



Recovery Assurance

with Cristie Recovery Software



Bare Machine Recovery for TSM

User Guide

For Windows

May 2015

Version 7.2.2

Cristie Software Ltd.
New Mill
Chestnut Lane
Stroud GL5 3EH
United Kingdom
Tel: +44(0)1453 847000
Fax: +44(0)1453 847001
cbmr@cristie.com

Cristie Data Products GmbH
Nordring 53-55

63843 Niedernberg
Germany
Tel: +49 (0) 60 28/97 95-0
Fax: +49 (0) 60 28/97 95 7-99
cbmr@cristie.de

Cristie Nordic AB
Knarrarnäsgatan 7
164 40 Kista
Sweden
Tel: +46(0)8 718 43 30
cbmr@cristie.se

Copyright © 2008-2015 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 Virtual I/O Server (VIOS) is a trademark of the IBM Corporation.

NetWorker and *Avamar* are trademarks of the EMC Corporation.

Simpana is a trademark of CommVault Inc.

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.

CloneManager® is a registered trademark of Cristie Software Ltd..

Cristie Management Console (CMC), PC-BaX, UBax, Cristie Connect, Cristie Storage Manager (CSM), SDB, ABMR (Bare Machine Recovery for EMC Avamar), NBMR (Bare Machine Recovery for EMC NetWorker), SBMR (Bare Machine Recovery for CommVault Simpana), TBMR (Bare Machine Recovery for TSM), CBMR (Cristie Bare Machine Recovery), Recovery Console (RC) and CRISP (Cristie Recovery ISO Producer) are all trademarks of Cristie Software Ltd.

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

Tel: +44 (0) 1453 847000
Email: cbmr@cristie.com
Website: <http://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	8
4	The TBMR Create Configuration Tool	9
	4.1 Creating the Configuration Information	9
	4.2 Backup of Boot and SystemState Files	11
5	Using a TSM Backup for Disaster Recovery	12
	5.1 Encrypted Backups	12
	5.2 Image Backups	13
	5.3 Backupsets	13
6	Restoring your System	15
	6.1 Booting the WinPE 2 or WinPE 5 DR Console from CD	15
	6.2 WinPE 2 or WinPE 5 Based TBMR Recovery Console	15
	6.2.1 TBMR Recovery Environment Main Menu	17
	6.2.2 Start the automatic Recovery wizard	19
	Restore from Node.....	19
	Specify Certificate File.....	19
	Specify TSM Details and Recovery Date/Time.....	21
	Confirm Volume Layout.....	23
	Select Filespaces To Restore.....	27
	Clone Settings	28
	Dissimilar Hardware.....	28
	Proceed With The Recovery	30
	Restore from Backupset.....	31
	Disk Recovery Sequence.....	33
	Disk Scaling.....	36
	6.2.3 Start the manual Recovery wizard	37
	Locate Configuration.....	37
	Restore From Node.....	41
	Restore From Backupset.....	42
	Create Partition and Volumes.....	43
	Restore Files	46

Make Bootable.....	49
Dissimilar Hardware.....	51
6.2.4 Tools	52
Cristie Network Configurator Tool.....	54
Configure NIC Parameters.....	54
Assign Static or DHCP IP Settings.....	58
Map a Network Drive.....	59
Unmap a Network Drive.....	60
Setup DNS Servers.....	61
Setup Network Identification.....	62
Display/Change MAC Address.....	63
Dissimilar Hardware Wizard.....	64
Load a Driver.....	70
6.2.5 Show a list of log files for viewing	71
6.2.6 Copy log files to removable media or network location	72
6.2.7 Reboot	72
7 Appendices	73
7.1 Windows 8/8.1 Storage Space and 2012/2012R2 Storage Pool Support	73
7.2 UEFI and MBR BIOS support	73
8 Cristie Technical Support	75

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 TSM (TBMR)** and **Disaster Recovery** based upon a tailored WinPE 2 or WinPE 5 recovery module. It is based upon version 7.2.2 of the software.

This document describes the steps required to install, configure and use the Bare Machine Recovery for TSM (TBMR) 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 TSM clients and servers is included in the Readme.

Ensure that the IBM BA Client **Open File Support** is installed and configured correctly. Select either **LVSA** or **VSS** as appropriate. This allows important OS files that are normally held open by the OS to be successfully backed up by TSM. TBMR will not successfully recover the OS without these files.

2.2 Backup Process

TBMR allows you to perform a bare machine recovery of your system direct from a TSM backup.

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

Installation (refer to the TBMR Installation and Licensing Guide)

- Install the TBMR 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 TBMR WinPE 2 or WinPE 5 based DR environment. This only needs to be done once.

Backup system and user data

- Perform regular standard TSM 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 TSM backup of the system and stored the configuration information, Windows WinPE 2 or WinPE 5 mode DR enables you to restore your system to the state at the last TSM backup.

The TBMR recovery console must be created first by using the Cristie Recovery ISO Producer (CRISP) tool. The output from this tool is a bootable WinPE 2 or WinPE 5 ISO which can be either burnt to physical CD/DVD media or used directly in a virtual environment.

If your machine supports bootable CDs, this is the most convenient way to boot the DR module. If the system does not support bootable CDs, you can boot from the network. Contact Cristie for details on how to set this up.

Windows WinPE 2 or WinPE 5 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*

The WinPE 2 or WinPE 5 recovery process has five main steps:

1. *Load Configuration data*
2. *Rebuild storage devices (hard disks)*
3. *Restore OS files from a TSM backup*
4. *Dissimilar Hardware and inject new drivers (if necessary)*
5. *Boot into Windows*

3 Create The Bootable Recovery Environment

The supplied CRISP tool is used to create the TBMR recovery environment. This environment is based upon a customised version of Microsoft's WinPE version 2 (WinPE2) or 5 (WinPE5).

The WinPE2 version is 32-bit based and the WinPE5 is 64-bit based. Cristie Software Ltd. recommend using the WinPE5 based environment if possible. This is based upon Windows 8.1/2012R2 and is more likely to be compatible with most modern hardware. Use the WinPE5 version for Windows 2008R2 and later. Use the WinPE2 version for legacy hardware (particularly when using Windows 2003).

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 WinPE2 and WinPE5 Filesets for TBMR 7.2.2. The fileset should be installed alongside the CRISP on the same host.

A full discussion of how to install and run CRISP is contained in the separate [CRISP User Guide](#). Note that the 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 a bootable WinPE 2 or WinPE 5 ISO file which can then be burnt to physical media (CD or DVD) or mounted directly in a VM environment. This media is then booted on the target machine to manage the recovery operation.

4 The TBMR Create Configuration Tool

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

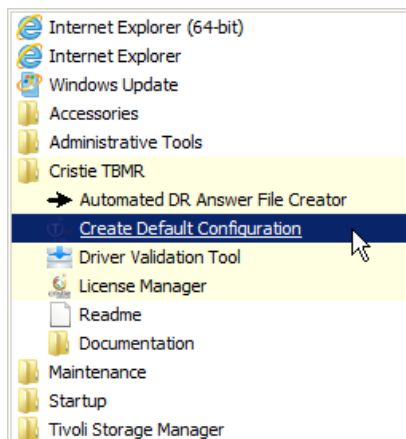
The Cristie tool that provides this function is called **TBMRCfg.exe** which is located in the TBMR installation folder (normally **Program Files\Cristie\TBMR**). This is a command line only tool which is licensed for use for a 30 initial day trial period. A full license is required to use the program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

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.

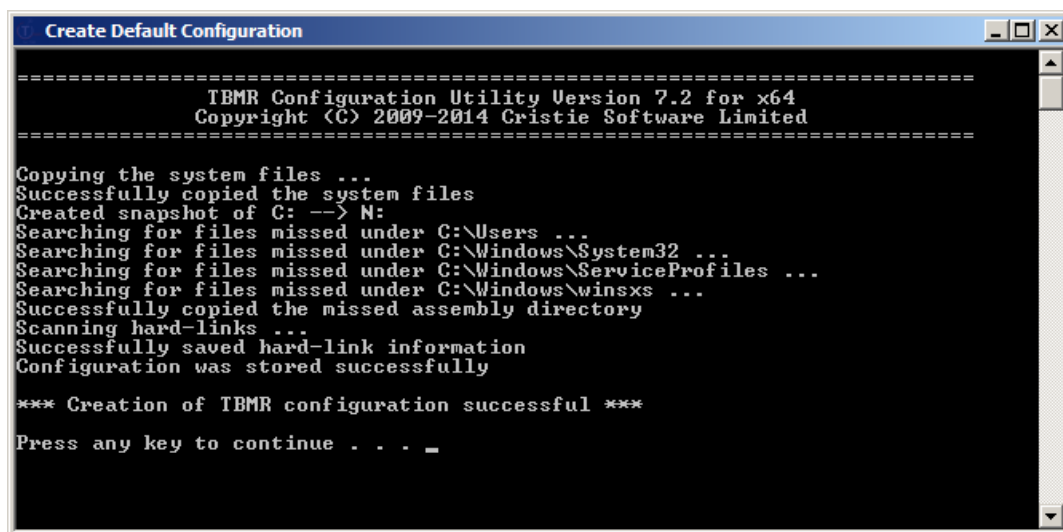
The next sections discuss this process in more detail.

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 TBMR. Note however that an initial configuration is created during the TBMR installation process.

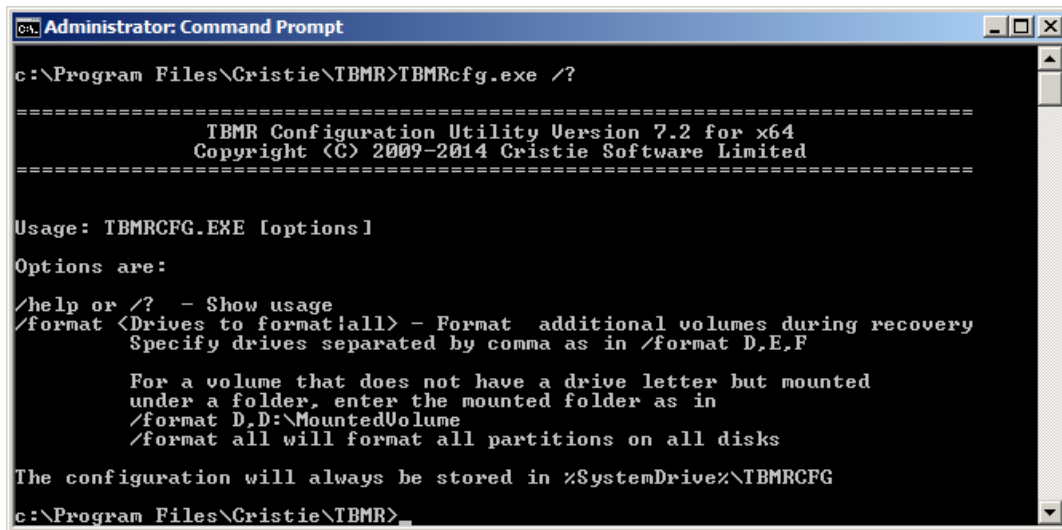


This will create a new configuration using the default settings.



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 TBMR is installed.

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



```

Administrator: Command Prompt

c:\Program Files\Cristie\TBMR>TBMRCfg.exe /?

=====
      TBMR Configuration Utility Version 7.2 for x64
      Copyright (C) 2009-2014 Cristie Software Limited
=====

Usage: TBMRCFG.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

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

c:\Program Files\Cristie\TBMR>
  
```

The command line options are very simple:

/help or **/?**

shows **TBMRCfg** 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 WinPE 2 or WinPE 5 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:

```
TBMRCfg.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:

```
TBMRCfg.exe /format all
```

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

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

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

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

TBMRCfg stores the configuration in `%SystemDrive%\TBMRCFG` folder (`%SystemDrive%` is the drive associated with the Windows folder, usually `C:\`). This location cannot be changed.

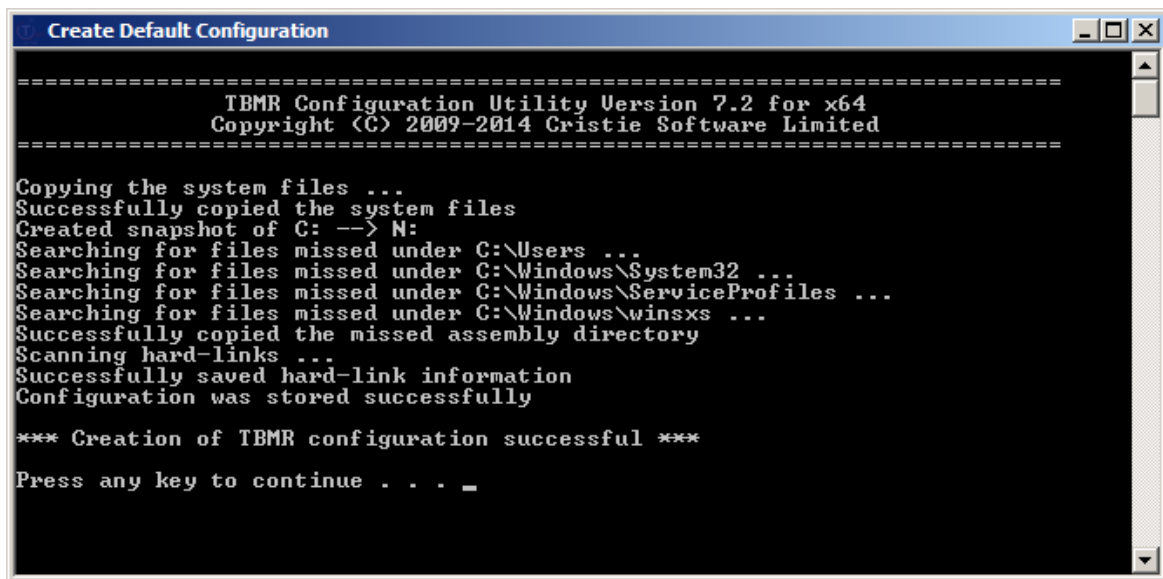
Note: it is important to remember that the TBMR configuration must be created before the BA

Client backup is made. Cristie suggests that this is done by creating a job to run on the TSM Scheduler containing a script that calls the TBMR Cfg.exe program installed in the TBMR installation folder.

4.2 Backup of Boot and SystemState Files

On all Windows OS's, files additional to the standard TSM backup dataset must be copied and saved. These include boot files and SystemState objects which are not normally backed up by the IBM BA 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 TBMR Cfg runs, it invokes VSS to take a snapshot copy of these extra files:



```
=====
      TBMR Configuration Utility Version 7.2 for x64
      Copyright (C) 2009-2014 Cristie Software Limited
=====

Copying the system files ...
Successfully copied the system files
Created snapshot of C: --> N:
Searching for files missed under C:\Users ...
Searching for files missed under C:\Windows\System32 ...
Searching for files missed under C:\Windows\ServiceProfiles ...
Searching for files missed under C:\Windows\winsxs ...
Successfully copied the missed assembly directory
Scanning hard-links ...
Successfully saved hard-link information
Configuration was stored successfully

*** Creation of TBMR configuration successful ***

Press any key to continue . . . _
```

5 Using a TSM Backup for Disaster Recovery

TBMR allows a previously created TSM backup or backupset to be used as a DR backup.

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

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

5.1 Encrypted Backups

TBMR supports encrypted TSM backups. This can be enabled in TSM by adding the line:

```
INCLUDE.ENCRYPT "*" : \... \*
```

to the dsm.opt file. TBMR works by creating the system configuration into the folder TBMRCFG. So the line above would mean that when the TSM backup is created, the TBMRCFG folder is also encrypted. This is not a problem, but would mean that you will be prompted for the password during the recovery. If you wish to avoid this prompt, add this additional line to dsm.opt after the line above:

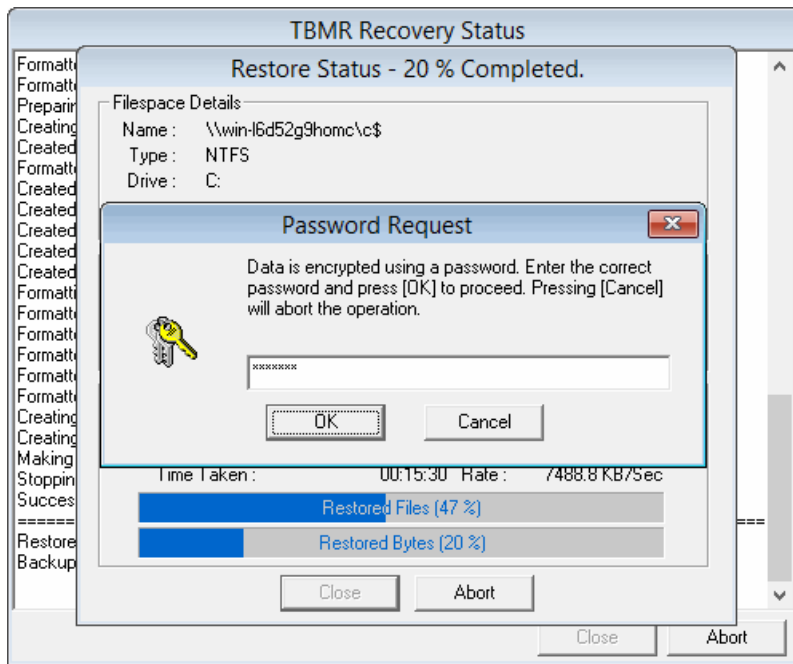
```
EXCLUDE.ENCRYPT "*" : \TBMRCFG \*
```

You can also choose to always prompt for the encryption key password, or have it stored locally. You will be prompted for the encryption key as follows:



You should also select the appropriate encryption algorithm for your backup.

If the folder containing the TBMR configuration has been encrypted, then during the recovery you will be prompted for the password:



If the configuration folder has been excluded from the encryption (as described above), you will be prompted for the password during the Restore Files phase of the DR.

Please enter the same password you entered during the backup.

Note 1: if you have elected to have the password stored locally (via the BA Client Preferences menu) and the TBMR configuration has been created post this change, then you will not be prompted for the password during the recovery. You may also need to perform a 'dummy' backup first to get the password stored locally before generating the TBMR configuration.

Note 2: Cristie recommends using a single password for the entire encrypted backup. With TSM it is possible to backup parts of the system with a different password. This could lead to confusion during the recovery and is discouraged.

5.2 Image Backups

TBMR supports TSM backups of the form incremental, image and backupsets. However, for image backups, it is essential that in addition to the image backup, an incremental backup of the TBMRCFG folder is made to the same Node.

This is because it is not possible to retrieve the configuration details from an image backup.

Note: if this extra incremental backup is not made, then it will not be possible to perform a DR. It is also not possible to restore an image backup to a smaller disk partition.

5.3 Backupsets

TBMR now supports DR recovery from TSM backupsets. At the moment, TBMR only supports **online** backupsets (ie. those maintained in a Node on a TSM server). Typically a backupset is created with a **dsmadm** command such as:

```
Generate Backupset <Nodename> <Prefix> Description="This is a backupset test"  
Retention=Nolimit Wait=Yes Datatype=File TOC=Yes DevClass=File
```

Where <Nodename> is the name of the node on the TSM server, <Prefix> is a short prefix to add to the backupset name.

Note that a backupset is created from a backup already present in the specified node. If this backup does not already contain a backup of the TBMRCFG folder generated by the TBMRCfg program, it will not be possible to recover the system from the backupset.

It is essential to specify TOC=Yes. **TBMR cannot recover a backupset created without a TOC (Table of Contents).**

6 Restoring your System

This section discusses the steps required to run a recover sequence using the TBMR Recovery Console. The console is booted from the media created by CRISP in conjunction with the CRISP WinPE2 and WinPE5 Filesets for TBMR 7.2.2 (see [Create the bootable cloning environment](#) for further details).

The WinPE 2 or WinPE 5 based recovery environment is booted on the **target** system. This could be the original or a dissimilar system.

A typical TBMR 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 TBMR WinPE 2 or WinPE 5 based recovery environment. This only needs to be done once.
2. Boot the TBMR WinPE 2 or WinPE 5 recovery environment on the **target** system.
3. Run a restore sequence from the recovery environment on the **target** system using the TSM 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.

6.1 Booting the WinPE 2 or WinPE 5 DR Console from CD

Insert the bootable TBMR WinPE 2 or WinPE 5 DR CD/DVD-ROM 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 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 creation stage. If the prompt is disabled then the DR ISO image will always be booted 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, WinPE 2 or WinPE 5 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; 32-bit for WinPE2 and 64-bit for WinPE5.

6.2 WinPE 2 or WinPE 5 Based TBMR Recovery Console

When the **WinPE 2 or WinPE 5 TBMR Console** is booted, a Windows installation-like boot procedure is started.

During the boot process, WinPE 2 or WinPE 5 drivers for your **Plug and Play** devices will be loaded - in particular the **Mass Storage** devices and **Network Adapters**.

When the WinPE 2 or WinPE 5 system has fully booted, it is possible to remove the CD/DVD if you wish.

Note: the DR Console will automatically reboot 72 hours after starting. This is an operating limitation of the Microsoft Windows WinPE 2 or WinPE 5 environment.



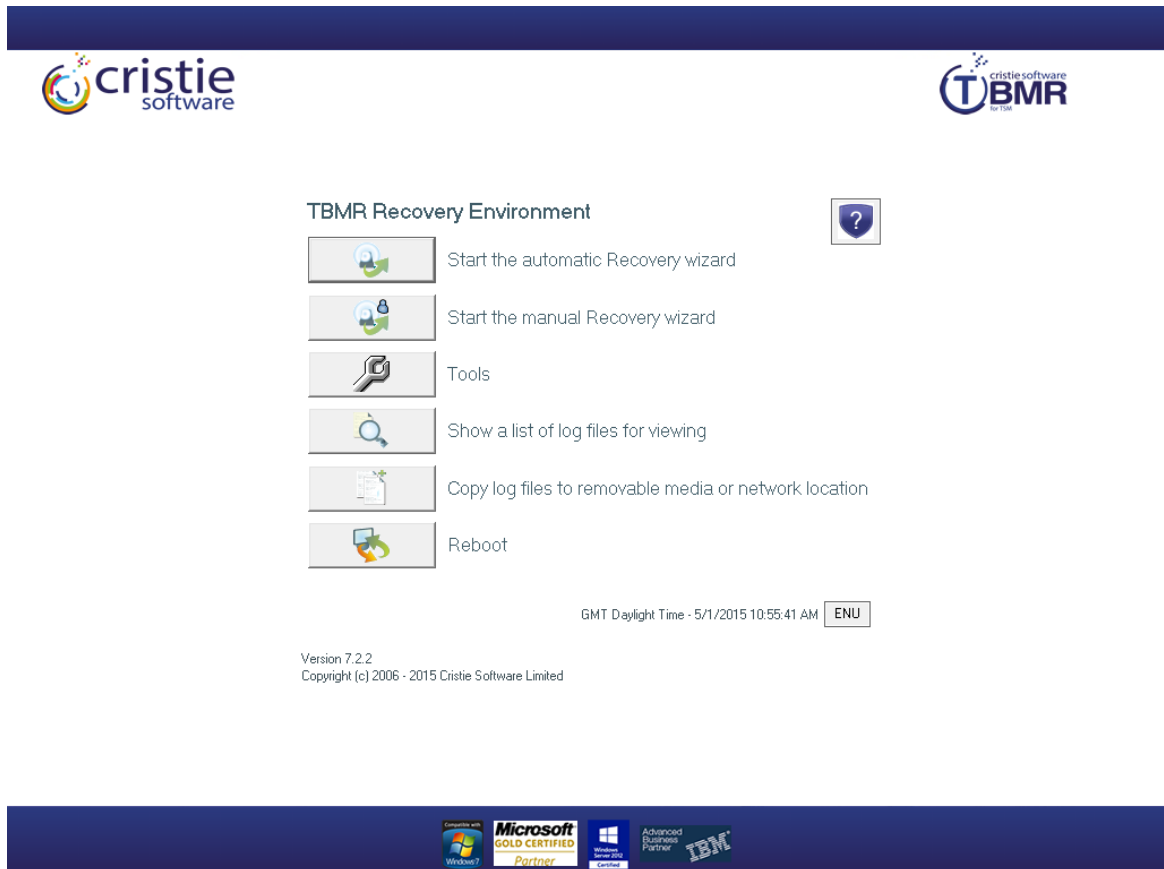
Please wait while your PnP devices are loaded ...



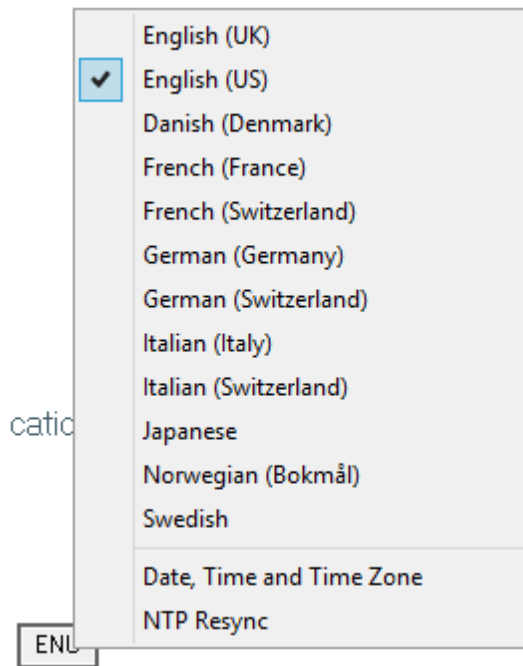
When this sequence completes, the **TBMR Recovery Console** will be shown.

6.2.1 TBMR Recovery Environment Main Menu

When you boot the **WinPE 2 or WinPE 5** DR environment (the WinPE2 and WinPE5 versions are very similar), you will see the **TBMR Recovery Console** Main Menu as below:

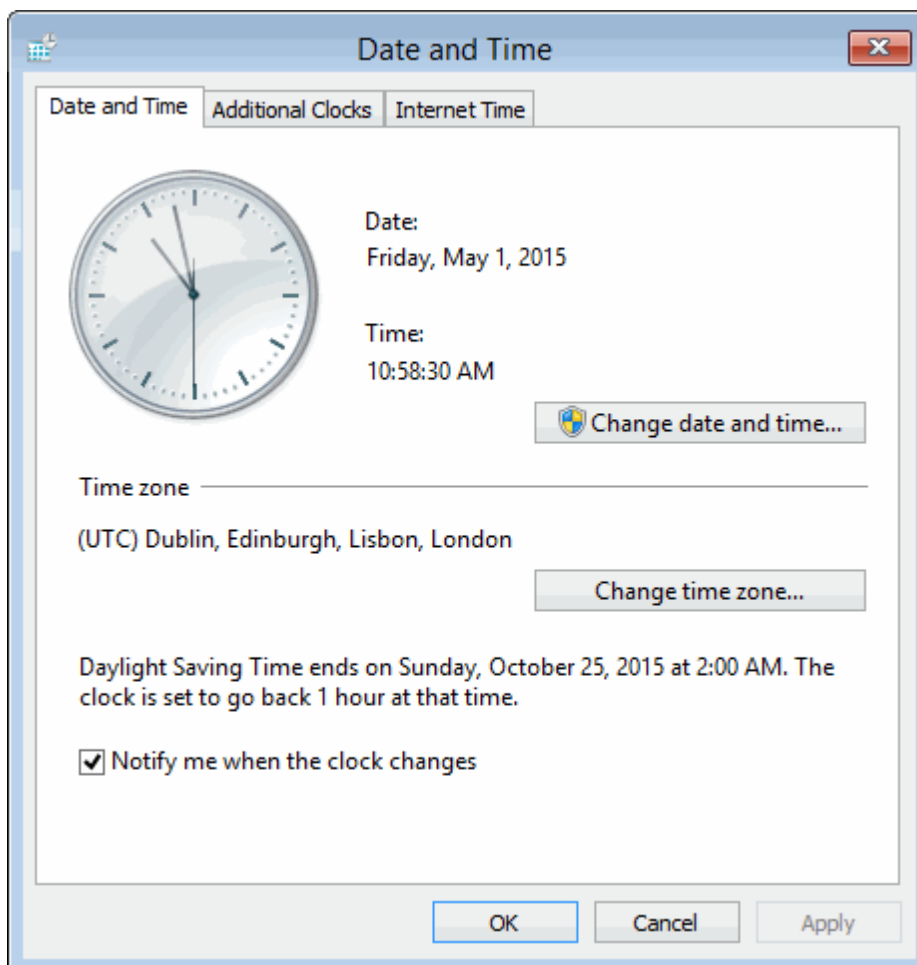


You may configure the format of the displayed date/time and the keyboard layout, by pressing the locale **ENU** icon. Note this icon will be shown according to the locale of the host system used to create the ISO using the CRISP utility so it may not match the version shown here. So if, for example, the ISO 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.

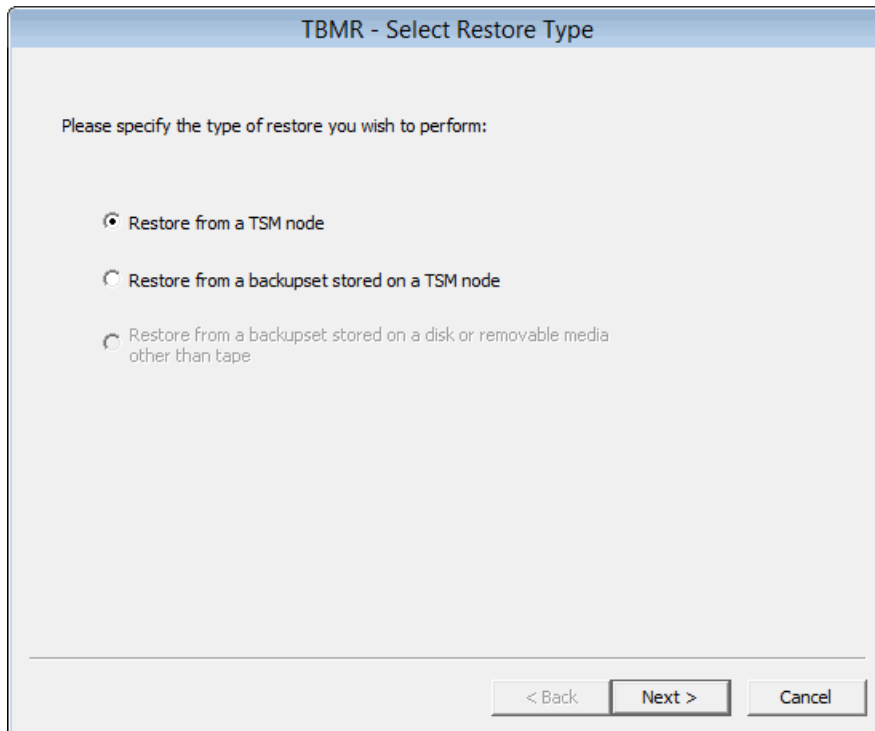


Note: the Additional Clocks and Internet Time tabs are operational. In fact it is possible to synchronise the system time with an NTP time server if required.

Select the Help button  to show online help for the recovery environment.

6.2.2 Start the automatic Recovery wizard

Select the **Start the automatic Recovery wizard** option to commence an automatic DR sequence.



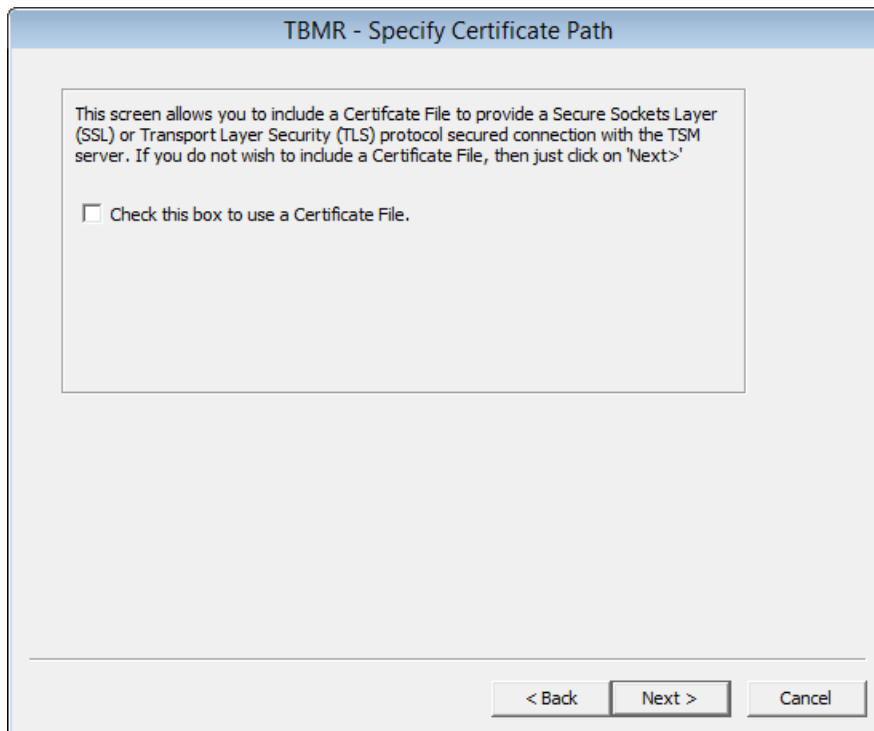
At the moment only restoring from a TSM node or an online backupset is supported. A future release will support restoring from a backupset stored on a disk or removable media. Make your choice and press **Next>** to continue.

6.2.2.1 Restore from Node

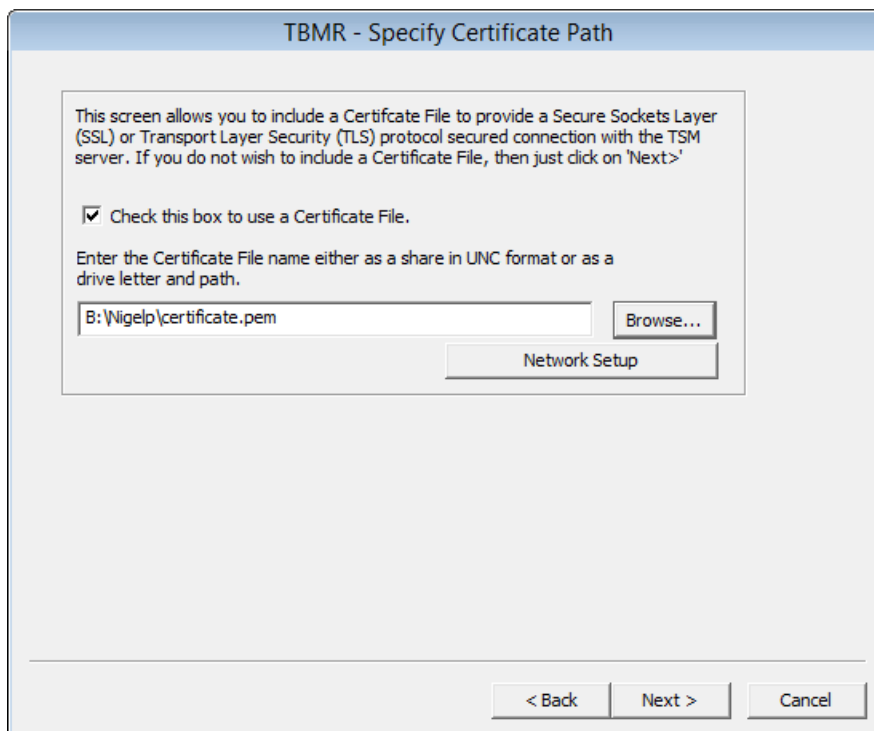
If you selected **Restore from a Node**, select **Next>**. This will then display the **Enter TSM server details** as shown in the next section.

Specify Certificate File

The first step of the automatic Node restore allows a **Secure Sockets Layer (SSL)** or **Transport Layer Security (TLS)** certificate to be provided to the TSM server. If you do not require to add an SSL or TLS certificate click **Next >** to continue directly to the next step.



To add a certificate, click the check box to open up a browser window. Then enter the full path or browse to the location of the certificate file.



Use the [Network Setup](#) button to connect a network share if required (as in the example). Click [Next >](#) to continue to the next step.

Specify TSM Details and Recovery Date/Time

The next step of the automatic recovery identifies the location of the **TSM Server** and **Node** used to back up the Client.

TBMR - TSM Settings

Please enter the TSM Server and Client details below and select [Next] to continue.

TSM Server Details

Server Address : 10.10.11.98 Port : 1500

Backupset Location : Browse

TSM Client Details

Node Name : NIGELPTBMR

User Id* :

* Leave blank if you wish to use the default (i.e. the same as the Node Name)

Password : *****

☐ Point-in-time (PIT) restore

Tuesday , November 18, 2014 2:15:28 PM

< Back Next > Cancel

Note: You may use an alternative to the normal Node credentials (such as the Administrator account) to access the account. In this case enter the username of the alternative in the User Id field and the corresponding password.

Selecting the **Point-in-time** (PIT) restore mode will allow the system to be recovered from the most recent backup before the specified date and time. This means the version of any file restored will be earlier than the specified date and time. Selecting the down-arrow in the calendar control will bring up a calendar:

TBMR - TSM Settings

Please enter the TSM Server and Client details below and select [Next] to continue.

TSM Server Details

Server Address : Port :

Backupset Location :

TSM Client Details

Node Name :

User Id* :

* Leave blank if you wish to use the default (i.e. the same as the Node Name)

Password :

☒ Point-in-time (PIT) restore

Friday , May 1, 2015 11:08:57 AM

May 2015

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Today: 5/1/2015

< Back Next > Cancel

This can be used to scroll the months/years backwards and forwards as necessary.

Note: a future date will result in the latest backup being recovered.

If PIT mode is not selected then, by default, the latest file versions will be restored.

Select **Next>** to continue.

If the backup including the TBMR configuration folder **TBMRCFG** is encrypted, a prompt for the encryption password will be displayed if not held locally:

TBMR Recovery Status

Restore Status - 20 % Completed.

Filespace Details

Name : \\win-l6d52g9hmc\c\$

Type : NTFS

Drive : C:

Password Request

Data is encrypted using a password. Enter the correct password and press [OK] to proceed. Pressing [Cancel] will abort the operation.

OK Cancel

Time Taken : 00:15:30 Rate : 7488.8 KB/Sec

Restored Files (47 %)

Restored Bytes (20 %)

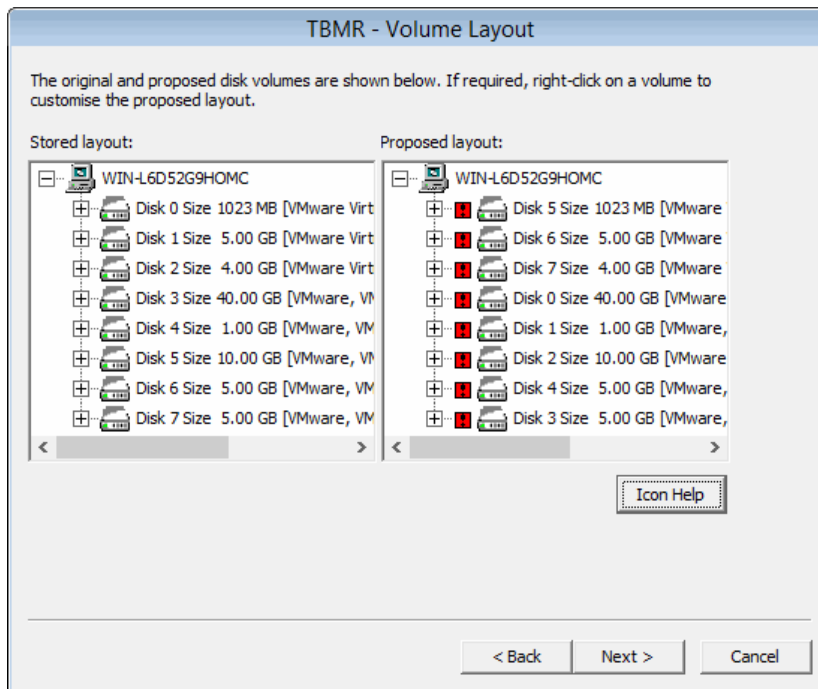
Close Abort

Enter the password used during the backup. Press **OK** to proceed. At this point the Node will be accessed on the specified server and the machine configuration extracted.

Note: TBMR assumes that TCP/IP is the communication method used between the Client and the Server. Other TSM communication methods are not supported.

Confirm Volume Layout

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



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.

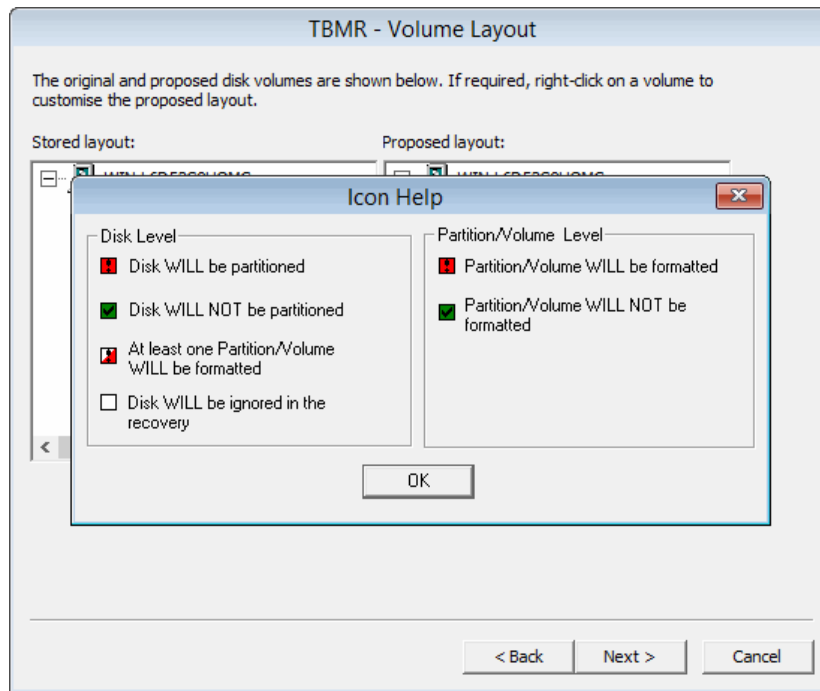
A green tick box ☒ next to a disk signifies that the disk and its underlying partitions will be left intact. Placed next to a partition/volume means that the corresponding partition/volume **WILL NOT** be partitioned.

A red 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 red/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.

Click on the **Icon Help** button to display a summary of this:

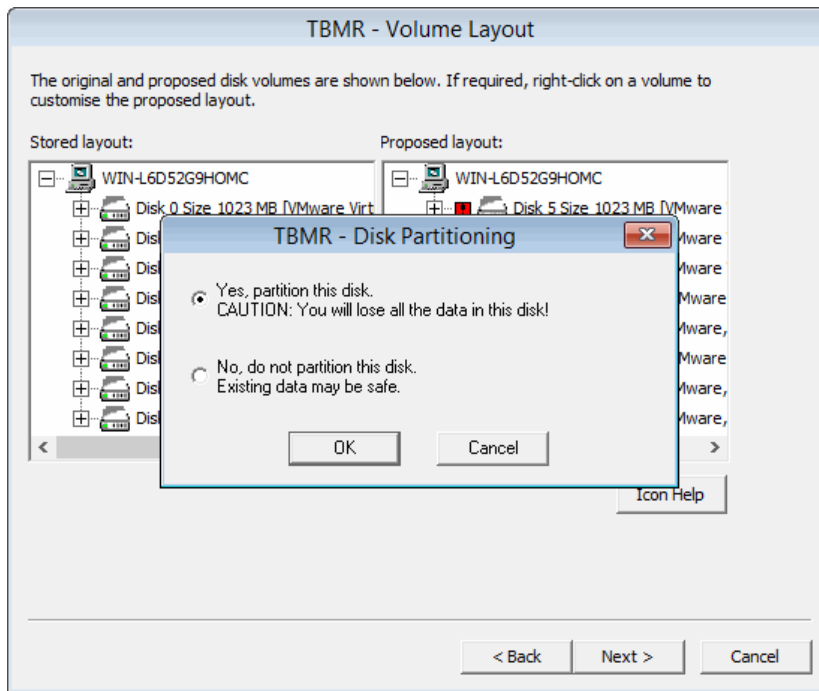


When the recovery is to the original system, the contents of both panels will look similar if the number of disks is the same. Possibly the disk sizes will be different.

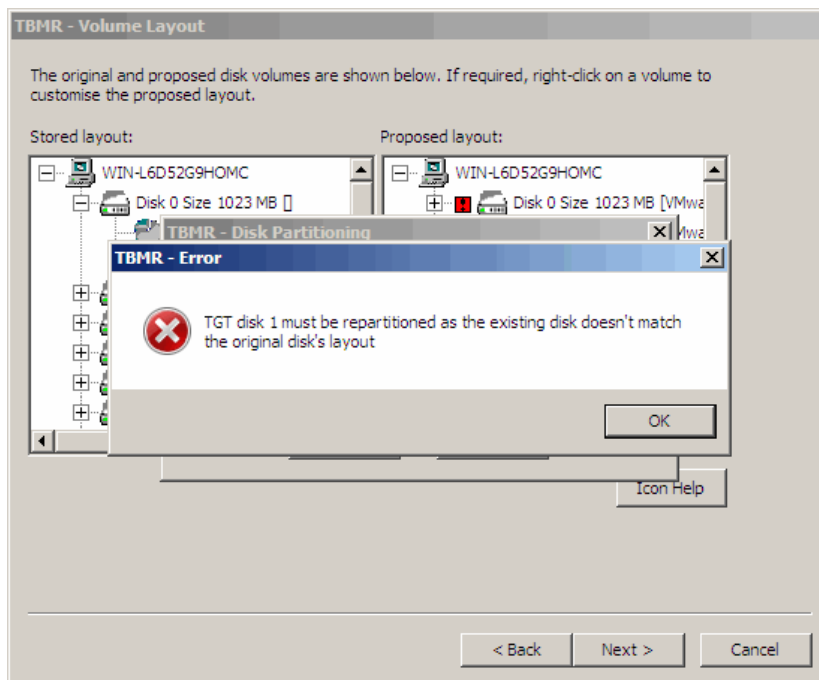
When performing a recovery to a dissimilar system, the disk mapping can be much more complex. Some of the criteria used to judge the disk mapping are:

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

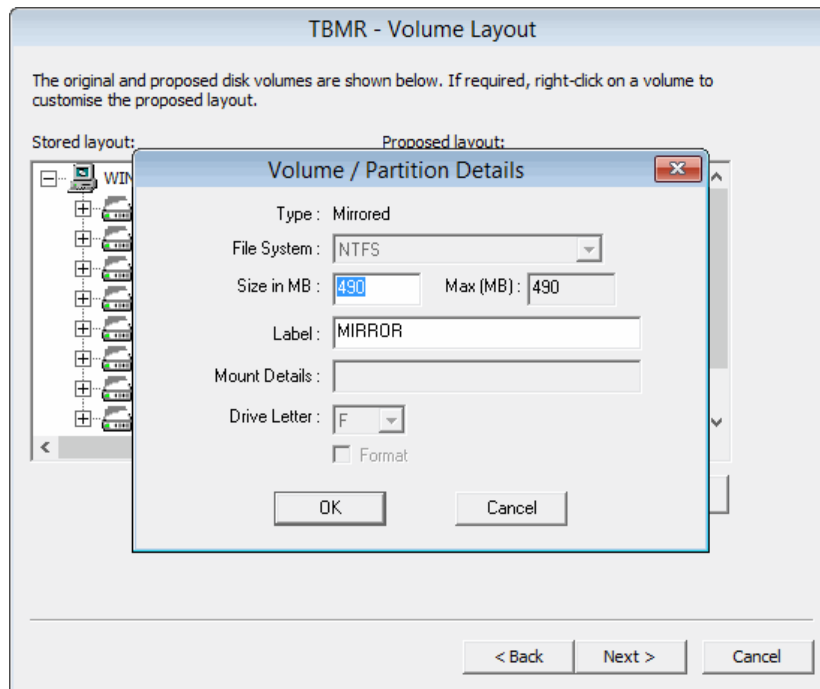
You may right-click on any disk shown in the right-hand panel to select whether the disk will be partitioned or not.




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



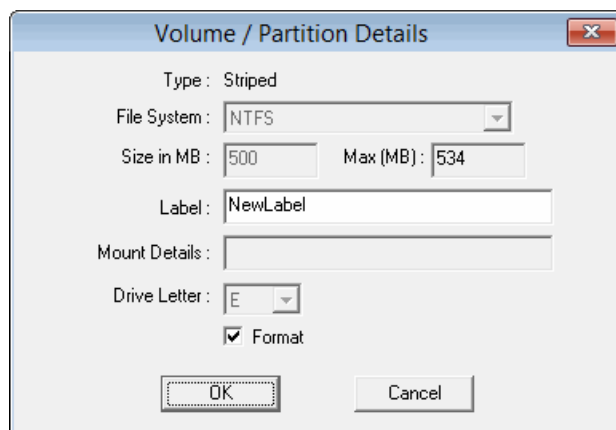
You may also right-click on a partition to allow you to selectively modify the partition parameters or remove it altogether.



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

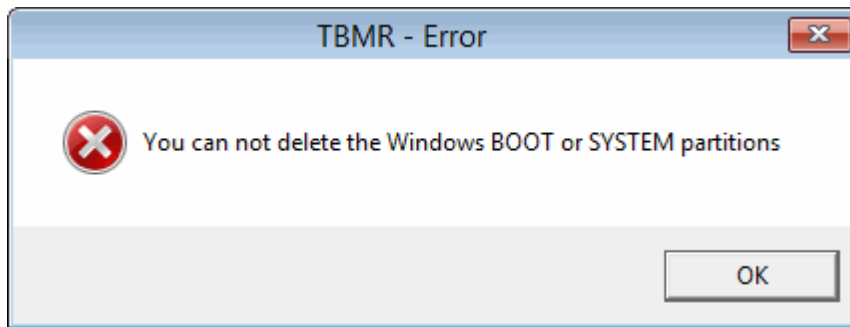
- size in MB (only if disk is shown with a )
- label
- format (yes/no)

The screenshot below shows an example:



Select **Delete** to remove the partition completely (only if disk is shown with a )

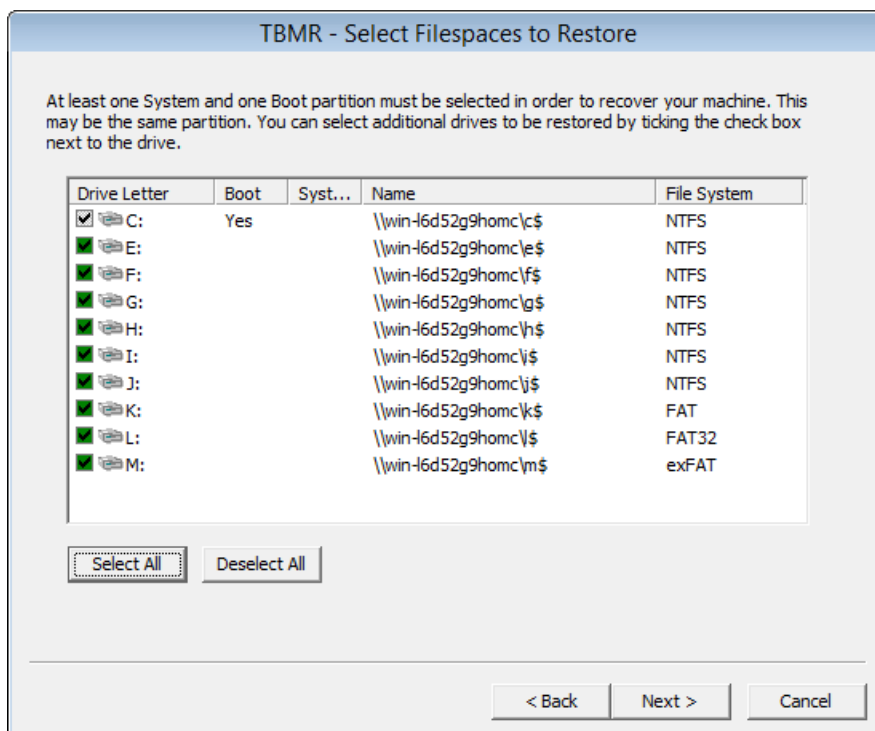
If you attempt to either not format or delete a Windows system partition, an error such as this will be displayed:



At this stage, nothing has happened to the disks. Press [Next>](#) to continue with the recovery.

Select Filespaces To Restore

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

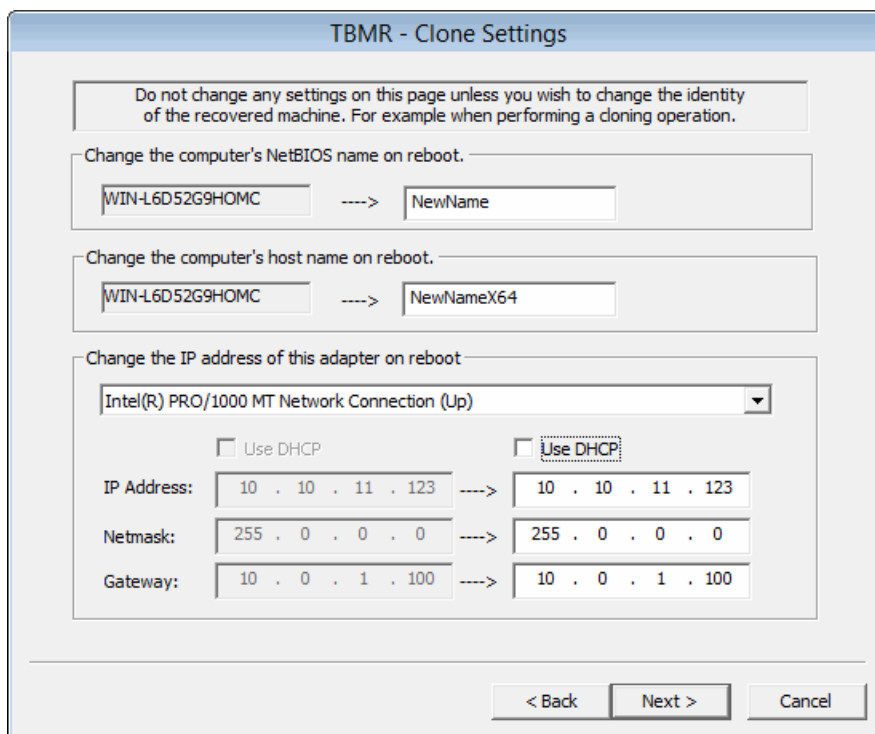


Note: the system and boot partitions (even if on different partitions) will always be restored by default.

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

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 dialog box is titled "TBMR - Clone Settings". It contains a warning message: "Do not change any settings on this page unless you wish to change the identity of the recovered machine. For example when performing a cloning operation." Below this, there are three sections for configuration:

- Change the computer's NetBIOS name on reboot.** This section has a text box with "WIN-L6D52G9HOMC" and a "---->" button, followed by a text box labeled "NewName".
- Change the computer's host name on reboot.** This section has a text box with "WIN-L6D52G9HOMC" and a "---->" button, followed by a text box labeled "NewNameX64".
- Change the IP address of this adapter on reboot.** This section has a dropdown menu showing "Intel(R) PRO/1000 MT Network Connection (Up)". Below the dropdown are two columns of settings, each with a "Use DHCP" checkbox and a "---->" button. The first column has:
 - IP Address: 10 . 10 . 11 . 123
 - Netmask: 255 . 0 . 0 . 0
 - Gateway: 10 . 0 . 1 . 100
 The second column has:
 - IP Address: 10 . 10 . 11 . 123
 - Netmask: 255 . 0 . 0 . 0
 - Gateway: 10 . 0 . 1 . 100

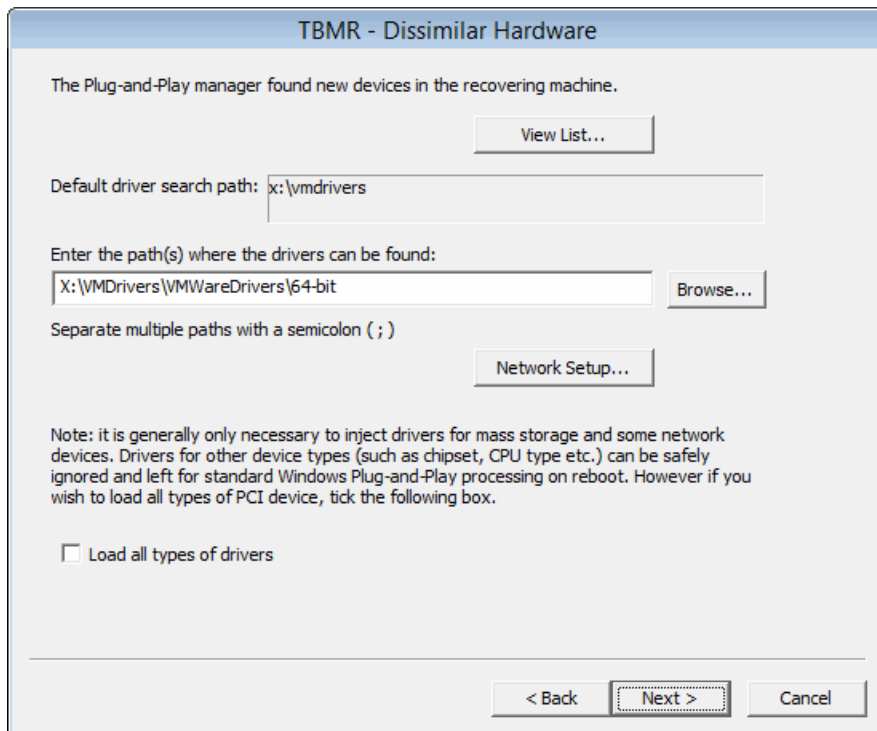
At the bottom of the dialog box are three buttons: "< Back", "Next >", and "Cancel".

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

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.

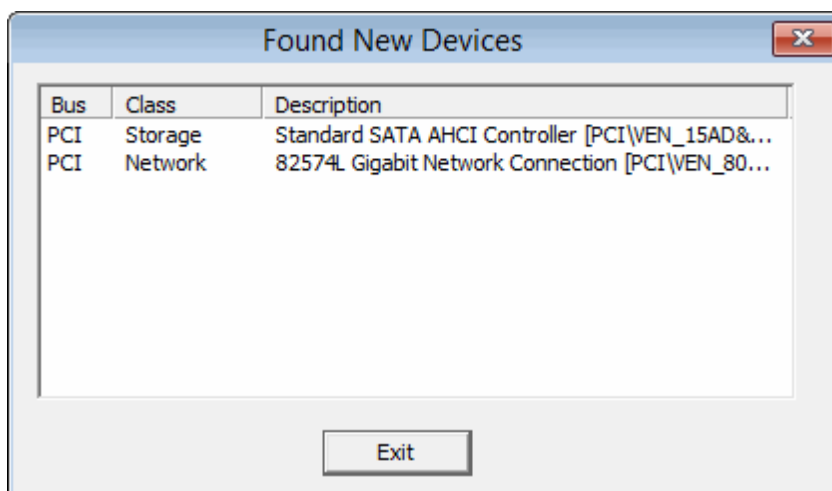
Dissimilar Hardware

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 [Network Setup...](#) button if you need to map a network share. In either case, the paths must be accessible to the WinPE 2 or WinPE 5 environment.

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



Ensure the specified path or paths contain the correct drivers for the dissimilar machine (ie. correct 32 or 64-bit version as appropriate for the OS). 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.

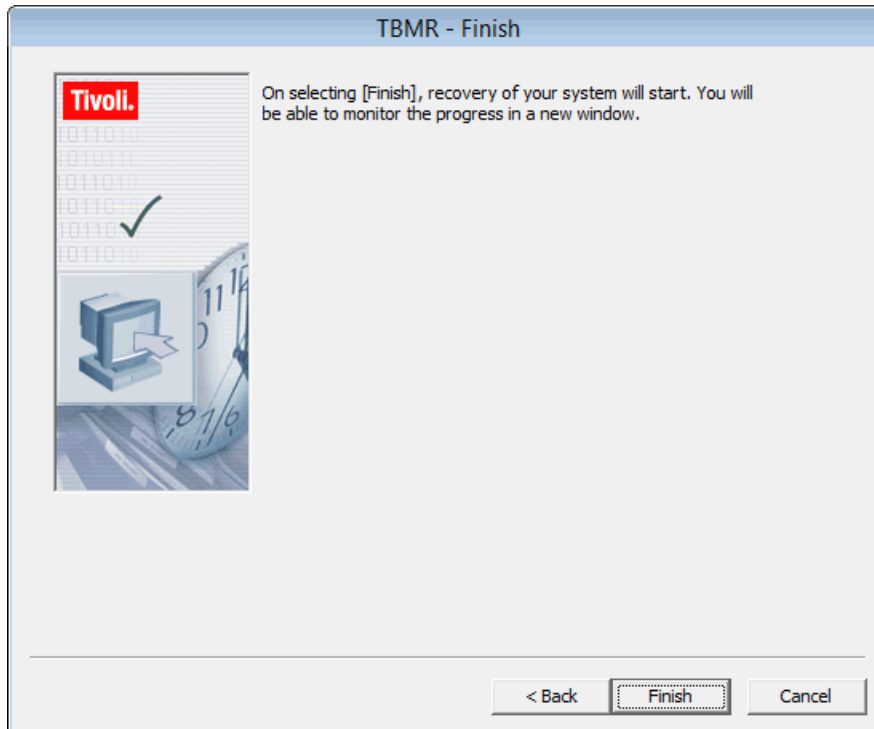
Note that if drivers are not found for the new boot disk then, although WinPE 2 or WinPE 5 will be

able to recover the files to the disk, there is a good chance that it will not boot correctly.

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

Proceed With The Recovery

Before continuing with the actual file recovery, a final warning screen is displayed.

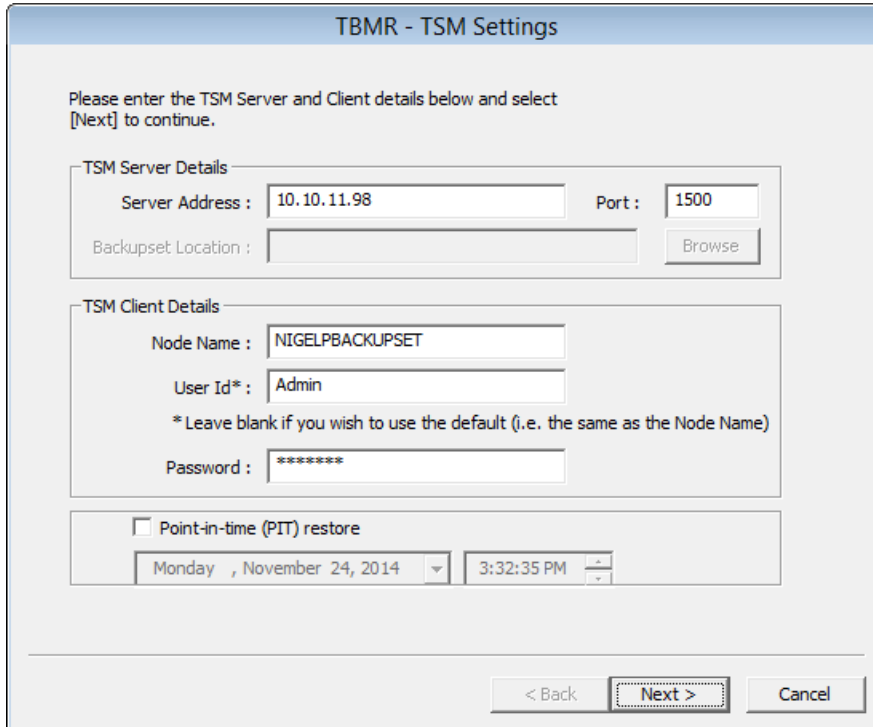


If you are happy with the specified recovery configuration, press **Finish**. This will commence the **actual** file recovery.

Note: this procedure will **COMPLETELY DESTROY** any existing data on those disks selected for format (ie. shown with a ). Disks or partitions tagged as no format (ie. shown with a ) will remain intact.

6.2.2.2 Restore from Backupset

If you selected **Restore from a Backupset**, select **Next>**. This will then display the **Enter TSM** server details:

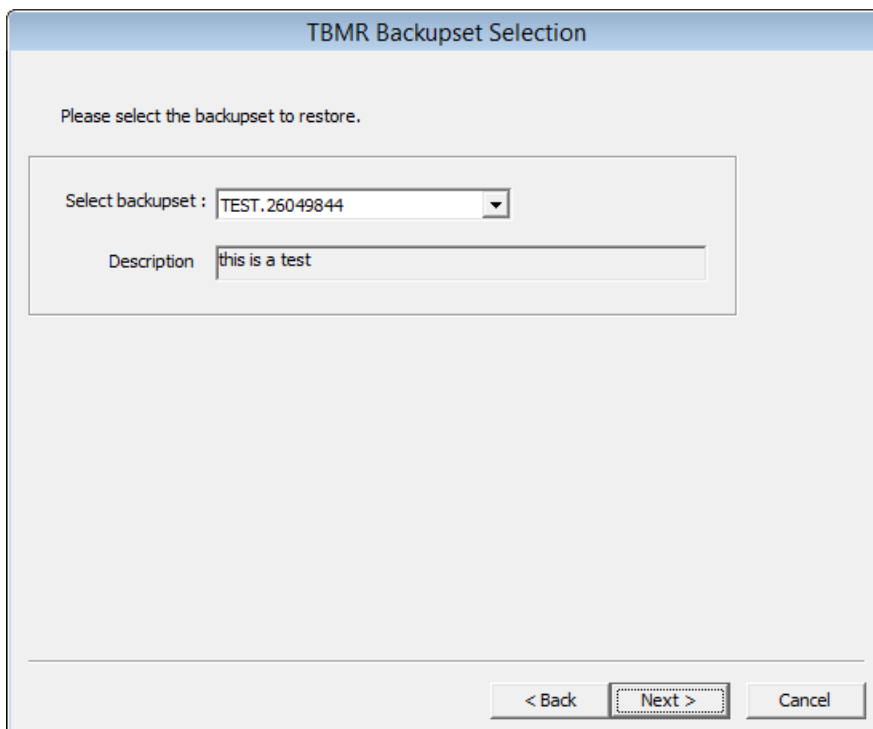


The dialog box is titled "TBMR - TSM Settings". It contains the following fields and controls:

- Instruction: "Please enter the TSM Server and Client details below and select [Next] to continue."
- TSM Server Details**
 - Server Address: 10.10.11.98
 - Port: 1500
 - Backupset Location: (empty field) with a "Browse" button.
- TSM Client Details**
 - Node Name: NIGELPBACKUPSET
 - User Id*: Admin
 - * Leave blank if you wish to use the default (i.e. the same as the Node Name)
 - Password: (masked with asterisks)
- ☐ Point-in-time (PIT) restore
 - Monday, November 24, 2014 (dropdown)
 - 3:32:35 PM (time picker)
- Navigation buttons: "< Back", "Next >" (highlighted), and "Cancel".

Note: Example above shows the server Admin credentials being used to recover the backupset instead of the standard Node credentials.

The system configuration will then be restored from the appropriate backupset, which is selected from the next dialogue:

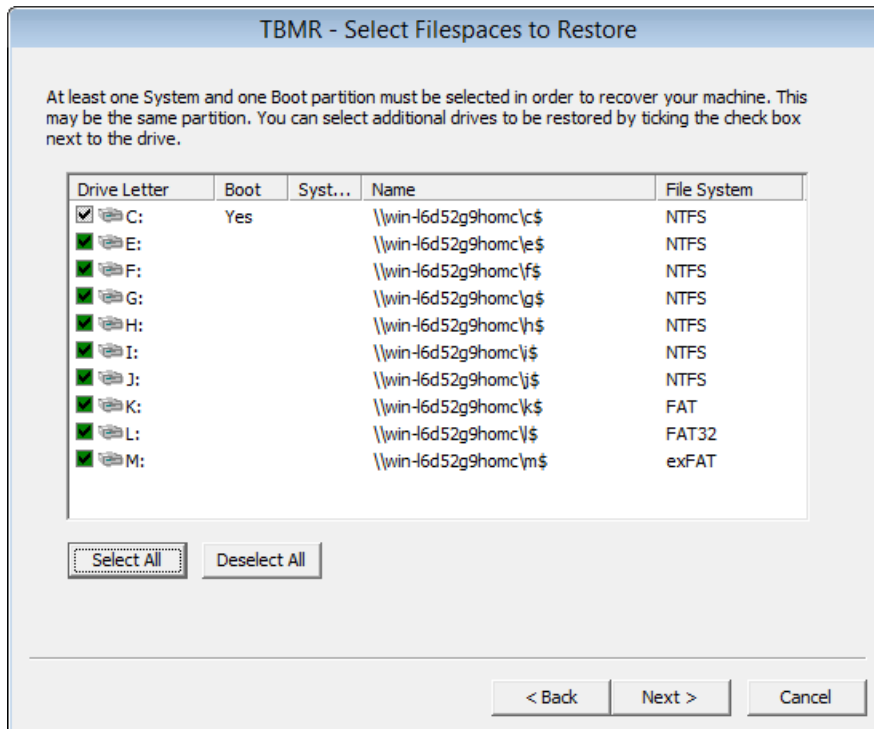


The dialog box is titled "TBMR Backupset Selection". It contains the following fields and controls:

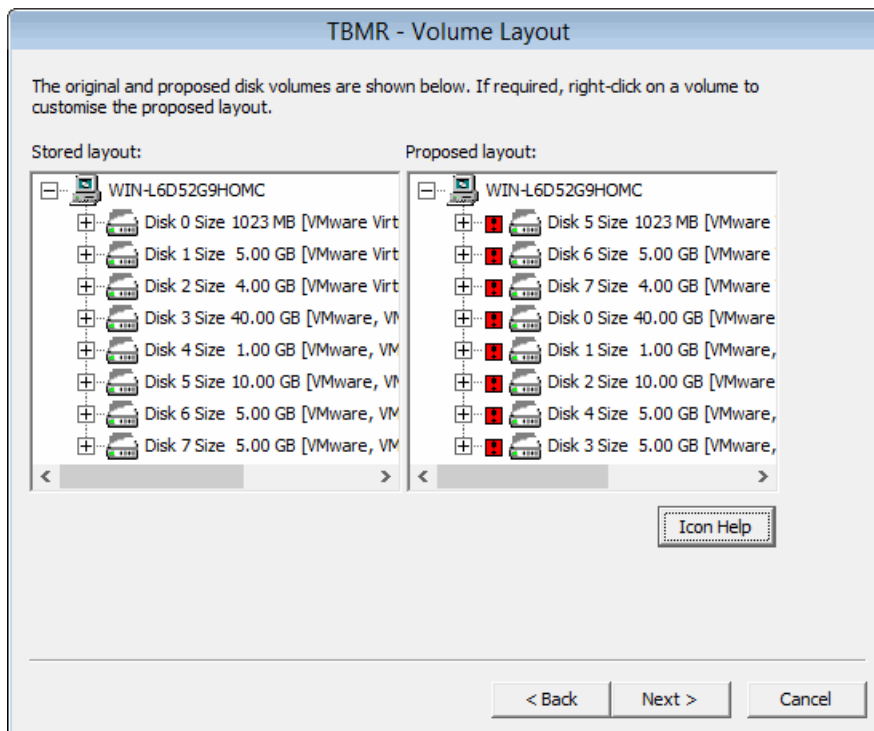
- Instruction: "Please select the backupset to restore."
- Select backupset: TEST.26049844 (dropdown menu)
- Description: this is a test (text field)
- Navigation buttons: "< Back", "Next >" (highlighted), and "Cancel".

If only 1 backupset is detected in the TSM node then the dialogue is not displayed.

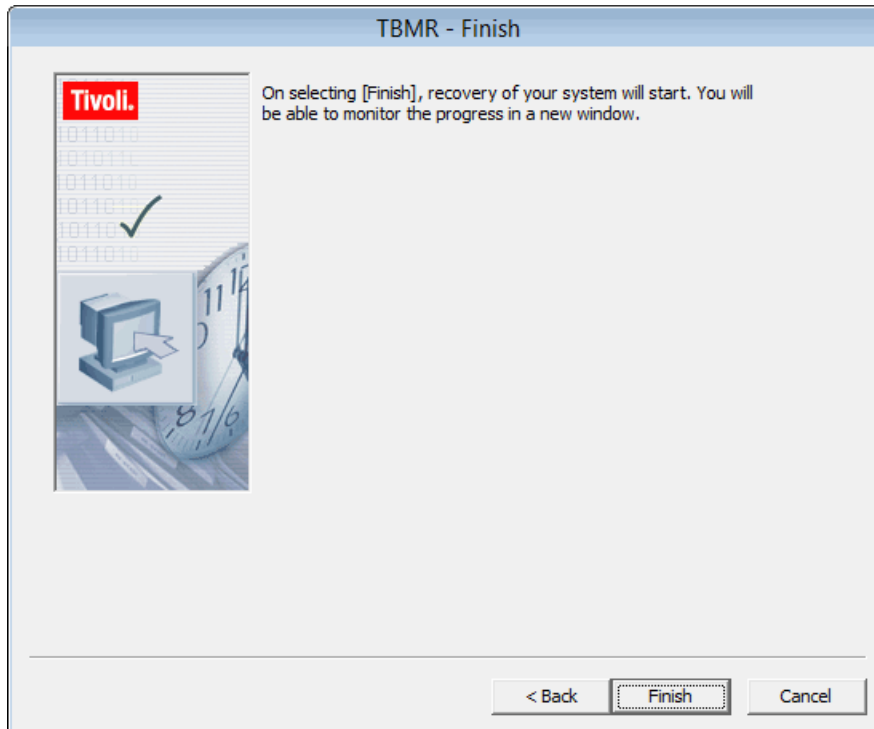
The configuration will then be retrieved from the selected backupset. The DR process continues from the **Select Filespaces to Restore** dialogue:



Select the filespaces to restore and then the partition layout for the recovering system:



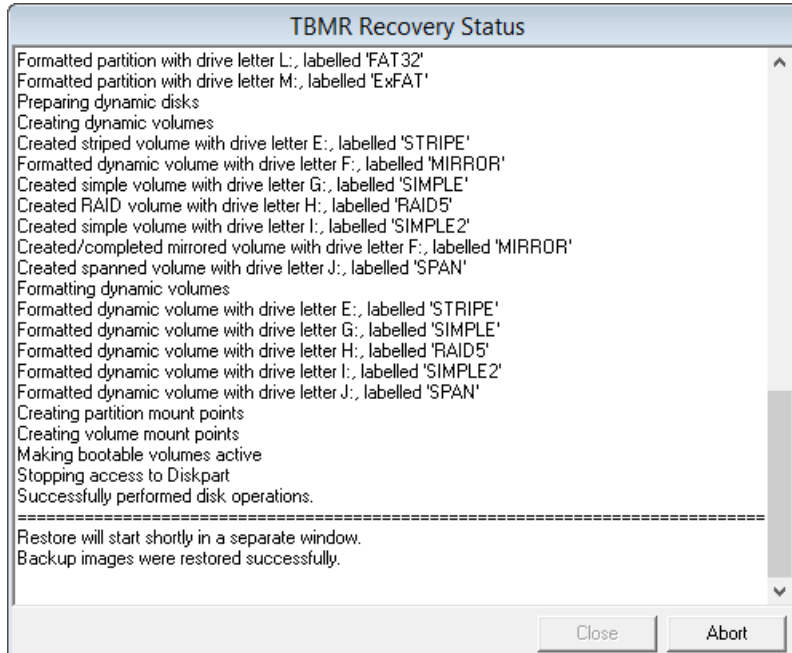
Finally, select **Finish** and the recovery will then proceed.



The subsequent recovery continues as described in section [Disk Recovery Sequence](#).

6.2.2.3 Disk Recovery Sequence

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



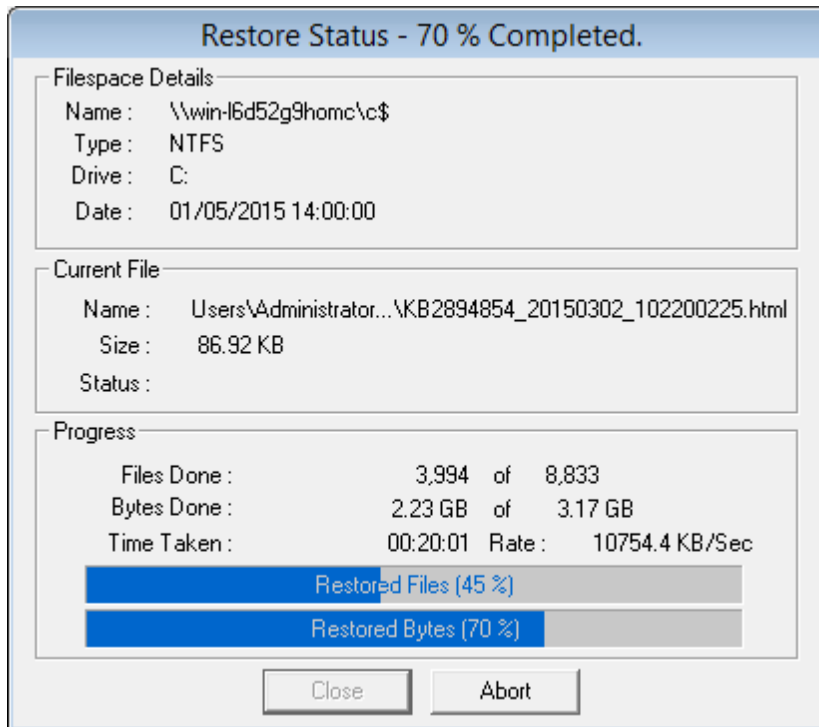
This involves:

- disk mapping original layout to new
- cleaning (removing any existing disk partitions)
- removing any existing dynamic volume databases
- re-creating the partitions

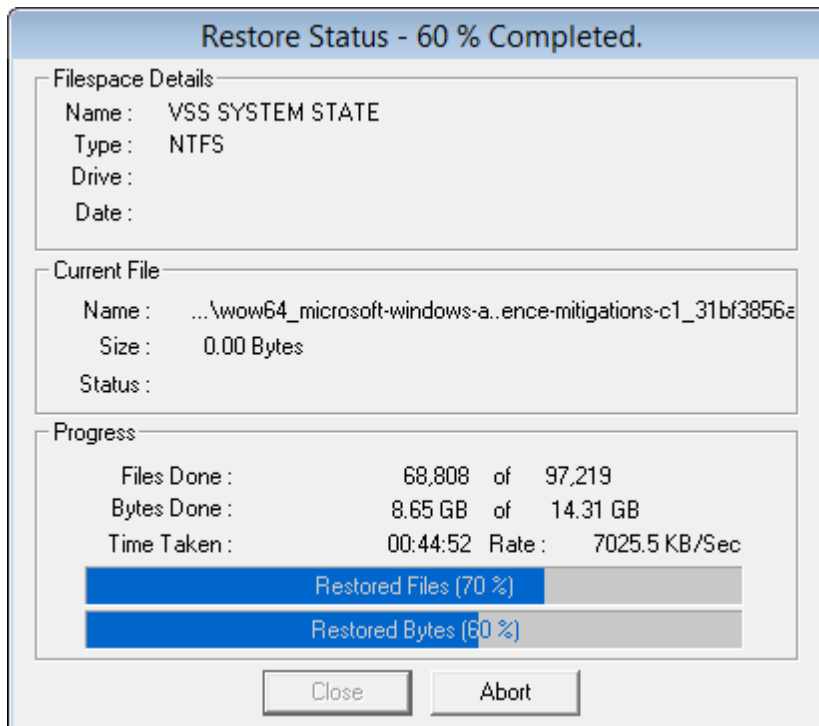
- converting to dynamic volumes if required
- formatting to the required partition type
- create partition/volume mount points
- make bootable volumes active

The next step is to recover the filespace to the selected target disks/partitions. A new window appears containing the restore status of recovered files, with progress bars 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 *volume filespace* selected,



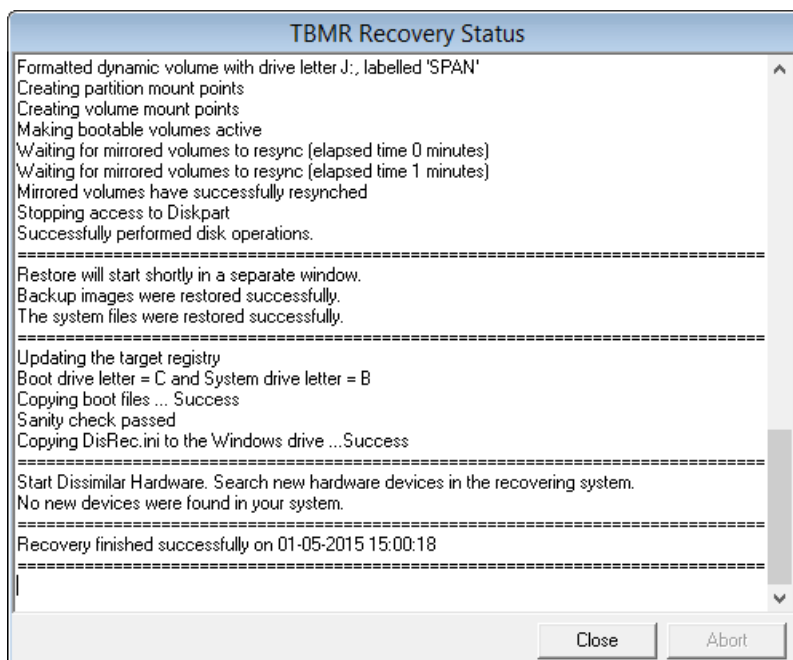
followed by *System State*:



This process may take some minutes 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



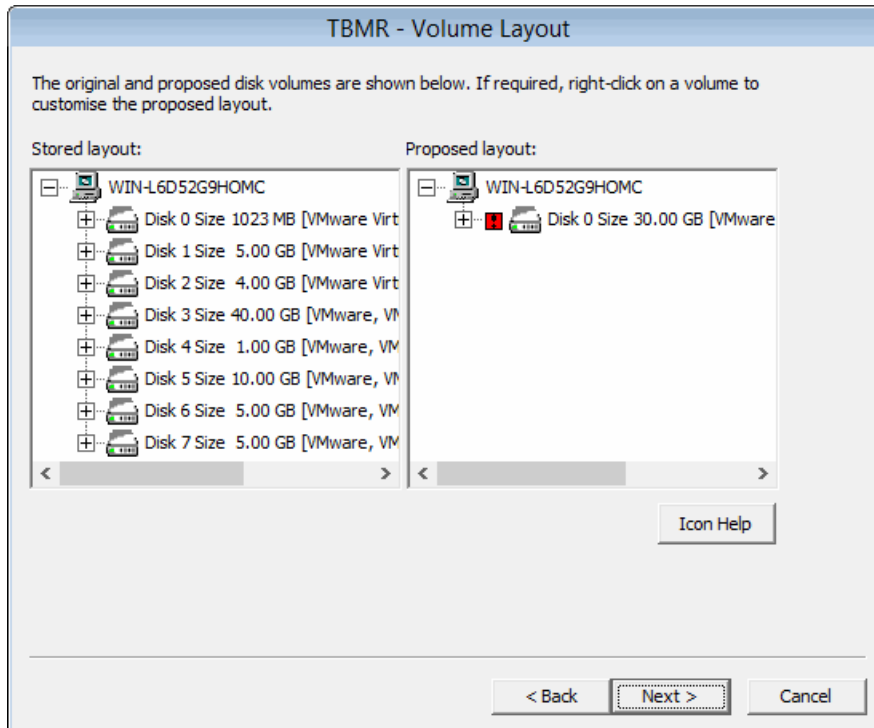
Finally, press **Close** to return to the **Recovery Environment** main menu. At this point, you may

want to view the recovery logs and perhaps copy the logs to a local device or remote share before selecting to reboot.

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

6.2.2.4 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, TBMR 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.

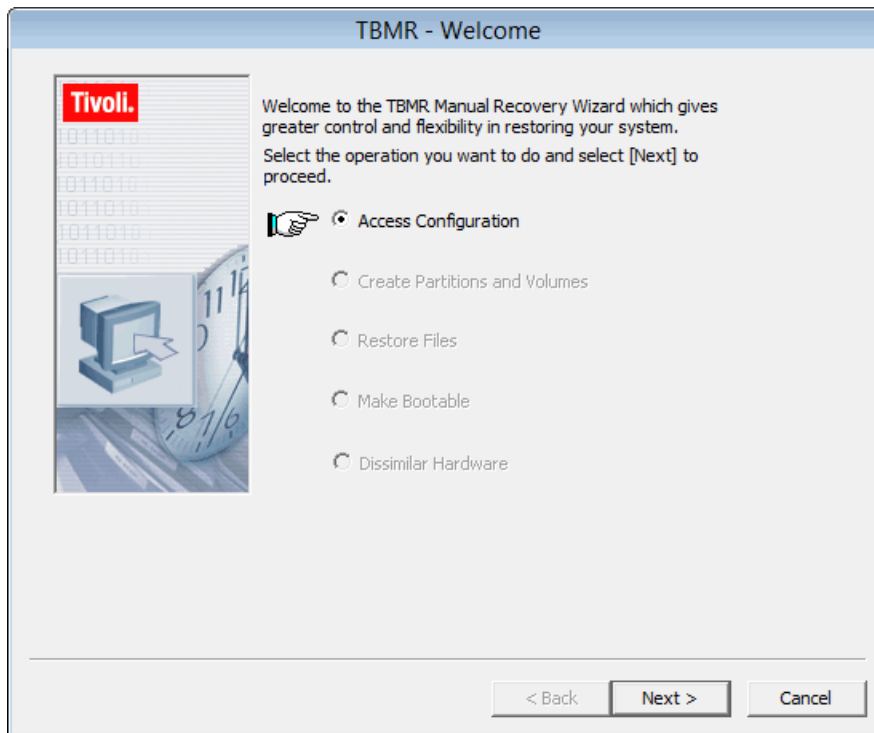
Note 2: during a recovery to a system with larger disks, the partition sizes will remain the same as the original by default. However, in this case, it is possible to increase partition size manually during the recovery by right-clicking on the partition icon and selecting Modify.

6.2.3 Start the manual Recovery wizard

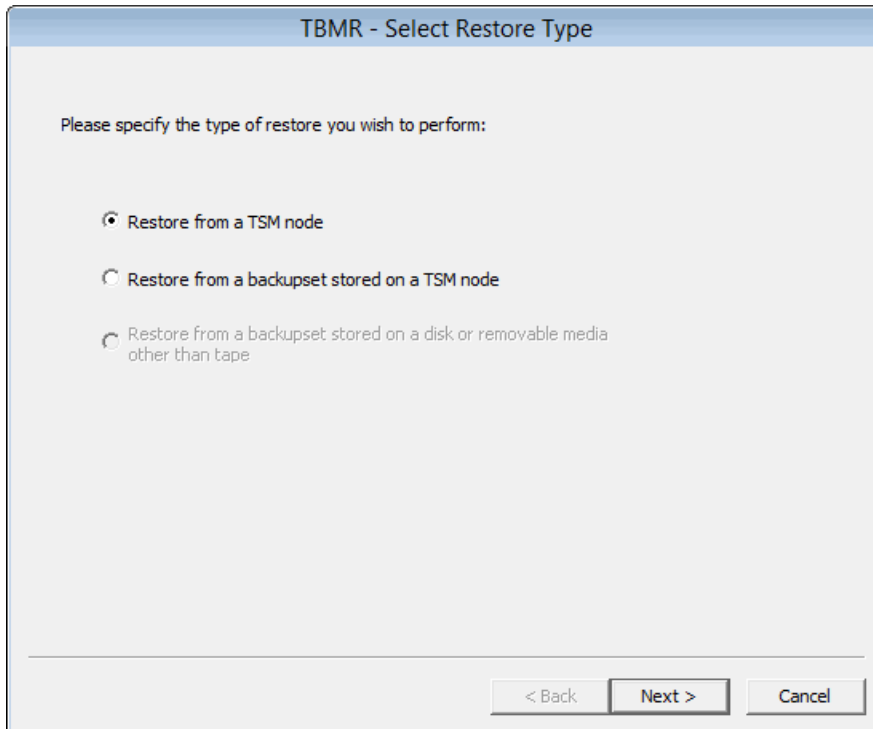
Select the **Start the manual Recovery wizard** to commence a manual DR sequence. This option will stop after each step in the DR sequence allowing the DR to be aborted or the step to be repeated with different parameters.

6.2.3.1 Locate Configuration

The first step of the manual DR sequence is to provide the location of the DR configuration.



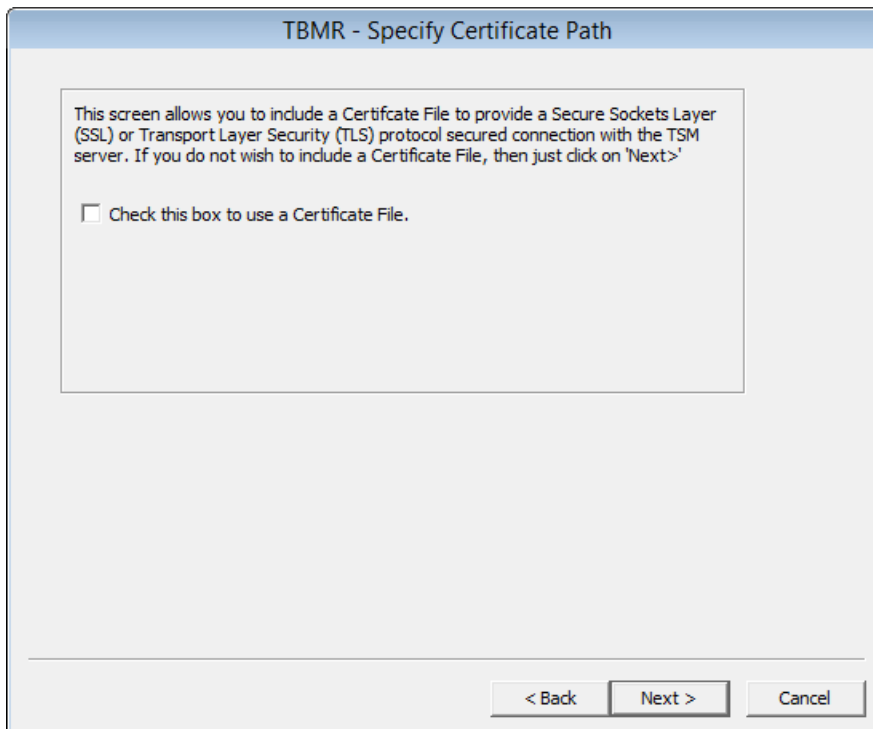
Press **Next>** to proceed to the first step of the sequence. Press **Cancel** to abort the recovery sequence at this point. You will then be presented with a dialogue prompting you to select the type of the TSM restore.



The dialog box is titled "TBMR - Select Restore Type". It contains the instruction "Please specify the type of restore you wish to perform:". There are three radio button options: "Restore from a TSM node" (which is selected), "Restore from a backupset stored on a TSM node", and "Restore from a backupset stored on a disk or removable media other than tape". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

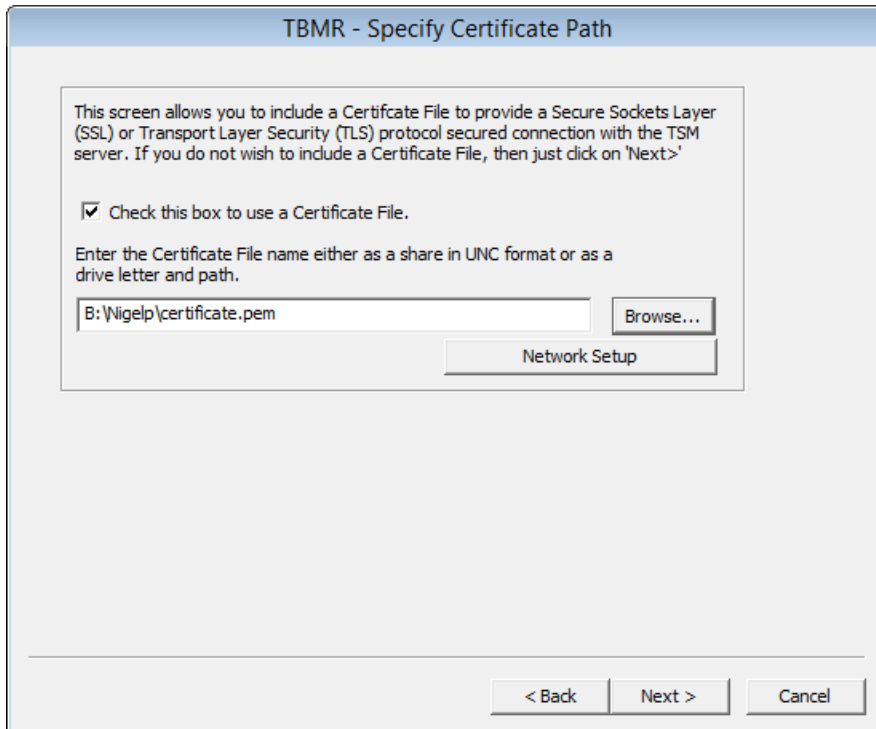
Restoring from a TSM node or an online backupset is supported.

Press **Next>** to continue to:



The dialog box is titled "TBMR - Specify Certificate Path". It contains a text box with the following text: "This screen allows you to include a Certificate File to provide a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol secured connection with the TSM server. If you do not wish to include a Certificate File, then just click on 'Next>'". Below this text is a checkbox with the label "Check this box to use a Certificate File.", which is currently unchecked. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

This dialogue allows an SSL or TLS security certificate to be provided to the TSM server. To add a certificate click the check box to open up a browse window.



TBMR - Specify Certificate Path

This screen allows you to include a Certificate File to provide a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol secured connection with the TSM server. If you do not wish to include a Certificate File, then just click on 'Next>'

☒ Check this box to use a Certificate File.

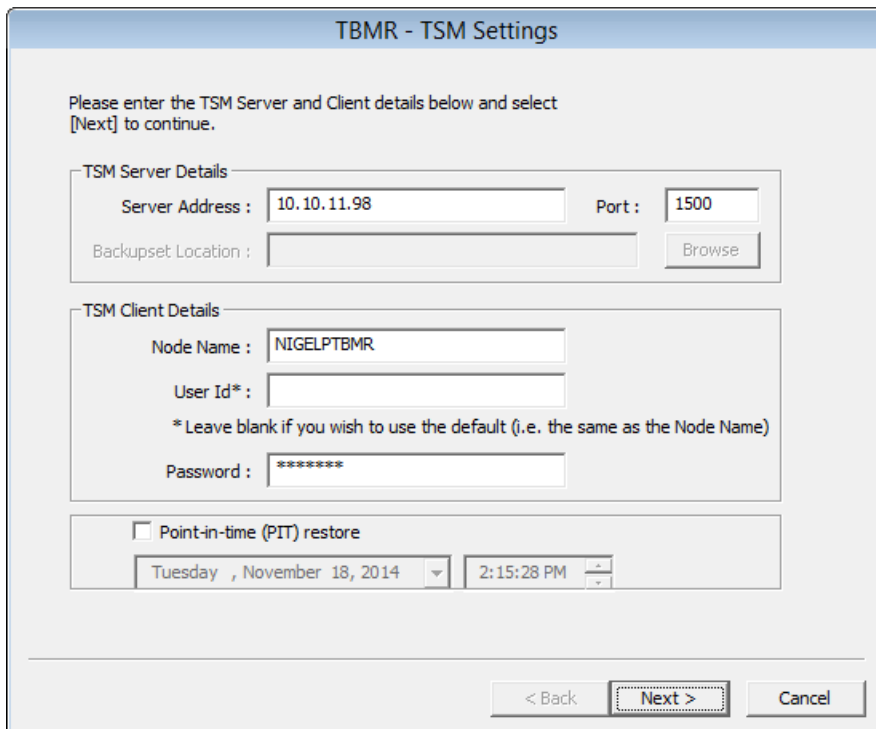
Enter the Certificate File name either as a share in UNC format or as a drive letter and path.

B:\Nigelp\certificate.pem Browse...

Network Setup

< Back Next > Cancel

Add a path to the certificate file or use the Browse button to navigate to the location of the certificate. You will be prompted to add any network access credentials or use the [Network Setup](#) button to add them in advance. Click [Next >](#) to continue to the [TSM Server Settings](#) dialogue.



TBMR - TSM Settings

Please enter the TSM Server and Client details below and select [Next] to continue.

TSM Server Details

Server Address : 10.10.11.98 Port : 1500

Backupset Location : Browse

TSM Client Details

Node Name : NIGELPTBMR

User Id* :
* Leave blank if you wish to use the default (i.e. the same as the Node Name)

Password : *****

☐ Point-in-time (PIT) restore

Tuesday , November 18, 2014 2:15:28 PM

< Back Next > Cancel

Specify the location of the [TSM Server](#) and [Node](#) used to back up the Client.

Selecting the [Point-in-time](#) (PIT) restore mode will allow the system to be recovered from the most recent backup before the specified date and time. This means the version of any file restored will be earlier than the specified date and time. Selecting the down-arrow in the calendar control will bring up a calendar:

TBMR - TSM Settings

Please enter the TSM Server and Client details below and select [Next] to continue.

TSM Server Details

Server Address : Port :

Backupset Location :

TSM Client Details

Node Name :

User Id* :

* Leave blank if you wish to use the default (i.e. the same as the Node Name)

Password :

☒ Point-in-time (PIT) restore

Friday , May 1, 2015

May 2015

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Today: 5/1/2015

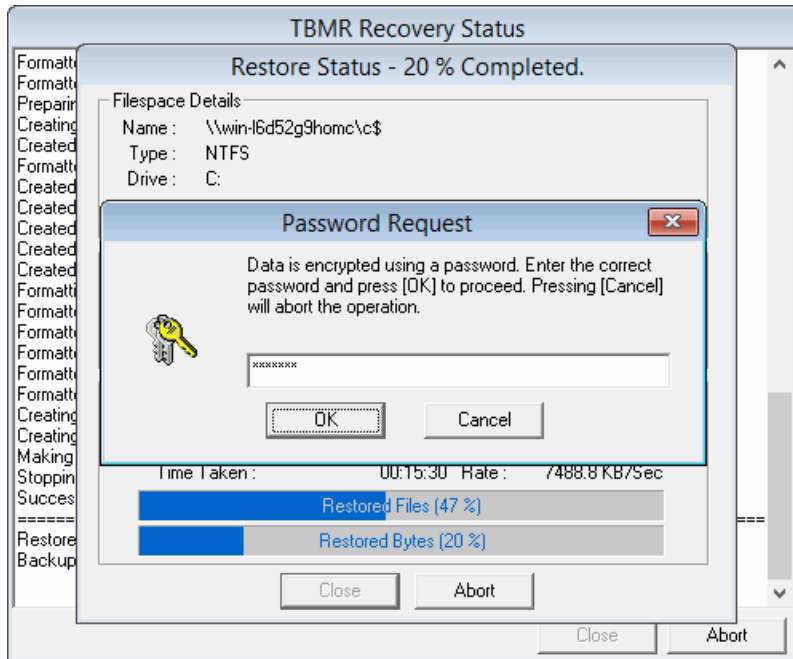
This can be used to scroll the months/years backwards and forwards as necessary.

Note: a future date will result in the latest backup being recovered.

The next dialogue displayed depends upon whether you selected **Restore from Node** or **Restore from Backupset**.

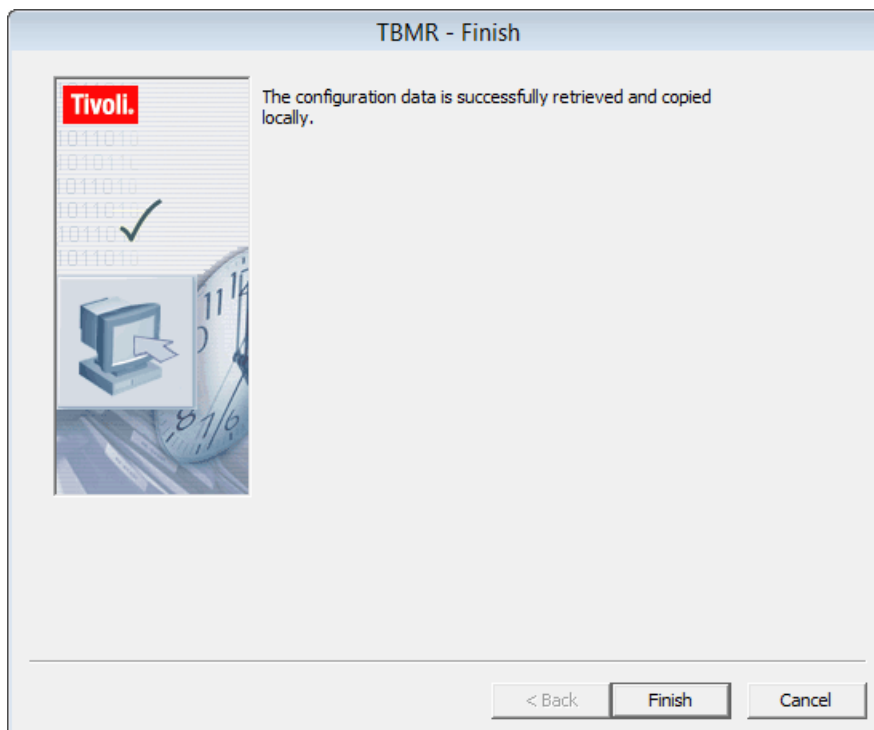
Restore From Node

Select **Next>** to continue. If the backup including the TBMR configuration folder **TBMRCFG** is encrypted, a prompt for the encryption password will be displayed if not held locally:



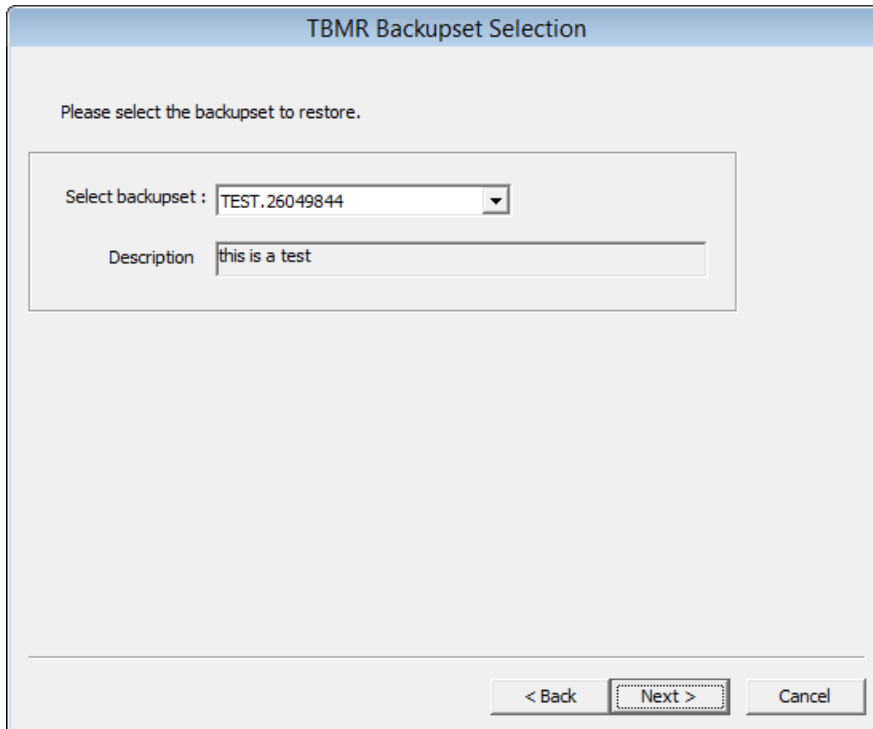
Enter the password used during the backup and press OK.

Successful extraction of the configuration from the server is confirmed with the following dialogue:



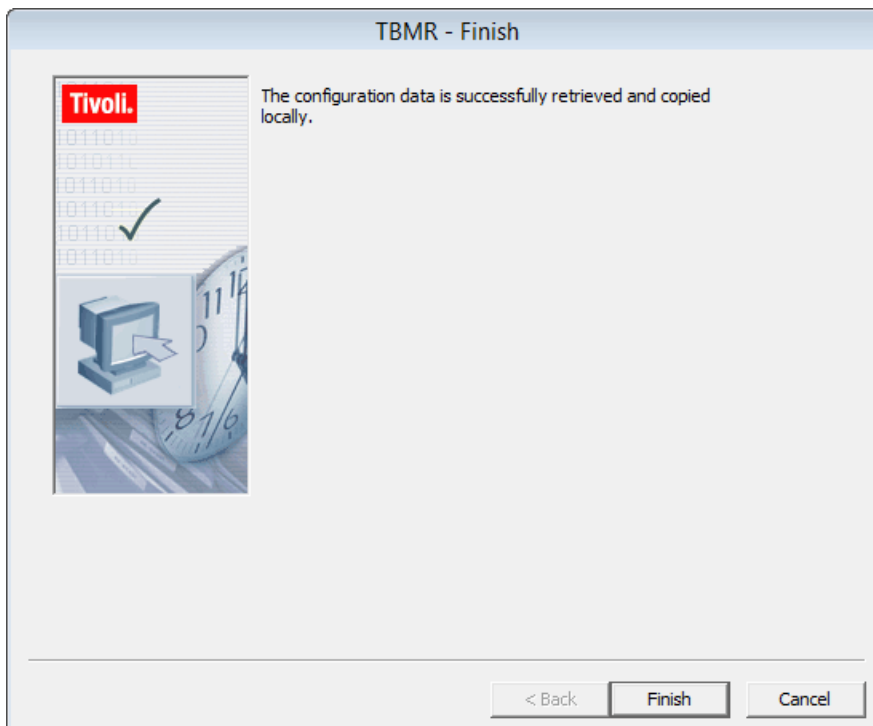
Restore From Backupset

The system configuration will be restored from the appropriate backupset, which is selected from the next dialogue:



The dialog box is titled "TBMR Backupset Selection". It contains the instruction "Please select the backupset to restore." Below this, there is a "Select backupset :" label followed by a dropdown menu showing "TEST.26049844". Underneath the dropdown is a "Description" label followed by a text box containing "this is a test". At the bottom right, there are three buttons: "< Back", "Next >" (which is highlighted with a dashed border), and "Cancel".

Successful extraction of the configuration from the server is confirmed with the following dialogue:

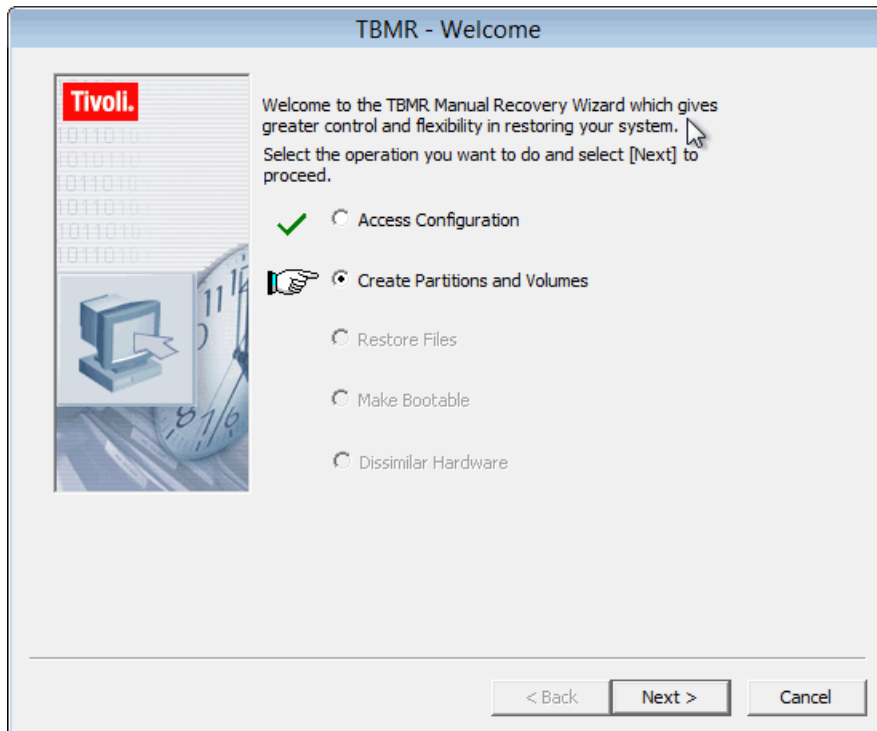


The dialog box is titled "TBMR - Finish". On the left side, there is a graphic featuring the Tivoli logo, a green checkmark, and a clock. To the right of the graphic, the text reads: "The configuration data is successfully retrieved and copied locally." At the bottom right, there are three buttons: "< Back", "Finish" (which is highlighted with a dashed border), and "Cancel".

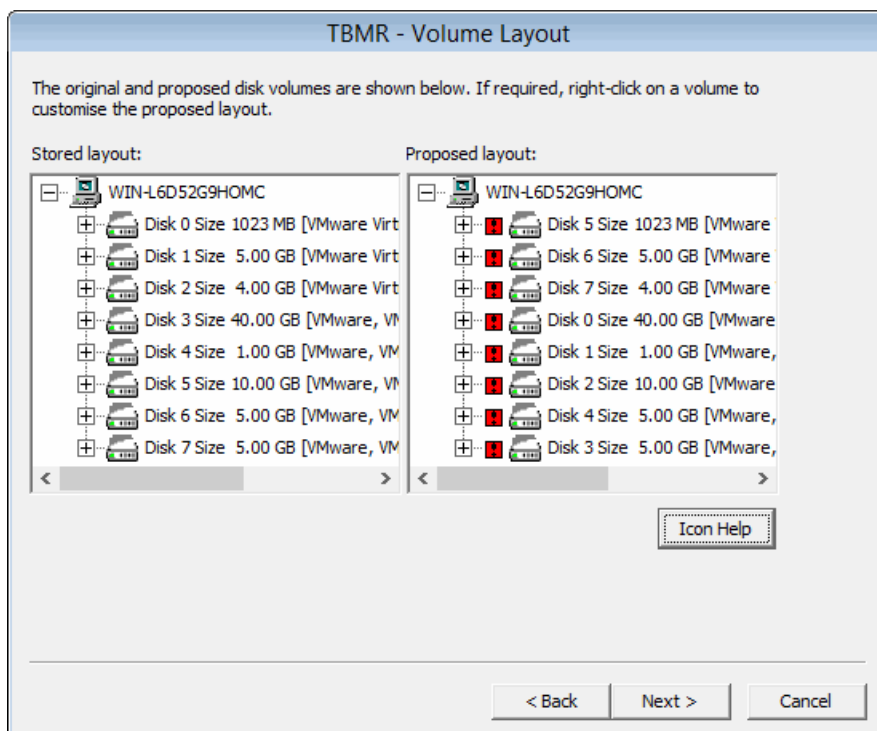
Select **Finish** and control returns to the next step in the **Manual Recovery** sequence.

6.2.3.2 Create Partition and Volumes

The next step of the manual recovery process is to configure the target disk **partitions** and **volumes**



Select **Next>** to display the Volume Layout dialogue:

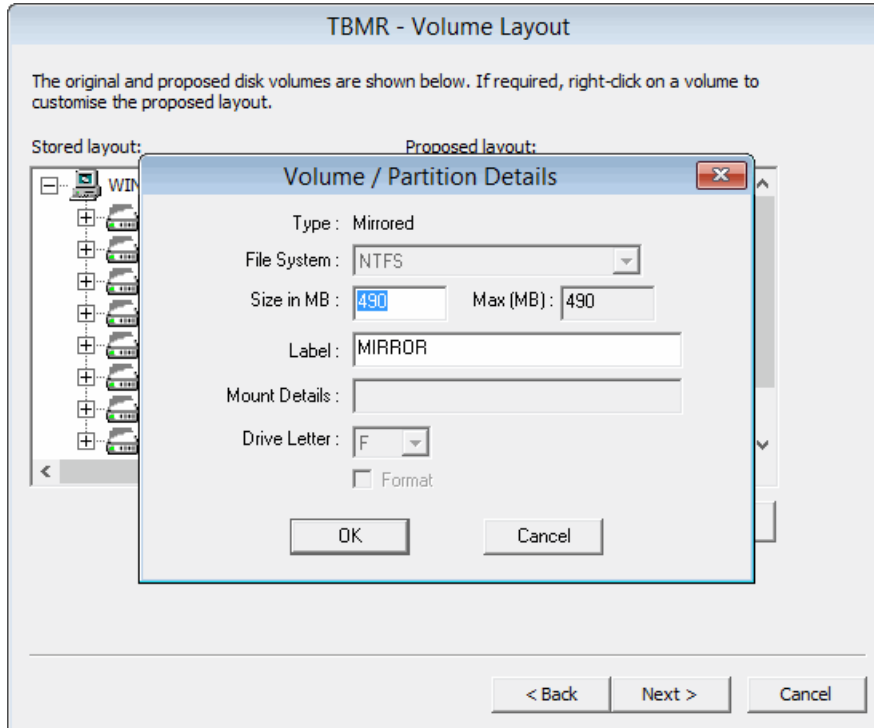


This screen shows the original disk layout against that of the target system. The target disk layout could be very different to the original. TBMR will attempt to match the disks using its own in-built criteria. Some of the criteria used to judge the match are:

- disk geometry (tracks, cylinders and sectors)

- disk capacity
- if currently formatted, the disk signature

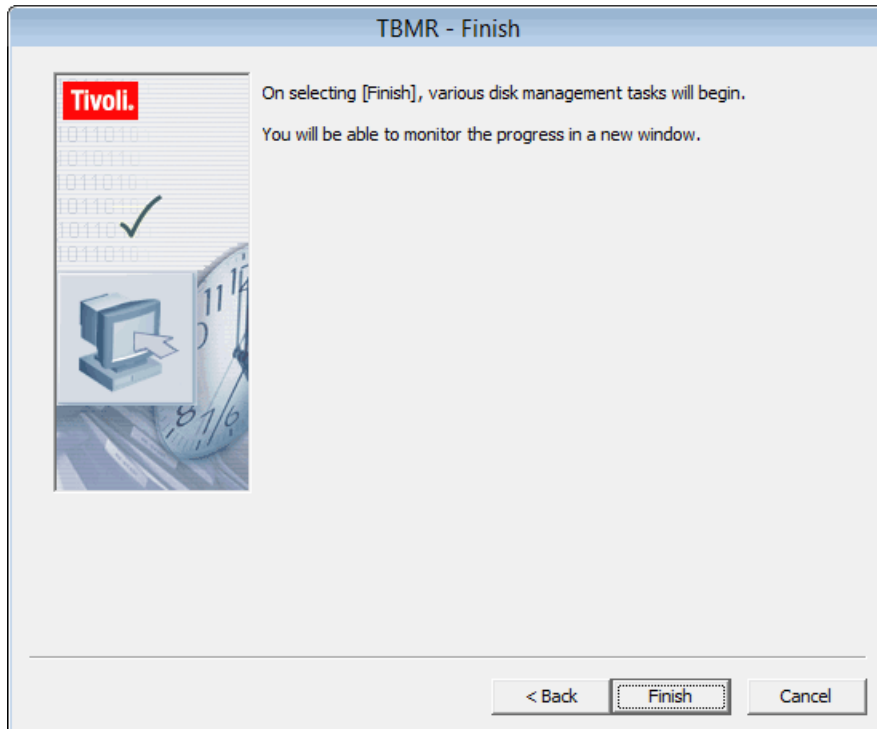
However, it is possible to change the partition size, or opt to tag/untag whether or not a partition should be formatted. To do this, right click on the the disk icon and the following configuration dialogue is displayed:



The indicator shown next to the disk icon indicates whether that disk will be left intact or not. A red exclamation mark indicates that the disk will be re-partitioned and/or formatted. A green tick indicates that the disk will be left intact.

Disks and partitions are discussed in more detail in the [Volume Layout](#) section.

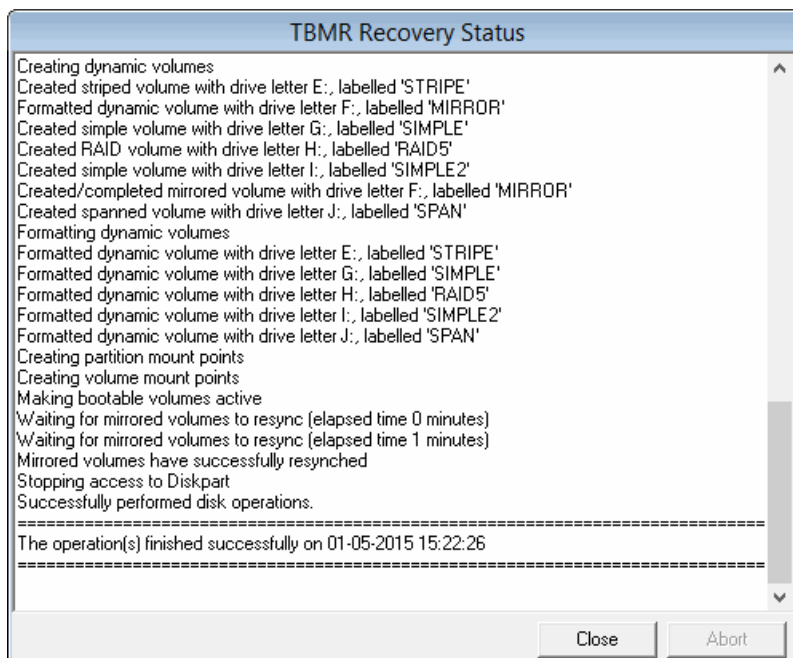
Press **<Back** to return to the previous step, **Finish** to commence the active part of this step, or **Cancel** to abort.



If you are happy with the recovery configuration, press **Finish**. This will commence the actual recovery.

Note: this procedure will completely destroy any existing data on the disks selected for recovery. Disks or partitions tagged as 'no format' will be retained.

The **Create Partitions and Volumes** step begins by preparing the disk selected for the recovery.



This involves:

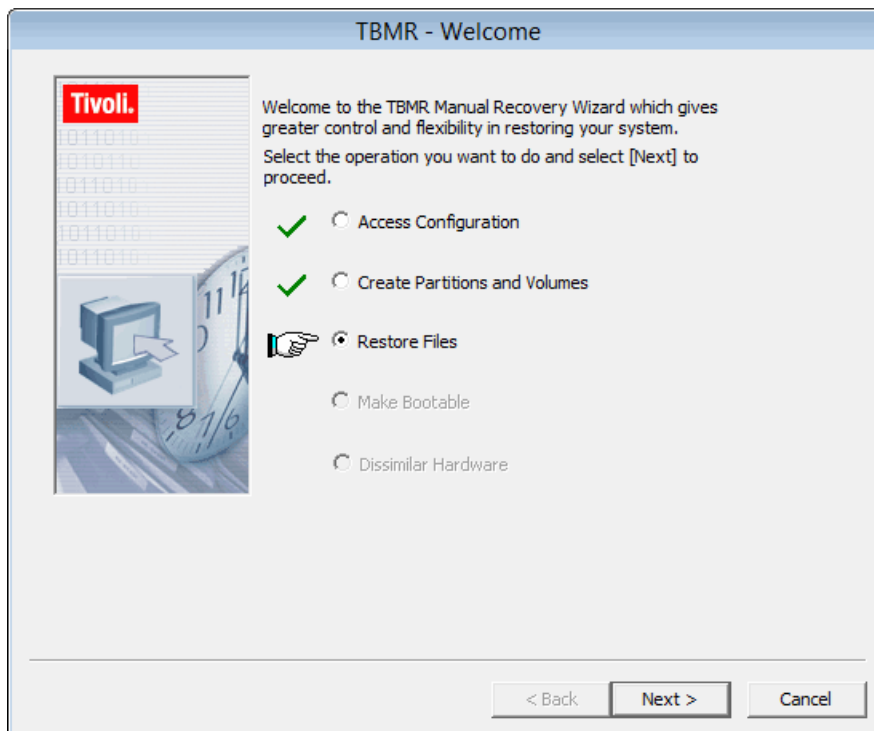
- disk mapping original layout to new
- cleaning (removing any existing disk partitions)
- removing any existing dynamic volume databases

- 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
- waiting for any mirrored volumes to resync

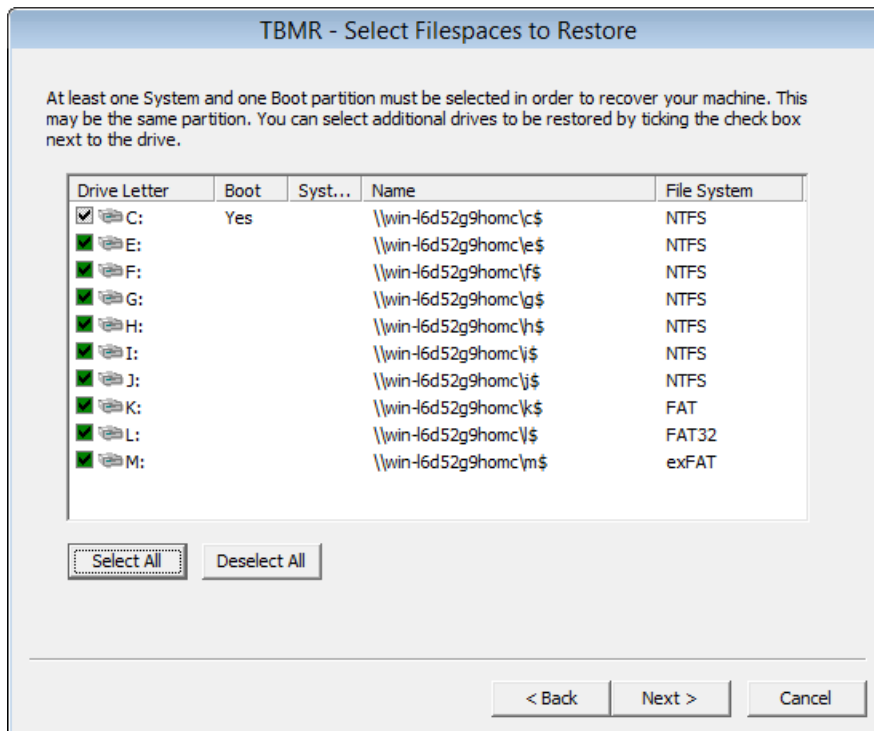
Press **Close>** to continue with the recovery.

6.2.3.3 Restore Files

The next step of the manual recovery process is to restore the DR backup files.



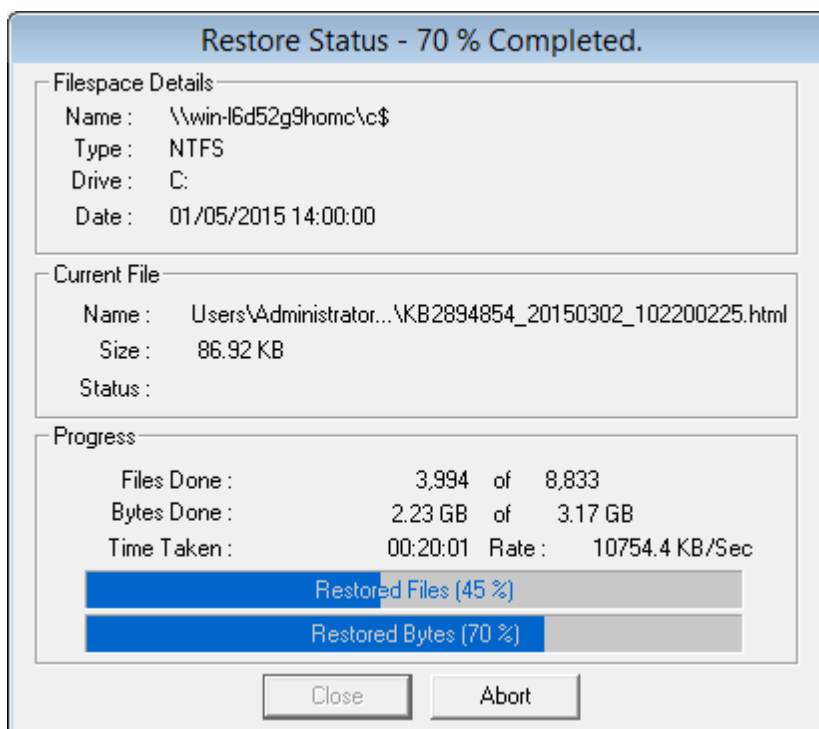
Press **Next>** to identify the TSM filespace that should be recovered. Note that the *SystemState* filespace will always be recovered by default.



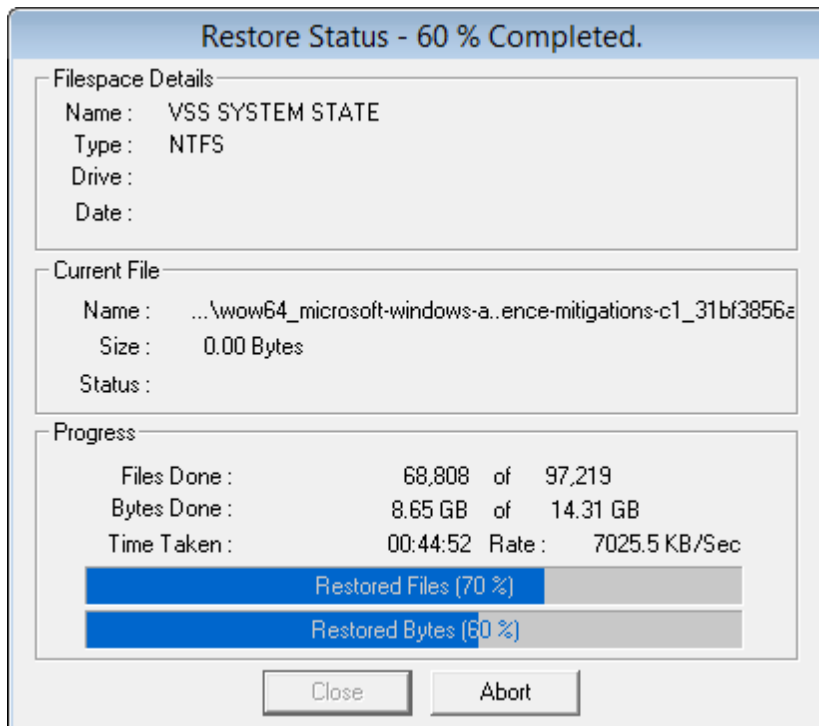
Press **Next>** to commence the restore of the TSM filespace to their target disks/partitions.

Finally, a new window appears containing the restore status of recovered files, with progress bars indicating how much of the backup has been restored. This display also shows the recovery statistics in terms of time, size and throughput.

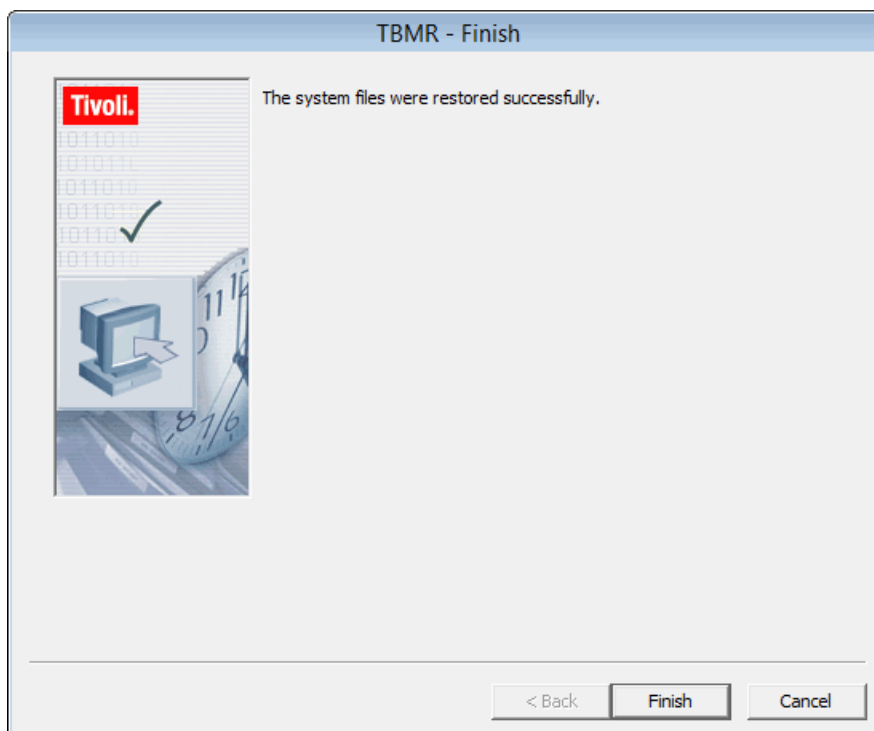
Note that the recovery is divided into different phases: firstly each **volume filespace** selected is restored with the **SystemState** filespace restored last.



This process may take some minutes if the backups are large. You may select the **Abort** button to terminate the file recovery process, but this may leave the disk or partition in an unpredictable state, which may render it unusable.



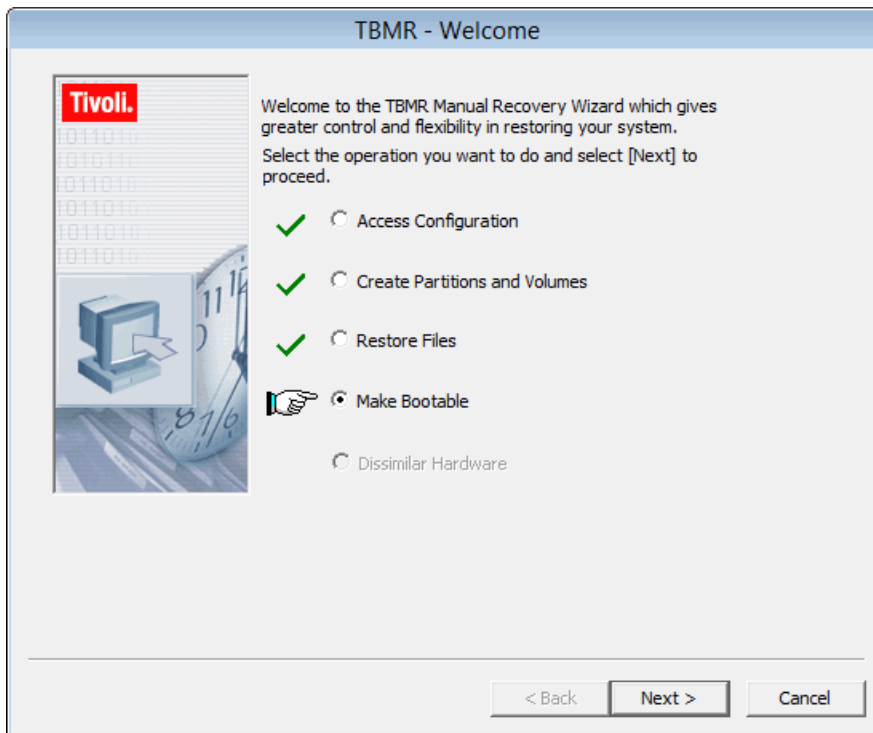
If any errors occur during the recovery, an error message will be shown in the window. Refer to the logs post recovery to establish the cause of any error. When the restore files step completes the following dialogue is displayed:



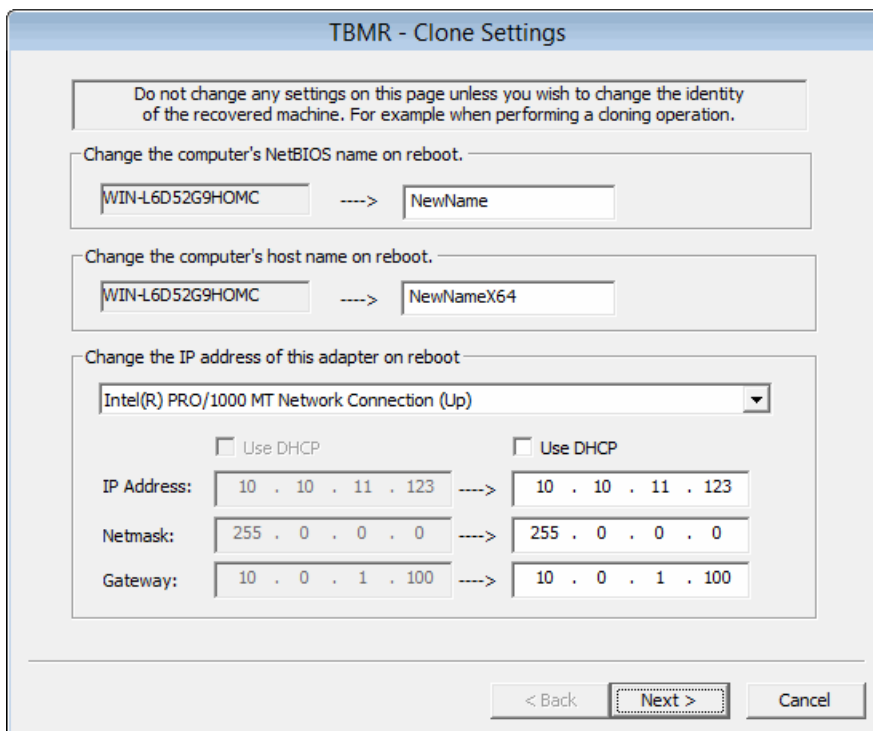
Select **Finish** and control returns to the next step in the **Manual Recovery** sequence.

6.2.3.4 Make Bootable

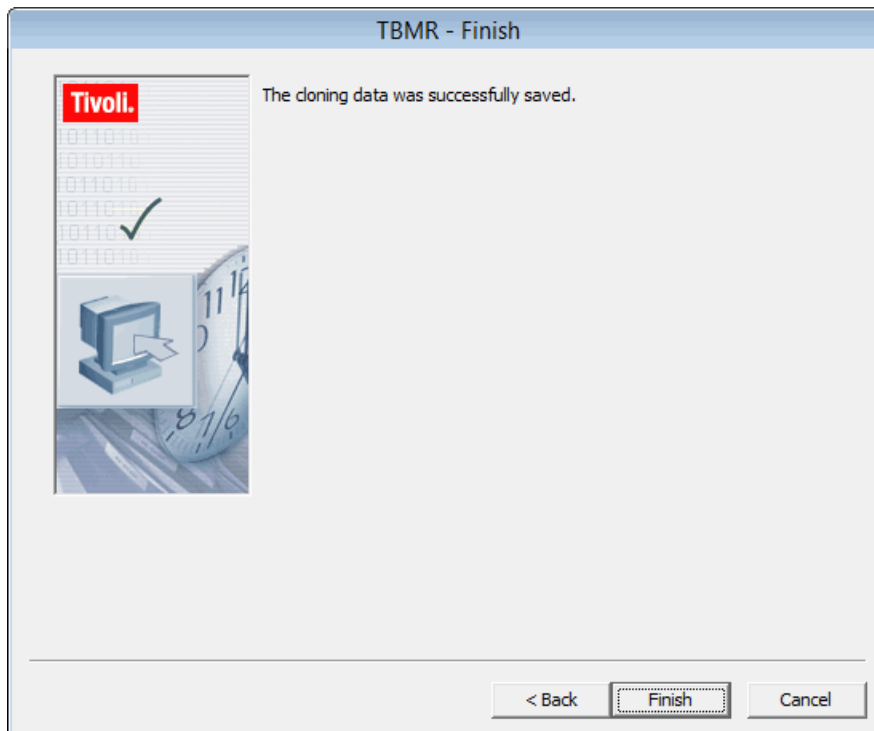
The next step in the manual recovery sequence is to make the original disk 'bootable'. This involves re-creating the MBR of the boot disk and modifying the registry with the new disk GUID.



Press **Next>** to commence the **Make Bootable** step. You will now be able to change the hostname and/or the machine's IP addresses on reboot.

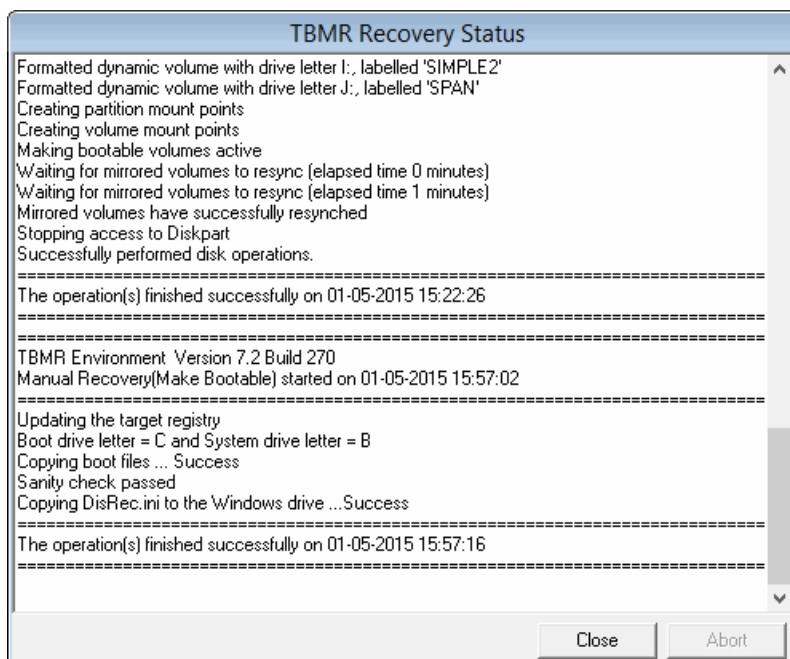


If no hostname or IP change is required, click **Next>** to continue. The cloning data is confirmed with the following dialogue.



Click **Finish** to complete the Make Bootable step.

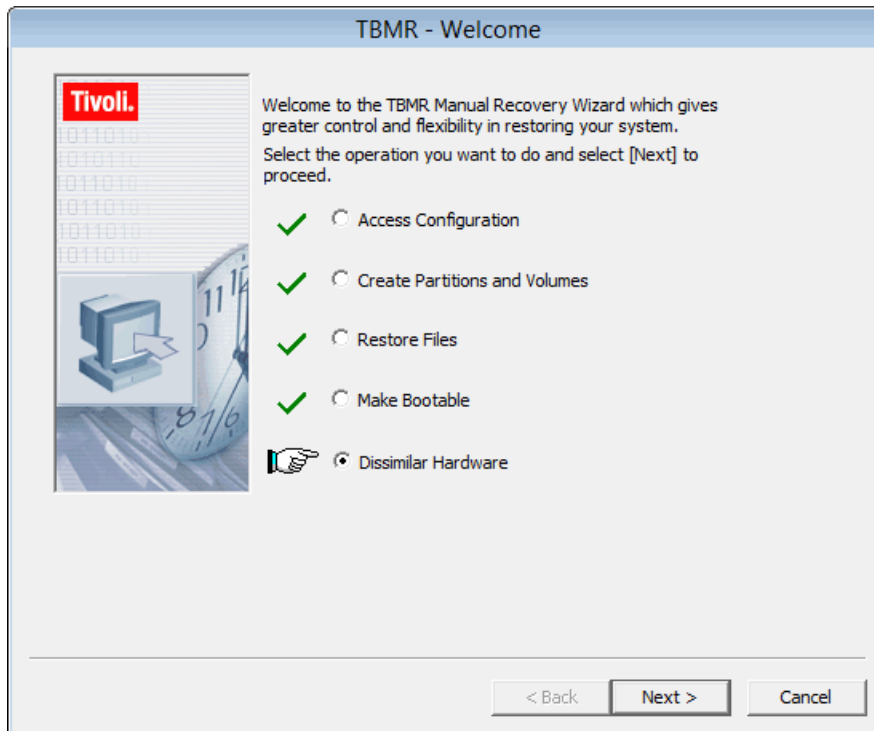
A new dialogue window opens summarising the success or failure of the operation:



Press **Close** to complete the step and return to the **Manual Recovery Wizard**.

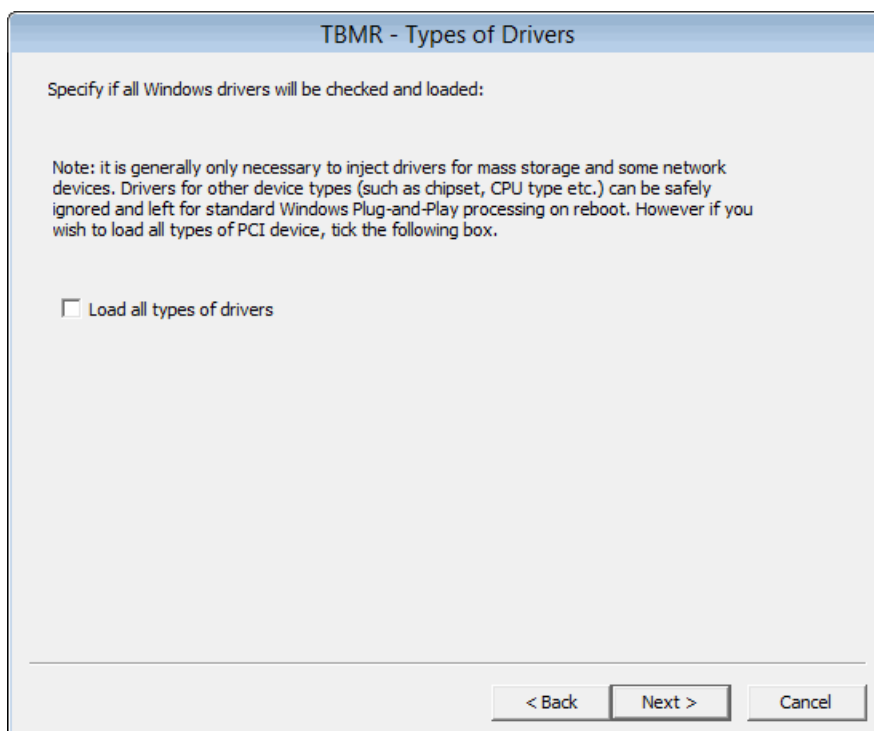
6.2.3.5 Dissimilar Hardware

The final step in the manual DR sequence is to check if the recovery is to **Dissimilar Hardware**.

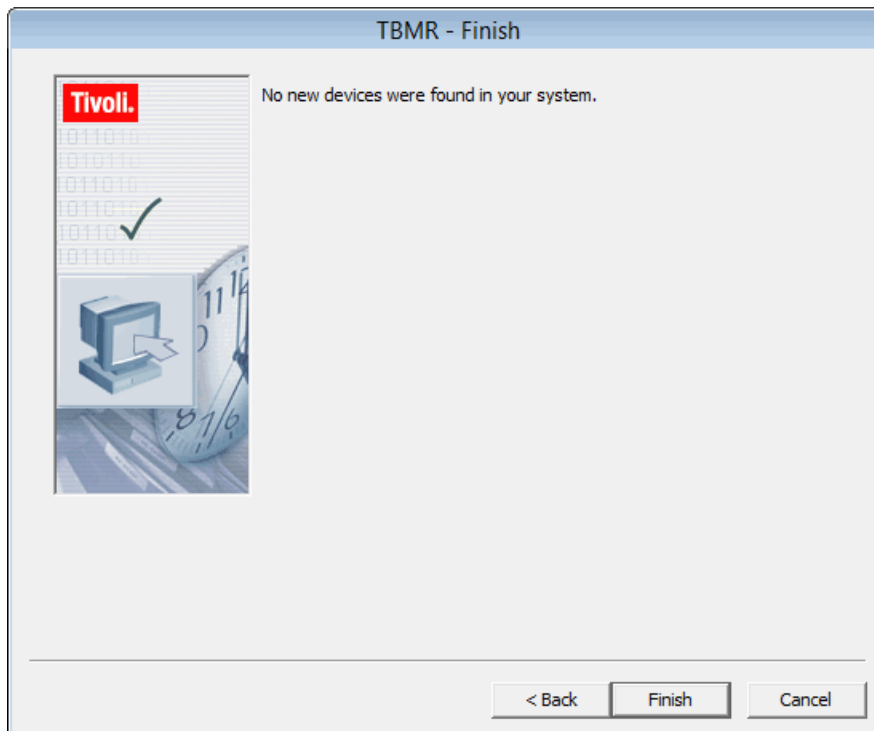


This is determined by comparing the drivers currently in use by Windows WinPE 2 or WinPE 5 and the drivers listed in the recovered machine's registry.

The step first prompts for what driver types should be checked. By default, only **Mass Storage** (disk) and **network devices** are checked.



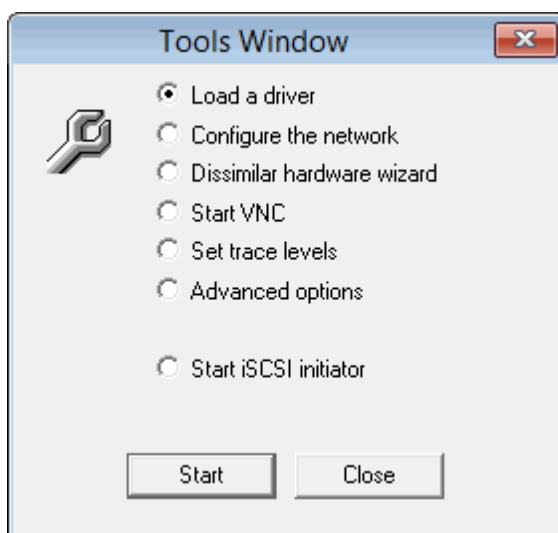
Press **Next>** to continue. For recovery to similar hardware, no new devices will be found and this will be confirmed by this dialogue:



Press **Finish** to complete the manual recovery sequence.

6.2.4 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
- Configure the network
- Dissimilar Hardware Wizard
- Start VNC
- Set trace levels

- Advanced options
- Start iSCSI initiator

Load a driver allows a new mass storage or NIC driver to be injected into the running booted WinPE 2 or WinPE 5 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.

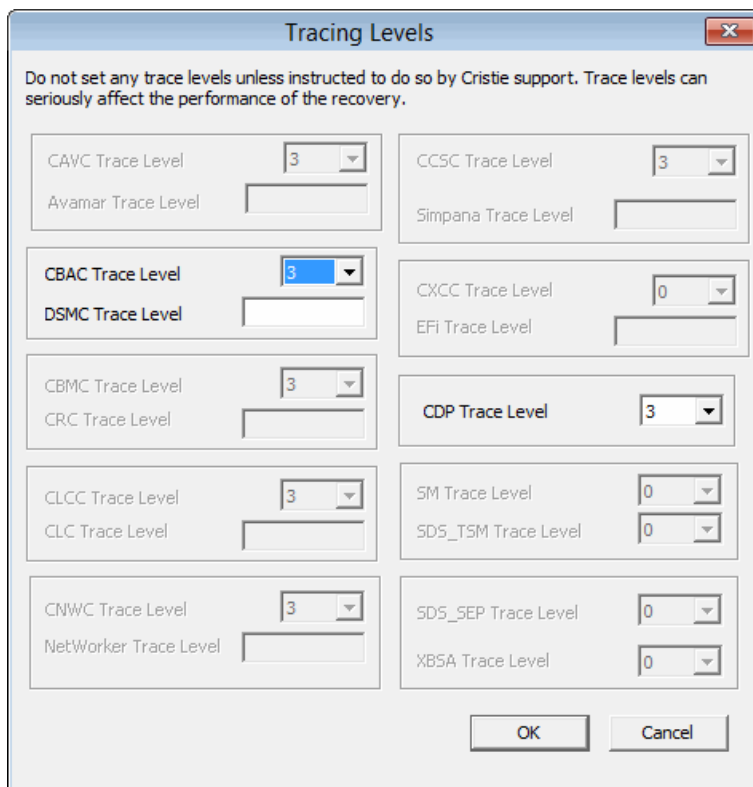
Selecting **Configure the network** will start the **Cristie Network Configurator** tool. This provides extensive facilities to configure networks during the DR process.

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 WinPE 2 or WinPE 5 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 WinPE 2 or WinPE 5 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:



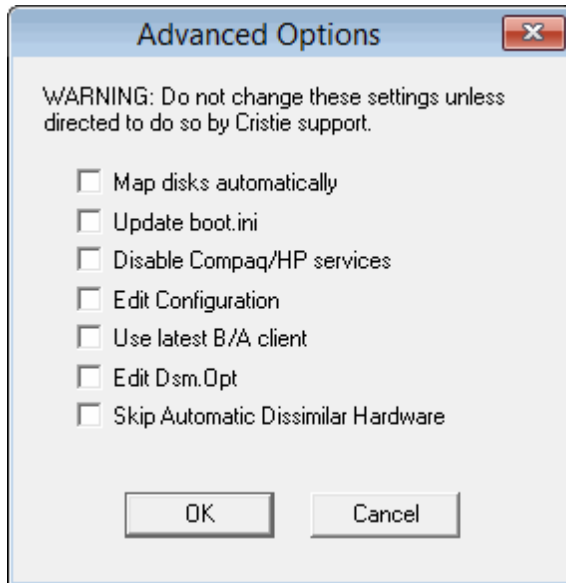
The 'Tracing Levels' dialog box contains a warning at the top: 'Do not set any trace levels unless instructed to do so by Cristie support. Trace levels can seriously affect the performance of the recovery.' Below this, there are two columns of settings, each with a label and a dropdown menu. The settings are as follows:

Trace Level	Value
CAVC Trace Level	3
CCSC Trace Level	3
Avamar Trace Level	
Simpana Trace Level	
CBAC Trace Level	3
CXCC Trace Level	0
DSMC Trace Level	
EFI Trace Level	
CBMC Trace Level	3
CDP Trace Level	3
CRC Trace Level	
CLCC Trace Level	3
SM Trace Level	0
CLC Trace Level	
SDS_TSM Trace Level	0
CNWC Trace Level	3
SDS_SEP Trace Level	0
NetWorker Trace Level	
XBSA Trace Level	0

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

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.




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

6.2.4.1 Cristie Network Configurator Tool

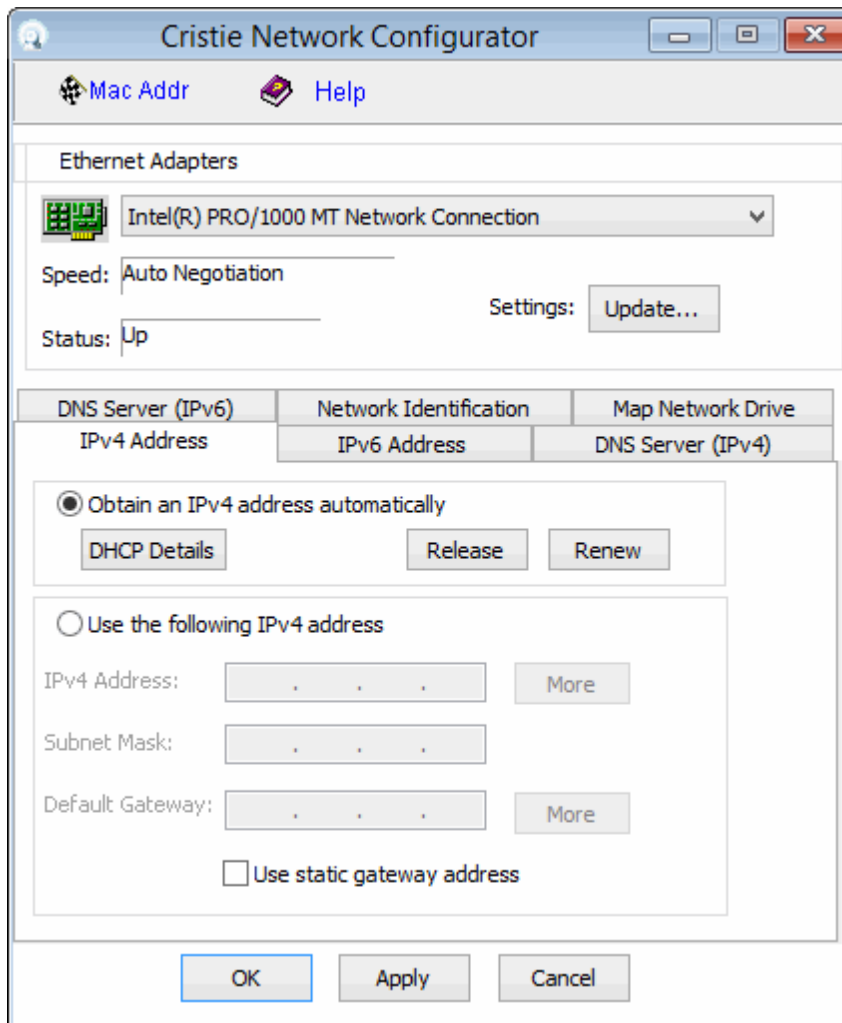
The **Cristie Network Configurator** tool provides extensive facilities to configure the network during the recovery process. It offers the following features:

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

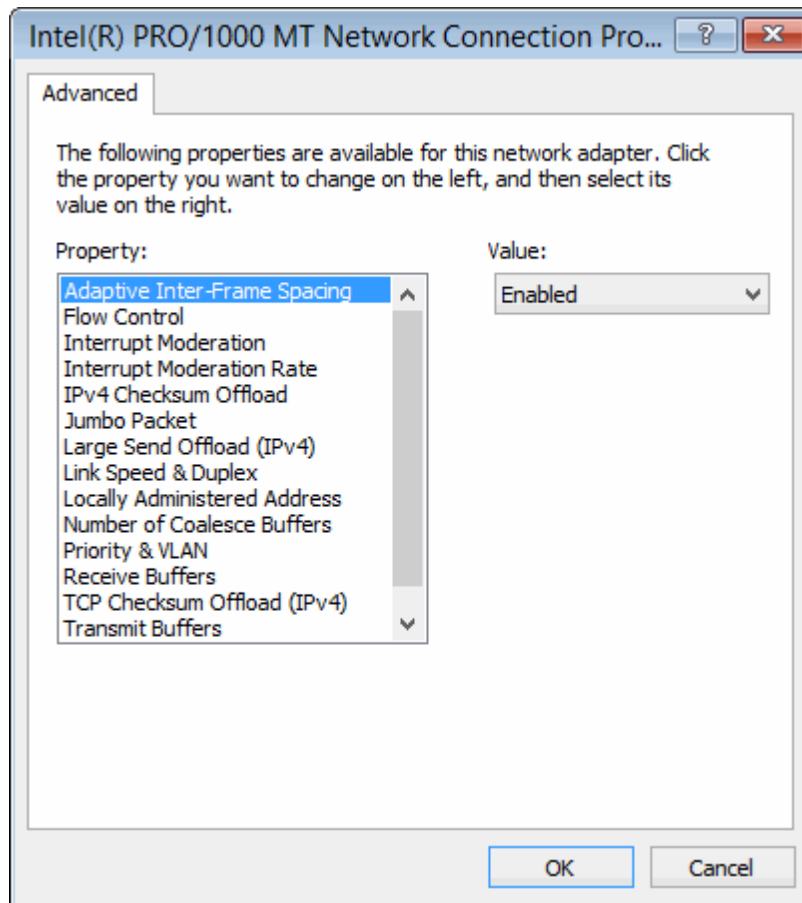
Select the  [Help](#) button at the top of the dialogue to show Network Configurator online help.

Configure NIC Parameters

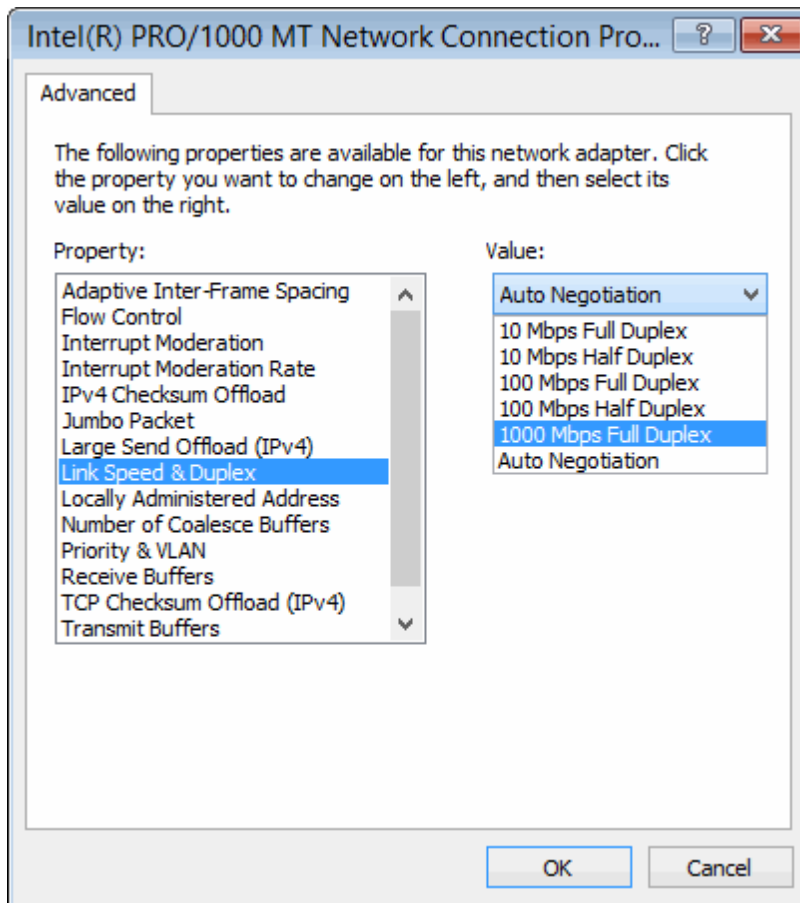
It is possible to change both the link speed and duplex mode for any NIC detected on the recovering target system. Select the desired NIC (there could be more than one) from the drop down box and then select [Update...](#)



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:



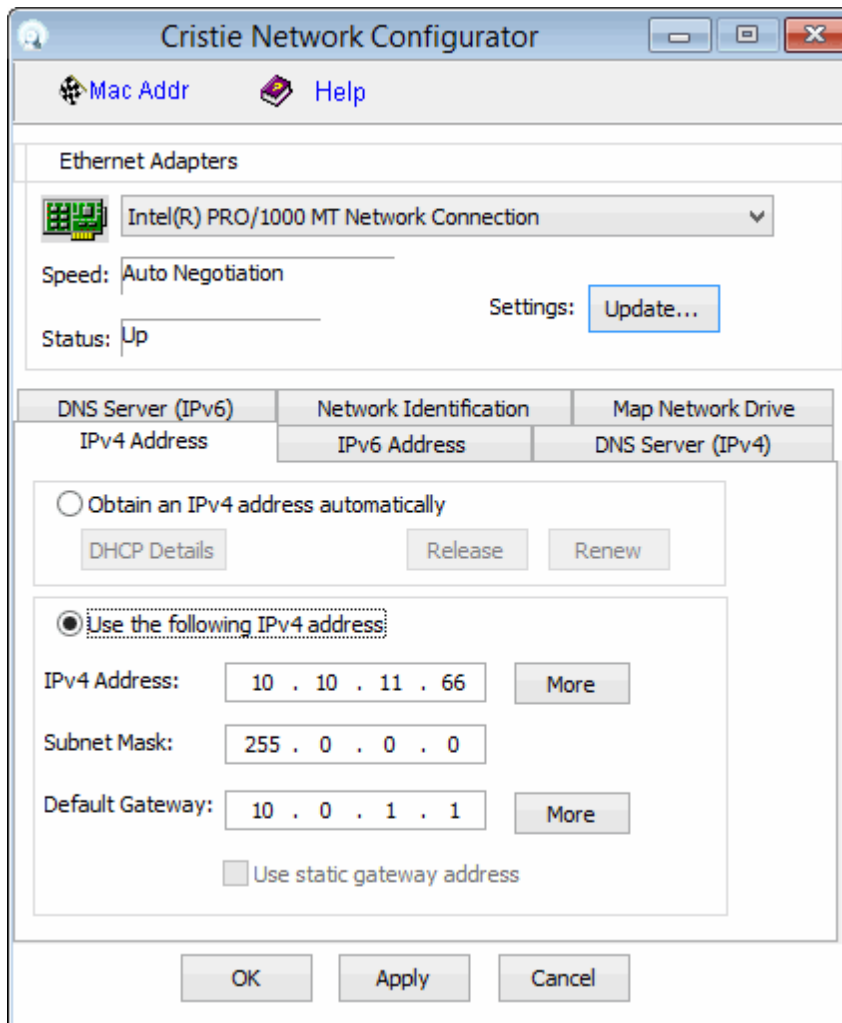
Again, note that the speed/duplex settings available are NIC dependent. *Auto Negotiation* is generally the NIC default setting. Other NIC properties may be changed as required.

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**.

Assign Static or DHCP IP Settings

Normally the WinPE 2 or WinPE 5 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.

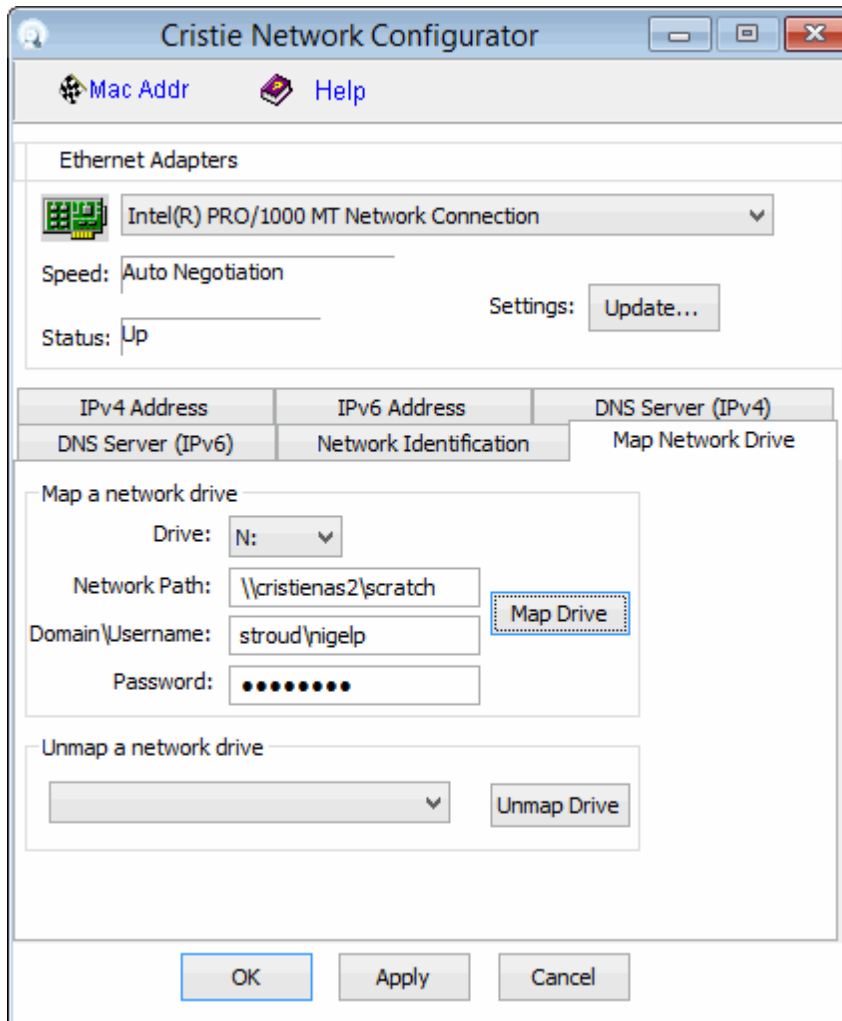


Set the new IP address, subnet mask and gateway IP address. The [More](#) button will allow the system to have more than one static IP address. Click on [Apply](#) to confirm the settings for the selected adapter.

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

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.

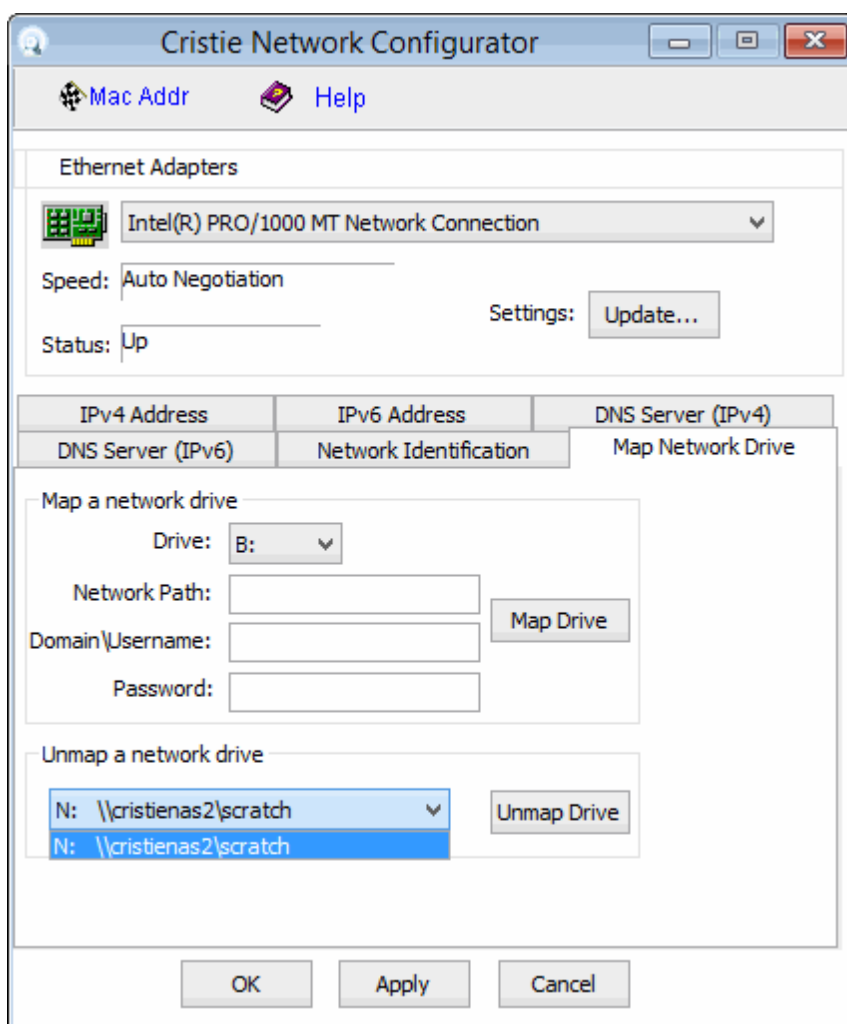


Select the drive letter that you wish to allocate from the **Drive** drop-down box and type in the share name that you wish to associate with it. Also specify the network credentials to be used to access the share.

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

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](#).

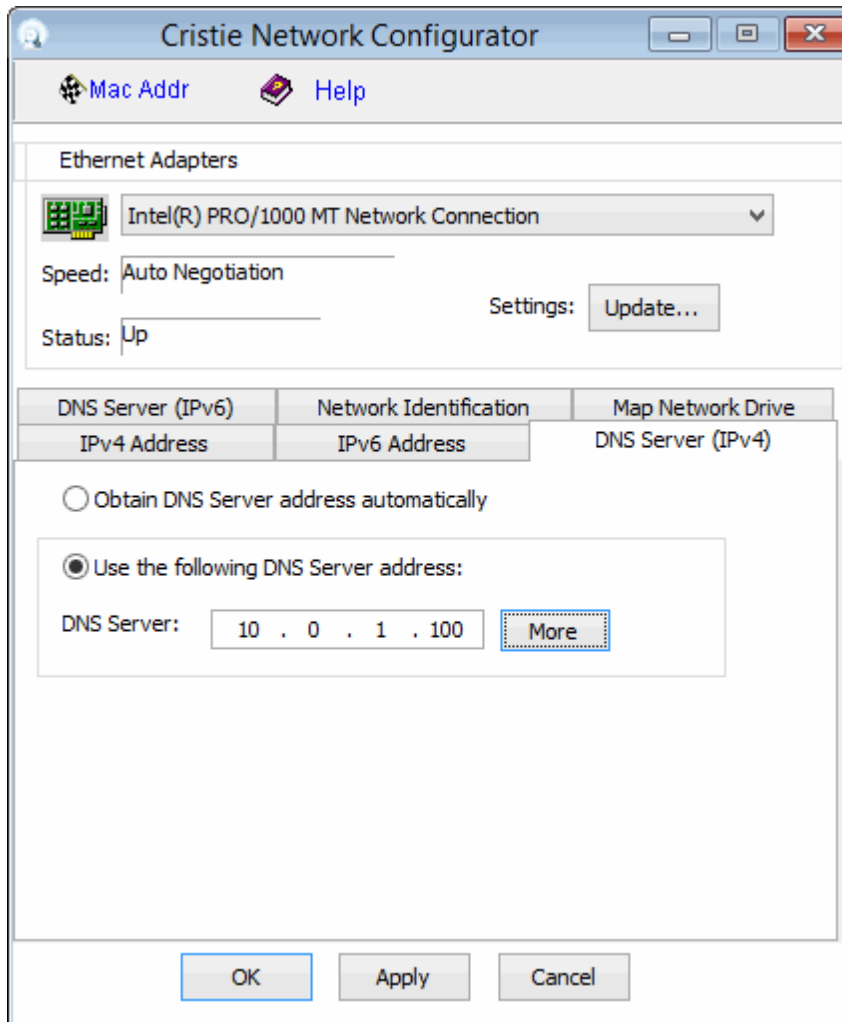


The mapped drive is removed from the list to confirm the operation.

Setup DNS Servers

DNS server IP addresses are automatically set when the WinPE 2 or WinPE 5 DR environment boots. However, options are provided to allow DNS server IP addresses to be manually set if required.

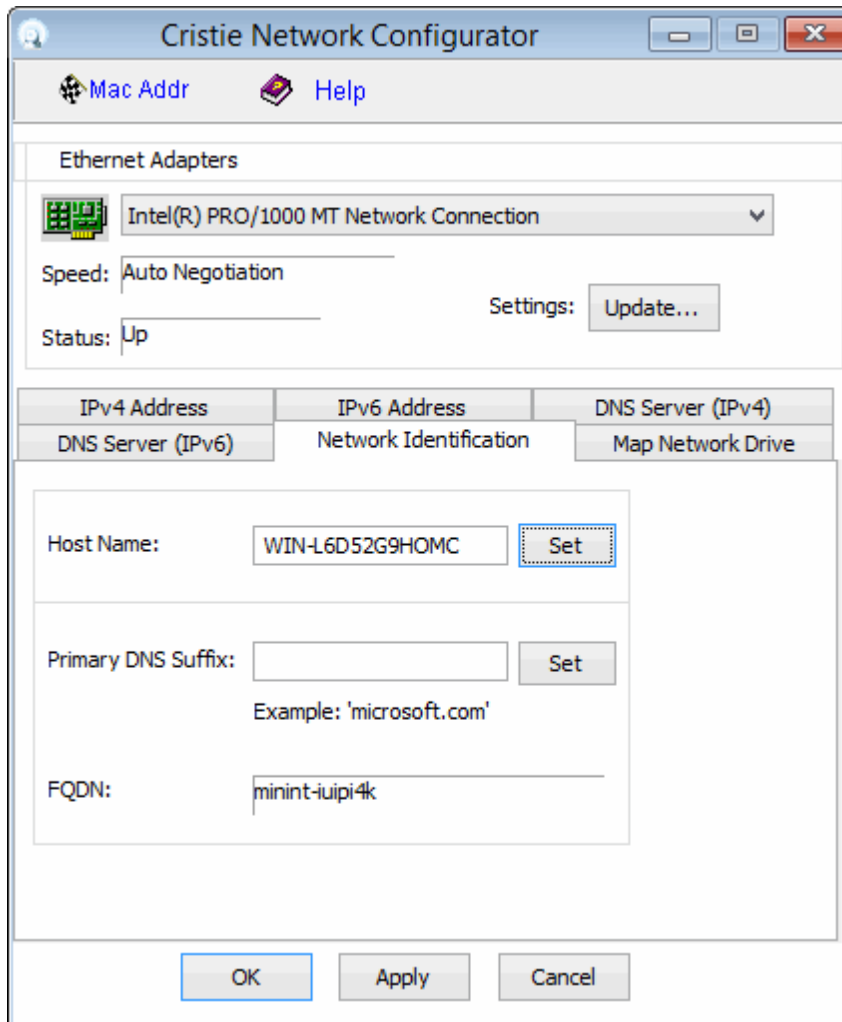
Note: WINS servers are not currently supported by this tool.



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.


Setup Network Identification

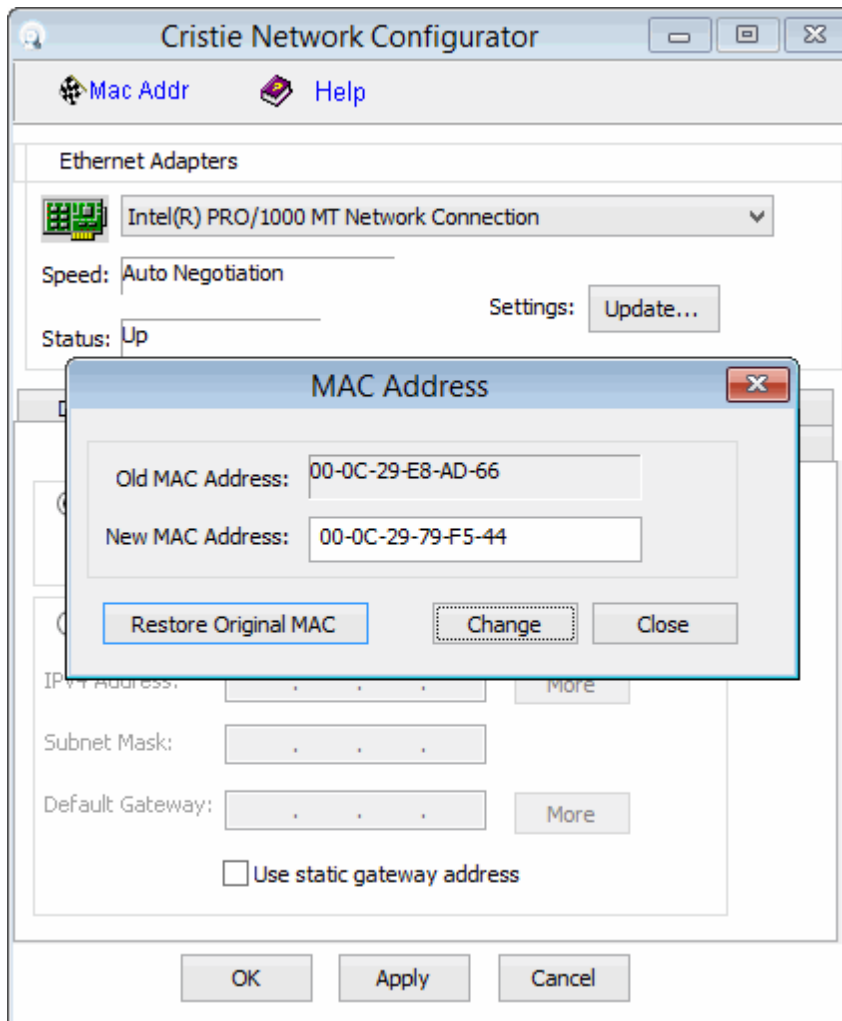
Click the **Network Identification** tab to setup a new hostname for the recovering system. This allows the WinPE 2 or WinPE 5 hostname and Primary DNS suffix to be changed during a DR session if required. These details are transient and only apply only while the WinPE 2 or WinPE 5 DR session is running. They are not applied to the recovered system when it reboots after the DR session.



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

Display/Change MAC Address

It is possible to display and change the local MAC address of the recovering system. Select the MAC Address  [Mac Addr](#) button at the top of the Main menu dialogue:



Change the MAC address by entering a new value in the form xx-xx-xx-xx-xx-xx and selecting [Change](#). The original MAC address will be preserved and can be restored using the [Restore Original MAC](#) button.

6.2.4.2 Dissimilar Hardware Wizard

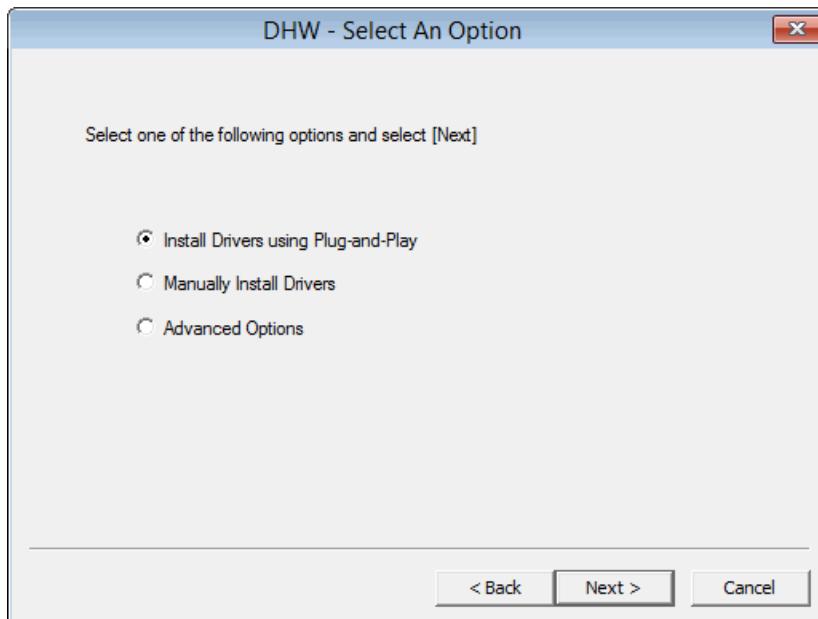
A restore to dissimilar hardware is normally detected during the Automatic or Manual DR sequence. Drivers will be injected automatically at the end of the restore sequence if a source location has been provided. However, if this process has failed for some reason, or additional drivers are required to 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>**.

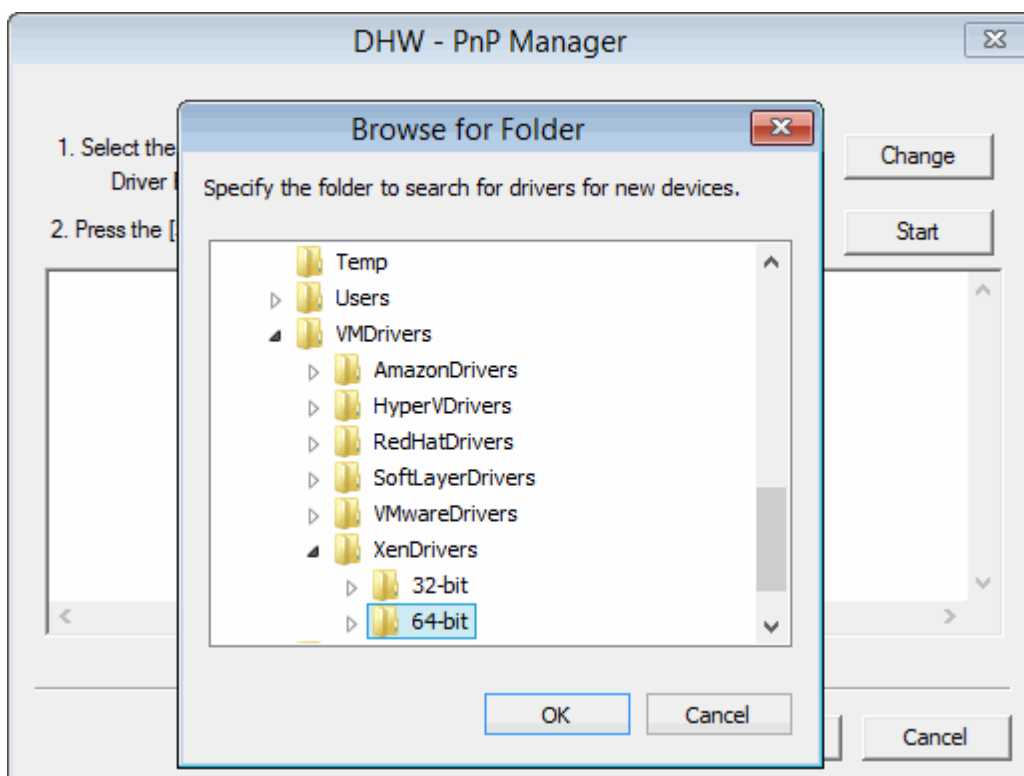


Select the **'Install Drivers using Plug-and-Play'** option:

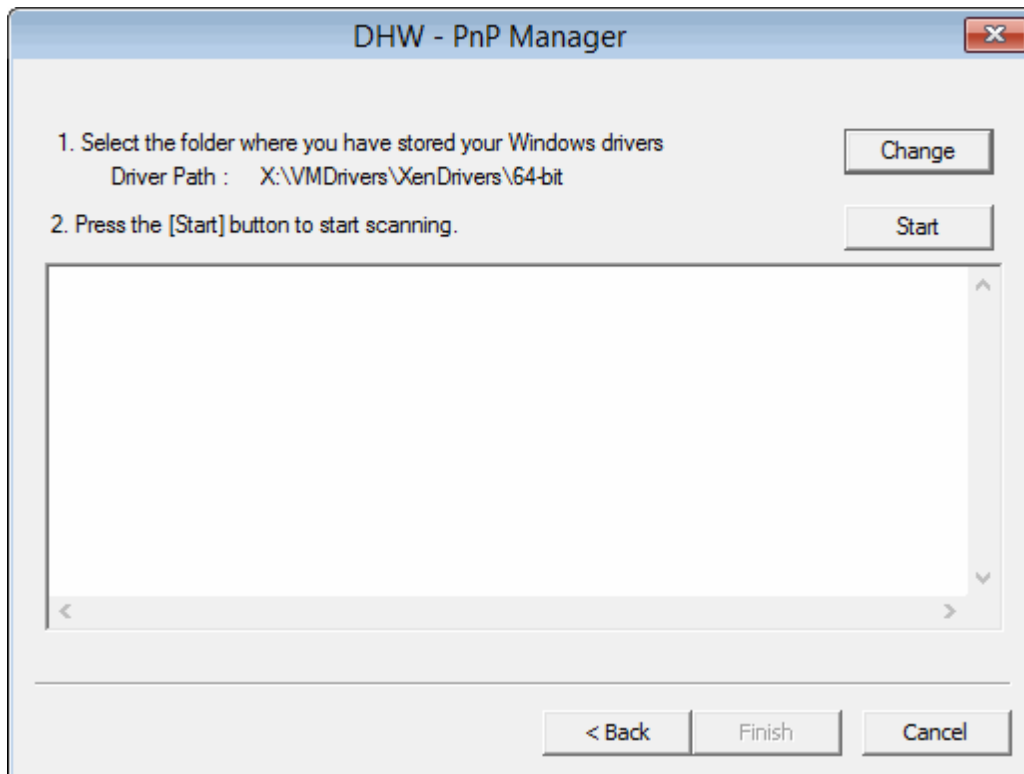


Install Drivers using Plug-and-Play

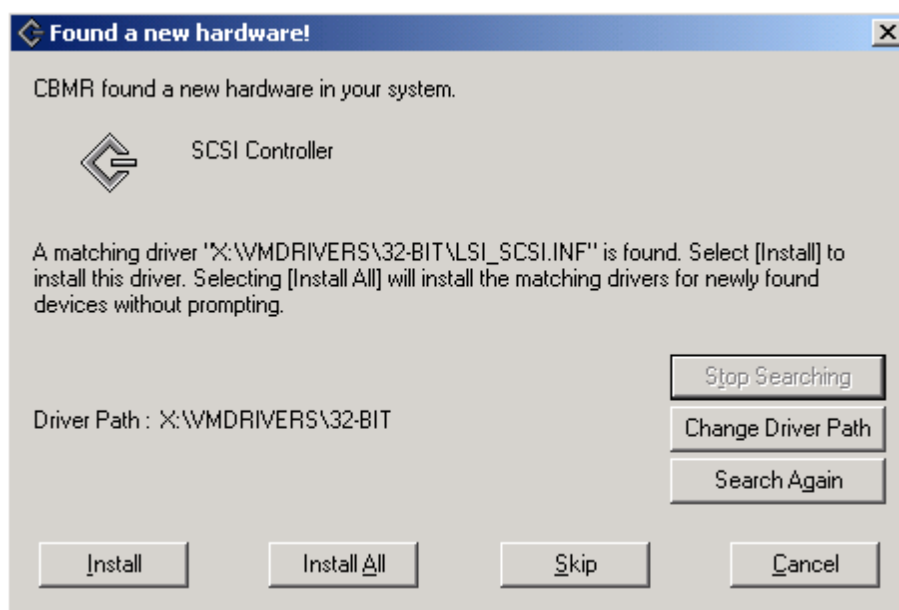
The window appears empty to start with. The set of drivers located on the recovery CD is the default choice, but in practice they should not be used. Instead, change the driver search path to where you have actually located your drivers (for example, to a network share or another CD) with the **Change**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



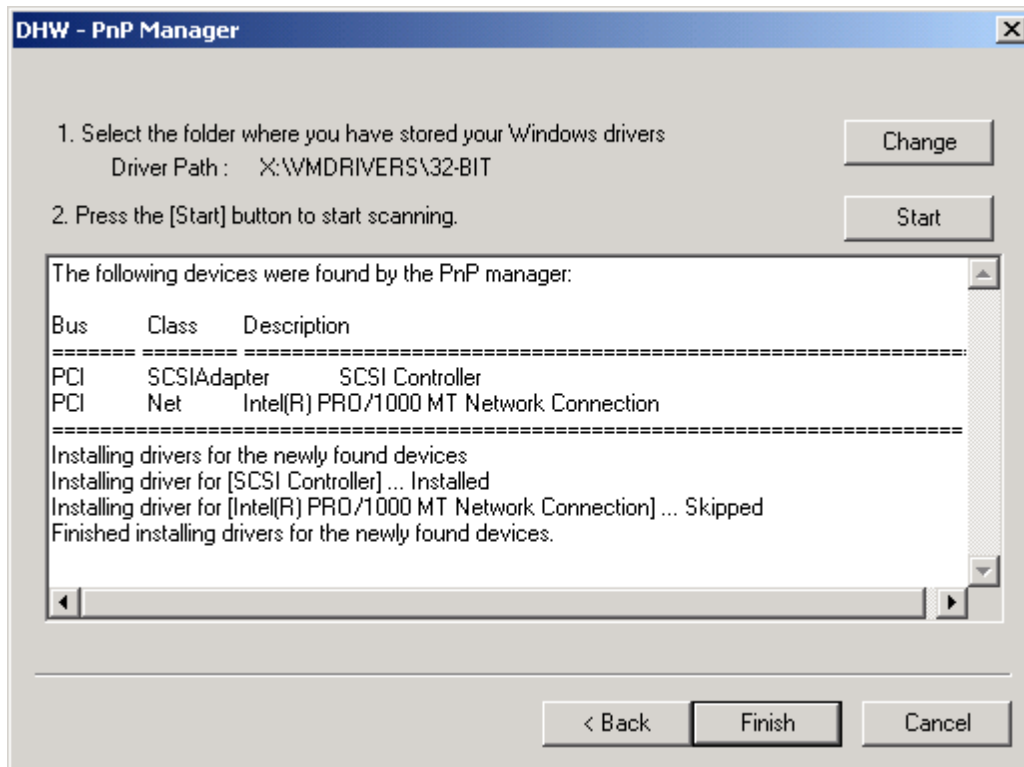
The process checks the devices that it can detect and when it finds one that does not have a driver loaded, it will offer to install it. The example below shows an LSI SCSI device being detected:



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.

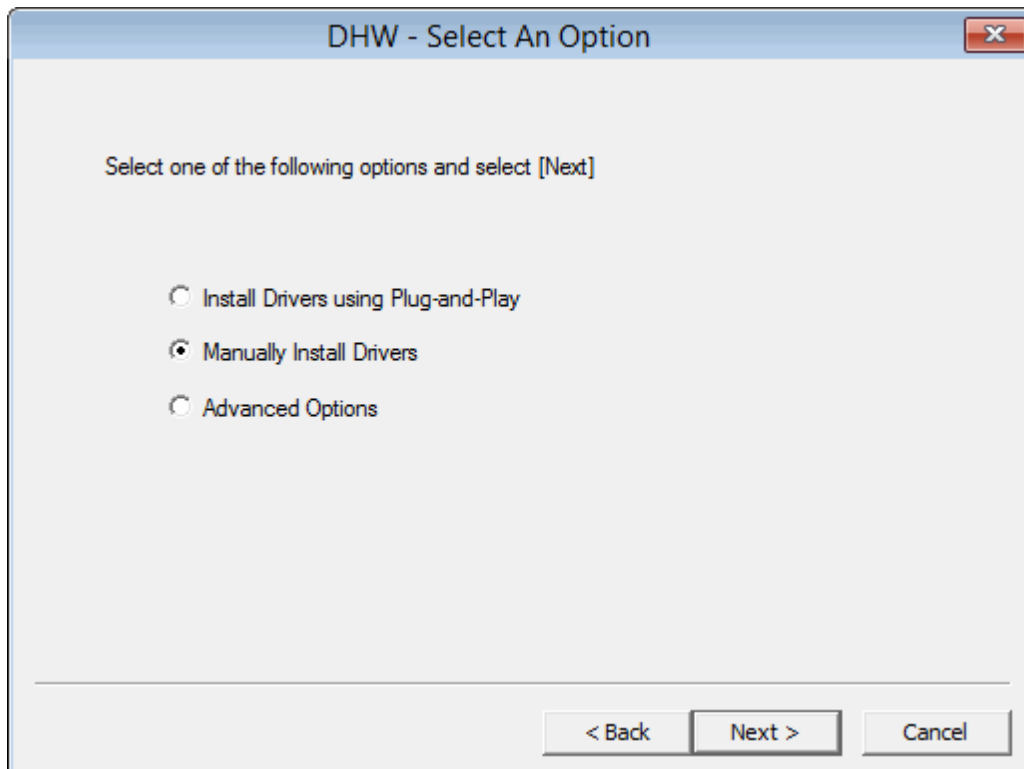
Drivers are usually .sys files. The .inf files define which driver files need to be loaded for a given device. You may need to confirm the location of the driver files for each device, or possibly find the path where they are stored. When you have the correct path, click on [OK](#) and the Wizard will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

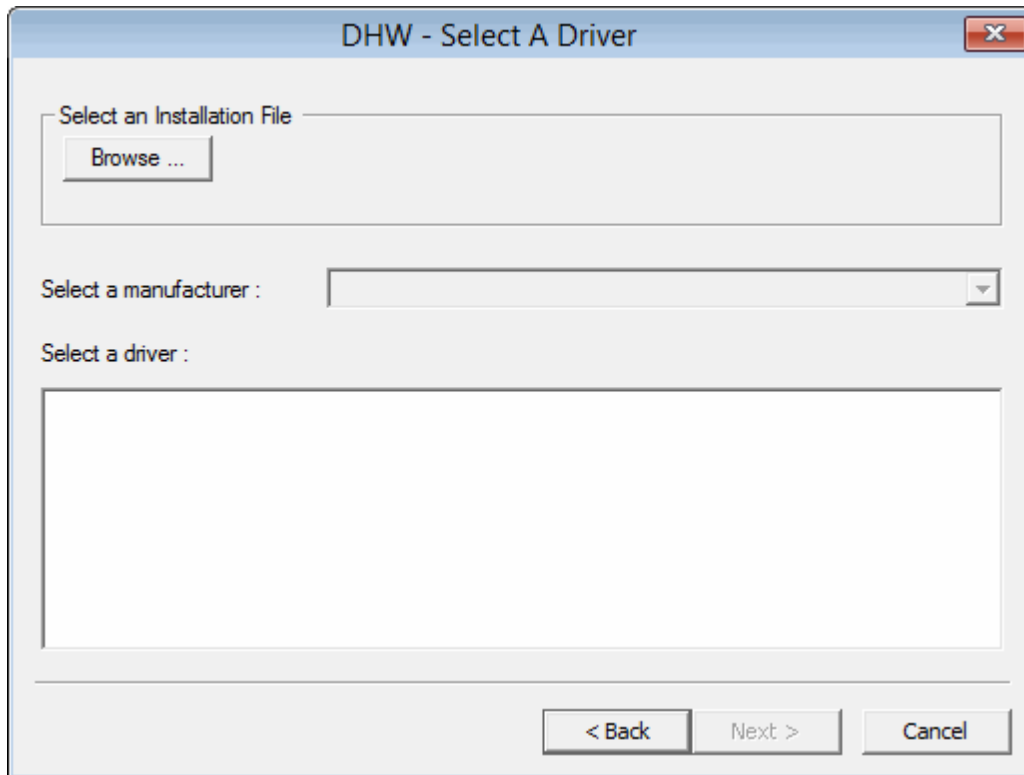


Manual Installation

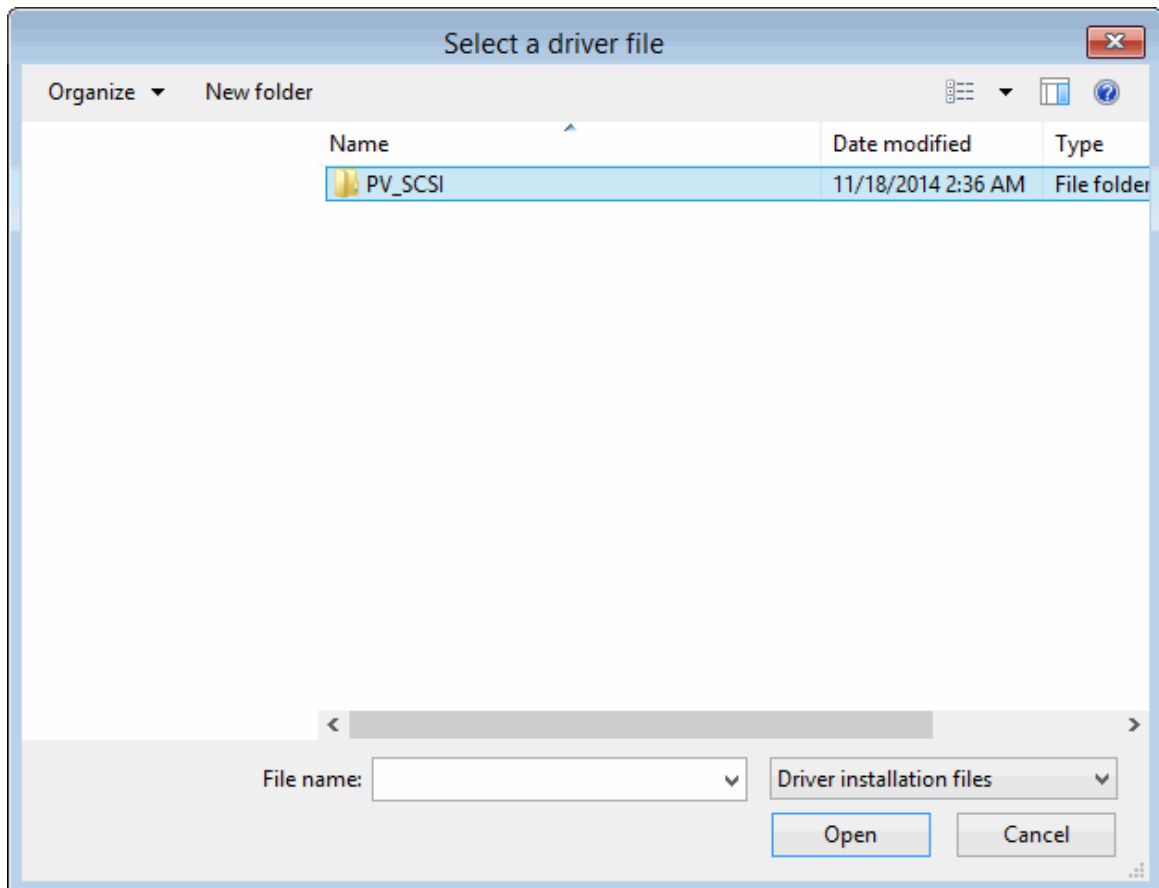
Typically, you would only manually install a driver for a CPU/HAL change. Select '**Manually Install Drivers**' from the option menu:



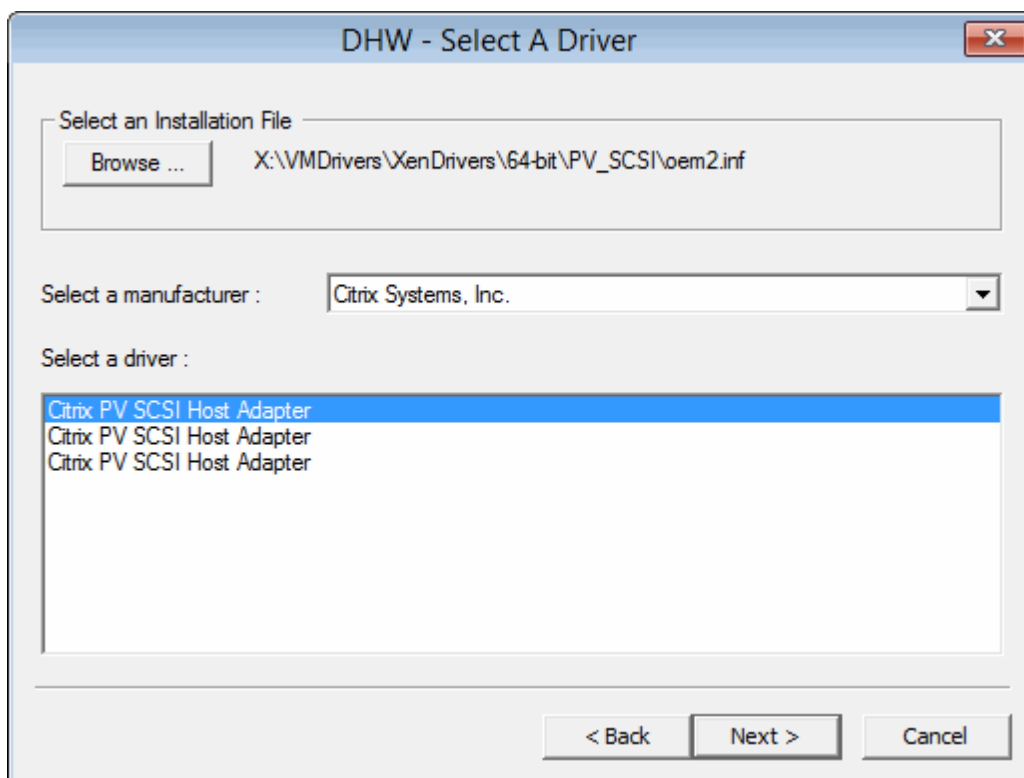
Then select [Next>](#).



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.

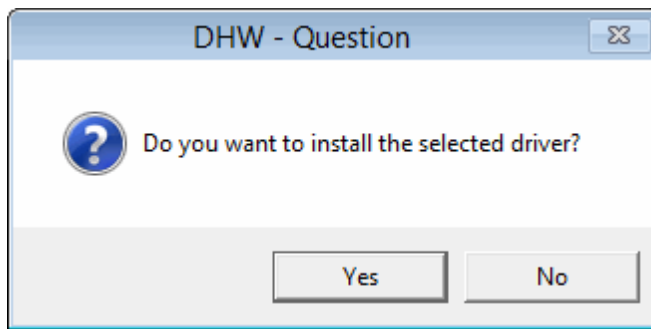


Here we are selecting the Citrix PV SCSI controller driver:



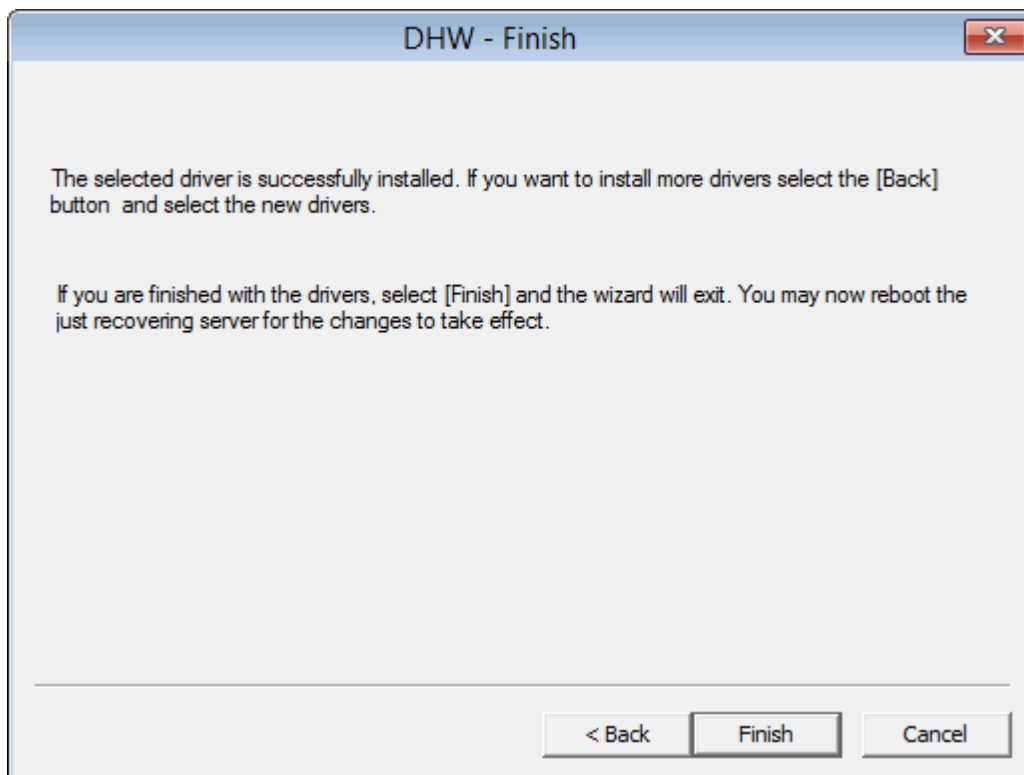
The Wizard allows you to select drivers that are grouped by manufacturer. Select the actual driver

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.

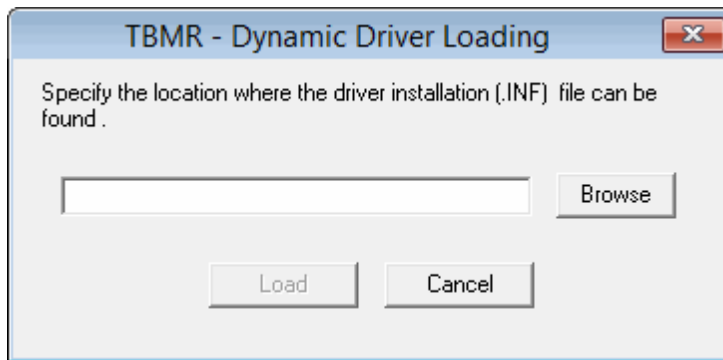


6.2.4.3 Load a Driver

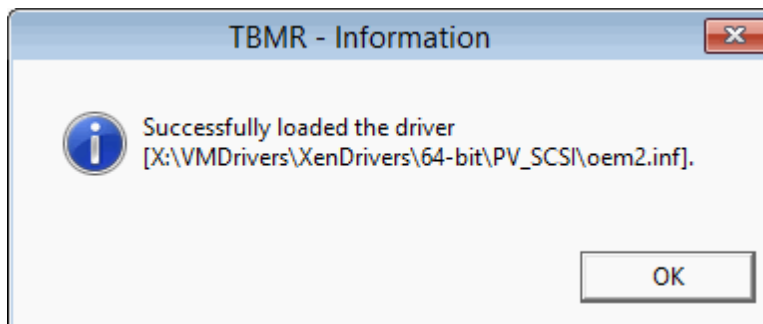
This option allows a **new mass storage** or **Network card driver** to be loaded into the WinPE 2 or WinPE 5 environment. Use this when WinPE 2 or WinPE 5 does not have a built-in driver for your hardware.

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:

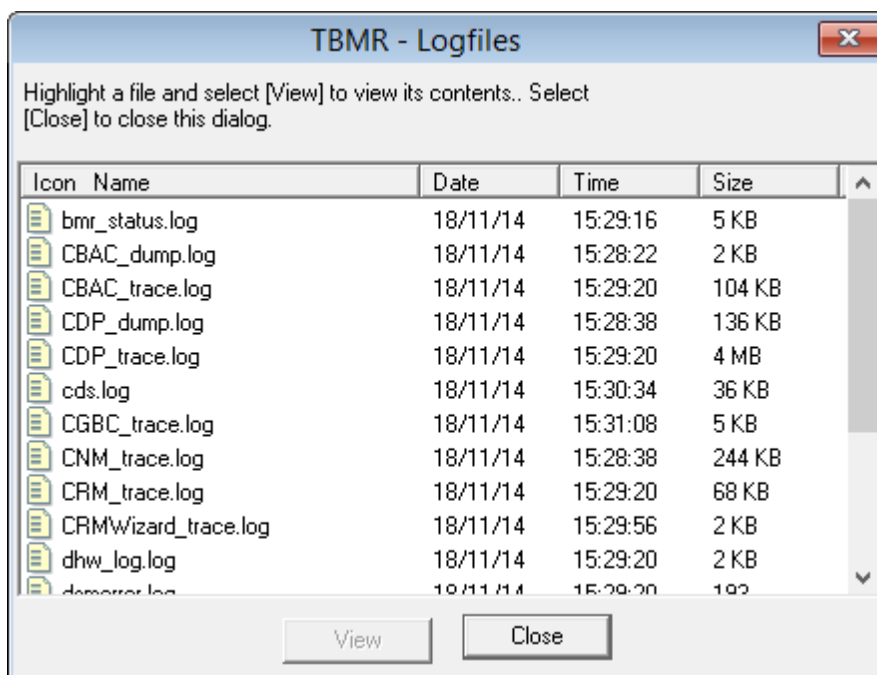


The INF file and other associated driver files (such as the .SYS file) can be located on a CD, USB device or a network share. The following confirmation dialogue is displayed if the driver is loaded successfully:



6.2.5 Show a list of log files for viewing

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.

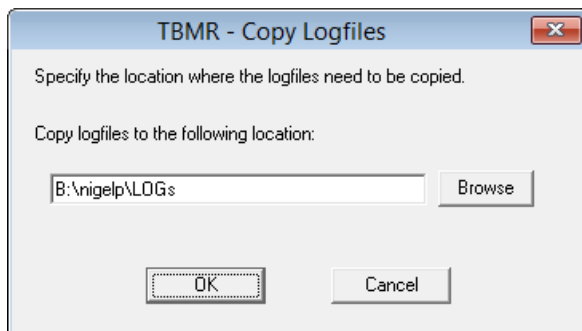


The important files are (this is not an exhaustive list):

6.2.6 Copy log files to removable media or network location

Since all log and error files generated during the recovery are only transitory (ie. they are lost as soon as the Windows WinPE 2 or WinPE 5 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.



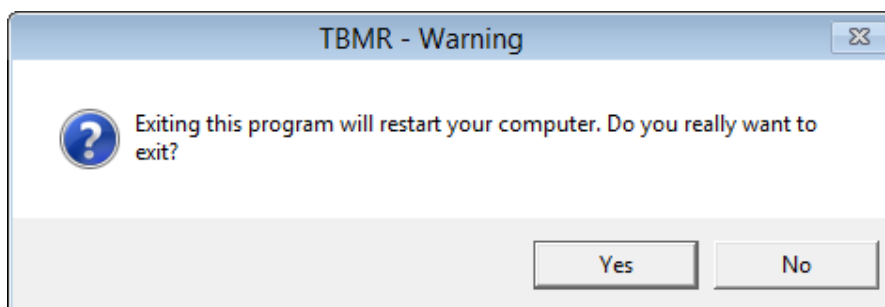
The example shows files being copied to a network share **A:**.

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

6.2.7 Reboot

After a successful recovery, select **Reboot** to exit the Windows WinPE 2 or WinPE 5 environment and boot the recovered system.

Press **Yes** on the confirmation warning to restart or **No** to continue running the DR console. If you choose to reboot, the recovered Windows system will boot into the OS:



7 Appendices

7.1 Windows 8/8.1 Storage Space and 2012/2012R2 Storage Pool Support

On Windows 2012, Windows 2012 R2, Windows 8 and Windows 8.1 based systems that are utilising the Storage Pool/Space feature, TBMR will support the backup of the Storage Pool/Space in a passive manner.

This is achieved by storing all the data contained on the Storage Pool/Space as a single volume, that will then be stored in the backup location, during the process of performing your backup. The actual physical construction of the storage pool/space will not be retained in this process.

The process required to protect the data contained on a Storage Pool/Space will typically consist of the following steps:

1. Create a TBMR backup of the system. (This consists of the local partitions, storage pools and the System State)
2. Recover the backup using the TBMR recovery media, choosing just to recover just the Operating System and associated System State.
3. Reboot the recovered system.

Note: When recovering to the original machine, the Storage Pool/Space should still be available. This enables step 4 below to be skipped.

4. Open Server Manager (Windows 2012/2012 R2) or Control Panel (Windows 8/8.1) and create a Storage Pool/Space. (This does not need to be a replica of the original Storage Pool/Space).
5. Launch TSM and recover the data from the backup location to an available Storage Pool/Space.

7.2 uEFI and MBR BIOS support

Note: No support is provided for conversion from uEFI to MBR BIOS or from MBR BIOS to uEFI.

The recovery ISO is not uEFI enabled. Therefore a successful recovery requires a uEFI environment capable of booting the recovery ISO in MBR BIOS.

Physical machines

There are no special considerations that need to be made by the customer for physical uEFI machines.

All Cristie Bare Metal Recovery software handles the recreation of the uEFI and MSR partitions during the recovery of the physical machine, this is transparent to the user. When recovering a uEFI enabled OS you must recover to uEFI capable hardware.

Virtual machines

Important note: When using virtualisation software check the virtualisation software documentation to determine if uEFI is supported.

To recover to uEFI take the following steps:

1. Once you have a “Recovery Success” message from the TBMR recovery, click Reboot, and then shutdown the recovered VM.
2. Edit the Options of the Virtual Machine, and change the BIOS to be uEFI (instead of the standard MBR BIOS).
3. Once the BIOS has been changed, you will need to boot the VM into the uEFI BIOS using the VM boot options.
4. When recovery is to a different machine, you may need to configure the uEFI boot Stanza in order to boot the recovered uEFI OS. Please refer to the Cristie Knowledgebase for further information on editing the boot Stanza. This consideration applies to Physical and Virtual recoveries.

Once the above steps have been performed, your recovered uEFI OS will boot in your virtualisation software.

8 Cristie Technical Support

If you have any queries or problems concerning your Bare Machine Recovery for TSM 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:

- TBMR 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
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 Limited are continually expanding their product range in line with the latest technologies. Please contact the Cristie Sales Office for the latest product range. Should you have specific requirements for data storage and backup devices, then Cristie's product specialists can provide expert advice for a solution to suit your needs.