for any NIC detected on the recovering target system. Select the desired NIC (there could be more than one) from the drop down box and then select [Update...](#)

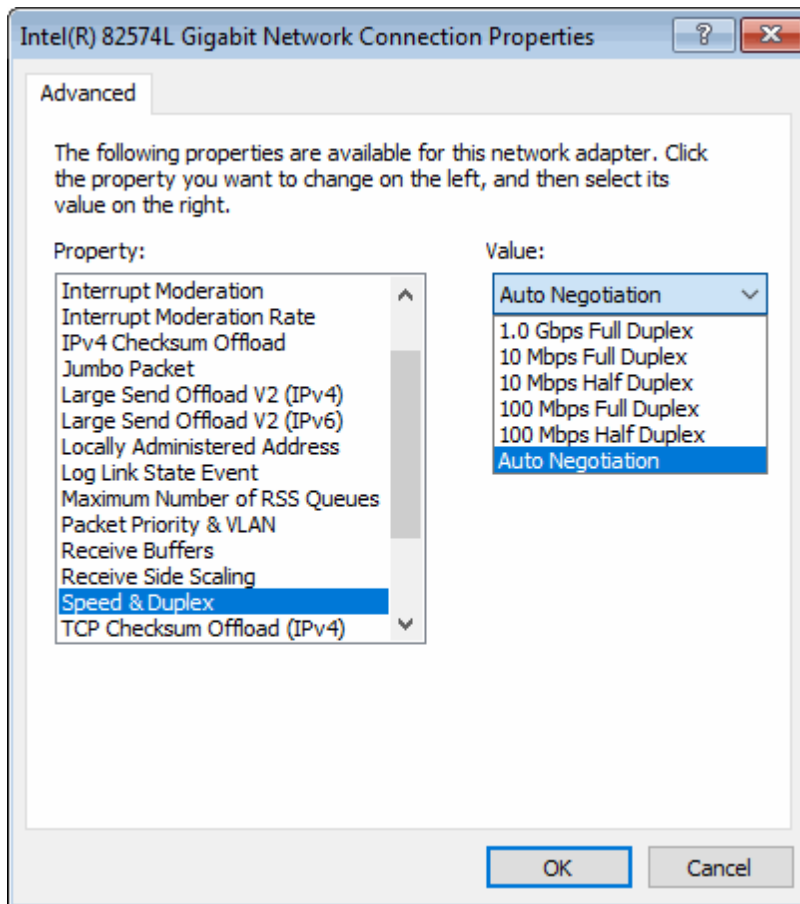


The resulting display offers numerous NIC properties that can be changed. This property list is dependent upon the NIC - ie. not all properties will be available for all NICs.



To change the NIC speed or duplex setting, select the corresponding Property from the dialogue and then select the required value from the Value drop down box as shown below:





Again, note that the speed/duplex settings available are NIC dependent. Auto Negotiation is generally the NIC default setting. Other NIC properties may be changed as required.

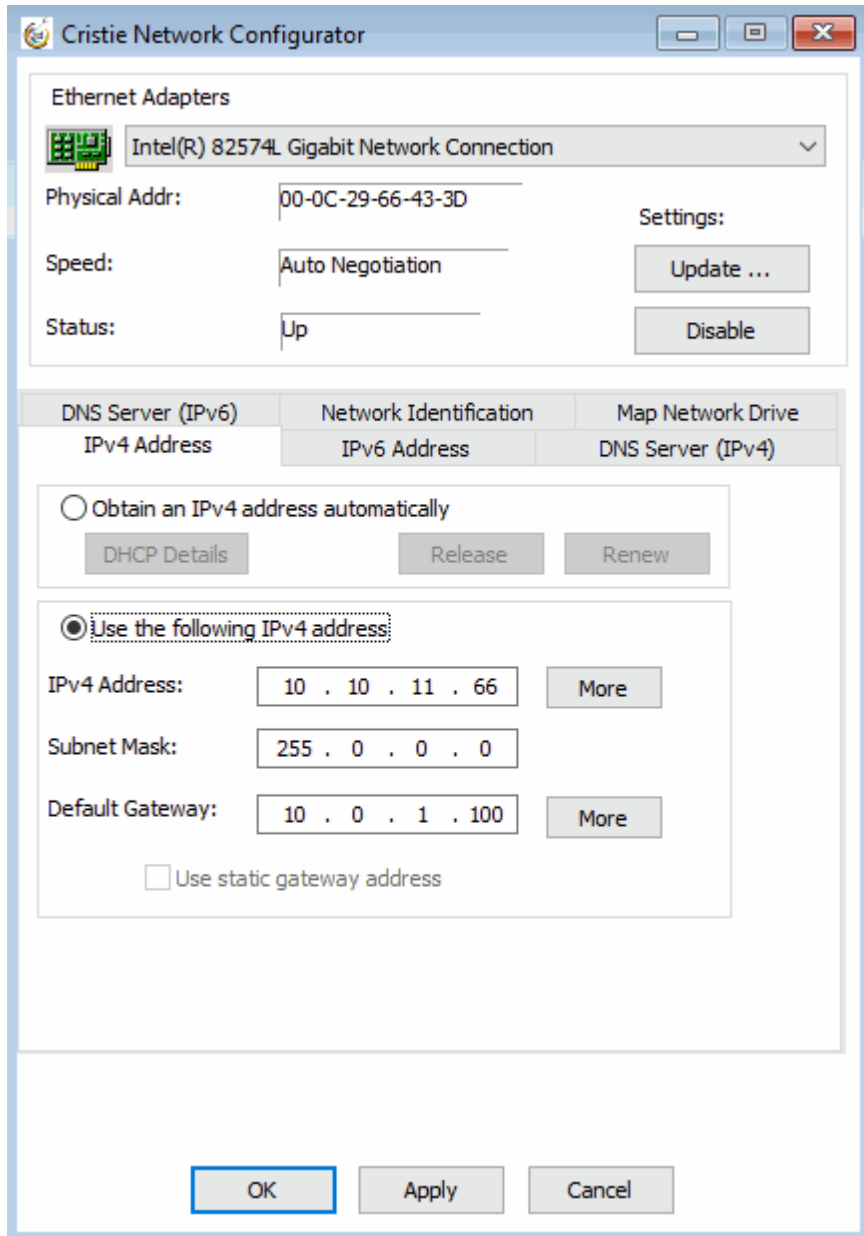
If the NIC is currently connected to the network then the *Status* will be shown as **Operational**. Otherwise the NIC is considered to be **Non-Operational**.



7.5.2 Assign Static or DHCP IP Settings

Normally the WinPE5, WinPE10 or WinPE11 DR environment will start with DHCP enabled and active. However, if a static IP is required, use the 'Use the following IP address' option to manually configure.

First ensure the desired network adapter is selected from the drop down list. If a static IP address is to be applied, select the 'Use the following IP address' button. This will automatically deselect the default DHCP option and allow the static IP parameters to be defined.



Set the new IP address, subnet mask and gateway IP address. The [More](#) button will allow the system to have more than one static IP address. Click on [Apply](#) to confirm the settings for the selected adapter.

This feature will also allow the DHCP lease to be released or renewed, as required.



7.5.3 Map a Network Drive

In order to simplify access to network resources, the Network Configurator allows you to map a network drive to a network share. Start the Cristie Network Configurator from the **Tools** menu and select the **Map Network Drive** tab.

The screenshot shows the 'Cristie Network Configurator' window. At the top, under 'Ethernet Adapters', the 'Intel(R) 82574L Gigabit Network Connection' is selected. Below this, fields for 'Physical Addr:' (00-0C-29-66-43-3D), 'Speed:' (Auto Negotiation), and 'Status:' (Up) are visible, along with 'Update ...' and 'Disable' buttons. A tabbed interface below has three tabs: 'IPv4 Address', 'IPv6 Address', and 'DNS Server (IPv4)'. The 'Map Network Drive' tab is active. It contains a 'Map a network drive' section with a 'Drive:' dropdown set to 'Q:', a 'Network Path:' field containing '\\10.1.1.60\\test-scratch', a 'Domain\\Username:' field with 'software\\nigelp', and a 'Password:' field with masked characters. A 'Map Drive' button is to the right. Below this is an 'Unmap a network drive' section with a dropdown menu and an 'Unmap Drive' button. At the bottom of the window are 'OK', 'Apply', and 'Cancel' buttons.

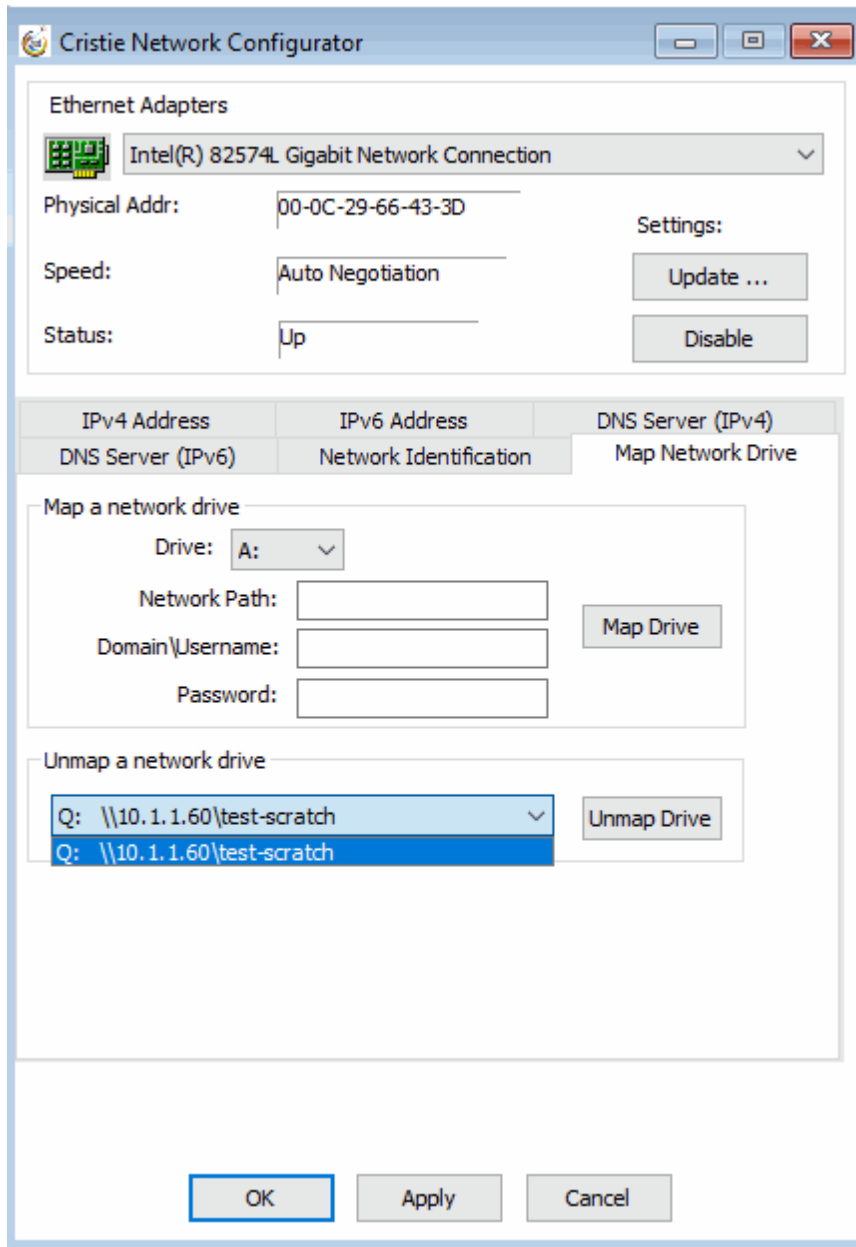
Select the drive letter that you wish to allocate from the **Drive** drop-down box and type in the share name that you wish to associate with it. Also specify the network credentials to be used to access the share.

Note: The network path may be specified either by hostname or IPv4 address.

Press **Map Drive** to confirm the share operation. If successful, the share will be added to the **Unmap a network drive** drop down list.

7.5.4 Unmap a Network Drive

If you need to disconnect a mapped drive for any reason, this option allows you to do this. Just select the drive that you wish to disconnect from the Unmap a network drive drop down list and then click [Unmap Drive](#).



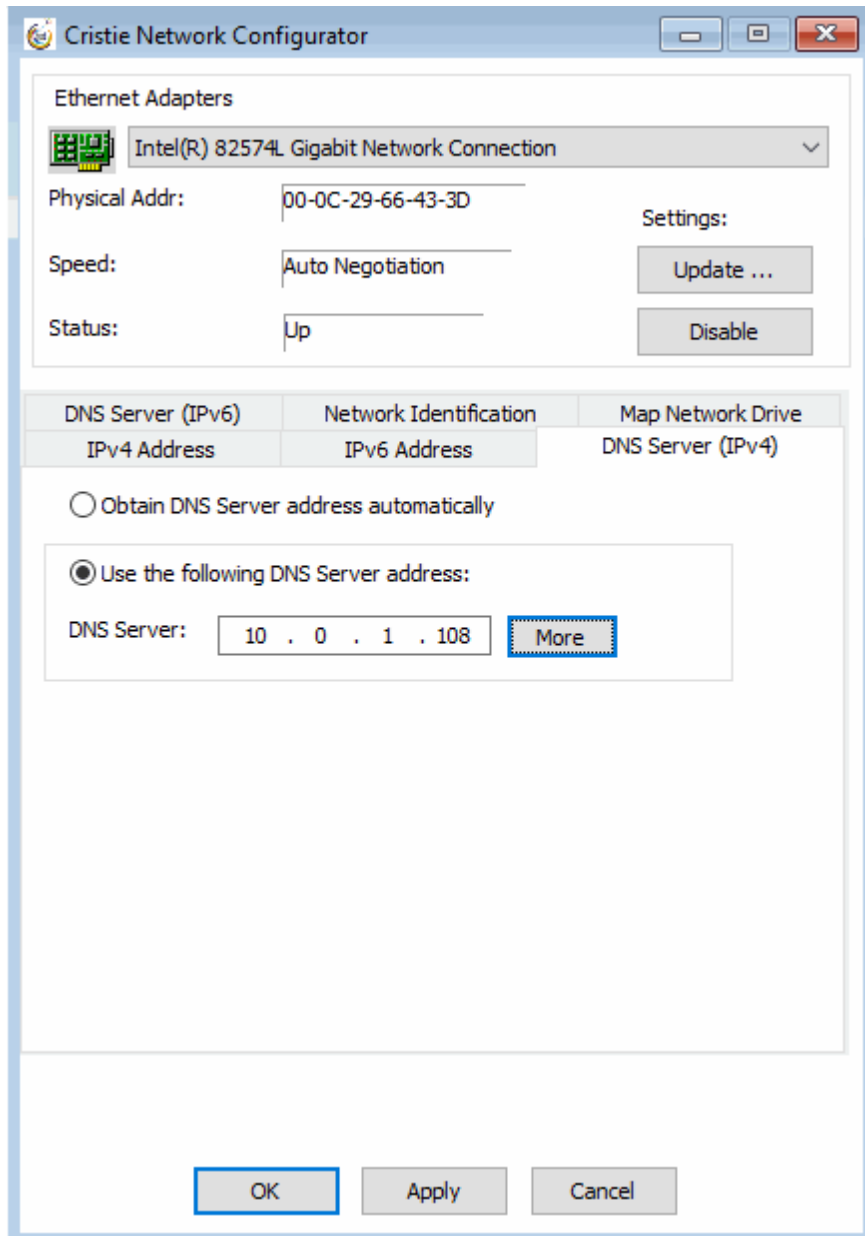
The mapped drive is removed from the list to confirm the operation.



7.5.5 Setup DNS Servers

DNS server IP addresses are automatically set when the WinPE5, WinPE10 or WinPE11 DR environment boots. However, options are provided to allow DNS server IP addresses to be manually set if required.

Note: WINS servers are not currently supported by this tool.



Select the '**Use the following DNS Server address**' radio button and enter the new DNS IP server address. If required, select the [More](#) button to add several DNS IP addresses. Press [Apply](#) to activate the new address.

7.5.6 Setup Network Identification

Click the **Network Identification** tab to setup a new hostname for the recovering system. This allows the WinPE5, WinPE10 or WinPE11 hostname and Primary DNS suffix to be changed during a DR session if required. These details are transient and only apply while the WinPE5, WinPE10 or WinPE11 DR session is running. They are not applied to the recovered system when it reboots after the DR session.

The screenshot shows the 'Cristie Network Configurator' window with the 'Network Identification' tab selected. The 'Ethernet Adapters' section at the top shows 'Intel(R) 82574L Gigabit Network Connection' selected, with a physical address of '00-0C-29-66-43-3D', speed set to 'Auto Negotiation', and status 'Up'. Below this is a tabbed interface with 'Network Identification' active. It contains fields for 'Hostname' (set to 'Win2022-DR'), 'Primary DNS Suffix' (empty), and 'FQDN' (set to 'minint-ipn4eof'). Each field has a 'Set' button. At the bottom are 'OK', 'Apply', and 'Cancel' buttons.

IPv4 Address	IPv6 Address	DNS Server (IPv4)

DNS Server (IPv6)	Network Identification	Map Network Drive
	<p>Hostname: Win2022-DR [Set]</p> <p>Primary DNS Suffix: [Set] Example: 'microsoft.com'</p> <p>FQDN: minint-ipn4eof</p>	

Enter the new Computer Hostname and press **Set** to confirm the change.



7.6 Configure Routing

The **Cristie Route Configurator** tool provides extensive facilities to configure the network routes during the recovery process.

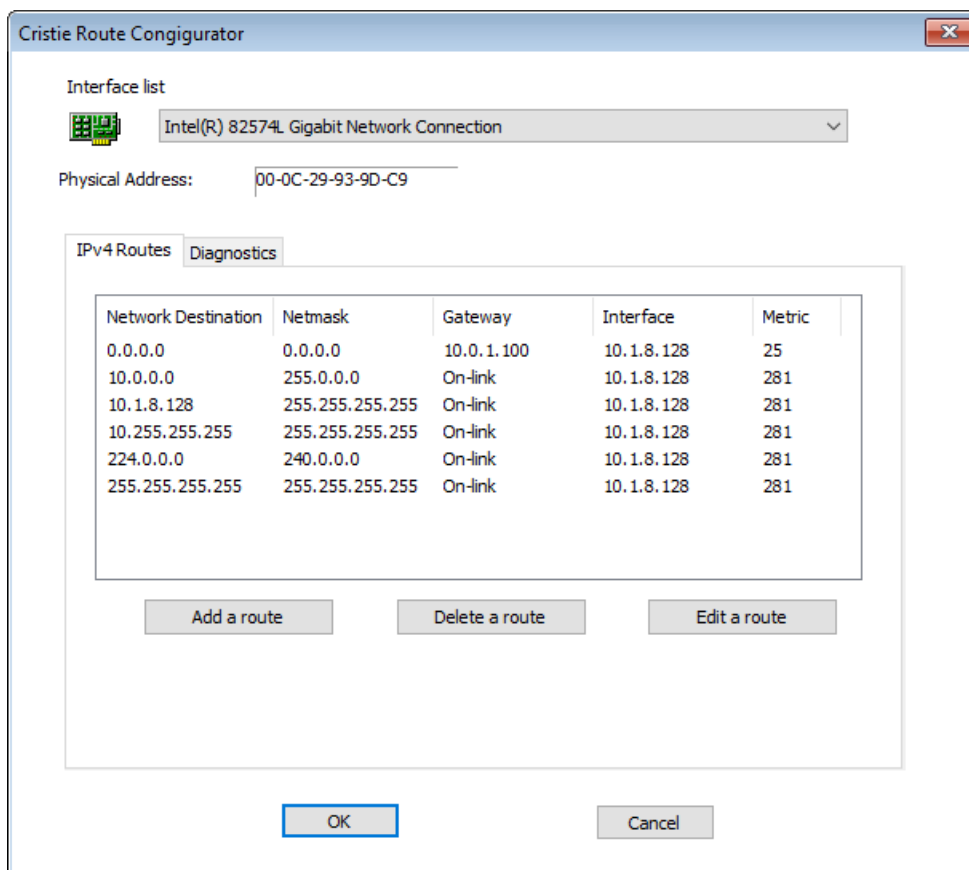
It offers the following features:

- supports multiple NICs
- provides the ability to add/modify/delete a route
- supports IPv4 routes
- allows IPv4 ping/tracert diagnostics to be run on a target hostname or IP address

Note: The WinPE5, WinPE10 or WinPE11 DR environments for CoBMR do not support IPv6. The IPv6 stack has been removed.

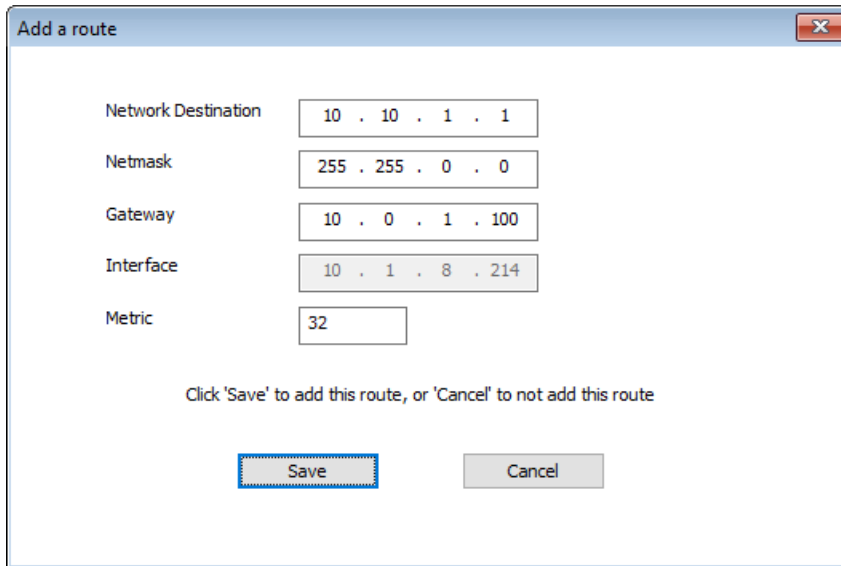
7.6.1 IPv4 Routes

Click the IPv4 Routes tab if not already selected. First select the required interface from the drop-down list.



You may then add a new route, delete or edit an existing route.

To add a new route, click **Add a route**. A data entry dialogue is displayed. To add a route identify the new route network, the route netmask, gateway and route metric. Click **Save** to add the new route or **Cancel** to cancel the creation of the new route.

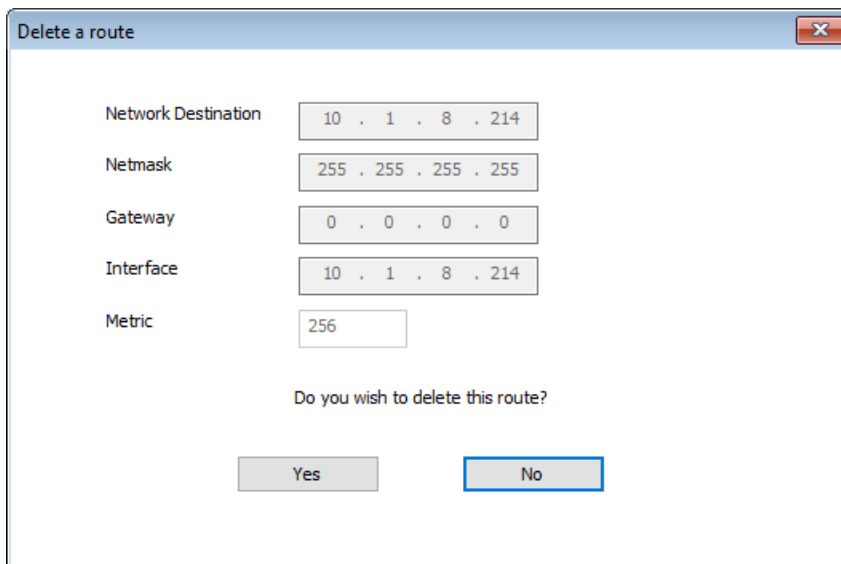


The 'Add a route' dialog box contains the following fields:

Field	Value
Network Destination	10 . 10 . 1 . 1
Netmask	255 . 255 . 0 . 0
Gateway	10 . 0 . 1 . 100
Interface	10 . 1 . 8 . 214
Metric	32

Click 'Save' to add this route, or 'Cancel' to not add this route

To delete an existing route, highlight the desired route in the displayed list and click [Delete a route](#). A confirmation dialogue is displayed. To delete click [Yes](#) to confirm or [No](#) to cancel the delete operation.



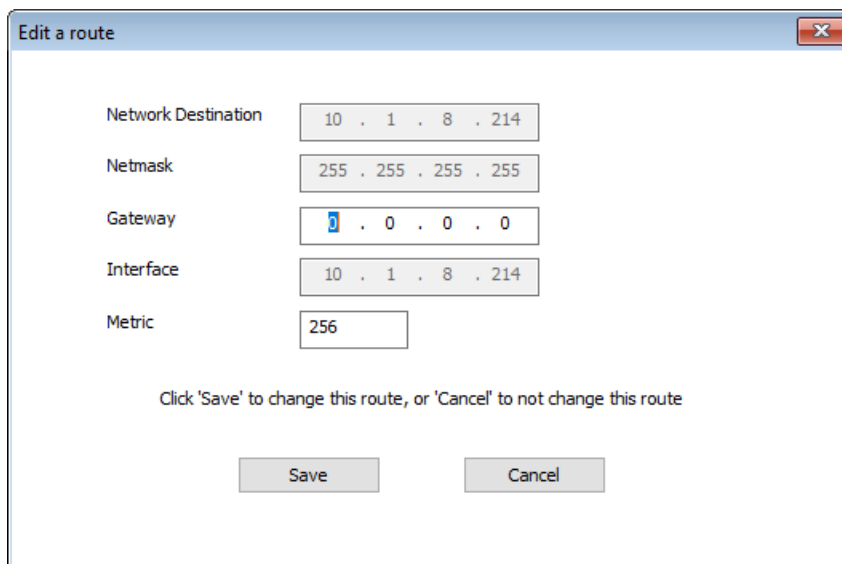
The 'Delete a route' dialog box contains the following fields:

Field	Value
Network Destination	10 . 1 . 8 . 214
Netmask	255 . 255 . 255 . 255
Gateway	0 . 0 . 0 . 0
Interface	10 . 1 . 8 . 214
Metric	256

Do you wish to delete this route?

To edit an existing route, highlight the desired route from the displayed list and click [Edit a route](#). A data entry dialogue is displayed. Only the network gateway and metric can be changed however. Click [Save](#) to make the changes or [Cancel](#) to abandon the changes.





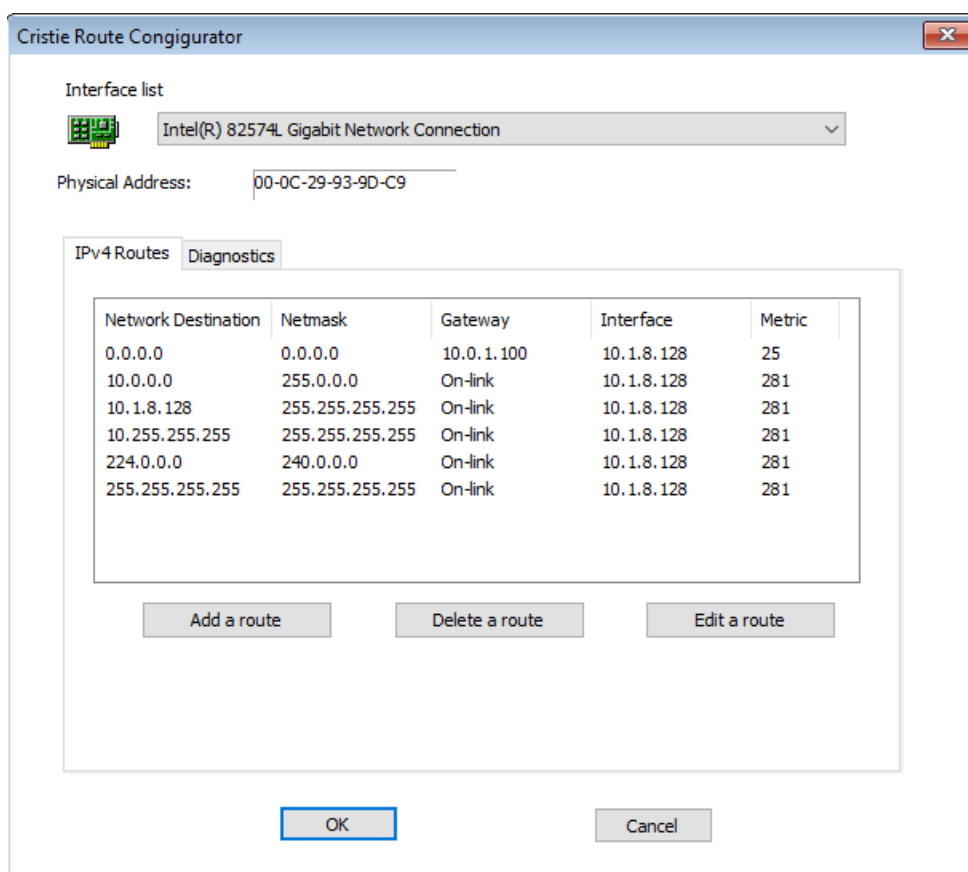
Dialog box titled "Edit a route" with a close button (X) in the top right corner. It contains the following fields:

- Network Destination: 10 . 1 . 8 . 214
- Netmask: 255 . 255 . 255 . 255
- Gateway: 1 . 0 . 0 . 0
- Interface: 10 . 1 . 8 . 214
- Metric: 256

Below the fields, it says: "Click 'Save' to change this route, or 'Cancel' to not change this route". At the bottom are "Save" and "Cancel" buttons.

7.6.2 Diagnostics

Click the diagnostics tab if not already selected. First select the required interface from the drop-down list.



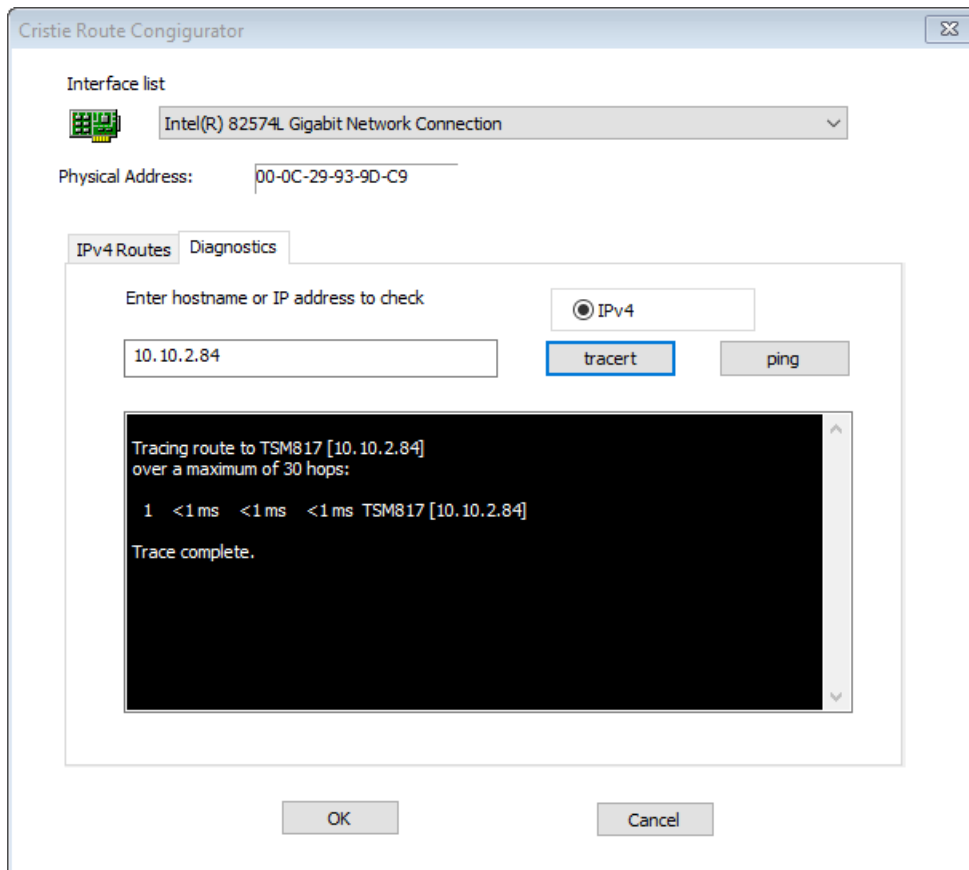
Dialog box titled "Cristie Route Configurator" with a close button (X) in the top right corner. It contains the following elements:

- Interface list: A dropdown menu showing "Intel(R) 82574L Gigabit Network Connection".
- Physical Address: 00-0C-29-93-9D-C9
- IPv4 Routes and Diagnostics tabs: The "Diagnostics" tab is selected.
- Table of IPv4 Routes:

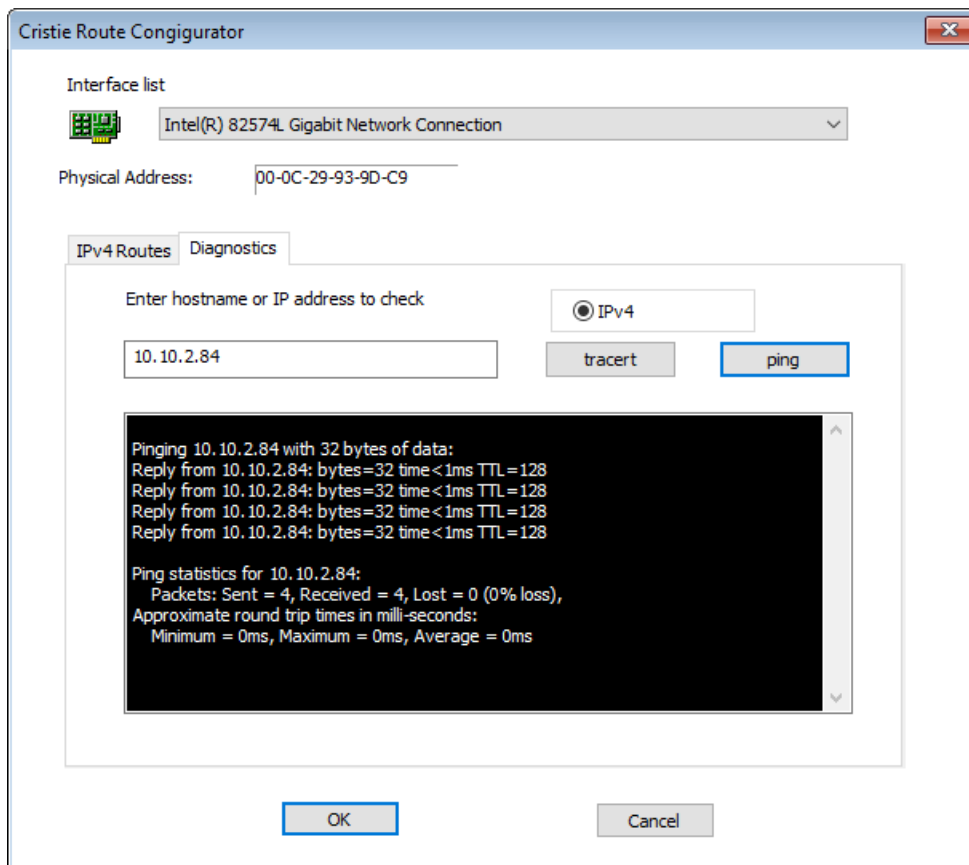
Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	10.0.1.100	10.1.8.128	25
10.0.0.0	255.0.0.0	On-link	10.1.8.128	281
10.1.8.128	255.255.255.255	On-link	10.1.8.128	281
10.255.255.255	255.255.255.255	On-link	10.1.8.128	281
224.0.0.0	240.0.0.0	On-link	10.1.8.128	281
255.255.255.255	255.255.255.255	On-link	10.1.8.128	281

Below the table are buttons: "Add a route", "Delete a route", and "Edit a route". At the bottom are "OK" and "Cancel" buttons.

Enter either the hostname or IPv4 IP address of the network target. Click [tracert](#) to examine the route to the selected target.



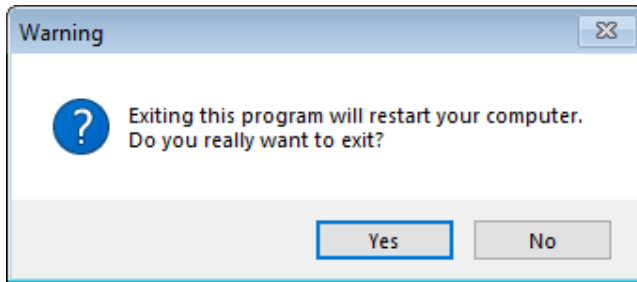
Click **ping** to check connectivity to the selected host. Click **OK** to exit the dialogue.



7.7 Reboot

After a successful recovery, select Reboot to exit the WinPE5, WinPE10 or WinPE11 environment and boot the recovered system. Note you may need to change the default boot device to be the OS boot disk since it may still be configured to boot from the CoBMR DR boot environment.

Click **Yes** on the confirmation dialogue to restart or **No** to continue running the DR console:



7.8 Active Directory Recoveries

To perform an **Active Directory (AD)** restore on a DC no additional user actions are required during the restore phase.

For *block* or *image* based restores the **SystemState** is implicitly restored. For file based restore the SystemState is only explicitly restored if it has been backed up separately otherwise it is implicitly restored along with all the other files. In either case changes are made to SystemState to account for differences in hardware between the source and target machines and minor changes to the boot files if necessary.

After completing the restore the post-recovery phase does differ slightly. On first boot after recovery the system will boot into **Directory Services Repair Mode (DSRM)**. It will then perform some cleanup (required to reintroduce the DC back into its forest) and then reboot again to finalise this. Once this second reboot has taken place the DC should come back up OK.

Note: This entire phase is automated - the Microsoft online documentation states that a user must "login" to DSRM using a special username and password and run some steps. For CoBMR AD recoveries this is not necessary and can cause issues. So the DC should be left alone until the second reboot takes place.



8 Appendices

8.1 Storage Space support

Windows **Storage Pools/Spaces** are now supported for Windows Server 2012 R2, 2016, 2019, 2022 and Desktop 10.

However, it is important you keep a note of your Storage Pool disk configuration since this will need to be manually re-configured during the recovery process. The Storage Pool names, physical and virtual disks will be saved, but not the disk mapping. For example, this is a typical Storage Pool configuration dialogue:

CBMR - Storage Pools

Stored Storage Pools (2)

Name	Capacity	Free Space
Pool-A	8.97 GB	6.72 GB
Pool-B	18.97 GB	14.97 GB

To configure, select a Virtual Disk from the table below and right-click to assign target Physical Disks to it.

Stored Virtual Disks (1)

Name	Layout	Provisioning	Capacity	Allocated	Volume
Pool-A-Disk0	Simple	Thin	5.00 GB	768.00 MB	E:

Stored Physical Disks (1)

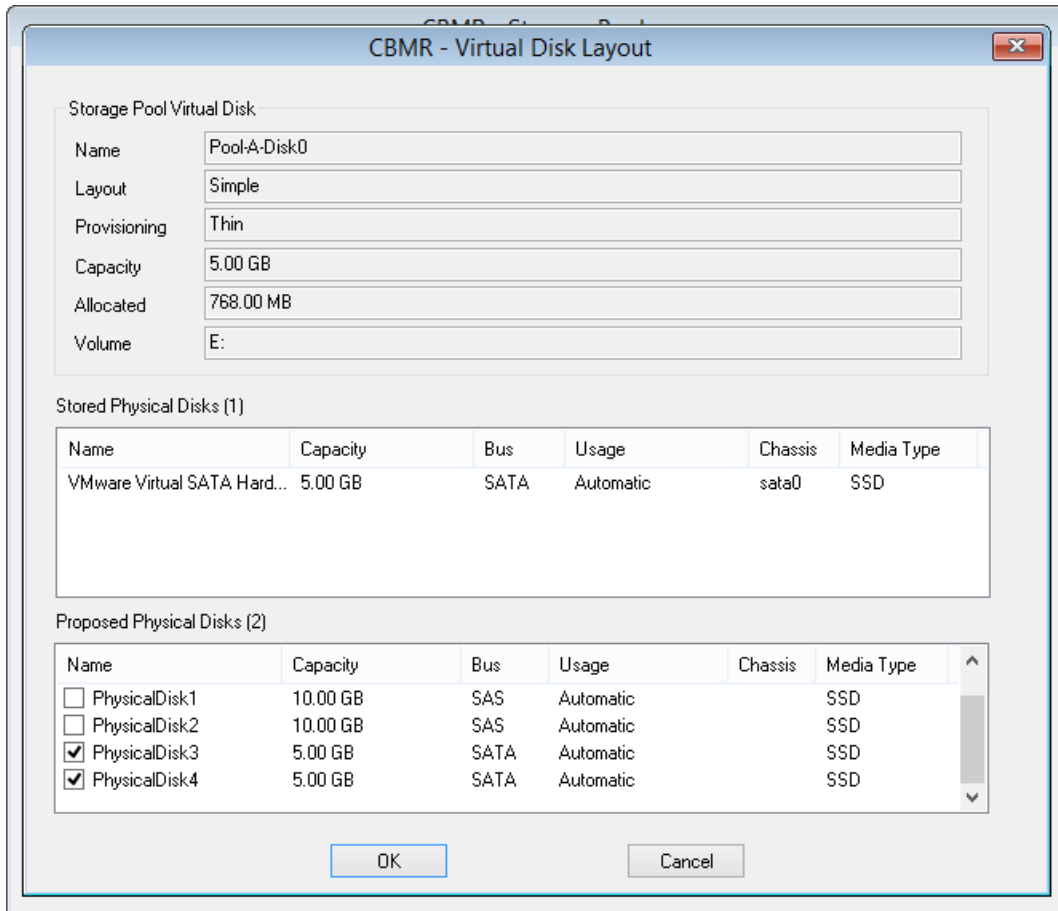
Name	Capacity	Bus	Usage	Chassis	Media Type
VMware Virtual SATA Hard...	5.00 GB	SATA	Automatic	sata0	SSD

Proposed Physical Disks (0)

< Back Next > Cancel

Right-click on a virtual disk to display the physical disk selection dialogue.





Note: nothing special needs to be done during the backup process as long as all the virtual disks in the pools are backed up.

Storage Pools created on iSCSI disks and restored to the same disks will need to be manually attached using the iSCSI initiator tool in the recovery environment **before** beginning the recovery sequence.

Similarly Storage Pools created on USB disks and restored to the same disks must be connected to the target host **before** booting the recovery environment.

Note: For a local USB disk to become part of a Storage Pool, it must be set to 'Not Removable' in the Windows settings Device properties. Otherwise it will not be offered as a candidate disk when setting up the pool.

If recovering a system with Storage Pools to a hypervisor or cloud, any source machine iSCSI or USB disks can be emulated with virtual disks on the target.

Note: Only the WinPE5 DR environment supports the recovery of storage pools at the moment.

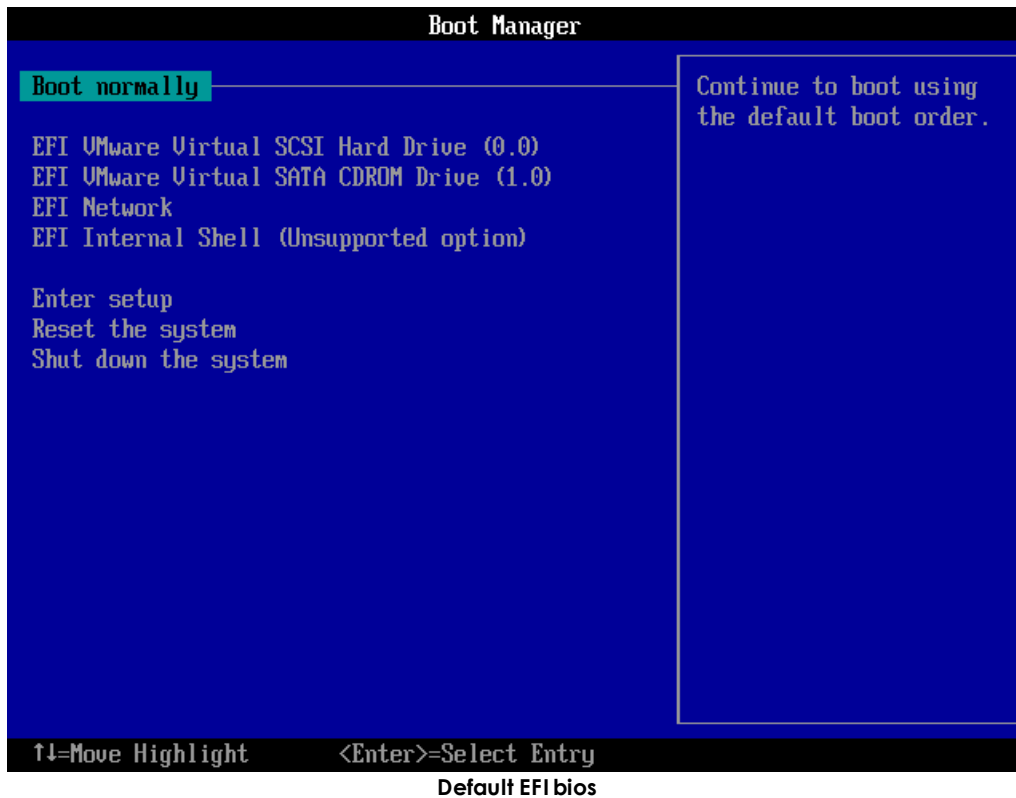
8.2 UEFI and MBR BIOS support

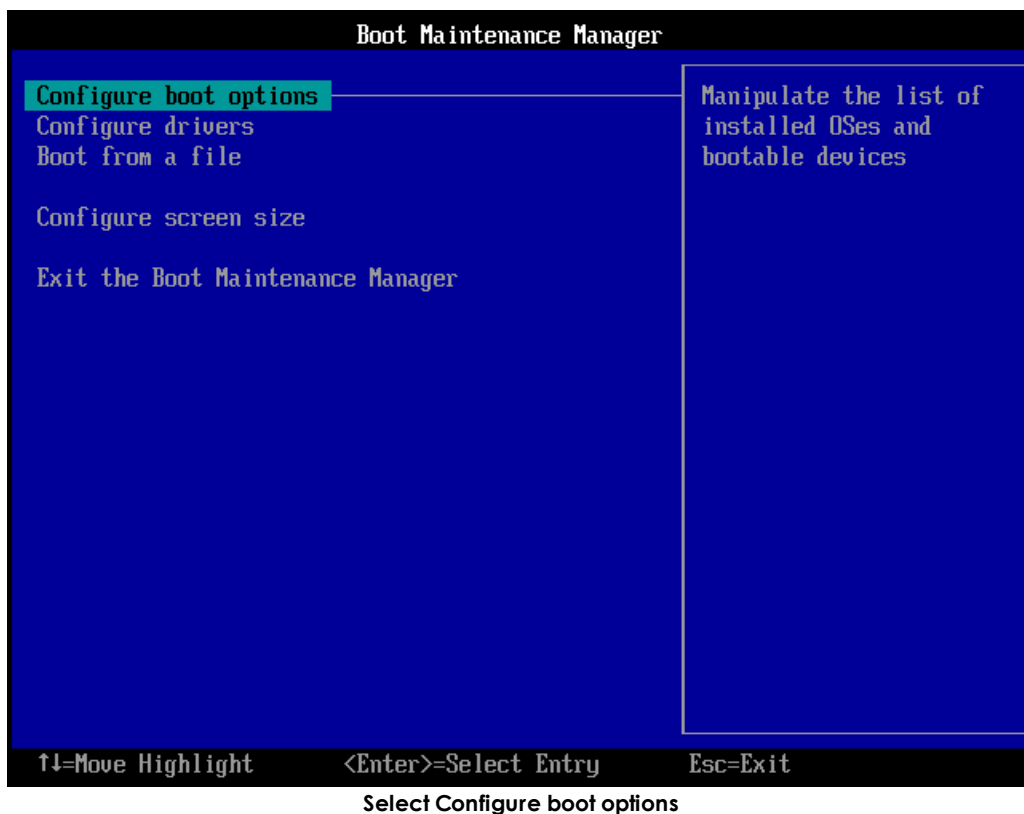
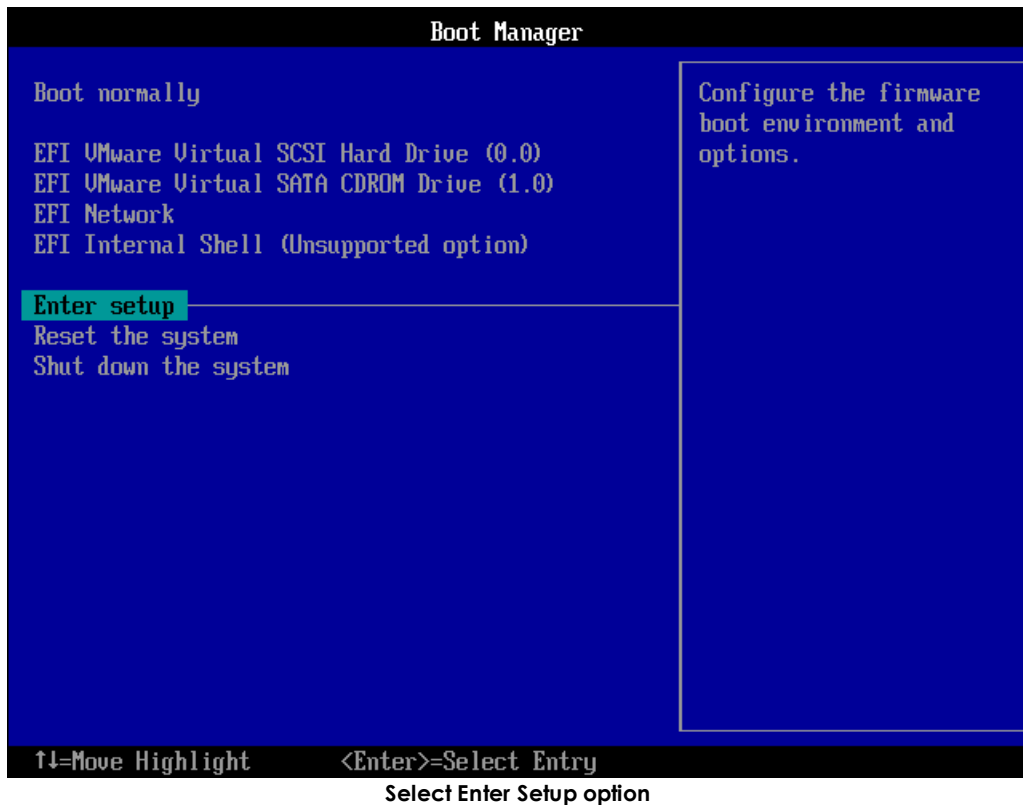
CoBMR has the ability to convert a legacy BIOS boot configuration to a more modern EFI based boot configuration during a Windows clone operation. It does this automatically by creating an extra EFI partition on the detected boot disk and adding the requisite boot files to this partition. Regardless of the original boot disk type it will be converted to GPT format in the clone target system.

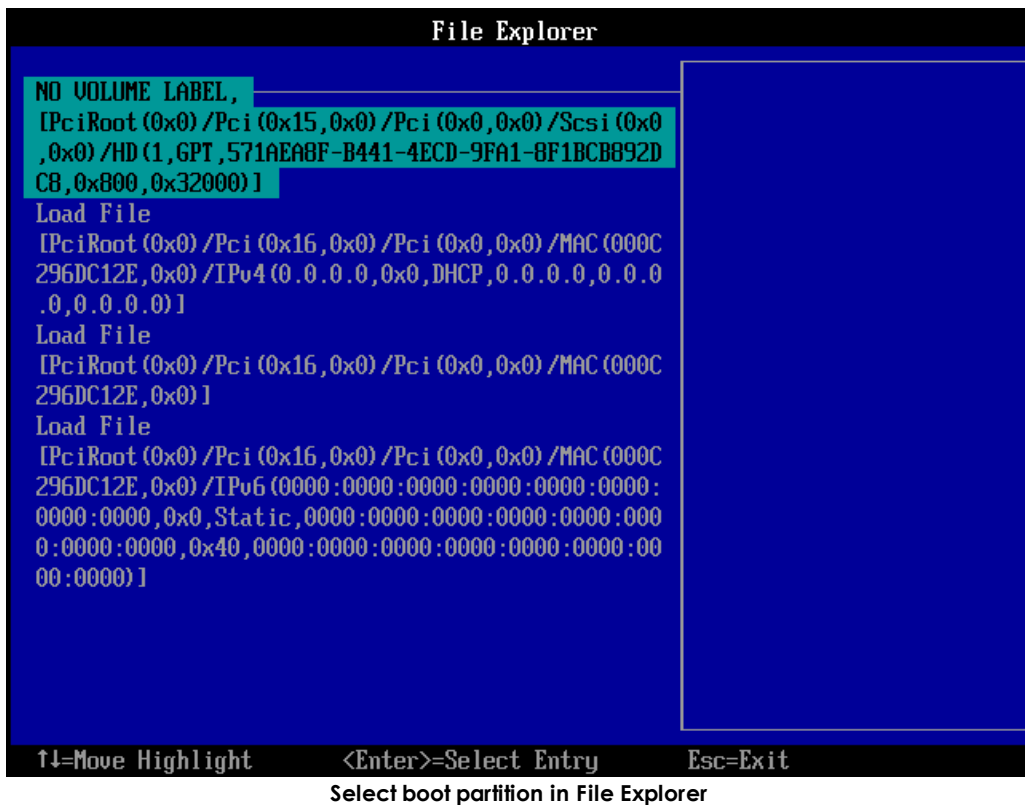
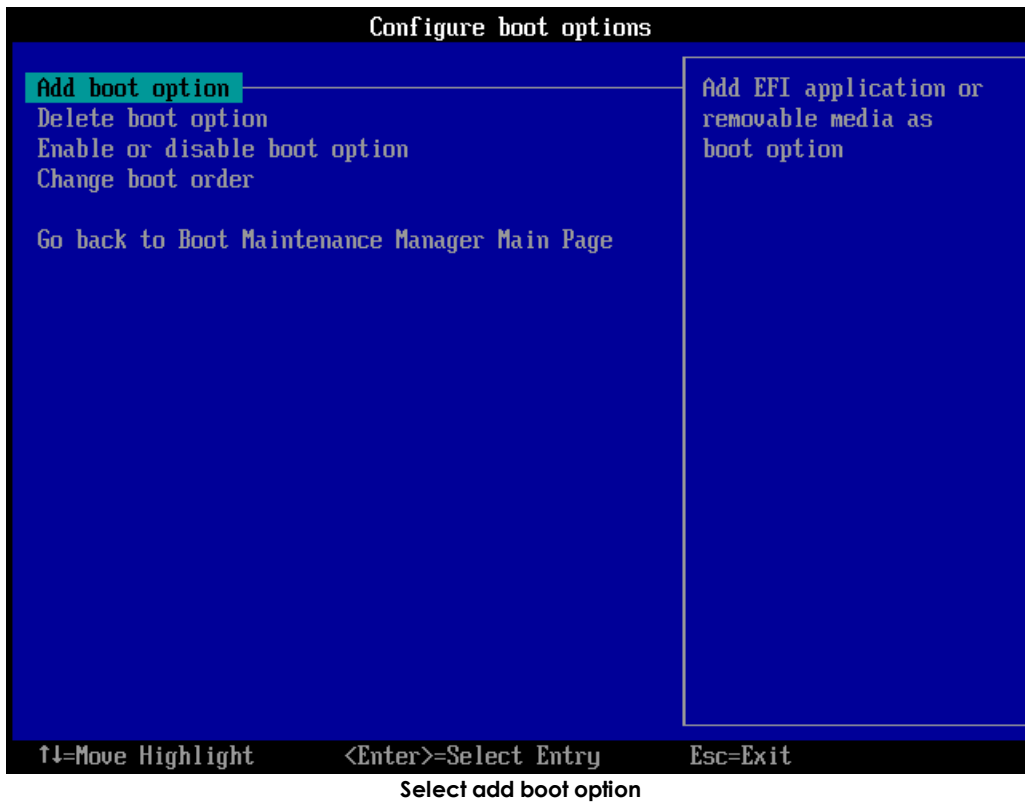


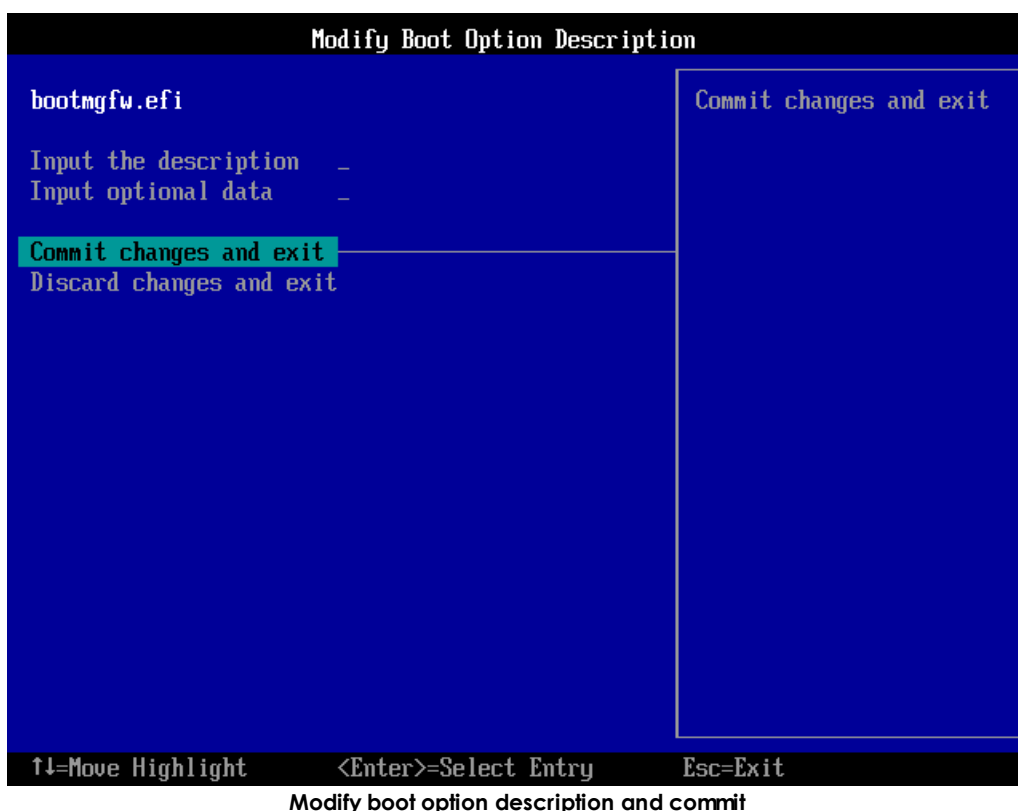
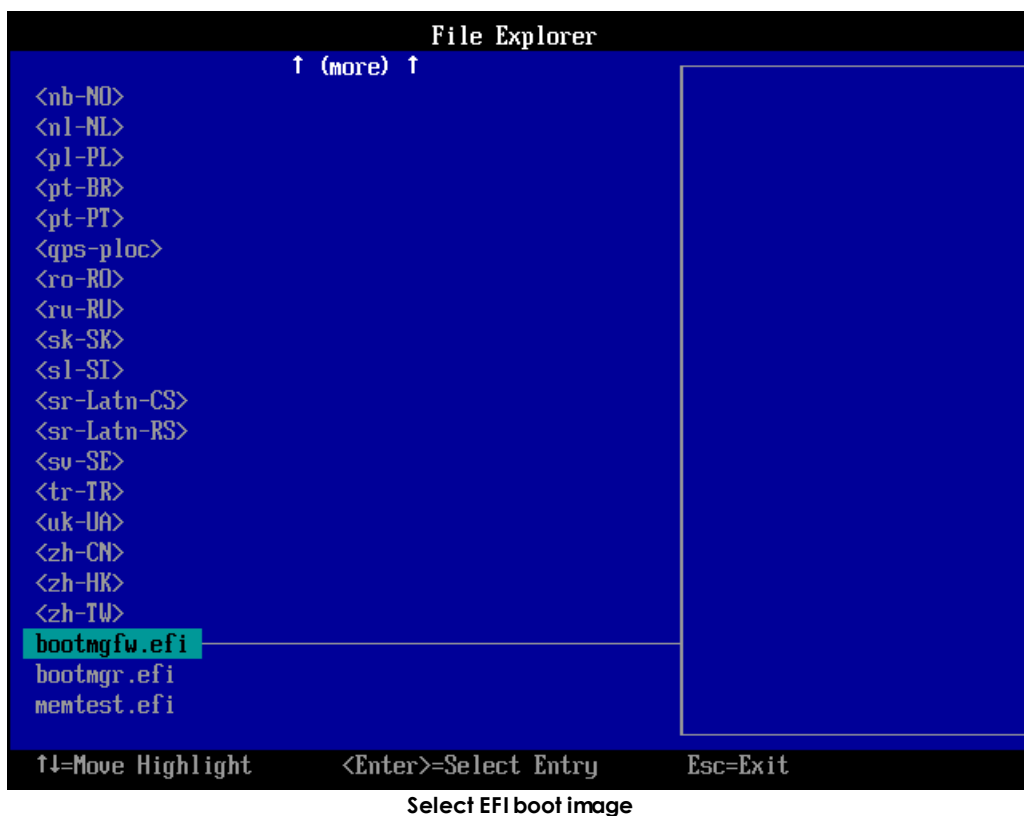
Note: This EFI BIOS conversion feature is only supported on compatible target environments such as physical machines, VMware Workstation™ and VMware vSphere™.

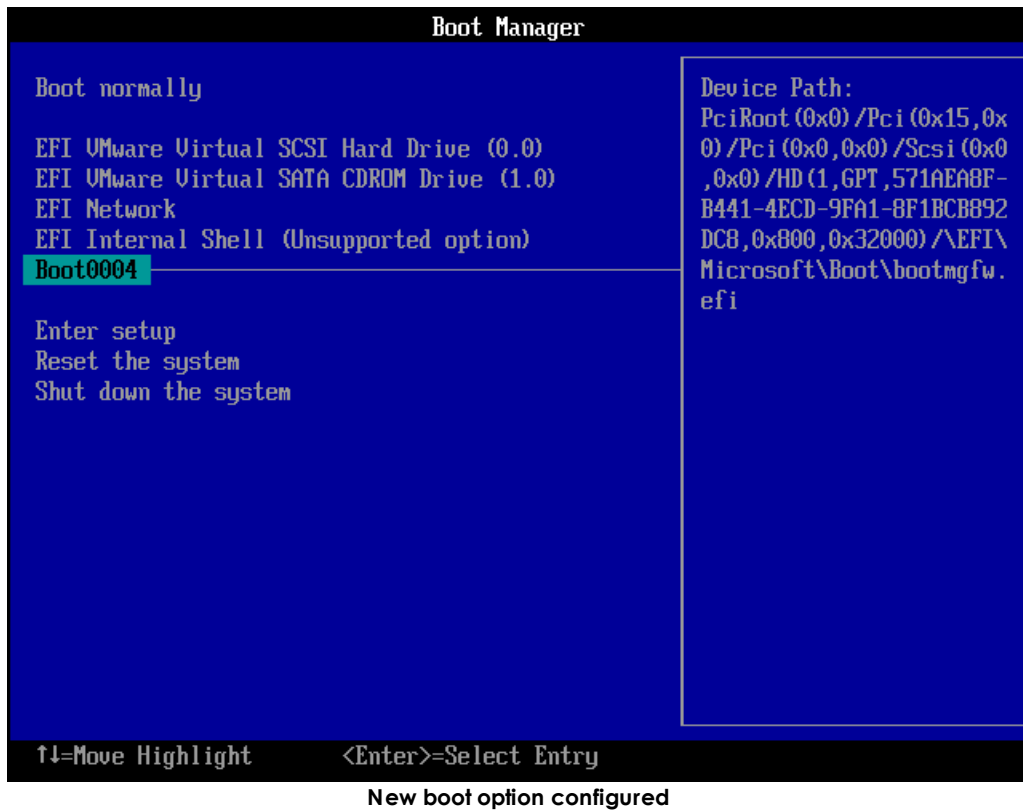
Prior to booting the new EFI clone target manual intervention will be required to configure a new boot option. An example of this obtained from a VMware Workstation™ clone target is shown below. Other virtual environments will be similar.











This feature supports clone source systems with a split boot configuration (i.e. *Boot* and *System* partitions on different disks or different *Boot/System* partitions on the same disk). The split boot configuration will be replicated on the clone target subject to the GPT conversion mentioned above.

This feature also supports source systems configured with a Windows dynamic boot volume (e.g. a dynamic mirror).

It is also possible to clone an EFI based source system to a target configured with a legacy BIOS. In this case any GPT based boot disks will be converted to legacy MBR disks and the EFI partition removed.



9 Cristie Technical Support

If you have any queries or problems concerning your Bare Machine Recovery for Cohesity DataProtect product, please contact Cristie Technical Support. To assist us in helping with your enquiry, make sure you have the following information available for the person dealing with your call:

- CoBMR Version Number
- Installed OS type and version
- Any error message information (if appropriate)
- Description of when the error occurs
- All Cristie log files relating to the source or recovery machine. This is very important to help us provide a quick diagnosis of your problem

Contact Numbers - Cristie Software (UK) Limited

Technical Support	+44 (0) 1453 847 009
Toll-Free US Number	1-866-TEC-CBMR (1-866-832-2267)
Knowledgebase	kb.cristie.com
Forum	forum.cristie.com
Sales Enquiries	sales@cristie.com
Email	support@cristie.com
Web	www.cristie.com

Support Hours

05:00 to 17:00 Eastern Standard Time (EST) Monday to Friday

Out-of-Hours support available to customers with a valid Support Agreement - Severity 1 issues* only

UK Bank Holidays** classed as Out-of-Hours - Severity 1 issues only.

*Severity 1 issues are defined as: a production server failure, cannot perform recovery or actual loss of data occurring.

**For details on dates of UK Bank Holidays, please see www.cristie.com/support/

Cristie Software Ltd. are continually expanding their product range in line with the latest technologies. Please contact the Cristie Sales Office for the latest product range.

